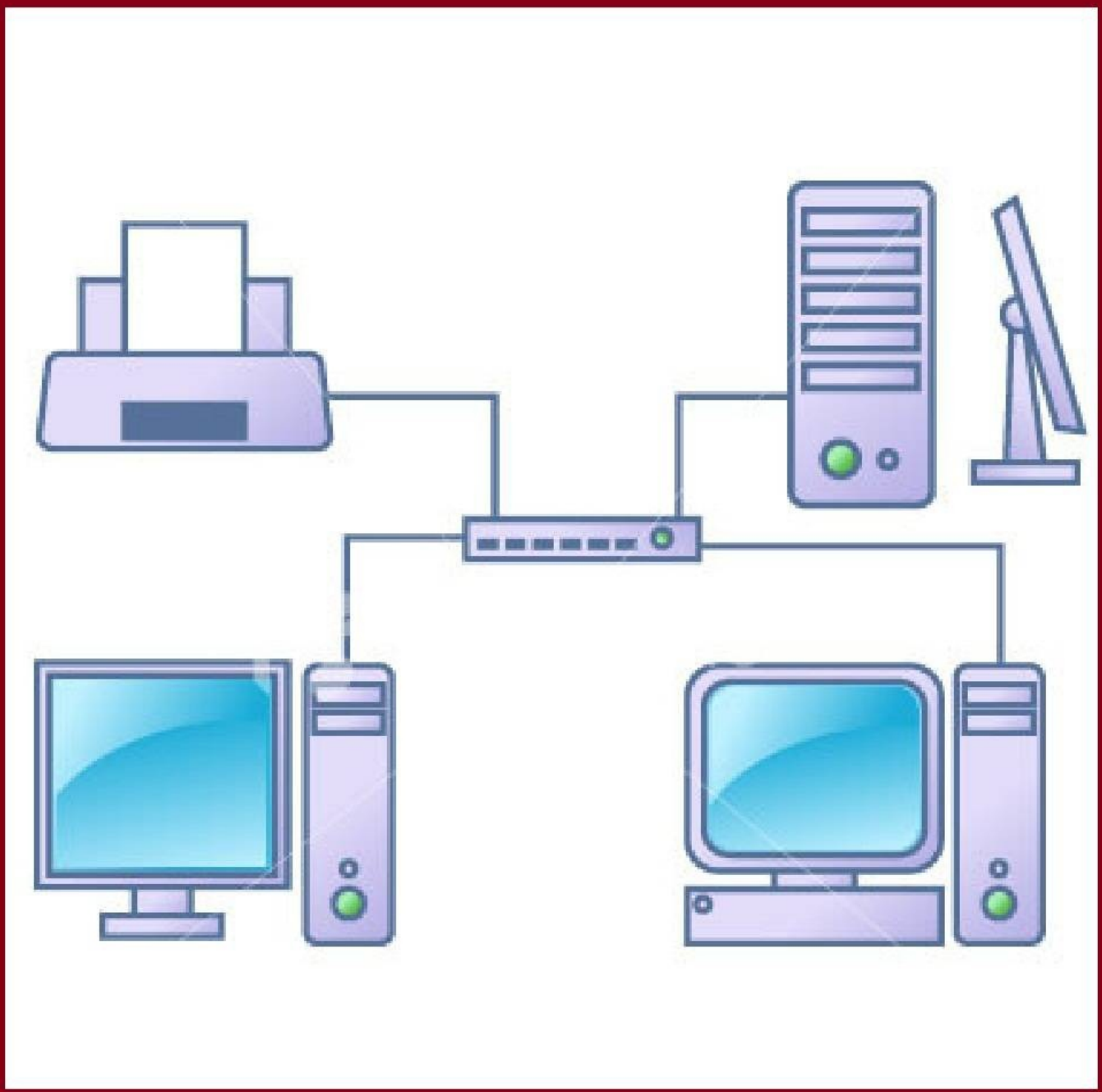
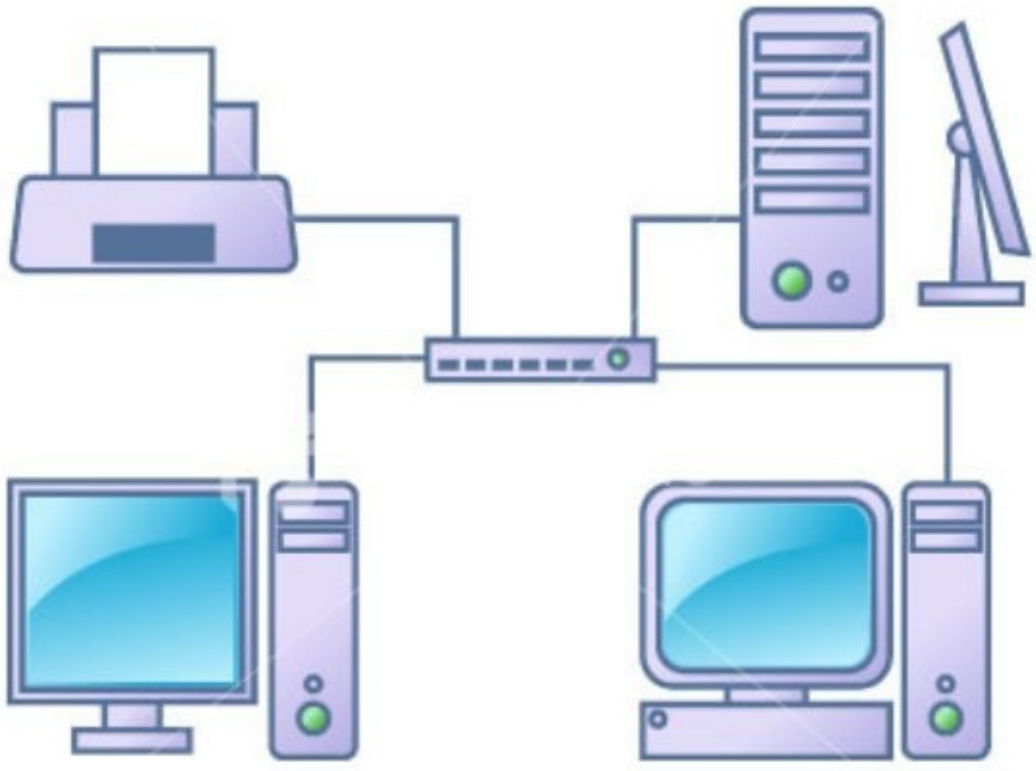
Computer Networking

N.S.REDDY



NEO Institute of Networking Technology

Computer Networking



Theory and Practical

Published by:

®

NEO Publishing House

CONTENTS

THEORY

1. Introduction to Networks, Advantages and Types 5

2. Network Interface Card (NIC) 13
3. Copper Cables 16
4. Optical Fibre Cable (OFC) 18
5. Network Equipment & Standards 19
6. Wireless LAN (Wi-Fi) 31
7. Wireless MAN (Wi-MaX) 37
8. VSAT Technology 40
9. Leased Networks 41
10. Powerline Networks 42

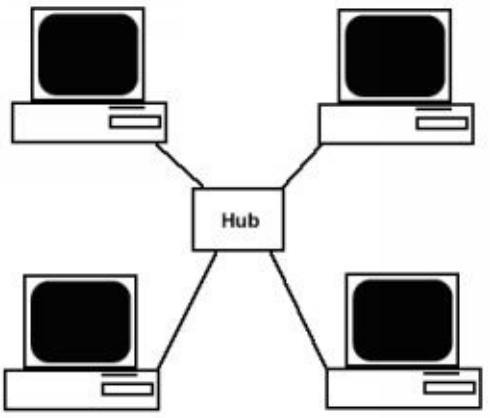
PRACTICAL

1. Cabling, Crimping and Connections 43
2. OSI Model and Network Layers 48
3. Networking using Windows XP 55
4. Introduction to TCP / IP Protocol 64
5. TCP / IP Classes and Addressing 67
6. Internet Connection Sharing in Windows 71
7. Wireless Networking in Windows 74
8. Internet Information Services (FTP & WWW Server) 80
9. Networking using Windows 7 82
10. FTP & WWW Server Services in Windows 7 86

11. TeamViewer

Introduction to Networks and Advantages

Network: Network is a group of two or more computers connected together, for the exchange of data and sharing of resources (such as printers and CD-ROMs).



Advantages and Applications of Networks :

1. Fast Service / Time Saving

   The Information can be synchronized among different computers at a high speed. When one user makes a change to an on-line data other can see the change immediately. (Ex : Reservation Systems, E-Seva, On-Line banking Etc)

2. Information / Data Sharing

   Information or Data can be shared between different departments, organizations and between different places (Data in Organizations, Internet Etc…)

3. High Security

   We can provide security by storing the Data in Server , instead of storing in different Computers (We can protect Data from Modification, Deletion, Theft, fire and floods etc)

4. High Reliability / Easy to Backup

   Data can replicated on two or more Hard Disks or even two or more computers, when one Hard Disk or machine goes down, the other can be used. (We can protect Data from power failures, Hard Disk failures, Heat Problem & Viruses)

5. Resources Sharing

   Hardware resources like Printers, Scanners , CD ROMs ,Floppy Drives, Modems Etc… can be shared to different clients on the Network.

6. Communications

   Communications across the network is cheap and fast (Internet Chatting, E-Mails, Net-to-Phone, Netmeeting Etc…)

7. Software can be shared

   The Application Software installed in the Server can be shared amongst different users, So cost will be reduced.

8. Cost reduced and Easy Maintenance if it is Time Sharing / Thin client Network.

   In Time Sharing Networks Dumb Terminals are used.

   In Thin client network thin clients / thin PC s (Without Hard Disk) are used.

Types of Networks (By Scale)

1. LAN – Local Area Network

Connects a number of computers located geographically close to one another. For example, two computers directly connected to each other can be considered to be a LAN. A corporate network that services multiple adjacent buildings can also be considered as a LAN.

2. WLAN - Wireless Local Area Network

A type of local-area network that uses high-frequency radio waves rather than wires to communicate between nodes.

3. CAN –Campus-Area Networks

A network that connects two or more LANs but that is limited to a specific and contiguous geographical area such **as a college campus**, industrial complex, or a military base. A CAN, may be considered a type of MAN (metropolitan area network), but is generally limited to an area that is smaller than a typical MAN.

4. MAN- Metropolitan Area Network

Connects computers or LANs within the Town / City / Metropolitan area by using Leased / Dedicated lines, ISDN, ADSL (Telephone lines) or Fiber Optic Cables. A MAN typically covers an area of between 5 and 50 km range.

5. WMAN- Wireless Metropolitan Area Network

Connects computers or LANs within the Town City / Metropolitan area by using long range wireless technology called Microwave.

6. WAN- Wide Area Network

Ties / connects together computers or LANs in locations that could be distributed throughout the country or even overseas by using PSTN, ISDN, Fiber Optic Cables. Most WANs comprise a number of LANs connected by long-distance, high-speed data-links.

7. WWAN- Wireless Wide Area Network

Ties / connects together computers or LANs in locations that could be distributed throughout the country or even overseas by using Satellite links.

8. GAN – Global Area Network

Refers to any network that is composed of different interconnected computer networks (WANs) and also covers an unlimited geographical area

9. PAN – Personal Area Network

is a computer network used for communication among computer devices (including telephones and personal digital assistants) close to one person. Personal area networks may be wired with computer buses such as USB, IrDA, Bluetooth and FireWire etc

10. SAN – Storage Area Network

In computing, a **storage area network** (**SAN**) is an architecture to attach remote computer storage devices (such as disk arrays, tape libraries and optical jukeboxes) to servers in such a way that, to the operating system, the devices appear as locally attached. Although cost and complexity is dropping, as of 2007, SANs are still uncommon outside larger enterprises.

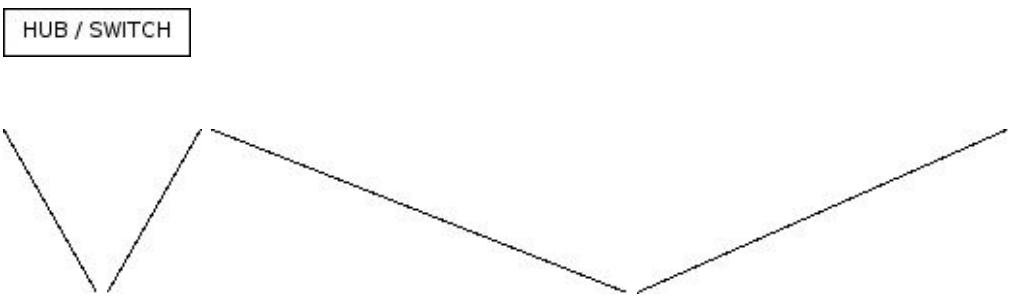
Network Hierarchies (Types by Architecture)

The connections between the various PCs in a network also can fit one of two logical hierarchies. The alternatives form a class system among PCs. Some networks treat all PCs the same; others elevate particular computers to a special, more important role. Although the network server the same role in either case, these two hierarchical systems enforce a few differences in how the network is used.

Peer-to-Peer Networks

Peer-to-Peer means that there is no dedicated file server as you would find in big, complex networks. All PCs can have their own, local storage, and each PC is (or can be) granted access to the disk drives and printers connected to the others. Even in Peer-to-Peer networks, some PCs are likely to be more powerful than others or have larger disk drives or some such distinction.

The advantage of Peer-to-Peer is , no need to by an expensive file server. Not only will that save cash, it can give you the security of redundancy. The failure of a server puts an entire network out of action. The failure of network peer only eliminates that peer; the rest of the network continues to operate. And also we can duplicate the data on two or more peers.

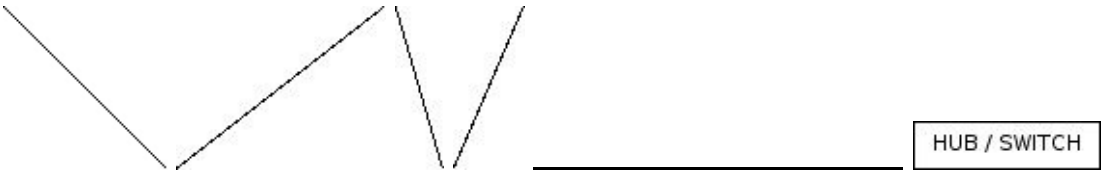


Windows 95 /98 /XP /Vista /7 / 2000 Professional running computers

Client / Server Networks

A Client / Server network provides for centralized control of network resources. One or more computers, called Servers, share the resources on the network. All other computers, called clients or workstations, uses the resources.

Most modern servers are designed to be fault-tolerant. That is, they will continue to run without interruption despite a fault, such as the failure of a hardware subsystem. Most servers also use the most powerful available microprocessors, not from need but because the price difference is tiny once the additional ruggedness and storage are factored in-and because most managers think that the single most important PC in a network should be the most powerful.



WINDOWS 2000/2003/2008 /

UNIX / LINUX SERVER

Clients / Workstations (WINDOWS 98/ XP / Vista / 7)

Peer-to-Peer Networks

(Suitable for Small to Medium Size Organizations)

Advantages :

1. No dedicated server.

2. Less expensive.

3. Easy to install and maintain.

4. Good file, printer, and CD-ROM sharing.

Disadvantages:

1. Slow operation.

2. Not good for database applications.

3. Less reliable (server is workstation).

4. Low Security

5. Limited expandability.

Client / Server Networks

(Suitable for Medium to Large Size Organizations)

Advantages :

1. Fast operation.

2. Expandable.

3. Will work with any application.

4. Handles shared database applications.

5. More reliable (dedicated server).

6. Highest level of security.

7. Applications can be shared.

Disadvantages:

1. Needs dedicated server.

2. More expensive to buy.

3. More expensive to maintain

Internet

The **Internet** is a worldwide, publicly accessible series of interconnected computer networks that transmit data by packet switching using the standard Internet Protocol (IP). It is a "network of networks" that consists of millions of smaller domestic, academic, business, and government networks, which together carry various information and services, such as electronic mail, online chat, file transfer, and the interlinked web pages and other resources of the World Wide Web(WWW).

The Internet is a collection of interconnected *computer networks*, linked by copper wires, fiber-optic cables, wireless connections, etc. In contrast, the Web is a collection of interconnected documents and other *resources*, linked by hyperlinks and URLs. The World Wide Web is one of the services accessible via the Internet, along with many others including e-mail, Usenet, file sharing and others described below.

ICANN

The Internet Corporation for Assigned Names and Numbers (ICANN) is the authority that coordinates the assignment of unique identifiers on the Internet, including domain names, Internet Protocol (IP) addresses, and protocol port and parameter numbers. A globally unified namespace (i.e., a system of names in which there is one and only one holder of each name) is essential for the Internet to function. ICANN is headquartered in Marina del Rey, California, but is overseen by an international board of directors drawn from across the Internet technical, business, academic, and non-commercial communities.

Common Uses of Internet

1. EMAIL
2. World wide Web
3. Remote Access
4. Collabortion
5. File Sharing
6. Streaming Media
7. Voice Telephone (VoIP)

Intranet

An intranet is a set of interconnected networks, using the Internet Protocol and uses IP-based tools such as web browsers, that is under the control of a single administrative entity. That administrative entity closes the intranet to the rest of the world, and allows only specific users. Most commonly, an intranet is the internal network of a company or other enterprise.

Extranet

An extranet is a private network that uses Internet protocols, network connectivity, and possibly the public telecommunication system to securely share part of an organization's information or operations with suppliers, vendors, partners, customers or other businesses. An extranet can be viewed as part of a company's intranet that is extended to users outside the company, usually via the Internet.

Network Topologies

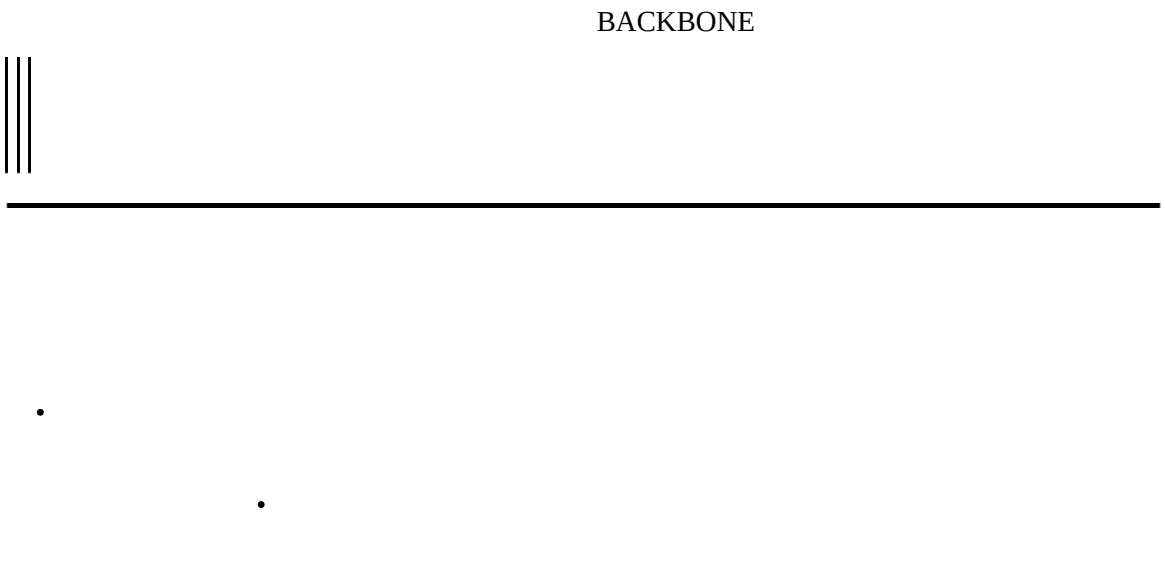
Topology: The geometrical arrangement of a computer systems in a network.

Topology refers to the shape of a network, or the network's layout. How different nodes in a network are connected to each other and how they communicate are determined by the network's topology.

Common topologies include a Bus, Star , Ring.

BUS / Linear Topology

The network with linear cabling has a single backbone, one main cable that runs from one end of the system to the other. Along the way, PCs tap into this backbone to send receive signals, the PCs link the backbone with a single cable through which they both send and receive. In effect, the network backbone functions as a data bus, and this configuration is often called as bus topology. Below is an illustration of a simple bus network.



In the typical installation a wire leads from the Pc to the backbone, and a T-Connector links the two. The network backbone has definite beginning and end. In most cases, these ends are terminated with a resister matching the characteristics impedance of the cable in the background. That is, a 50 ohm network cable will have a 50 ohm termination at either end. These termination prevent signals from reflecting from the ends of the cable, helping assure signal integrity.

Advantages of a Linear / Bus Topology

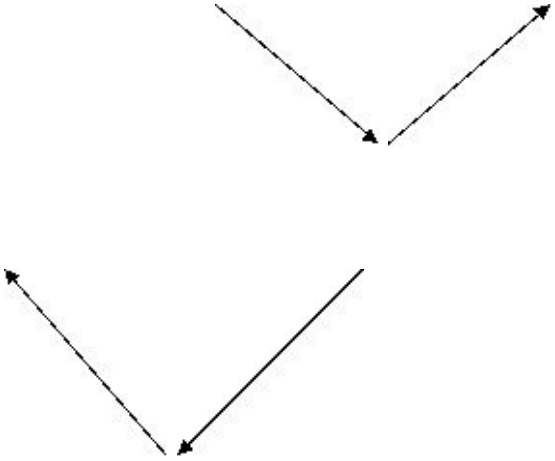
- Easy to connect a computer or peripheral to a linear bus.
- Requires less cable length than a star topology.

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.

Ring Topology

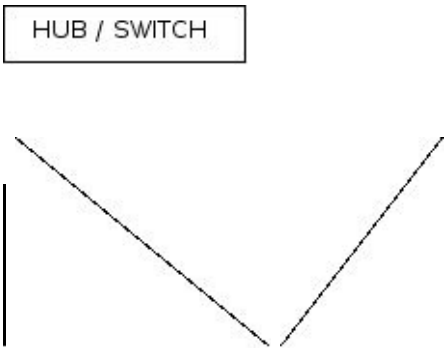
The ring topology looks like a linear network that biting its own tail. The backbone is continues loop, a ring , with no end. But the ring is not a single, continues wire. Instead it is made of short segments daisy chained from one PC to the next, the last connected, in turn, to the first. Each PC thus has two connections. One wire connect a PC to the PC before it in the ring, and a second wire leads to the next PC in the ring.



Signals must traverse through one PC to get to the next, and the signals typically or listed to and analyzed along the way.

Star Topology

In the star topology connecting cables emanate from a centralized location called a Hub, and each cable links a single PC in to the network. In the most popular network systems based on the star topology, each cable is actually twofold. Each has two distinct connections, one for sending data from the Hub to an individual PC and one for the PC to send data back to the Hub. These paired connections are typically packaged in to a single cable.



.

Advantages of a Star Topology

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

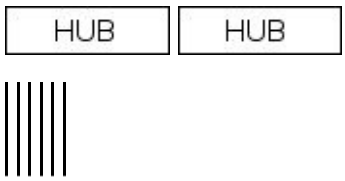
Disadvantages of a Star Topology

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

Hybrid (BUS + STAR) Topology

STAR TOPOLOGY

BUS TOPOLOGY



STAR TOPOLOGY STAR TOPOLOGY

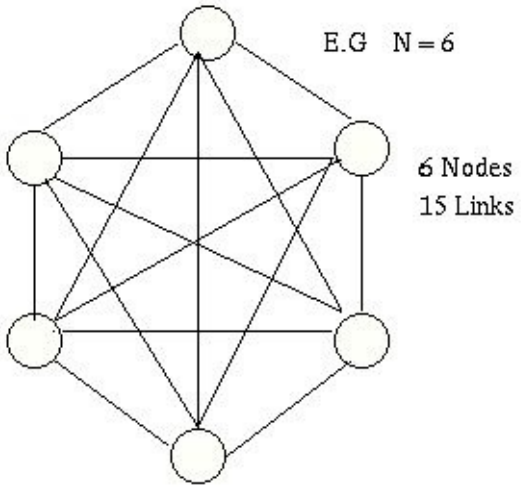
Tree Topology

Mesh / Fully Connected:

The type of network topology in which each of the nodes of the network is connected to

each of the other nodes in the network with a point-to-point link – this makes it possible for data to be simultaneously transmitted from any single node to all of the other nodes.

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.



Network hardware

Networks are made up of both hardware and software. The network hardware provides the physical connections between the network's various nodes and typically includes:

Network Interface Cards (NICs), one for each PC

Network devices such as hubs, bridges, routers and switches, that are together responsible for connecting the various segments of a network and for ensuring that packets of information are sent to the intended destination

Network cables (sheathed copper wiring like telephone cords) which connect each NIC to the hub or switch.

A file server stands at the heart of most networks. It is a very fast computer with a large amount of RAM and storage space, along with a fast network interface card. The network operating system software resides on this computer, along with any software applications and data files that need to be shared.

Workstations

All of the user computers connected to a network are called workstations. A typical workstation is a computer that is configured with a network interface card, networking software, and the appropriate cables. Workstations do not necessarily need floppy disk drives because files can be saved on the file server. Almost any computer can serve as a network workstation.

NICs

Network interface cards, commonly referred to as NICs, are used to connect a PC to a network. The NIC provides a physical connection between the networking medium and the computer's internal bus, and is responsible for facilitating an "access method" to the network (OSI Layers 1 and 2).

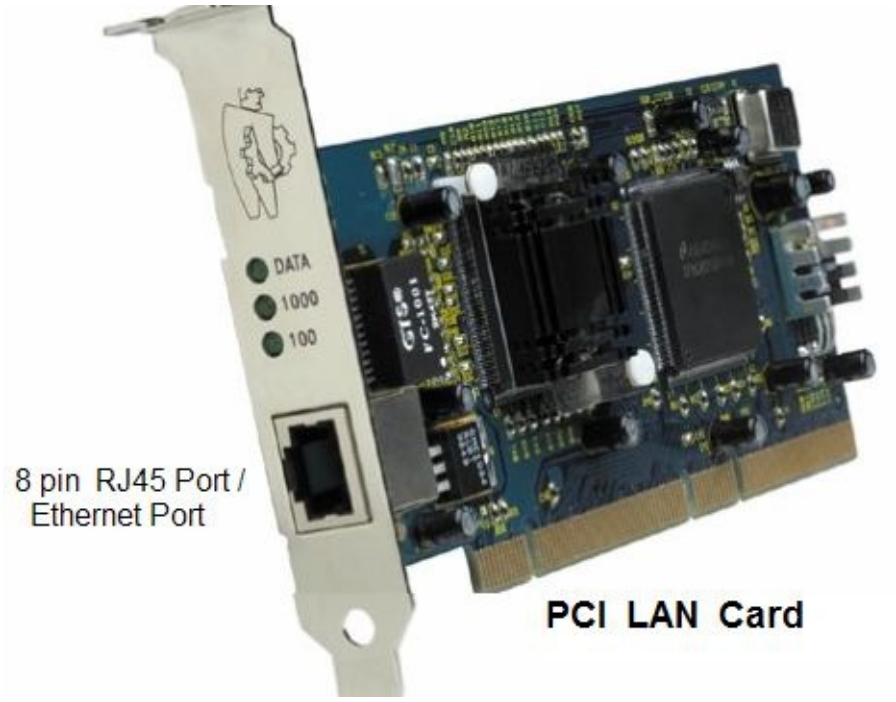
Most NICs are designed for a particular type of network, protocol, and media, although some can serve multiple networks. Cards are available to support almost all networking standards, including the latest Fast Ethernet environment. Fast Ethernet NICs are often 10/100/1000 Mbps capable, and will automatically set to the appropriate speed. Full-duplex networking is another option, where a dedicated connection to a switch allows a NIC to operate at twice the speed.

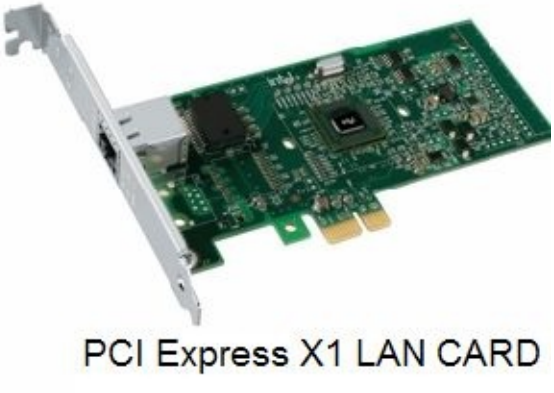
Types (By speed):

1. Arcnet - 2Mbps
2. Ethernet - 10Mbps

3. Fast Ethernet - 100Mbps
4. Gigabit (Gb) Ethernet - 1000Mbps /1Gbps

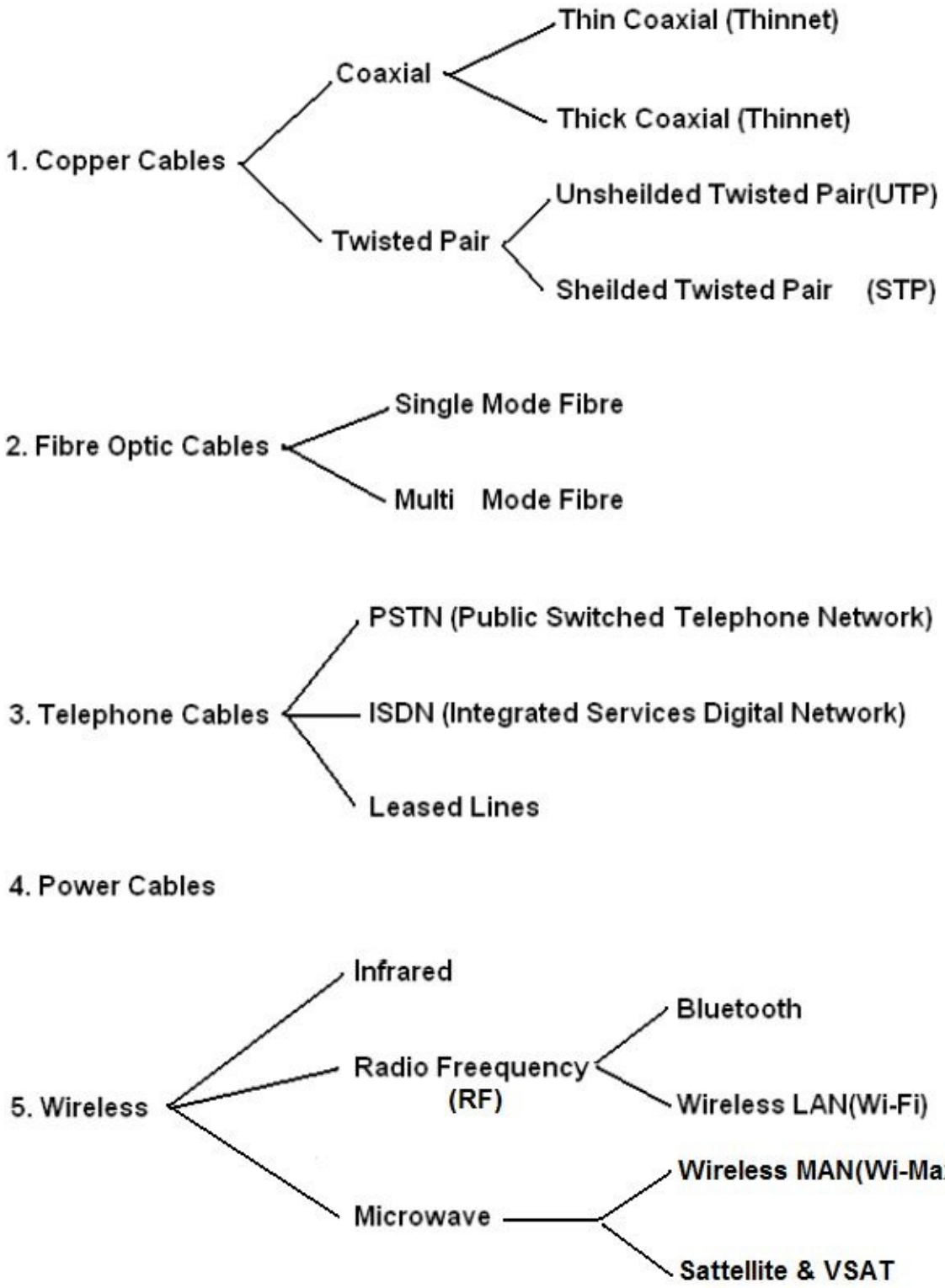
Types (By Architecture)





Network Media

The network media is the device that physically carries the data from computer to computer, the three major types of network media are:



Copper Cables

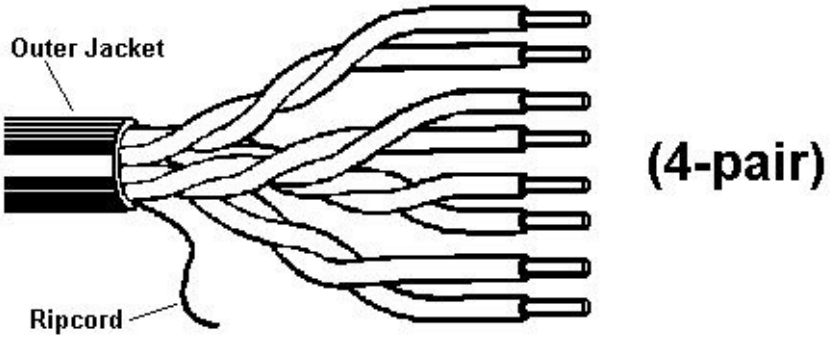
Coaxial Cable

Thinnet (10Base2)- Thinnet uses a British Naval Connector (BNC) on each end. Thinnet is part of the **RG-58** family of cable*. Maximum cable length is 185 meters. Transmission speed is 10Mbps. Thinnet cable should have 50 ohms impedance and its

terminator has 50 ohms impedance. A T or barrel connector has no impedance.

Thicknet (10base5) - Half inch rigid cable. Maximum cable length is 500 meters. Transmission speed is 10Mbps. Expensive and is not commonly used. (**RG-11 or RG-8)**. A vampire tap or piercing tap is used with a transceiver attached to connect computers to the cable. 100 connections may be made. The computer has an attachment unit interface (AUI) on its network card which is a 15 pin DB-15 connector. The computer is connected to the transceiver at the cable from its AUI on its network card using a drop cable. (RG – Radio guide)

Twisted pair - Wire is twisted to minimize cross talk interference.



Twisted Pair Cable Categories

Type	**Characteristics**
Category 1	Used for telephone communications and is not suitable for transmitting data
Category 2	Capable of transmitting data at speeds up to 1Mbit/s.
Category 3	Used in 10BaseT networks and capable of transmitting data at speeds up to 16Mbit/s.

Category 4	Used in Token Ring networks and capable of transmitting data at speeds up to 20Mbit/s.
Category 5	Capable of transmitting data at speeds up to 100Mbit/s.
Category 6	Two pair with foil and braided shield Capable of transmitting data at speeds up to 1000Mbit/s.
Category 7	Un defined
Category 8	Flat cable for under carpets with two twisted pair
Category 9	Plenum cable with two twisted pair. It is safe if you’re having a fire.

UTP-Unshielded Twisted Pair.

Normally UTP contains 8 wires or 4 pair. 100 meter maximum length.

4-100 Mbps speed.

Unshielded twisted pair (UTP)

STP-Shielded twisted pair.

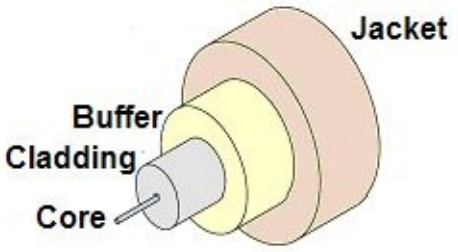
100 meter maximum length.

16-155 Mbps speed. Lower electrical interference than UTP.

Optical Fiber Cable (OFC)

Fiber optic cable consists of thin glass filaments that transmit light waves carrying very large amounts of data for very long distances. Since signals are transmitted with the use of light waves, electromagnetic and radio frequency interference (EMI / RFI) is nonexistent. Lightning and high voltage interference is also eliminated. A fiber network is best for conditions where EMI / RFI interference is heavy or where safe operation free from sparks and static is a must. Fiber optic cable also offers added security because transmissions are safe from electronic eaves - dropping.

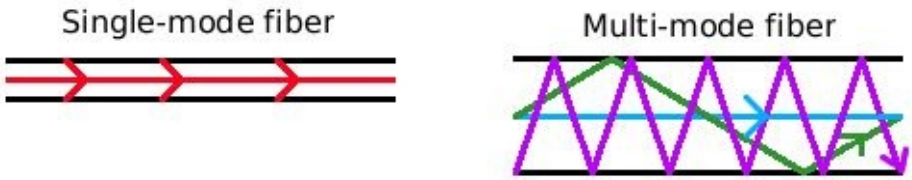
Data is transmitted using light rather than electrons. Usually there are two fibers, one for each direction. Cable length of 2 Kilometers. Speed from 100Mbps to 2Gbps. This is the most expensive and most difficult to install, but is not subject to interference. Two types of cables are:



1. Single mode cables for use with lasers.
2. Multimode cables for use with Light Emitting Diode (LED) drivers.

The simplest type of optical fiber is called **single-mode**. It has a very thin core about 5-10 microns (millionths of a meter) in diameter. In a single-mode fiber, all signals travel straight down the middle without bouncing off the edges (red line in diagram). Cable TV, Internet, and telephone signals are generally carried by single-mode fibers, wrapped together into a huge bundle. Cables like this can send information over 100 km (60 miles).

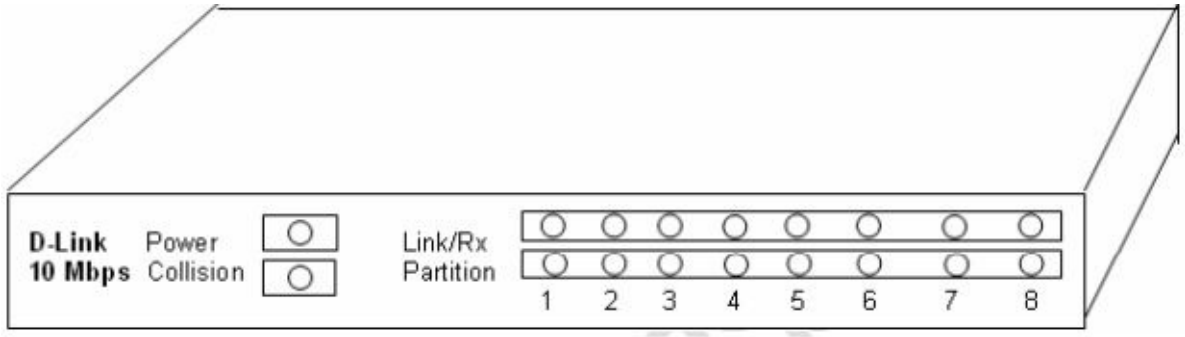
Another type of fiber-optic cable is called **multi-mode**. Each optical fiber in a multi-mode cable is about 10 times bigger than one in a single-mode cable. This means light beams can travel through the core by following a variety of different paths (purple, green, and blue lines) – in other words, in multiple different modes. Multi-mode cables can send information only over relatively short distances and are used (among other things) to link computer networks together.



Network Equipment

Hubs / Repeaters

Hubs/repeaters are used to connect together two or more network segments of any media type. In larger designs, signal quality begins to deteriorate as segments exceed their maximum length. Hubs provide the signal amplification required to allow a segment to be extended a greater distance. Passive hubs simply forward any data packets they receive over one port from one workstation to all their remaining ports. Active hubs, also sometimes referred to as “multi port repeaters”, regenerate the data bits in order to maintain a strong signal.



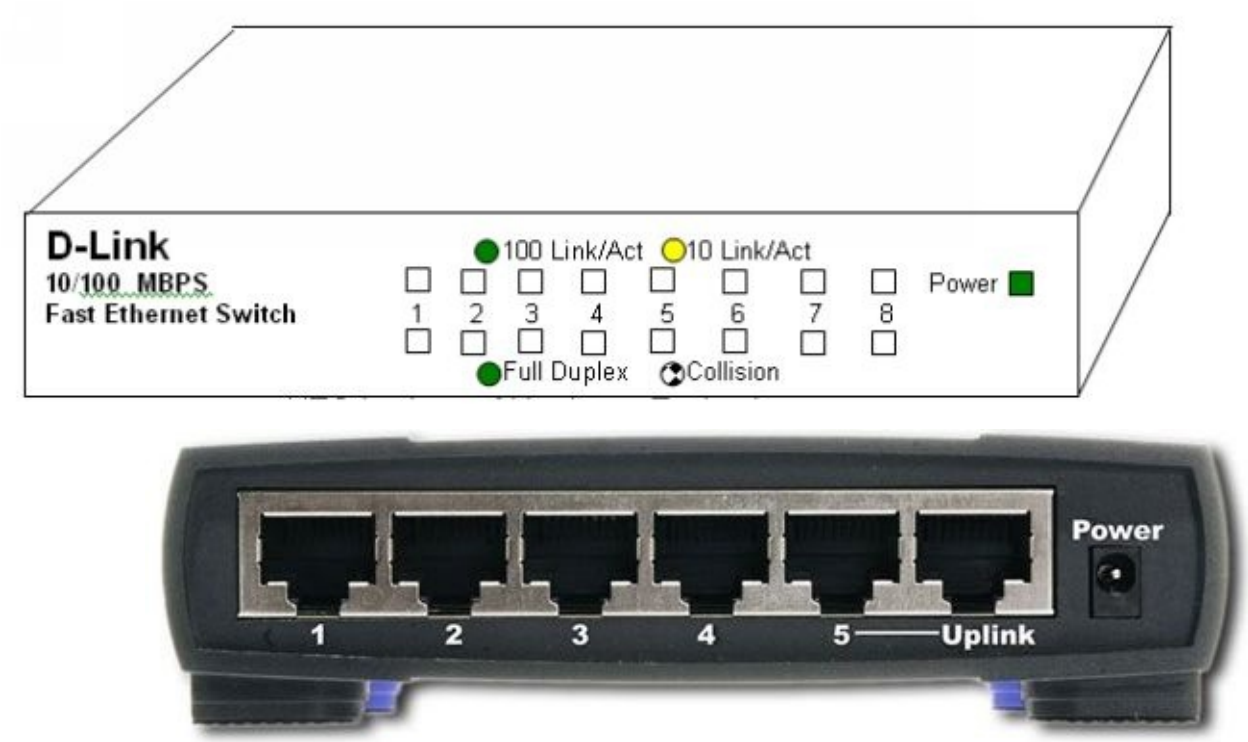
Hubs are also used in star topologies such as 10BaseT. A multi-port twisted pair hub allows several point-to-point segments to be joined into one network. One end of the point-to-point link is attached to the hub and the other is attached to the computer. If the hub is attached to a backbone, then all computers at the end of the twisted pair segments can communicate with all the hosts on the backbone.

An important fact to note about hubs is that they only allow users to share Ethernet. A network of hubs/repeaters is termed a “shared Ethernet”, meaning that all members of the network are contending for transmission of data onto a single network (collision domain). This means that individual members of a shared network will only get a percentage of the available network bandwidth. The number and type of hubs in any one collision domain for 10BaseT Ethernet is limited by the following rules:

Switches (Fast Ethernet / Gigabit Ethernet)

LAN switches are an expansion of the concept in LAN bridging. They operate at Layer 2 (link layer) of the OSI reference model, which controls data flow, handles transmission

errors, provides physical (as opposed to logical) addressing, and manages access to the physical medium. Switches provide these functions by using various link-layer protocols - such as Ethernet, Token Ring and FDDI - that dictate specific flow control, error handling, addressing, and media-access algorithms.



LAN switches can link four, six, ten or more networks together, and have two basic architectures: cut-through and store-and-forward. In the past, cut-through switches were faster because they examined the packet destination address only before forwarding it on to its destination segment. A store-and-forward switch, on the other hand, accepts and analyses the entire packet before forwarding it to its destination.

It takes more time to examine the entire packet, but it allows the switch to catch certain packet errors and keep them from propagating through the network. By the late 1990s, the speed of store-and-forward switches had caught up with cut-through switches so the difference between the two was minimal. By then, a large number of hybrid switches had become available that mixed both cut-through and store-and-forward architectures.

While repeaters allow LANs to extend beyond normal distance limitations, they still limit the number of nodes that can be supported. Bridges, routers and switches, however, allow LANs to grow significantly larger by virtue of their ability to support full Ethernet segments on each port.

Network Standards

Copper Ethernet Standards

Ethernet is a family of frame-based computer networking technologies for local area networks (LANs). The name came from the physical concept of the ether. It defines a number of wiring and signaling standards for the Physical Layer of the OSI networking model as well as a common addressing format and Media Access Control at the Data Link Layer.

Ethernet is standardized as IEEE 802.3. The combination of the twisted pair versions of Ethernet for connecting end systems to the network, along with the fiber optic versions for site backbones, is the most widespread wired LAN technology. It has been used from around 1980[1] to the present, largely replacing competing LAN standards such as token ring, FDDI, and ARCNET.

10BASE-T, one of several physical media specified in the IEEE 802.3 standard for Ethernet local area networks (LANs), is ordinary telephone twisted pair wire. 10BASE-T supports Ethernet's 10 Mbps transmission speed. In addition to 10BASE-T, 10 megabit Ethernet can be implemented with these media types:

10BASE2 (Thinwire coaxial cable with a maximum segment length of 185 meters)

10BASE5 (Thickwire coaxial cable with a maximum segment length of 500 meters)

10BASE –T (Twisted pair cable)

10BASE - F (Optical fiber cable)

Copper Fast Ethernet Standards

100BASE-T is any of several **Fast Ethernet** standards for twisted pair cables, including: 100BASE-TX (100 Mbit/s over two-pair Cat5 or better cable), 100BASE-T4 (100 Mbit/s over four-pair Cat3 or better cable, defunct), 100BASE-T2 (100 Mbit/s over two-pair Cat3 or better cable, also defunct). The segment length for a 100BASE-T cable is limited to 100 metres (328 ft) (as with 10BASE-T and gigabit Ethernet). All are or were standards under IEEE 802.3 (approved 1995).

In the early days of Fast Ethernet, much vendor advertising centered on claims by competing standards that "ours will work better with existing cables than theirs." In practice, it was quickly discovered that few existing networks actually met the assumed standards, because 10-megabit Ethernet was very tolerant of minor deviations from specified electrical characteristics and few installers ever bothered to make exact measurements of cable and connection quality; if Ethernet worked over a cable, it was deemed acceptable. Thus most networks had to be rewired for 100-megabit speed whether or not there had supposedly been CAT3 or CAT5 cable runs. The vast majority of common implementations or installations of 100BASE-T are done with 100BASE-TX.

100BASE-TX

100BASE-TX is the predominant form of Fast Ethernet, and runs over two wire-pairs inside a category 5 or above cable (a typical category 5 cable contains 4 pairs and can

therefore support two 100BASE-TX links). Like 10BASE-T, the proper pairs are the orange and green pairs (canonical second and third pairs) in TIA/EIA-568-B's termination standards, T568A or T568B. These pairs use pins 1, 2, 3 and 6.

In T568A and T568B, wires are in the order 1, 2, 3, 6, 4, 5, 7, 8 on the modular jack at each end. The color-order would be green/white, green, orange/white, blue, blue/white, orange, brown/white, brown for T568A, and orange/white, orange, green/white, blue, blue/white, green, brown/white, brown for T568B.

Each network segment can have a maximum distance of 100 metres (328 ft). In its typical configuration, 100BASE-TX uses one pair of twisted wires in each direction, providing 100 Mbit/s of throughput in each direction (full-duplex). See IEEE 802.3 for more details.

The configuration of 100BASE-TX networks is very similar to 10BASE-T. When used to build a local area network, the devices on the network (computers, printers etc.) are typically connected to a hub or switch, creating a star network. Alternatively it is possible to connect two devices directly using a crossover cable.

With 100BASE-TX hardware, the raw bits (4 bits wide clocked at 25 MHz at the MII) go through 4B5B binary encoding to generate a series of 0 and 1 symbols clocked at 125 MHz symbol rate. The 4B5B encoding provides DC equalization and spectrum shaping (see the standard for details). Just as in the 100BASE-FX case, the bits are then transferred to the physical medium attachment layer using NRZI encoding. However, 100BASE-TX introduces an additional, medium dependent sublayer, which employs MLT-3 as a final encoding of the data stream before transmission, resulting in a maximum "fundamental frequency" of 31.25 MHz. The procedure is borrowed from the ANSI X3.263 FDDI specifications, with minor discrepancies.

100BASE-T4

100BASE-T4 was an early implementation of Fast Ethernet. It requires four twisted copper pairs, but those pairs were only required to be category 3 rather than the category 5 required by TX. One pair is reserved for transmit, one for receive, and the remaining two will switch direction as negotiated. A very unusual 8B6T code is used to convert 8 data bits into 6 base-3 digits (the signal shaping is possible as there are three times as many 6-digit base-3 numbers as there are 8-digit base-2 numbers). The two resulting 3-digit base-3 symbols are sent in parallel over 3 pairs using 3-level pulse-amplitude modulation (PAM-3). This standard can be implemented with CAT 3, 4, 5 UTP cables, or STP if needed against interference. Maximum distance is limited to 100 meters and most likely to be found with old UTP media.

100BASE-T2

In 100BASE-T2, the data is transmitted over two copper pairs, 4 bits per symbol. First, a 4 bit symbol is expanded into two 3-bit symbols through a non-trivial scrambling procedure based on a linear feedback shift register; see the standard for details. This is needed to flatten the bandwidth and emission spectrum of the signal, as well as to match transmission line properties. The mapping of the original bits to the symbol codes is not constant in time and has a fairly large period (appearing as a pseudo-random sequence). The final mapping from symbols to PAM-5 line modulation levels obeys the table on the right.

Copper Gigabit Ethernet Standards

1000BASE-T (also known as IEEE 802.3ab) is a standard for gigabit Ethernet over copper wiring. Each 1000BASE-T network segment can be a maximum length of 100 meters (328 feet), and must utilize Category 5 cable at a minimum. Category 5e cable or Category 6 cable may also be used.

1000BASE-T requires all four pairs to be present. If two gigabit devices are connected through a non-compliant Cat5 cable with two pairs only, negotiation takes place on two pairs only, so the devices successfully choose ‘gigabit’ as the highest common denominator (HCD), but the link never comes up. Most gigabit physical devices have a specific register to diagnose this behaviour.

1000BASE-T details

In a departure from both 10BASE-T and 100BASE-TX, 1000BASE-T uses all four cable pairs for simultaneous transmission in both directions through the use of echo cancellation and a 5-level pulse amplitude modulation (PAM-5) technique. The symbol rate is identical to that of 100BASE-TX (125 Mbaud) and the noise immunity of the 5-level signaling is also identical to that of the 3-level signaling in 100BASE-TX, since 1000BASE-T uses 4-dimensional trellis coded modulation (TCM) to achieve a 6 dB coding gain across the 4 pairs.

The data is transmitted over four copper pairs, eight bits at a time. First, eight bits of data are expanded into four 3-bit symbols through a non-trivial scrambling procedure based on a linear feedback shift register; this is similar to what is done in 100BASE-T2, but uses different parameters. The 3-bit symbols are then mapped to voltage levels which vary continuously during transmission.

1000BASE-TX

The Telecommunications Industry Association (TIA) created and promoted a version of 1000BASE-T that was simpler to implement, calling it 1000BASE-TX (TIA/EIA-854). The simplified design would, in theory, have reduced the cost of the required electronics by only using one pair of wires in each direction. However, this solution required Category 6 cable and has been a commercial failure, likely due to the cabling requirement as well as the rapidly falling cost of 1000BASE-T products. Many 1000BASE-T products are advertised as 1000BASE-TX due to lack of knowledge that 1000BASE-TX is actually a different standard. The most popular form of Fast Ethernet (100 Mbit/s) is known as 100BASE-TX.

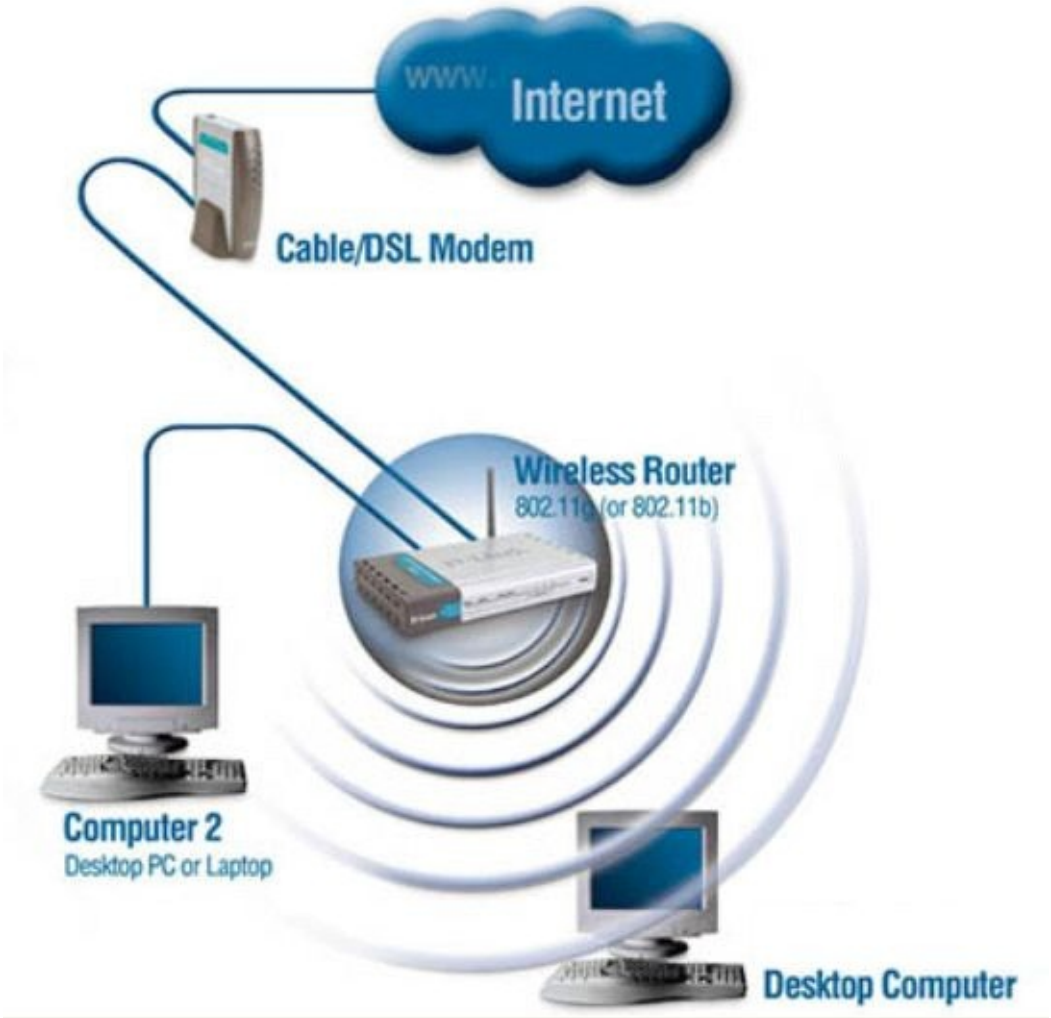
1000BASE-CX

1000BASE-CX is an initial standard for gigabit Ethernet connections over copper cabling with maximum distances of 25 meters using balanced shielded twisted pair. It is still used for specific applications where cabling is not done by general users, for instance the IBM BladeCenter uses 1000BASE-CX for the Ethernet connections between the blade servers and the switch modules. 1000BASE-T succeeded it for general copper wiring use.

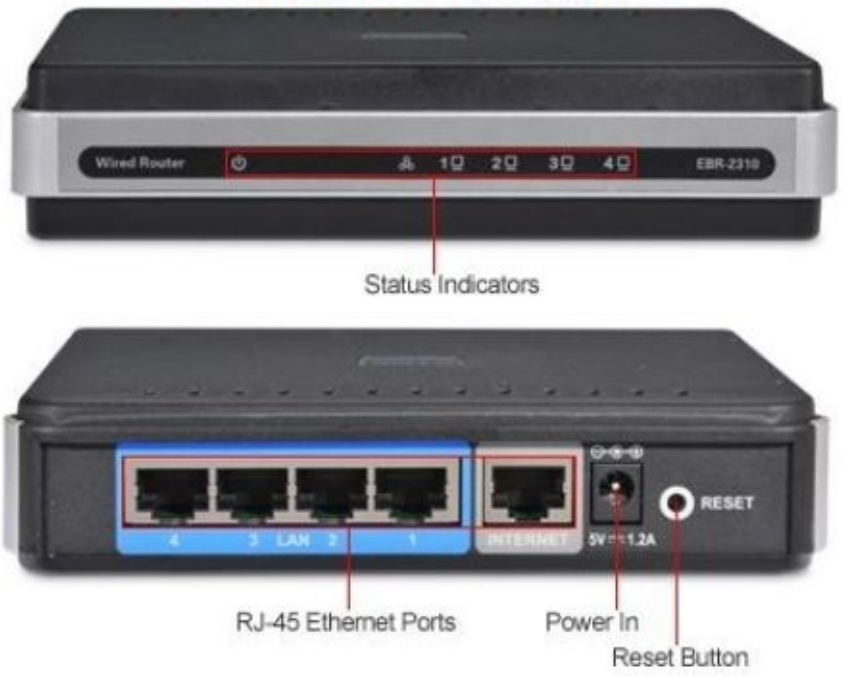
Routers

Routing achieved commercial popularity in the mid-1980s - at a time when large-scale internetworking began to replace the fairly simple, homogeneous environments that had been the norm hitherto. Routing is the act of moving information across an internetwork from a source to a destination. It is often contrasted with bridging, which performs a similar function. The primary difference between the two is that bridging occurs at Layer 2 (the link layer) of the OSI reference model, whereas routing occurs at Layer 3 (the network layer). This distinction provides routing and bridging with different information to use in the process of moving information from source to destination, so the two functions accomplish their tasks in different ways.

Routers use information within each packet to route it from one LAN to another, and communicate with each other and share information that allows them to determine the best route through a complex network of many LANs. To do this, routers build and maintain “routing tables”, which contain various items of route information - depending on the particular routing algorithm used. For example, destination/next hop associations tell a router that a particular destination can be gained optimally by sending the packet to a particular router representing the “next hop” on the way to the final destination. When a router receives an incoming packet, it checks the destination address and attempts to associate this address with a next hop.



Wired Router



PRINT SERVERS

Parallel Port
Print Server

USB Print Server

NETWORK STORAGE

LAN

WirelessLAN

NETWORK CAMERAS

LAN

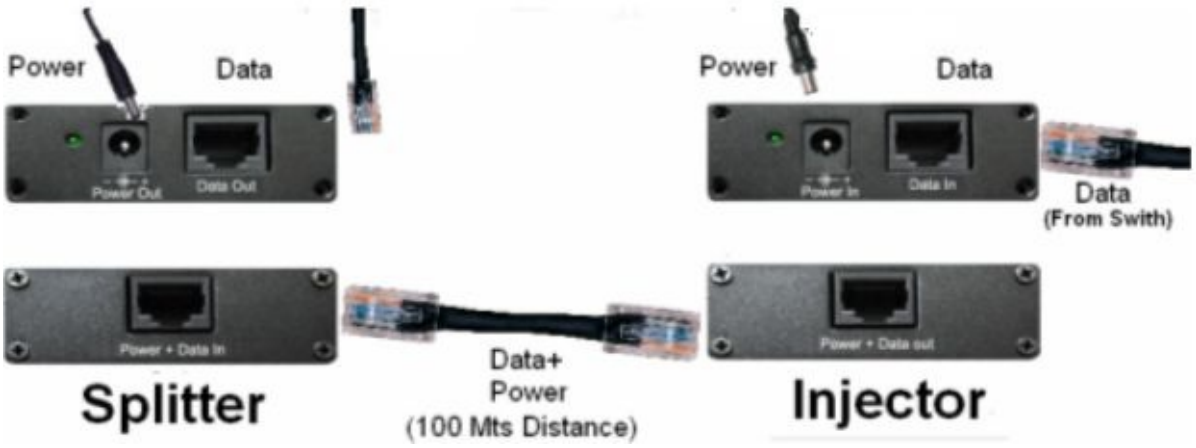
Wireless LAN

Passive Power over Ethernet (POE)

Power over Ethernet is a technology which enables to connect network devices through Ethernet cable. Therefore it is not necessary to use two individual lines/1x data, 1x power supply/ for assurance of data connectivity and supplying. One Ethernet line is sufficient. This technology is applicable for wide range of network products such as Access Points, Routers, IP cameras, modems, switches, embedded computers or other network products.

Standard Power over Ethernet is defined by standard IEEE 802.3af, (at the same time it is defined by new prepared standard IEEE 802.3at). Power over Ethernet products using these standards contain of two individual active pieces /injector and splitter/. Each active piece includes an electrical circuit which ensures the function of this solution. There is guaranteed selected supply to 100 m / 328 ft at these standards.

Our technology Passive Power over Ethernet, in comparison with IEEE 802.3af uses no active electronic components for transmission. It is a simple way of connecting the cables in order to transfer the data and power supply along the same ethernet cable at the same time. Ehternet cable contains 8 cables. 4 cables (1,2,3,6) are used for data transmission and the rest (4,5,7,8) is used for supplying. Passive PoE`s range is form 30-40 metres / 100-130 ft. According to the latest statistics 90% of installations using Power over Ethernet do not exceed the distance of 20 - 30 meters / 65-100 ft. Therefore Passive Power over Ethernet is advantageous and sufficient option in comparison with expensive Power over Ethernet (IEEE 802.3af).



Fiber Media Converter

A **fiber media converter** is a simple networking device that makes it possible to connect two dissimilar media types such as twisted pair with fiber optic cabling. They were introduced to the industry nearly two decades ago[*when?*], and are important in interconnecting fiber optic cabling-based systems with existing copper-based, structured cabling systems. They are also used in MAN access and data transport services to enterprise customers.

Fiber Optic Cable

Fiber Optic Fast Ethernet Standards

100BASE-FX

100BASE-FX is a version of Fast Ethernet over optical fiber. It uses a 1300 nm near-infrared (NIR) light wavelength transmitted via two strands of optical fiber, one for receive(RX) and the other for transmit(TX). Maximum length is 400 metres (1,310 ft) for half-duplex connections (to ensure collisions are detected) or 2 kilometres (6,600 ft) for full-duplex over multimode optical fiber. Longer distances are possible when using single-mode optical fiber. 100BASE-FX uses the same 4B5B encoding and NRZI line code that 100BASE-TX does. 100BASE-FX should use SC, ST, or MIC connectors with SC being the preferred option.

100BASE-FX is not compatible with 10BASE-FL, the 10 MBit/s version over optical fiber.

100BASE-SX

100BASE-SX is a version of Fast Ethernet over optical fiber. It uses two strands of multi-mode optical fiber for receive and transmit. It is a lower cost alternative to using 100BASE-FX, because it uses short wavelength optics which are significantly less expensive than the long wavelength optics used in 100BASE-FX. 100BASE-SX can operate at distances up to 300 metres (980 ft).

100BASE-SX uses the same wavelength as 10BASE-FL, the 10 MBit/s version over optical fiber. Unlike 100BASE-FX, this allows 100BASE-SX to be backwards-compatible with 10BASE-FL.

Because of the shorter wavelength used (850 nm) and the shorter distance it can support, 100BASE-SX uses less expensive optical components (LEDs instead of lasers) which makes it an attractive option for those upgrading from 10BASE-FL and those who do not require long distances.

100BASE-BX

100BASE-BX is a version of Fast Ethernet over a single strand of optical fiber (unlike 100BASE-FX, which uses a pair of fibers). Single-mode fiber is used, along with a special multiplexer which splits the signal into transmit and receive wavelengths. The two wavelengths used for transmit and receive are either 1310/1550nm or 1310/1490nm. Distances can be 10, 20 or 40 km.

100BASE-LX10

100BASE-LX10 is a version of Fast Ethernet over two single-mode optical fibers. It has a nominal reach of 10km and a nominal wavelength of 1310nm.

Fiber Optic Gigabit Ethernet Standards

1000BASE-SX

1000BASE-SX is a fiber optic gigabit Ethernet standard for operation over multi-mode fiber using a 770 to 860 nanometer, near infrared (NIR) light wavelength.

The standard specifies a distance capability between 220 meters (62.5/125 µm fiber with low modal bandwidth) and 550 meters (50/125 µm fiber with high modal bandwidth). In practice, with good quality fibre and terminations, 1000BASE-SX will usually work over significantly longer distances. This standard is highly popular for intra-building links in large office buildings, co-location facilities and carrier neutral internet exchanges. Optical power specifications of SX interface: Minimum output power = -9.5 dBm. Minimum receive sensitivity = -17 dBm.

1000BASE-LX

1000BASE-LX is a fiber optic gigabit Ethernet standard specified in IEEE 802.3 Clause 38 which uses a long wavelength laser (1270 to 1355 nm), and a maximum RMS spectral width of 4 nm. 1000BASE-LX is specified to work over a distance of up to 5 km over 10 µm single-mode fiber. 1000BASE-LX can also run over all common types of multi-mode fiber with a maximum segment length of 550 m. For link distances greater than 300 m, the use of a special launch conditioning patch cord may be required.[4] This launches the laser at a precise offset from the center of the fiber which causes it to spread across the diameter of the fiber core, reducing the effect known as differential mode delay which occurs when the laser couples onto only a small number of available modes in multi-mode fiber.

1000BASE-LX10

1000BASE-LX10 was standardized six years after the initial gigabit fiber versions as part of the Ethernet in the First Mile task group. It is very similar to 1000BASE-LX, but achieves longer distances up to 10 km over a pair of single-mode fiber due to higher quality optics. Before it was standardized 1000BASE-LX10 was essentially already in widespread use by many vendors as a proprietary extension called either 1000BASE-LX/LH or 1000BASE-LH.[5]

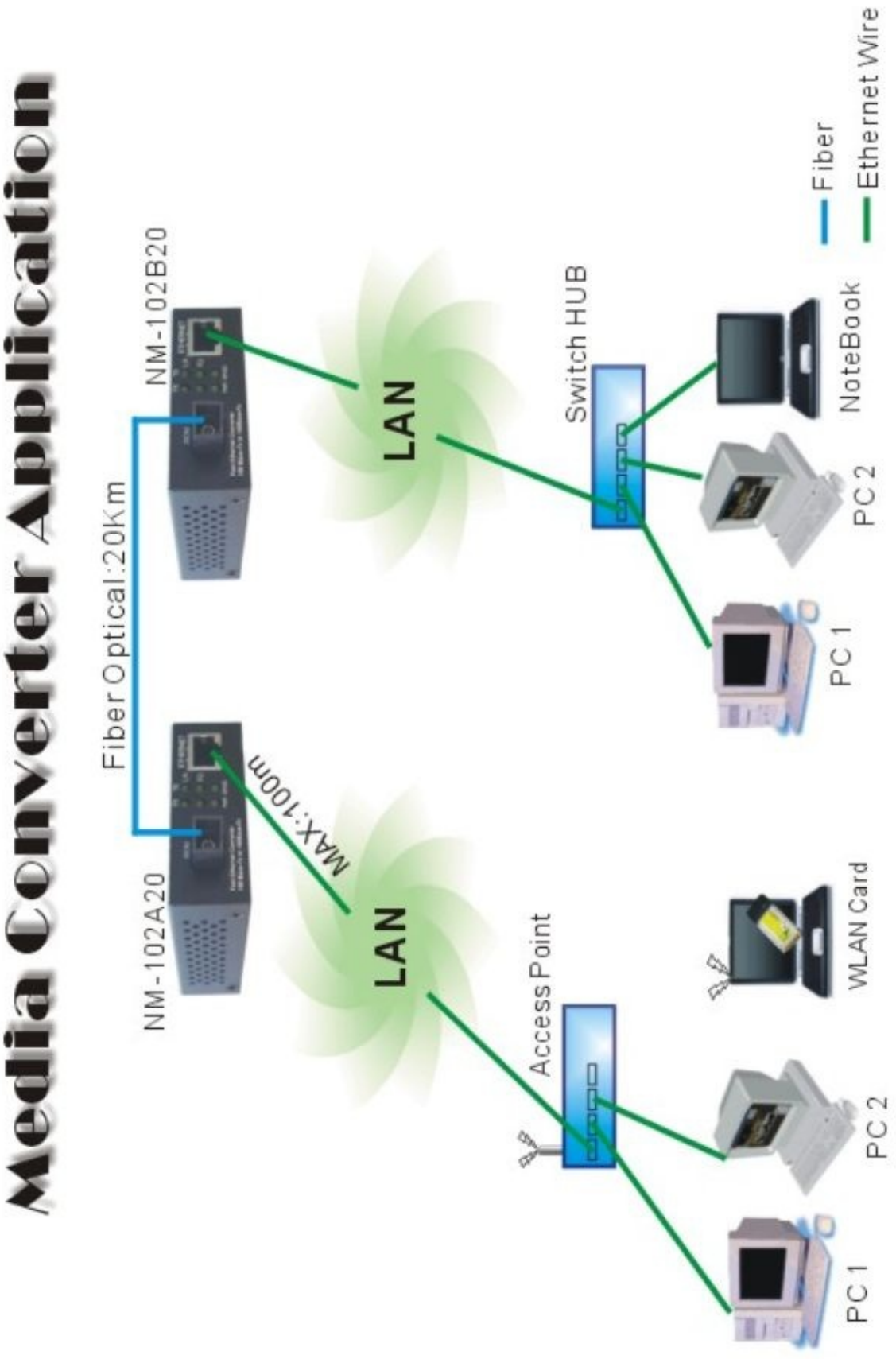
1000BASE-BX10

1000BASE-BX10 is capable of up to 10 km over a single strand of single-mode fiber, with a different wavelength going in each direction. The terminals on each side of the fibre are not equal, as the one transmitting “downstream” (from the center of the network to the outside) uses the 1490 nm wavelength, and the one transmitting “upstream” uses the 1310 nm wavelength.

Non IEEE versions

1000BASE-ZX

1000BASE-ZX is a non-standard but industry accepted term to refer to gigabit Ethernet transmission using 1550 nm wavelength to achieve distances of at least 70 km over single-mode fiber.



Wireless

The main advantage of wireless networks over wired networks is that you don’t have to

run and connect cables to the various computers. The three major types of wireless networks today are the following:

- Infrared
- Microwave
- Radio Frequency

Infrared Networks

Infrared networks are normally used in small places where you don't have to transmit the signal very far. The problem of with infrared networks is that they are line-of-sight, which mean the port on the computer has to be able to see the network port. Other disadvantages are their expensive cost and slow speed. Most of today's copper networks operate at 10 to 100Mbps. Most infrared adapters can operate from 0.3 to 4 Mbps.

Radio frequency (RF) Networks

Radio Frequency (RF) Networks are becoming more popular these days. Radio waves can go through walls and can be installed where it would be difficult to install cable. With all the satellites in orbit, radio waves can reach almost any place in the planet. Radio is more reliable than microwaves as it is unaffected by weather and does not need line-of-sight.

A. **Bluetooth:** Bluetooth is a proprietary open wireless protocol for exchanging data over short distances (using short length radio waves) from fixed and mobile devices, creating personal area networks (PANs).

B. Wi-Fi / WLAN : Wireless Fidelity (Wi-Fi) (Pronounced as waifai) is a trademark of the Wi-Fi Alliance that manufacturers may use to brand certified products that belong to a class of wireless local area network (WLAN) devices based on the IEEE 802.11 standards.

Microwave Networks

Microware networks are normally used to transmit data over a long distance where cables cannot be used. Microwaves also require line-of-sight, but it can carry over long distances. Microwave networks use a string of towers to carry data across long distances. The disadvantage of microware is that rain or fog can degrade the signal to the point were it is unreadable.

A. WiMax / WMAN : WiMAX**,** meaning *Worldwide Interoperability for Microwave Access*, is a telecommunications technology that provides wireless transmission of data using a variety of transmission modes, from point-to-multipoint links to portable and fully mobile internet access

B. VSAT : A Very Small Aperture Terminal (VSAT), is a two-way satellite ground station with a dish antenna that is smaller than 3 meters. Most VSAT antennas range from 75 cm to 1.2 m. Data rates typically range from 56 Kbit/s up to 4 Mbit/s. VSATs access satellites in geosynchronous orbit to relay data from small remote earth stations (terminals) to other terminals (in mesh configurations) or master earth station "hubs" (in star configurations).

Wi-Fi / IEEE 802.11 / WLAN

The name of a popular wireless networking technology that uses radio waves to provide wireless high-speed Internet and network connections. The Wi-Fi Alliance, the organization that owns the Wi-Fi (registered trademark) term specifically defines Wi-Fi as any "wireless local area network (WLAN) products that are based on the Institute of Electrical and Electronics Engineers' (IEEE) 802.11 standards."

Wi-Fi works with no physical wired connection between sender and receiver by using radio frequency (RF) technology, a frequency within the electromagnetic spectrum associated with radio wave propagation. When an RF current is supplied to an antenna, an electromagnetic field is created that then is able to propagate through space. The cornerstone of any wireless network is an access point (AP). The primary job of an access point is to broadcast a wireless signal that computers can detect and "tune" into. In order to connect to an access point and join a wireless network, computers and devices must be equipped with wireless network adapters

Wi-Fi is supported by many applications and devices including video game consoles, home networks, PDAs, mobile phones, major operating systems, and other types of consumer electronics. Any products that are tested and approved as "Wi-Fi Certified" (a registered trademark) by the Wi-Fi Alliance are certified as interoperable with each other, even if they are from different manufacturers. For example, a user with a Wi-Fi Certified product can use any brand of access point with any other brand of client hardware that also is also "Wi-Fi Certified". Products that pass this certification are required to carry an identifying seal on their packaging that states "Wi-Fi Certified" and indicates the radio frequency band used (2.4GHz for 802.11b, 802.11g, or 802.11n, and 5GHz for 802.11a).

A common misconception is that the term Wi-Fi is short for "*wireless fidelity*," however this is not the case. Wi-Fi is simply a trademarked term meaning IEEE 802.11x.

WLAN standards

WLAN standards below the metropolitan level are fairly well defined; most people have heard about 802.11b and g Wi-Fi standards. Some upcoming standards like 3G are attempting to increase range and seamless availability. Others like 802.1x, EAP, and 802.11i are attempting to increase security. Currently, the industry emphasis is on extending range or strengthening security rather than trying to increase speed, but that

may change in the future. 802.11a, b, and g: The big three standards. The 802.11a, b, and g standards are by far the most common ones for home wireless access points up through large business wireless systems. The differences in the protocols are these:

802.11a

Shortest range of the big three standards (generally around 60 to 100 feet)

Broadcasts in the 5GHz frequency

Supports up to 54Mbps (megabits per second) speed

Less able to penetrate physical barriers like walls

Better speed than 802.11b, supports more simultaneous connections, and because it operates in a more regulated frequency, gets less signal interference from other devices, so is considered to be more consistent in terms of maintaining a connection. In certain circumstances, such as areas with major radio interference (e.g., airports, business call centers), 802.11a will outperform and actually outrange 802.11b.

802.11b

Better range than 802.11a: up to 300 feet in ideal circumstances, and better than 802.11a even in real-world circumstances (Tests by independent reviewers tend to achieve anywhere from 70 to 150 feet.)

Broadcasts in the 2.4GHz frequency

Supports up to 11Mbps speed

Hardware tends to be lower in cost nowadays.

Better able than 802.11a to penetrate physical barriers, and lower in cost, but cannot support as many simultaneous connections. Also, it operates on the same frequency as many cordless phones and other appliances; therefore, it is more susceptible to interference and other things that degrade its performance, so it’s not considered a good technology for certain applications requiring absolutely reliable connections, such as live video streaming.

802.11g

Very close to 802.11b in certain aspects; is actually backwards compatible with 802.11b products (but will run only at 802.11b speeds when operating with them)

Faster speed than 802.11b; supports up to 54Mbps. Some proprietary solutions (Netgear, Linksys) manage to get 108Mbps out of the 802.11g standard by broadcasting on more than one of the eight channels that 802.11b uses.

Also uses the 2.4GHz frequency

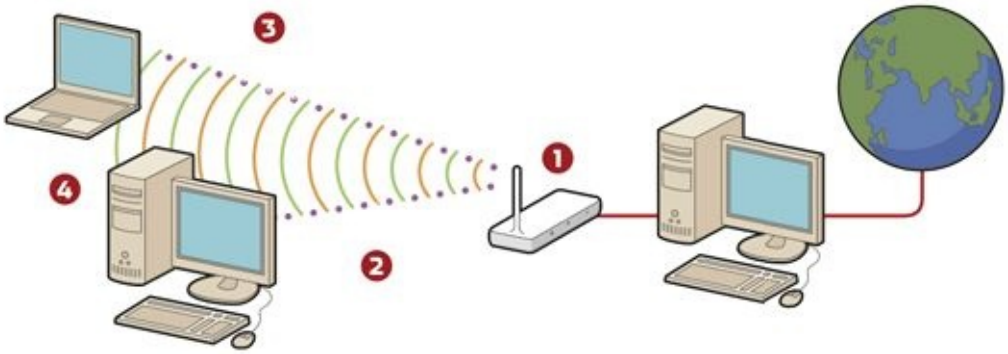
Slightly shorter range than 802.11b, but still better than 802.11a. Most independent reviews report around 65 to 120 feet in real-world situations. Suffers from the same problems, such as interference and absolute reliability, as 802.11b

802.11n (Different than current generations of Wi-Fi?)

The 802.11n standard uses some new technology and tweaks existing technologies to give Wi-Fi more speed and range. The most notable new technology is called multiple input, multiple output (**MIMO**). MIMO uses several antennas to move multiple data streams from one place to another. Instead of sending and receiving a single stream of data, MIMO can simultaneously transmit three streams of data and receive two. This allows more data to be transmitted in the same period of time. This technique can also increase range, or the distance over which data can be transmitted.

A second technology being incorporated into 802.11n is channel bonding, which can use two separate non overlapping channels at the same time to transmit data. This technique also increases the amount of data that can be transmitted. A third technology in 802.11n is called payload optimization or packet aggregation, which, in simple terms, means more data can be stuffed into each transmitted packet.

How Wireless LAN works



In a typical home network, your Wi-Fi hotspot—a wireless on-ramp to the Net and/or your network—is provided by an ***access point*** (AP), or a ***router*** with an AP built-in **(1)**. You might have one in your home as part of your LAN, or share one with other sippers at your local pricey-java mart. The AP has a radio transmitter/receiver inside, similar to that in a Walkie-Talkie. Data is converted first into a ***radio signal*** **(2)**, then beamed out at one of two frequencies: 2.4GHz for devices using the 802.11b/g Wi-Fi standard, or 5GHz for 802.11a hardware. Both are unlicensed portions of the radio spectrum in the United States.

The AP transmits, many times a second, tiny ***beacon signals*** **(3)** containing network-identification and other info (notably, the Service Set Identifier, or SSID, though the broadcast of this info can be disabled for security). Your ***Wi-Fi-enabled laptop or desktop*** **(4)** contains a Wi-Fi card or chipset that also has a transmitter/receiver; picking up the signal, it determines whether the system can and should connect to the AP. The card also gauges signal strength and access characteristics of competing APs.

When authentication occurs, data transmission begins, but if Wired Equivalent Privacy (WEP) or the stronger Wi-Fi Protected Access (WPA) encryption is in use, both client and AP must agree on a pre-entered alphanumeric “key” to decrypt the transmissions. Access might also be limited by a Media Access Control (MAC) address; all devices on a network have a MAC address, and most wireless routers can allow or disallow access according to these addresses.

If you move your PC away from your AP, transfer rates gradually decline, and vice versa. 802.11b is designed to run at a maximum data rate of 11Mbps, and its 802.11g and 802.11a variants at up to 54Mbps. The rate steps down, however, when it encounters interference or physical signal obstruction. Hardware supporting multiple input, multiple output (MIMO) technology employs several receivers and transmitters for accelerated throughput.

Wireless LAN cards and Wireless Access Point

PCMCIA Adapter
(For LAPTOPS)

IEEE802.11n Wireless Access Point

IEEE802.11n Wireless LAN Cards / Adapters

WiMax / IEEE802.16 / WMAN

(Wireless Metropolitan Area Network / Wireless Broadband)

WiMax is the industry term for a long-range wireless networking standard. WiMax technology has the potential to deliver high-speed Internet access to rural areas and other locations not serviced by cable or DSL technology. WiMax also offers an alternative to satellite Internet services.

WiMax technology is based on the IEEE 802.16 WAN communications standard. WiMax signals can function over a distance of several miles / kilometers. Data rates for WiMax can reach up to 75 megabits per second (Mb/s). A number of wireless signaling options exist ranging anywhere from the 2 GHz range up to 66 GHz.

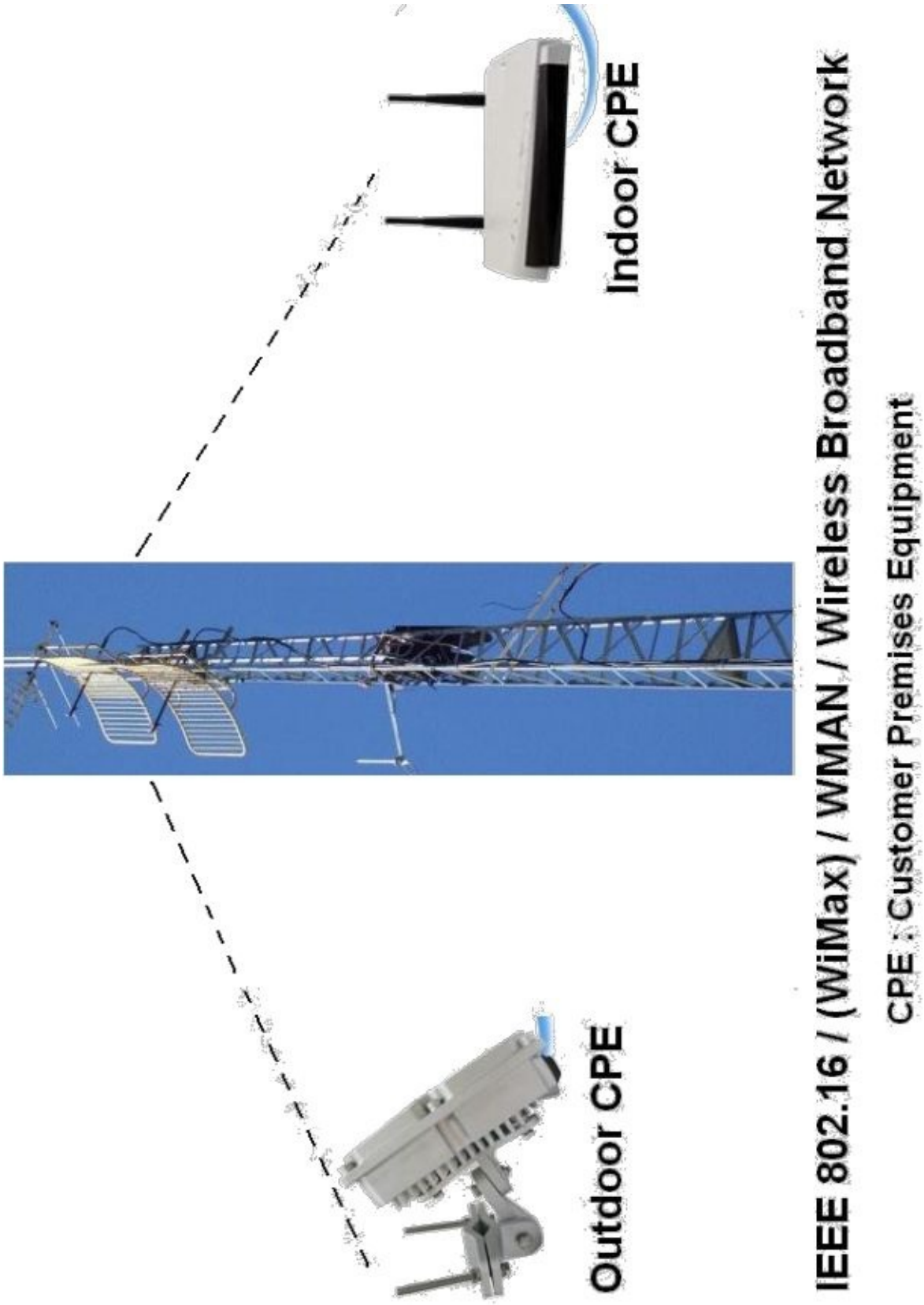
WiMax equipment exists in two forms. **WiMax base stations** are installed by service providers to deploy the technology in a coverage area. **WiMax Receiver / Antenna / CPE** (Customer Premises Equipment) must be installed at the home or other receiving location. As WiMax evolves, these antennas will change from being mounted outdoors, to smaller varieties set up indoors, and then finally to built-in versions integrated inside mobile computers. Similar to other types of Internet access, consumers will subscribe and pay a recurring fee to connect to the Internet via WiMax. WiMax is developed by an industry consortium, overseen by a group called the WiMax Forum. The WiMax Forum certifies WiMax equipment to ensure it meets the technology standards. WiMax is not a replacement for Wi-Fi hotspot and home networking technologies primarily for cost reasons.

1. **WiMAX base station**: As name explains base station is placewhere WiMax signals are broadcasted. It consists of electronic devices and WiMax Tower. This tower works exactly like GSM network phones towers standing high up in the air to broadcast radio signals. WiMAX tower base station can cover up 10Km radius. In theory it suggests to cover a lot more distance than just 10Km, it can reach some where about 50 km (30 miles), but in fact due to certain geographical limitations it goes as far as 10 km approx. 6 mils. Any wireless connecting device for WiMAX will connect to WiMAX network if fallen in to the range.
2. **WiMAX Receiver:** It is device or devices which receives the signals from WiMAX base station and connects to the WiMAX networks. These devices are usually stand alone Antenna or PCMCIA slot card for laptops or computers. Connecting to WiMAX base stations works as similar as connection of Wifi to access point works, the only difference is that WiMAX covers much wider area.

One WiMAX base stations can be connected to several other base stations using high speed microwave link, this link is usually known as backhaul. This way WiMAX roaming can be achieved and connections can be maintained on move.

Wimax support many protocols like ATM, IPv4 Ethernat, VLAN etc, this makes WiMax a rich choice for full of services from data to voice.

Also Known As: **Worldwide Interoperability for Microwave Access**



IEEE Wireless Networking Standards

Protocol	Release	Frequency	Channels	Net bit rate	Range

	date			(Max)	(Indoor)
802.11a (Wi-Fi)	October 1999	5 GHz	8	54 Mbit/s	~35 m/ 110ft
802.11b (Wi-Fi)	October 1999	2.412 GHZ	14	11Mbits/s	~38m/ 120ft
802.11g (Wi-Fi)	June 2003	2.412 GHZ	14	54Mbits/s	~38m/ 120ft
802.11n (Wi-Fi)	Dec 2008	2.412GHZ 5GHZ	24	72.2Mbits/s X4 150Mbits/s X4	~70m/ 230ft
802.16 (WiMax)	Dec 2001	10-66GHZ (Line of Sight)		134Mbp/s	~5km
802.16a (WiMax)	Jan 2003	<11GHZ		75Mbp/s	~50Km
802.16e (WiMax)	Mid 2004	<6GHZ		15Mbp/s	~5Km
802.15.1 (Bluetooth)		2.54GHZ	1	1Mbps (1.2) 3Mbps (2.0) 24Mbps (3.0) 24Mbps (4.0)	~5m(class1) ~10m(class2) ~100m(class3)

VSAT

Dish with Sattellite Modem

A Very Small Aperture Terminal (VSAT), is a two-way satellite ground station with a dish antenna that is smaller than 3 meters (most VSAT antennas range from 75 cm to 1.2 m). VSAT data rates typically range from narrowband up to 4 Mbit/s. VSATs access satellites in geosynchronous orbit to relay data from small remote earth stations (terminals) to other terminals (in mesh configurations) or master earth station “hubs” (in star configurations).

VSATs are most commonly used to transmit narrowband data (point of sale transactions such as credit card, polling or RFID data; or SCADA), or broadband data (for the provision of Satellite Internet access to remote locations, VoIP or video). VSATs are also used for transportable, on-the-move (with phased-array antennas) or mobile maritime (such as Vizada or Eutelsat services) communications.

VSAT ARCHITECTURE

TELEPHONE LEASED LINE NETWORK

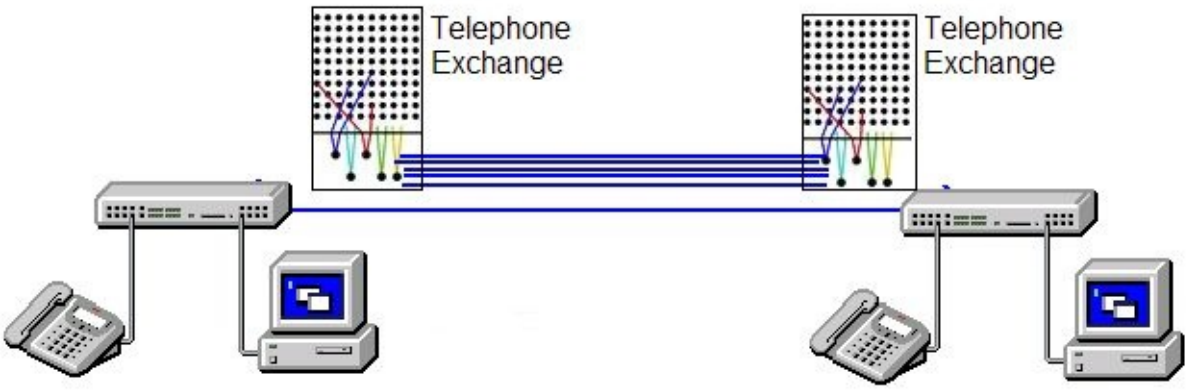
A **leased line** is a symmetric telecommunications line connecting two locations. It is sometimes known as a 'Private Circuit' or 'Data Line' in the UK. Unlike traditional PSTN lines it does not have a telephone number, each side of the line being permanently connected to the other. Leased lines can be used for telephone, data or Internet services.

A **leased line** connects two locations for private voice and/or data telecommunication service. Not a dedicated cable, a leased line is actually a reserved circuit between two points. Leased lines can span short or long distances. They maintain a single open circuit at all times, as opposed to traditional telephone services that reuse the same lines for many different conversations through a process called "switching."

Leased lines most commonly are rented by businesses to connect branch offices, because these lines guarantee bandwidth for network traffic. So-called **T1** leased lines are common and offer the same data rate as symmetric DSL (1.544 Mbps). Individuals can theoretically also rent leased lines for high-speed Internet access, but their high cost deters most. **Fractional T1** lines, starting at 128 Kbps, reduce this cost somewhat and can be found in some apartment buildings and hotels.

To transmit data between computer and electronic information devices, BSNL provides data communication services to its subscribers. It offers a choice of high, medium and low speed leased data circuits as well as dial-up lines. Bandwidth is available on demand in most of the cities. Managed leased Line Network (MLLN) offers flexibility of providing circuits with speeds of n x 64 Kbps up to 2 Mbps. Useful for internet leased lines and international principle Leased Lines(IPLCs).

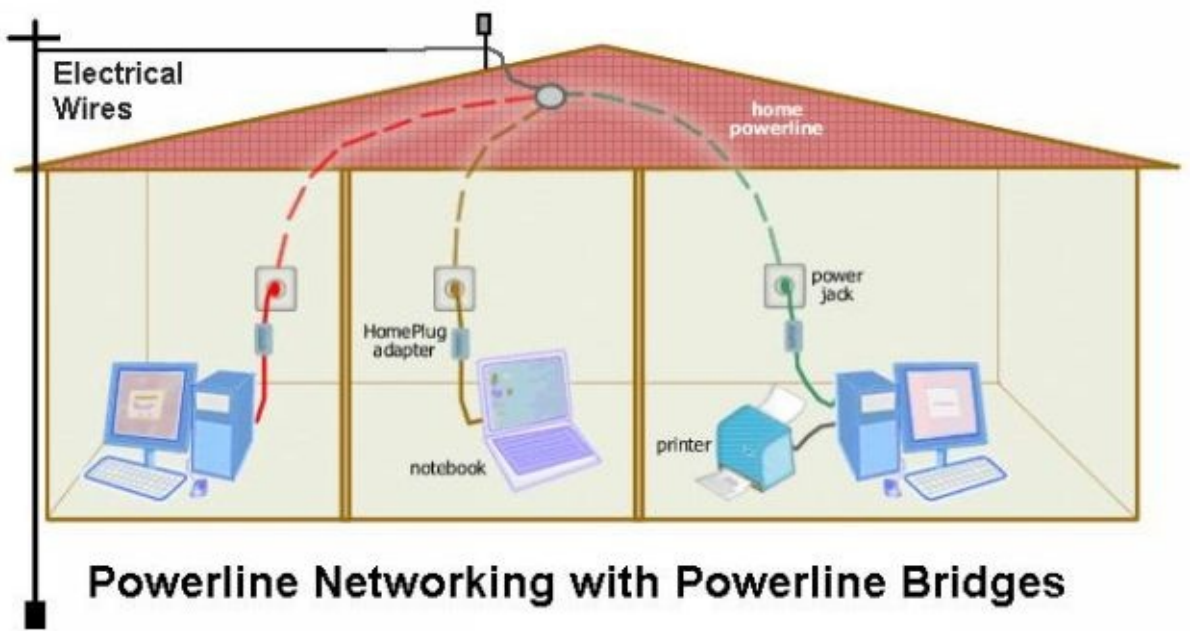
For dedicated point to point speech, private wire, tele-printer and data circuits are given on lease basis. Leased circuits are provided to subscribers for internal communication between their offices/factories at various sites within a city/town or different cities/town on point to point basis, or on a network basis interconnecting the various sites.



Powerline Networking

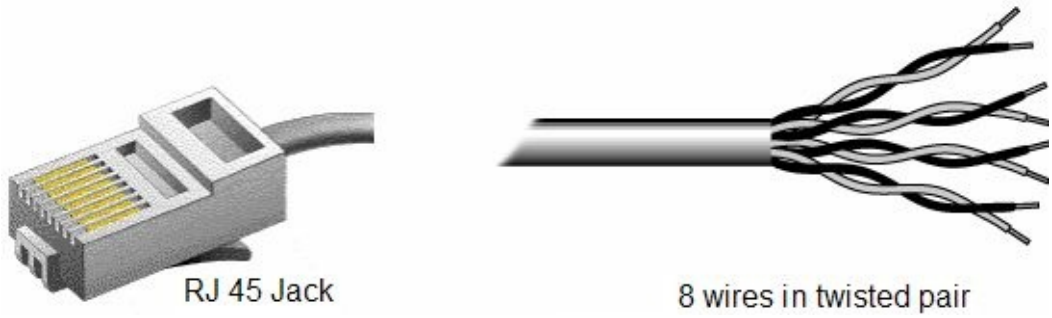
Power-line networking is one of several ways to connect the computers in your home. It uses the electrical wiring in your house to create a network. Power-line networking is based on the concept of “no new wires.” The convenience is even more obvious in this case because while not every room has a phone jack, you will always have an electrical outlet near a computer. In power-line networking, you connect your computers to one another through the same outlet.

Setting up a Powerline Network is really simple, just plug in the powerline adapter into a power socket and connect the adaptor to your router or modem, with a network cable ,repeat this in the other room/s where other network outlets are going this time connecting the powerline adaptor to the PC’S network port. Status lights on each adaptor will confirm that you have an active network connection and that it is working well.



Cabling and Crimping

10BaseT /100BaseT (Twisted Pair / CAT cable) cable



HUB / SWITCH

Max 100 Meters, 10/100/1000 Mbps, Star Topology

Crimping (Straight-through) Color Coding for 10/100Base-T

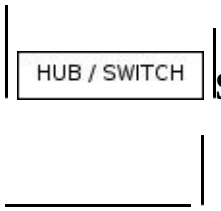
T568A (Computer) T568A (Switch)

White - Green (RX+)	**1.** White – Green (TX+)	**1.**
2. Green (RX-)	**2.** Green (TX-)	
White - Orange (TX+)	**3.** White - Orange (RX+)	**3.**
4. Blue		4. Blue
5. White – Blue		5. White - Blue
6. Orange (TX-)	**6.** Orange (RX-)	
7. White - Brown		7. White - Brown
8. Brown		8. Brown

(OR)

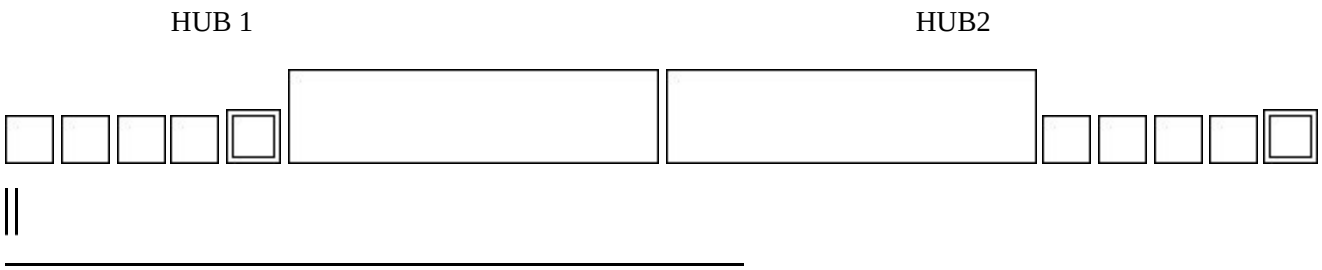
T568B (Computer) T568B (Switch)

White - Orange (RX+)	**1.** White – Orange (TX+)	**1.**
2. Orange (RX-)	**2.** Orange (TX-)	
3. White - Green (TX+)	**3.** White - Green (RX+)	
4. Blue		4. Blue
5. White - Blue		5. White - Blue
6. Green (TX-)	**6.** Green (RX-)	
7. White - Brown		7. White - Brown
8. Brown		8. Brown



Straight – Through Cable

Note: Use Wall Mounted Jack / Network I/O box and Patch cords for big networks.



Uplink port / MDI port **Normal ports/ MDI-X ports**

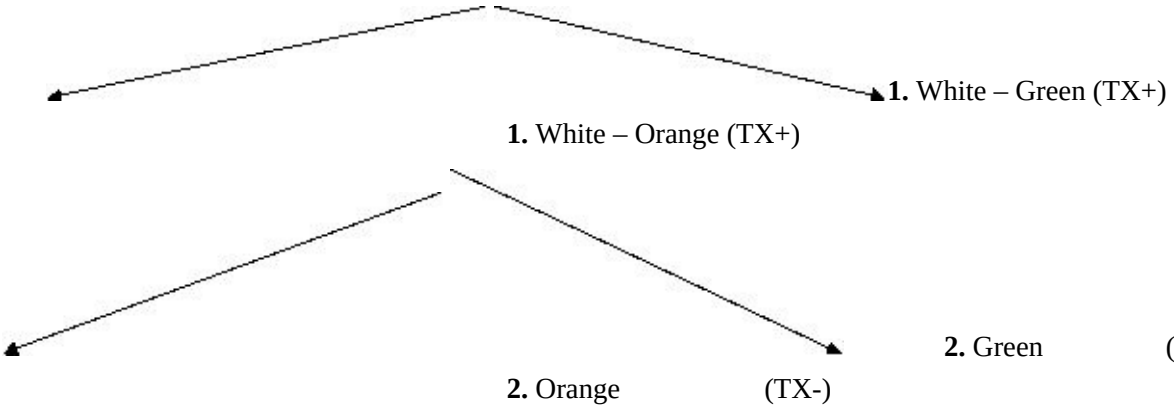
Uplink port/ MDI port **Normal ports/ MDI-X ports**

MDI : Medium Dependent Interface

MDI-X: Crossed Medium Dependent Interface

Crimping (Cross over) Color Coding for 10/100Base-T

T568A (Computer) **T568B (Computer)**



3. White - Orange (RX+)

4. Blue

5. White - Blue

6. Orange (RX-)

7. White - Brown

8. Brown

3. White – Green (RX+)

4. Blue

5. White - Blue

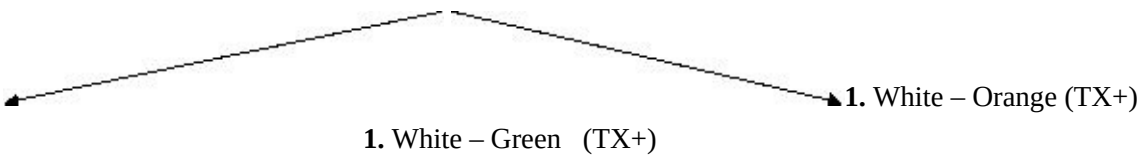
6. Green (RX-)

7. White - Brown

8. Brown

(OR)

T568B (Computer) **T568A (Computer)**



2. Green (TX-)

2. Orange (TX-)

3. White - Green (RX+)

3. White – Orange (RX+)

4. Blue

4. Blue

5. White - Blue

5. White - Blue

6. Green (RX-)

6. Orange (RX-)

7. White - Brown

7. White - Brown

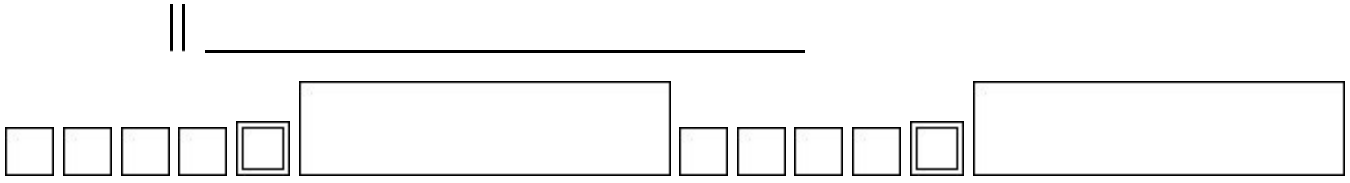
8. Brown

8. Brown

Cross over Cable

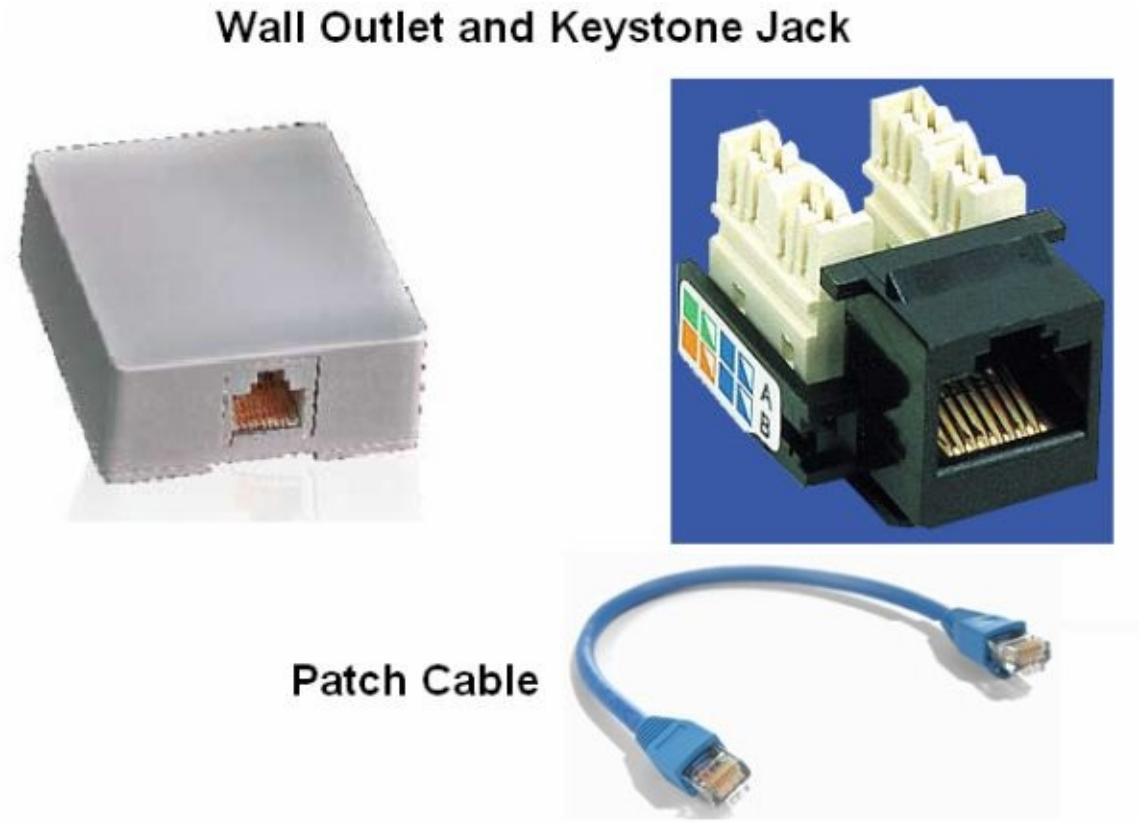
HUB 1

HUB2



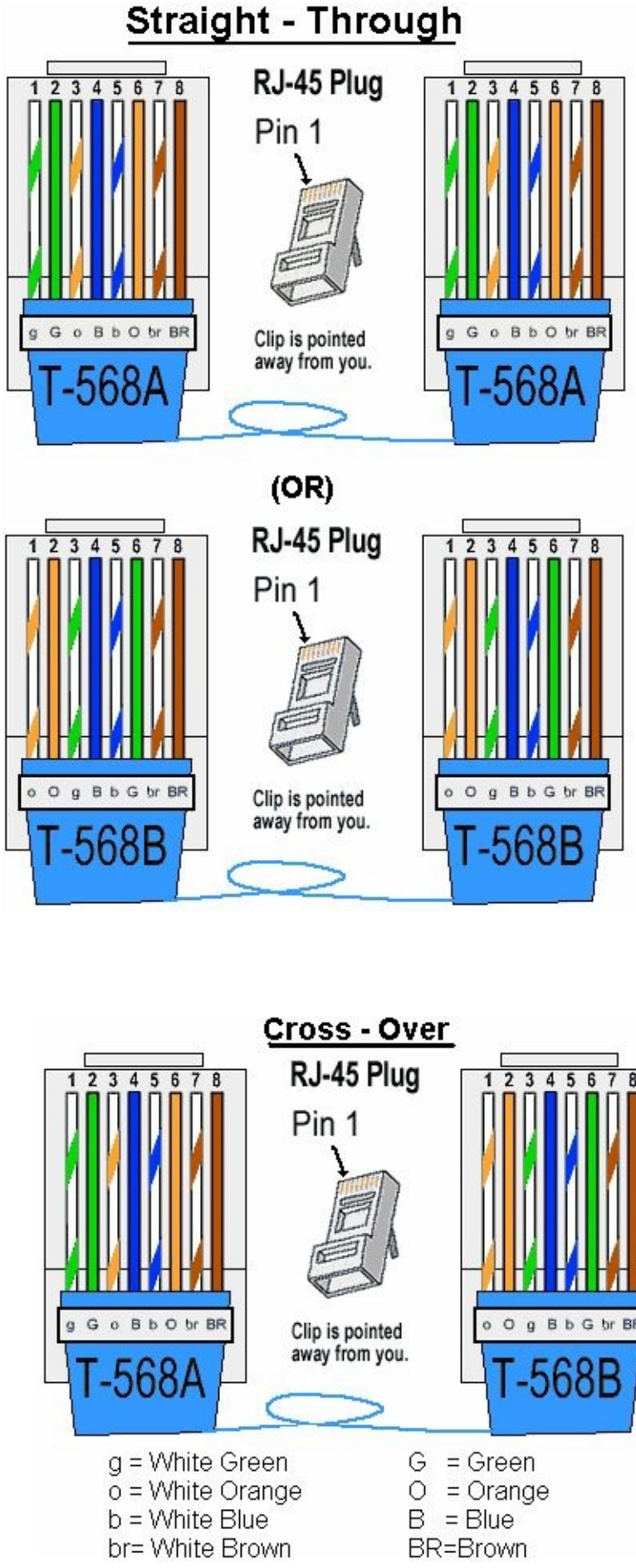
OR

Uplink port / MDI port **Normal ports/ MDI-X ports** **Uplink port/ MDI port** **Normal ports/ MDI-X ports**



For Wall Mounted Box give the connections in U shape.

For Keystone Jack follow the color coding given on it.



Crimping (Straight-through) Color Coding for 1000Base-T

T568A (Computer) **T568A (Switch)**

1. White – Green (BI-DA+)	**1.** White - Green (BI-DA+)
2. Green (BI-DA-)	**2.** Green (BI-DA-)
3. White - Orange (BI-DB+)	**3.** White - Orange (BI-DB+)
4. Blue (BI-DC+)	4. Blue (BI-DC+)
5. White – Blue (BI-DC-)	5. White – Blue (BI-DC-)
6. Orange (BI-DB-)	**6.** Orange (BI-DB-)
7. White – Brown (BI-DD+)	7. White – Brown (BI-DD+)
8. Brown (BI-DD-)	8. Brown (BI-DD-)

(OR)

T568B (Computer) **T568B (Switch)**

1. White – Orange (BI-DA+)	**1.** White - Orange (BI-DA+)
2. Orange (BI-DA-)	**2.** Orange (BI-DA-)
3. White – Green (BI-DB+)	**3.** White - Green (BI-DB+)
4. Blue (BI-DC+)	4. Blue (BI-DC+)
5. White – Blue (BI-DC-)	5. White – Blue (BI-DC-)
6. Green (BI-DB-)	**6.** Green (BI-DB-)
7. White – Brown (BI-DD+)	7. White – Brown (BI-DD+)
8. Brown (BI-DD-)	8. Brown (BI-DD-)

Crimping (Cross over) Color Coding for 1000Base-T

(For 1000Base-T all Four Pairs should be Crossed)

T568A (Computer) **T568B (Computer)**

1. White – Green (BI-DA+)

2. Green (BI-DA-)

3. White - Orange (BI-DB+)

4. Blue (BI-DC+)

5. White - Blue (BI-DC-)

6. Orange (BI-DB-)

7. White – Brown (BI-DD+)

8. Brown (BI-DD-)

1. White – Orange (BI-DB+)

2. Orange (BI-DB-)

3. White – Green (BI-DA+)

4. White –Brown (BI-DD+)

5. Brown (BI-DD-)

6. Green (BI-DA-)

7. Blue (BI-DC+)

8. White – Blue (BI-DC-)

BI-DA+ = Bi-Directional Pair A+

BI-DB+ = Bi-Directional Pair B+

BI-DC+ = Bi-Directional Pair C+

BI-DD+ = Bi-Directional Pair D+

BI-DA- = Bi-Directional Pair A-

BI-DA- = Bi-Directional Pair B-

BI-DA- = Bi-Directional Pair C-

BI-DA- = Bi-Directional Pair D-

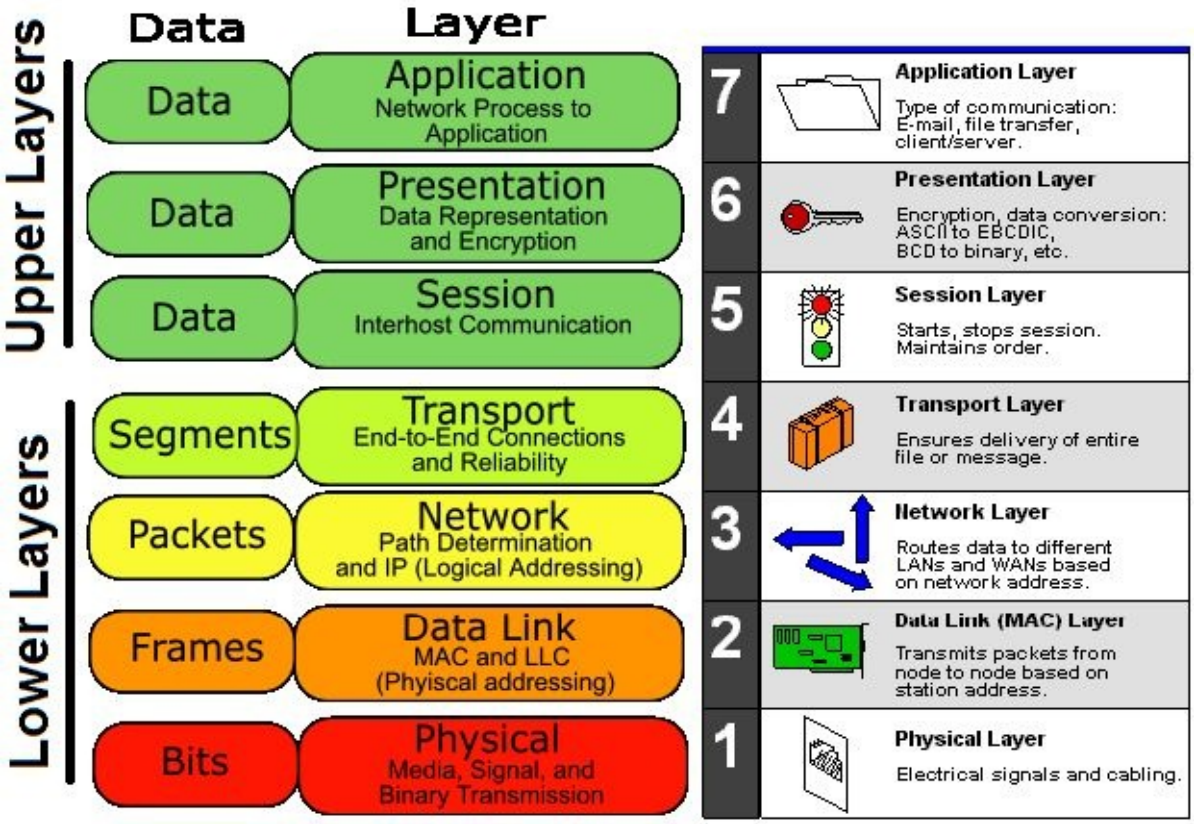
OSI Model & Network Layers

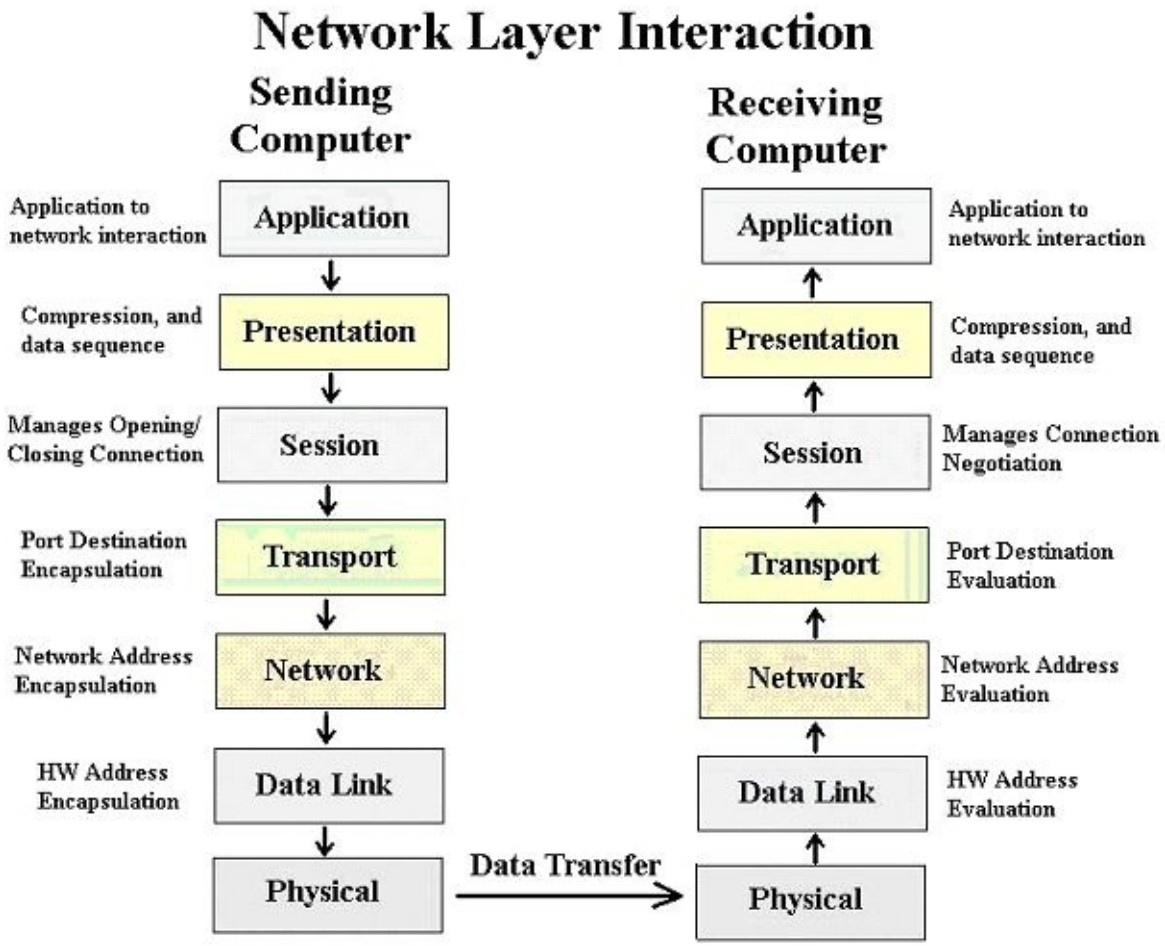
The Open Systems Interconnection (OSI) reference model describes how information from a software application in one computer moves through a network medium to a software application in another computer. The OSI reference model is a conceptual model composed of seven layers, each specifying particular network functions. The model was developed by the International Organisation for Standardisation (ISO) in 1984, and it is now considered the primary architectural model for intercomputer communications. The OSI model divides the tasks involved with moving information between networked computers into seven smaller, more manageable task groups. A task or group of tasks is then assigned to each of the seven OSI layers. Each layer is reasonably self-contained, so that the tasks assigned to each layer can be implemented independently. This enables the solutions offered by one layer to be updated without adversely affecting the other layers.

The seven layers of the OSI reference model can be divided into two categories: upper layers and lower layers. The upper layers of the OSI model deal with application issues and generally are implemented only in software. The highest layer, application, is closest to the end user. Both users and application-layer processes interact with software

applications that contain a communications component. The term upper layer is sometimes used to refer to any layer above another layer in the OSI model. The lower layers of the OSI model handle data transport issues. The physical layer and data link layer are implemented in hardware and software. The other lower layers generally are implemented only in software. The lowest layer, the physical layer, is closest to the physical network medium (the network cabling, for example) , and is responsible for actually placing information on the medium.

7	**Application Layer**	**Application programs that use the network**
6	**Presentation Layer**	**Standardizes data presented to the applications**
5	**Session Layer**	**Manages sessions between applications**
4	**Transport Layer**	**Provides error detection and correction**
3	**Network Layer**	**Manages network connections**
2	**Data Link Layer**	**Provides data delivery across the physical connection**
1	**Physical Layer**	**Defines the physical network media**





Segment = chunk of data.

Packet = contains IP addresses of the source and destination hosts.

Frame = it contains source and destination Mac address

Application Layer (Layer 7)

- Contains protocols that allow the users to access the network (FTP, HTTP, SMTP, etc)
- Does not include application programs such as email, browsers, word processing applications, etc.
- Protocols contain utilities and network-based services that support email via SMTP, Internet access via HTTP, file transfer via FTP, etc

Presentation Layer (Layer 6)

Responsibilities of this layer are:

- Translation
  - Different computers use different encoding systems (bit order translation)
  - Convert data into a common format before transmitting.
  - Syntax represents info such as character codes - how many bits to represent data – 8 or 7 bits
- Compression – reduce number of bits to be transmitted

- Encryption – transform data into an unintelligible format at the sending end for data security
- Decryption – at the receiving end

Session Layer (Layer 5)

Main functions of this layer are:

- Dialog control – allows two systems to enter into a dialog, keep a track of whose turn it is to transmit
- Synchronization – adds check points (synchronization points) into stream of data.

Transport Layer (Layer 4)

Main functions of this layer are:

- Responsible for source-to-destination delivery of the entire message
- Segmentation and reassembly – divide message into smaller segments, number them and transmit. Reassemble these messages at the receiving end.
- Error control – make sure that the entire message arrives without errors – else retransmit.

Network Layer (Layer 3)

Main functions of this layer are:

- Responsible for delivery of packets across multiple networks
- Routing – Provide mechanisms to transmit data over independent networks that are linked together.
- Network layer is responsible only for delivery of individual packets and it does not recognize any relationship between those packets

Data Link Layer (Layer 2)

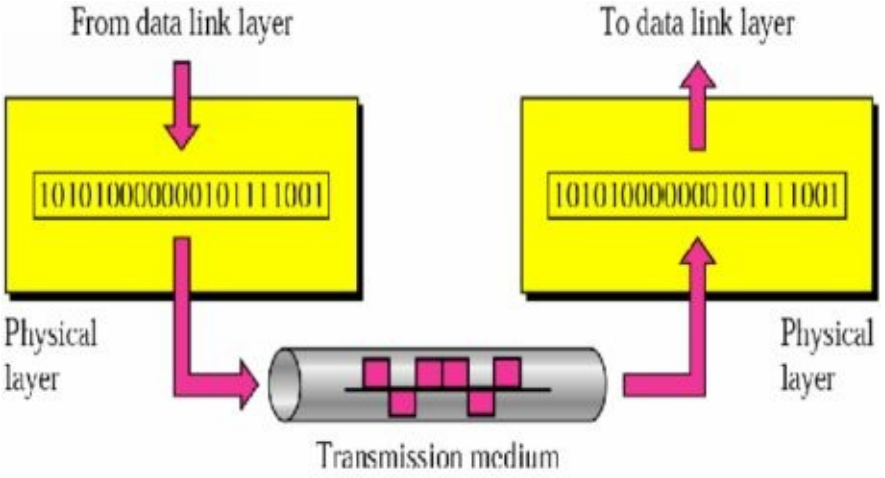
Responsible for delivery of data between two systems on the same network

Main functions of this layer are:

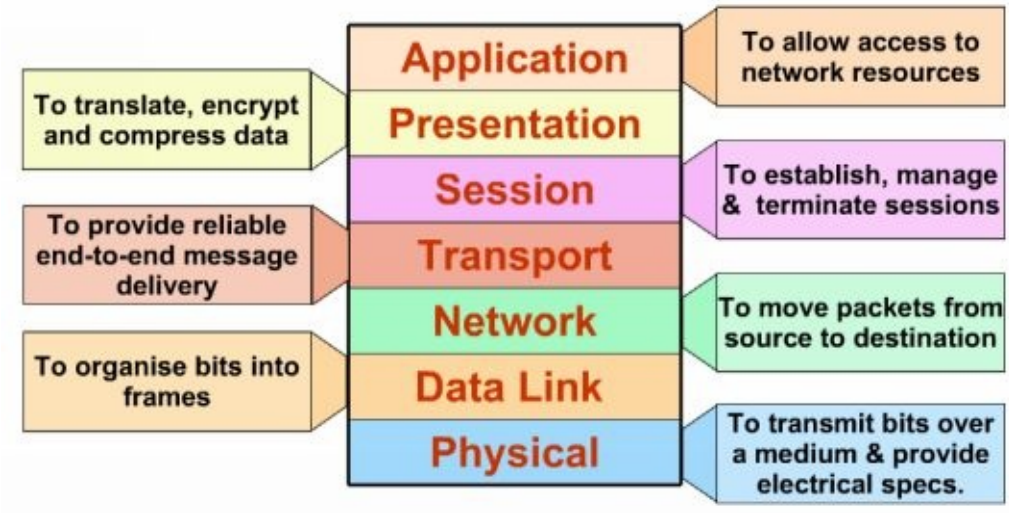
- Framing – divides the stream of bits received from network layer into manageable data units called frames.
- Physical Addressing – Add a header to the frame to define the physical address of the source and the destination machines.
- Flow control – Impose a flow control – control rate at which data is transmitted so as not to flood the receiver (Feedback-based flow control)
- Error Control – Adds mechanisms to detect and retransmit damaged or lost frames. This is achieved by adding a trailer to the end of a frame

Physical layer (Layer 1)

- Specifications for the physical components of the network.
- Functions of Physical Layer:
  - Bit representation – encode bits into electrical or optical signals
  - Transmission rate – The number of bits sent each second
  - Physical characteristics of transmission media
  - Synchronizing the sender and receiver clocks
  - Transmission mode – simplex, half-duplex, full duplex
  - Physical Topology – how devices are connected – ring, star, mesh, bus topology



Summary of Functions of Layers



The IEEE 802 Model

The institute of electrical and electronic engineers (IEEE) developed standards called the *project 802* for the physical connection of network adapters. The 802 standards are listed below define the way data is laced on the network media by the network adapters.

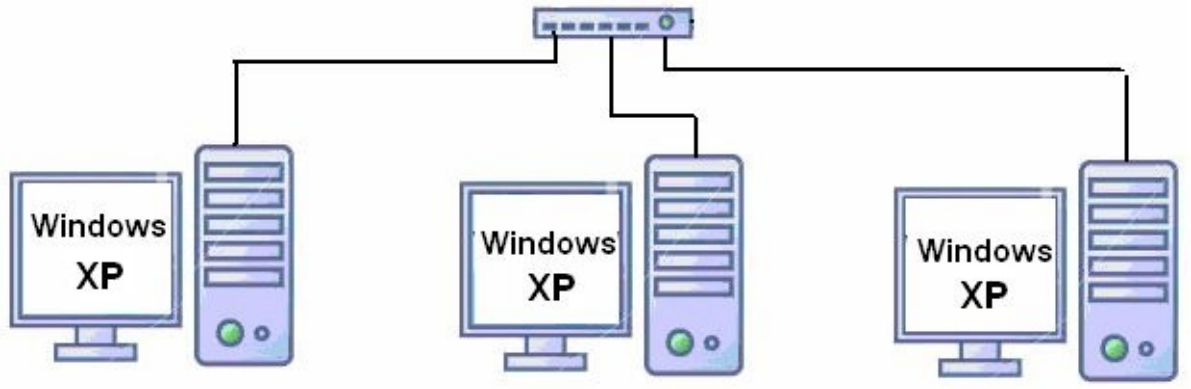
IEEE Project 802 Model Standards and Functions

Number	Category

		Defines
802.1	Internetworking	Transparent bridging (Standards related to network management)
802.2	Logical Link Control	The LLC sub layer of the Data Link Layer
802.3	Ethernet	CSMA/CD For Ethernet Networks
802.4	Token Bus	Networks that use token-passing bus
802.5	Token Ring	IBM’s token-ring network
802.6	Metropolitan Area Network (MAN)	A network with two physical channels
802.7	Broadband Technology	The Broadband Technical Advisory Group
802.8	Fiber-Optic Technology	The Fiber-Optic Technical Advisory Group
802.9	Integrated Voice and Data	Integrated Voice and Data Networks
802.10	Network Security	Network Security Issues

802.11	Wireless LAN / Wi-Fi	Wireless Application Protocol Networks (WAP)
802.12	100Base VG-AnyLAN	The new standard for 100Mbps LAN’s
802.14	Cable Modems	Data transport over traditional cable TV networks
802.15	Wireless PAN / Bluetooth	For low-rate wireless personal area networks
802.16	Wireless MAN / WiMax	Long Range wireless for Broadband Internet
802.20	Mobile Wireless Access	Mobile broadband wireless access networks
802.22	Wireless RAN	For Wireless Regional Area Network (WRAN) using white spaces in the TV frequency spectrum

Peer to peer Networks using Windows XP



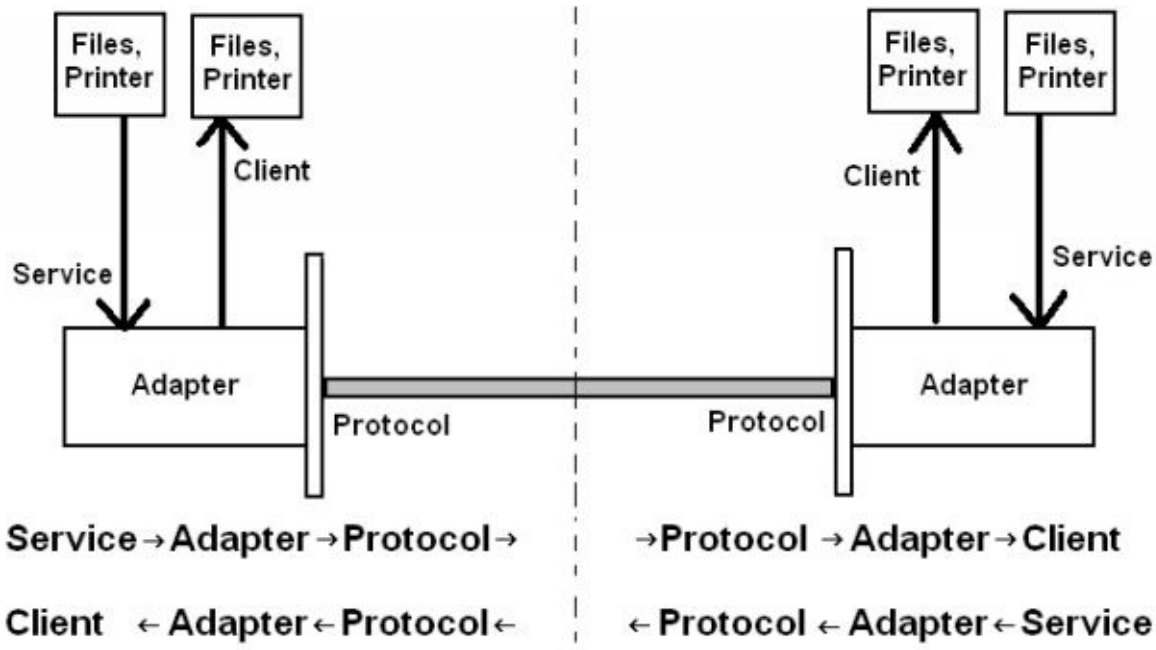
To setup simple network we have to install the following four components

1. Adapter : An adapter is the hardware device that physically connects your computer to the network.

2. Protocol : A protocol is the language a computer uses to communicate over a network. Computers must use the same protocol to communicate with each other.

3. Client : Client software enables you to use files and printers shared on other network computers.

4. Service : Some services enable you to share your files and printers with other people on the network. Other services include automatic system backup, remote registry, and network monitor agent.



Supported Protocols

Win98/ME/XP 1. NETBEUI **2. TCP/IP (Default),** 3. IPX/SPX (For Netware)

2000/2003/VISTA

Unix / Linux / SUN Solaris : **1. TCP / IP**

Novell Netware **1. TCP / IP** 2. IPX / SPX

NetBEUI

Pronounced *net-booey,* NetBEUI is short for ***NetBios Extended User Interface***. It is an enhanced version of the **NetBIOS** protocol used by network operating systems such as LAN Manager, LAN Server, Windows for Workgroups, Windows 95 and Windows NT.

NetBIOS Enhanced User Interface (NetBEUI) is a non-routable network transport suited for use in small networks that consist of a single network segment with less than 50 computers.

NETBEUI supports: 1. File Sharing

2. Printer Sharing

TCP/IP

Transmission Control Protocol/Internet Protocol (TCP/IP) is a suite of industry-standard protocols. TCP/IP, also known as the Internet protocol, is a routable network protocol that also provides access to the Internet. TCP/IP has become the most common protocol for internetworking because of its capability to be used with almost any network operating system and equipment.

To install the above four components first install the LAN card driver and restart. Then right click on “network Neighborhood” icon and select properties. And add the required protocols and service by using add option as follows. Then go to Identification Tab and give the Computer name Workgroup names.

TCP/IP supports : 1. File Sharing

2. Printer Sharing

3. Internet Sharing

4. Netmeeting (Voice & Video)

5. Network Testing

6. Network Split

7. Network Security

IPX / SPX

The IPX/SPX protocol stack is supported by Novell’s NetWare network operating system. Because of Netware’s popularity through the late 1980s into the mid 1990s, IPX became a popular internetworking protocol

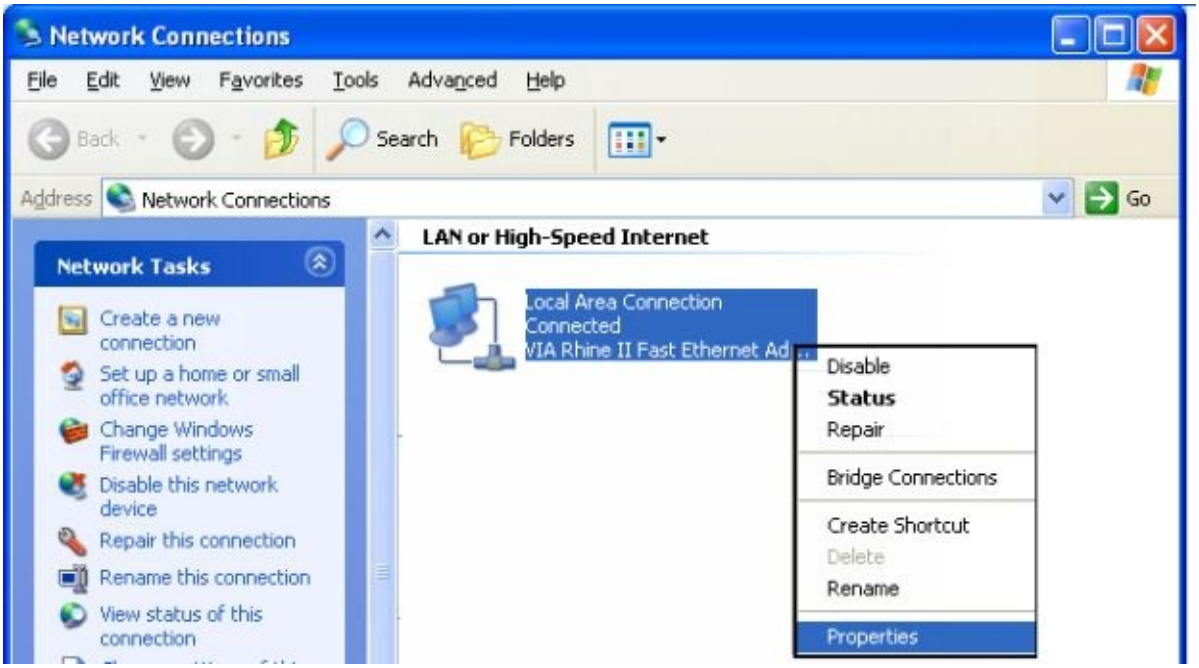
Internet Packet Exchange (IPX) is the native NetWare protocol used on many earlier Novell networks. Sequenced packet exchange, part of the IPX/SPX protocol suite.

Network Setup (One Time only)

To setups Network in Windows XP One setup will be run after installation of LAN card driver as follows.

1. Install LAN Card Driver (Ignore if already installed)
2. Right click on My Network Places and select Properties.
3. Right click on Local Area connection and select properties.

4. Select Advanced and click on network setup Wizard and next, next
5. Select “Other” in Network Selection method and
6. Select “This Computer belongs to Network that does not have an internet Connection” in Other internet connection method.
7. Enter Computer Name and Description.
8. Enter Workgroup Name
9. Turn on File and Printer Sharing.
10. And select “Just Finish the Wizard and Restart the Computer” as follows.



Changing the Identification

Computer Name :

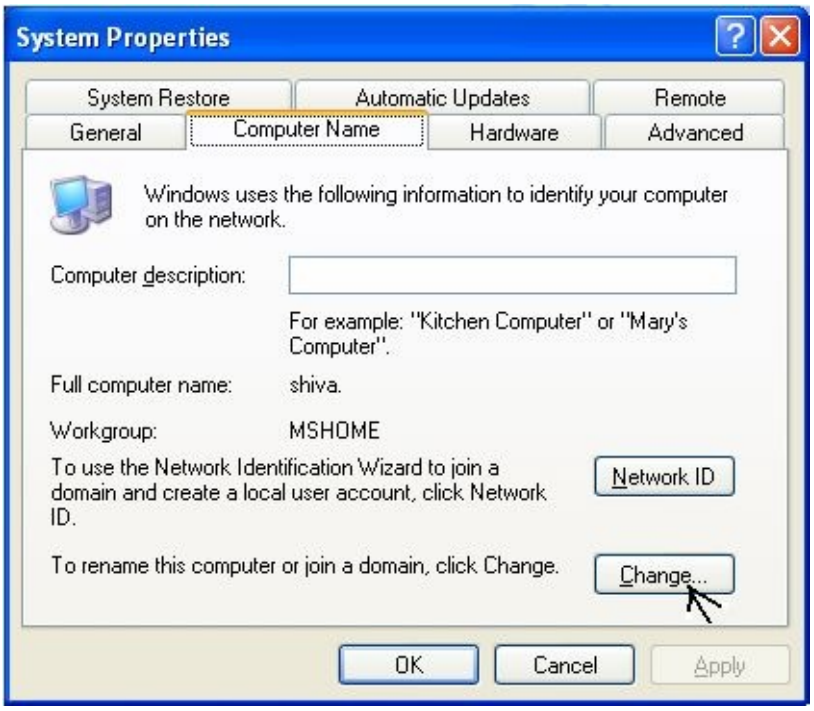
Identifies your computer to other people on the network. You Can Give your computer a unique name of up to 15 characters. The name cannot include blank spaces.

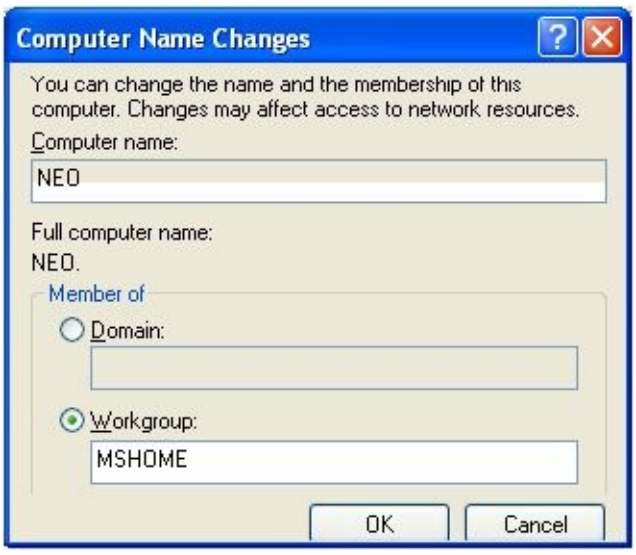
Workgroup :

Identifies the group of computers that your computer is in. You can type an existing workgroup name or create a new workgroup contains up to 15 characters. A workgroup is generally composed of the computers you are most likely to communicate with (Generally Department)

Computer Description:

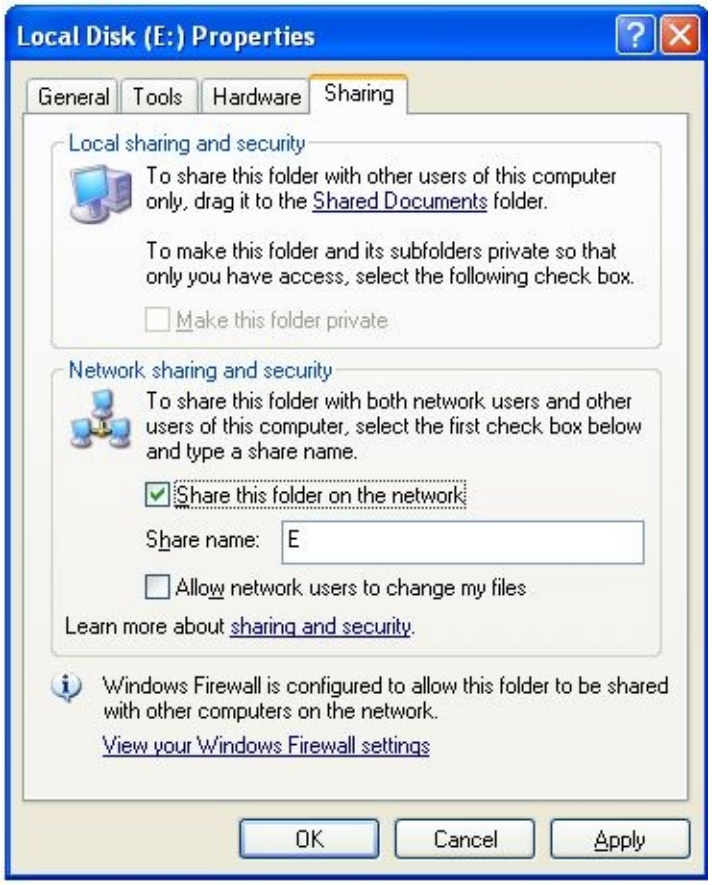
Specifies an optional comment that other people see when they look at your computer on the network. Use it to describe your computer (for example, your name, department, or location) or the type of information on it that you're sharing.





File Sharing

To give access to your Drives or folders to other on the network you have to share them, to do this right click on the drive or folder which you want to give access, and select the "Sharing and Security…" option and configure as the follows



Share Name **:** Specifies the name of the shared folder. You can use the suggested name or type a new one. When someone wants to use this folder, they will look for this name when they look at your computer on the network.

Access Type **:** Specifies the type of access you want others to have to this folder.

Note: If Network or File Sharing is not Accessible, Disable the Firewall in "My Network Places", "Local Area Connection" Properties as follows.

Printer Sharing:

To give access to your Printers to other on the network you have to share them , to do this first install printer driver by running “Setup” from Installation CD / DVD or selecting “Local Printer” option through “Add Printer” ,and select sharing. If already installed just right click on the printer and select the “Sharing” option as follows

Client Side:

1. In all clients in the same network Printer Driver will be Automatically Installed.

2. If not installed automatically then install by running Start, Printers and Faxes, Add Printer. And select “Network Printer” option and click on browse, then select the computer and printer.

(OR)

3. Open My Network Places and select workgroup Computers, and open the computer where the printer was installed and shared. Then double click on the printer name.

Message Sending

We can send instant messages to other computer by using the following command

C:\>NET SEND **User Name / Computer Name/ IP Address / Workgroup** “message”

Note: To send and receive messages "**Messenger**" service will be started on both computers in Windows XP.

Note : In Windows Vista / 7 use

C:\>MSG **User Name / Computer Name/ IP Address / Workgroup** "message"

Remote desktop Connection

With Remote Desktop on Windows XP Professional, you can have access to a Windows session that is running on your computer when you are at another computer. This means, for example, that you can connect to your work computer from home and have access to all of your applications, files, and network resources as though you were in front of your computer at work. You can leave programs running at work and when you get home, you can see your desktop at work displayed on your home computer, with the same programs running.

Advantages of Remote Desktop Connection

- Working at home - Access work in progress on your office computer from home, including full access to all local and remote devices.
- Collaborating - Bring your desktop to a colleague's office to debug some code, update a Microsoft PowerPoint slide presentation, or proofread a document.
- Sharing a console - Allow multiple users to maintain separate program and configuration sessions on a single computer, such as at a teller station or a sales desk.

Server Side Configuration:

1. Install LAN Card Driver and assign Fixed IP Address as usual.

(For Internet users IP address will be assigned automatically, by your ISP)

2. Right click on "My Computer" and select "Properties", "Remote" , "Remote Desktop"

3. Select "Allow users to connect remotely to this computer" option.

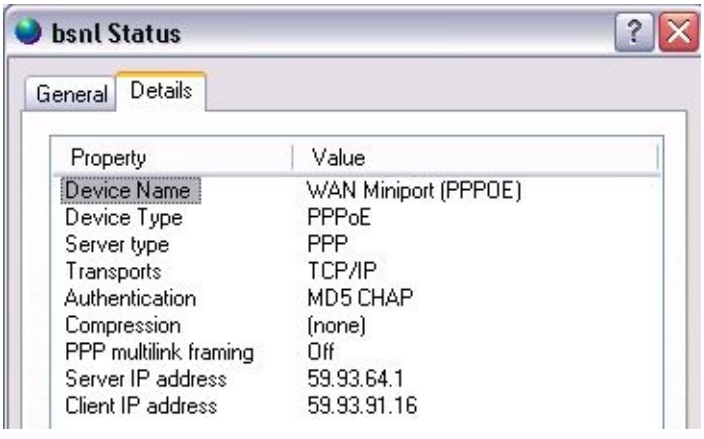
4. And Select Remote users by click on Add, Advanced, Find Now.

5. Remote users must have password Protection

5. Disable Firewall for this LAN connection or Internet Connection by Selecting My Network Places Properties, Local Area Network / Dial – Up / Broadband Properties, Advanced, Setting as follows.

Note : 1. If you want to use this Remote Desktop feature over Internet, Connect Internet as usual. After connection is established know your Internet IP address by

Right click on Internet connection Icon in system tray and select status and Details. And know the client IP address.



Client Side

1. Install LAN card Driver and assign Static IP Address as usual.

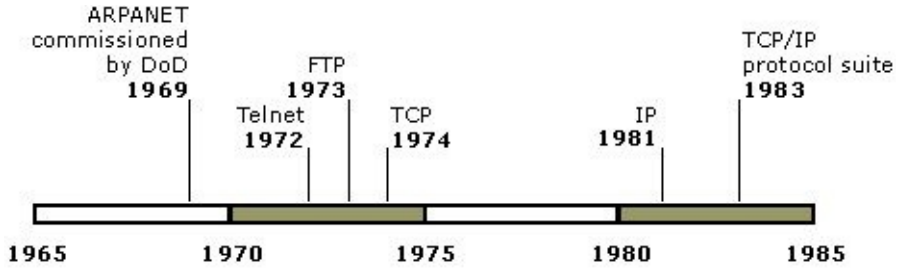
(For Internet users IP address will be assigned automatically, by your ISP)

2. Open Start, All Programs, accessories, communications, Remote Desktop connection and enter the IP address as follows.

3. To connect Local drives to Remote computer for file transfer select the disk drives in Local Resources, Local Devices, Local Drives as follows

TCP/IP

Transmission Control Protocol/Internet Protocol (TCP/IP) is a suite of industry-standard protocols. TCP/IP, also known as the Internet protocol, is a routable network protocol that also provides access to the Internet. TCP/IP has become the most common protocol for internetworking because of its capability to be used with almost any network operating system and equipment.



TCP/IP background

Transmission Control Protocol/Internet Protocol (TCP/IP) is an industry-standard suite of protocols designed for large-scale internetworks that span LAN and WAN environments.

As the following timeline shows, the origins of TCP/IP began in 1969, when the U.S. Department of Defense (DoD) commissioned the Advanced Research Projects Agency Network (ARPANET).

The ARPANET was the result of a resource-sharing experiment. The purpose was to provide high-speed network communication links between various supercomputers located at various regional sites within the United States.

Early protocols such as Telnet (for virtual terminal emulation) and the File Transfer Protocol (FTP) were first developed to specify basic utilities needed for sharing information across the ARPANET. As the ARPANET grew in size and scope, two other important protocols appeared:

- In 1974, the Transmission Control Protocol (TCP) was introduced as a draft specification that described how to build a reliable, host-to-host data transfer service over a network.
- In 1981, the Internet Protocol (IP) was introduced in draft form and described how to implement an addressing standard and route packets between interconnected networks.

On January 1, 1983, ARPANET began to require standard use of the TCP and IP protocols for all network traffic and essential communication. From this date forward, ARPANET started to become more widely known as the Internet and its required protocols started to become more widely known as the *TCP/IP protocol suite*.

The TCP/IP protocol suite is implemented in a variety of TCP/IP software offerings available for use with many computing platforms. Today, TCP/IP software remains widely in use on the Internet and is used often for building large routed private internetworks.

TCP/IP is made up of two protocols, TCP and IP. The TCP/IP suite, however, contains a number of other protocols that might pop up on the exam. The following sections will cover the TCP and IP protocols as well as some of the other protocols in the suite.

Transmission Control Protocol (TCP)

Transmission Control Protocol, TCP, is a connection-oriented protocol that functions on the Transport layer of the OSI model. When two computers on a network need to communicate, TCP opens a connection between the computers. When the data packet is ready to be sent, TCP adds to the packet header information that contains flow control and

error checking.

A computer may have more than one connection at a time. To make sure that the data goes to the right place, each connections is assigned a port number. The header on the data packet contains the port number to which the data needs to be delivered on the receiving computer. When the data arrives, the receiving computer delivers the data to the appropriate port, where an application is “listening” and ready to process the data.

How TCP works

TCP is based on point-to-point communication between two network hosts. TCP receives data from programs and processes this data as a stream of bytes. Bytes are grouped into segments that TCP then numbers and sequences for delivery.

Before two TCP hosts can exchange data, they must first establish a session with each other. A TCP session is initialized through a process known as a three-way handshake. This process synchronizes sequence numbers and provides control information that is needed to establish a virtual connection between both hosts.

Once the initial three-way handshake completes, segments are sent and acknowledged in a sequential manner between both the sending and receiving hosts. A similar handshake process is used by TCP before closing a connection to verify that both hosts are finished sending and receiving all data.

Internet Protocol (IP)

The Internet Protocol, IP, is a connectionless protocol that operates at the Network layer of the OSI model. When data packets are sent over the network, IP is responsible for addressing the packets and routing them through the network. Attached to each packet is an IP header that contains the sending address and the receiving address. If data is transmitted across networks that do not have the same packet size, the packets may be split up during transmission. If this happens, a new IP header is added to each part of the split packet. When the packets reach their final destination, the IP puts all the packets together again in the correct order.

TCP/IP configuration items

For Windows 2000 TCP/IP to function properly, you need to configure the following:

IP address

You must configure each interface on each TCP/IP node (host or router) with a unique IP address that is correct for the attached network segment. The IP address is a required configuration item.

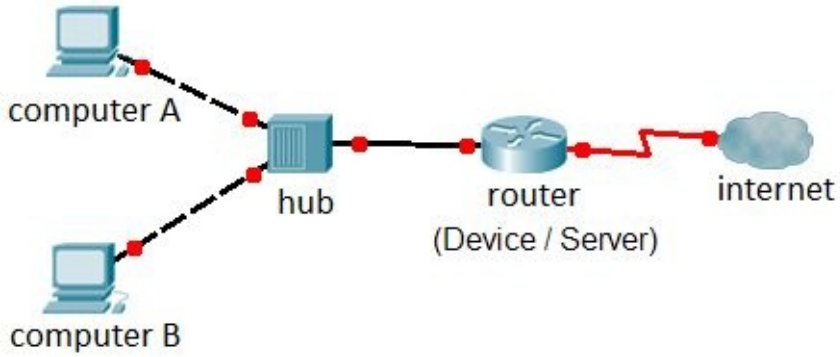
Subnet mask

You must configure each interface on each TCP/IP node (host or router) with a subnet mask that, when combined with the IP address, yields the network ID. All IP interfaces on the same network segment must use the same network ID. Therefore, all IP interfaces on the same network segment must use the same subnet mask. The subnet mask is a required configuration item.

Default gateway

To communicate with TCP/IP nodes on other network segments, you must configure at least one interface with the IP address of a default gateway (a local router that forwards remote TCP/IP traffic to its destination).

You do not need to configure a default gateway for a network that consists of a single network segment.



DNS server

A DNS server can resolve domain names to IP addresses. When a TCP/IP host is configured with the IP address of a DNS server, the TCP/IP host sends DNS name queries to the DNS server for resolution. A DNS server is required for computers running Active Directory–based Windows 2003 / 2008 Server .

You do not need to configure a DNS server for a network that consists of a single network segment.

TCP/IP Classes and Addresses

IP ADDRESS

IP addresses are similar to street addresses. The address 110 Main Street identifies what street you are on and in which house on that street you live. TCP/IP addresses simply switch this around, identifying the more general information first (network ID), followed by the more specific (host ID). Thus, the street address expressed like a

TCP/IP address would be Main Street 110.

The system views an IP address as a 32-bit binary number. Obviously, this would be difficult for most people to work with. Therefore, the address is entered in dotted decimal notation, such as 209.206.202.64. Each of the four numbers represents eight bits of the address, which means that each of the four can be between 0 and 255 (8 bits provide 256 possible combinations.)

SUBNET MASK

The subnet mask is a representation of the number of bits that represent the network ID. The portion that holds the network ID is set to all 1s, and the remainder (the host ID) is set to 0s.

Class A : Suitable for Large Networks (up to 16,646,144 Clients / Network)

1 - 126	0 – 255 0 – 255 1 - 254	IP Address

Network Address Host Address

255	0	0	0	Subnet Mask

11111111 00000000 00000000 00000000

Sample Network with Class A

IP Address: **96**.140.169.35 **96**.200.67.128 **96**.174.20.39

Subnet Mask: 255.0.0.0 255.0.0.0 255.0.0.0

Class B : Suitable for Medium Size Networks (up to 65,024 Clients / Network)

128 – 191 0 – 255	0 – 255 1 - 254

IP Address

Network Address Host Address

255	255	0	0

Subnet Mask

11111111 11111111 00000000 00000000

Sample Network with Class B

IP Address: **131.140.**169.35 **131.140**.67.128 **131.140.**20.39

Subnet Mask: 255.255.0.0 255.255.0.0 255.255.0.0

<u>Class C</u>: Suitable for Small Networks (up to 254 Clients / Network)

192 – 223 0 – 255 0 – 255	1 - 254

IP Address

Network Address Host Address

255	255	255	0

Subnet Mask

11111111 11111111 11111111 00000000

Sample Network with Class C

IP Address: **192.140.169**.35 **192.140.169**.128 **192.140.169**.39

Subnet Mask: 255.255.255.0 255.255.255.0 255.255.255.0

ADDRESSES SUMMARY

Class	First Octet	Number of Networks	Hosts/ Network	Total Hosts / Class
A	1 - 126	126	16,646,144	2,097,414,144
B	128 - 191	16,384	65,024	1,065,353,216
C	192 - 223	2,097,152	254	532,676,608
D	224 - 239	Reserved for Multicast Groups		
E	240 - 255	Reserved for Experimental Use		

Total Hosts in all Classes 3,695,443,968

Unicast

Unicast is a type of transmission in which information is sent from only one sender to only one receiver. In another words, Unicast transmission is between one-to-one nodes (involving two nodes only).

Broadcast

Broadcast is a type of transmission in which information is sent from just one computer but is received by all the computers connected to the network. This would mean that every time a computer or a node would transmit a packet of type ‘broadcast’, all the other computers will receive that information packet.

Multicast

In computer networking, **multicast** is the delivery of a message or information to a group

of destination computers simultaneously in a single transmission from the source creating copies automatically in other network elements, such as routers

Anycast

Anycast is a network addressing and routing methodology in which datagrams from a single sender are routed to the topologically nearest node in a group of potential receivers all identified by the same destination address.

Public and Private IP Addresses

A unique Internet Protocol (IP) address, known as a public IP address, is assigned to every computer that connects to the Internet. The IP addressing scheme makes it possible for computers to "find each other" online and exchange information. Within a private network, computers use addresses excluded by convention from use on the Internet. The difference between a private IP address and a public IP address then, is that private IP addresses are reserved for private networks, and public IP addresses are reserved for the Internet.

The Internet Assigned Numbers Authority (IANA), a once-autonomous organization, now works within the purview of the Internet Corporation for Assigned Names and Numbers (ICANN). IANA is responsible for overseeing global allocation of IP numbers, among other related protocols. Within the range of publicly available IP addresses are specific, excluded ranges withheld for private network use. These private IP ranges are as follows:

Reserved IP Addresses for Private Networks

The Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of the IP address space for private internets (local networks

Class A: 10 . X . X . X - Any IP Address beginning with 10

Class B: 172.16.X.X to 172.31.X.X - Any IP Address with 172.16 to 172.31

Class C: 192.168.X.X - Any IP Address Starting with 192.168

169.254.X.X - For automatic IP ADDRESS Generation

127.X.X.X - Internal loop back (Assigned for OS)

After assigning IP addresses we can test Network Communication by "**PING**" command

Ping is a computer network administration utility used to test the reachability of a host on an Internet Protocol (IP) network and to measure the round-trip time for messages sent from the originating host to a destination computer. The name comes from active sonar terminology.

Ex: C:\ > **Ping 192.168.0.2 –t** (192.168.0.2 is destination Computer IP address)

Ping localhost (127.X.X.X)

Pings your local computer. This is useful if you want to verify that your computer is able to send information out and receive information in return. Take note that pinging your local host computer does not send information over a network; however it can verify that your network card is being seen.

Now we can get the following Messages depends on situation

Transmit Error - LAN Card / Protocol Error

Hardware Failure - Problem between you and HUB

Request Timed Out - Problem with Destination Computer

Reply from 192.168.0.1: bytes=32 time - Everything Fine

Destination Host Unreachable - You are testing another network

To know IP address of a computer use **IPCONFIG** command in command Prompt

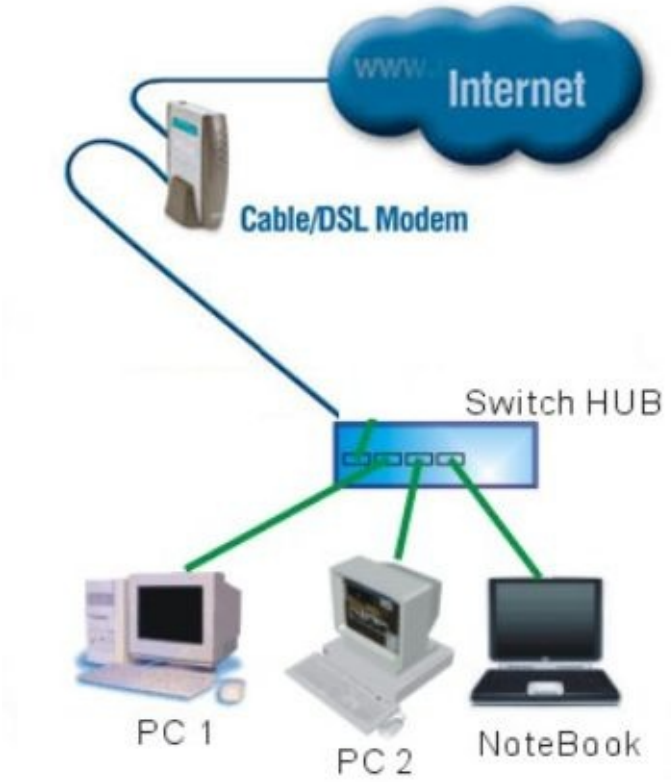
IPCONFIG Command options

/all Displays full configuration information

/release Releases the IP address for the specified adapter

/renew Renews the IP address for the specified adapter

Internet Connection Sharing in Windows XP



Server Side Configuration

1. Configure Internet connection as usual (Explained in Hardware course)
2. Right click on Internet Connection Icon and select properties, advanced.
3. Select “Allow other network users to connect through this computer’s Internet Connection” option.
4. And deselect “Establish a dial-up connection …” and “ Allow other network users…”
5. Server IP address will be automatically assigned to 192.168.0.1

Client Side Configuration

1. Install Network / LAN card driver (Ignore if already installed).

2. Run “IPCONFIG” command in “Command Prompt” to confirm and know the IP address.

3. If the Address appears as 169.254.X.X , this is not Server assigned IP Address. Then run **IPCONFIG / RENEW**. 4. Run **IPCONFIG /ALL** for all Address details.

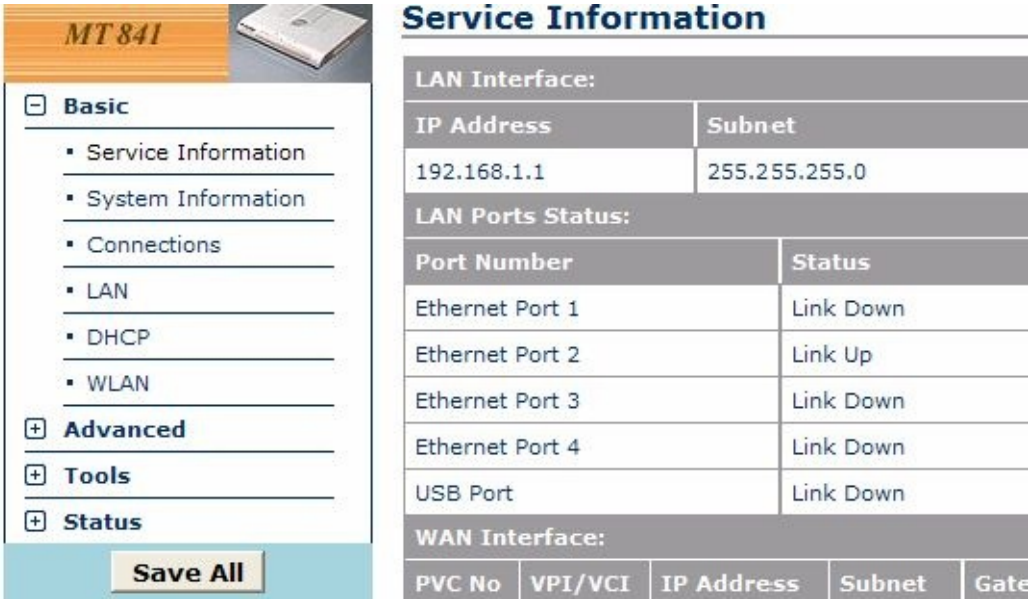
Note : If you want to assign Static IP address, we have to specify IP Address, Gateway and DNS address. (Enter Server IP address in Gateway and DNS (192.168.0.1))

Selecting ADSL MODEM as Internet Server (Old Modem)

1. Open Internet Explorer and type the address as 192.168.1.1 and enter.

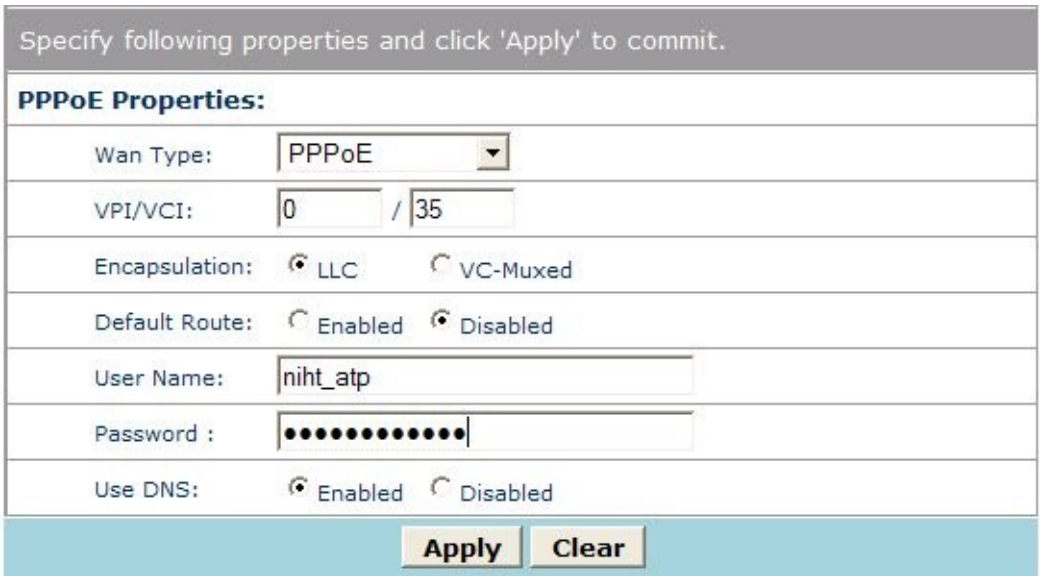
2. Enter User Name and Password as “admin and admin”

3. Now the following Web page appears in that select “Basic”, “Connections.”



4. Now remove the PVC with VPI /VCI values with 0/35

5. Select New and select WAN type as **PPPoE**, VPI/VCI values as 0 / 35 and Broadband user name and Password and apply as follows and save.



6. When Internet Connects the ADSL Link light will turn into orange from green.

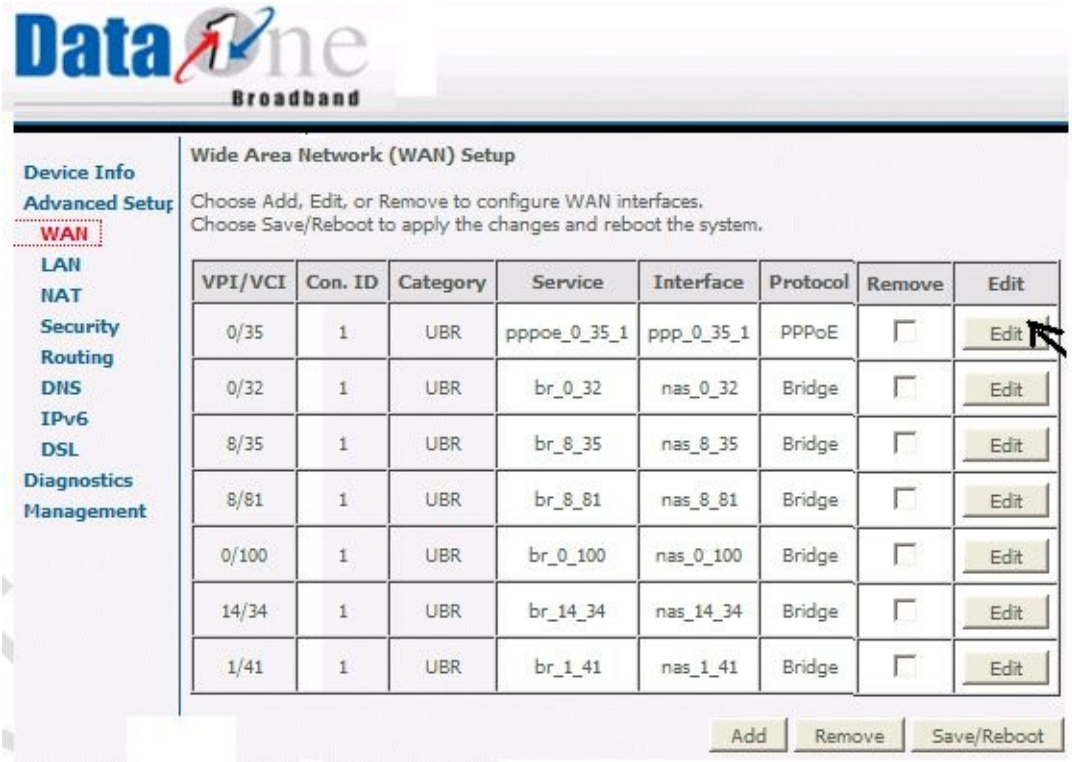
Deselecting ADSL MODEM as Internet Server

1. Now remove the PVC with VPI /VCI values with 0/35
2. Select New and select WAN type as **Bridge** and VPI / VCI values as 0 / 35

PPPoE: Point to Point Protocol over Ethernet **PVC:** Permanent Virtual Circuit

VPI: Virtual Path Identifier **VCI:** Virtual Circuit Identifier

Deselecting ADSL MODEM as Internet Server (New Modem)



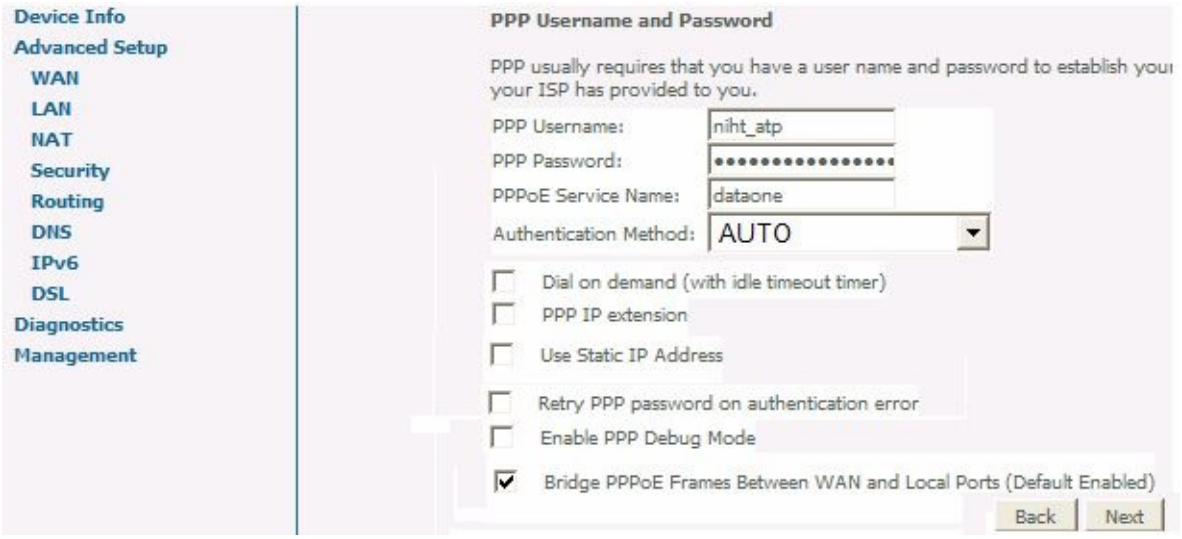
1. Select “WAN” in “Advanced Setup” and Edit the VPI/VCI values with 0/35
2. In “Connection” Type select **“Bridging”** and select next.

Selecting ADSL MODEM as Internet Server

1. Select “WAN” in “Advanced Setup” and Edit the VPI/VCI values with 0/35

2. In “Connection Type” select PPP over Ethernet **(PPPoE)** and select next.

3. In the following screen enter the broadband username & password and select next.



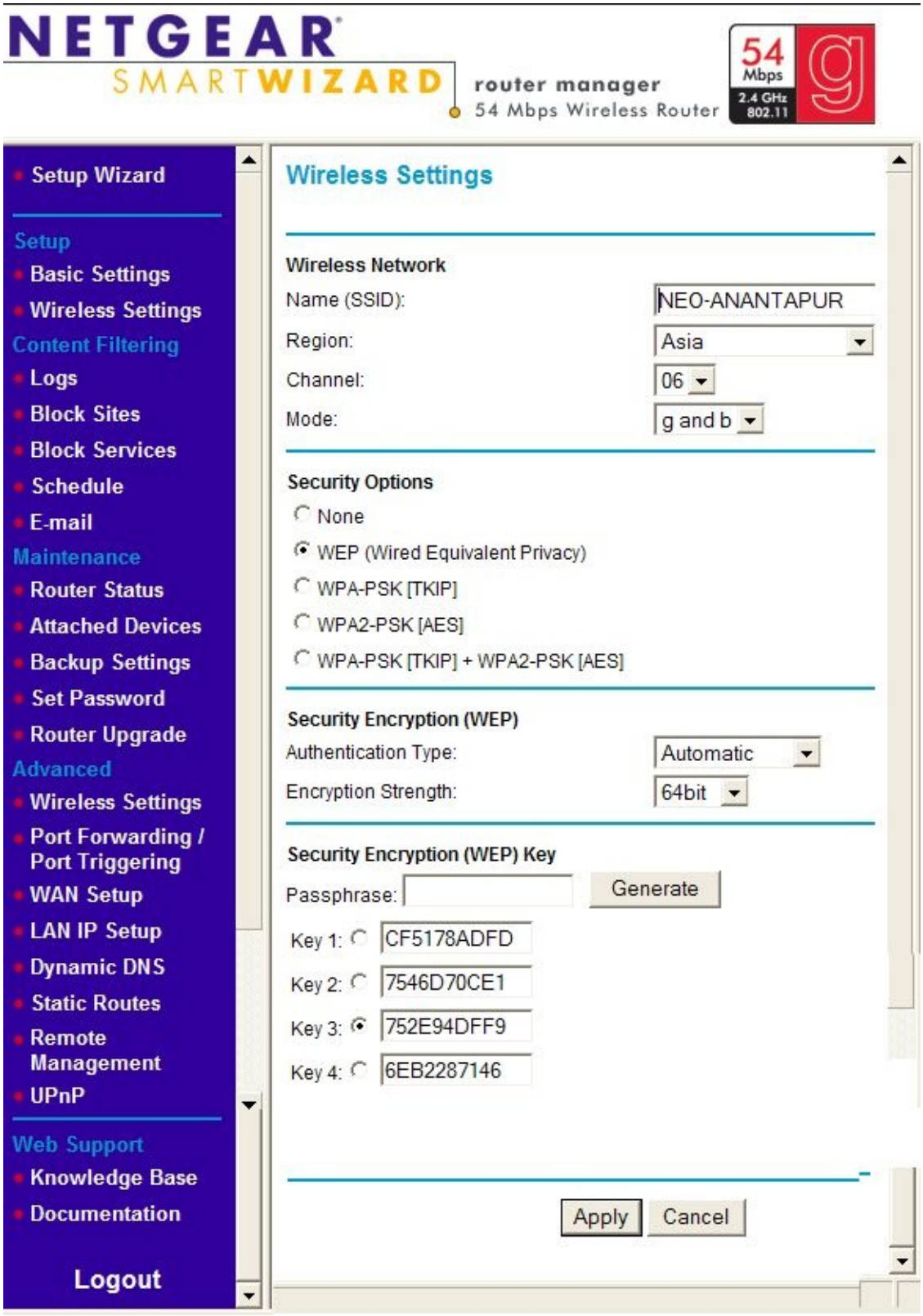
4. when Internet Connects the Internet light will glow.

Note: To change Broadband Password and Usage check open the website (http://selfcare.sdc.bsnl.co.in) and register.

Wireless Access Point Configuration

1. For first time (If wireless is not activated in Access point) use Copper cable.

2. In client Computer remove the IP address and open the Internet Explorer and enter the address as 192.168.1.1 and enter, then the following web page will appear.



Channels in 802.11b/g Networks

Channel	Frequency GHz / MHz	North America	Japan	Most of world
1	2.412 / 2412	Yes	Yes	Yes
2	2.417 / 2417	Yes	Yes	Yes

3	2.422 / 2422	Yes	Yes	Yes
4	2.427 / 2427	Yes	Yes	Yes
5	2.432 / 2432	Yes	Yes	Yes
6	2.437 / 2437	Yes	Yes	Yes
7	2.442 / 2442	Yes	Yes	Yes
8	2.447 / 2447	Yes	Yes	Yes
9	2.452 / 2452	Yes	Yes	Yes
10	2.457 / 2457	Yes	Yes	Yes
11	2.462 / 2462	Yes	Yes	Yes
12	2.467 / 2467	No	Yes	Yes
13	2.472 / 2472	No	Yes	Yes
14	2.484 / 2484	No	b	No

Wireless Network

Name (SSID)

Enter a value of up to 32 alphanumeric characters. The same Name (SSID) must be assigned to all wireless devices in your network. The default SSID is NETGEAR, but NETGEAR strongly recommends that you change your network's Name (SSID) to a different value. This value is also case-sensitive. For example, *NETGEAR* is not the same as *NETGEAr*.

Region

Select your region from the drop-down list. This field displays the region of operation for which the wireless interface is intended. It may not be legal to operate the router in a region other than the region shown here. If your country or region is not listed, please check with your local government agency or check our web site for more information on which channels to use.

Channel

This field determines which operating frequency will be used. It should not be necessary to change the wireless channel unless you notice interference problems with another nearby access point.

Mode

Select the desired wireless mode. The options are:

g & b - Both 802.11g and 802.11b wireless stations can be used.

g only - Only 802.11g wireless stations can be used.

b only - All 802.11b wireless stations can be used. 802.11g wireless stations can still be used if they can operate in 802.11b mode.

The default is “g & b”, which allows both “g” and “b” wireless stations to access this device.

Security Options

1. None - no data encryption

2. WEP - Wired Equivalent Privacy, use WEP 64- or 128-bit data encryption

3. WPA-PSK [TKIP] - Wi-Fi Protected Access with Pre-Shared Key, use WPA-PSK standard encryption with TKIP encryption type

4. WPA2-PSK [AES] - Wi-Fi Protected Access version 2 with Pre-Shared Key, use WPA2-PSK standard encryption with the AES encryption type

5. WPA-PSK [TKIP] + WPA2-PSK [AES] - Allow clients using either WPA-PSK [TKIP] or WPA2-PSK [AES]

Security Encryption (WEP)

Authentication Type

Normally this can be left at the default value of “Automatic.” If that fails, select the appropriate value - “Open System” or “Shared Key” Check your wireless card’s documentation to see what method to use.

Encryption Strength

Select the WEP Encryption level:

64-bit (sometimes called 40-bit) encryption

128-bit encryption

Security Encryption (WEP) Key

If WEP is enabled, you can manually or automatically program the four data encryption keys. These values must be identical on all PCs and Access Points in your network.

Automatic Key Generation (Passphrase)

Enter a word or group of printable characters in the Passphrase box and click the Generate button to automatically configure the WEP Key(s). If encryption strength is set to 64 bit, then each of the four key boxes will automatically be populated with key values. If encryption strength is set to 128 bit, then only the selected WEP key box will automatically be populated with key values.

Manual Entry Mode

Select which of the four keys will be used, and enter the matching WEP key information for your network in the selected key box.

For 64-bit WEP - Enter ten hexadecimal digits (any combination of 0-9, A-F).

For 128-bit WEP - Enter twenty-six hexadecimal digits (any combination of 0-9, A-F).

Be sure to click Apply to save your settings in this menu.

Security Encryption (WPA-PSK, WPA2-PSK, WPA-PSK + WPA2-PSK)

Enter a word or group of printable characters in the Passphrase box. The Passphrase must be 8 to 63 characters in length.

Note: 1. By Setup, Basic setting you can setup wireless router as Internet Server.

2. By Advance, LAN IP you can change access point Address. And also you can enable or disable the DHCP server

3. By Advanced, Wireless setting you can provide security through MAC addresses.

10 Tips for improving your wireless network

1. Position your wireless router (or wireless access point) in a central location

When possible, place your wireless router in a central location in your home. If your wireless router is against an outside wall of your home, the signal will be weak on the other side of your home. Don’t worry if you can’t move your wireless router, because there are many other ways to improve your connection.

2. Move the router off the floor and away from walls and metal objects (such as metal file cabinets)

Metal, walls, and floors will interfere with your router’s wireless signals. The closer your router is to these obstructions, the more severe the interference, and the weaker your connection will be.

3. Replace your router’s antenna

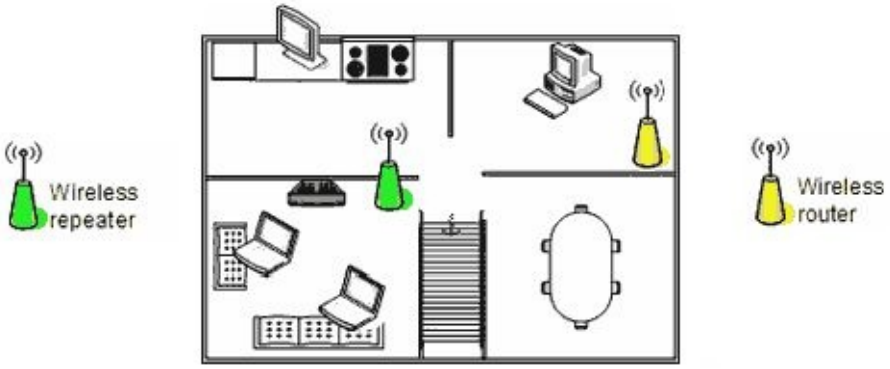
The antennas supplied with your router are designed to be omni-directional, meaning they broadcast in all directions around the router. If your router is near an outside wall, half of the wireless signals will be sent outside your home, and much of your router’s power will be wasted. Most routers don’t allow you to increase the power output, but you can make better use of the power. Upgrade to a hi-gain antenna that focuses the wireless signals only one direction. You can aim the signal in the direction you need it most.

4. Replace your computer’s wireless network adapter

Wireless network signals must be sent both to and from your computer. Sometimes, your router can broadcast strongly enough to reach your computer, but your computer can’t send signals back to your router. To improve this, replace your laptop’s PC card-based wireless network adapter with a USB network adapter that uses an external antenna. In particular, consider the Hawking Hi-Gain Wireless USB network adapter, which adds an external, hi-gain antenna to your computer and can significantly improve your range.

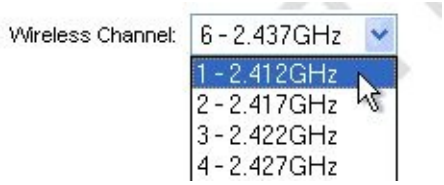
5. Add a wireless repeater

Wireless repeaters extend your wireless network range without requiring you to add any wiring. Just place the wireless repeater halfway between your wireless access point and your computer, and you'll get an instant boost to your wireless signal strength. Check out the wireless repeaters from ViewSonic, D-Link, Linksys, and Buffalo Technology.



6. Change your wireless channel

Wireless routers can broadcast on several different channels, similar to the way radio stations use different channels. In the United States and Canada, these channels are 1, 6, and 11. Just like you'll sometimes hear interference on one radio station while another is perfectly clear, sometimes one wireless channel is clearer than others. Try changing your wireless router's channel through your router's configuration page to see if your signal strength improves. You don't need to change your computer's configuration, because it'll automatically detect the new channel.



7. Reduce wireless interference

If you have cordless phones or other wireless electronics in your home, your computer might not be able to “hear” your router over the noise from the other wireless devices. To quiet the noise, avoid wireless electronics that use the 2.4GHz frequency. Instead, look for cordless phones that use the 5.8GHz or 900MHz frequencies.

8. Update your firmware or your network adapter driver

Router manufacturers regularly make free improvements to their routers. Sometimes, these improvements increase performance. To get the latest firmware updates for your router, visit your router manufacturer’s Web site.

9. Pick equipment from a single vendor

While a Linksys router will work with a D-Link network adapter, you often get better performance if you pick a router and network adapter from the same vendor. Some vendors offer a performance boost of up to twice the performance when you choose their hardware: Linksys has the SpeedBooster technology, and D-Link has the 108G enhancement.

10. Upgrade 802.11g devices to 802.11n

Internet Information Services (IIS) – In Windows XP

The powerful features in Internet Information Services (IIS), a part of Microsoft Windows, make it easy to share documents and information across a company intranet or the Internet. Using IIS, you can deploy scalable and reliable Web-based applications, and you can bring existing data and applications to the Web. Windows XP supports 10 simultaneous client connections only.

FTP Service

Transfers files to and from a computer running an FTP server service

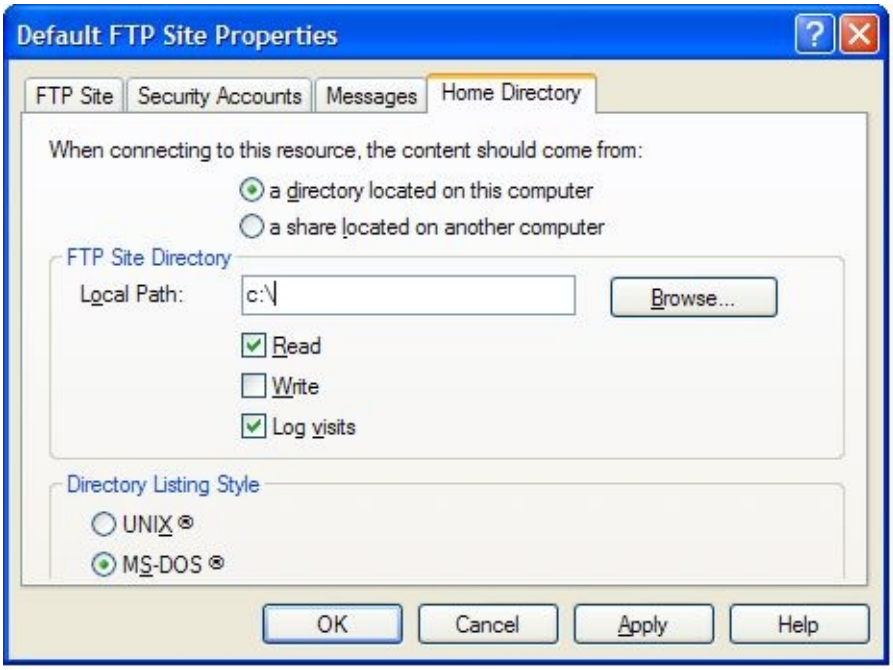
Server side configuration (Windows XP):

1. Add File Transfer Protocol (FTP) service through Start, Settings, Control Panel, Add/Remove Programs, Add/Remove Windows Components, Internet Services Information (IIS). (Now insert Windows XP CD).

2. To open Internet Information Services, Right click on My Computer and select “Manage” in Computer Management Double click on “Services and Applications” and on “Internet Information Services”.

3. In FTP Sites Right click on Default FTP site and select properties.

4. In Home Directory enter the local path (which you want give access) as follows.



Client Side (Windows XP / Vista / 7)

1. Connect to LAN / Internet.

2. Open internet explorer, in Address bar enter server IP Address (Local / Internet)

3. Folders and Files in the server will be displayed.

NOTE : To know Server IP address, Run “**IPCONFIG**” command in Server Computer.

after connected to the Internet.

WWW Service

Share information across a company intranet or the Internet through interlinked hypertext documents . With a web browser, one can view web pages that may contain text, images, videos, and other multimedia and navigate between them via hyperlinks.

Server side configuration (Windows XP):

1. Add World Wide Web (WWW) Service through Start, Settings, Control Panel, Add/Remove Programs, Add/Remove Windows Components, Internet Services Information (IIS). Ignore if already installed.

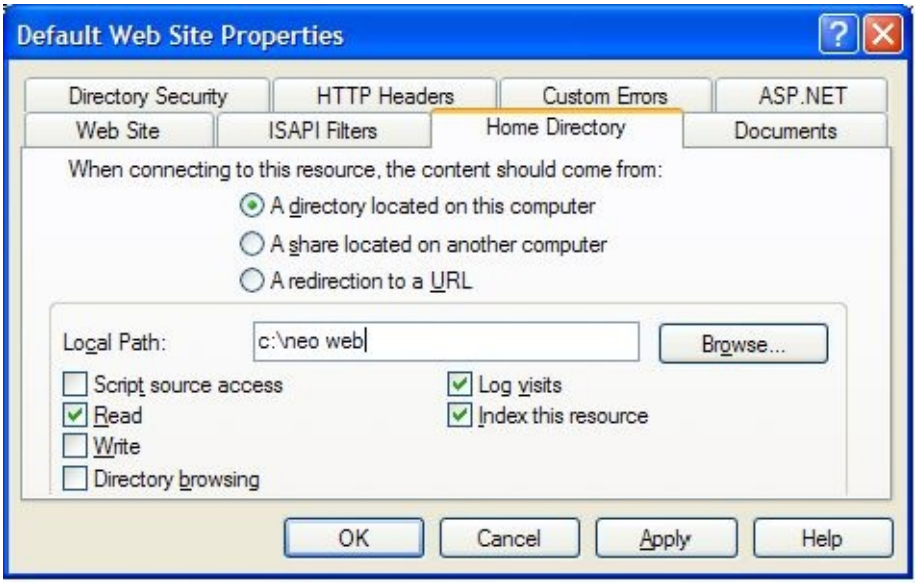
2. **For Practice** Copy \utility\neo web directory from **Drivers CD** into C drive.

(It Contains default.htm file)

3. To open Internet Information Services, Right click on My Computer and select “Manage” in Computer Management Double click on “Services and Applications” and on “Internet Information Services”.

4. In Web Sites Right click on Default WEB website and select properties

5. In home directory enter the local path as c:\neo web



Client Side (Windows XP / Vista /7):

1. Connect to LAN / Internet.

2. Open internet explorer in Address bar enter Server IP Address (Local / Internet)

3. Neo InfoTech Web Page will be displayed.

NOTE : To know Server IP address, Run "**IPCONFIG**" command in Server Computer after connected to the Internet.

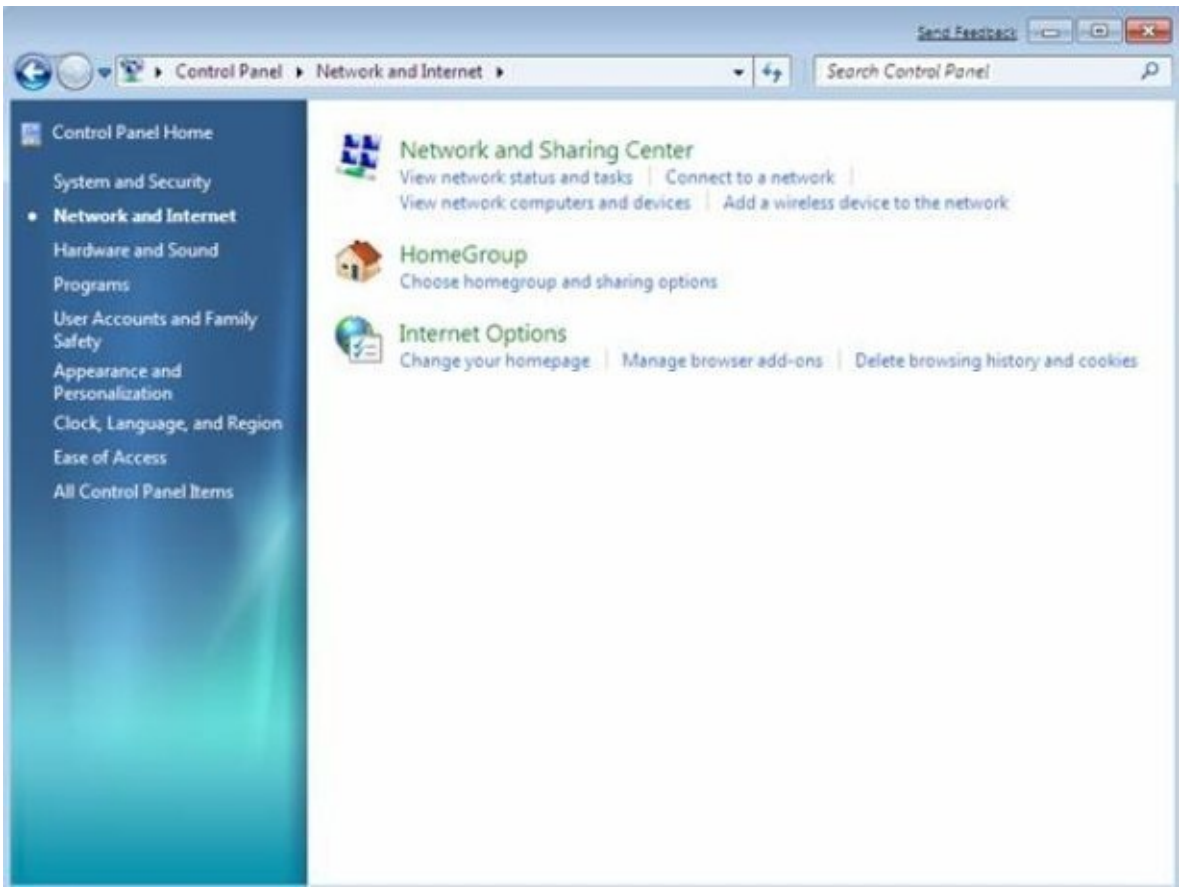
Networking in Windows 7

Introduction

At first glance there aren’t too many differences between configuring Windows 7 networking and configuring Windows Vista networking. However, there are important differences once you start using Windows 7. Let us find them out.

Navigation – getting to Windows 7 Network Configuration

How do you get to Windows 7 Network configuration? Just go to the **Start Menu**, then to **Control Panel**, and click on **Network and Internet**. You also can get to your network configuration, using the same navigation path in Windows Vista. However, when you get to the **Network and Internet** settings in Windows Vista, you will see a lot more options. Let us compare by starting with the Windows 7 **Network and Internet** window (shown in Figure , below).



Windows 7 Network and Internet Configuration

As you can see this new Windows 7 configuration window offers you a few new choices and a few old choices but, overall, not a lot of choices to choose from. We are used to seeing both the Network and Sharing Center and the Internet Options but the HomeGroup is new. I will come back to HomeGroup and the new and improved Network and Sharing Center in Windows 7, below.

Now let us compare what we saw in Windows 7 to the Network and Internet configuration in Windows Vista, shown in Figure 2, below:

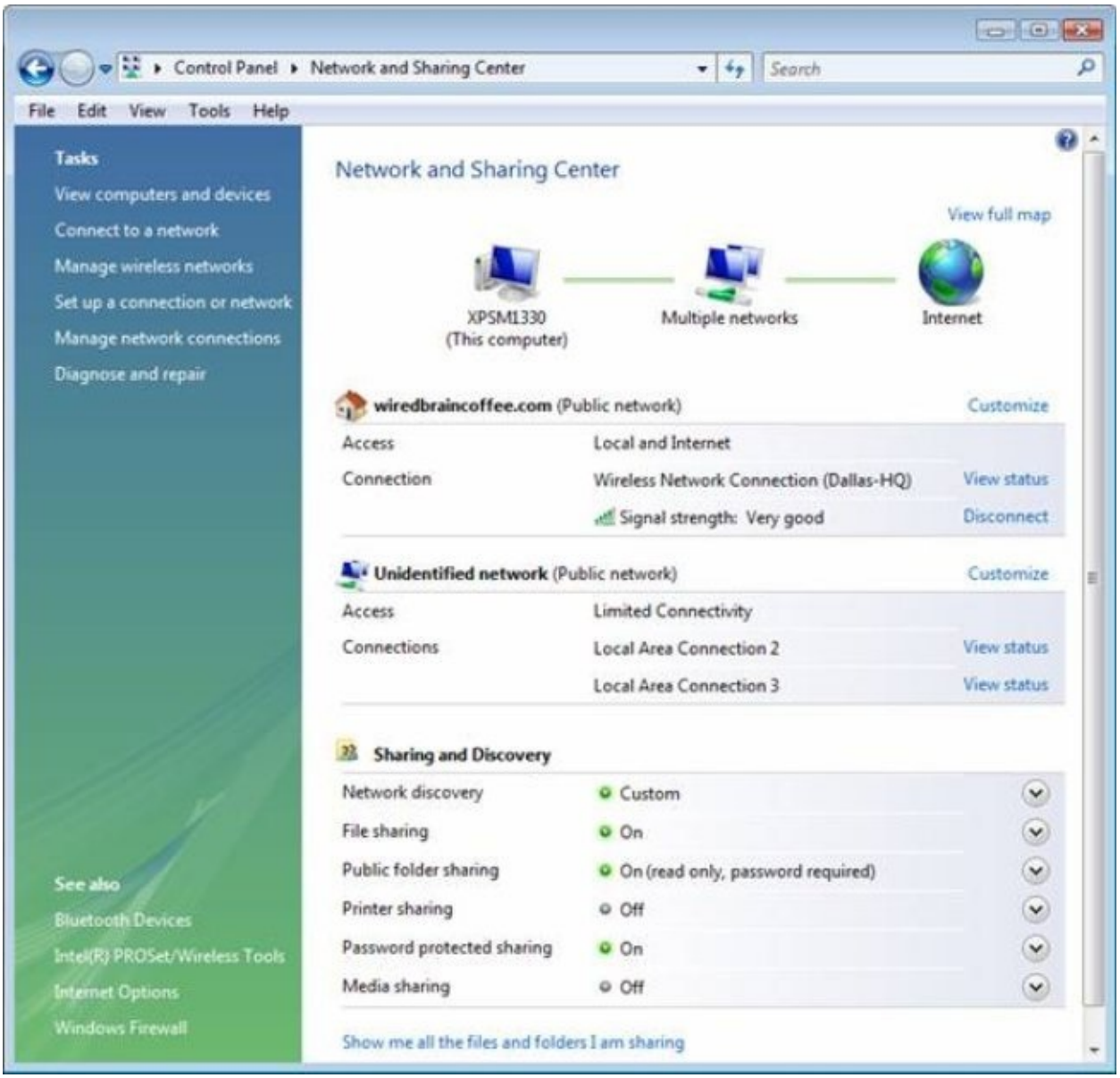
Windows Vista Network and Internet Configuration

The first thing you notice is that there are tons of options to choose from in Vista. However, I do not think that this is such a good thing as some of these seem much less important than others. For example, I don’t think that the Windows Firewall or Offline Files deserve their own section here (these are removed in Windows 7).

Windows 7 Network and Sharing Center

99% of the time, in Windows 7 or Vista, to configure networking, you are going to click on the **Network and Sharing Center**. It offers the most functionality and the most common tasks that a Windows Vista or 7 Administrator would perform. So, let us look at how the Network and Sharing Center differs between these two operating systems.

First, here is the Network and Sharing Center from Windows Vista that most of us are familiar with:



Windows Vista Network and Sharing Center

Now, let us compare that to Windows 7's Network and Sharing Center, below in Figure.

Windows 7 Network and Sharing Center

One of the big differences is caused by these two computers being different. The Vista computer has many more network adaptors as compared to the Windows 7 computer. That aside, as you can see, the Windows 7 computer actually has many fewer options than the Vista computer. Options have been removed from the left navigation and the Sharing and Discovery options have been removed from the main window. These options have just been moved to other sections.

The Network and Sharing options have been moved to the **Choose homegroup and sharing options** window (which we will look at in a minute). The left navigation options shown on the Vista computer have just been moved to the level above this, Network and Internet.

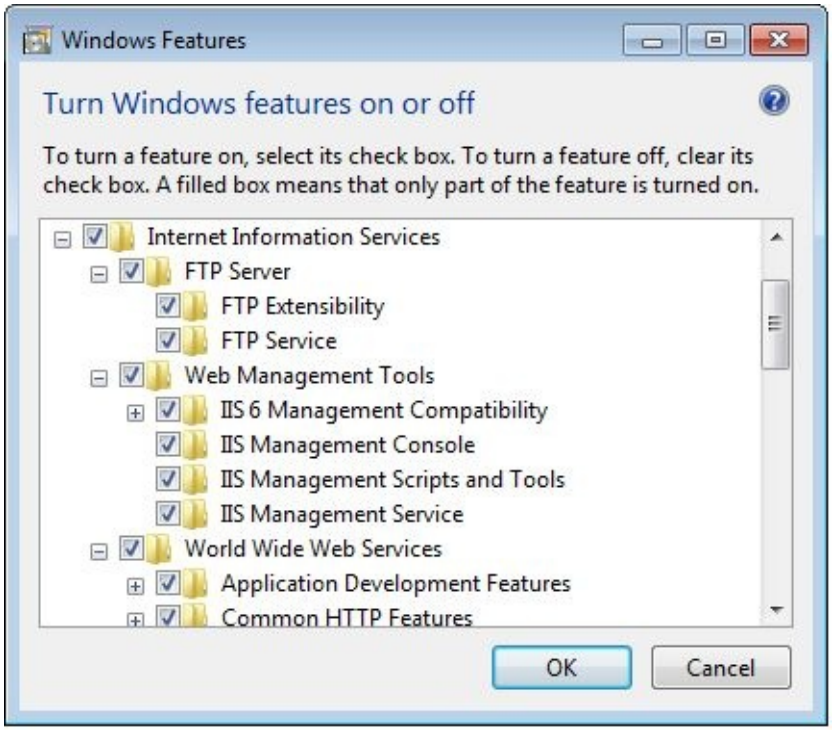
What I like about the new Windows 7 Network and Sharing center is that the less related options have been moved off to reduce the clutter on the page. There are two things that I do not care for, concerning the changes with the Network and Sharing center:

- Why did they remove the **Sharing and Discovery** options from this page? I mean, it is not that what the Network and Sharing center should have – sharing and discovery options?
- Also, I have never cared for how in Vista or Windows 7 there are no technical networking details on the network and sharing center page. I should be able to see if I have an IP address here. I should be able to see if it is 169.254.xxx.xxx automatic (useless) IP address or if it is a real IP address. I would think that they would have added / improved this in Windows 7.

IIS – In Windows 7

Add Internet Information Services In Windows 7 (Server)

To add Internet Information Services, Open Control Panel, Programs and Features, “Turn Windows Features On or Off”, and select the following Services.



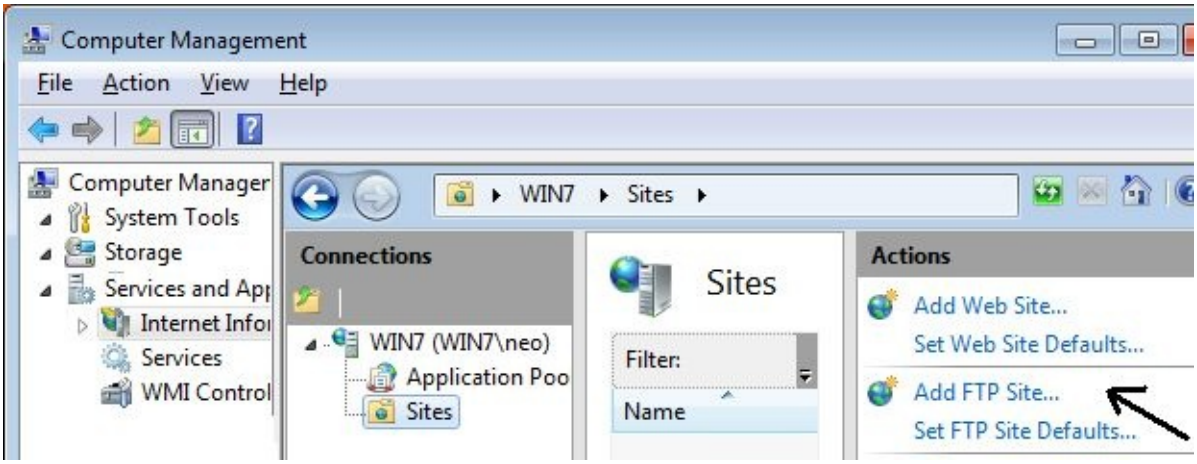
FTP Service

Server side configuration (Windows 7):

1. To open Internet Information Services, Right click on My Computer and select “Manage” in Computer Management Double click on “Services and Applications” and on “Internet Information Services”

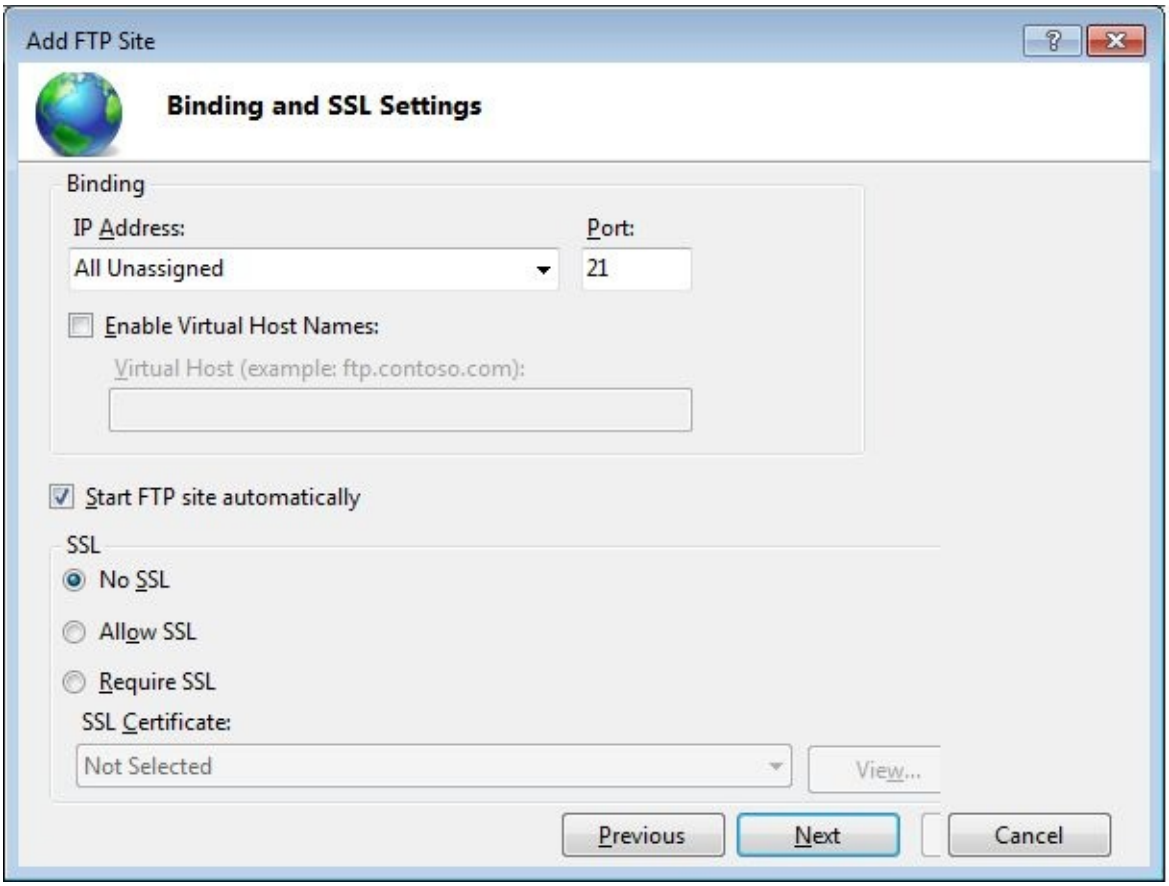
2. In Connections, Server Name, Sites remove all Sites.

3. In Actions select “Add FTP Site…” as follows.

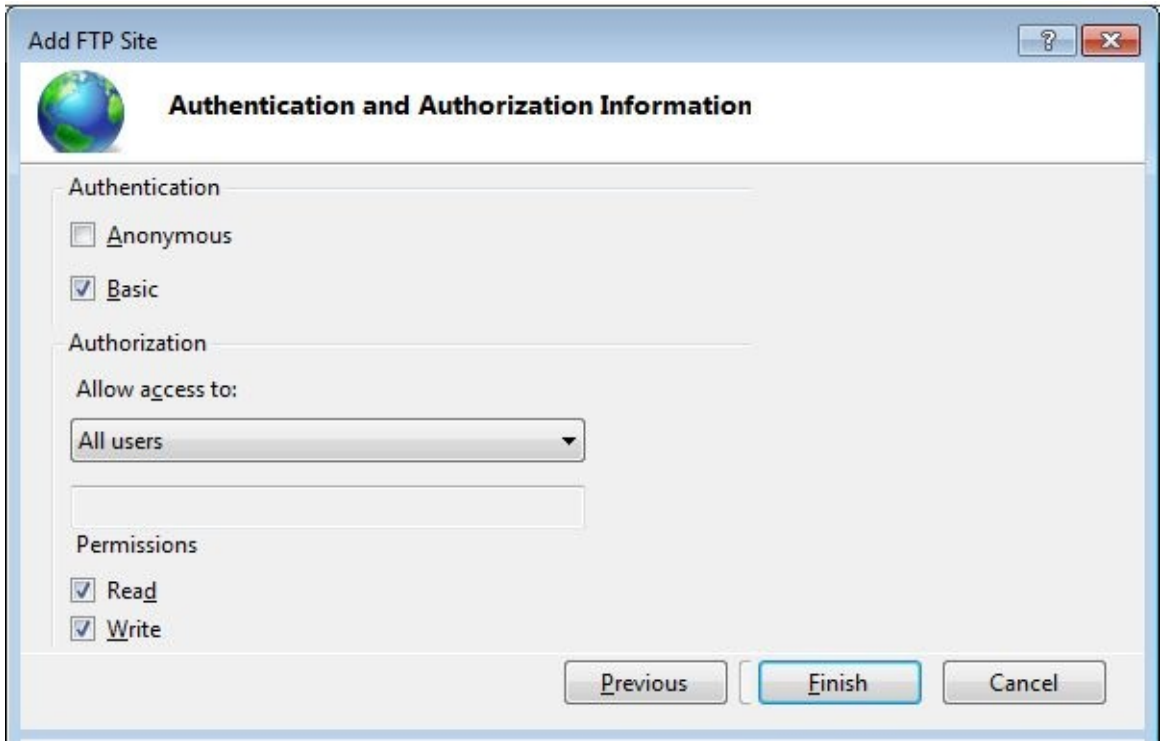


4. Now enter “FTP site Name”, “Physical path”.

5. In Binding and SSL Setting select “No SSL” in SSL as follows.



6. In Authentication and Authorization select “Basic” and “All Users” as follows (Select “Anonymous” to access anybody, “Basic” to access only Windows 7 users.)



In clients open Internet Explorer and enter server address as FTP://192.168.0.1

WWW Service

Server side configuration (Windows 7):

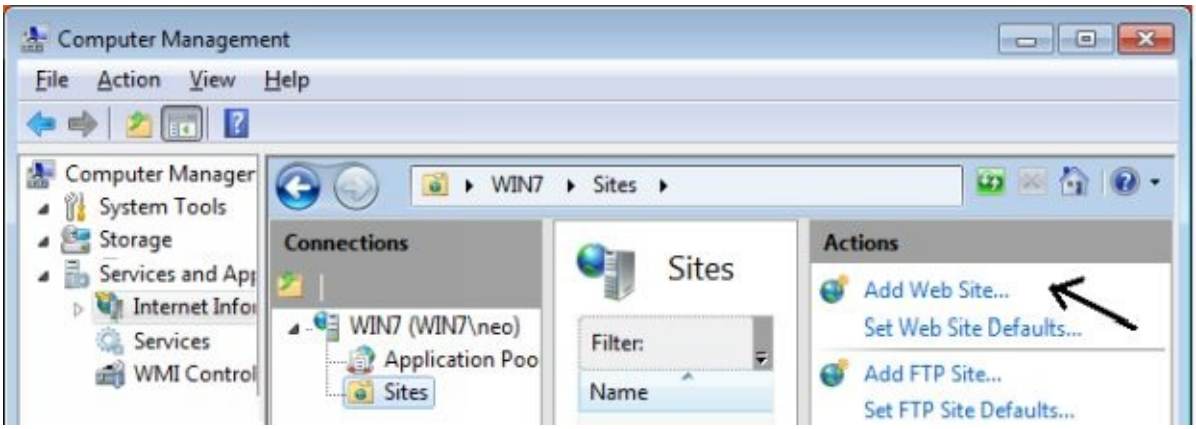
1. **For Practice** Copy \utility\neo web directory from **Drivers CD** into D drive.

(It Contains default.htm file)

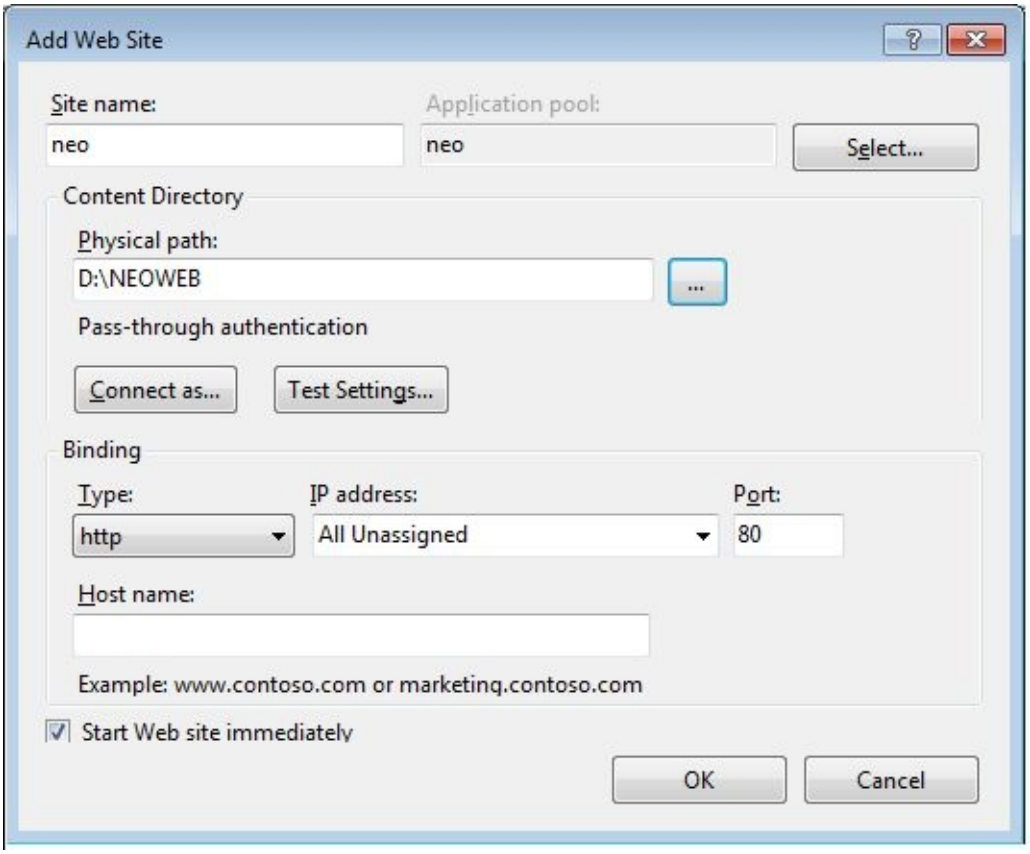
2. To open Internet Information Services, Right click on My Computer and select “Manage” in Computer Management Double click on “Services and Applications” and on “Internet Information Services”.

3. In Connections, Server Name, Sites remove all Sites.

4. In Actions select “Add Web Site…” as follows.



5. Now enter Site name and Physical path as follows



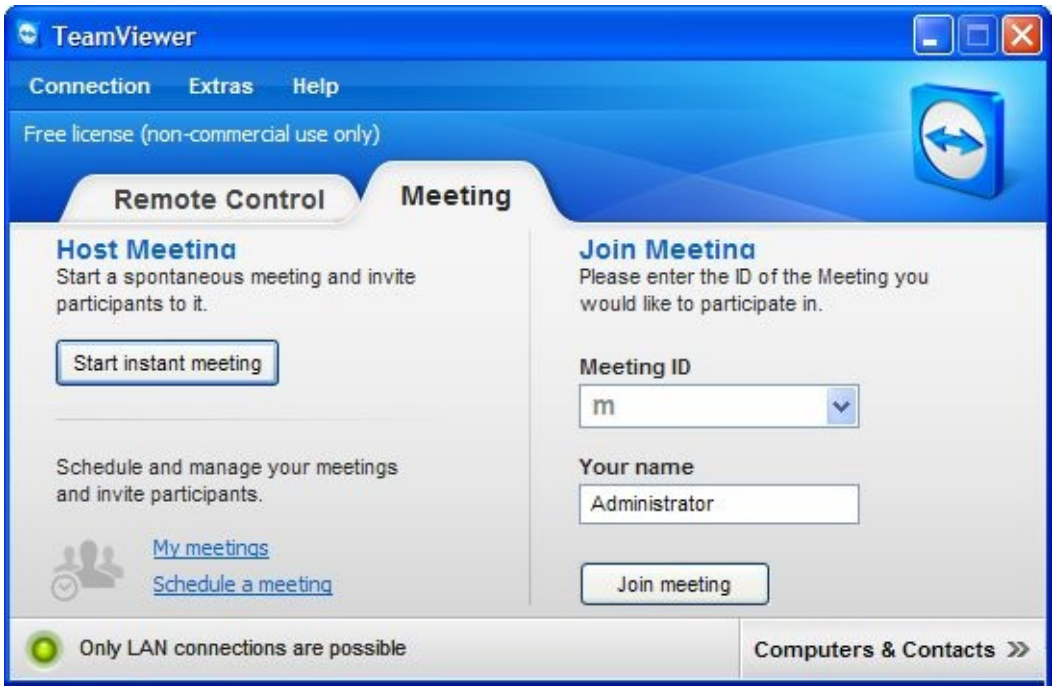
In clients open Internet Explorer and enter server address as HTTP://192.168.0.1

TeamViewer

TeamViewer is an excellent screen-sharing and file-transfer app that can be used to facilitate business collaborations, remotely access a second computer, or help distraught relatives diagnose and cure computer problems. Along with being free for non corporate use, it gives users precisely the tools they need to share screens securely, send files with a minimum of hassle, control access rights, and even flip which user has control.

The options available while you're in control work smoothly. You can maximize the pane that the other computer's screen is visible in, as well as utilize several smart options from a drop-down toolbar in the center of the window. A big X lets you close the connection, while the Actions button lets you switch who's in control, disable remote input, and reboot remotely. The View menu hides options to adjust the screen resolution, the optimization toward speed or quality, and control multiple-monitor displays. New features that work just as effortlessly as the old ones include VoIP audio and video conferencing, and integrated teleconferencing. These features push TeamViewer a notch above the rest because they will work without requiring firewall reconfiguration.

When you log in, you're given an access code and a password. Sharing those allows your computer to be controlled by the level you set it to: remote support, presentation, file transfer, or VPN. The TeamViewer servers remember which computers you've connected to, so reconnecting to previously shared computers happens faster. TeamViewer also has a Web-based version, for remote connecting to home from public computer. Even the installation process is impressive. Users can toggle admin rights, can opt out of running at startup, and can opt into installing the TeamViewer VPN driver for more secure screen sharing. TeamViewer makes screen-sharing and file-sharing as fluid and unobtrusive as it should be, and is a must-have for the home or remote office user.


TeamViewer
Connection
Extras
Help
Free license (non-commercial use only)
Remote Control
Meeting
Host Meeting
Start a spontaneous meeting and invite participants to it.
Start instant meeting
Schedule and manage your meetings and invite participants.
My meetings
Schedule a meeting
Join Meeting
Please enter the ID of the Meeting you would like to participate in.
Meeting ID
m
Your name
Administrator
Join meeting
Only LAN connections are possible
Computers & Contacts


Free license (non-commercial use only)
Participants
Meeting ID
m16-918-698
Administrator (Presenter)
Invite...
Screen sharing
Presenting screen
File box
My video
Voice over IP
Conference call
Whiteboard
on
off