INDEX

Sr. No.	Experiment Description	Experiment Date	Submission Date	Remark/ Signature
01	Introduction to local area network with its cable, connectors and topology			
02	Case study of Ethernet (10 base 5, 10 base 2, 10 base T)			
03	Installation and working of net meeting and remote desktop			
04	Installation and working with telnet			
05	Working with null modem			
06	Installation of windows 2003 server/ Windows 2000 server			
07	Configuration of DHCP			

1. Experiment – 1

1.1. Object : Instruction to Local Area Network with its cables, connectors and topologies.

1.2. Local Area Network :

LANs are privately owned network with maximum span of 10Km and provides local connectivity within a single building or campus of few Kilometer in size.
LANs are distinguished from other kinds of networks by three characteristics:
Size : LANs are restricted in size, transmission time is bounded and known inadvance and thus ease of maintenance
Transmission technology : consisting of single cable to which all the machinesare attached. Runs at speed of 10 to 100 Mbps
Topology : Like BUS, STAR, TREE, HYBRID etc.

1.3. Transmission Media :

Transmission media can be divided into two broad categories : GUIDED AND UNGUIDED MEDIA.

- GUIDED MEDIA(CABLE)

Guided media is the one which provides a conduit from one device to another; include twisted pair cable, co-axial cable and fiber optic cable.
Twisted and co-axial use metallic (Cu) conductor that transport signals in the form of electric current, whereas optical fiber is a glass or plastic cable and transport signal in the form of light.

Twisted Pair Cable
Frequency range of Twisted Pair Cable is 100 Hz to 5 MHz.Twisted pair cable comes in two forms : 1 Unshielded Twisted Pair (UTP), 2 Shielded Twisted Pair (STP).

Unshielded Twisted Pair (UTP)
UTP is the most common type of telecomm. Medium and is use in telephone system,which consists of two conductor (Cu), each with of different plastic color insulation toidentify specific conductor.

Advantage of UTP
UTP is cheap, flexible and easy to install, higher grade of UTP are used in many LAN technologies.

UTP cable standardsEIA has developed standard to grade UTP cables by Quality with 1 as lowest and 5 as highest
Category 1: Used for telecommunication system. Works fine for voice transmissionbut not for low-speed data transmission.
Category 2: Suitable for voice and data transmission up to 4 Mbps.
Category 3: Required to have at least 3 twists per foot and used for transmission up to10 Mbps.
Category 4: It must also have at least 3 twists per foot and is capable of transmissionrates up to 16 Mbps
Category 5: Used for data transmission up to 100 Mbps.

UTP connector
UTP is most commonly connected to n/w devices via a snap-in plug like RJ45connector with 8 conductors.

Shied Twisted Pair Cable (STP)
STP has a metal foil or braided-mesh covering that encases each pair of insulatedconductors. The metal casing prevents the penetration of electromagnetic noise. Through the use of STP we can eliminate the phenomenon called cross talk. STP has the same quality consideration as UTP. STP is more expensive than that of UTP but less susceptible to noise.

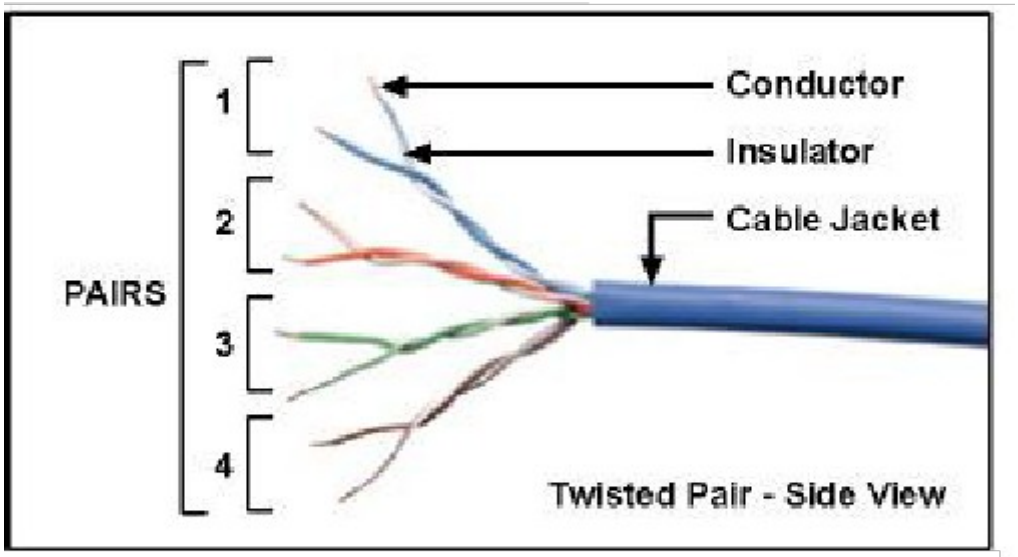


Fig 1.1 Twisted pair Cable

STP connector
STP Uses same connectors as UTP but shield must be connected to ground.

Co-axial cable
Coaxial cable carries signal of higher frequency ranges (100 KHz – 500 Mhz). Coax has a central core conductor of solid or stranded wire enclosed in an insulatingsheath, which in turn, encased in an outer conductor of metal foil, braid, or acombination of two (usually copper). The outer metallic wrapping serves both as a shield against noise and secondconductor which completes the circuit. The outer conductor is also enclosed in an insulating sheath and the whole cable isprotected by a plastic cover.

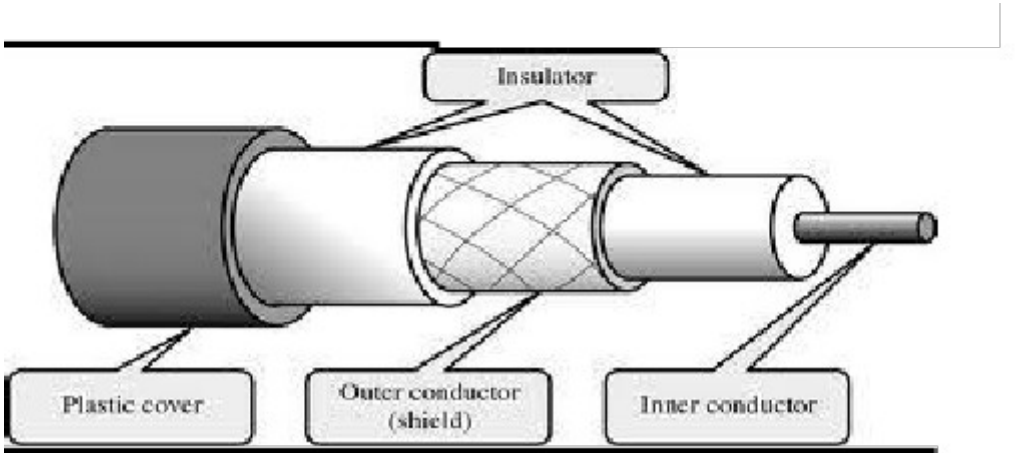


Fig 1.2 Coaxial Cable

Coaxial cable standards Different coaxial cable designs are categorized by the Radio Government (RG) ratings.Each denotes a unique set of physical specifications, including wire gauge, the thicknessand type of inner insulator. The following are:
RG – 8,
RG – 9,

RG – 11 : Used in thick Ethernet.
RG – 58 : 00 Used in thin Ethernet.
RG – 59 : Used for TV.

Coaxial cable connectors
There are number of connectors available for coax some of them are
BNC (bayonet n/w connector)
T-connectors which allow secondary cable to branch off from main line3.
Terminators used in Bus topologies.

OPTICAL FIBER

Optical fiber is made of glass or plastic and transmits signals in the form of light. A core is surrounded by cladding, forming the fiber. Fiber is covered by a buffer layerthat protects it from moisture; finally the entire cable is encased in an outer jacket. Both core and cladding can be made either of glass or plastic but must be of differentdensities. The inner core must be completely regular in size and shape. The outer jacket can be made either of Teflon coating, plastic coating, fibrous plastic,metal tubing etc. each of which has its own purpose and depends on where the cableis to be installed.

Optical fibers use reflection to guide light through a channel. A glass or plastic core issurrounded by a cladding of less dense glass or plastic. The difference in density of the two materials must be such that a beam of lightthrough the core is reflected off the cladding instead of being refracted into it. There are two types of Propagation Modes:

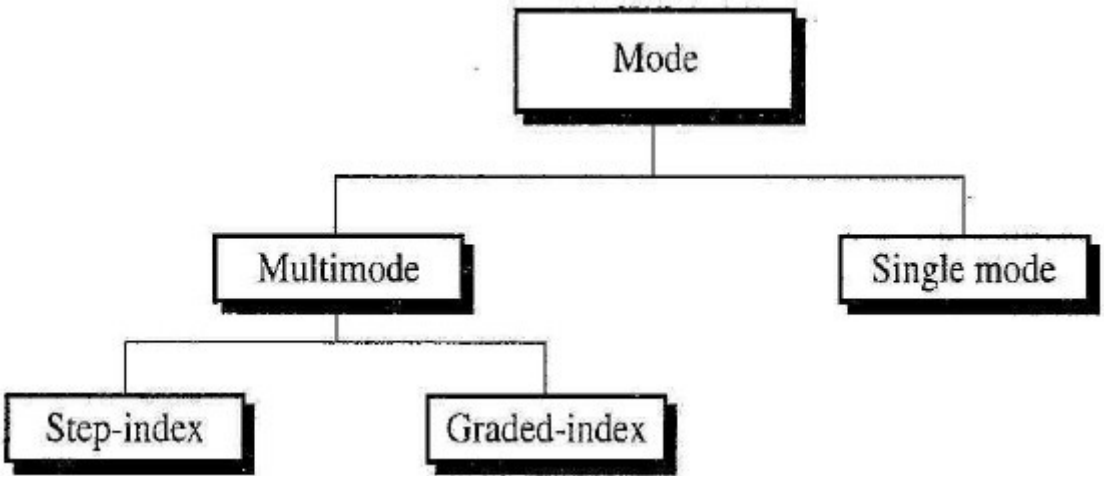


Fig 1.3 Mode of Optical Fiber

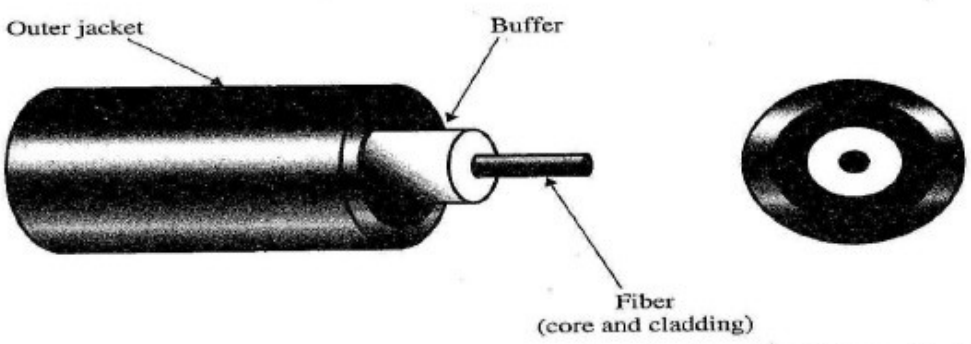


Fig 1.4 Optical Fiber Cable

The purpose of fiber optic cable is to contain & direct a beam of light from source totarget. For transmission, the sending device must be equipped with a light source &the receiving device with a photosensitive cell. The light source can be either LED or ILD (Injection Laser Diode)

Advantages of Optical fiber
Noise Resistance
Less signal attenuation
Higher Bandwidth

Disadvantages of Optical fiber
Cost
Installation/maintenance
Fragility or delicate

1.4. TOPOLOGY :

The term topology refers to the way physically or logically arrangement of network.There are five basic topologies:
1) Mesh
2) Star
3) Tree
4) Bus
5) Ring

Mesh
Every device has a dedicated point-to-point link to every other device. It needs n-1 I/O ports and a fully connected mesh has n(n-1)/2 links for n devices.

Advantages
Dedicated links eliminates traffic problems
Robust
Privacy and Secure for communications.
P2P makes fault identification and fault isolation easy.

Disadvantages
High amount of cabling and number of I/O ports
Expensive and need large space

Star
Each device has a dedicated point-to-point link to a central controller, usually called hub.

CHARACTERISTICS
The failure of medium does not seriously affect the network.
The malfunctioning of a station does not seriously affect the performance of network.
The network can use a variety of guided and unguided transmission media.
The failure of HUB seriously affects the network.

Advantages
Less expensive than a mesh topology
Needs only one cable and one I/O port to connect to hub
Easy to install and reconfigure

Easy addition and deletion of nodes
Robust, Easy default identification & fault isolation

Disadvantages
Central node dependency.

Tree
Tree is variation of a star, in which majority devices connected to a secondary hubthat is connected to central hub.

Ring
Ring topology, each device has a dedicated P2P line configuration. Each device in thering incorporates repeaters.

CHARACTERISTICS
The failure of medium seriously affects the network.
Because the interface are active devices, their malfunctioning seriously affectthe performance of network.
Because the interface is active devices, there is no limitation on the length of network.
Because each interface creates a delay, the total propagation delay isdependent on the no. of station on the network.
The network can use one of a variety of transmission media including fiberoptics cable.

Advantages:
A ring is relatively easy to install and reconfigure.
Fault isolation is simplified

Disadvantage:
Unidirectional traffic can be disadvantage. The weakness can be solved byusing dual ring or a switch capable of closing off the break

Bus
A bus topology is multipoint; one long cable is act as a backbone to link. Nodes areconnected to the bus cable by drop lines and taps. As signal travels along backbone, some of its energy is transformed into heat;therefore it becomes weaker & weaker the farther to travel. For this reason there is alimit on the number of taps.

CHARACTERISTICS
The failure of medium seriously affects the network.
Because the interfaces are passive their malfunctioning does not seriouslyaffect the performance of network.
Because the interfaces are passive there is limit on the length of network unless repeaters are used.
The propagation delay is independent of number of stations on the network.

Advantages
Ease of Installation
Use less cable than mesh, star or tree topology

Disadvantages
Difficult reconfiguration and fault tolerance
Fault break in the bus cable stops all transmission

2. Experiment – 2

2.1. Object : Case study of Ethernet (10 base 5, 10 base 2, 10 base T)

2.2. Ethernet Overview :

If you have an existing network, there's a 90% chance it's Ethernet. If you're installing a newnetwork, there's a 98% chance it's Ethernet. The Ethernet standard is the overwhelming favorite network standard today. Ethernet was developed by Xerox®, DEC™, and Intel® in the mid 1970s as a 10-Mbps(Megabits per second) networking protocol very fast for its day operating over a heavycoax cable (Standard Ethernet).Today, although many networks have migrated to Fast Ethernet (100 Mbps) or even GigabitEthernet (1000 Mbps), 10-Mbps Ethernet is still in widespread use and forms the basis of most networks.Ethernet is defined by international standards, specifically IEEE 802.3. It enables theconnection of up to 1024 nodes over coax, twisted-pair, or fiber optic cable. Most newinstallations today use economical, lightweight cables such as Category 5 unshielded twisted-pair cable and fiber optic cable.

2.3. How Ethernet Works :

Ethernet signals are transmitted from a station serially, one bit at a time, to every other stationon the network.Ethernet uses a broadcast access method called Carrier Sense Multiple Access/Collision Detection (CSMA/CD) in which every computer on the network —hears‖ every transmission, but each computer —listens‖ only to transmissions intended for it. Each computer can send a message anytime it likes without having to wait for network permission. The signal it sends travels to every computer on the network. Every computerhears the message, but only the computer for which the message is intended recognizes it.This computer recognizes the message because the message contains its address. Themessage also contains the address of the sending computer so the message can beacknowledged.

If two computers send messages at the same moment, a collision occurs, interfering withthe signals. A computer can tell if a collision has occurred when it doesn't hear its own message within a given amount of time. When a collision occurs, each of the colliding computers waits a random amount of time before resending the message.The process of collision detection and retransmission is handled by the Ethernet adapter itself and doesn't involve the computer. The process of collision resolution takes only a fraction of a second under most circumstances. Collisions are normal and expected events on an Ethernetnetwork. As more computers are added to the network and the traffic level increases, morecollisions occur as part of normal operation. However, if the network gets too crowded,collisions increase to the point where they slow down the network considerably.

2.4. Standard (Thick) Ethernet (10BASE5)

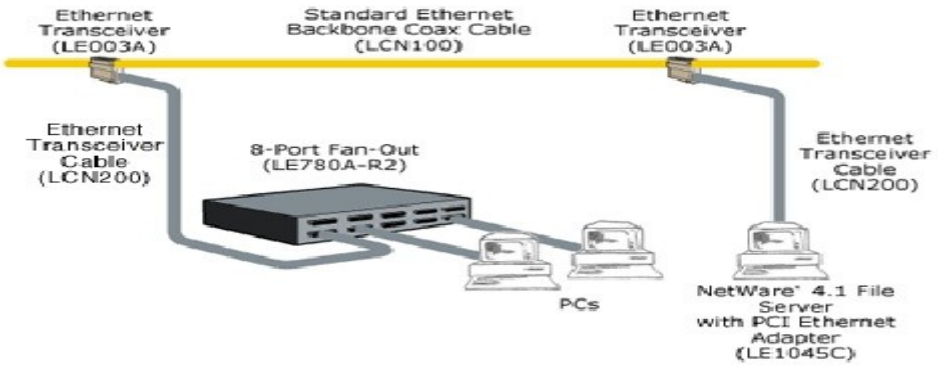


Fig 2.1 Standard Ethernet (10 Base 5)

- Uses “thick” coax cable with N - type connectors for a backbone and a transceivercable with 9-pin connectors from the transceiver to the NIC.
- Both ends of each segment should be terminated with a 50-ohm resistor.
- Maximum segment length is 500 meters.
- Maximum total length is 2500 meters.
- Maximum length of transceiver cable is 50 meters.
- Minimum distance between transceivers is 2.5 meters.
- No more than 100 transceiver connections per segment are allowed.

2.5. Thin Ethernet (ThinNet) (10BASE2)

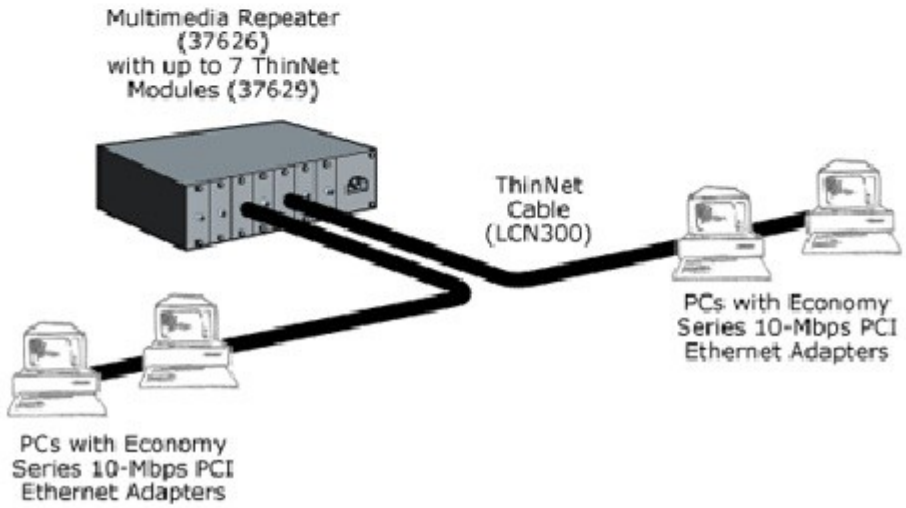


Fig 2.2 Twisted Pair Ethernet (10 Base 2)

- Uses “Thin” coax cable.
- The maximum length of one segment is 185 meters.
- The maximum number of segments is five.
- The maximum total length of all segments is 925 meters.
- The minimum distance between T-connectors is 0.5 meters.
- No more than 30 connections per segment are allowed.
- T-connectors must be plugged directly into each device.

2.6. Twisted-Pair Ethernet (10BASE-T)

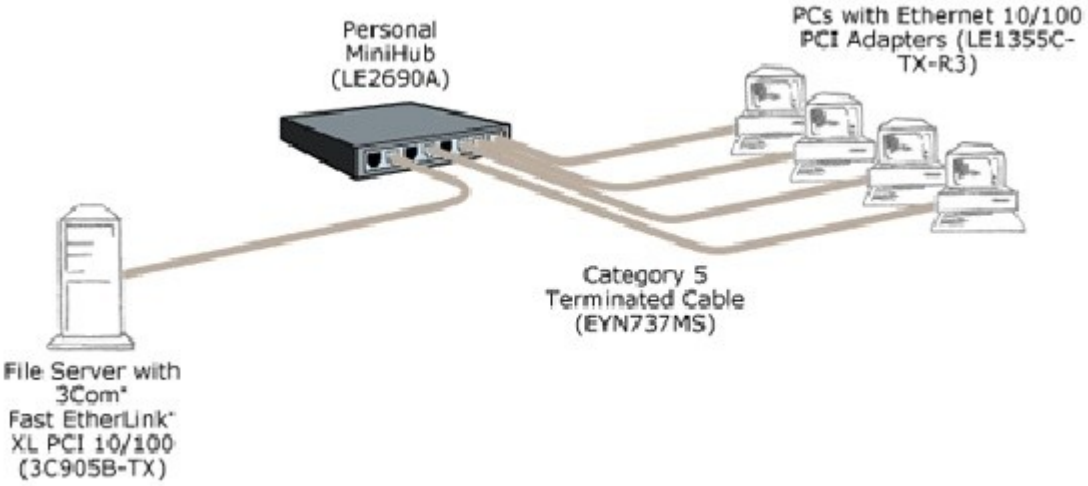


Fig 2.3 Twisted Pair Ethernet (10 Base T)

- Uses 22 to 26 AWG unshielded twisted-pair cable (for best results, use Category4 or 5 unshielded twisted pair).
- The maximum length of one segment is 100 meters.
- Devices are connected to a 10BASE-T hub in a star configuration.
- Devices with standard AUI connectors may be attached via a 10BASE-Ttransceiver.

2.7. Fiber Optic Ethernet (10BASE-FL, FOIRL)

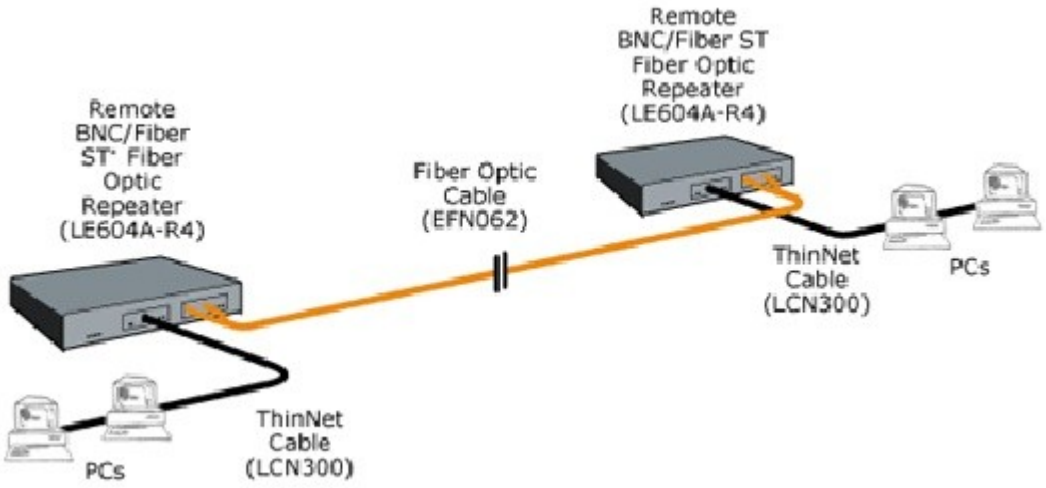


Fig 2.4 Fiber Optic Ethernet (10 Base FL, FOIRL)

- Uses 50-, 62.5-, or 100-micron duplex multimode fiber optic cable (62.5 micron isrecommended).
- The maximum length of one 10BASE-FL (the new standard for fiber opticconnections) segment is 2 kilometers.
- The maximum length of one FOIRL (the standard that preceded the new 10BASE-FL) segment is 1 kilometer.

3. Experiment – 3

3.1. Object : Installation and working of Net Meeting and Remote Desktop.

3.2. Hardware Required:

LAN Card, LAN drivers, 2-computers, Modem, Cables.

3.3. Theory:

Remote Desktop, a function included with Windows XP Professional, enables you to connect to your computer across the Internet from virtually any computer, Pocket PC, or smartphone. Unlike a typical VPN connection (which will give aremote PC access to the company network) Remote Desktop will actually allow you to see and control your connected PC as though you were sitting directly in front of it. Remote desktop technology makes it possible to view another computer's desktop on your computer. This means you can open folders, move files, and even run programs on the remote computer, right from your own desktop. Both Windows and Macintosh computer support remote desktop connections, though they use different implementations.

Fig 3.1 Remote Desktop

Windows XP and Vista both include Remote Desktop as part of the operating system. TheRemote Desktop program uses Microsoft Terminal Services and the Remote Desktop Protocol (RDP) to connect to a remote machine. Remote connections can be opened using Windows' Remote Desktop Connection (RDC), which is also referred to as Terminal Services Client (TSC). This program allows users to configure and manage remote connections toother computers. Of course, to connect to another machine, the remote system must be configured to accept incoming RDC connections.

A Windows computer can be configured to accept incoming remote desktop connections by opening the Control Panel and selecting "Performance and Maintenance." Then click the"System" icon and select the "Remote" tab in the System Properties window. Next, check the box that says, "Allow users to connect remotely to this computer." Then click OK. This should enable remote desktop connections to your machine. You can then click "Select Remote Users..." to only provide access to specific users. Of course, if you don't want your computer to be accessed by anyone, leave the "Allow users to connect..." box unchecked.

Mac OS X 10.5 and later includes a feature called Screen Sharing that allows other users to remotely access the computer's desktop. To turn on Screen Sharing, open System Preferences

and select the Sharing option. Next, check the "Screen Sharing" check box. You can then addaccess for specific users in the "Allow access for:" section of the window. If the Mac OS XScreen Sharing option feels a bit limited, you may want to try a program called "Apple Remote Desktop." This program, which is developed by Apple, provides more advanced remote access features and is often used for managing several computers on a network. Remote desktop is a program or an operating system feature that allows the user to connect toa computer in another location, see that computer's desktop and interact with it as if it were local.

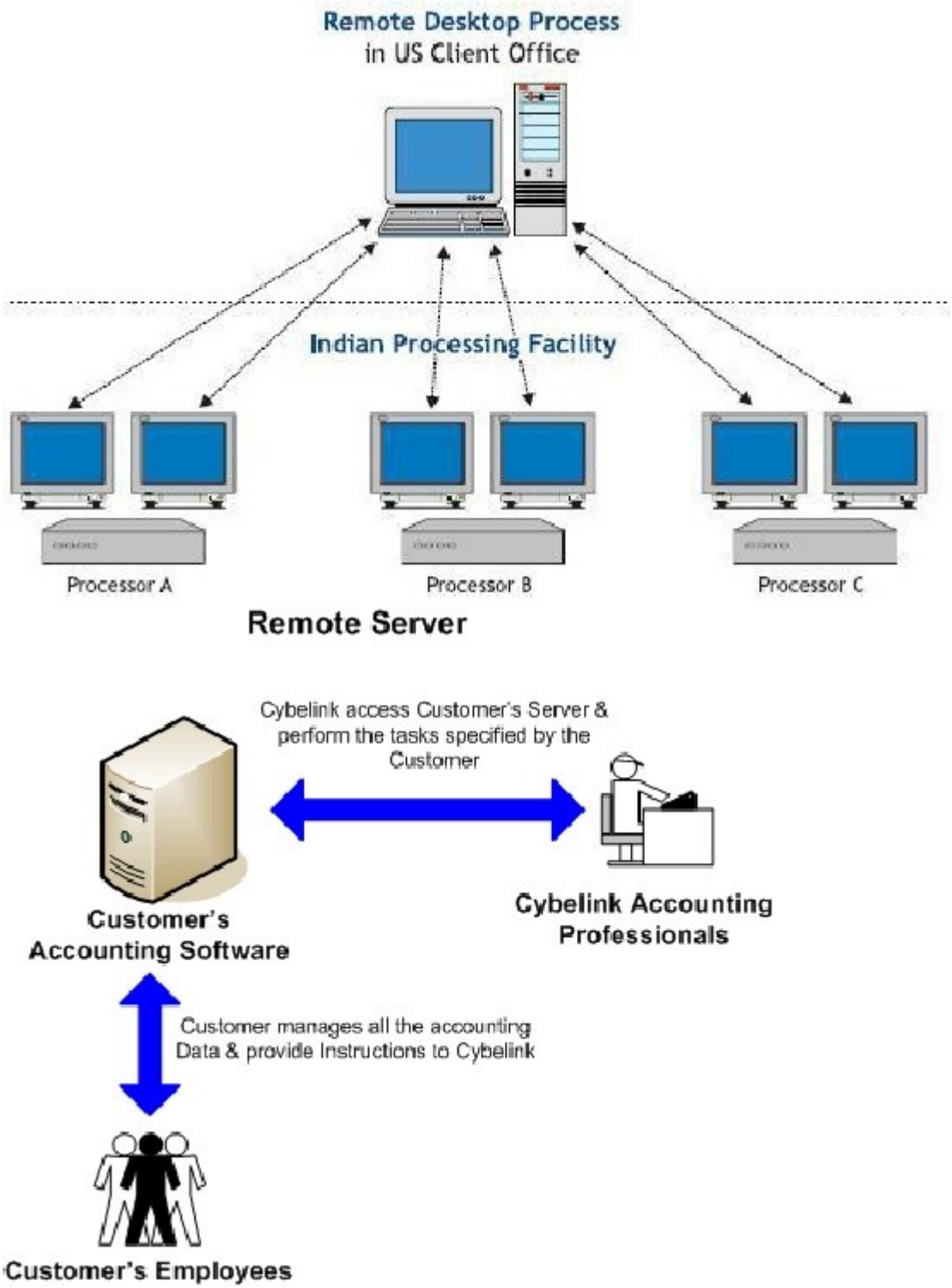


Fig 3.2 Remote Desktop Process

People use remote desktop capability to do a variety of things remotely, including the following:

- Access a workplace computer from home or when traveling.
- Access a home computer from other locations.
- Fix a computer problem.
- Perform administrative tasks.
- Demonstrate something, such as a process or a software application.

Remote desktop connectivity relies upon any of a number of protocols, including Remote Desktop Protocol (RDP), Virtual Network Computing (VNC), NX technology and Independent Computing Architecture (ICA).
Remote desktop software exists for most operating systems and platforms, including handheld computing devices. Microsoft and Apple each have a product called "RemoteDesktop." Other remote desktop products include Citrix XenApp, Cross Loop, Jaadu (for theiPhone and iPod Touch), GoToMyPC, PCAnywhere and Chicken of the VNC.

3.4. Procedure:

- Go to My Computer properties window by right clicking and selecting propertiesfrom menu that appears
- Select Remote
- For successful connection we have to perform 3 things:-
  - Check the checkbox —Allow users to connect remotely to this computer
  - Turn the Firewall off
  - Set password by:
    a) Right clicking My computer and click Manage.
    b) Select —Local user & group.
    c) Right click on —Administrator
- Set IP of 2nd computer in — Remote Desktop Connection window.
- To open -> RemoteDesktop Connection -> Start -> All programs -> Accessories -> Communication -> Remote Desktop Connection
- Give username and password of 2nd computer. The 2nd computer will automatically Log off while 1st one is working remotely on it. The remote connection is last once the user of 2nd computer logs in again.

3.5. Result :

The two computers are now accessing each-other by remote desktopconnection. The accessing of remote systems is possible by configuring remote desktop.

4. Experiment – 4

4.1. Object : Installation and working with Telnet (Terminal Network).

4.2. Hardware Requirement:

LAN Card, LAN drivers, 2-computers, Modem, Cables

4.3. Theory:

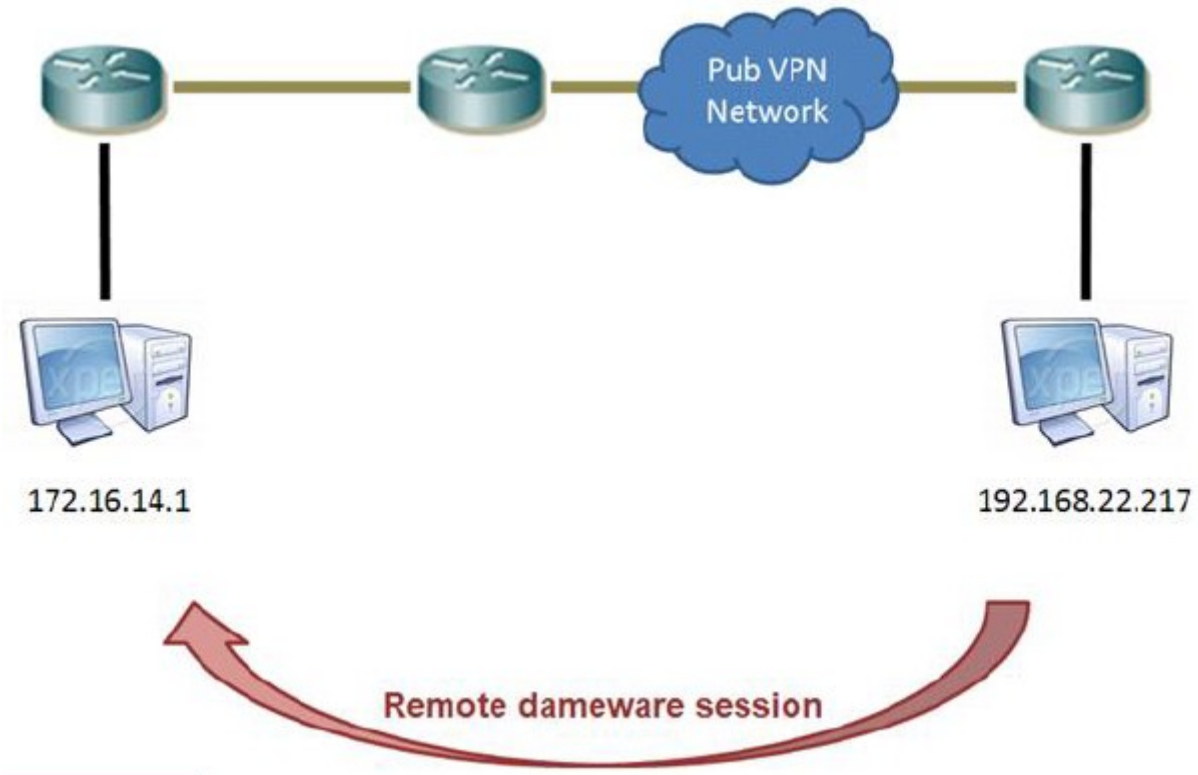


Fig 4.1 Telnet

Its an abbreviation for Terminal Network. Telnet is a protocol that allows a user to log onto other computers. You use an IP address or domain name to log on. Bulletin boards are still available to play games, download files or read information. In addition, you can play games with your friends over this type of network. Telnet is not as common as it once was. Never the less, it is a simple method of connecting to different friends or online communities. Telnet is a user command and an underlying TCP/IP protocol for accessing remote computers. Through Telnet, an administrator or another user can access someone else's computer remotely. On the Web, HTTP and FTP protocols allow you to request specific files from remote computers, but not to actually be logged on as a user of that computer. With Telnet, you log on as a regular user with what ever privileges you may have been granted to the specific application and data on that computer. A Telnet command request looks like this (the computer name is made-up) telnetthe.Libraryat.whatis.edu The result of this request would be an invitation to log on with a user-id and a prompt for a password. If accepted, you would be logged on like any user who used this computer everyday. Telnet is most likely to be used by program developers and anyone who has a need to use specific applications or data located at a particular host computer.

4.4. Procedure:

1. Go to —My Computer right click and select properties.

2. Then go to Manage. In the opened window select - Services and Application then select Telnet from right hand side of window.
3. In property window of telnet set – start – up box to – Automatic
4. Go to Start - All Programe – Accessories- Command prompt
5. In - C: prompt (C:\>) type telnet and type the IP of the 2nd computer after space. Eg: telnet 192.27.24.1
6. Enter username and password of 2nd computer when prompted.
7. To quit type —exit

4.5. Properties of Telnet:

Telnet is done via command prompt
Telnet works on password protected system
Telnet service must be – ON on both the system

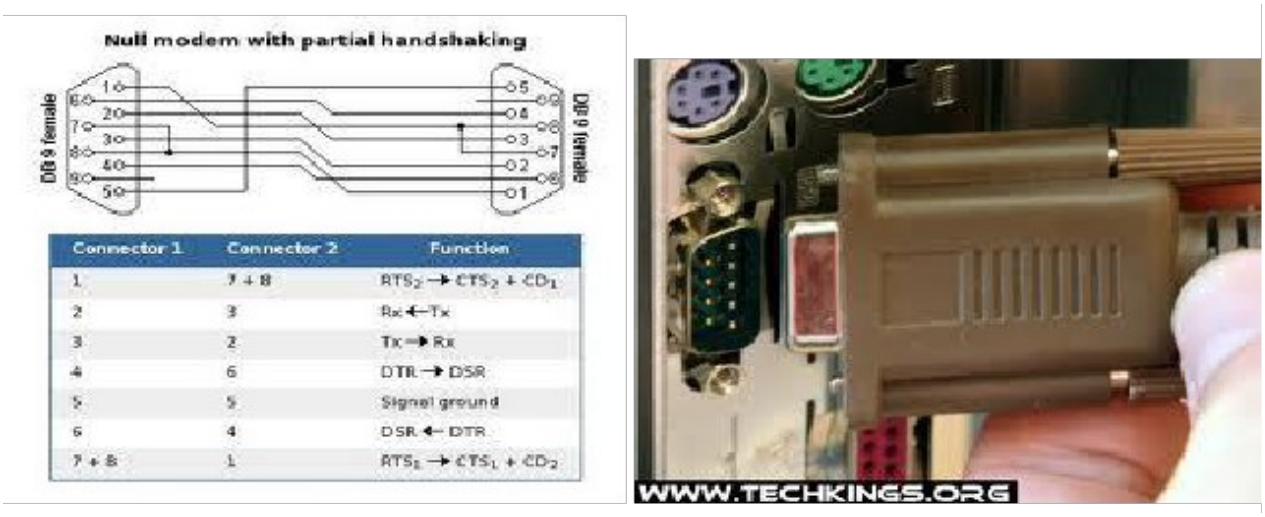
4.6. Result:

The experiment completed successfully accessing of system which is for possible telnet.

5. Experiment – 5

5.1. Object : Working with Null Modem

5.2. Null Modem Cable



Connector 1	Connector 2	Function
1	7 + 8	$RTS_2 \rightarrow CTS_2 + CD_1$
2	3	Rx ← Tx
3	2	Tx → Rx
4	6	DTR → DSR
5	5	Signal ground
6	4	DSR ← DTR
7 + 8	1	$RTS_1 \rightarrow CTS_1 + CD_2$

Fig 5.1 Null Modem

After all, isn't this why you came to this site?The purpose of a null-modem cable is to permit two RS-232 "DTE" devices tocommunicate with each other without modems or other communication devices (i.e.,"DCE"s) between them.To achieve this, the most obvious connection is that the TD signal of one devicemust be connected to the RD input of the other device (and vice versa).

Also, however, many DTE devices use other RS-232 pins for out-of-band (i.e.,"hardware") flow control. One of the most common schemes is for the DTE (the PC)to assert the RTS signal if it is ready to receive data (yes, it DOES sound backwards,but that's how it works), and for the DCE (the modem) to assert CTS when it is ableto accept data. By connecting the RTS pin of one DTE to the CTS pin of the otherDTE, we can simulate this handshake.

Also, it is common convention for many DTE devices to assert the DTR signal whenthey are powered on, and for many DCE devices to assert the DSR signal when theyare powered on, and to assert the CD signal when they are connected. Byconnecting the DTR signal of one DTE to both the CD and DSR inputs of the otherDTE (and vice versa), we are able to trick each DTE into thinking that it is connectedto a DCE that is powered up and online. As a general rule, the Ring Indicate (RI)signal is not passed through a null-modem connection.

5.3. Common Null Modem Connection

Signal Name	DB-25 PIN	DB-9 Pin		DB-9 PIN	DB-25 PIN	
FG (Frame Ground)	1	-	X	-	1	FG
TD (Transmit Data)	2	3	-	2	2	RD
RD (Recieve Data)	3	2	-	3	3	TD
RTS (Request to Send)	4	7	-	8	5	CTS
CTS (Clear to Send)	5	8	-	7	4	RTS
SG (Signal Ground)	7	5	-	5	20	SG
DSR (Data Set Ready)	6	6	-	4	20	DTR

CD (Carrier Detect)	8	1	-	4	20	DTR
DTR (Data Terminal Ready)	20	4	-	1	8	CD
DTR (Data Terminal Ready)	20	4	-	6	6	DSR

Here's a good set of figures for DB-25 male and female connectors, as viewed fromthe pin side (not the solder side).

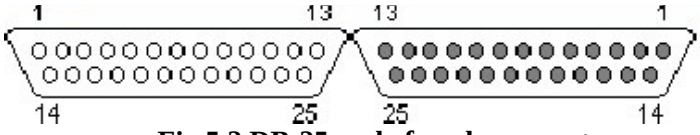


Fig 5.2 DB-25 male female connector

6. Experiment – 6

6.1. Object : Installation of Windows 2003 server

6.2. Theory and Procedure:

Windows Server 2003 operating systems take the best of Windows 2000 Server technologyand make it easier to deploy, manage, and use. The result: a highly productive infrastructurethat helps make your network a strategic asset for your organization.Windows Server 2003SP2 provides enhanced security, increased reliability, and a simplified administration to helpenterprise customers across all industries.Microsoft Windows Server 2003 R2 Standard Edition Requirements

Computer and processor - PC with a 133-MHz processor required; 550-MHz or faster processor recommended; supportfor up to four processors on one server

Memory - 128 MB of RAM required; 256 MB or more recommended; 4 GB maximum

Hard disk - 1.2 GB for network install; 2.9 GB for CD install

Drive -CD-ROM or DVD-ROM drive

Display - VGA or hardware that supports console redirection required; Super VGA supporting 800 x600 or higher-resolution monitor recommended

6.3. Plan your installation

When you run the Windows Server 2003 Setup program, you must provide information abouthow to install and configure the operating system. Thorough planning can make your installation of Windows Server 2003 more efficient by helping you to avoid potential problems during installation. When planning for your Windows Server 2003 installation

- Check System Requirements
- Check Hardware and Software Compatibility
- Determine Disk Partitioning Options
- Choose the Appropriate File System: FAT, FAT32, NTFS
- Decide on a Workgroup or Domain Installation
- Complete a Pre-Installation ChecklistAfter you made sure you can go on, start the installation process.

6.4. Beginning the installation process

You can install Windows Server 2003 in several methods – all are valid and good, it all depends upon your needs and your limitations. In this we are installing directly from a CD by booting your computer with the CD.

- Start the computer from the CD.

Fig 6.1 Installation of windows server 2003

- You can press F6 if you need to install additional SCSI adapters or other mass-storagedevices
- Setup will load all the needed files and drivers.
- Windows server 2003 welcome screen and available options press enter
- Read and accept the licensing agreement and press F8 if you accept it
- Select or create the partition on which you will install Windows Server 2003.Now you needto click C to create new partition

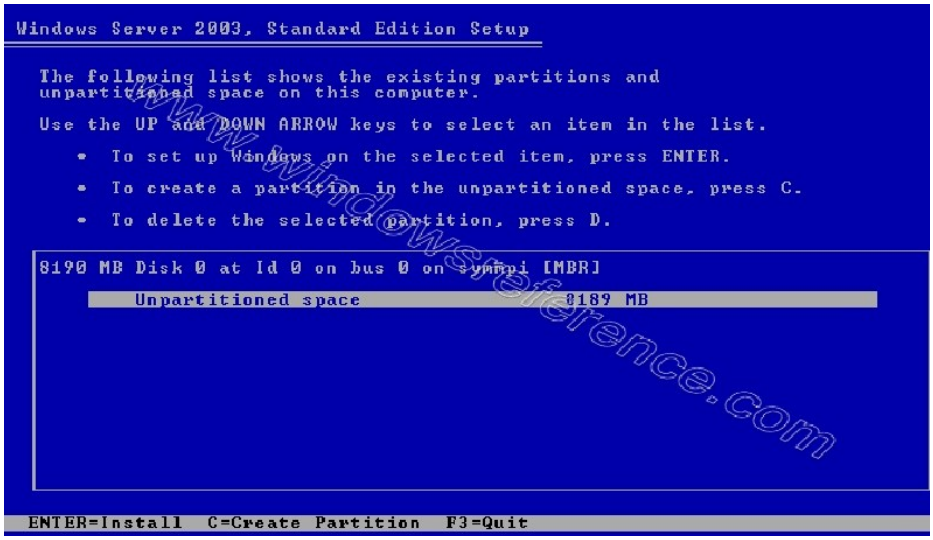


Fig 6.2 Creating partition

- Enter the partition size and press enterAfter creating the partition you need to select where you want to install windows server 2003press enter
- Now you need to format your new partition with NTFS select the option as below and pressenterDrive Format is in progress
- After format setup will start copying files is in progressSetup Initializes your windows configuration

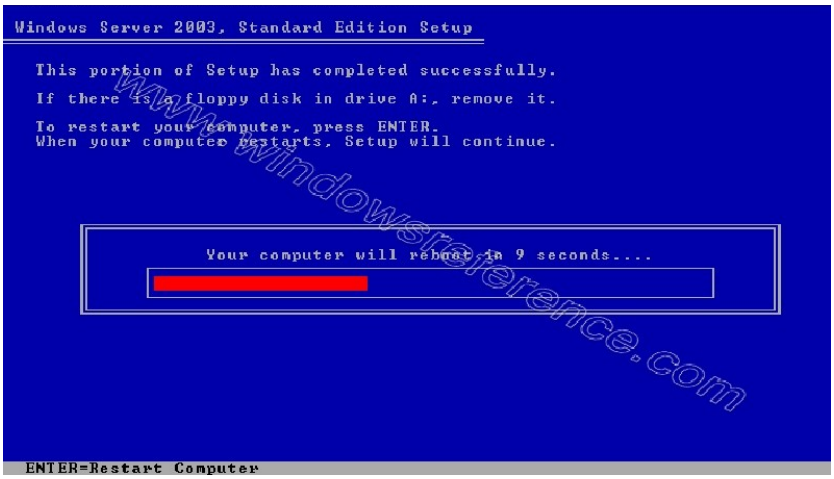


Fig 6.3 Progressing setup of installation

- The computer will restart now and the installation process will start in graphical mode.It will then begin to load device drivers based upon what it finds on your computer. You don't need to do anything at this stage.
- Click Customize to change regional settings, if necessary.Current System Locale – Affects how programs display dates, times, currency, and numbers.Choose the locale that matches your location, for example, United Kingdom.Current Keyboard Layout – Accommodates the special characters and symbols used indifferent languages. Your keyboard layout determines which characters appear when youpress keys on the keyboard.
- If you don't need to make any changes just press Next.
- Enter the name and Organization click next

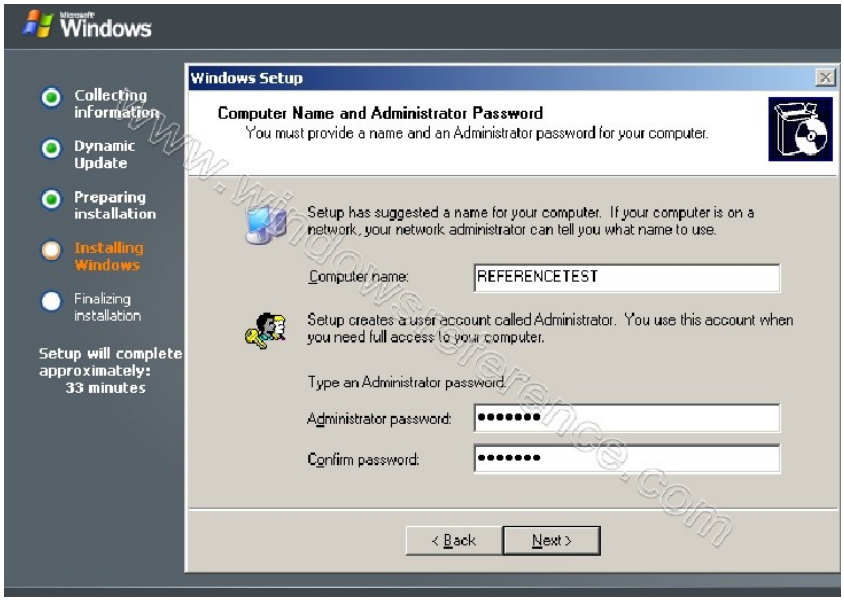


Fig 6.4 Installation of windows server

- Enter your product key click nextSelect the license mode you want to use click next
- Enter the computer name and administrator password click nextSelect the correct date and time for your computer click next
- Installing network in progressNow you need to set the network settings here select custom settings click next
- Select Internet Protocol (TCP/IP) click on properties
- Select use the following ip address radio button and enter you ip address details click ok After configuring IP address you need to click next
- In the Workgroup or Domain window enter the name of your workgroup or domain.A workgroup is a small group of computers on a network that enables users to work togetherand does not support centralized administration.A domain is a logical grouping of computers on a network that has a central security databasefor storing security information. Centralized security and administration are important forcomputers in a domain because they enable an administrator to easily manage computers thatare geographically distant from each other. A domain is administered as a unit with commonrules and procedures. Each domain has a unique name, and each computer within a domainhas a unique name.

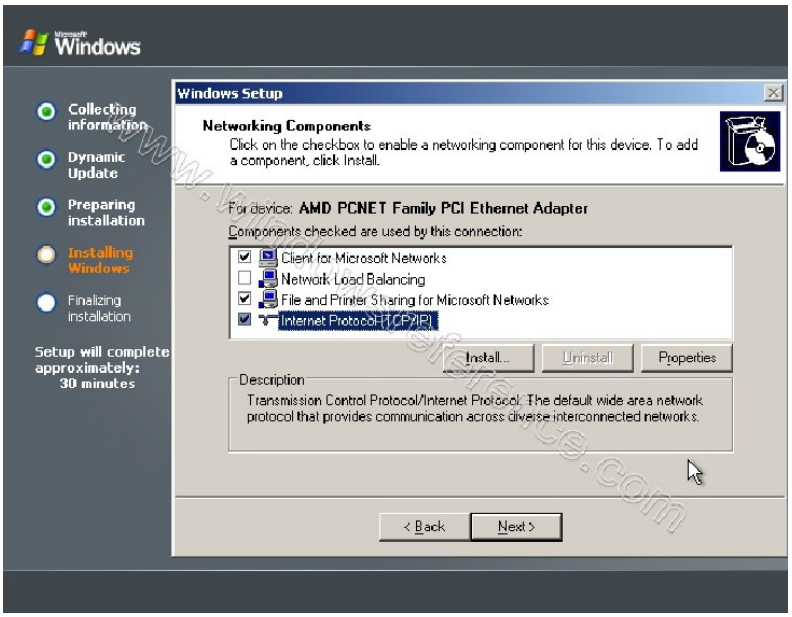


Fig 6.5 Windows server installation

- If you’re a stand - alone computer, or if you don’t know what to enter, or if you don’t have the sufficient rights to join a domain – leave the default entry selected and press Next.

- Next the setup process will finish copying files and configuring the setup. You do not need todo anything.
- After finishing installation process your system will reboot and you can see logon screen
- After logging in you should see similar to the following screen for Windows server 2003 R2editions now you need to insert CD2 to install extra components click ok

That’s it you have completed windows server 2003 R2 installation**.**

7. Experiment – 7

7.1. Objective : Installation of Dynamic Host Configuration Protocol (DHCP)

7.2. Theory:

Dynamic Host Configuration Protocol, a protocol for assigning dynamic IP addresses todevices on a network. With dynamic addressing, a device can have a different IP addressevery time it connects to the network. In some systems, the device's IP address can evenchange while it is still connected. DHCP also supports a mix of static and dynamic IPaddresses.Dynamic addressing simplifies network administration because the software

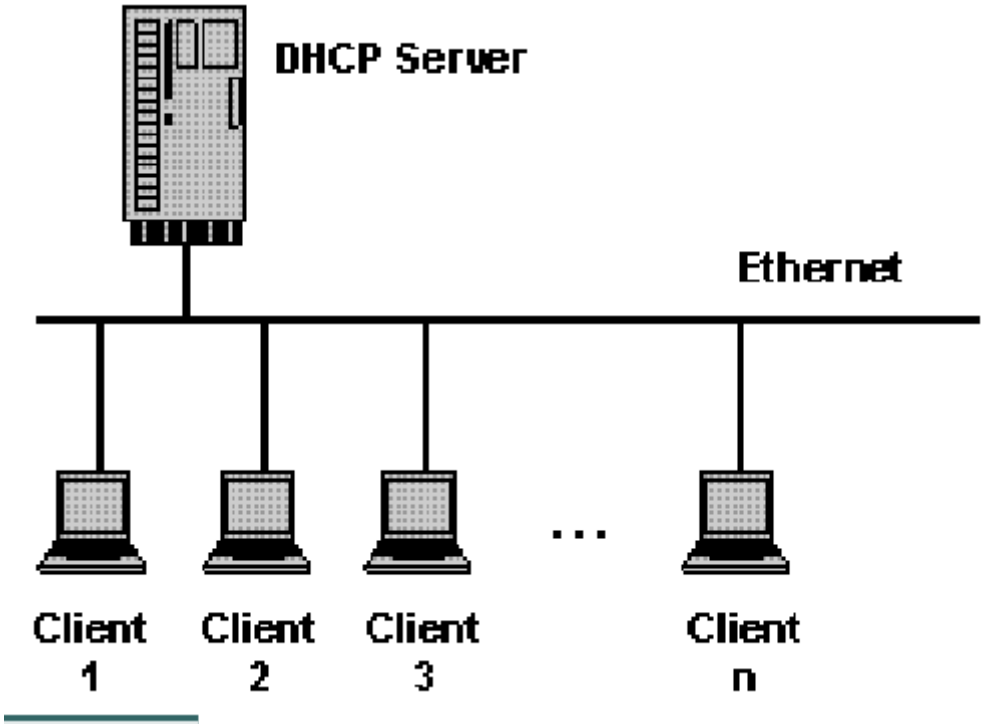


Fig 7.1 DHCP Server

keeps track of IP addresses rather than requiring an administrator to manage the task. This means that a new computer can be added to a network without the hassle of manually assigning it a unique IPaddress. Many ISPs use dynamic IP addressing for dial-up users.A DHCP Server assigns IP addresses to client computers. This is very often used in enterprise networks to reduce configuration efforts. All IP addresses of all computers are stored in adatabase that resides on a server machine.

7.3. Procedure:

- Installing DHCP Server is very easy in win server 2003 or win XPFirst you need to go to Start – All Programs – Administrative Tools – >Manage Your ServerHere you need to select Add or remove a role
- Verify the following steps click on NextSelect Server Role as DHCP Server option click on NextSummary selection click on Next
- Installing DHCP Server in progressNow this will prompt new scope welcome scree click next
- A scope is a collection of IP addresses for computers on a subnet that use DHCP.enter the name and description of your scope click nextNow you need to define the range of addresses that the scope will distribute across thenetwork,the subnet mask for the IP address . Enter the appropriate details and click next.
- Enter the IP address range that you want to exclude and click on nextSelect lease duration how long a client can use an IP address assigned to it from this scope. Itis recommended to

add longer leases for a fixed network (in the office for example) andshorter leases for remote connections or laptop computers and click next

- You are given a choice of whether or not you wish to configure the DHCP options for thescope now or later.You can select Yes,I want to… radion button and click next
- Enter the router, or gateway, IP address click next. The client computers will then knowwhich router to use and click next
- Enter the DNS and domain name settings can be entered. The DNS server IP address will bedistributed by the DHCP server and given to the client click nextIf you have WINS setup then here is where to enter the IP Address of the WINS server. Youcan just input the server name into the appropriate box and press Resolve to allow it to find the IP address itself click next
- Now you need to activate this scope now and click nextDHCP Server new scope installation was finished and click finish
- Now your server is now a DHCP server message and click finish

7.4. Configuring DHCP

- Now you need to go to Start - Administrative Tools – DHCP
- Right Click on your server click on Authorize your DHCP Server
- Authorization completed now your DHCP server is up and runningDHCP servers permit you to reserve an IP address for a client. This means that the specificnetwork client will have the same IP for as long as you wanted it to. To do this you will haveto know the physical address (MAC) of each network card. Enter the reservation name,desired IP address, MAC address and description - choose whether you want to supportDHCP or BOOTP and press add. The new reservation will be added to the list.

That’s it it is very easy to configure DHCP server in win server 2003 now you can configure your windows client pc to check your dhcp server is working or not