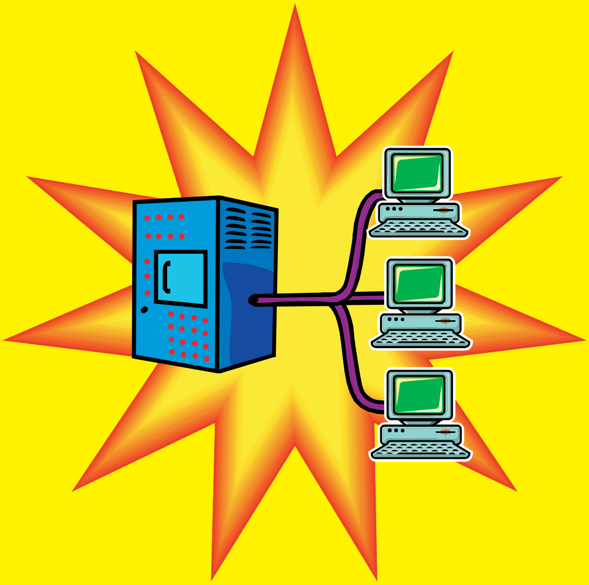
Everything you wanted to know about.....

Networking & Windows NT



Learn

all new features and skills needed to master Windows NT

Apply

easy steps for fast results!

Build

foundation of Windows NT knowledge step-by-step

Master

Advance features that Windows NT offers

Silicon Media PRESS

Networking & Windows NT

Munishwar Gulati
Mini Gulati

SILICON MEDIA PRESS
New Delhi

ISBN-81-87870-10-9

Every effort has been made to supply complete and accurate information. Silicon Media Press does not guarantee the accuracy or completeness of any information and assumes no responsibility for its use.

First Edition 2001

Published by Silicon Media Press, Regd. Off. I-19, Lajpat Nagar - II, New Delhi. B.O. : KJ-75, Kavi Nagar, Ghaziabad. mng@siliconmedia.org Ph - 0120-(91)-4702867 **Typeset by** : Ram Ganga Computers (P) Ltd. and **Printed by** : Digisoft, D-30, Secotr 6, Noida. Ph - 0118-91-4444598, 9810236378.

Dedicated to my parents,

who has always supported my decisions

Contents

CHAPTER 10 MANAGING FILES & FOLDERS 201

CHAPTER 11 WINDOWS NT NETWORKING 219

Acknowledgments

We would like to thank all of the many people who helped bring this book to print. It's really fascinating for us to write a book, because what begins as a few thoughts ends up as a physical, tangible thing that goes into the hands of many readers. The trip from thought to thing is a long one and involves inputs from lots of people. Thanks goes to all of our editors, art personnel and staff at Silicon Media.

Munishwar Gulati

I would especially want to thank my wife and co-author Mini Gulati, who always cooperated and went through the whole book to rectify me at many places.

Mini Gulati

It has been delight working with my husband and co-author Munishwar Gulati. He persuaded me to write, what I knew and rectified it, to give it a shape of chapter. My deep appreciation goes to him for his constant enthusiasm and hard working.

About this book

As you read the book, you will find the answers to many of the questions you have about Windows NT and Networking.

How the book is organised

Chapter 1 introduces you to concepts of Networking, methods of Data Transmission, and various connectivity devices. It also discussed about OSI seven layer Model.

Chapter 2 covers the architectural view of Windows NT, and various features which makes NT perfect for Networking.

As you move on to Chapter 3, you will know about Windows NT installation.

Chapter 4 takes you through the first Windows NT session and covers the desktop, where you will interact with the operating system. It covers all the salient point about usage of the desktop for navigation and customization.

Chapter 5 continues with the Command prompt operation familiar to MS-DOS user, running other windows based programs and working with windows. It also tells about using help in Windows.

Chapter 6 starts with file system used in NT and move on to Disk Management using Disk Administrator.

Chapter 7 tells you about the control panel, which contains all the programs for setting up your windows. Adding new programs, fonts, setting display properties, networking, modem installation, telephony etc. are the things that are covered in this chapter.

Chapter 8 covers user administration in NT. It covers all aspect of creating and modifying users, creating groups, giving rights & permission , trust relationships and logging process.

Chapter 9 talks about printing administration with local and network printers.

Chapter 10 discusses about sharing files and folders.

Chapter 11 tells about networking using Windows NT. It discusses about the various protocols and installation of TCP/IP.

Chapter 12 discuss about the Dynamically Host Configuration Protocol, Windows Internet Name Server and Domain Name Server.

Chapter 13 covers all about Remote Access Server.

Chapter 14 discusses about the Server Administration using Server Manager, Reapir Disk Utility and Backup.

Chapter 15 deals with Internet and using NT server as Internet Information Server.

This book is a sincere effort for explaining the concepts of Windows NT and Networking Technology. I sincerely hope that you find this work to be informative and enjoyable. Thank you for purchasing the book and great luck using Windows NT and Networking.

Munishwar Gulati
Mini Gulati
mng@siliconmedia.org

Tell us what you think!

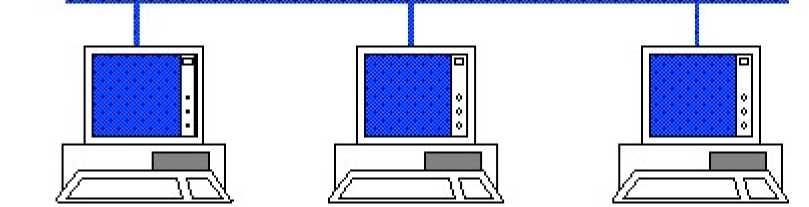
As a reader, you are the most important critic and commentator of our books. We value your opinion and want to know what we are doing right, what we could do better, what areas you would like to see us publish in, and any other words of wisdom you are willing to pass.

As the publishing manager of the group that created this book, I welcome your comments. You can e-mail at siliconmedia@hotmail.com, to let me know what you did or didn't like about this book.

CHAPTER 1

Networking Concepts

NETWORKING
NETWORK ARCHITECTURE
COMPUTER NETWORKS
NETWORK REQUIREMENT
METHODS OF DATA TRANSMISSION
THE OSI SEVEN LAYER MODEL
NETWORK CONNECTIVITY DEVICES



NETWORKING

Networking is the sharing of information and services. Networking is possible when individual or groups have information or abilities that they wish to share with others. Computer networking provides the communication tools to allow computers to share information and abilities.

They are three types computing networking

- Centralized computing
- Distributed computing
- Collaborative computing

CENTRALIZED COMPUTING

Large centralized computers called *Mainframes*, were used to store and organize data. Local nodes connected to central computer through serial ports. Computing done by Mainframe and process output communicated to terminal via serial port. These terminals consisting of monitor, keyboard, they are known as Dumb terminal.

DISTRIBUTED (CLIENT/SERVER) COMPUTING

Instead of centralizing all computing processing into a single mainframe, distributed computing uses multiple personal computers to achieve the goals. The chief advantage of this is each personal computer having its own processing power also takes advantage of sharing files, printers and communications. This type of network also known as SERVER/CLIENT network. Novell NetWare is one such a network.

Here are some benefits of server-based networks:

- They provide centralized user accounts, security, and access controls, which simplifies network administration.
- More powerful equipment means more efficient access to network resources as well.
- Users only have to remember a single password for network login, which allows them to access all resources that they have permission to access.

Now, let’s take a look at some server-based networking disadvantages:

- A server failure can render a network unusable; at best, it results in loss of network resources.
- Such networks require an expert staff to manage the complex, special-purpose server software, which adds to the overall cost.
- Costs also increase due to the requirements of dedicated hardware and specialized software.

COLLABORATIVE COMPUTING

Collaborative computing is a synergistic type of distributed computing where Network computers actually share processing abilities. All PC in the network acts as server and client and shares the resources of individual computer. This kind of network is known as PEER TO PEER network. Windows 95/98 is one such example.

Here are some benefits of peer-to-peer networks:

- They are easy to install and configure.
- Individual machines do not depend on a dedicated server.
- Users are able to control their own-shared resources.
- This type of network is inexpensive to purchase and operate.
- You don't need any equipment or software other than an operating system.
- It is not necessary to have an employee act as a dedicated administrator to run the network.
- This type of network is well suited for networks with 10 or fewer users.

Peer-to-peer networks have following drawbacks as well:

- You can only apply network security to one resource at a time.
- Users might have to remember, as many passwords as there are shared resources.
- You must perform individual backups on each machine to protect all shared data.
- When someone accesses shared resources, the machine where the resource resides suffers a performance hit.
- There is no centralized organizational scheme to locate or control access to data.

Distributed v/s Collaborative Network

Selecting a network depends on the circumstances. You should select a peer-to-peer network only when all of the following conditions apply:

- There are no more than 10 network users (preferably, no more than 5).
- All machines on the network are in close proximity to fit within a single LAN.
- Budget considerations require an inexpensive solution.
- You don't need any specialized servers, (for example, fax servers, communication servers, or application servers).

On the other hand, a server-based network makes sense when one or more of the following conditions are true:

- More than 10 users must share the network.

- You require centralized control, security, resource management, or backup.
- You require access to specialized servers, or there is a heavy demand for network resources.
- You are using an Internetwork or you require WAN access.

NETWORKARCHITECTURE

In communications, data is transferred either in parallel or serial. Parallel communications is faster but requires more wires. Serial communications is much slower but requires fewer wires. Serial is more practical for communications with remote sites, and the existing telephone system can be used for the communications link to various locations by the use of modems. Most, if not all, computer networks use serial communications for linking computers.

The network architecture defines the message and data formats as well as the protocols and other standards to which the hardware and software must conform to in order to meet certain objectives. These objectives are listed below:

Connectivity

This objective specifies that the hardware and software, which are built in conformance to the standards, must be able to communicate with each other over the network.

Flexibility

Due to the constant enhancement in technology or due to the change in the user needs, the network may have to be modified. Flexibility specifies that this upgradation must be possible without the need for costly new interfaces or software modification.

Modularity

Modularity specifies that the hardware and software modules must be capable of production in large quantities so that they can be used in variety of devices.

Reliability

Reliability deals with the issues, which concern error free communication over the network. Error free communication has to be realized by providing appropriate error detection and correction capabilities.

Simplicity

This aspect of architecture specifies that the network should permit its easy implementation, installation and re-configuration. Even the services that are provided by a network must be simple to implement and maintain.

Diversity

The network must provide a variety of services and at the same time, isolating the user from the network structure or implementation details.

In our discussion, we will refer to each computer on the network as a node or station, and the facilities for linking the computers as a link. There are several different ways to organize structure these nodes and links to form a network. The structure is referred to as a topology which has been discussed in detail, later in the chapter.

COMPUTER NETWORKS

A computer network is an interconnection of various computer systems located at the same/different places. The interconnection is done through a communication link also known as the physical layer of the network and this link is such that it is totally transparent to the users of the network. The transparency of the communication link is brought about by interfacing software known as protocols which enables a user in one location to freely access a computer system/database/process/software in another location.

However if the computers in the network operate together as a single unit, which to the user appears as a single computer, albeit physically dispersed, then the complete system is more accurately described as a distributed system. Therefore although any interconnected set of computers is often conveniently referred to as a computer network. The use of the term often implies an interconnected set of independent computers and not a distributed system. However, it may be useful when considering a distributed system to be able to recognise the particular type of network on which it is based.

The hierarchy of a typical network has terminals at the lowest level. Terminals are connected to the terminal controllers which in turn are linked to the host computer. Terminals are connected either serially or in parallel. In a series connection, which is also called a multidrop line, the terminals are wired to the same line which connects to the terminal controller. Each terminal is connected directly by a separate line to the terminal controller in a parallel connection. Terminal controllers are also connected to each other and the nodes in a similar fashion.

COMPUTER NETWORKS CLASSIFICATION

Network could be classified into following three categories:

- Local Area Network. (LAN)
- Metropolitan Area Network (MAN)
- Wide Area Network (WAN)

LOCAL AREA NETWORK

Network used to interconnect computers in a single room, rooms within a building or buildings one site are normally called Local Area Networks (LANs). LANs normally transmit data in a digital form with typical transmission speeds of up to several megabytes per second. These speeds can be achieved using parallel transmission where a cable with multiple core is used, or serial transmission, making use of high frequency carriers, using coaxial cables, fibre optical or even a simple pair of wires because distances are short. Modems are not normally required although some mechanism for converting from parallel to serial transmission and back again may be needed. In Fig.1.1, there is an example of local Area Network as may be used on a single site within an organization. The terminals and workstations in Fig 1.1 are able to connect to either of two host computers.

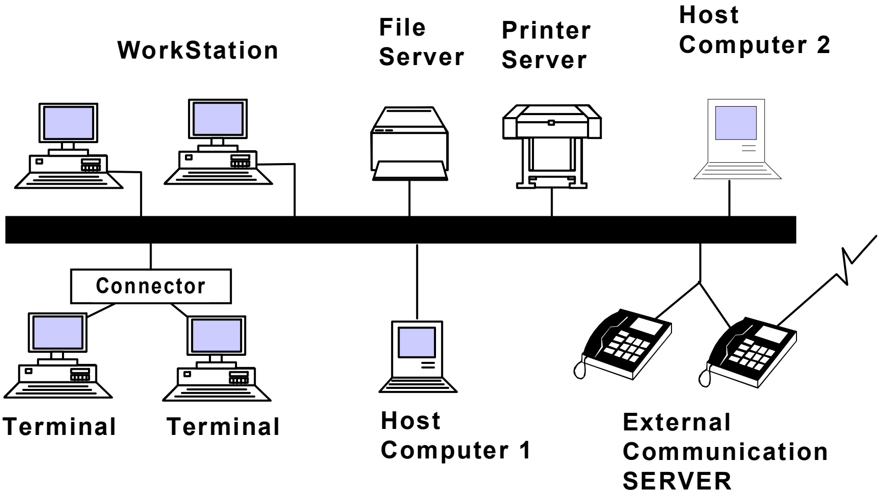


Fig 1.1 Local Area Network

The network also has a file server and a print server. The former is a special computer which provides a form of auxiliary storage which can be used by any other computer and print it. There is also an external communication server on the LAN which enables communication between equipment on the network and system elsewhere.

Local Area Network links computers in the same general area for the purpose of sharing information and hardware. Usually the computers are within 300 meters of each other, because they must be connected by a cable hookup, which can be expensive. People at the work stations in a LAN gain more capabilities in word processing data processing information retrieval, and communication without duplication of equipment database, and activities. LANs are just starting to become popular. Many businesses are installing LANs in order to improve the efficiency of office functions and to facilitate office automation. The configuration of the LAN can be a star, a ring or simply devices attached along a length of cable.

The typical local area network connects computers located within half a mile of each other. The attached computers may be of different types and be performing a variety of functions such as data processing, word processing and electronic mail. The two main purposes of the local area network are to link workstations within a facility so that they may share peripherals (such as magnetic disks holding the database) and to allow workstations to communicate with each other.

It is not unusual to connect a local area network to an intercity network or a value added network. This allows all devices attached to the LAN to have access to outside sources of data.

Characteristic Attributes of using Local Area Networks

The main attributes of present day local area networks are:

- inexpensive transmission media.
- inexpensive devices to interface to the network.
- easy physical connection of devices to the network.
- high data transmission rates.
- network data transmission rate is independent of the rates used by the attached devices, making it easier for devices of one speed to send information to devices of another speed.
- a high degree of interconnection between devices.
- every attached device has the potential to communicate with every other device on the network.
- a central controlling processor seldom present.
- in the majority of cases, each attached device hears (but does not process) message intended for other devices as well as for itself.

It is important to note that neither the actual data transmission rate used, nor the access method, nor the topology of the network are essential characteristics.

Uses of Local Area Networks

All local area networks primarily suited to devices generating digital data streams at a moderate rate such as :

- computers (minis, micros, and mainframes)
- computer terminals, both dumb and intelligent
- personal computer systems based on microprocessors
- office workstations
- mass storage devices
- printers and plotters
- file servers

- photo-and teletypesetters
- process monitoring and control equipment
- bridges and gateways to other networks.

The most relevant applications are

- file transfer and access
- word and text processing
- electronic message handling
- personal filing and information handling
- graphical information
- remote database access
- personal computing
- digital voice transmission and storage.

WIDE AREA NETWORK

The term wide area network (WAN) is used to describe a computer network spanning a regional, national, or global area.

Facilitating Communications

Corporations often use wide area networks to facilitate employee communications, to save on long- distance phone calls, to cut costs on the preparation of written documents and to overcome the time lag involved in overseas communication. Computer conferences, in which users communicate with each other through their computer systems, is another possible function of wide area networks.

Whereas most local area networks are limited in their applications, most wide area networks are complex, multifaceted systems that serve many users and many functions. However, many of the incentives and disincentives for installing local area networks are applicable to the installation of wide area networks. Several functions that might be considered especially important as incentives for installing a wide area network are discussed in the paragraphs that follow.

Remote Data Entry

It is often inconvenient to place a computer at the point at which business data is generated e.g. at the grocery store checkout counter. Wide area network permit companies to collect transaction data on site through point of sale terminals or automated teller machines and also to centralize this data in a computer for processing or reporting purpose.

Remote Job Entry

Remote job entry (RJE) refers to the submission of both data and computer programs to a remote computer for processing. For example, RJE at colleges and universities enables faculty and students to write and execute their own programs on a central computer. In some RJE application, both data and computer programs are stored locally and transmitted to the remote computer at the time of execution. In other application, programs and/or data are stored at the computer site and must be requested by the user before data processing can commence.

Centralizing Information

It is often convenient for a business to centralize regional or national file information. For example, auto-parts dealers can better help customers locate rare auto parts using a centralized computer file of inventoried items. Wide area networks enable such users to query centralized databases.

Time Sharing

Time sharing enables many individuals to use the same computer for executing computer programs or acquiring specific data. In some instances, time sharing enables users to write computer programs in a specialized computer language, while in other cases, it enables businesses to perform additional data processing not available locally.

Using Specialized Databases

Sometime-sharing companies specialize in the collection and maintenance of unique databases. CompuServe, for example, collects stock-market data and other financial information of interest to financial investors.

Over recent years, there has been steady trend towards using computer systems which have several interconnected processors placed in separate locations. Each processor tends to have its own local peripherals (disks, printers, Terminals) in addition to any peripherals attached to some central processor.

WIDE AREA AND LOCAL AREA NETWORKS

In local Area Network the distance between the communicating computers/peripherals may range from a few feet to a few kilometers-normally within the premises of the user. The terminals/peripherals may be physically connected using wires or coaxial cables. The cost of transfer is low as the distances are short, the errors in transmission are also few, In Wide Area Network, distances between the points connected being larger, use is made of telephone lines, microwave and satellite links. Speed of data transfer in WAN may be between 300 to 9600 bits per second (bps) as against 0,1 to 100 Mbps achieved in a LAN.

In contrast to local area networks which only have a few components, wide area networks involve a large number of devices between the source and destination of data (normally computer and terminal). This can be achieved in the local situation but for transmission over any distance it is necessary to insert modems. As more lines are needed and because of the special requirements of transmission (the protocols error checking and correction), communication controllers (often known as front end processors) have to be introduced. At the other end, concentrators are inserted which allow terminals to share the same transmission facility. It also means that any intelligence required could be put in the concentrator, thus reducing the cost of terminals.

Front end processors and concentrators may also be used as nodes on the network or additional devices may be introduced as nodes to facilitate networking.

Once the signal passes into the network, it goes through other devices such as the exchange equipment. Other modems are also used to boost the signal to higher frequencies and combine it with others for transmission across the network. Transmission can be by coaxial cable or microwave.

LANs cannot be used over long distances, instead Long Haul Networks (LHNs) are used. Long Haul Networks connect computers on separate sites, separate cities or even separate countries. They are also called Wide Area Networks (WANs). LHNs tend to use packet switching methods or message switching methods and exploit optical fibre media and satellite transmissions in many cases.

Local and wide area networks can be connected together by devices called gateways. These are intelligent devices which are capable of converting the protocols used in one network to those used in the other.

A typical LHN is used for electronic mail. The gateway connection normally takes the form of some kind of IMP (Interface Message Processor) which has the ability to receive, store and forward messages. The communication links between IMPs can take a variety of forms such as cable, optical fibre or satellite transmission.

This configurations are used both separately and in combination to build up more extensive networks. The first is wide area networks. WAN makes use of public phone links and, covers a large geographical distance or area, national and international. The local area networks LAN on the other hand connect many local devices. This requirement has increased greatly with the advent of microcomputers. Hence so resources such as processing power, disk space, printers etc. and data present at a location, are not only accessible locally (using a LAN) but also accessible through a computer located perhaps hundreds or thousands of kilometers away.

DIFFERENCE BETWEEN LAN & WAN

- A LAN is restricted to a limited geographical coverage of a few kilometers, but a WAN spans greater distance and may operate nationwide or even worldwide.
- The cost to transmit data in a LAN is negligible since the transmission medium is usually owned by user organization. However in case of a WAN, this cost may be very high because the transmission medium used are leased lines or

public systems such as telephones lines, microwave and satellite links.

- In a LAN, the computer, terminals and peripheral devices are usually physically connected with wires and coaxial cables. Whereas, in a WAN there may not be a direct physical connection between various computers.
- Data transmission speed is much higher in LAN than in a WAN. Typical transmission speeds in LAN are 0.1 to 100 mega bits per second. On the other hand, in a WAN the data transmission speed is normally of the order of 1800 to 9600 bits per second.
- Fewer data transmission errors occur in case of a LAN as compared to a WAN. This is mainly because, in case of a LAN, the distance covered by the data is negligible as compared to a WAN.

NETWORK REQUIREMENT

The following are the basic requirement of a typical network:

- Servers and clients to share information
- Physical medium to connect each other
- Rules for communication (Protocols)

Normally, servers provide services of:

- File services, so you can organize your work
- Print services, to handle the process of printing your documents
- Message services, to share your work with other people by putting it on paper or using a variety of e-mail systems.
- Application services, so as to run various applications smoothly.
- Database services, to maintain the data in database.

The above services can be provided by network operating system. The system classified as SERVER CENTRIC NETWORK OPERATING SYSTEM (like Novell Netware, Banyan vines and Windows NT) and PEER TO PEER NETWORK OPERATING SYSTEM (such as Microsoft Windows for Workgroups, Novell personal NetWare, Windows for Workgroups, Windows 95.).

METHODS OF DATA TRANSMISSION

COMMUNICATION CHANNELS

The term internal data transmission refers to the transfer of data within a computer, while external data transmission refers to the transfer of data to either local peripheral equipment (e.g., printers) or remote computers. A data communications channel is a path through a medium that data can take to accomplish a communication task.

In effect, channels are data highways carrying signals from sending station to receiving stations along predefined routes.

The communication links are established using following methods:

Paired wires and cables

The twisted pair transmission medium consists of two insulated copper wires, typically about 1mm thick. These two wires are twisted together in a helical form. This twisting reduces the electrical interference from similar cables close by. The telephone system is an excellent example of a twisted pair network. Twisted pair can be used for both analog and digital transmission. The bandwidth that can be achieved with twisted pair depends on the thickness and the distance travelled. Typically, a transmission rate of several megabits per second can be achieved for a few kilometers. Twisted pair, due to their adequate performance and low cost, is widely used in many areas.

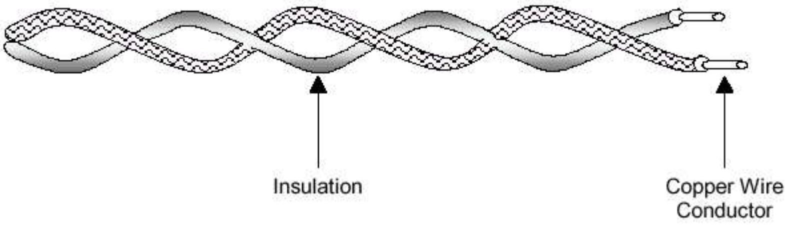


Fig 1.2 Paired Wires & Cables

Co-axial cables

Coaxial cable, as shown in Fig 1.3, has better shielding than twisted pair. Thus, they have the advantage that they can span longer distance at relatively higher speed.

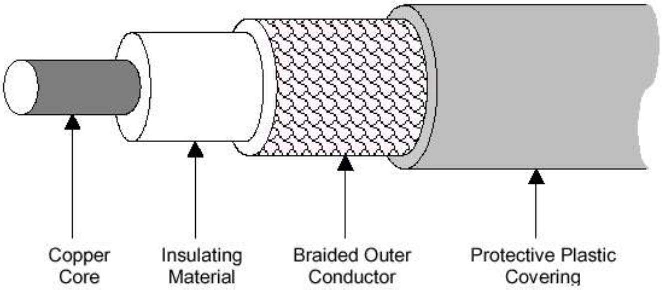


Fig 1.3 Co-axial Cables

A coaxial cable consists of a stiff copper wire as the core, which is surrounded by an insulating material. The insulator is surrounded by a cylindrical conductor in the form of a closely woven braided mesh. This entire setup is then covered by a plastic coating. Two types of coaxial cables that are widely used. The baseband coaxial cable is a 50- ohm cable and is commonly used for digital transmission. Due to the shielding structure, they give excellent noise immunity. The bandwidth depends on the length of the cable. Typically, 1 to 2 Gbps is possible for a 1-km cable. Longer cables may also be used. They, however, provide lower data rates unless used with amplifiers or repeaters.

Fibre optic cables

Fibre Optic Cable or Optical fibers, as the name suggests, employ the medium of light to transmit information. Thus, information can be transmitted at very high speed - the speed of light and it eliminates problems like heat dissipation. Optical fibers are typically used to provide a bandwidth of 1 Gbps although bandwidth in excess of 50,000 Gbps is possible. This limitation is due to the unavailability of technology that can convert optical signals to electrical signals and vice versa at such a fast rate. The technology behind optical fibers employs three components: the light source, transmission medium and the detector. The light source, connected at one end of the transmission medium, generates a pulse of light that corresponds to 1 bit of data.

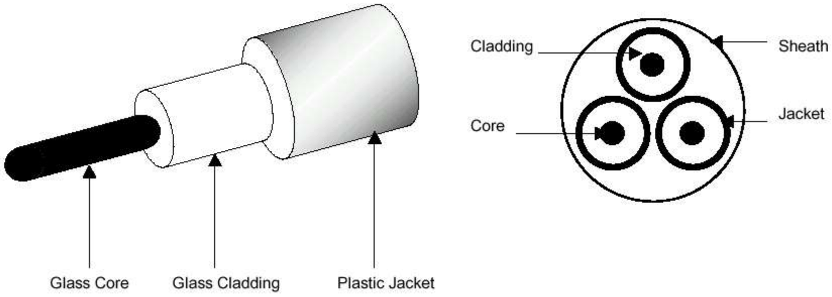


Fig 1.4 Fiber-optic Cables

The presence of no light is equivalent to 0 bit. The transmission medium used is an ultrathin fiber of glass. The detector at the other end of the transmission medium detects the presence of light pulses and generates an electrical signal accordingly. From the above discussion, optical fibers allow unidirectional transmission. Fig 1.4 gives the structure of an optical fiber.

WIRELESS TRANSMISSION

The transmission media described above provides a physical connection between two computers. This is quite often not feasible especially when the geographical distance between the two computers are very large. Communication in these types of setup is carried out by employing various other mediums such as microwaves, radio waves etc. Communication, employing these types of mediums, is called wireless communication.

Radio Transmission

The obvious advantage of using radio waves comes from the fact that radio waves are easily generated, can travel longer distances, can penetrate buildings and are omnidirectional. However, radio waves have the disadvantage that arises from the fact that radio waves are frequency dependent. At low frequencies, the power of the radio waves deteriorates as the distance traveled from the source increases. At high frequencies, the radio waves tend to travel in a straight line and bounces of obstacles. They are also absorbed by rain and are subjected to interference from motors and other electrical equipment.

Microwave Transmission

Microwave transmission offers a high signal to noise ratio. However, it necessitates the transmitter and the receiver to be aligned in a straight line without interference. In addition, because of the fact that microwaves travel in a straight line, it becomes necessary to provide repeaters for long distances since the curvature of the earth becomes an obstacle. Some waves may be refracted off low-lying atmospheric layers and thus may take slightly longer to arrive. They may also be out of phase with the direct wave thus creating a situation called multipath fading where the delayed wave tend to cancel out the direct wave. Microwaves have the advantage that they are relatively inexpensive and require less space to setup antennas. They can also be used long distance transmission.

Infrared and Millimeter Waves

Infrared and millimeter waves can be effectively used for short-distance communication. They are relatively cheap, directional and easy to build. However, they do not pass through obstacles. This feature of infrared and millimeter waves is often desirable because they do not interfere with other infrared setup nearby. They also provide better security than radio waves.

Lightwave Transmission

Modern lightwave transmission employs lasers for transmission. They however are unidirectional. Thus, both transmitter and receiver are required to be present in one site. They offer high bandwidth, very low cost and are relatively easy to install. The disadvantage of using lightwave transmission is that they cannot penetrate rain or thick fog. Focussing is also a problem that can be caused by heat. Mirrors are required to focus the beam to the detector.

The preferable method used for a particular data transmission system can be selected from following table:

Medium	Type of signaling	Maximum data(without transfer rate	Range cost repeaters	Comparative
Twisted pair	Digital	9600 bps.	2-3 km.	Low

	Analog	2 Mbps.	5-6 km.	Low
Coaxial cable	Digital	1-2 Mbps.	5 km.	Moderate
	Analog	50 Mbps	1 km.	Moderate
Optical fibre	Digital	200Mbps.	26 km.	Moderate
Microwave	Digital Analog	1-3 Mbps	80 km.	Low
Infrared light	Digital	1-3Mbps	-	Low
Laser	Digital	1-3Mbps	-	Low

Coaxial cables, microwave circuits and communications satellite are commonly used to provide these channels. Coaxial cables are groups of specially wrapped and insulated wire lines that are able to transmit data at high rates. Microwave systems use very high frequency radio signals to transmit data through space. When microwave facilities are used, the data may be transmitted along a ground route by repeater stations that are located about 25 miles apart. The data signals are received amplified, and retransmitted by each station along a route.

THE OSI SEVEN LAYER MODEL

Communication over a network is a complex task. To simplify the task of discussing and building networks, the OSI (Open Systems Interconnection) seven-layer networked model was developed by the International Standards Organization (ISO), a branch of the United Nations headquartered in Geneva.

The OSI reference model consists of the following seven layers:

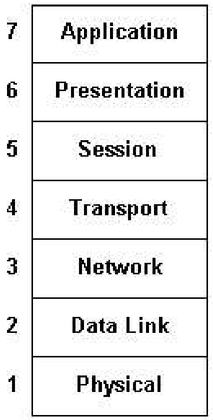


Fig 1.5 OSI Seven Layer Model

OSI applies to a great variety of networking situations. The seven layers, numbered from the bottom to the top, represent the seven different aspects of networking. Layer 1, the physical layer, is the most concrete, consisting of components that can actually be touched. On the other hand, layer 7, the application layer, is the most abstract, consisting of high-level software.

DATA TRANSMISSION ON OSI MODEL

The sending process has some data it wants to send to the receiving process. It gives the data to the application layer, which then attaches the application header, AH (which may be null), to the front of it and gives the resulting item to the presentation layer.

The presentation layer may transform this item in various ways and possibly add a header to the front, giving the result to the session layer. It is important to realize that the presentation layer is not aware of which portion of the data given to it by the application layer is AH, if any, and which is true user data.

This process is repeated until the data reach the physical layer, where they are actually transmitted to the receiving machine. On that machine the various headers are stripped off one by one message propagates up the layers until it finally arrives at the receiving process.

How does a receiving layer know what the sending peer is requesting? Each layer adds its own control information, called a header which contains that layer's request and /or information. This header is read and processed by the peer layer.

Suppose you are using two network applications based on DOS and UNIX, when the DOS application's layer 7 needs to accomplish some task, it produces a request. This request, along with some layer 6 parameters, are passed to the DOS application's layer 6. Layer 6 accepts the request as data and sends a new package, including layer 7's data and a header of its own to the layer below.

Eventually, the data packages are transferred from DOS application's layer 1 to the UNIX application's layer 1. UNIX application layer strips of each header perform the requested tasks, and pass what it considers a data package to the layer above. Finally UNIX application's layer 7 receives the package from its layer 6 and interprets the request. As you can see, headers add a lot of extra information, but this information is necessary for each application layer to communicate with peer application layers.

The layer's data packages are called different names depending on the layer of the model being discussed.

The following names are commonly used terms:

■	Physical layer data	Bits
■	Data link layer data	Frames
■	Transport layer data	Datagrams and Segments
■	Application layer data	Messages

PHYSICAL LAYER

The physical layer interfaces directly with the physical media in the network . It sends bits over the wire or over another connection, such as a fiber-optic cable or wireless connection, between computers. It also deals with the electrical signals that represent the 0 (off) or 1 (on) state of a bit traveling over the network cabling. The design issues have to do with making sure that when one side sends a 1 bit, it is received by the other side as 1 bit, not as '0' bit .The decision to use a particular type of network interface card or a choice between twisted-pair and coaxial cable is a decision about the physical layer, which is implemented in networking hardware.

The physical layer governs following basic areas of media connectivity.

Point to Point A point to point connection is a direct link between two devices. When you attach a personal computer directly to a printer, you have created a point to point link. Point to point connections are often associated with modems, but the term can be used to describe any system where two devices are directly connected to one another.

Multi Point to Point Multipoint connection is a link between three or more devices. In Lan a server connected to multiple nodes and devices is the bus. Multipoint connection share the same bandwidth so the over all capacity divided among the every device connected to the media.

Physical Topology All computers on network relay multiple connections. The physical connection of computer in transmission media is called physical topology. Following are the various topologies:

Ring Topology (closed loop)

In a ring topology, information is passed from one node to the other in series as illustrated in Fig. This topology is often referred to as a loop, if one of the nodes is designated as the network control node. Information is divided into packets for transmission between nodes, and each packet contains the address of the node that is to receive the information. The ring topology is typically found in local network applications. Its major disadvantage is that the entire network goes down if any one of the nodes or links fail.

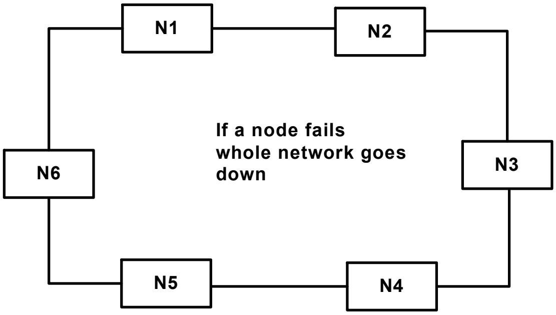


Fig 1.6 Ring Topology

Multidrop Topology

A more popular topology is the multipoint, or multidrop topology illustrated in Fig 1.7. It is also referred to as a bus topology.

In the multidrop structure, nodes share a single link or communication channel somewhat similar to the multiplexed microcomputer bus structure. Each node has a unique address. All nodes will receive a message, but only the addressed node is to respond. Notice that if one node is down, the network is still available for communications between the other nodes. Of course, if the link is broken then parts of the network will be separated. Also with nodes sharing a common channel, fewer wires or lines are needed for communication between the nodes.

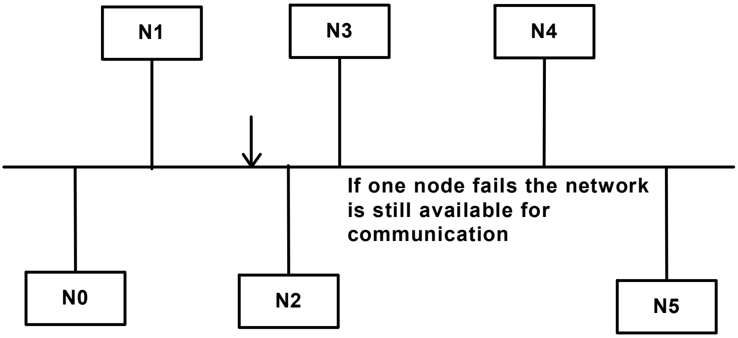


Fig 1.7 Multidrop Topology

Star Topology

The last network topology we'll discuss is the star structure, which is illustrated in figure. In the star structure, the central node is often the master. Each of the other nodes are joined to the master via separate links. When communications is primarily between the central node and the outer nodes, this network can be fairly effective. However when communications is between two or more outer nodes, this structure often has problems particularly if there is a lot of traffic. Since all communications is primarily between the central node and the outer nodes, this network can be fairly effective. However when communications is between two or more outer nodes, this structure often has problems, particularly if there is a lot of traffic. Since all communications must go through the central node, if the central node ever goes down, then the complete network will be down.

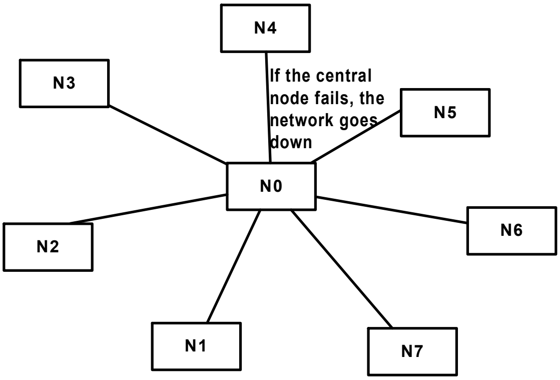


Fig 1.8 Star Topology

Tree Topology

The tree topology is shown in figure. It follows a hierarchical organization of machines.

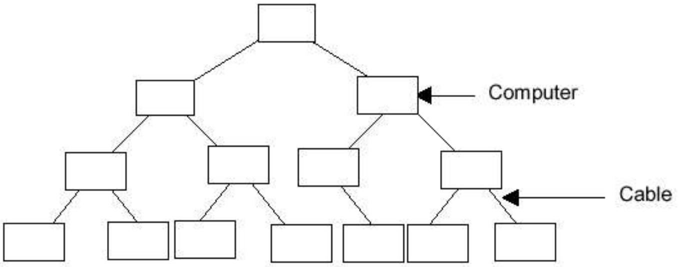


Fig 1.9 Tree Topology

Mesh Topologies

A mesh topology is the one in which each machine is connected to each other. This topology has the advantage that data is transferred at a much faster rate. It also reduces concentration of network traffic at one point. A mesh topology is shown in figure.

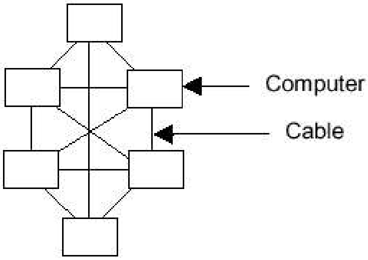


Fig 1.10 Mesh Topology

Other Topologies

Certain other topologies do not fit into the models described above. Practically, a network is a combination of two or more of the above models. One of these are shown in figure. This topology is called intersecting rings topology. The other could be irregular topology.

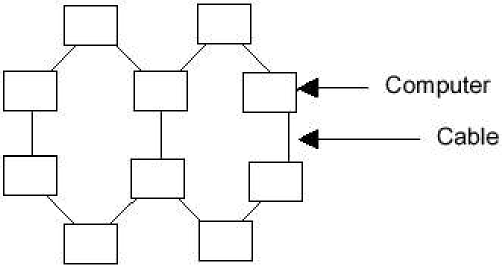


Fig 1.11 Other Topology

DATA LINK LAYER

The main task of the data link layer is to take a row transmission facility. It accomplish this task by having the sender break the input data up into data frames (typically a group of few hundred or a few thousand bytes transmitted over the network) and process the acknowledged frames sent back by the receiver.

The data-link layer ensures that frames sent over the network are received and, if necessary, resends them. Ethernet is an example of a data-link layer, as is Token Ring, and each has a different layout for a frame.

Since the physical layer merely accepts and transmits a stream of bits without any regard to meaning or structure, it is up to the data link layer to create and reorganize frame boundaries. This can be accomplished by attaching special bits patterns to the beginning and end of the frame. If these bit patterns can accidentally occur in the data, special care must be taken to make sure these patterns are not incorrectly interpreted as frame starting and ending signals.

THE NETWORK LAYER

The network layer deals with *packets*, which may be larger or smaller than frames. If the packets are larger than frames, the network layer breaks the packet into frames to send them, and reassembles them on receipt. If the packets are smaller than frames, the network layer bundles frames into packets to send them and breaks them apart on receipt.

In either case, the network layer relies on the data-link layer to transmit the frames themselves. The network layer also deals with routing packets between computers (*hosts*) on the network, and it knows the addresses of the hosts on the network.

Typically, the network layer can adjust the routing of packets to deal with network traffic. If too many packets are present in the subnet at the same time, they will get in each other's way, forming bottlenecks. The control of such congestion also belongs to the network layer. But, network layer doesn't keep track of whether packets arrived at their destination or whether any errors occurred during transmission-that job is handled by the transport layer.

In the broadcast networks, (read as LAN) the routing problem is simple, so the network layer is often thin or even nonexistent. WAN needs lot of emphasis on Networking and transporting layers of the model.

TRANSPORT LAYER

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

NetBEUI, TCP/IP, IPX/SPX, and other transport protocols handle the duties of the network layer and the transport layer. It's quite common for these two layers to be combined into a single protocol.

Under normal conditions, the transport layer creates a distinct network connection for each transport connection required by the session layer. If the transport connection requires a high throughput, however, the transport layer might create multiple network connections, dividing the data among the network connection to improve throughput.

The transport layer also determines what type of service to provide the session layer, and ultimately, the users of the network. The most popular type of transport connection is an error-free point-to-point channel that delivers messages or bytes in the order in which they are sent. However, other possible kinds of transport services are transport of isolated messages with no guarantee about the order of delivery, and broadcasting of messages to multiple destinations. The type of service is determined when the connection is established.

THE SESSION LAYER

The session layer establishes and maintains a session between applications running on different computers. It knows the names of other computers on the network and handles security issues. A session might be used to allow a user to log into a remote time sharing system or to transfer a file between two machines.

One of the services of the session layer is to manage dialogue control. Sessions can allow traffic to go in both directions at the same time, or in only one direction at a time. If traffic can only go one way at a time (analogous to a single railroad track), the session layer can help keep track of whose turn it is.

THE PRESENTATION LAYER

The presentation layer performs certain functions that are requested sufficiently often to warrant finding a general solution for them, rather than letting each user solve the problems. In particular, unlike all the lower layers which are just interested in moving bits reliably from here to there, the presentation layer is concerned with the syntax and semantics of the information transmitted.

The presentation layer provides services that a number of different applications use, such as encryption, compression, or character translation (PC ASCII to IBM's EBCDIC, for example). It relies on the session layer to pass on the encrypted, compressed, or translated material. One implementation of a presentation layer is XDR (External Data Representation) under RPC (Remote Procedure Call).

THE APPLICATION LAYER

The application layer contains a variety of protocols that are commonly needed. For example, there are hundreds of incompatible terminal types in the world. Consider the plight of full screen editor that is supposed to work over a network with many different terminal types, each with different screen layouts, escapes sequences for inserting and deleting text, moving the cursor, etc.

Many important protocols span the presentation and application layers-for example, named pipes and FTP (the File Transfer Protocol, not the application itself). Clients use named pipes, for example, to communicate with Microsoft SQL Server. FTP is familiar to all UNIX and Internet users.

Another application layer function is file transfer. Different file systems have different file naming conventions, different ways of representing text lines, and so on. Transferring a file between two different systems requires handling these and other incompatibilities. This work, too, belongs to the application layer, as do electronic mail, remote job entry, directory lookup, and various other general-purpose and special-purpose facilities.

NETWORK CONNECTIVITY DEVICES

Network connectivity devices used for networking can be divided into two categories:

- Basic networking devices
- Internetworking devices.

BASIC NETWORKING DEVICES

Devices that are used to set up a network such as a network interface card, cables, hubs and modems are referred to as basic networking devices.

- Transmission media connectors
- Network INTERFACE Boards (NIC)
- Modems
- Repeaters
- Hubs

TRANSMISSION MEDIA CONNECTORS

One of the most common connector in local area networks is the **BNC connecto**r. BNC is short for British Naval Connector or Bayonet Nut Connector or Bayonet Neill Concelman, a type of connector used with coaxial cables such as the RG-58 A/U cable used with the 10Base-2 Ethernet system. The main function of the BNC connector is to connect, extend or terminate coaxial cable networks such as the Ethernet. The various types of BNC connectors are BNC T- Connector, BNC Barrel Connector and the BNC Terminator.

The basic BNC connector is a male type mounted at each end of a cable. This connector has a center pin connected to the center cable conductor and a metal tube connected to the outer cable shield. A rotating ring outside the tube locks the cable to any female connector.

BNC **T-connectors** (used with the 10Base-2 system) are female devices for connecting two cables to a network interface card (NIC). The cables branch out from either side of the T to the next stations up or down in the trunk cable.

- A BNC **barrel connector** allows connecting two cables together.
- A BNC **Terminator** has a resistor to terminate the coaxial cable.
- BNC connectors can also be used to connect some monitors, which increases the accuracy of the signals sent from the video adapter.

NETWORK INTERFACE BOARD (NIC)

Today local area networking is a **shared access** technology. This means that all of the devices attached to the LAN share a single communications medium, usually a coaxial, twisted pair, or fiber optic cable. The physical connection to the network is made by putting a **network interface card (NIC)** inside the computer in one of the expansion slot and connecting it to the network cable. Once the physical connection is in place, it is up to the network software to manage communications between stations on the network.

The Network Interface Card (NIC) includes the circuitry and mechanical connections to convert the computer's electric signals to the electric or electromagnetic signals used on the medium. A card usually includes a signal transceiver but may provide one or more connector types.

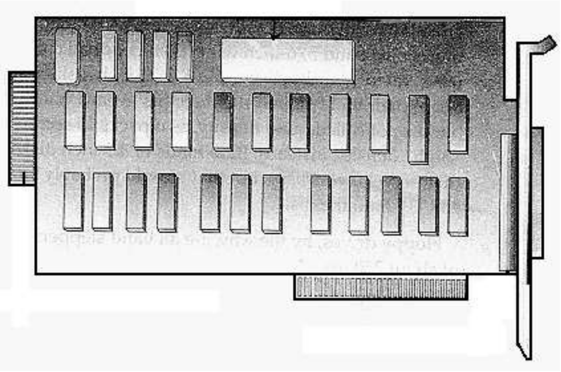


Fig 1.12 Network Interface Card

Usually, there are two different network interface cards

- One that is compatible with EISA slots
- One for PCI slots

Both the EISA base and PCI base controllers can be used with interchangeable modules for commonly used local area networks such as 10Base-T, 100Base-TX, 100Base-T4, or 100VG-AnyLAN. Each of the modules slides into the baseboard. A common driver is used for all configurations.

Transceivers

It is a device that can transmit as well as receive electric or electromagnetic signals on the transmission media. It is built in to NIC. Network card supports various types of network connections. On a NIC, the physical interface between itself and the network is called a transceiver-a term used to refer to a device that both transmits and receives data. Transceivers on network cards can receive and transmit digital or analog signals. The type of interface that the network adapter uses can often be defined on the physical network adapter. Jumpers (small connectors that create a circuit between two pins on the physical card) can usually be set to specify the type of transceiver the adapter should use, according to the networking scheme. For example a jumper set in one position may enable the RJ-45 connector to support a twisted-pair network; in other position, the same jumper might enable an external transceiver to be used in a 10Base5 (Thicknet) network. (This option may be selected by setup software in newer NICs.)

Transmission Media Adapter

The purpose of this adapter is to receive signals from one type of connector and convert them for use with another type. They receive signals from a computer's bus and convert them for use with transmission media (the computer bus and the transmission media each uses a different type of connector like BNC, AUI, RJ-45).

Modems

When a communication link must be established between a PC and another computer more than 50 feet away, the most economical way of doing so is usually through the public telephone systems. These systems are generally called as the General Switched Telephone Networks (GSTN). To do this a device called the modem must be installed between the PCs system board and the telephone system.

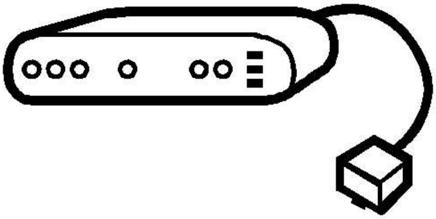


Fig 1.13 Modem

Modem is acronym for **mo**dulator-**dem**odulator. A modem is a device or program that enables a computer to transmit data over telephone lines. A modem converts the binary digital signals it receives into analog signals the telephone system can transmit. Modems can also convert analog signals they receive from the telephone system into digital signals a PC can receive. The nature of signal conversion process depends upon the source and the destination of the signal the modem receives.

REPEATERS

Electromagnetic waves become weaker (attenuate) as they pass through a transmission medium. Repeater is a type of amplifier, amplifies all incoming electromagnetic waves including noise. Another type of referred as a signal regenerating repeater, scripts data out of the transmission signal. It then reconstructs and retransmit the signal on the media segment. The new signal is an exact duplicate of the original signals, boosted to its original strength.

Repeaters are used in networks with digital signaling schemes to combat attenuation. Also known as baseband transmission, digital signals consist of data bits that are either on or off, represented by a series of ones and zeros. Repeaters allow for reliable transmission at greater distances than the media type would normally allow. When a receiver receives an attenuated incoming baseband transmission, it cleans up the signal, increases its strength, and passes it on to the next segment.

Amplifiers, though similar in purpose, are used to increase transmission distances on networks that use analog signaling, referred to as broadband transmission. Analog signals can transfer both voice and data simultaneously—the wire is divided into multiple channels so different frequencies can be transferred at the same time.

Repeaters (and amplifiers) operate at the Physical layer of the OSI model. They can be used to connect cable segments - even those using different media types - as long as both segments to be joined use the same media-access method.

Usually, network architectures specify the maximum number of repeaters allowed on a single network. The reason for this is a phenomenon called “propagation delay”. In cases where there are multiple repeaters on the same network, the brief period of time each repeater takes to clean up and amplify the signal, multiplied by the number of repeaters/amplifiers, can cause a noticeable delay of transmissions on the network. When deciding whether to choose repeaters as a connection option, you must also consider that they have no addressing or translation capability, and thus, cannot be used to ease network congestion.

HUBS

A hub is a hardware device, operating at the OSI Physical layer, that acts as a central connecting point and joins lines in a star network configuration.

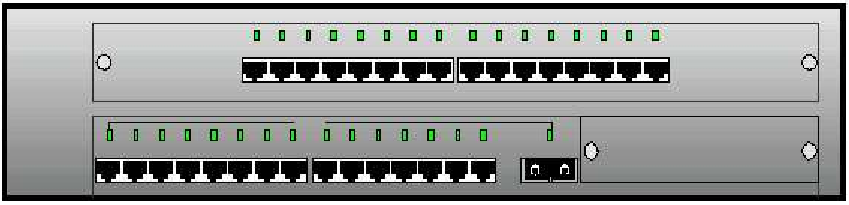


Fig 1.14 A Hub

There are three main types of hubs: passive, active, and intelligent. Passive hubs, which don’t require power, act merely as a physical connection point, adding nothing to the signals that pass through. Active hubs, on the other hand, require power, which they use to regenerate and strengthen signals passing through them. Intelligent hubs can provide services such as packet switching and traffic routing.

The hubs are three types :

(a) Passive

(b) Active

(c) Intelligent

Passive Hub A passive hub connects medium segments together. No signal regeneration is performed.

Active Hub A active hub is like a passive hub except it regenerates or amplifies signal.

Intelligent Hub Intelligent hub are, in addition to signal regeneration and network management, also perform activities such as intelligent path selection.

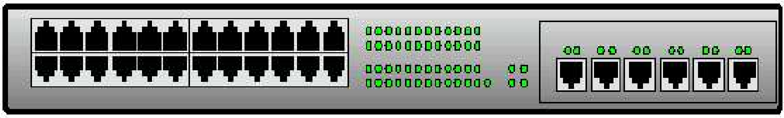


Fig 1.15 Intelligent Hub

BRIDGES

A device that connects two local area networks (LANs) or two segments of the same LAN is known as a **bridg**e. Bridges can be an improvement over repeaters because bridges ease congestion on busy networks: Bridges read the target destination's MAC address from each incoming data packet, then examine the "bridging" tables to determine what to do with the packet.

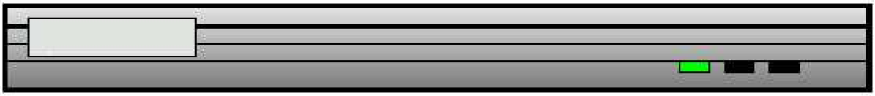


Fig 1.16 A bridge

Because it functions basically as a repeater, a bridge can receive transmissions from any segment; however, it is more discriminating than a repeater in retransmitting these signals. If the packet's destination lies on the same media segment as the bridge, the bridge knows that the packet has reached its destination, and so it is discarded. But, if the packet's destination lies on a different segment, the bridge knows to pass it along. This action helps to lessen network congestion; for example, a segment doesn't have to deal with transmissions not meant for it. However, bridges do forward all broadcast transmissions they receive, and therefore, are unable to reduce broadcast traffic.

Bridges can connect segments that use different media types; for example, a connection of 10BaseT to 10Base2. They cannot, however, connect networks using different media-accessing schemes—you could not connect an Ethernet network to a Token Ring network. The exception to this would be a translation bridge, which is a bridge that translates between different media-access methods, allowing the Translation Bridge to link various network types. Another special type of bridge, a transparent bridge (or learning bridge), “learns” over time where to direct packets it receives. It does this by continually building bridging tables, adding new entries when they become necessary.

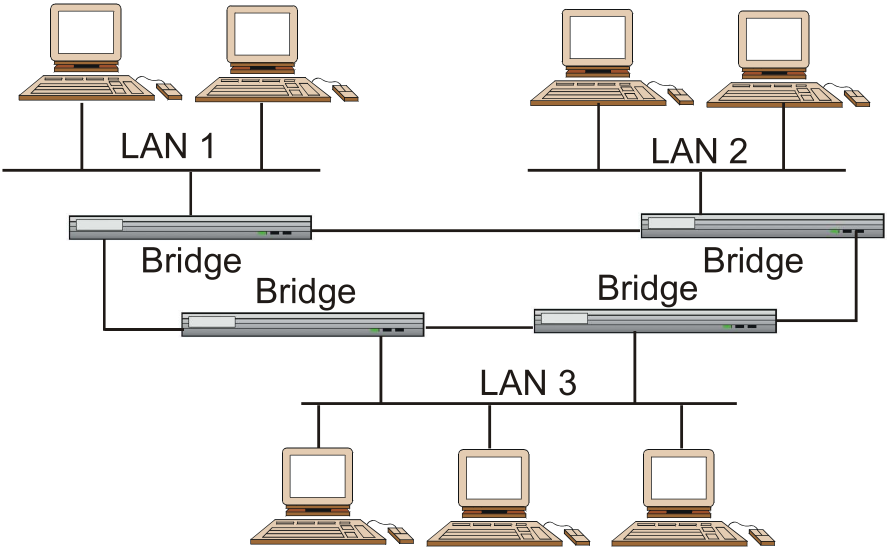


Fig 1.17 Connecting various LAN using bridges

Possible disadvantages of bridges are that bridges take longer than repeaters to pass data through because they examine the MAC address of each packet. They are also more difficult to operate, and are more expensive.

ROUTERS

A router is a networking connectivity device that works at the OSI Network layer, and can link two or more network segments (or subnets). It functions in a similar manner to a bridge; but, instead of using the machine’s MAC address to filter traffic, it uses the network address information found in the Network layer area of the data packet. After obtaining this address information, the router uses a routing table of network addresses to determine where to forward the packet. It does this by comparing the packet’s network address to the entries in the routing table—if a match is found, the packet is sent to the determined route. If a match is not found, however, the data packet is usually discarded.

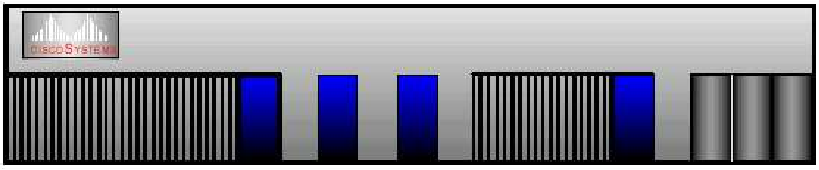


Fig 1.18 A CISCO router

There are two types of routing devices: static and dynamic. Static routers use routing tables that a network administrator must create and update manually. In contrast, dynamic routers build and update their own routing tables. They use information found on both their own segments and data obtained from other dynamic routers. Dynamic routers contain constantly updated information on possible routes through the network, as well as information on bottlenecks and link outages. This information lets them determine the most efficient path available at a given moment to forward a data packet to its destination.

As routers can make intelligent path choices—and filter out packets they do not need to receive—they help reduce network congestion, conserve resources, and boost data throughput. Additionally, they make data delivery more reliable, because routers can select an alternate path for the packet if the default route is down.

Routers are superior to bridges in their ability to filter and direct data packets across the network. And unlike bridges, they can be set to not forward broadcast packets, which reduce network broadcast traffic. Another major advantage of the router as a connectivity device is that, because it works at the Network layer, it can connect networks that use different network architectures, media-access methods, or protocols. A router can, for example, connect an Ethernet subnet to a Token Ring segment. It can link several smaller networks that use different protocols, provided the protocols in use are routable.

BROUTERS

The term "brouter" is a combination of the words "bridges" and "router". As its name would suggest, a brouter combines the functions of a bridge and a router. When a brouter receives a data packet, it checks to see if the packet was sent in either a routable or non-routable protocol. If it is a routable protocol packet, the brouter will perform a routing function, sending the packet to its destination outside the local segment, if necessary.

In contrast, if the packet contains a non-routable protocol, the brouter performs a bridging function, using the MAC address to find the proper recipient on the local segment. Brouters must maintain both bridging and routing tables to perform these two functions;

therefore, they operate at both the Data Link and Network layers of the OSI model.

GATEWAYS

A gateway is a method of enabling communications between two or more network segments. A gateway is usually a dedicated computer that runs gateway software and provides a translation service, which allows for communications between dissimilar systems on the network. For example, using a gateway, an Intel-based PC on one segment can both communicate and share resources with a Macintosh computer or a mainframe.

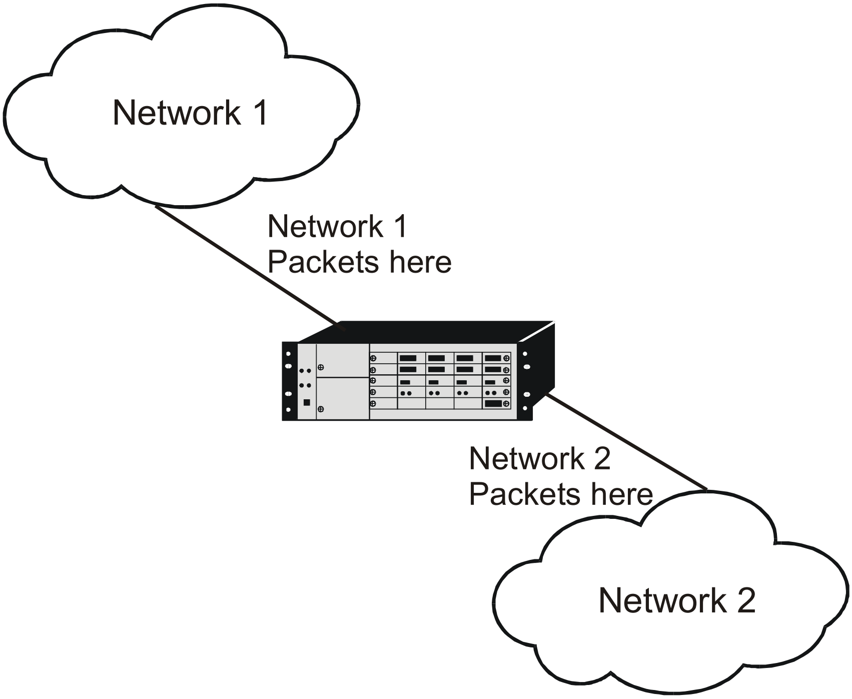


Fig 1.19 Gateway communication between two Networks

Another function of gateways is to translate protocols. A gateway can receive an IPX/SPX message that is bound for a client running another protocol, such as TCP/IP, on a remote network segment. After it determines that the message packet's destination is TCP/IP protocol. (This is in contrast with a bridge, which merely "tunnels" a message using one protocol inside the data format of another protocol—if translation is to occur, the receiving end does it.) Mail gateways perform similar translation operations, converting emails and other mail transmissions from your native mail application's format to a more universal mail protocol, such as SMTP, which can then be used to route the message across the Internet.

Gateways can function at the Network layer but they can also work at the layers higher than the Network Layer. In other words they can function at the Gateways are of two types. They are:

Transport gateways	connect two parts of an application in the transport layer.
Application gateways	connect two parts of an application in the application layer.

Gateways primarily operate at the application layer of the OSI model, although they often fulfill certain functions at the session layer, and occasionally as low as the Network layer. However, for the purposes of the Networking Technology, consider the gateway to only operate at or above the Transport layer.

Although gateways have many advantages, you need to consider a few things when deciding whether to use them on your network. Gateways are difficult to install and configure. They are also more expensive than other connectivity devices. One other issue: Due to the extra processing cycle that the translation process requires, gateways can be slower than routers and related devices.

EXERCISE

Fill in the banks :

1. Collections of computers that are able to communicate with each other are known as ___________.
2. Two types of transmission technologies used in computer networks are ______ and __________.
3. The LANs can be distinguished from other networks based on the following characteristics: _______, _________ and ________.
4. The three main types of networks are _______, _________ and _________.
5. A collection of interconnected networks is called ___________.
6. Short messages sent across on the network are known as ___________.
7. In OSI model, the __________ layer consists of components that can actually be touched where as the _________ layer, is the most abstract, consisting of high-level software.
8. A BNC barrel connector allows connecting _____ cables together.
9. There are three main types of hubs: _____, ____, and _____.
10. __________ is a device or program that enables computer to transmit data over telephone lines.
11. A device, which is used to regenerate signal on a network, is known as __________.

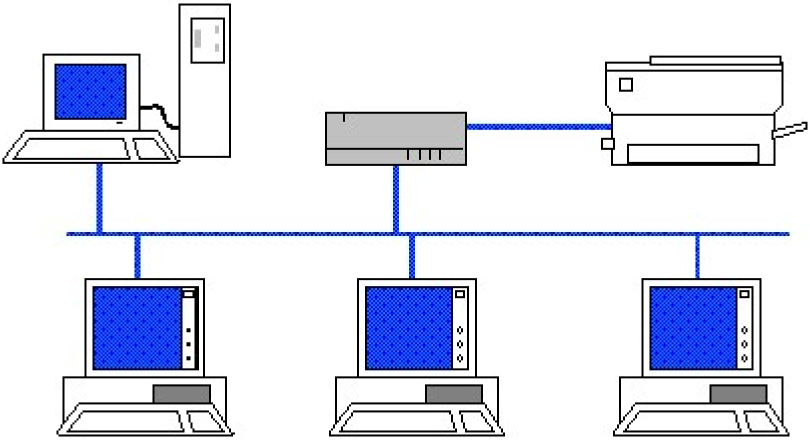
Answer the following questions:

1. What are the basic objectives of Networking Architecture? Discuss them in brief.
2. Explain briefly the LAN and WAN.
3. List the advantages and disadvantages of networking.
4. What are networking applications? Explain briefly.
5. What are the software components required for providing basic network services?
6. What are the three roles of computer and how are they different from each other?
7. What are the different methods of Data transmission. Discuss them in brief.
8. What is the role of modem, NIC, brouter, router in data transmission.
9. Discuss various layers of OSI model.
10. What is the difference in static & dynamic routing?
11. How will you differentiate Hubs with Bridges?
12. Discuss various types of physical topologies in physical layer.

CHAPTER 2

Networking & Windows NT

NETWORKING AND WINDOWS NT
WINDOWS NT ARCHITECTURAL VIEW
WINDOWS NT SERVER AND WORKSTATION
DOMAIN MODELS
WORKGROUPS
MULTIPLE DOMAINS
SECURITY STRUCTURE OF WINDOWS NT



NETWORKING AND WINDOWS NT

Microsoft Windows NT Server version 3.5 was released in September of 1994. Unlike the earlier version, it was less memory hungry, included TCP/IP and Novell connectivity and included Windows for workgroups versions of the administrative tools so that network administrators could work from a workgroup machine rather than an NT machine.

Version 3.51 was released in October 1995 which had support for PCMCIA cards, file compression and a host of bug fixes.

NT version 4 was released in 1996 It has no networking changes though it does have a few changes in looks and a few new features.

FEATURES OF WINDOWS NT

When you install Windows NT Server 4.0, you end up with a system that can immediately function as a file and print server or a Web server and has the potential (and underlying foundation) to serve as an application server (but no applications are included). You also receive a number of services and utilities in support of these core functions.

Windows NT is said to be an architecturally independent operating system. It has following main features:

Reliability by protecting the core operating system from malfunctioning applications and by isolating the operating system and applications from direct operations on hardware. Structured exception handling handles processing of application and low-level errors. NTFS provides increased reliability for file operations by a built-in transaction logging system.

Extensibility by adopting a client/server model using a base operating system (kernel, the client) extended by application programming interfaces (APIs, the servers). In this case, the term *client/server* is used in its UNIX context, not that of the client/ server model applied to networks and database applications.

Portability across different processor platforms, including RISC systems, through the use of a processor-specific Hardware Abstraction Layer (HAL) that provides the isolation layer between the operating system and hardware. Portability of Windows NT is provided by writing the source code for the operating system, with a few exceptions, in an ANSI-standard C programming language.

Security Security in Windows NT primarily is implemented through ACLs (Access Control Lists). The Windows NT security has following criteria.

Secure logon The system must require the user to provide a unique logon identifier (username) and password to gain access to the system.

Discretionary access control

The person who owns a resource (directory, for example) can specify which other users can access the resource and what level of access they'll have over it.

Auditing This refers to the capability to identify and log several security events to identify and protect against security breaches.

Memory protection

Secure memory protection prevents one process from reading another process data without authorization and ensures that memory is reinitialized before being reused.

Compatibility with existing 16-bit DOS and Windows applications, plus the most common PC hardware devices and peripherals. Windows NT also provides the capability to execute applications written to the POSIX.1 standard. Early versions of Windows NT supported NTFS, HPFS (OS/2's High-Performance File System), and FAT file systems. Windows NT 4.0 no longer handles HPFS volumes.

Personality is the key to compatibility. Most operating systems, such as DOS, are limited to a single personality. DOS can only run DOS programs. However, Windows NT was designed to support multiple simultaneous personalities. When Microsoft first began working on NT, they planned that it would support the OS/2 Presentation Manager interface as its primary personality. In addition, Windows NT supports a POSIX personality, an OS/2 personality, and a DOS/Windows personality

Scalability for better performance through the use of multiple CPUs with a Symmetrical Multiprocessing (SMP) architecture. To take advantage of SMP, 32-bit Windows applications must be written to use multiple threads of execution.

Fault-Tolerance In order for Windows NT to be accepted as an enterprise workstation and server product, it was important to enable it to gracefully handle abnormal conditions. This is the essence of fault-tolerance. Windows NT has many features that provide varying levels of fault-tolerance for the system. Included in NT's list of fault-tolerant features are NT's journal-based, recoverable file system (NTFS), disk mirroring and disk stripping with parity (RAID 1 and RAID 5), disk sector sparing, and support for an uninterruptible power supply (UPS).

WINDOWS NT ARCHITECTURAL VIEW

Windows NT architecture has two main properties : modular and client/server.

Modular means each component (or module) within the architecture has sole responsibility for the function it is designed to provide. In addition, no other module repeats the functions performed by another. In the other possible architecture, called monolithic design, the blocks of code often provide many functions with little clear definition. This allows for smaller and tighter code, but also makes the system less adaptable. The NT operating system has two modes: **User Mode** and **Kernel Mode**, which will be discussed in next section.

The client/server property of NT architecture doesn't refer to NT's capability to be used in client/server database or network systems. It means that the internal pieces of NT communicate based on a client/server paradigm. When a piece of code needs something, it is considered the client. The piece of code that fulfills the request is the server. As shown in the Fig. 2.1, the client server refers to the organizational layout of NT's modular components.

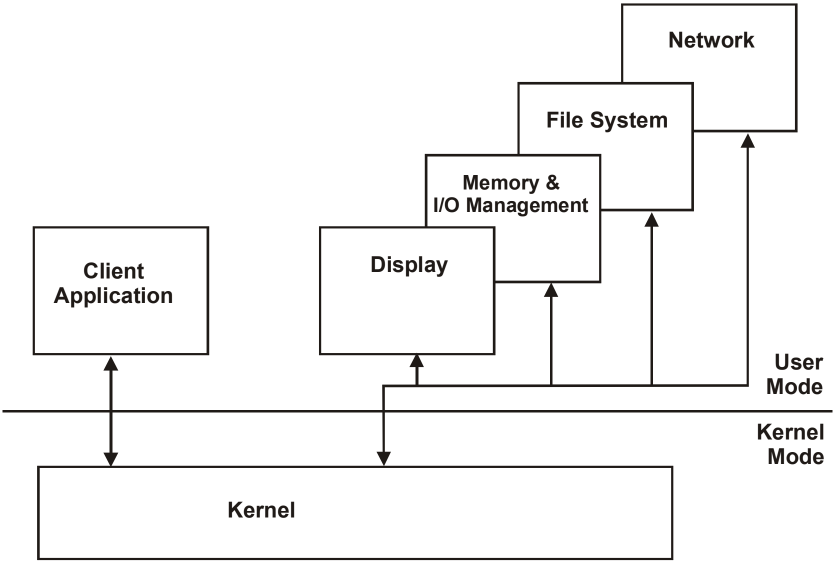


Fig 2.1 The client/server operating system design

USER MODE

Applications and their subsystems run in **User Mode**. This mode is referred to as a less privileged processor mode compare to kernel mode. **User Mode** applications are limited to assigned memory address spaces and can't directly access other memory address spaces. **User Mode** uses specific application program interfaces (APIs) to request system services from a **Kernel Mode** component.

The purpose of separating the applications in **User Mode** from the hardware, of restricting the memory address spaces that applications can access, and of forcing the applications to run all requests for system services through the **Kernel Mode**, is to protect against the possibility of an application crashing the system, and also to protect against unauthorized user access.

User mode subsystems

There are four main subsystems in **User Mode.** This include three **protected environment subsystem** and a security subsystem. :

- Win32 Subsystem
- OS/2 Subsystem
- POSIX (Portable Operating System Interface) Subsystem
- Security Subsystem

In addition to the four formal subsystems, an **NT Virtual DOS Machine** (NTVDM) is also a feature of **User Mode**. Its function is to run MS-DOS-based and Windows 3.x based (all 16-bit) applications.

The **Win32 Subsystem** is the primary application subsystem. All 32-bit Windows applications run in the **Win32 Subsystem**. The **OS/2 Subsystem** environment created by win32 system to run OS/2 1.x compatible applications.

The **OS/2 Subsystem** obtains its user interface and its screen functions from the **Win32 Subsystem**, and requests Executive Services in **Kernel Mode** to perform all other functions for it. (Executive Services is covered in the next section of this chapter.)

The **POSIX Subsystem** is designed to run POSIX 1.x compatible applications. It functions very much like the **OS/2 Subsystem**. The **POSIX Subsystem** uses the **Win32 Subsystem** to provide all of its screen and graphical displays, and it requests Executive Services in **Kernel Mode** to perform all other functions for it.

Finally, the **Security Subsystem** supports the logon process. The **Security Subsystem** also communicates with the **Win32 Subsystem**.

KERNEL MODE

Kernel Mode refers to a highly privileged mode of operation. It is called "highly privileged" because all code that runs in **Kernel Mode**

can access the hardware directly, and can also access all memory. A process running in **Kernel Mode** is not restricted to its own specific address space as, an application running in **User Mode**.

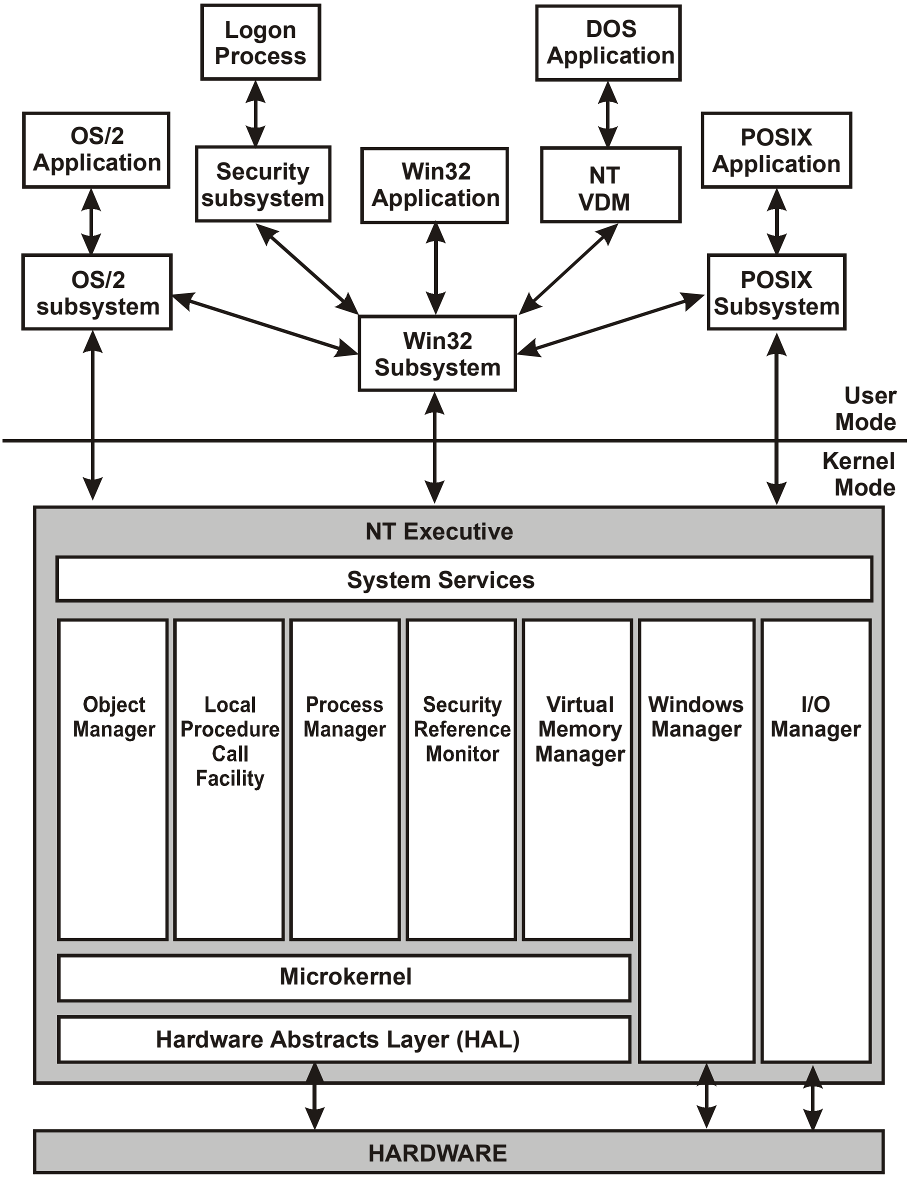


Fig 2.2 Windows NT Architectural View

The **kernel** is ultimately responsible for all actions on the system and almost all functions on the system pass through the kernel. Windows NT also uses a **microkernel** which communicates with the hardware.

The entire set of services that comprise **Kernel Mode** is called Executive Services (or sometimes the **Windows NT Executive**). Executive Services provide **Kernel Mode** services as requested by applications in **User Mode**. A clear, concise definition is that the NT Executive provides the operating system fundamentals that can be provided to all other applications running on the system.

Thus the three kernel - The **kernel**, **kernel mode** and **microkernel** are although related but are not the same thing. The **kernel** is a discrete piece of code that makes up the core of the operating system. **Kernel mode** is a privileged state of operations supported by the microprocessor. In Windows NT, the **microkernel** runs in **kernel mode**, which means that it runs in a privileged processor mode, where the microprocessor is responsible for protecting the kernel from harm.

Kernel Mode components

Kernel Mode is made up of numerous components, integrated to form the major Windows NT operating system. Aside from the kernel itself, the major pieces of the NT Executive are as follows:

- I/O Manager
- Windows Manager
- Object Manager
- Process Manager
- Virtual Memory Manager
- Local Procedure Call Facility
- Security Reference Monitor

I/O Manager

The I/O Manager is responsible for all input and output to disk storage subsystems. As it manages input and output, the I/O Manager also serves as a manager and supporter of communication between the various drivers. The I/O Manager can communicate directly with system hardware if it has the appropriate hardware Device Drivers. Subcomponents of the I/O Manager include a Cache Manager, various file system drivers, and network drivers. Another subcomponent of the I/O Manager is the Hardware Device Drivers that perform direct hardware access.

Windows Manager

Window Manager is responsible for providing all of the graphical user interface. Window Manager communicates directly with the Graphics Device Drivers, which in turn communicate directly with the hardware.

Object Manager

The Object Manager piece of the NT Executive is used to create, modify, and delete objects used by all the systems that make up the NT Executive.

Process Manager

The Process Manager is responsible for creating, removing, and modifying the states of all processes and threads.

Virtual Memory Manager

The Virtual Memory Manager (VMM) provides management of the system's virtual memory pool.

Local Procedure Call Facility

The Local Procedure Call (LPC) Facility is integral to the client/ server design of Windows NT.

Security Reference Monitor

The Security Reference Monitor (SRM) is the bedrock of the all security on a Windows NT system and is responsible for enforcing all security policies on the local computer.

There last five Kernel Mode subsystems communicates directly with the **microkernel**. The **microkernel** is the very heart of the NT operating system. It handles interrupts, schedules threads, and synchronizes processing activity. The microkernel, in turn, communicates with the hardware abstraction layer (HAL). The HAL is designed to hide the varying characteristics of hardware so that all hardware platforms appear the same to the microkernel. As a result, only the HAL, and not the entire microkernel, needs to address each and every hardware platform. The HAL can communicate directly with the computer's hardware.

WINDOWS NT SERVER AND WORKSTATION

Microsoft NT comes in two flavours - Server and Workstation. Both of there products although has the same core technology but has different roles to play.

Windows NT Workstation was designed as a robust, 32-bit multi-threaded, multi-tasking operating system that was capable of running high-end engineering or mission-critical client/server applications, whereas Windows NT Server was designed to provide file, print, and application services to diverse clients.

As both the product are using same core technology, they have more similarities than difference. Some of the features common to both Windows NT products are:

- The Windows NT platform is designed to provide a powerful operating system platform capable of scaling from the simplest file and print services network, to the largest enterprise network providing file and print services to users.
- The core networking components are virtually identical between NT Server and NT Workstation.

- Windows NT includes a full set of powerful GUI tools for administering most parts of the operating system. These include - User Manager, Server Manager, Disk Manager, Performance Monitor, Event Viewer, RAS Admin, DHCP Manager and WINS Manager.
- Windows NT integrates well with other desktop operating systems and network operating systems. Making both NT Workstation and NT Server fit seamlessly into a NetWare environment.
- The world is continuing to advance toward a worldwide computer network infrastructure, and the primary protocol for that network is TCP/IP. Both Windows NT products provide robust TCP/IP services.
- The Remote Access Service (RAS) in Windows NT is a very robust tool for creating WAN connections to support today's advanced client/server computing environments.
- NT was intended for use in enterprise environments, therefore it was vital that NT be able to prevent unauthorized access to business-critical information. As part of the security system, Windows NT requires that the actions of all users, both local and remote, be verified against a built-in security database. So access to any part of the system would only be granted after a user provides a valid user account and password.
- Security is important for protecting your data from accidental or intentional mishandling; however, regular backups are important for protecting your data from other kinds of problems. Microsoft has included a full-featured, graphical tape backup utility with Windows NT.
- Windows NT supports two major files systems:
  - NT File System (NTFS)
  - File Allocation Table (FAT)

Beside above features, which are common to both Windows NT Server and Windows NT workstation, following features are available in NT Server product only.

- Whereas NT Workstation is limited to 10 incoming network connections, Windows NT Server has no such limitation.
- NT Server is designed to meet the needs of high-end, mission-critical systems. It has a fault-tolerant disk driver, called FTDISK.SYS. This driver uses redundant array of inexpensive disks (RAID) levels 1 and 5 to handle fault-tolerant disk configurations such as disk mirroring, disk duplexing, and disk striping with parity.
- There are two major TCP/IP-related enhancements provided by Windows NT Server.
  - **DHCP Server service** - The Dynamic Host Configuration Protocol (DHCP) is a client/server-based

system that allows dynamic assignment of IP addresses and configuration information from a centralized server.

  - **WINS Server service** - The Windows Internet Naming Service (WINS) provides dynamic NetBIOS name registration and resolution on a TCP/IP network. It is often configured to work hand in hand with the DHCP service.
  - **DNS Server service**: The Domain Name System (DNS) is a standard TCP/IP service that provides static name resolution on a TCP/IP network.

- One major difference between Windows NT Server and NT Workstation is very fast Internet server that is at the foundation of Microsoft's Internet strategy. It supports the hypertext transport protocol (HTTP), which is the fundamental transport protocol of the World Wide Web, as well as support for FTP and gopher services.
- Although the RAS client in NT Workstation and NT Server are virtually identical, the RAS server service of NT Server can support upto 256 connections against one connection in NT Workstation. NT Server also provides support for third party security products.
- NT Server also includes two main Novel-related utilities : Gateway Service for Netware and Netware Migration tool.
- NT Server can to act as a domain controller where as NT workstation can't. This is one of the most differentiating feature between the two product.
- Windows NT 4.0 now includes the Microsoft Network Monitor Tool, which enables you to directly view network traffic as it passes across the network wire.

DOMAIN MODELS

A Windows NT Domain is a logical group of networked computers in which one or more of the computers have one or more shared resources, such as a shared folder or a shared printer. Common central domain directory database which contains user account and security information control access to the resources.

When a client logs on to Windows NT, he or she isn't actually logging on to a server but to a domain. The creation of a domain means that you, as an administrator, can configure and administer a logical grouping of servers. The domain gives Administrators a single point of administrating user accounts, hard drives (known as shares), and network printers. Whatever security you implement today on a single server will also apply to a new server that tries to be a part of this existing domain. A domain can include clients and servers. A server can play any of the three under mentioned roles: -

- Primary Domain Controller (PDC)
- Backup Domain Controller (BDC)
- Stand-alone server

A stand-alone server may or may not be a part of a Windows NT Domain, but is the only option that can be part of a workgroup.

On an average a single domain might contain a Primary Domain Controller and one or more Backup Domain Controllers. The Primary Domain Controlleris the host for the user account database and the logon scripts. The Backup Domain Controller replicates the data on the Primary Domain Controller and it can be promoted to the Primary Domain Controller if there is any problem in the actual Primary Domain Controller thus preventing the entire network from crashing even when the server (primary domain controller) has gone down. The clients in a domain can be running Windows NT Workstation, Windows for Workgroups, Windows 3.x, MS-DOS, Windows 95, Apple, and OS/2.

One distinct advantage of using a domain (or domain model, as it is sometimes called), particularly on a large network, is that administration and security for the entire network can be managed from a centralized location.

In a Windows NT domain, at least one of the networked computers is a server computer that runs Windows NT Server. The server computer is configured as a Primary Domain Controller (PDC), which maintains the domain directory database. Typically, there is at least one additional server computer that also runs Windows NT Server. This additional computer is usually configured as a Backup Domain Controller (BDC). The other computers on the network normally run Windows NT Workstation or Windows 95 (although they may utilize other operating systems). These non-server computers can share their resources (such as hard disks and printers) on the network, but these shared resources are secured by the domain directory database that is maintained by the PDC.

WORKGROUPS

A workgroup is a logical grouping of networked computers in which one or more of the computers has one or more shared resources, such as a shared folder or a shared printer. In a workgroup environment, the security and user accounts are all maintained individually at each separate computer. Resources and administration are distributed throughout the computers that make up the workgroup. In a workgroup configuration there is no centrally maintained user accounts database, nor any centralized security.

Typically, all of the computers in a workgroup run desktop operating systems, such as Windows 95 or Windows NT Workstation.

The basic difference between Domain and workgroup is that in domain each account validated by PDC. In workgroup each server resource is accessible only for the accounts in that server. For example a workgroup may contain ten servers, each should have all user account to access the resources of that server only.

Workgroup computing is a good alternative for a small number of computers that do not want to utilize centralized administration, but do want to include a computer running Microsoft Windows NT Server because of some of the services that an NT server can offer, such as Dynamic Host Configuration Protocol (DHCP), or Remote Access Services (RAS).

MULTIPLE DOMAINS

The single domain allows for central administration of user accounts and resources, such as disk drives and printers. But what if the company has offices in different locations, or if different departments would prefer to administer their own users or resources. Thus we move on to the multi-domain environment. Before two serves of two different domains are brought together, a trust relationship is to be set between them. A trust is an agreement between two domains. One of the Domains in the trust relationships is known as the trustee and the other is known as the trusted domain. The relationship is maintained by giving the trusting domain an access to the trusted domains user account database. This arrangement eradicates the necessity of creating the same user in more than one domain, which in turn makes the administration of user accounts easier.

SECURITY STRUCTURE OF WINDOWS NT

Microsoft Windows NT Server security structure is based on permissions; these give users the right to access a resource and specify the way in which the users can access the resource. Each Windows NT computer contains a security accounts database, known as the SAM. On computers running Windows NT Workstation, the SAM contains security information specific to that computer. On a Microsoft Windows NT Server Domain Controller computer, the SAM contains security information about the local machine and the entire domain.

USER ACCOUNT

In a domain, there exist different user and every user account has a unique ID called the security ID (SID). With the help of SID, NT tracks permissions. These permissions are placed in an Access Control List (ACL). At the time of logon, each user is assigned a security access token, which includes the user's SID and information on group memberships and the associated SIDs for those groups. The security access token is created by Windows NT, and a copy is passed to whatever process the user requests to access.

The external identification used for client to logon in Windows NT is termed as User Account. Every User Account is associated with an internal SID, which is never seen by user or administrator. When a user account is deleted from a domain, the SID associated with that account is never reused. Even if the same user name is used with a new account, a new SID is generated.

The User Account includes information about the client, such as the user name (the ID used for logging onto a Windows NT network); permissions; and, among other administrative items, rules, which are known as profiles.

GROUPS

NT Server domain groups contains multiple user accounts grouped logically. When a group containing the user account is assigned some permission, all the user account contained in the group are assigned those permission. Each group has a SID associated with it, and that SID is included in a user's security access token.

NT server domain groups can be divided into two parts :

- Local Groups
- Global groups

When a single domain NT network groups user accounts to assign permission, it is called local group. When you define a group of user accounts that then can be added to local groups that exist in other domain. it is called a global group.

DOMAIN

As mentioned earlier, a Microsoft Windows NT Server domain consists of one or more servers and clients. A Windows NT network can include more than one domain. To administrate more than one domain from the Server Manager applet, however, the Administrator must have an account on all the domains he or she needs to administer.

TRUST RELATIONSHIPS

To allow one domain to access resources on another domain, you must establish a trust relationship. Trust relationships also can allow for centralized administration of networks that go beyond a single domain.

EXERCISE

Fill in the Blanks :

1. NT Operating System has two modes _______ and _______.
2. NT _________ can to act as a domain controller where as NT ________ can't. (Server/Workstation)
3. The two type of file system NT supports are:
4. User Mode has ________ subsystems.
5. The entire set of services that comprise Kernel Mode is called _________________.
6. In kernal mode, microkernal communicates with the hardware through _______________.

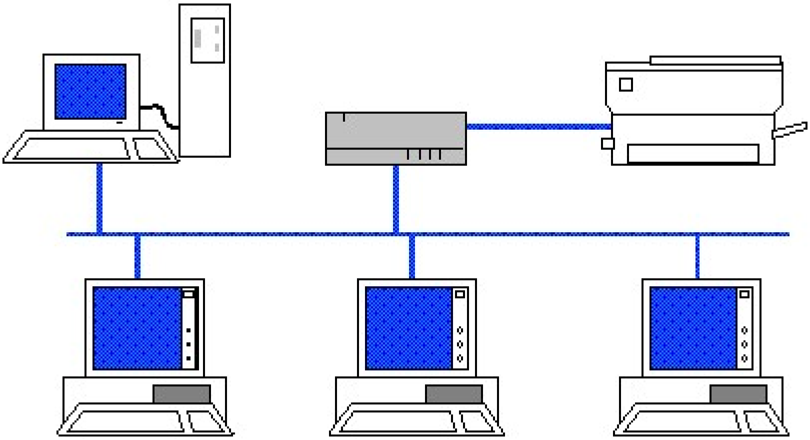
Answer the following questions:

1. Discuss the main feature of Windows NT operating System.
2. What do you understand by client-server?
3. What is the difference between NT Server & NT Workstation?
4. What are two modes of NT operating Syatem and what role they play?
5. What is the basic difference between a PDC and BDC?
6. Discuss the advantages of using the Domain model.
7. Discuss the three protected environment subsystem.
8. Discuss the various kernal mode components.
9. What is the base of security system in NT ?
10. Explain the following
    a) POSIX
    b) DHCP
    c) VLL
    d) LPC
    e) SRM
    f) HAL

CHAPTER 3

Windows NT Installation

WINDOWS NT INSTALLATION
Information Required to Install Windows NT
File System
Licensing Model
Domain Role
Protocols
Services
Installing NT Server



WINDOWS NT INSTALLATION

Hardware plays an important role in a system running on Windows NT. The system should be error free as far as hardware part is concerned as NT is very sensitive to Hardware. Hardware must be tested thoroughly before installing NT. That is why Microsoft publishes Windows NT hardware compatibility list (HCL). The HCL provides a list of hardware compatible with Windows NT. This list is constantly updated and the latest versions of the list are available on the Internet at the Microsoft site.

Adequate hard drive space is also a concern when setting up a Microsoft Windows NT Server. When you are planning your server, you must think about the hard drive space required for these items:

- The Microsoft Windows NT Server operating system
- The individual users' home directories
- Application software
- Implementation of fault tolerance
- Additional operating systems
- Virtual memory

Early in the history of Microsoft Windows NT Server (when it was called Advanced Server), hard drives were still quite expensive. Now, however, allotting a 4GB partition of your hard drive to a server is a fairly reasonable and cost-effective upgrade.

Following table shows the minimum hardware required for installing Windows NT Workstation and Windows NT Server. The requirements listed apply only to Intel-based platforms. Windows NT can also be installed on DEC Alpha AXP, PowerPC, and MIPS platforms, but additional hardware may be necessary, depending on the type of processor you plan to use.

Hardware Component	**Windows NT Workstation**	**Windows NT Server**
Processor	486/33	486/33
Memory	16MB of RAM	16MB of RAM
Hard disk space	117MB	124MB
Display	VGA or better	VGA or better
Floppy disk drive	3.5-inch high -density	3.5-inch high-density
CD-ROM drive	Required (If your computer does not have a CD-ROM drive, you can still install NT Server using an over-the-network installation)	
Network adapter	Optional (Required for over-the-network installation)	
Mouse	Optional	Optional

Because Microsoft Windows NT Server is shipped on CD-ROM, an NT-compatible CD-ROM drive is required for the server. Although there are workarounds to installing Microsoft Windows NT Server on a server without a CD-ROM drive, it is highly advisable to have this drive available because most applications for Microsoft Windows NT Server ship on CD-ROM as well.

INFORMATION REQUIRED TO INSTALL WINDOWS NT

A substantial amount of user input is required during the Windows NT installation process. To make the installation go smoother and to avoid the possibility of having to redo it, you should gather all the information you will need before doing the installation. This will enable you to give the appropriate responses as you are prompted by the Windows NT installation program.

Before you install Windows NT Server on your computer, you must be clear about the five key areas of installation :

- File system
- Licensing mode
- Role in the domain
- Protocol(s) to activate
- Services

These five areas has a major impact on the performance of your NT server.

FILE SYSTEM

There are basically two types of file system : FAT (File Allocation Table) and NTFS (Windows NT File System). Both have their own characteristics which make them desirable. These characteristics are:

Windows NT File System (NTFS)

NTFS is incompatible with MS-DOS, and Windows 95/98. If you plan to load an additional OS and dual boot with Windows NT, you will not be able to read the information on the NTFS partition. NTFS provides directory-level and file-level security.

File Allocation Table (FAT)

FAT is compatible with all Microsoft operating systems and gives slightly better performance than NTFS, depending on the size of the partition. FAT has no directory-level or file-level permission capability. With FAT, two or more operating systems can access the data on the partition.

Both NTFS and FAT support long file names. If your server is a dedicated Windows NT Server, then NTFS should be your choice for data storage. It’s a safe practice to create a small (300M) boot partition, which should be formatted with the FAT file system. If the operating system fails to boot, you can still access your boot file via MS-DOS.

LICENSING MODEL

Microsoft Windows NT Server, has two schemes under which it can be licensed - per server or per client. Again both have their own advantages and disadvantages:

Per server

In this scheme, the client access license resides on the Windows NT Server. This scheme is best utilized with a single Windows NT Server that multiple clients access. This manner of licensing can be changed/upgraded to the per client scheme.

Per client

In this scheme, the client access license resides on the client. This manner of licensing is useful when a client accesses multiple Windows NT Servers. You cannot change the licensing model from per client to per server.

DOMAIN ROLE

A Windows NT Server-based network can be implemented in two models: the domain model or the workgroup model. If the workgroup model is followed, no domain-specific options are available; the server is installed as a stand-alone server, similar to the third option in the following list (member server).

In domain model, a Windows NT server can play three different roles. These are:

Primary domain controller (PDC)

The first machine must be set up as a PDC, if you are setting a domain model in Windows NT. A PDC is responsible for validating log-ons and retaining user information and includes a unique security identifier.

Backup domain controller (BDC)

The BDC is used to off-load some of the PDC activity. The BDC obtains a copy of the accounts database from the PDC, which is updated with information at scheduled intervals. If a PDC goes off-line for any reason, a BDC can be promoted to the role of PDC until the original PDC can be brought back on-line.

Member server

Also known as a stand-alone server, a member server does not carry the overhead associated with the domain controllers. A member server is generally dedicated to an intensive application or database like Microsoft SQL Server.

Domains Versus Workgroups

An alternative to defining a domain is using a function of Microsoft networking, which is known as workgroups.

Any computer that is running the Microsoft networking client software, but is not defined as part of a domain is automatically part of a workgroup. If you implement an NT server as a Stand-Alone Server, it is then part of a workgroup.

A workgroup can include one or more computers. Computers that do not participate in a domain, and are therefore part of a workgroup and are responsible for their own security and administration.

Implementing Domains

When planning a Microsoft Windows NT Server domain, you can choose from four domain structures:

Single domain model

Places one or more Microsoft Windows NT Servers into one domain. Here all user accounts and all resources are within the same domain and there is no need to set up trust relationships. Also all the administrative tasks can be handled in one place.

Master domain model

If you do not require breaking up clients into separate domains, and you want to administer all the user accounts from one domain, you can use this model. Here multiple domains are created but these created domains do not have any user accounts. Instead they work as resource domain and offer users in the master domain access to disk space, applications, printers, or any other type of shared resource. Usually implemented in multiple departments having their own resources, but each department is administered through master domain.

Multiple master domain model

This choice provides more than one account domain and one or more resource domains. Here administration of different groups of user account is independent of each other but trust between resource domain and account domain can allow the user account to share the resources.

Complete trust domain model

This choice has multiple domains that all trust each other. Like the multiple master domain model, administration of the user accounts is broken up into different domains. The complete trust, which implies that each domain trusts all the other domains, shares its resources.

PROTOCOLS

You need proper protocol to let your Windows NT server work properly with other members of the network. Windows NT loads TCP/IP and IPX/SPX by default. Another widely used protocol is NetBEUI. You muse install one of these three protocol to enable network clients to access file and print services as only these protocol can be used by Windows NT to transfer Server Message Blocks (SMB) traffic.

NetBIOS Extended User Interface (NetBEUI)

Typically used in small LAN implementations of 50 nodes or less, NetBEUI is a non-routeable protocol, impractical for larger installations. It supports NetBIOS connectivity.

IPX/SPX compatible protocol

This is Microsoft's implementation of Novell's IPX/SPX (Internetwork Packet Exchange/Sequenced Packet Exchange) protocol. This protocol is routable and can accommodate a larger LAN than NetBEUI while still supporting NetBIOS connectivity.

Transfer Control Protocol/Internet Protocol (TCP/IP)

This is quickly becoming the most popular protocol, providing connectivity to the Internet and is used mostly in large LAN/MAN/WAN implementations. Provides connectivity to UNIX and mainframe boxes running TCP/IP. Windows NT offers additional tools that help manage an IP network. Dynamic Host Configuration Protocol (DHCP) is used to dynamically assign IP addresses to clients.

Data Link Protocol (DLC)

This is widely used for IBM mainframe connectivity. Another use of DLC is network connection to Hewlett Packard network printers.

Point-to-Point Tunneling Protocol (PPTP)

Provides a secure connection over the Internet. This protocol enables private virtual networks to exist over the Internet.

Streams

These provides specific connectivity with UNIX machines. Adds porting protocols to the Windows NT environment.

SERVICES

Services are the executable programs that run as background tasks on Windows NT. Services provide additional functionality to Windows

NT. There are a minimum of five services loaded when Windows NT is installed:

Computer Browser

Enables the server to maintain a list of resources in the domain.

Network Basic Input/Output System (NetBIOS)

Interface Provides support for the machine-naming convention used by Microsoft networking products.

Remote Procedure Call (RPC)

Configuration Services remote procedure calls made to the server from clients requesting resources.

Server

Makes resources available to client requests.

Workstation

Opposite the request for resources is the client. If this service is not functioning, requesting resources will not be possible.

Beside these services, additional services can be loaded depending on the environment.

INSTALLING NT SERVER

Once you have decided about the five key area noted above, you are ready to install the NT server on the computer. Before installation, it is necessary to boot the system to start the process. There are three methods of doing that.

- Boot from the three floppies that come along with the CD-ROM and Windows NT starts installing itself from there.
- You can also boot from the existing OS and CD-driver. Now insert the Windows NT Server installation CD-ROM in CD-drive and type **WINNT/B** on the CD-drive.

  The proper syntax for the WINNT.EXE command follows:

  WINNT [/S[:]sourcepath] [/T[:]tempdrive] [/I[:]inffile] [/O[X]] [/X |[F][/C]] [/B]

/B	Specifies floppyless operation.
/C	Skips the free-space check on the Setup boot floppy disks you provide.
/F	Does not verify files as they are copied to the Setup boot floppy disks.
/O	Creates boot floppy disks only.
/OX	Creates boot floppy disks for CD-ROM or floppy-disk-based installation.

/X Does not create the Setup boot floppy disks.

- You may also be presented with a Windows NT dialog box as shown in Fig 3.1. Select the Windows NT Setup option to start loading Windows NT.

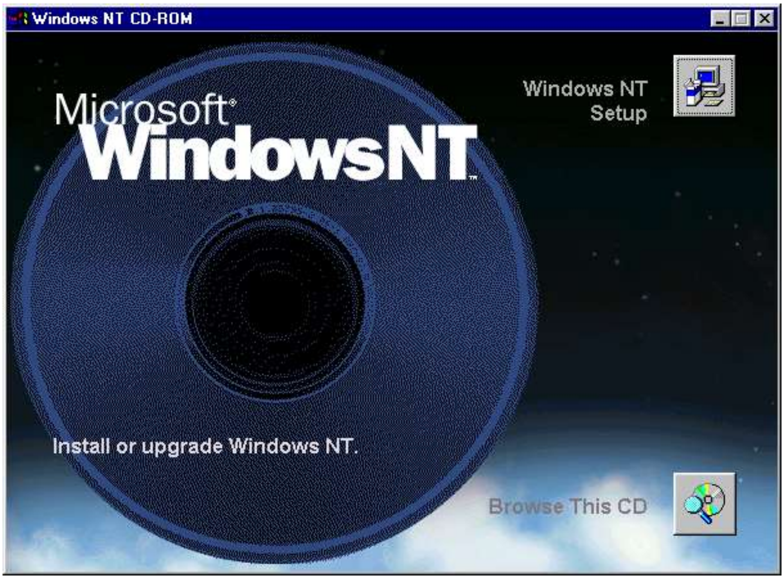


Fig 3.1 Windows NT Setup dialog box

- You can also boot directly from CD-ROM. For this you require a bootable CD-ROM. Select the CD-ROM boot option from CD-ROM.

Once you boot the system in one of the above fashion, the installation of Windows NT starts. The installation can be divided into two parts - text phase installation and GUI installation.

In text phase installation, you see the screen displaying messages in the character mode. Press the required key at each screen as per the instructions on the screen.

1. The first screen is welcome screen displaying the option of either installing a new version of Windows NT or repair an existing installation.

   Microsoft (R) Windows NT (TM) version 4.0 (Build 13.0)

   1 System Processor [64 MB Memory] Multiprocessor Kernal

   The next screen gives you the following choices on how to proceed with your installation:

   - You can get more information about the Microsoft Windows NT Server installation process by pressing the F1 key.

- You can proceed with the installation by pressing Enter.
- You can repair a previously installed copy of Microsoft Windows NT Server that may have been damaged.
- You can quit the installation process and restart the server.

2. Now NT detects the storage devices where NT can be installed. If there are additional devices that has not been detected by NT, you can add them manually at this point.
3. Now NT presents a license agreement screen, which you must read. Press PgDn to view the complete agreement. When you reach the bottom of the agreement, F8 key is activated, which you can press to accept the agreement.
4. Now NT detects the previous installed version, if any. If there exist any previous version, you can choose to upgrade the previous version or install new version in a different directory.
5. Now NT detects the computer hardware and software components, which you can change, if they don't match with your actual components. To change, highlight a component and press Enter.

   - **Computer type:** This refers to the type of architecture your PC uses, such as MPS Multiprocessor, IBM PS/2, Standard PC, and so on.
   - **Display:** This refers to the video display adapter in your computer. This component setting defaults to Auto Detect. You can change this setting at the end of Phase 3 of the installation process.
   - **Keyboard:** This component's default is a single setting that includes XT, AT, or Enhanced Keyboard (83-104 keys). You can change this setting if you have a different keyboard and the appropriate drivers for it.
   - **Keyboard layout:** This setting defaults to U.S. Change this setting if necessary to support your keyboard layout correctly.
   - **Pointing device:** Setup should automatically detect your pointing device. You can change the setting by selecting another pointing device from the list, or you can supply your own driver from a diskette.

   After making modification, select the option '**The above list match my computer**" at the bottom of the list to bring the next screen.
6. NT identifies free disk space and partitions available on the disk. You can install NT on existing partition or create a new partition.

7. If you create a new partition to install NT, you can format it in FAT or NTFS. If you are using existing partition, you can use the existing file system or convert the system into NTFS.

8. Now select the location, where NT is to be installed. Default location is WINNT folder. It displays the message.

   "To change the suggested location, press backspace key to delete characters and then type the dir where you want WINNT installed."

9. Now Windows NT starts installation. The progress bar indicates the percentage completed. Once all the files are copied, the NT reboots the system.

10. On rebooting, the Graphical User Interface portion of Setup begins. Here click on the next button to continue to the next screen.

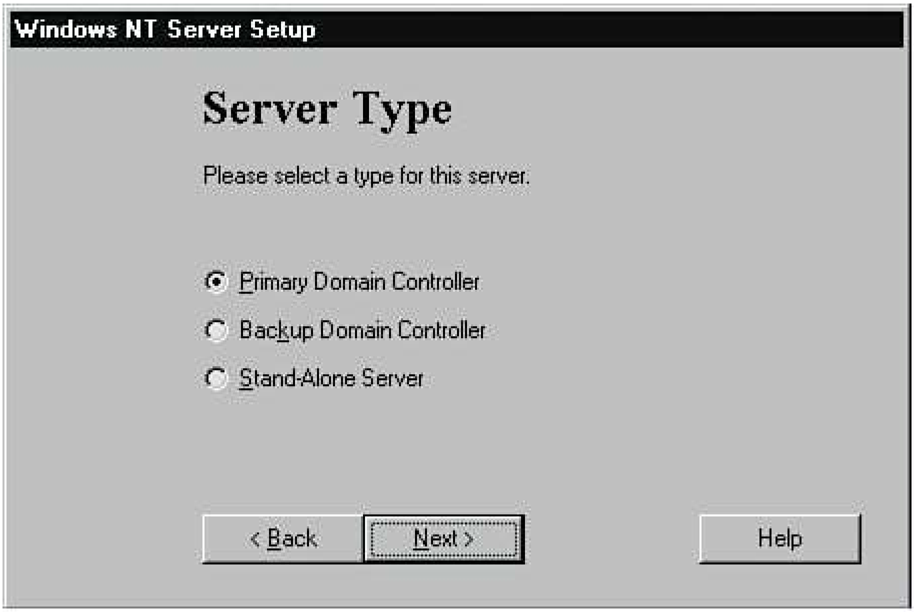
    a) Input the name and organization.

    b) Input the CD-key.

    c) Select licensing Model - per server or per client.

    d) Identify your computer in less than 15 characters.

    e) Select the role machine has to play - network domain controller or stand-alone server.



Windows NT Server Setup

Server Type

Please select a type for this server.

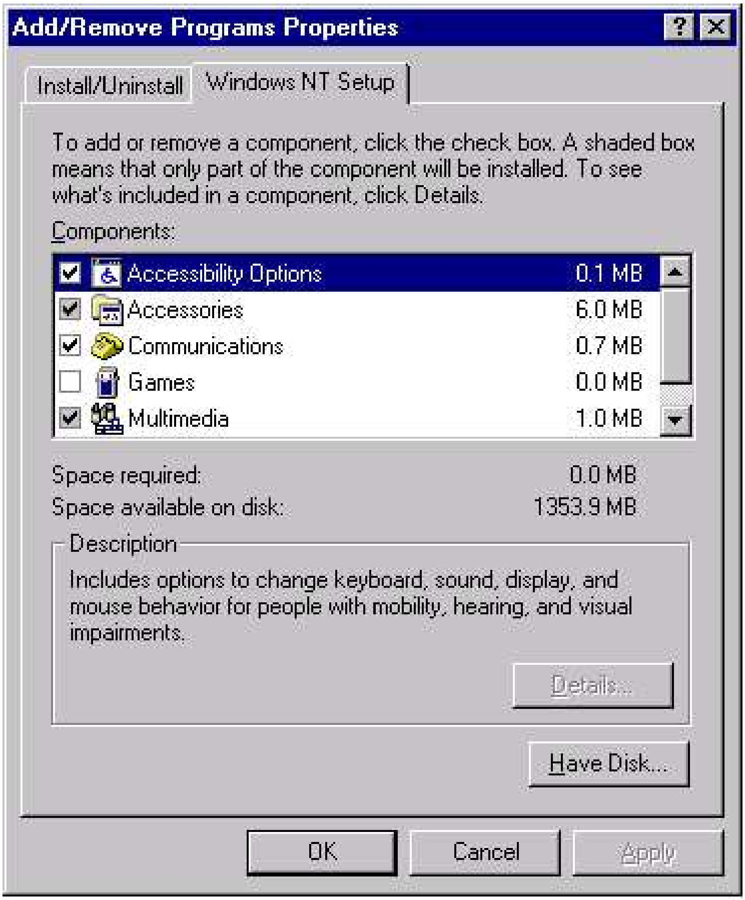
● Primary Domain Controller
○ Backup Domain Controller
○ Stand-Alone Server

Fig 3.2 Selecting the role of the Server

    f) Define the password for default administrator account in 14 or less character.

11. You can create ERD (Emergency Rescue Disk) now. This disk reflect the current state of system. You can skip ERD creation at this moment and create it later by running RDISK.EXE.

12. Now setup present you with the option to install various components including screen savers, games etc. as shown in Fig 3.3. Select the appropriate applications and click OK.



To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Components:

☑	Accessibility Options	0.1 MB
☑	Accessories	6.0 MB
☑	Communications	0.7 MB
□	Games	0.0 MB
☑	Multimedia	1.0 MB

Space required: 0.0 MB

Space available on disk: 1353.9 MB

Description

Includes options to change keyboard, sound, display, and mouse behavior for people with mobility, hearing, and visual impairments.

Fig 3.3 Adding Applications

13. As the installation proceeds, it ask you following option

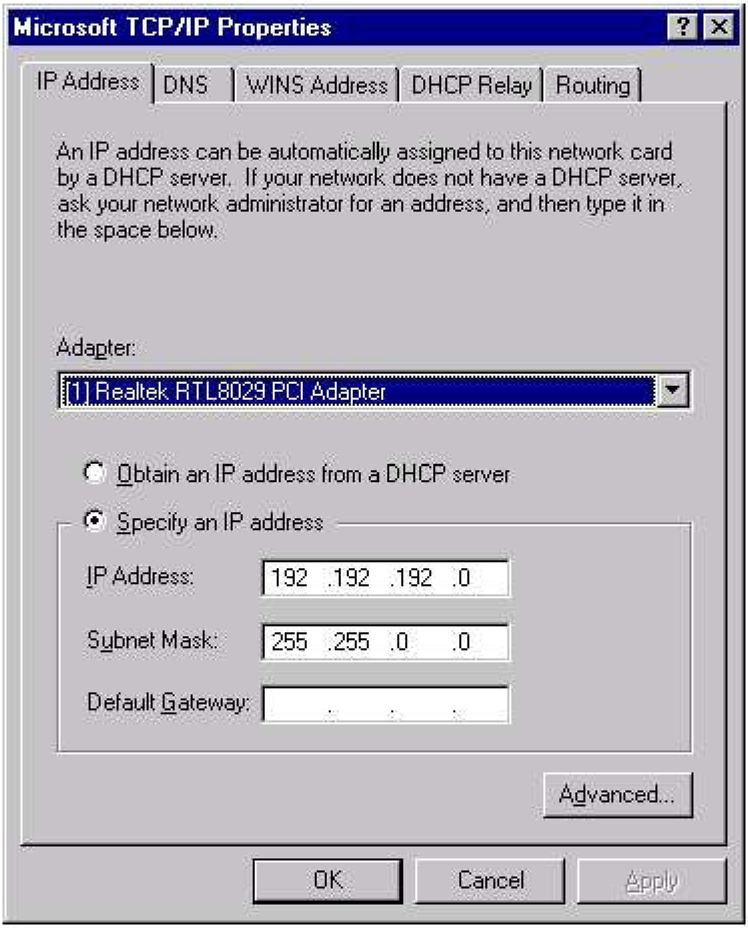
Is this machine physically attached to the network by a network adapter or will it connect over a modem to the network?

Select the appropriate option.

14. Now Windows NT searches for any adapters installed in the machine. If an adapter is not detected, you can select from a list or install from the manufacturer-provided media. Select one or more protocols. TCP/IP and IPX/SPX are selected by default.

15. Click Next to install all the selected components.

16. If you are installing NT Server, don't use DHCP (Dynamic Host Configuration Protocol). Instead select an IP address for the Server. To configure a static IP address, you must enter the IP address and subnet mask, as shown in Fig 3.4. If you wish to access IP resources outside of your local subnet, a default gateway must be entered.



An IP address can be automatically assigned to this network card by a DHCP server. If your network does not have a DHCP server, ask your network administrator for an address, and then type it in the space below.

Adapter:
[1] Realtek RTL8029 PCI Adapter

○ Obtain an IP address from a DHCP server
● Specify an IP address

IP Address: 192 .192 .192 .0
Subnet Mask: 255 .255 .0 .0
Default Gateway: . . .

Fig 3.4 Configuring static IP Address

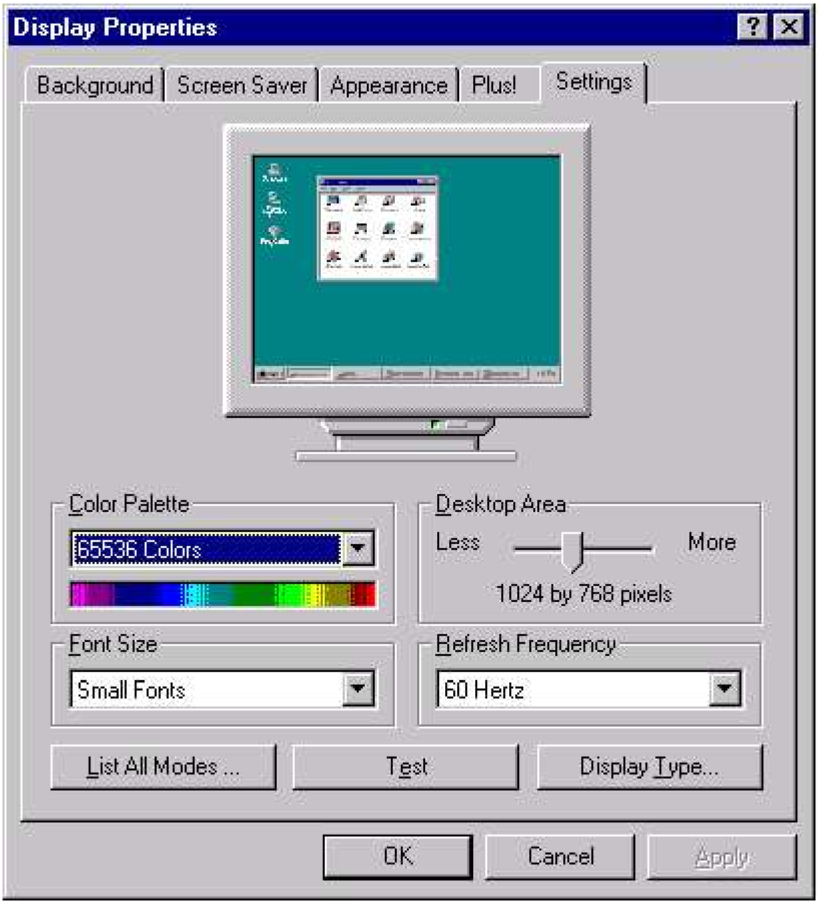
17. The host name and domain must be entered to do DNS resolution. You can enter one or more IP addresses of DNS servers. The host name should be identical to the NetBIOS name for simplicity sake.

18. If you are using WINS for NetBIOS name resolution, you must enter the IP of a WINS server.

19. Now you are provided with several options to install Internet Information Server (IIS). Create a directory to hold your information regarding IIS.

20. Now after setting all these configuration setting, you are presented with Date/time dialog box. Select the appropriate zone for your country.

21. After setting this, NT detects the video card and installs driver for the same. At this point, select the color depth and resolution, as shown in Fig 3.5. You're required to test the configuration before proceeding with the setup.



Display Properties

Color Palette: 65536 Colors

Desktop Area: Less — More; 1024 by 768 pixels

Font Size: Small Fonts

Refresh Frequency: 60 Hertz

Fig 3.5 Setting Display Properties

22. Windows NT saves the configuration to the Registry. The machine reboots into the Windows NT Server OS.

EXERCISE

State True or False :

1. NTFS supports long file names where as FAT doesn't support
2. A workgroup can include one or more computers.
3. Dynamic Host Configuration Protocol (DHCP) is used to dynamically assign IP addresses to clients.
4. Windows NT can be installed only on NTFS partition.
5. Emergency Repair Disk can't be created after installation.

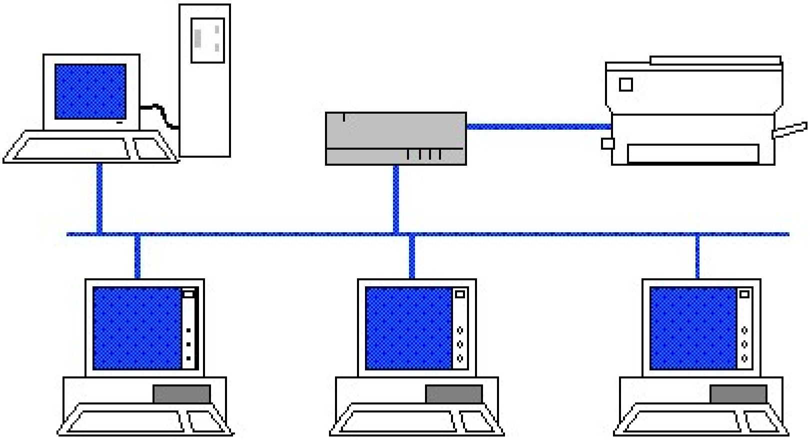
Answer the following questions:

1. What are the key areas you must decide, before installing the NT Server?
2. Can you install Windows NT on system running on Windows 95. If yes, how?
3. What are the two types of file system NT supports?
4. Differnetiate between
   a) Single Domain Model & Master Domain Model
   b) PDC & BDC
5. Discuss the various protocol that NT supports.

CHAPTER 4

Starting Windows NT

THE WINDOWS NT SCREEN
DESKTOP
ICONS
TASKBAR
USING NT HELP
SHUTTING DOWN WINDOWS NT



THE WINDOWS NT SCREEN

Windows NT uses windows to display information on your screen, and icons to provide pictorial buttons for you to click. Windows 95/98, Windows NT Workstation 4, and Windows NT Server 4, all share the same look and feel. Windows NT has a Taskbar, a start menu beside various other applications. All of these objects appear on the Windows NT desktop - your screen.

DESKTOP

Windows NT uses your screen as a desktop, a work area on which you see your programs. The desktop can contain windows, icons, and the Taskbar. You can think of the icons and windows that appear on your screen as “sitting” on your desktop.

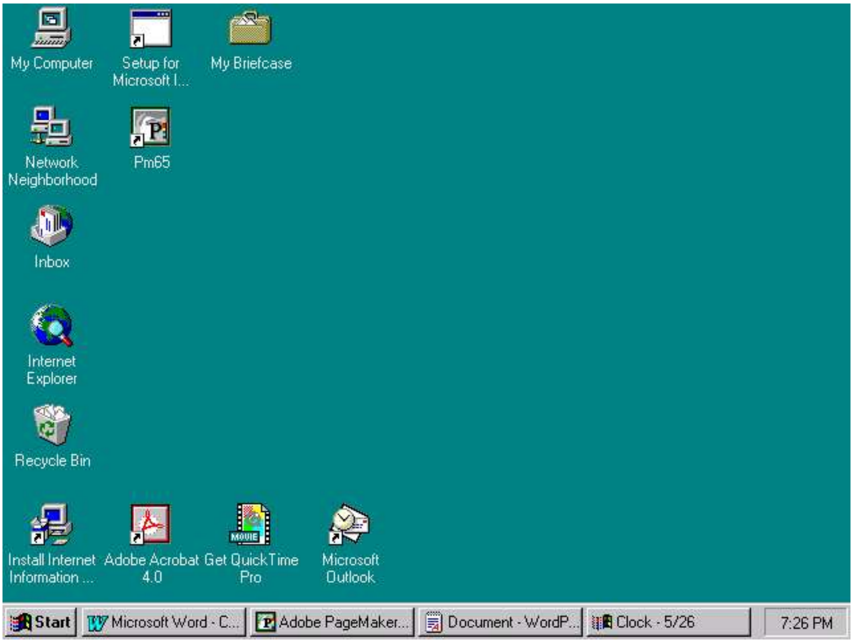


Fig 4.1 Windows NT Screen

THE ACTIVE DESKTOP

The Active Desktop in Windows NT integrates the Windows desktop with the Internet Explorer browsing software to provide a single metaphor for accessing content or applications, whether on a local computer, a corporate intranet, or the World Wide Web (WWW). The Active Desktop makes it easier for users to access favorite applications, files, folders, and Web sites. It also lets network and workgroup administrators create customized Active Desktop configurations specific to the needs of individuals or workgroups. Using the Active Desktop, you can, customize the Start, Programs, and Favorites menus.

ICONS

Icon represent programs in graphical forms such as (the Internet, Word for Windows, Excel, and so on), folders, files, printer information computer information and so on, in both Windows NT and programs designed to run under Windows. Icons on your desktop that include a little back arrow in a little white box in the lower-left corner of the icon are shortcuts, and represent files or programs on your computer.

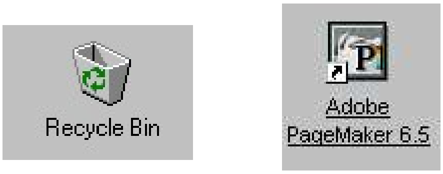


Fig. 4.2 Various icons

TASKBAR

The Taskbar is a row of buttons and icons that usually appears along the bottom of the screen. It’s consist of Start Button and Current time. One of the Taskbar's primary jobs is to display buttons indicating which applications are currently running.

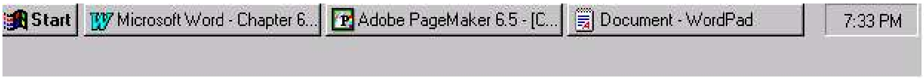


Fig. 4.3 Windows taskbar

THE START BUTTON

It is usually at the left end of the Taskbar. When you click the Start button on the Taskbar, the Start menu appears. The Start menu lists commands and additional menus that list most or all the programs that you can run on your computer.

Using Start menu, you can perform almost any action such as launching an application, finding files, obtaining Help, changing system settings, accessing recently-used documents, and even logging off or shutting the server down. As you move your mouse pointer up and down over the Start menu's options, a highlight bar will appear and travel right along with your mouse pointer's movement until it moves off of the Start menu. (Fig 4.4).

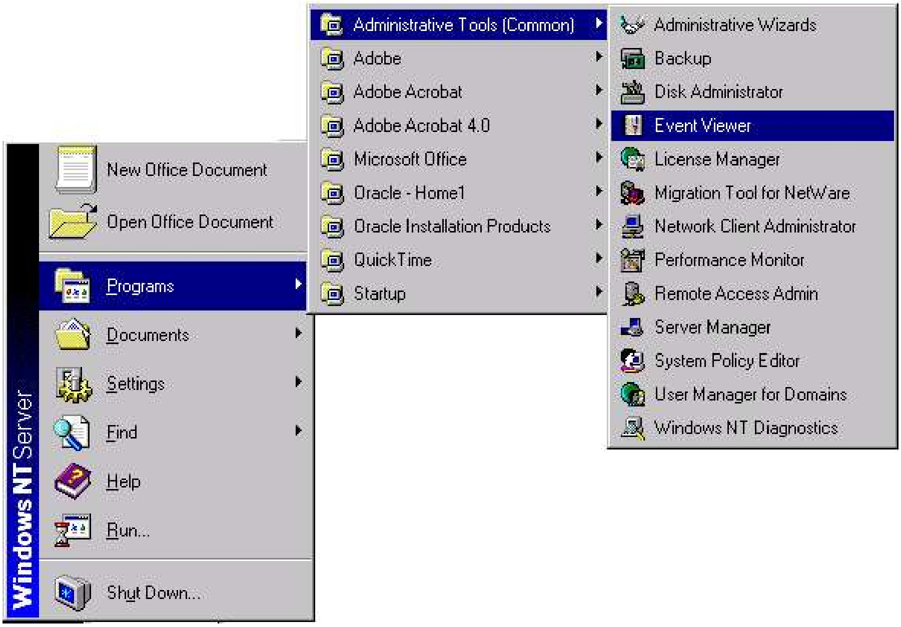


Fig. 4.4 Start menu

Running An application

To run a program, click one of the programs from the cascading submenu or position your mouse over one of the submenu items until you locate the program that you want to run. (See Fig 4.4)

Opening recently accessed Documents

Windows NT Server 4 gives you the ability to quickly retrieve recently worked-on documents such as word-processing files, spreadsheet files, even database files.

Settings

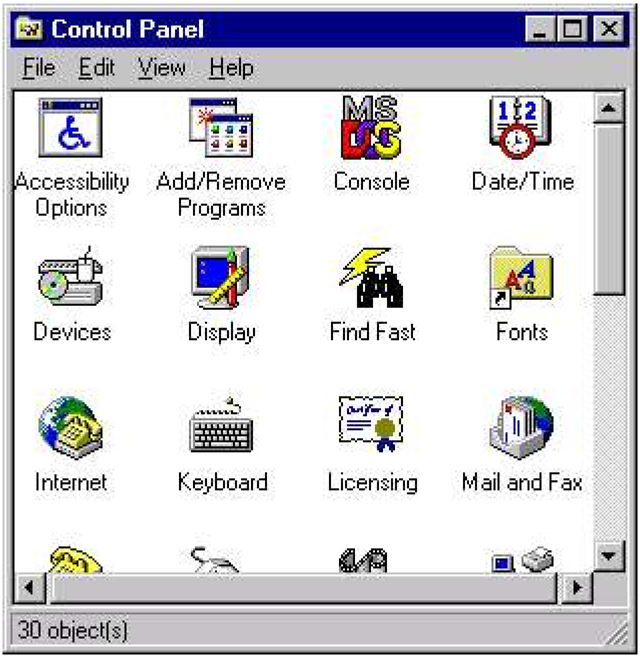
To change general settings, access the Control Panel from the Start menu, select the **Settings** option and then click **Control Panel**. (Fig 4.5) To add or remove a printer, select the **Printer option** from submenu of Settings.

Find

There are two new commands on this menu:

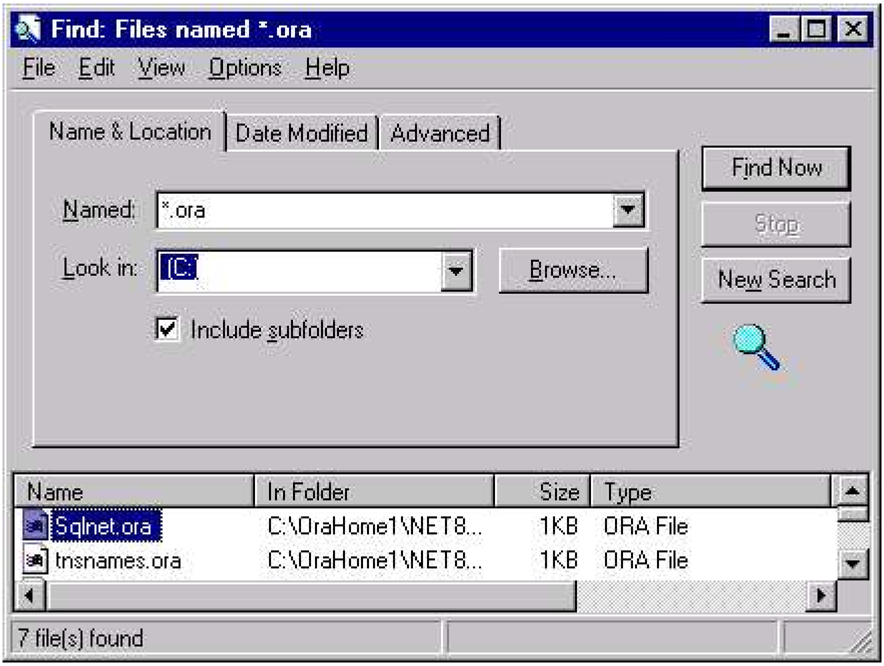
Files or Folder You can use this command to search the files or folders in your computer or in network. (Fig 4.6).

Computer Using this command, you can consult several directory services and address books in order to find an address.



30 object(s)

Fig 4.5 The Control Panel



Find: Files named *.ora

Named: *.ora

Look in: (C:)

☑ Include subfolders

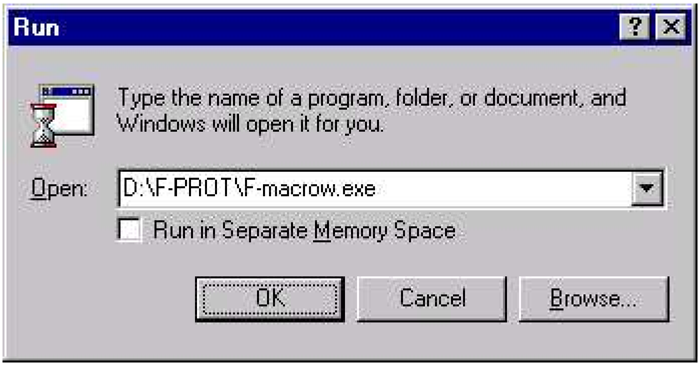
Name	In Folder	Size	Type
Sqlnet.ora	C:\OraHome1\NET8...	1KB	ORA File
tnsnames.ora	C:\OraHome1\NET8...	1KB	ORA File

7 file(s) found

Fig 4.6 Find dialog box

Running Applications

The Start menu's Run option enables you to execute applications as well as to open folders or documents that may not be listed on either the Start menu or as icons on the Desktop.



Type the name of a program, folder, or document, and Windows will open it for you.

Open: D:\F-PROT\F-macrow.exe

□ Run in Separate Memory Space

Fig 4.7 Run dialog box

Log Off

You can quickly log off and log on again as a different user.

SWITCHING AMONG APPLICATIONS

Taskbar shows a button for each program that is running. If a program displays more than one window, more than one button may appear. On each Task Manager button, Windows NT displays the icon for the program and as much of the program name as can fit.

Click a window's button to select that window, that is, make that window active. You can also right-click a button to see the system menu, a menu of commands you can give regarding that window, including opening and closing the window.

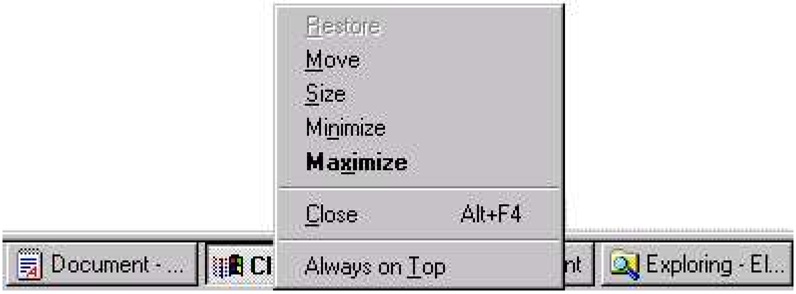
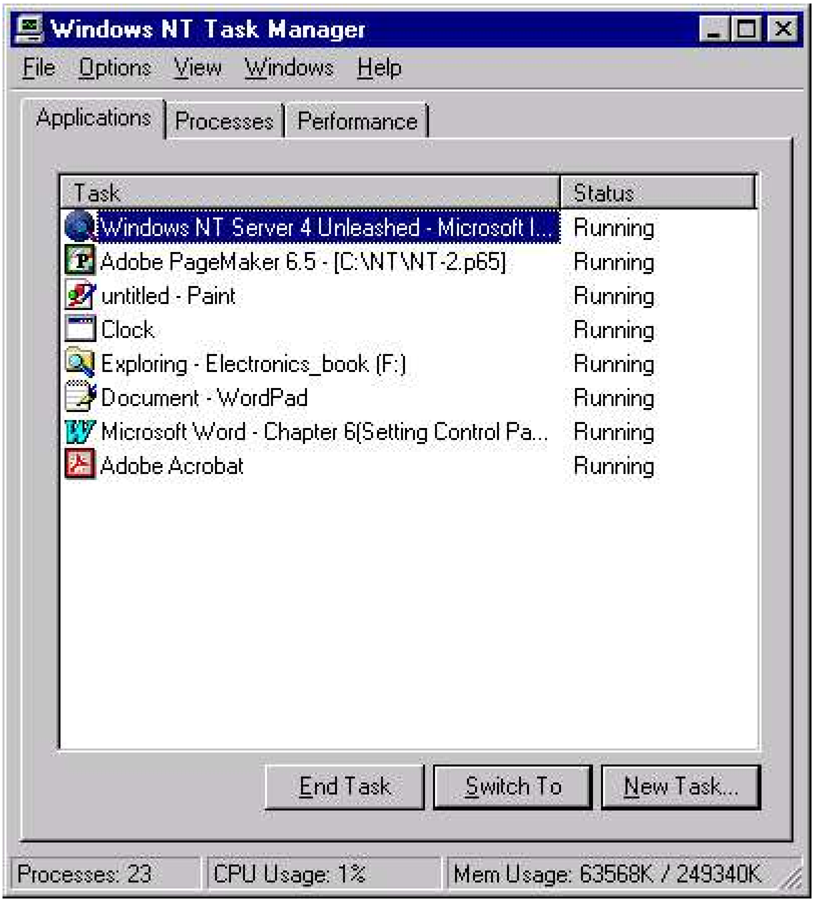


Fig 4.8 System menu

Task switching between programs can be done quite easily using the new Taskbar. Click your mouse on the Taskbar button of the application that you wish to switch to. The is the simple substitute of the keystroke combination of Alt+Tab to switch among between different programs.

WINDOWS NT TASK MANAGER

Windows NT Server now sports a highly informative Task Manager. To access this updated tool, right-click a blank area of the Taskbar, or, press **CTRL+ALT+DEL** on the keyboard to invoke the Windows NT Security dialog and select **Task Manager**.

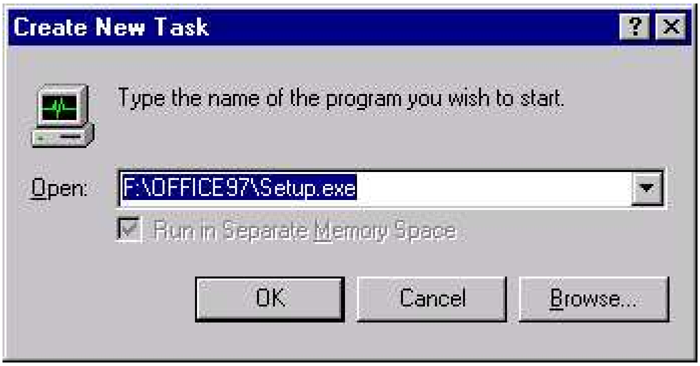


Task	Status
Windows NT Server 4 Unleashed - Microsoft I...	Running
Adobe PageMaker 6.5 - [C:\NT\NT-2.p65]	Running
untitled - Paint	Running
Clock	Running
Exploring - Electronics_book (F:)	Running
Document - WordPad	Running
Microsoft Word - Chapter 6(Setting Control Pa...	Running
Adobe Acrobat	Running

Processes: 23 CPU Usage: 1% Mem Usage: 63568K / 249340K

Fig 4.9 Windows NT Task Manager

When you first launch the Task Manager, you will see the Applications tab. From this tab of the Task Manager, you can view all of the tasks that are currently running on your Windows NT Server computer. If you select one of the tasks by clicking it, you then have the option of terminating that task by clicking the **End Task** button at the bottom of the window. You can also task switch to one of the running programs by clicking the program that you want to switch to and clicking the Switch To button. By clicking the **New Task** button, you can select to run an application from the Create New Task dialog which appears.



Type the name of the program you wish to start.

Open: F:\OFFICE97\Setup.exe

☑ Run in Separate Memory Space

Fig 4.10 Creating New Task

Click the **Processes tab** to see a listing of all of the operating system's processes that are presently running. You can select one of the processes by clicking it and if you then click the **End Process** button, the Windows NT Server will kill that process.

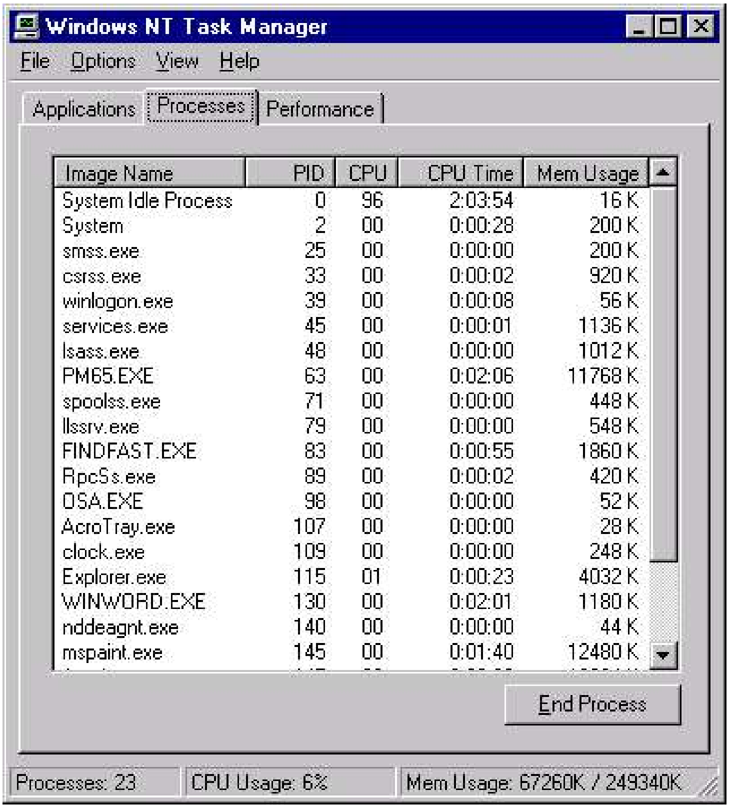
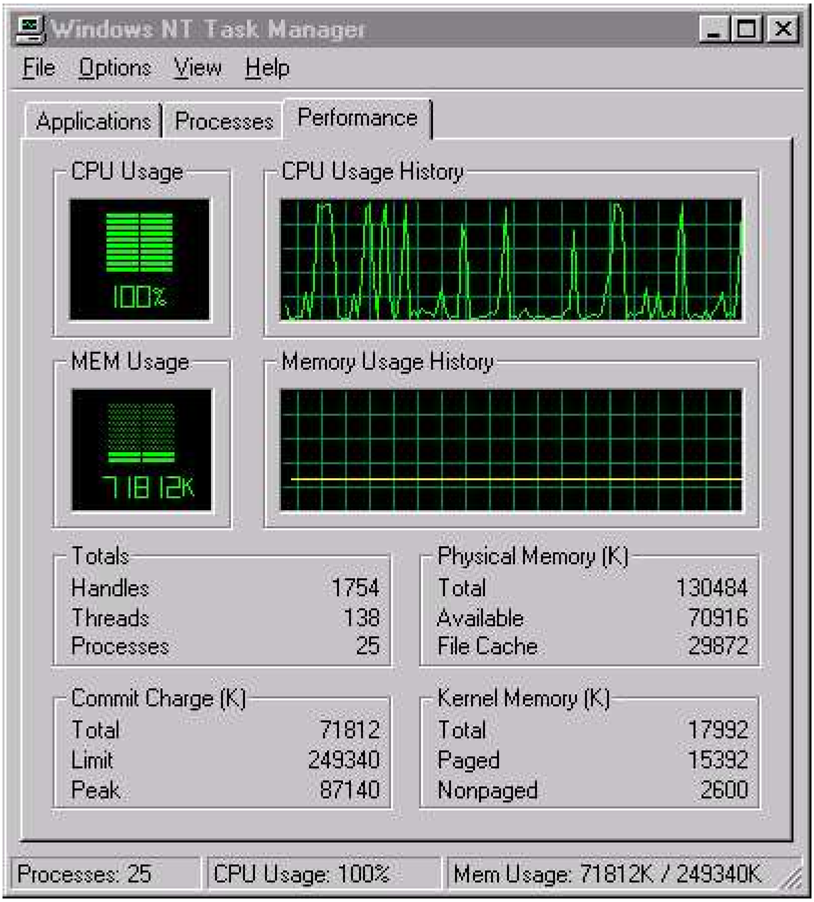


Image Name	PID	CPU	CPU Time	Mem Usage
System Idle Process	0	96	2:03:54	16 K
System	2	00	0:00:28	200 K
smss.exe	25	00	0:00:00	200 K
csrss.exe	33	00	0:00:02	920 K
winlogon.exe	39	00	0:00:08	56 K
services.exe	45	00	0:00:01	1136 K
lsass.exe	48	00	0:00:00	1012 K
PM65.EXE	63	00	0:02:06	11768 K
spoolss.exe	71	00	0:00:00	448 K
llssrv.exe	79	00	0:00:00	548 K
FINDFAST.EXE	83	00	0:00:55	1860 K
RpcSs.exe	89	00	0:00:02	420 K
OSA.EXE	98	00	0:00:00	52 K
AcroTray.exe	107	00	0:00:00	28 K
clock.exe	109	00	0:00:00	248 K
Explorer.exe	115	01	0:00:23	4032 K
WINWORD.EXE	130	00	0:02:01	1180 K
nddeagnt.exe	140	00	0:00:00	44 K
mspaint.exe	145	00	0:01:40	12480 K

Processes: 23 CPU Usage: 6% Mem Usage: 67260K / 249340K

Fig 4.11 Processes Tab of Task Manager

The Task Manager's third tab shows four graphical displays: CPU Usage, CPU Usage History, MEM Usage, and Memory Usage History. This window allows you to gauge your server's performance at a glance without invoking the Windows NT Performance Monitor.



Totals

Handles	1754
Threads	138
Processes	25

Physical Memory (K)

Total	130484
Available	70916
File Cache	29872

Commit Charge (K)

Total	71812
Limit	249340
Peak	87140

Kernel Memory (K)

Total	17992
Paged	15392
Nonpaged	2600

Processes: 25 CPU Usage: 100% Mem Usage: 71812K / 249340K

Fig 4.12 Performance Tab of Task Manager

SYSTEM CLOCK

The system clock shows the current time according to your computer's internal clock. When you move the mouse pointer to the clock, after a moment, the current date appears, too.

VARIOUS DEFAULT ICONS & FOLDERS

My Computer

The My Computer icon represents the contents of your computer, including the hard drive, floppy and CD drives, applications, folders, files, and so on.

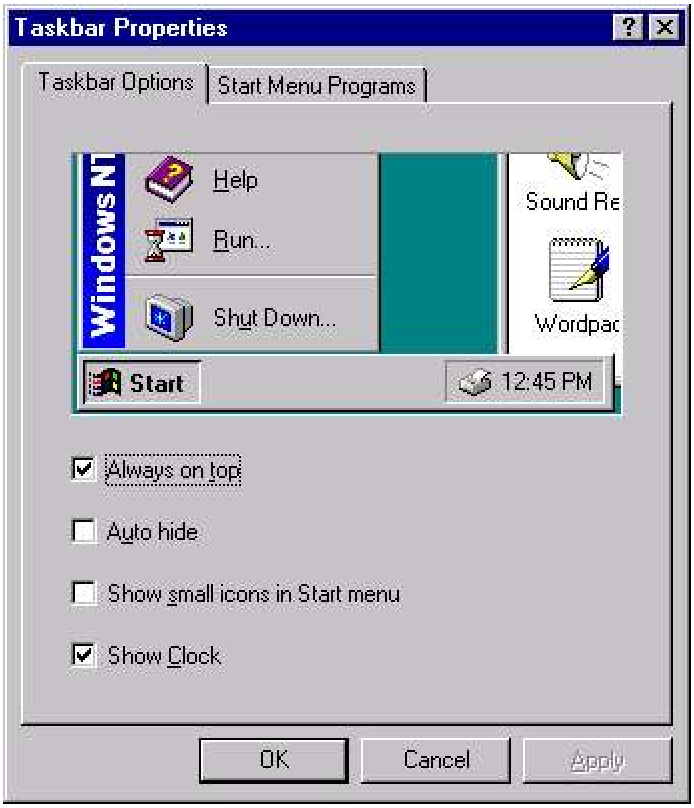
Recycle Bin

The Recycle Bin is a place in which deleted objects remain until you empty the trash. You can retrieve items files, programs, pictures, and so on- from the Recycle Bin after you delete them.

CUSTOMIZING THE TASKBAR

You can customize both the Windows NT Taskbar and Start menu by selecting **Settings** from the Start menu and clicking Taskbar The Taskbar Properties dialog will appear. Notice that this dialog contains two tabs: Taskbar Options and Start Menu Programs. The Taskbar Options tab shows four options, each with its own checkbox.

- Always on top
- Auto hide
- Show small icons in Start menu
- Show Clock



☑ Always on top

□ Auto hide

□ Show small icons in Start menu

☑ Show Clock

Fig 4.13 Taskbar Properties

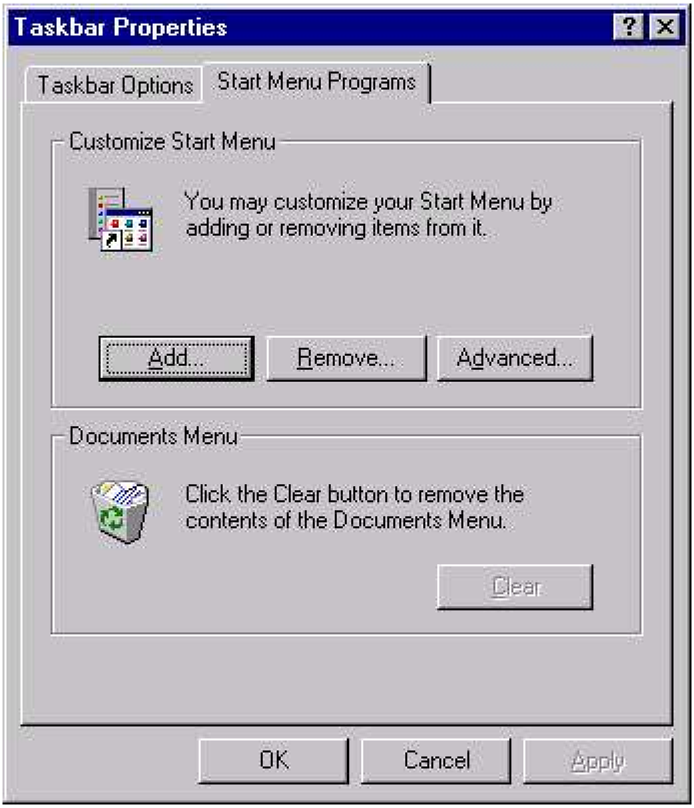
The **Always on top** and the **Show clock** checkboxes are marked by default. You may clear either one or both of these checkboxes if you want to not always have the Taskbar on top and/or if you do not want for the system clock to display. The Auto hide and the Show small icons in Start menu checkboxes are both cleared by default. Mark the Auto hide checkbox if you do not want to see the Taskbar until you explicitly move your mouse pointer off of the desktop, beyond where the Taskbar should be. This will activate the Taskbar and make it visible. When you move your mouse pointer back onto the desktop and off of the Taskbar, the Taskbar will automatically hide.

CONFIGURING THE START AND PROGRAMS MENUS

Windows NT lets you customize the contents of the Start menu (the menu that appears when a user clicks the Start button on the taskbar) and the Programs menu (the cascading menu of program groups and applications that appears when a user clicks the Start button and then points to Programs).

In Windows NT, you can rename, add and remove items from the Start menu. To rename, add or remove an item in the Start menu

- Click the Start button, and then point to Settings.
- Click Taskbar, and then click the Start Menu Programs tab as shown below in Fig 4.14.



Customize Start Menu

You may customize your Start Menu by adding or removing items from it.

Documents Menu

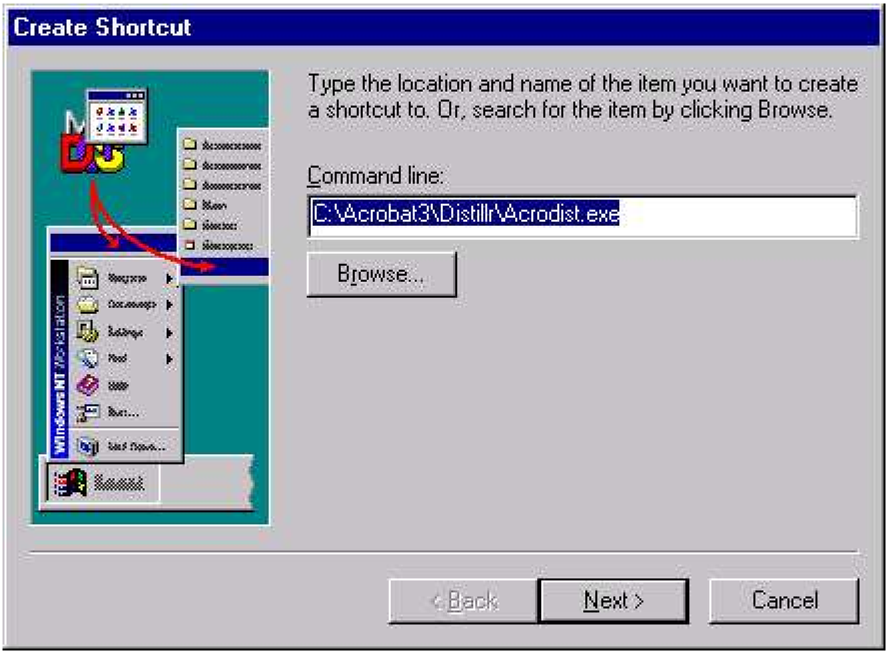
Click the Clear button to remove the contents of the Documents Menu.

Fig. 4.14 Start Menu tab of Taskbar Properties

- Click **Advanced**.
- To rename an item in the Start Menu:
  - Right-click the item you want to rename, and then click **Rename**.
  - Type the new name for the item.

To add or remove items from the Programs menu, click the **Start** button, point to Settings, and then click **Taskbar**. Now, click the Start Menu **Programs tab**, and then do one of the following:

- To add an item, click **Add**, and then follow the wizard's instructions.


Create Shortcut

Type the location and name of the item you want to create a shortcut to. Or, search for the item by clicking Browse.

Command line: C:\Acrobat3\Distillr\Acrodist.exe

Fig 4.15 Creating Shortcut

- Click **Next** to proceed.
- Select a **Program Folder** in which to place the program that you are adding to the Start menu. Click the folder of your choice (Fig 4.16) or click **New Folder** to add a new folder to the Start menu and place the program inside of it.
- Click **Next** to continue.
- Type a name for the program (Windows NT calls it a Shortcut to the program) and click **Finish**. You have just added a program to the Start menu.

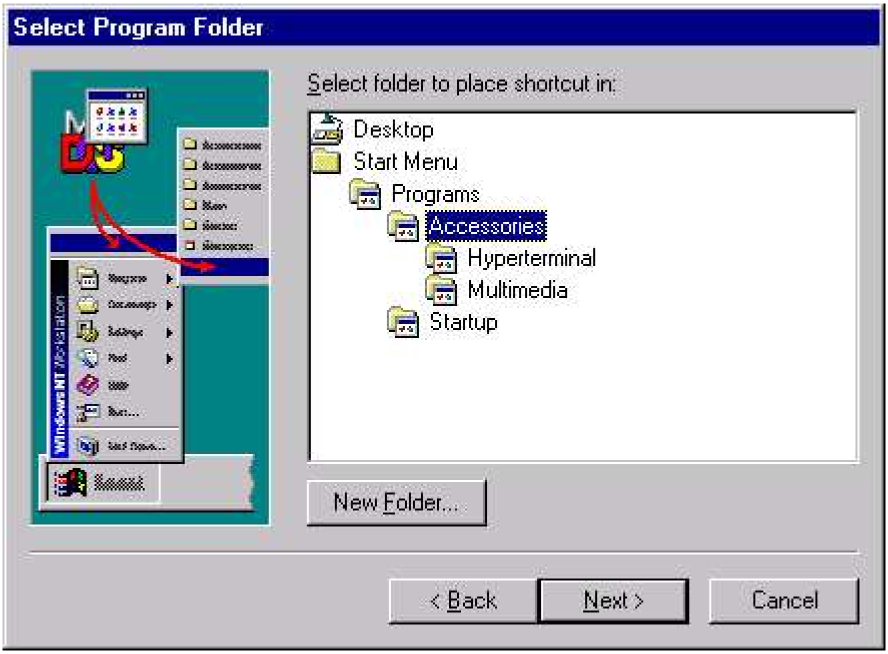
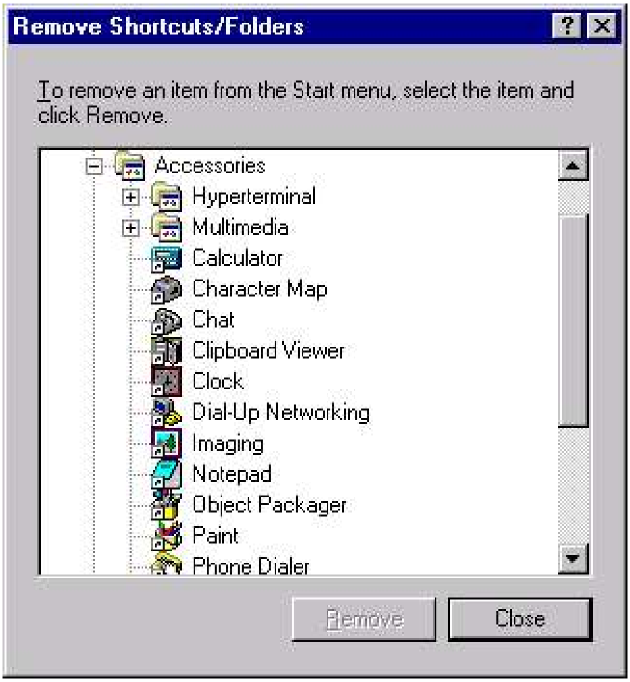


Fig 4.16 Selecting folder for placing shortcut

- To remove an item, click **Remove**, select the item you want to remove, and then click **Remove**.



To remove an item from the Start menu, select the item and click Remove.

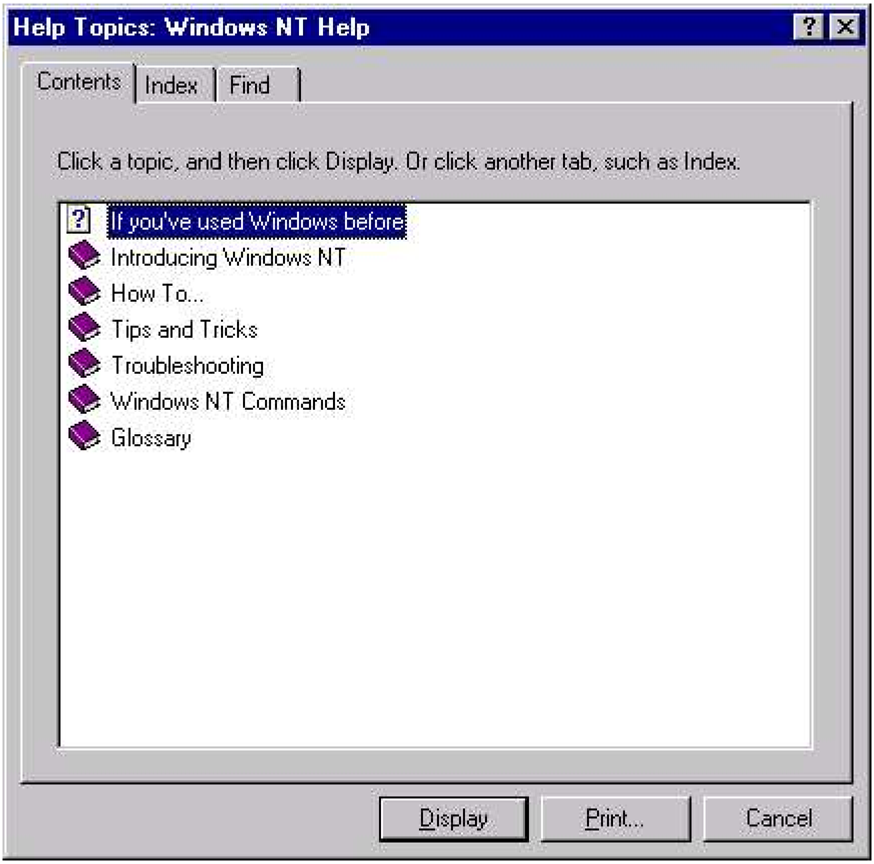
Fig. 4.17 Removing Shortcut

- To reorder items on the Programs menu:
    - Click the **Start** button, and then point to Programs.
    - On the Programs submenu, click the item you want to move, and then drag it to the new location.

USING NT HELP

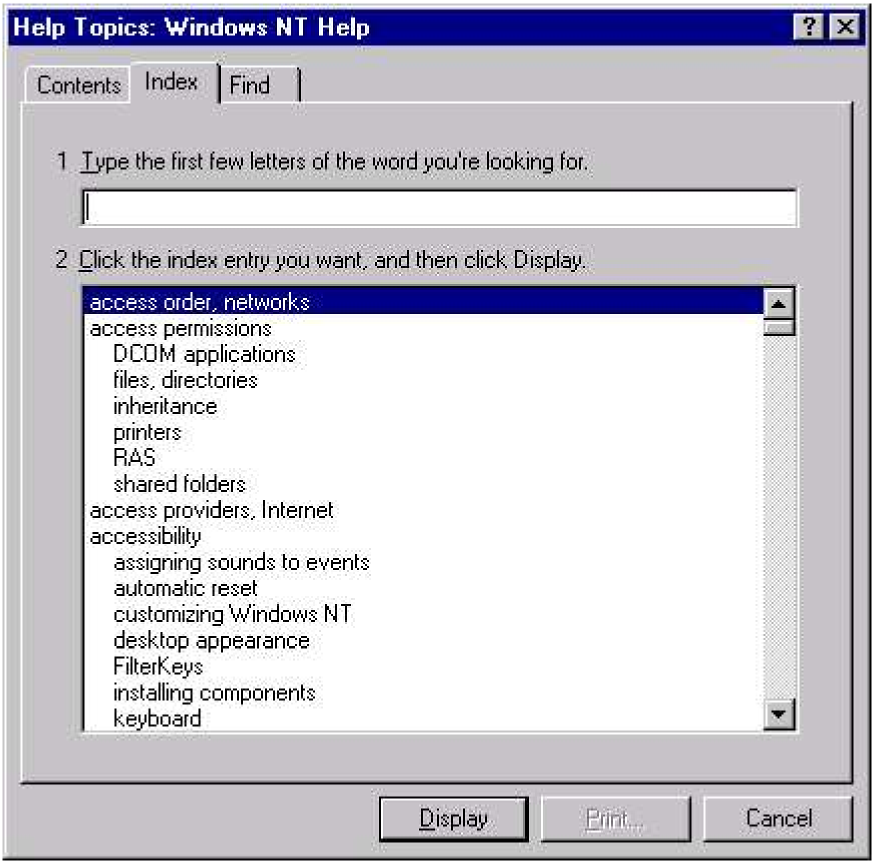
The Start menu provides access to Windows NT HELP. You can also press the F1 key from the Windows NT Server Desktop to access HELP. In Help, click one of the following tabs:

- To browse through topics by category, click the **Contents** tab. Select the category by double clicking it and then view the list of the topics. Double click the topic to display the help information.


Help Topics: Windows NT Help

Click a topic, and then click Display. Or click another tab, such as Index.

Fig 4.18 The Help Window



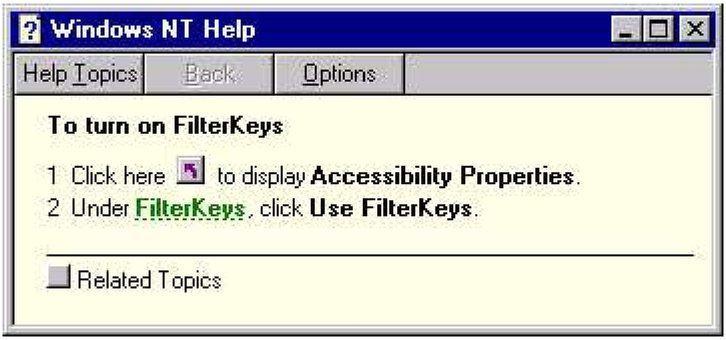
1 Type the first few letters of the word you're looking for.

2 Click the index entry you want, and then click Display.

access order, networks
access permissions
  DCOM applications
  files, directories
  inheritance
  printers
  RAS
  shared folders
access providers, Internet
accessibility
  assigning sounds to events
  automatic reset
  customizing Windows NT
  desktop appearance
  FilterKeys
  installing components
  keyboard

Fig 4.19 The Index Tab of help window

- To see a list of index entries, click the **Index** tab, (Fig. 4.19) and then either type a word or scroll through the list. Choose the required topic to get help. (Fig 4.20).

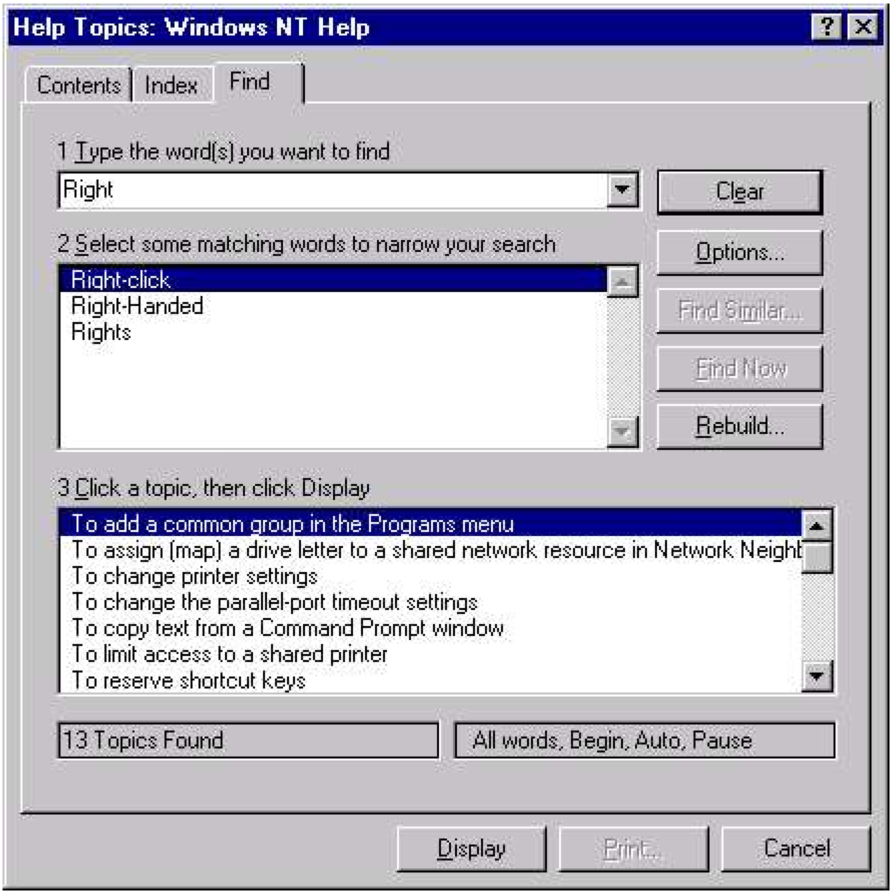


To turn on FilterKeys

1 Click here to display **Accessibility Properties**.
2 Under FilterKeys, click **Use FilterKeys**.

Fig 4.20 Windows NT help

- To search for words or phrases that may be contained in a Help topic, click the **Find** tab. Find tab permits you to search for Help topics that contain specific key words that you are looking for, instead of having to locate Help references only by typing in names of categories. The Options button gives you the flexibility of changing various search parameters such as requiring exact word matching with what is typed. You can allow matching for any words that begin, end, or simply contain the same characters that are typed. First, type in the word(s) you want to find in the top drop-down box. Next, click one of the matching terms shown in the middle drop down. Finally, click the topic that you want to view and then click the **Display** button.



1 Type the word(s) you want to find

Right

2 Select some matching words to narrow your search

Right-click
Right-Handed
Rights

3 Click a topic, then click Display

To add a common group in the Programs menu
To assign (map) a drive letter to a shared network resource in Network Neighb
To change printer settings
To change the parallel-port timeout settings
To copy text from a Command Prompt window
To limit access to a shared printer
To reserve shortcut keys

13 Topics Found

All words, Begin, Auto, Pause

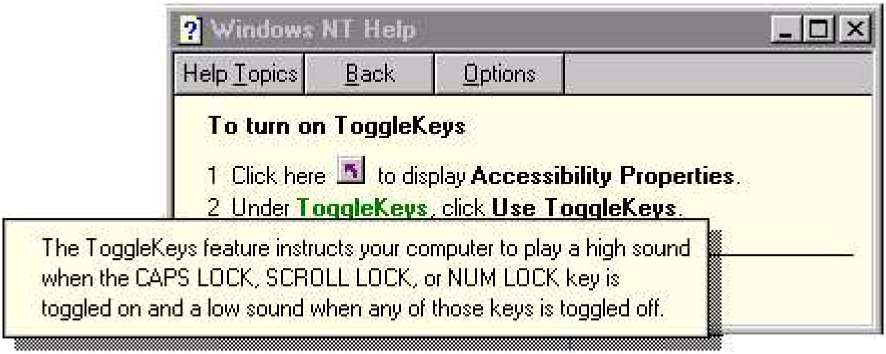
Fig 4.21 Find Tab of Windows NT help

In addition to printing Help topics, you can copy the information contained in them using the **Option** ➢ **Copy** command and then paste it into another application using the **Edit** ➢ **Paste** command. You can even add your own annotation to a help topic by choosing **Option** ➢ **Annotate**. Type your comments, click **Save**, and you see a paper-clip icon at the top of the topic. You can click this icon to view or edit the comment.

WORKING WITH HELP SCREENS

Once you have arrived at the help screen you want, look for two useful features.

- You see phrases underlined in green. Click on any of these to jump to further information relating to that phrase. (Fig 4.22)



To turn on ToggleKeys

1 Click here to display **Accessibility Properties**.

2 Under ToggleKeys, click **Use ToggleKeys**.

The ToggleKeys feature instructs your computer to play a high sound when the CAPS LOCK, SCROLL LOCK, or NUM LOCK key is toggled on and a low sound when any of those keys is toggled off.

Fig 4.22 The hidden information

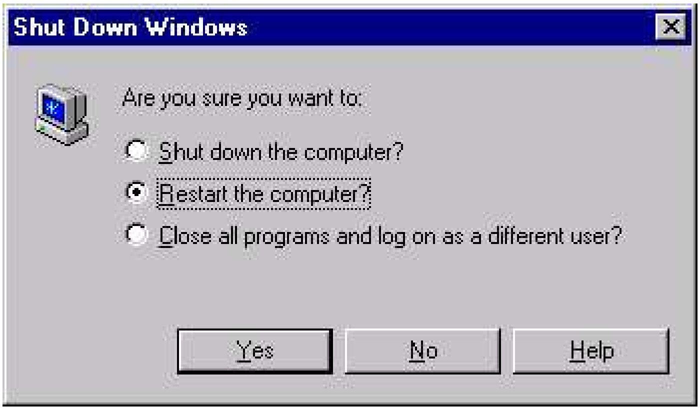
- At the top of most screens are several buttons, the selection of buttons depends on which aspect of help you are accessing. These buttons assist you to navigate the help system quickly and easily.

Button	**Action**
Help Topics	Displays the main Contents screen, with the last used tab on top
Back	Returns you to the last help screen you viewed
Options	Lets you copy or print the topic, or keep the help topic on top while you work.

SHUTTING DOWN WINDOWS NT

When you need to turn off the computer, you must shut down Windows first. Shutting down Windows allows Windows to close all its files and do other housekeeping tasks before terminating.

To shut down Windows, choose **Start ➢ Shut Down** (or click the desktop and press **ALT-F4**, or press **CTRL-ESC** and choose **Shut Down**). You see the Shut Down Windows dialog box, shown in Figure 4.23. Your Shut Down Windows dialog box may contain different options if your computer is connected to a local area network or has a suspend mode.



Shut Down Windows

Are you sure you want to:

○ Shut down the computer?

● Restart the computer?

○ Close all programs and log on as a different user?

Fig. 4.23 Exiting from Windows

Choose and click OK. Windows displays a message when you can safely turn off the computer. Don't turn off the computer until you see the message.

Shut Down Choose this option when you're finished using your computer for the day.

Restart Many programs require that you restart Windows after installing the program to ensure that the program's components are correctly loaded. Choose this option to shut down and then restart the computer in Windows mode.

Close all program and log on as different user?

Select this option if you want to logon as a different user.

Click the appropriate option button and then click **Yes**. If you want to cancel and not shut down or log off, click **No**.

EXERCISE

1. Start Windows NT desktop by specifying your user name, password and domain name. Also try logging in by specifying the user name as Administrator and a blank password. What error message do you get, if any?
2. What happens when you press Ctrl+Alt+Del after logging in successfully? Does the computer restart or an application gets terminated?
3. After successful login, when you get the Windows NT desktop there are certain icons present on it. Explain them in brief.
4. How can you find out the hardware configuration of our machine after logging in?
5. How will reveal a list of known networks, servers and network shares? Also identify your machine and find whether it is on network or not.
6. What is Task bar? Can you move your taskbar to the right side of the screen. Also explore the right click options of the Taskbar?
7. How and from where you can install a printer?
8. What Administrative Tools are available in Windows NT?
9. What are the various methods of shutting down your machine?
10. What sort of help Windows NT provides? Explain the possible options in brief.
11. Search RDISK.EXE file in your computer and create a shortcut of this file names as “Repair Disk” in your computer’s Program Menu.
12. Discuss the various ways to switch among applications. Is it possible to display the desktop while all the applications are minimized with one commands? If yes, how?

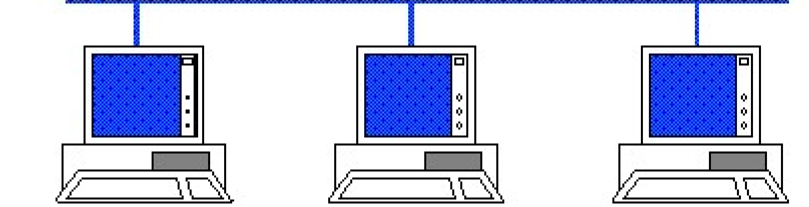
State True of false :

1. The size and position of Taskbar is Fixed.
2. System tray can contain more than one icon.
3. Task Manager can stop the application but can’t start them.
4. The entries in Start menu can be added as well as removed.
5. When you press Ctrl+Alt+Del, it stops all the application and shut down.
6. Find command lets you find the computers on the network.

CHAPTER 5

Running Windows NT

STARTING PROGRAMS
USING START MENU
USING DOS
NAVIGATING THRIUGH FILES & FOLDERS
THE RIGHT CLICK SUPPORT
THE RECYCLE BIN
THE NETWORK NEIGHBOURHOOD



STARTING PROGRAMS

Windows NT gives you many ways to start a program, including clicking its icon on your Windows desktop, choosing it from a menu, clicking a document you want to edit or view by using the program, clicking the name of the file that contains the program, and typing the program name into a Run or DOS window.

USING DESKTOP

If an icon for the program appears on your Windows NT desktop, click the icon twice to run the program. Another way to start a program from the desktop is to select the icon, then press ENTER.

USING START MENU

As discussed earlier, to launch a program from the Start menu, click the **Start** button. Your Start menu may have additional options, depending on which programs you have installed.

When your mouse pointer is on a menu name, the menu appears to its right. Point to menus until you see the name of the program that you want to run; then click the program name. Most programs appear on the Programs menu, while many Windows utility programs appear on the Settings menu. Other programs appear on submenus of the Programs menu. You may need to try several menus to find the one that contains the program you want.

BY CLICKING PROGRAM FILENAMES

Programs are stored in files, usually with the filename extension EXE. Windows NT displays the names of program files in Windows Explorer or Folder windows.

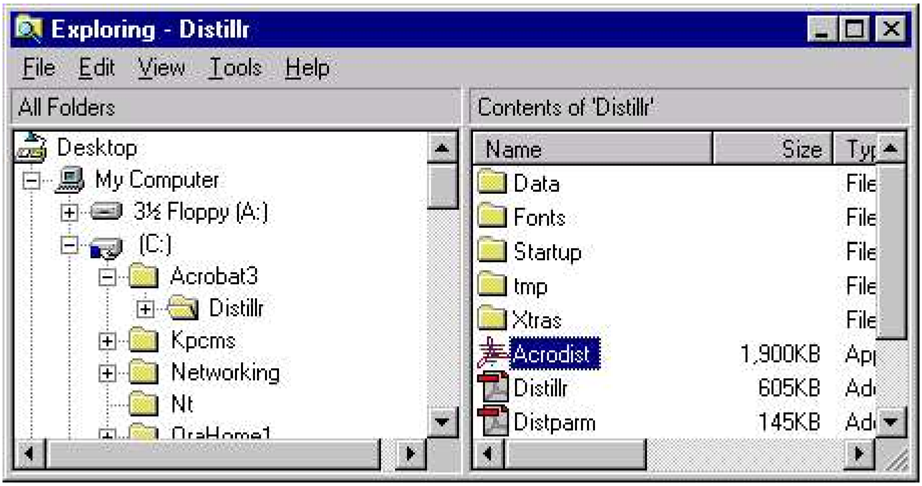
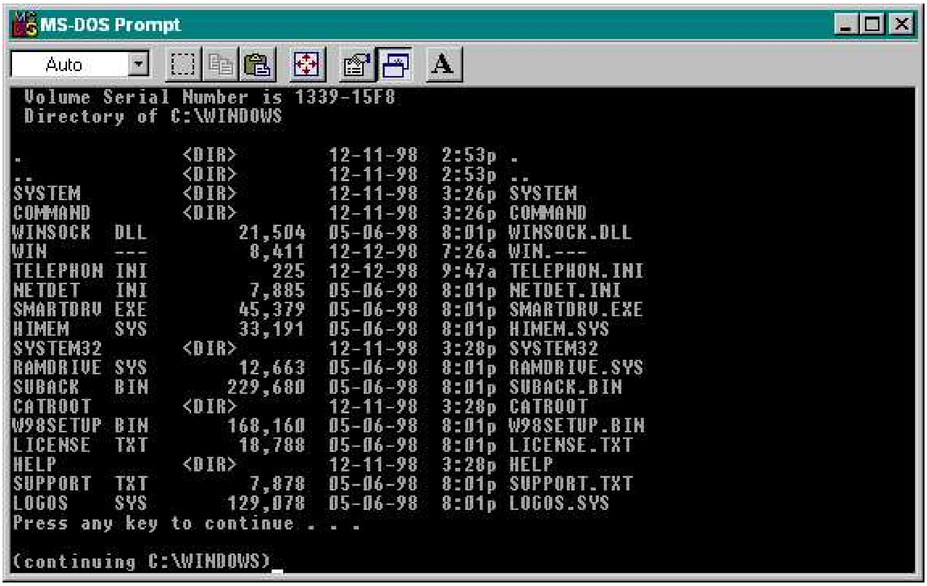


Fig. 5.1 Running program by clicking file name in Explorer

USING DOS

To run programs from the DOS prompt, choose **Start ➤Programs ➤ MS-DOS Promp**t as shown in Fig 5.2. (Alternatively, you can choose **Start ➤ Run**, then type command and press ENTER.). You see an MS-DOS Prompt window, a window that looks like the screen of a computer running DOS. Type the filename of the program you want to run and press ENTER.



```
 Volume Serial Number is 1339-15F8
 Directory of C:\WINDOWS

.              <DIR>        12-11-98  2:53p .
..             <DIR>        12-11-98  2:53p ..
SYSTEM         <DIR>        12-11-98  3:26p SYSTEM
COMMAND        <DIR>        12-11-98  3:26p COMMAND
WINSOCK  DLL        21,504  05-06-98  8:01p WINSOCK.DLL
WIN      ---         8,411  12-12-98  7:26a WIN.---
TELEPHON INI           225  12-12-98  9:47a TELEPHON.INI
NETDET   INI         7,885  05-06-98  8:01p NETDET.INI
SMARTDRV EXE        45,379  05-06-98  8:01p SMARTDRV.EXE
HIMEM    SYS        33,191  05-06-98  8:01p HIMEM.SYS
SYSTEM32       <DIR>        12-11-98  3:28p SYSTEM32
RAMDRIVE SYS        12,663  05-06-98  8:01p RAMDRIVE.SYS
SUBACK   BIN       229,680  05-06-98  8:01p SUBACK.BIN
CATROOT        <DIR>        12-11-98  3:28p CATROOT
W98SETUP BIN       168,160  05-06-98  8:01p W98SETUP.BIN
LICENSE  TXT        18,788  05-06-98  8:01p LICENSE.TXT
HELP           <DIR>        12-11-98  3:28p HELP
SUPPORT  TXT         7,878  05-06-98  8:01p SUPPORT.TXT
LOGOS    SYS       129,078  05-06-98  8:01p LOGOS.SYS
Press any key to continue . . .

(continuing C:\WINDOWS)_
```

Fig. 5.2 Running commands from DOS prompt

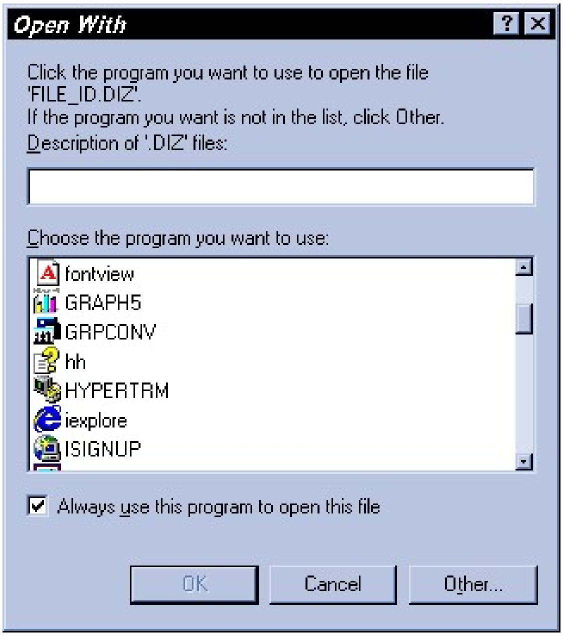
When you are done using the MS-DOS window, close the window by clicking the **Close** button (the button with an X) in the upper right corner of the window. You can close DOS window by typing EXIT at C:\> prompt. You can run DOS commands at the DOS prompt, too.

BY OPENING FILES

When you click or double-click a filename, you are telling Windows NT to run the appropriate program to handle that file (if the program isn't already running), and then to open the file in that program. If an icon for a file appears on your desktop, double-clicking the icon tells Windows NT to do the same thing.

If you try to open a file for which Windows doesn't know which program to run, you see the Open With dialog box, shown in Fig. 5.3.

Choose the program that can open the type of file you clicked; if the program doesn't appear on the list, click the **Other** button to find the filename of the program.



Open With

Click the program you want to use to open the file 'FILE_ID.DIZ'.
If the program you want is not in the list, click Other.

Description of '.DIZ' files:

Choose the program you want to use:

- fontview
- GRAPH5
- GRPCONV
- hh
- HYPERTRM
- iexplore
- ISIGNUP

☑ Always use this program to open this file

Fig. 5.3 Windows asking for the application name

EXITING PROGRAMS

Most programs provide several ways to exit, including some or all of these:

- Choose the **File ➢ Exit** command from the menu bar.
- Click the **Close** button in the upper-right corner of the program's window. If a program displays multiple windows, close them all.
- Press **ALT+F4**.
- Click the **System Menu** button in the upper-left corner of the program's window and choose **Close** from the menu that appears.
- Right-click the program's button on the Taskbar and choose **Close** from the menu that appears.

NAVIGATING THROUGH FILES & FOLDERS

MY COMPUTER

Opening the My Computer icon on the desktop causes a Folder window to appear, as in Fig 5.4. Any folder that you open from the desktop creates a new Folder window. All currently available resources are displayed within this window, including all currently mapped network drives. The system's Printers folder is available within My Computer as is the Control Panel folder.

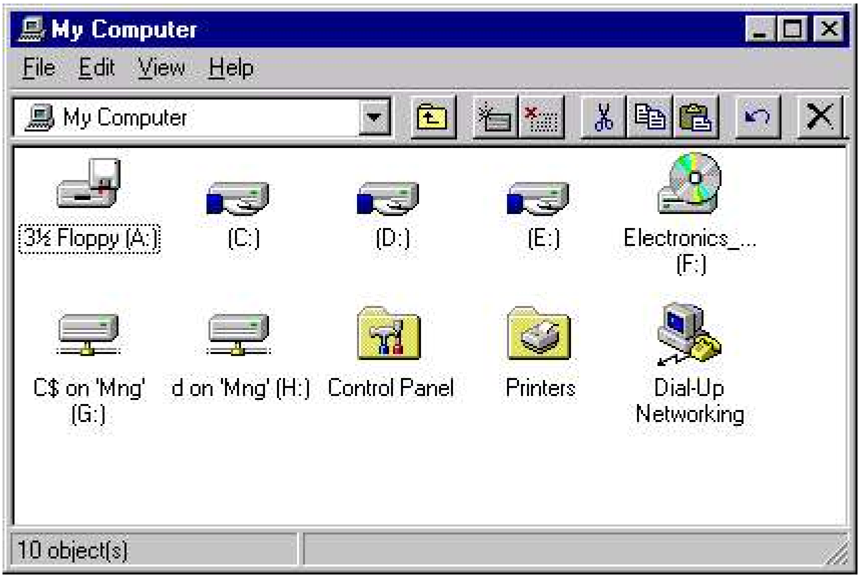
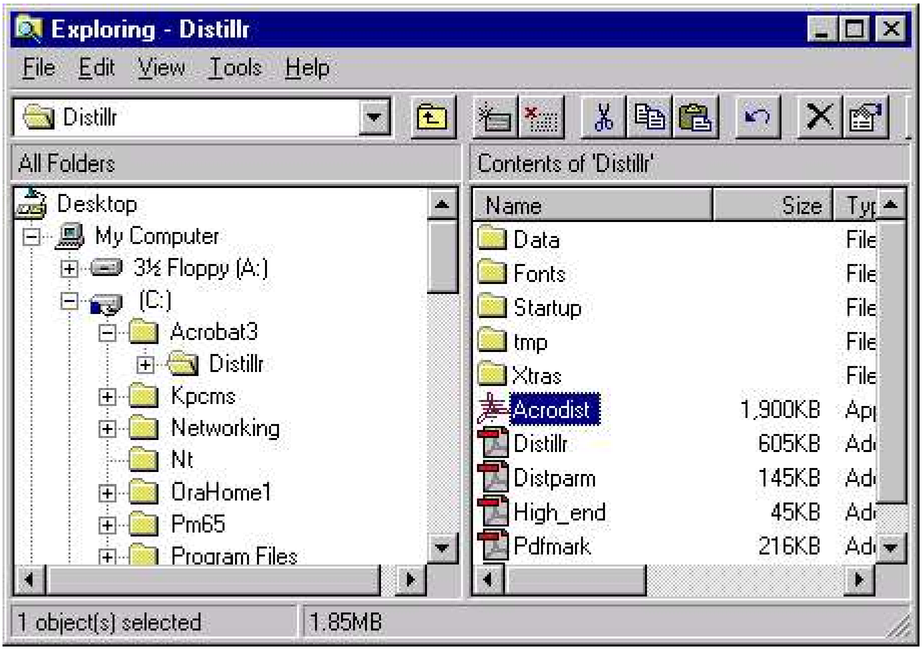


Fig. 5.4 My Computer Folder Window

WINDOWS EXPLORER

The Windows NT Explorer window, shown in Fig 5.5, opens when you run Windows NT Explorer.



Name	Size	Typ
Data		File
Fonts		File
Startup		File
tmp		File
Xtras		File
Acrodist	1,900KB	Ap
Distillr	605KB	Ad
Distparm	145KB	Ad
High_end	45KB	Ad
Pdfmark	216KB	Ad

Fig 5.5 Windows NT Explorer

You can run Windows NT Explorer by choosing **Start ➢ Programs ➢ Windows NT Explorer**. Or, you can put a shortcut to Windows NT Explorer somewhere more convenient, such as the top of the Start menu or on the desktop.

The folder tree is displayed in the left pane (the left side of the window), called the Explorer bar, with the open folder highlighted. The contents of the open folder appear in the right pane.

The rest of the Windows NT Explorer window is similar to the Folder window: The title bar gives the name of the open folder. Beneath the title bar are the same menu bar and toolbars as in the Folder window. At the bottom of the window lies the status bar. The toolbars and status bar can be made to appear or disappear by toggling the Toolbar or Status Bar commands on the View menu.

CREATING SHORTCUTS

Technically, a shortcut is a file of type Shortcut, with a .lnk extension. Less technically, a shortcut is a placeholder in your filing system. It has a definite position on the folder tree, but it points to a file or folder that is somewhere else on the folder tree.

The purpose of a shortcut is to allow an object to be in two places at once. You usually should leave a program file inside the folder where it was installed, so that you don't mess up any of the relationships between it and its associated files. At the same time, you might want the program to be on the desktop, so that you can conveniently open files by dragging them to the program's icon. Therefore, leave the program file where it is, but make a shortcut pointing to it, and place the shortcut on the desktop. When you drag a file to the shortcut icon, Windows opens the file with the corresponding program.

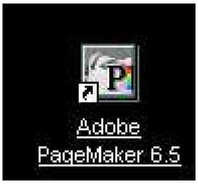


Fig. 5.6 Shortcut for an application on Desktop

You can recognize a shortcut icon by the curving arrow that appears in its lower-left corner. A shortcut icon otherwise looks just like the icon of the object it points to: a document, folder, or application. A shortcut can be on your desktop or in a folder. Shortcuts provide you with easy access to files and programs. Once you place a shortcut icon on the desktop, you can click that icon to start up a program or open a file or folder that you use frequently.

MAKING SHORTCUTS

Shortcuts are created when you:

- Drag-and-drop an application to a new folder or to the desktop.
- Hold down the right mouse button while you drag any object to a new location, and then select **Create Shortcut(s) Here** from the menu that appears when you drop the object.
- Invoke the Create Shortcut Wizard either by selecting **File ➤ New ➤ Shortcut** in a Folder or Windows Explorer window or by right-clicking an open space on the desktop and selecting **New ➤ Shortcut** from the menu that appears.
- A copy of the icon appears in the window with the words ”Shortcut To” in front of the name. Drag that icon from the folder onto the desktop.

THE RIGHT CLICK SUPPORT

You have just seen how desktop shortcuts are created by right-clicking or how Task Manager is activated by right-clicking in the blank-area in the Task bar. You can also right-click a blank area of the Taskbar to cascade or tile, horizontally or vertically, or to minimize all active windows. In addition, you can select **Properties** from the right-click pop-up menu, which is identical to clicking the **Start** button and selecting **Settings ➤ Taskbar**. You can right-click the **Start** button, too. Here, you get three options: Open (open the Start menu folder), Explore (open the Start menu folder from within the Windows NT Explorer), or Find (the same as clicking **Start ➤ Find ➤ Find Files or Folders**).

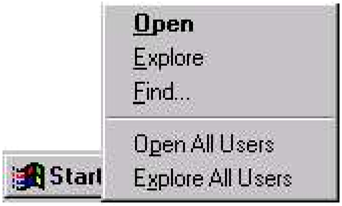
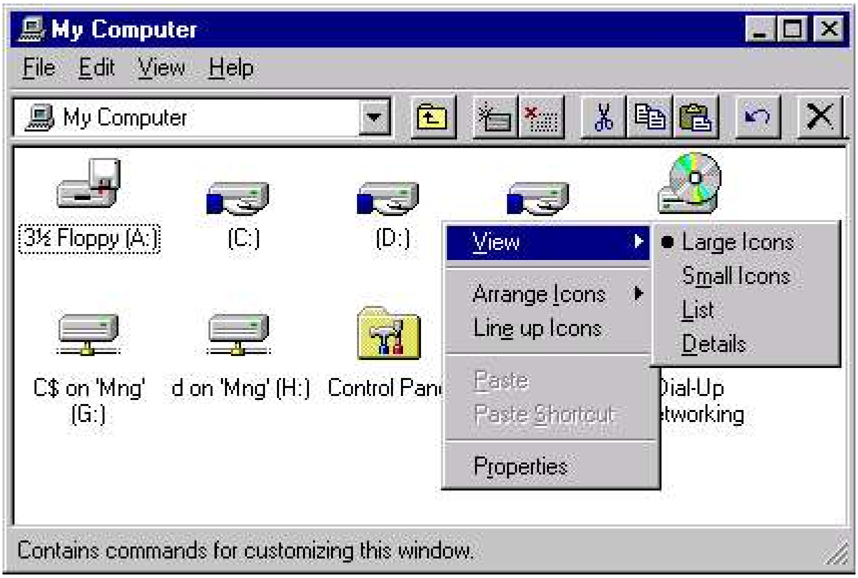


Fig 5.7 Right Click Menu

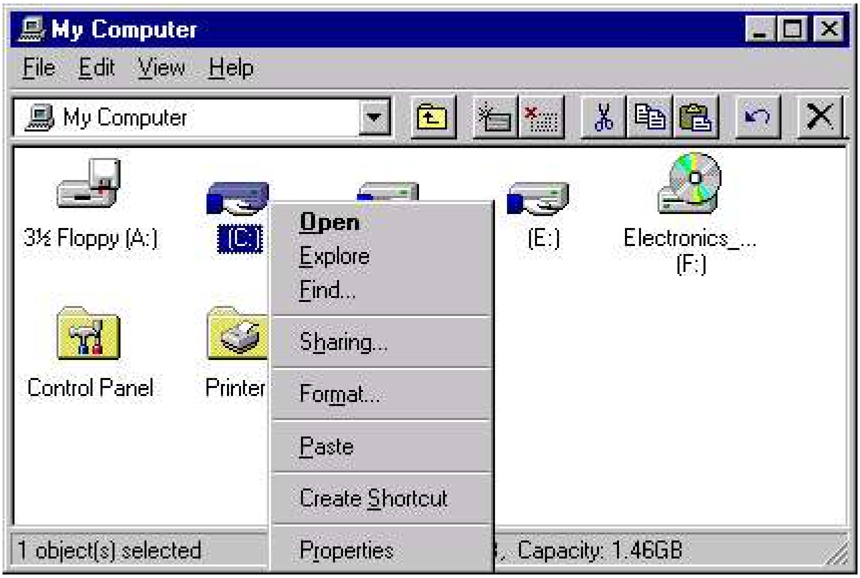
From My Computer, Network Neighborhood, Recycle Bin, and My Briefcase, you can right-click a blank area of the window to change the window's view, to arrange icons, to line up icons, or to paste. You can also undo a delete, undo a copy, or undo a move action and view properties of your Windows NT Server's system. (Fig 5.8)

Similarly, from the My Computer windows, you can look at the properties of a floppy disk by right-clicking the floppy drive icon and choosing properties. To format a floppy disk (or a hard disk, right-click its drive letter icon and select **Format**. (Fig 5.9)



Contains commands for customizing this window.

Fig 5.8 Right Click Menu in My Computer



1 object(s) selected

, Capacity: 1.46GB

Fig 5.9 Right Click Menu on hard disk partition

When you right-click and then drag a folder or file, Windows NT asks you exactly what you want to do with the objects. As soon as you complete a right-click and drag operation, a small pop-up menu appears offering you four options: Move Here, Copy Here, Create Shortcut(s) Here, or Cancel.

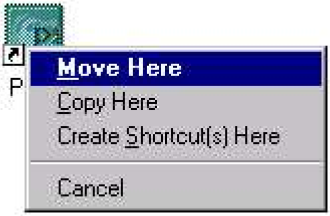


Fig 5.10 Right Click Menu on file or folder

THE RECYCLE BIN

Files and folders deleted from your hard drives do not go away completely, they remain inside the Recycle Bin. From there, they can be either restored to the folder they were in before you deleted them, or moved from the Recycle Bin to any other folder via cut-and-paste or drag-and-drop.

The Recycle Bin icon lives on the desktop and looks like a waste-basket. When you open the icon, a Folder window opens, showing you the files and folders that have been deleted since the Recycle Bin was last emptied.

The Recycle Bin is a hybrid object that behaves like a folder in some ways, but not in others. Like a folder, it contains objects, and can be viewed in either a Folder window or a Windows Explorer window. Fig 5.11 shows empty & filled Recycle Bin.

Fig. 5.11 Recycle Bin, Empty and Filled

Files and folders sent to the Recycle Bin may disappear from the folder tree, but Windows still stores them on your hard drive and keeps track of them. Eventually, one of four things happens:

- You get rid of things in the Recycle Bin, either by emptying it or by deleting some of the files and folders there.
- You retrieve files from the Recycle Bin and put them in some other folder.
- The Recycle Bin gets full.
- You turn off the Recycle Bin so that deleted files aren’t put there any more.

To open the Recycle Bin, click the **Recycle Bin** icon on the desktop select it using the arrow keys, and then press. Enter or right click the icon and choose **Open** from the pop up menu.

The Recycle Bin Window then opens. The Recycle Bin Window has the same look and much of the functionality as My Computer Except for the network buttons, the toolbar is the same (if you can't see your toolbar choose **View**, **Toolbar** from the menu). The status bar at the bottom of the screen shows the number of objects in the window or the number of selected items and the total amount of disk space they use.

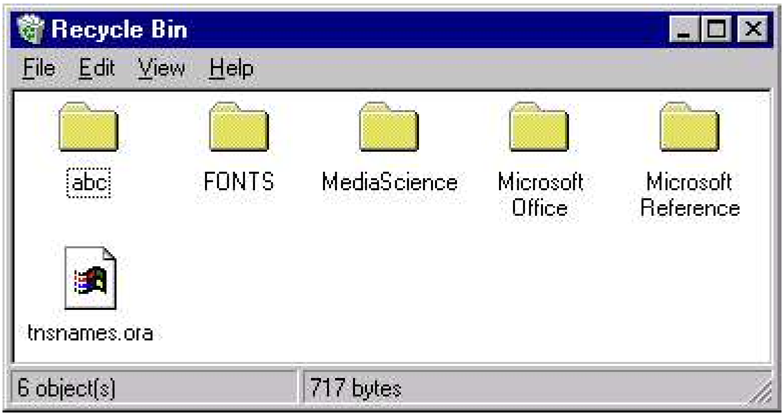


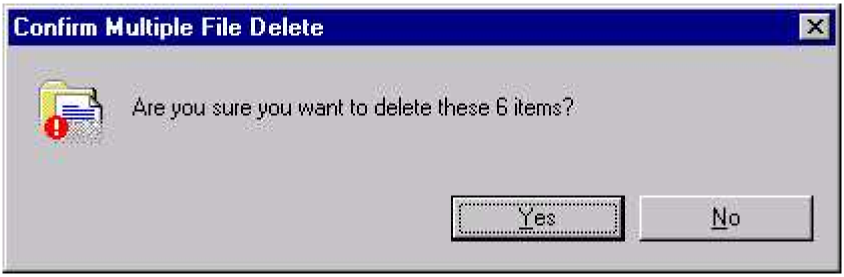
Fig. 5.12 Files in Recycle Bin, which are temporarily deleted

EMPTYING THE RECYCLE BIN

Getting rid of old files serves two purposes: It clears useless files away so that you don't confuse them with useful files, and it reclaims the disk space they occupy. The first purpose is served by deleting a file - once it's in the Recycle Bin, you aren't going to open it or work on it by mistake. But a file in the Recycle Bin still takes up disk space: The space isn't reclaimed until the Recycle Bin is emptied.

To empty the Recycle Bin:

- Open the Recycle Bin in either a Folder or Windows Explorer window.
- Choose **File ➢ Empty Recycle Bin**. A dialog box asks you to confirm your choice.


Confirm Multiple File Delete

Are you sure you want to delete these 6 items?

Fig. 5.13 Confirmation before deleting the files permanently

- Click **Yes**. Windows empties the Recycle Bin.
- Close the Recycle Bin.

Another method is to right-click the Recycle Bin and choose **Empty Recycle Bin** from the menu that appears.

Restoring Files

The simplest way to recover an object from the Recycle Bin is to follow these steps:

- Open the Recycle Bin.
- Select the object (or collection of objects) you want to recover.
- Choose **File ➢ Restore** from the menu bar.

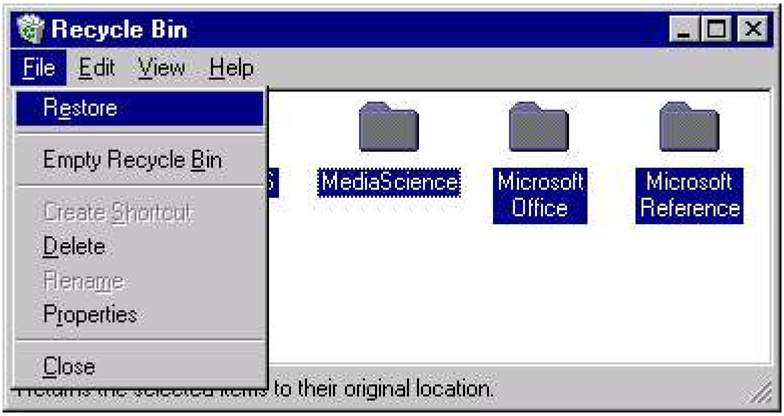


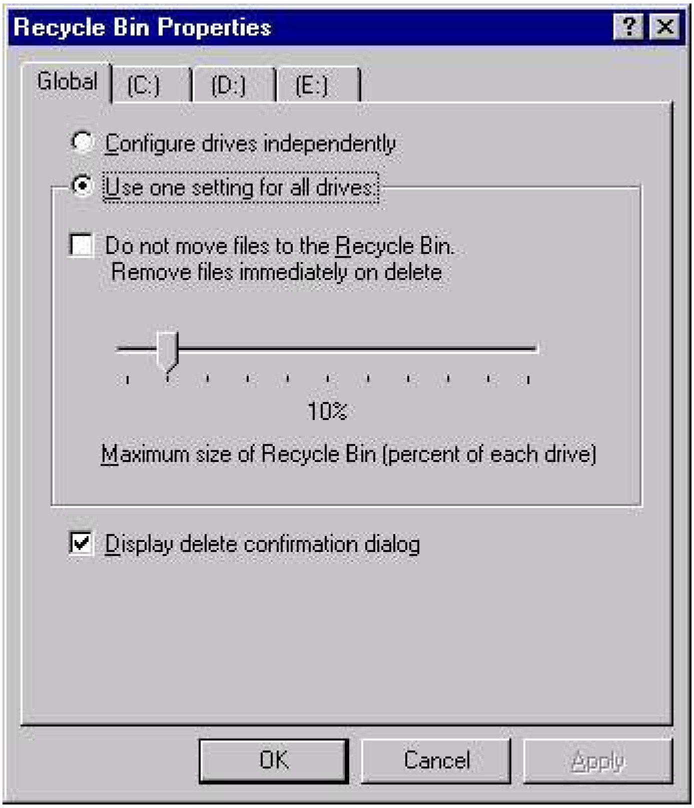
Fig. 5.14 Restoring files from Recycle bin

The object returns to the folder it was deleted from - the address given in the Original Location column of the Details view. If the object is a folder, all of its contents return with it. You can use Restore even if the object was deleted from a folder that no longer exists. A folder of the appropriate name will be created to contain the restored object.

- To recover an object, but put it in a new place, you can either cut-and-paste from the Recycle Bin to the new location, or Open the Recycle Bin with Windows Explorer. Expand the folder tree in the left-hand window so that the target folder icon is visible. In the right pane, select the object(s) you want to recover. Drag-and-drop to the target folder in the left-hand window.

Recycle Bin Properties

Like most other things in Windows NT, the Recycle Bin has properties. To display them, right-click the Recycle Bin icon on the desktop, and choose **Properties** from the menu; or, select the Recycle Bin in a Folder or Windows Explorer window and click the **Properties** button on the toolbar. In either case, the Properties dialog box for the Recycle Bin is displayed. The Properties dialog box contains a Global tab, plus a tab for each hard drive on your system.



○ Configure drives independently

● Use one setting for all drives:

□ Do not move files to the Recycle Bin. Remove files immediately on delete

10%

Maximum size of Recycle Bin (percent of each drive)

☑ Display delete confirmation dialog

Fig. 5.15 Setting size of Recycle bin

To open the Recycle Bin Properties box, click the **Recycle Bin** icon with the right mouse button and choose **Properties** from the pop up menu.

	Setting	**Description**
■	Configure drives independently	Allows you to use different on the tab settings for each hard disk.
■	Use one setting for all drives	Specifies that the settings on the General tab apply to all hard drives.
■	Do not move files to the Recycle Bin, Remove files immediately when deleted.	Specifies that when you delete files or folders, Windows deletes them directly rather than moving them to the Recycle Bin.
■	Maximum size of Recycle Bin (percent of each drive)	Specifies the maximum amount of disk space that the Recycle Bin can occupy, as a percentage of total disk space.

■	Display delete confirmation dialog box	Specifies that Windows ask you to confirm whenever you move a file to the Recycle Bin.

THE NETWORK NEIGHBORHOOD

The Network Neighborhood icon displays all of the networked computers and printers that are present on your network. Double-click the Network Neighborhood icon to open up its window. The initial view shows your current network workgroup or Windows NT Server domain resources. To view other workgroups and domains that exist on your network, double-click the Entire Network (globe) icon.

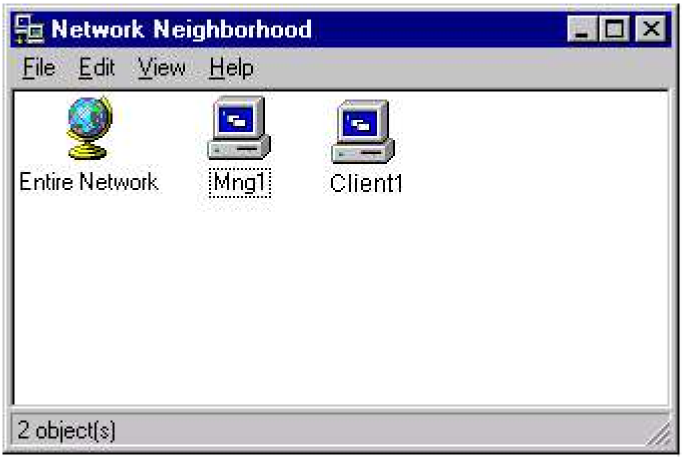


Fig 5.16 The Network Neighborhood

In a Microsoft Windows network, you would then view a set of icons representing available workgroups and/or Windows NT Server domains. (Fig 5.17). Double-click the workgroup or domain icon of your choice to view its available computers.

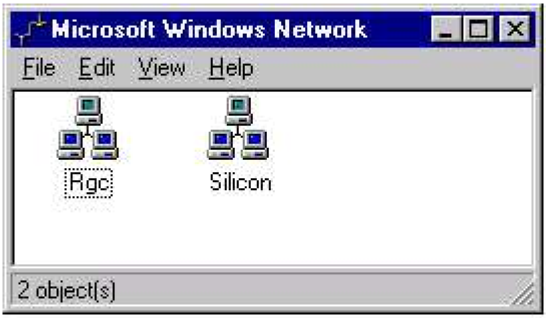


Fig 5.17 Windows Network

Within the workgroup or domain that you select, double-click the computer/server icon that you want to browse. After you double-click one of the computers, you will see a set of icons that represent all of the shared folders and shared printers for that specific computer. You can double-click each of the shared folders to browse their contents or right-click one or more of the shared folders and map a local drive letter to each one.

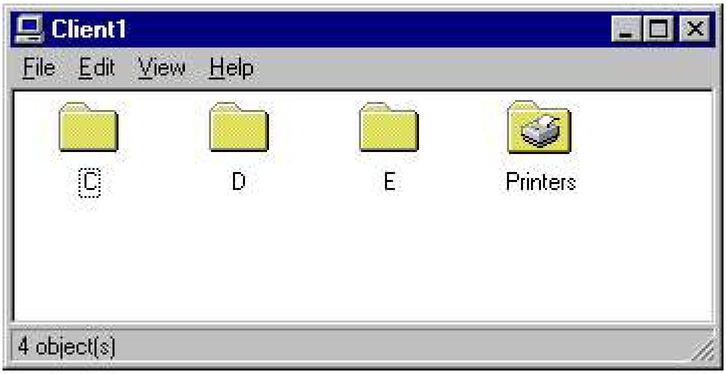


Fig 5.18 Folders of a Network Client

EXERCISE

State True or False:

1. Once removed from the Recycle bin, the deleted contents can't be retrieved.
2. Right Click support is not available at Desktop.
3. MS-DOS application can't run on Windows NT Operating System.
4. Network Neigborhood doesn't display the shared network printers.
5. If you right click the shared network drive, the mapping option will be available in that.

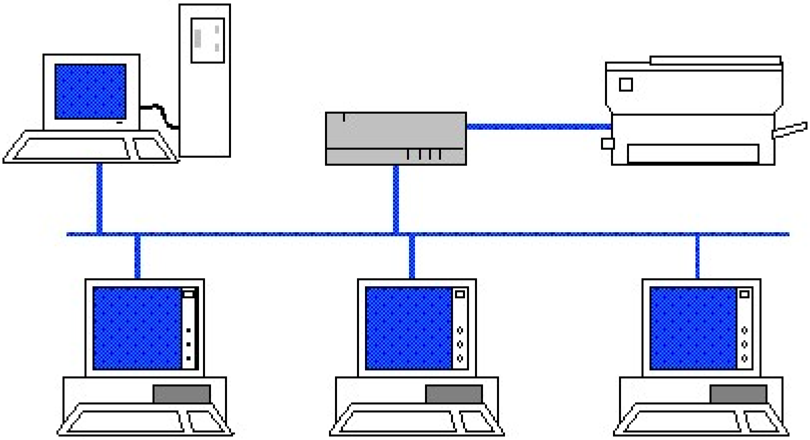
Answer the following questions:

1. Discuss the various methods or running an application.
2. Create the shortcut of "Word Pad" icon, available in **Start ➢ Program ➢ Accessories ➢ WordPad**, on the desktop using the right click menu.
3. What is the difference between My Computer and Windows Explorer. Can you convert the My Computer View as Windows NT Explorer or vice-versa?
4. Create a new directory "SILICON" in root of your Drive C using My Computer and Windows Explorer.

CHAPTER 6

File System & Disk Management

FILE SYSTEM IN NT
FAT AND NTFS
DISK ADMINISTRATOR
FAULT TOLERANCE
RAID (Redundant Array of Inexpensive Disks)
VOLUME SETS
STRIPE SET
MIRRORING
STRIPPING WITH PARITY
RECOVERING FROM HARD DISK FAILURES



FILE SYSTEM IN NT

Windows NT support three major file system

- FAT (File Allocation Table)
- NTFS (NT File System)
- HFPS (High-Performance File System)

Beside these file systems, there exist also CD File System (CDFS). CDFS provides support and performance optimization for CD-ROM drives.

The FAT file system was designed originally for the DOS operating system and is the primary file system for computers running DOS/ Windows 3.x and Windows 95. FAT was not designed with larger capacities in mind, and has since required the use of new operating systems and system BIOS's to allow for the use of larger hard drives and directory trees of files that number in the thousands or millions.

A new version of FAT, called FAT32, has been added to the OEM 2 release of Windows 95 and Windows 98. FAT32 extends the original FAT file system but is not supported by Windows NT Server 4.0. (If you add a secondary master with FAT32 partition, Windows NT server will not recognize it.)

NTFS was developed specifically for Windows NT. NTFS provides much greater security and auditing than does the FAT file system. The NTFS provide security of C2 level (a standard defined by the U.S. Government). NTFS also offers more efficient storage, eliminating the waste of empty sectors, called sector slack, inherent in the FAT file system. (In FAT16 system, data is stored in the block of 16 bits. If your file size is 49 bits, it will be stored in 4 block of 16 bits, thus wasting 15 bits of space. The space wastage in more in FAT32 system as the block size is of 32 bits.)

FAT

Partitions formatted with FAT are broken into clusters. A disk formatted with the FAT file system contains four control areas.

Reserve Area

Comprises of one or more sectors. Boot sector is the first sector and contains partition table and bootstrap program. The partition table contains information about the partitions on the disk, including the type of partition, starting and ending sector, which partition is active, and other information. The bootstrap program executes when the system starts and is responsible for booting the operating system in the active partition.

FAT

The second control area is the FAT. The FAT essentially is a reference table that maintains a list of clusters on the disk. The value of the each cluster entry in the FAT records the status of the associated disk cluster.

Root Directory Table

The root directory table, the third control area of the disk, works in conjunction with the FAT. The root directory table contains the names of files in the root directory, including subdirectories (which are really nothing more than files) and the starting cluster of each file.

Files Area

Here file data is stored.

Thus, FAT keeps track of a few attributes for each file, such as the name of the file, the address of the starting sector, whether the file was deemed a system file, a read-only attribute, an archive bit, and a date for the file's creation or the last time the file was modified.

The FAT file system is prone to fragmentation, as data is written to the noncontiguous clusters. This slows down the read/write process. FAT writes files to the first available cluster it can find, and then skips ahead past used clusters to complete writing a file.

HPFS

HPFS (High-Performance File System) was introduced in 1990 as part of OS/2 and (optionally) Windows NT 3.x. The following were the main advantages of HPFS system:

- HPFS allowed for greater capacity of hard drives and instituted technologies that would help prevent the occurrence of fragmentation
- HPFS implemented a data structure called a B-Tree, which allows for directory searches to occur in a more logical manner, as opposed to FAT's linear structure.
- HPFS implements physical separation between files giving each file room for expansion, which would then result in less chance of fragmentation.
- HPFS introduced long filenames of up to 255 characters, along with other attributes, such as the same attributes kept by FAT, and an access control list (ACL).

NTFS

NTFS (NT File System) is specifically designed for Windows NT. It’s most important feature is that it is a recoverable file system. If the system fails during a file operation, NTFS reconstructs the volume and recovers from the failure. This recovery happens automatically the first time the disk is accessed after a failure, requiring no intervention from you. In addition, NTFS further secures the file system by maintaining redundant copies of critical file system data, enabling it to recover if the data becomes corrupted.

Another important NTFS feature is its support for fault tolerance such as mirroring drives. If one drive fails, the data is still available and secure on a redundant drive. Windows NT Server supports a full range of fault tolerance options, and Windows NT Workstation supports stripe sets. It will be discussed in more detail later in the chapter.

MASTER FILE TABLE

NTFS also supports very large disk sizes. Whereas FAT allocates clusters using 16-bit numbers (32-bit numbers for FAT32), NTFS uses 64 bits to number clusters, allowing for 264 clusters - a huge number (over 16 quintillion). NTFS uses different cluster size on different size of the disk. The following table gives a fair idea about the cluster size according to the disk size:

Partition Size	**Cluster Size**
512MB	512 bytes
513MB-1GB	1K
1GB-2GB	2K
2GB-4GB	4K
4GB-8GB	8K
8GB-16GB	16K
16GB-32GB	32K
> 32GB	64K

NTFS tracks the contents of a file using its database called Master File Table (MFT). MFT contains a record for each file, and directory and a log file along with other attributes for the file. The size of each MFT file record is constant and is set when the volume is formatted. Depending on the disk, the size could be either 1K, 2K, or 4K.

Many copies of MFT are stored at different places. A mirror of MFT is stored in boot sector along with pointers of MFT and its mirror. A copy of the boot sector is stored in the logical centre of the disk.

One of the fields in the MFT for each file record is the Data field. For a small file, the Data field contains the file's data, which means that a small file can be contained completely within one MFT record. When all of a file's attributes (including its data) reside in the MFT, the attributes are called resident attributes.

If the file's attributes increases, NTFS creates additional 2K size area on the disk called runs. These runs contains additional attributes and these are called, nonresident attributes.

When a partition is formatted as NTFS, numerous system files are created that keep track of certain attributes of that partition.

Filename	System File	Description
$Mft	Master File Table	The MFT
$MftMirr	Master File Table2	The mirror copy of the MFT
$LogFile	Log File	A file activity log that can be used to help rebuild information in case of a failure
$Volume	Volume	The name of a volume, along with other volume information
$AttrDef	Attribute Definitions	A table of attribute names, numbers, and descriptions.
$	Root Filename Index	The root directory
$Bitmap	Cluster Bitmap	A representation of the volume showing which allocation units are in use
$Boot	Boot File	If this partition is bootable, a bootstrap is included here
$BadClusBad	Cluster File	Pointers to all the bad clusters on this volume

The attributes of a file on an NTFS volume may contain all or some of the items listed in following table.

Standard Attributes (Standard Information)

Contains standard file attributes, such as time stamps, archive status, and linkage data, plus an attribute list for large files.

Filename

Contains the Unicode file name (up to 255 characters) and the DOS 8.3 file name, created from the Unicode file name.

Security Descriptor

Contains information on ownership, access rights, and other security-related information used by the Security Reference Monitor.

Data

Contains file data for files up to about 1.5K long; otherwise, a pointer to the data.

Index Root

Contains relative location of directory information (index records only).

Index Allocation

Contains the size and location of directory index (index records only).

Bitmap

Contains a bitmapped image of the directory structure (index records only).

Volume Information

Contains the version number and name of a volume.

Extended Attributes

Not used by NT, but contains data that can be used by OS/2 systems

THE RECOVERABLE FILE SYSTEM

As discussed earlier, if the system fails during a file operation, NTFS reconstructs the volume and recovers from the failure. This recovery happens automatically the first time the disk is accessed after a failure, requiring no intervention from the user. Following is a brief description of the process of recoverable writing to an NTFS file:

- The NTFS file I/O driver initiates the write process, including an instruction to the Log File Service to log the transactions involved.
- The data is written to cache memory under control of Cache Manager.
- Cache Manager sends the data to the Virtual Memory Manager for background writing to the disk file, a process called lazy writes, achieved by periodic flushing of the cache to the disk drive.
- The Virtual Memory Manager sends the data back to the NTFS driver, which passes the data through the Fault Tolerant driver to the disk driver.
- The disk driver sends the data to the host controller, which passes the data to the destination fixed disk(s).
- If write caching is enabled on the fixed-disk drive(s), the data is written to on-drive memory, and then transferred locally to the disk. Otherwise, the data is written directly to the disk.
- If the write operation proceeds without an error, the transaction log record is deleted.
- If an error occurs, the transaction log record remains in the transaction table. On the next disk access, the Log File Service detects the log record and restores the corresponding MFT record to its original condition before the write attempt.

FAT AND NTFS

- NTFS file system is more complex than FAT, as NTFS supports greater security and reliability, and these features can generate a performance overhead that is noticeable on some systems, especially large database transactions and certain other types of file I/O, including dealing with very large data files.

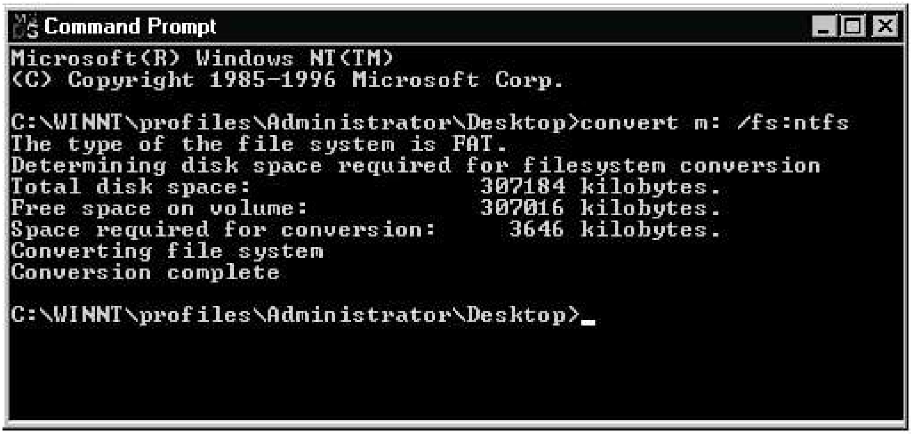
- NTFS is more robust and reliable than FAT. NTFS's capability to recover the file system after system failures or transaction failures and its fault tolerant options are critical to many users.
- The FAT file system is usable by all three operating systems, DOS, Windows95/98 and Windows NT, but NTFS is usable only by Windows NT.
- NTFS is way ahead FAT, as far as security is concerned. Although you can protect a FAT volume through Windows NT's security database on a user-by-user basis, the levels of security you can apply are not as comprehensive as with NTFS.

CONVERTING TO NTFS

The CONVERT.EXE utility is a command-line utility that can convert HPFS and FAT partitions over to NTFS.

```
Syntax      CONVERT [drive letter] /fs:ntfs
```

where [drive letter] is the drive for the partition you are converting. You cannot convert the boot partition while it is active, so if the CONVERT command is attempted on the boot partition, an entry is written to the Registry that will initiate the conversion the next time the system is booted. Also you can't convert back to FAT or HPFS or FAT to HPFS using this utility.



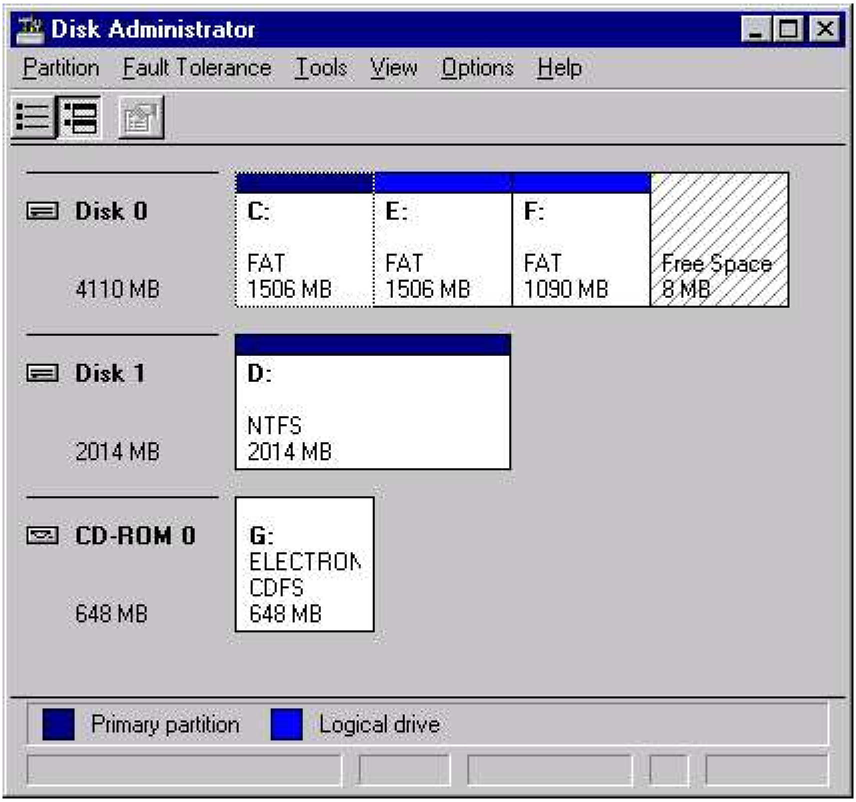
```
Microsoft(R) Windows NT(TM)
(C) Copyright 1985-1996 Microsoft Corp.

C:\WINNT\profiles\Administrator\Desktop>convert m: /fs:ntfs
The type of the file system is FAT.
Determining disk space required for filesystem conversion
Total disk space:                 307184 kilobytes.
Free space on volume:             307016 kilobytes.
Space required for conversion:      3646 kilobytes.
Converting file system
Conversion complete

C:\WINNT\profiles\Administrator\Desktop>_
```

Fig 6.1 Converting to NTFS using Convert command

DISK ADMINISTRATOR

Disk Administrator is the utility to handle the physical and logical drive after installation of NT. This utility is available only to member of Administrative group of NT server.

You can start Disk Administrator by clicking **Start ➢ Program ➢ Administrative Tools (Common) ➢ Disk Administrator**. You can also start Disk Administrator by executing the program WINDISK.EXE. As seen in Fig 6.2, Disk Administrator shows a graphical representation of your physical hard drives and CD-ROM drives. You can see at a glance the different partitions and their size, the volume names, the file systems in use, the drive letter assignments, and the amount of free space that is available for creating new partitions.



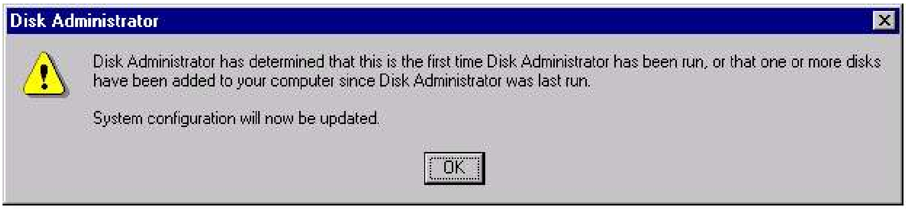
Disk 0
4110 MB
C:
FAT
1506 MB
E:
FAT
1506 MB
F:
FAT
1090 MB
Free Space
8 MB

Disk 1
2014 MB
D:
NTFS
2014 MB

CD-ROM 0
648 MB
G:
ELECTRON
CDFS
648 MB

Fig 6.2 The Disk Administrator

When you run the Disk Administrator for the first time, it will prompt you to to allow Disk Administrator to write a nondestructive signature to each of your hard drives. This signature helps Windows NT to identify if a change of hardware has occurred. This prompt will appear each time you add a new hard drive to your system.

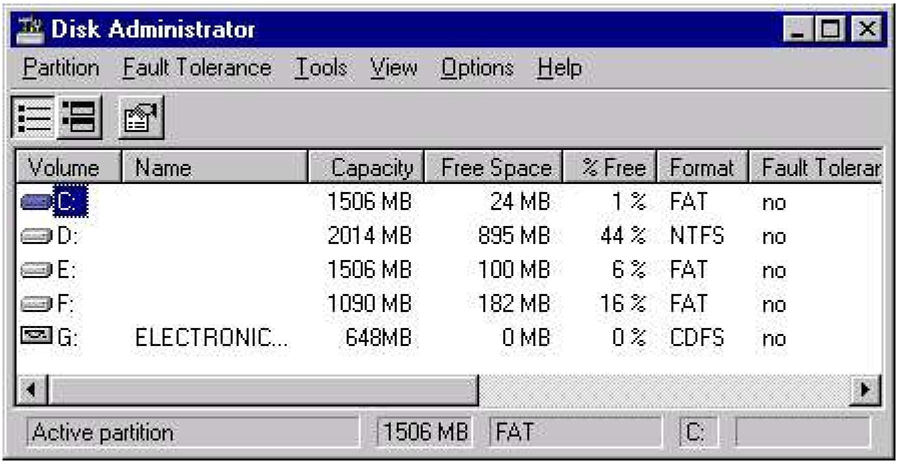


Disk Administrator has determined that this is the first time Disk Administrator has been run, or that one or more disks have been added to your computer since Disk Administrator was last run.

System configuration will now be updated.

Fig 6.3 Confirmation for updating system configuration

There exist another view of Disk Administrator, called Volumes view shown in Fig 6.4. Whereas Disk Configuration view (Fig 6.2) shows unpartitioned space, Volumes view shows only partitioned volumes, although Volume view does show the capacity of partitioned drives.



Volume	Name	Capacity	Free Space	% Free	Format	Fault Tolerar
C:		1506 MB	24 MB	1 %	FAT	no
D:		2014 MB	895 MB	44 %	NTFS	no
E:		1506 MB	100 MB	6 %	FAT	no
F:		1090 MB	182 MB	16 %	FAT	no
G:	ELECTRONIC...	648MB	0 MB	0 %	CDFS	no

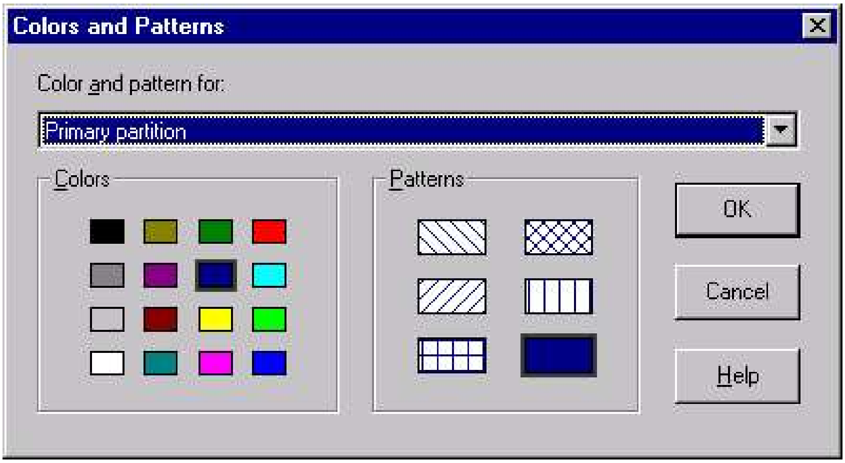
Active partition | 1506 MB | FAT | C:

Fig 6.4 Volume view of Disk Administrator

To switch in between Disk Configuration view and Volume view, press Ctrl+V for Volumes view or Ctrl+D for Disk Configuration view. or you can select the required view from the view menu.

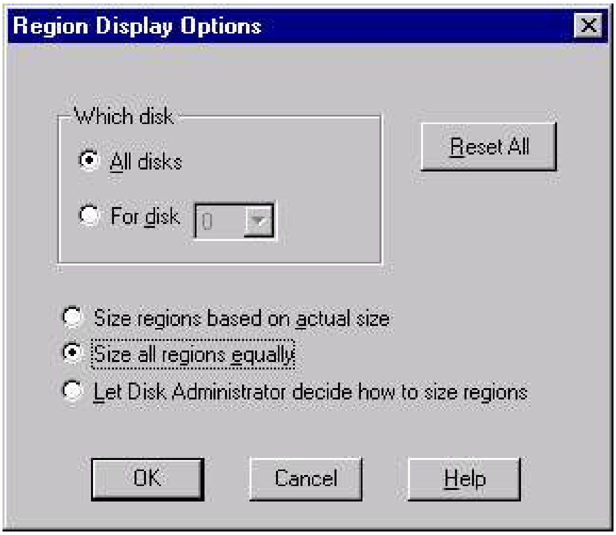
You can further configure you Disk Administrator as per your requirement using Option menu. The Option menu lets you display or hide the Status bar, Legend and Toolbar. It also provides you option to change the colours and patterns that used as a legend to identify a primary partition, a logical drive, a stripe set, a mirror set, and a volume set. Use **Option ➤ Colours and Patterns** option to define the colours. (Fig 6.5)

The Region Display Options (Fig 6.6) enables you to control the size relationship for each partition/logical disk on a drive. If you choose the **Size All Regions Equally** option, each logical drive is shown using the same size box within the drive's overall box. Selecting the **Size Regions Based On Actual Size** option causes Disk Administrator to size the box for each logical drive proportionally to its capacity.



Color and pattern for: Primary partition

Fig 6.5 Changing Colour & Patterns



Which disk

● All disks

○ For disk 0

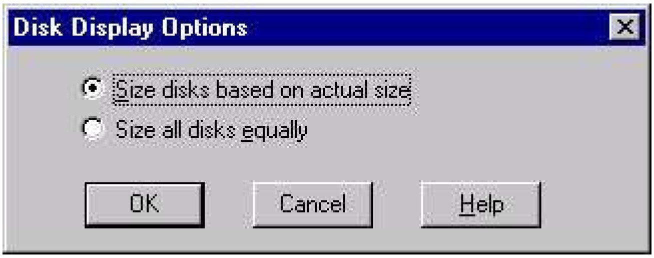
○ Size regions based on actual size

● Size all regions equally

○ Let Disk Administrator decide how to size regions

Fig 6.6 Region display dialog box

You can also configure Disk Administrator to show all drives the same size by choosing the **Option ➢ Disk Display**. (Fig 6.7)



● Size disks based on actual size

○ Size all disks equally

Fig 6.7 Disk Display options

WORKING WITH PARTITIONS

You must have used FDISK in DOS to create partition on a hard disk. This utility allows you to create two types of partition - primary partition for Operating System and an extended partition. In the extended partition, you have various logical drives as logical storage area. (There is a difference between logical drive and partition. Logical drive is a part of extended partition).

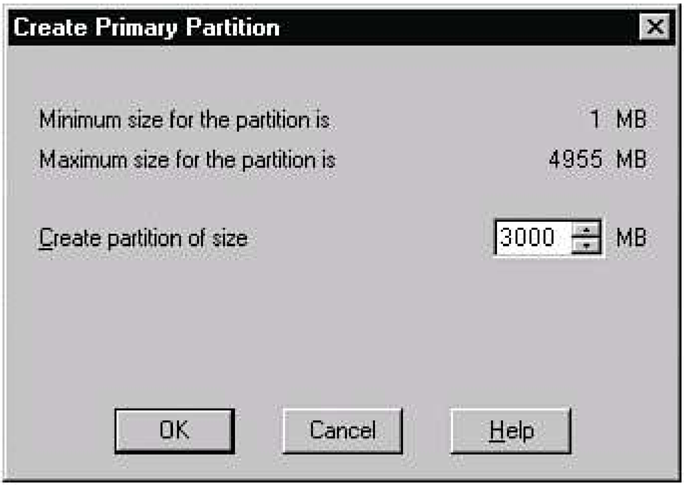
Windows NT allows upto four partition on the hard disk, out of which atmost one could be the extended partition. An extended partition could contain one or more logical drives.

Once you create the partition on the harddisk, you could format it as FAT, NTFS or HPFS. The FAT partition as well as logical drive will be recognised by DOS also. An extended partition is not limited to a single file system. You can create both FAT and NTFS file systems within an extended partition. You first create the extended partition, create multiple logical drives in the partition, and then format each logical drive according to the file system you want on it.

Creating Primary Partition

To create a primary partition, select the hard disk by clicking on the disk noted as free space, and choose **Create** from the Partition menu. This brings the Create Primary Partition dialog box as shown in Fig 6.8.

Enter the size in MB for primary partition. You can create the extended partition in the left over space. Click **Ok** and the new partition will appear on the screen.


Create Primary Partition

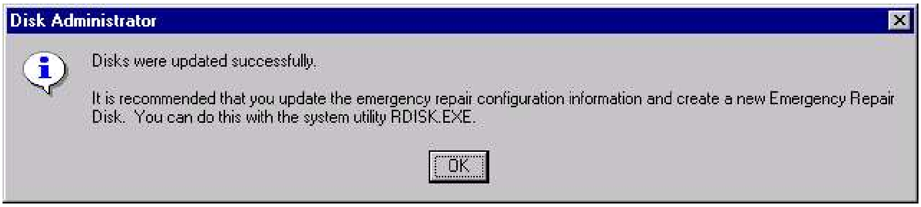
Minimum size for the partition is 1 MB

Maximum size for the partition is 4955 MB

Create partition of size 3000 MB

Fig 6.8 Creating Primary Partition

To complete the partition creation process, select **Partition ➤ Commit Changes Now**. You can also exit Disk Administrator to commit changes. Until you commit the changes, the disk remains unaffected and you can't apply any further process (Formatting etc.) to the disk. When you say in affirmative to the Commit Changes dialog box, it brings the confirmation dialog box.



Disks were updated successfully.

It is recommended that you update the emergency repair configuration information and create a new Emergency Repair Disk. You can do this with the system utility RDISK.EXE.

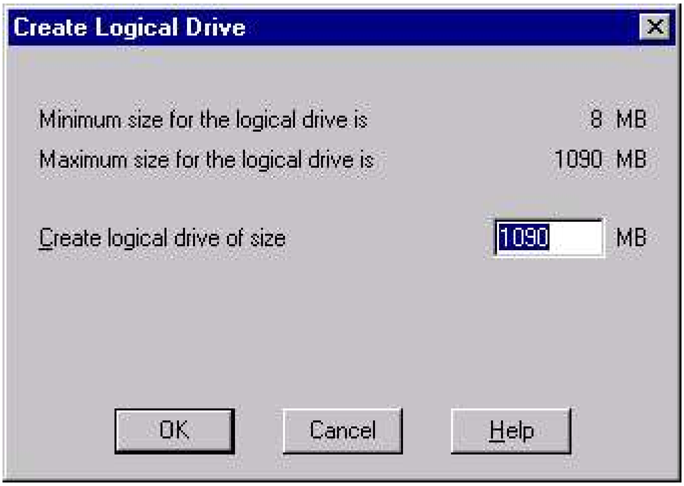
Fig 6.9 Committing Changes

Creating Extended Partition

You can create one extended partition on a disk. As discussed earlier, the extended partition can contain multiple logical drives. To create an extended partition, select the unpartitioned free space in which you want to create the extended partition and choose **Partition ➢ Create Extended**. This brings Create Extended Partition dialog box similar to shown in Create Primary Partition dialog box.

Creating Logical Drive

After creating the extended partition, you must create at least one logical drive in the partition. To create a logical drive, choose **Partition ➢ Create** to display Create Logical Drive dialog box. (Fig 6.10). Enter the desired size for the logical drive in the Create Logical Drive of Size text box and then choose OK.



Minimum size for the logical drive is 8 MB

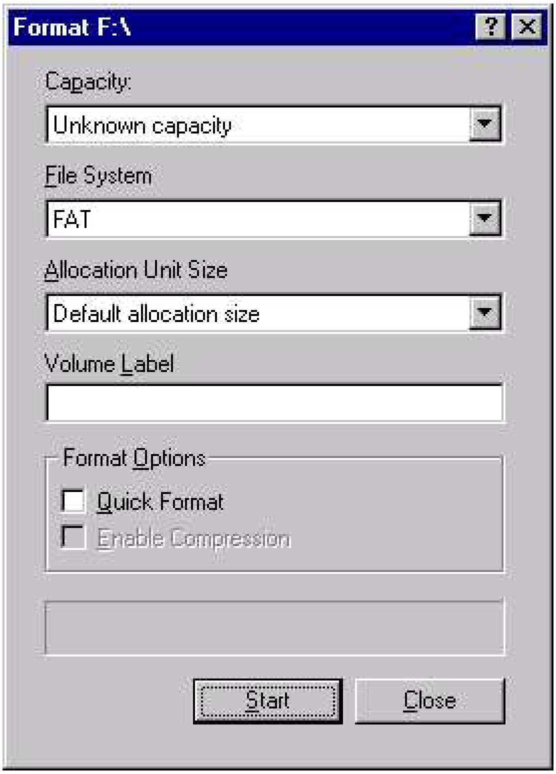
Maximum size for the logical drive is 1090 MB

Create logical drive of size 1090 MB

Fig 6.10 Creating Logical Drive

FORMATTING PARTITION

Once you create the partition and logical drives and committed the changes, it's time now to format each partition. To format a partition, select the partition on the Disk Administrator by clicking on it and select **Tools ➤ Format**. (Remember, the Format option will remain disabled, if you don't commit the changes.) This brings the Format dialog box. Fig 6.11.


Format F:\

Capacity:
Unknown capacity

File System
FAT

Allocation Unit Size
Default allocation size

Volume Label

Format Options
□ Quick Format
□ Enable Compression

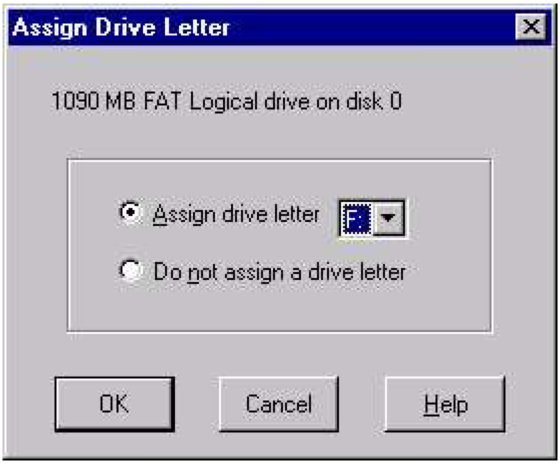
Fig 6.11 Formatting Partition

Here select the appropriate File System in which you want to format the disk partition. You can also define the cluster size for NTFS in the Allocation Unit Size. You can choose among 512, 1,024, 2,048, and 4,096 bytes. You can Quick Format the disk, if it is already formatted. The Enable Compression option remains disabled for FAT File System. Now click **Start** button to Start Format.

The bottom bar displays the Format Status. Once format is complete the Format Complete message appears.

ASSIGNING A LETTER TO DRIVE

You can assign a drive letter of your choice to any drive thus giving you complete flexibility over drive identification. To assign a particular letter to drive, click on the partition or logical drive and select **Tools ➢ Assign Drive Letter**. This brings the Assign Drive Letter dialog box.



Assign Drive Letter

1090 MB FAT Logical drive on disk 0

● Assign drive letter F:

○ Do not assign a drive letter

Fig 6.12 Assigning Drive Letter to the partition

From the Assign Drive Letter drop-down list, choose the letter you want to assign to the drive and then choose **OK**. Or, if you don't want to use a drive letter at all, select the **Do Not Assign a Drive Letter** option button and then choose **OK**. If you select this option, Disk Administrator removes the existing drive letter ID from the drive.

FAULT TOLERANCE

Windows NT plus point is that it provides reliability. It has many features to increase reliability and the integrity of your system. Fault Tolerance is one of them.

A fault-tolerant disk system is intended to provide mechanisms for reducing the likelihood of data loss in the event of a failure. There are three different techniques, with which Windows NT provides fault tolerance to the system.

- Redundant Array of Inexpensive Disks (RAID)
- NTFS Recoverability
- Sector Sparing

RAID (REDUNDANT ARRAY OF INEXPENSIVE DISKS)

A redundant array of inexpensive disks (RAID) uses multiple fixed-disk drives, high-speed disk controllers, and special software drivers. RAID was designed to remove the bottleneck of low performance of Disk drives. It used multiple-fixed disk and spread the data in all of them in parallel, and allowing the same data to be retrieved from different locations. This increases the performance of hard disk subsystem.

RAID has also tools to increase the safety of your data by spreading it over multiple disk drives and then calculating and storing parity information. This redundancy allows any one drive to fail without causing the array itself to lose any data.

All commercial RAID subsystems use the Small Computer System Interface (SCSI). The latest Ultra-wide SCSI host adapters for the PCI bus can deliver up to 40M per second (40M/s) of data to and from the PC's RAM.

The basic concept behind RAID is a technique called striping. When the system tries to write a block of information to the array, the array controller (NT) breaks the information into smaller chucks of a predetermined size and writes these chunks in parallel across all drives in the array.

There are six kinds of RAID implementations, each of which works in a different way. The NT server can handle 0, 1 and 5 levels, also known as the striping without parity, Disk Mirroring, and striping with parity respectively.

RAID 0 - Stripping :

It is not considered as proper RAID, as it provides high efficiency (fast writing and reading) but no redundancy. It stripes data across various drives thus allowing simultaneous I/O to the drives. This improves the performance of the system a lot but if one drive fails in a RAID 0 array, the data on all drives on the array becomes inaccessible.

RAID 1 : Disk Mirroring:

This provides hundred percent redundancy at the cost of performance of the system. It makes two complete copies of everything to mirrored or duplexed pairs of disk drives. Therefore if you loose data on one drive, you have its clone available with you. But in writing the contents to other drive, performance is lost. Also it requires double the investment on the storage.

But at the same time, the Read performance is greatly enhanced, as reading can be done from any of the drive having its head closest to the data.

RAID 1, therefore, provides a high level of data security by replicating all data, an increase in read performance by allowing either physical drive to fulfill the read request, and a lower level of write performance due to the necessity of writing the same information to both drives.

RAID 2

RAID 2 is a proprietary RAID architecture and it distributes the data across multiple dedicated disks to store parity information. It stripes data bit by bit across these drives in parallel and records parity information to the dedicated parity drives for complete redundancy.

RAID 2 isn't a good choice for random-access applications, which require frequent, small reads and writes.

RAID 3

RAID 3 stripes data across drives, usually at the byte level, although bit-level implementations are possible. Unlike RAID 2, RAID 3 dedicated only one parity disk. A single parity disk creates bottlenecks for writing because the parity information must be written before the next write can take place. Similar to RAID 2, RAID 3 is optimized for long sequential disk access in applications such as imaging and digital video storage, and is inappropriate for random-access

RAID 4

RAID 4 is improved form of RAID 3, and stripes data at the block or sector level rather than at the byte level. This helps in better read performance than RAID 3 for small random reads but hardly address the bottleneck caused by the fact that write updates often have to wait to access the parity drive.

RAID 5 : Stripping with Parity

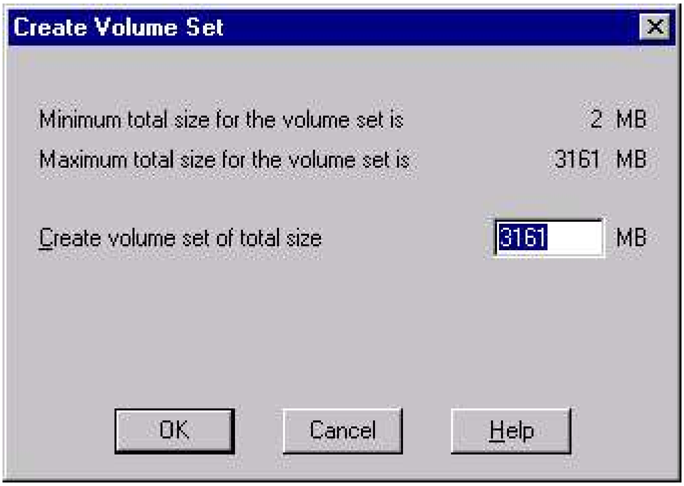
RAID 5 stripes both user and parity data across all the drives in the array, consuming the equivalent of one drive for parity information. With RAID 5, all drives are of the same size, and one drive is unavailable to the operating system. The parity information spreads equally across all the drives, thereby allowing both parallel reads and writes.

Windows NT includes software support for RAID levels 0 - Disk Stripping, 1 - Disk Mirroring and 5 - Disk Stripping with Parity. These are the most common RAID implementations. All these options are included in Disk Administrator. Besides these, Disk Administrator also provides another disk management function called Volume Set.

VOLUME SETS

Oftenly confused with RAID, Volume Set neither provides the data safety of RAID 1 or RAID 5, nor the performance benefits of RAID 0. It simply group together a bunch of drives and the group in a single logical drive name.

To create a Volume Set, select the first area (free space) by clicking on it, press **Ctrl** key and select second area and so on. Once all the free spaces to be grouped together has been selected, select **Partition ➢ Create Volume Set** to bring the Create Volume Set dialog box. (Fig 6.13)



Create Volume Set

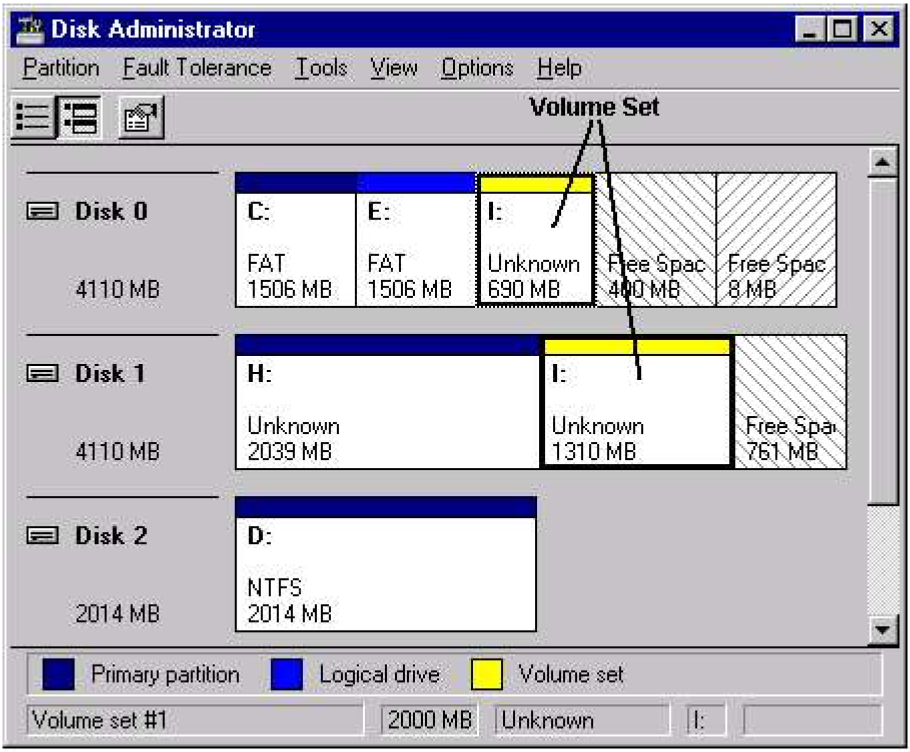
Minimum total size for the volume set is 2 MB

Maximum total size for the volume set is 3161 MB

Create volume set of total size 3161 MB

Fig 6.13 Creating Volume Set

Select the required size and Click **OK**. It creates the required set as shown in Fig 6.14. Note the same drive letter assigned to volume set.



Disk 0 4110 MB — C: FAT 1506 MB | E: FAT 1506 MB | I: Unknown 690 MB | Free Spac 400 MB | Free Spac 8 MB

Disk 1 4110 MB — H: Unknown 2039 MB | I: Unknown 1310 MB | Free Spa 761 MB

Disk 2 2014 MB — D: NTFS 2014 MB

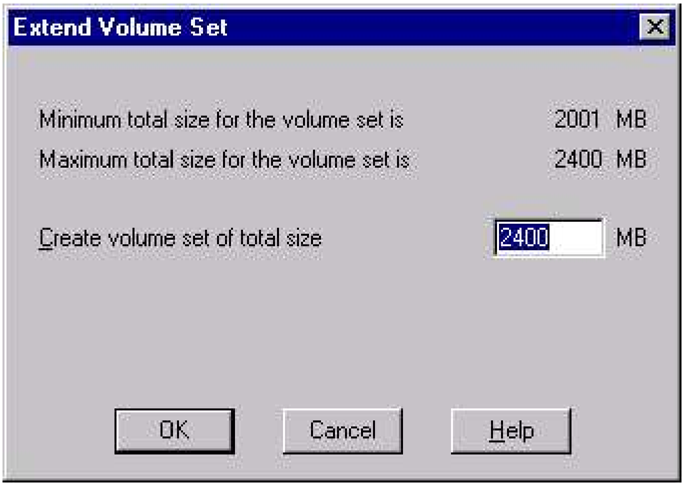
■ Primary partition ■ Logical drive ■ Volume set

Volume set #1 | 2000 MB | Unknown | I:

Fig 6.14 Disk Administrator after creating Volume Set

The basic disadvantage of the volume set is that it doesn't provide any redundancy. Its size also can not be reduced. To decrease the volume set, you must delete the existing volume set and create a new one. You cannot also combine two volume sets, nor add a logical drive to a volume set.

You can extend the volume set only if the volume set supports the NTFS. To extend the volume set select the free space you want to add to NTFS partition of the disk and select **Partition ➤ Extend Volume Set**. This brings the Extend Volume Set dialog box. Specify the MB and click **OK**.



Minimum total size for the volume set is 2001 MB

Maximum total size for the volume set is 2400 MB

Create volume set of total size 2400 MB

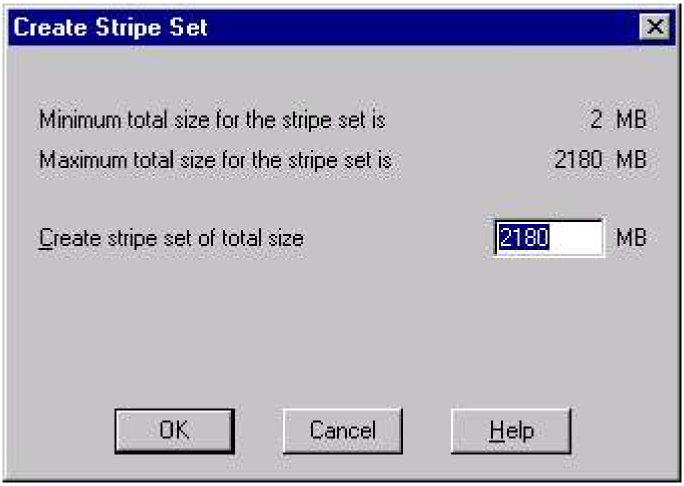
Fig 6.15 Extending Volume Set

STRIPE SET - RAID 0

Disk Stripping offers no fault-tolerance and slow performance in writing but offers increased performance in reading. In Stripe set partitions are of equal size. When you create a disk stripe from free space on your disks, each member (disk) of the stripe set is divided into stripes. Then when you write data to a stripe set the data is distributed over the stripes of the various members. The data is not stored onto a single member even if there is room in that member for the entire file. Windows NT Server allows a stripe set to comprise from two to 32 individual disks.

To create a RAID 0 stripe set, select the free space on one disk. Press Ctrl and select the free space on second disk. Similarly you can select as many disk you want to include in the stripe set. The size of the partition is decided by the minimum available space in any disk. (i.e. if one disk has 100 MB, other has 200 MB and third has 400 MB, the maximum size of stripe set will be 300 MB, as first disk can't have a partition more than 100 MB. These 300 MB will be distributed equally - 100 MB over three disk).

After selecting all the free space on different physical drive, select **Partition ➢ Stripe Set** to bring up the Create Stripe Set dialog box.



Minimum total size for the stripe set is 2 MB

Maximum total total size for the stripe set is 2180 MB

Create stripe set of total size 2180 MB

Fig 6.16 Creating Stripe Set

Here the maximum size of Stripe set is 2(no. of disk) x 1090 (The minimum space available on any disk) as shown in Fig 6.17.

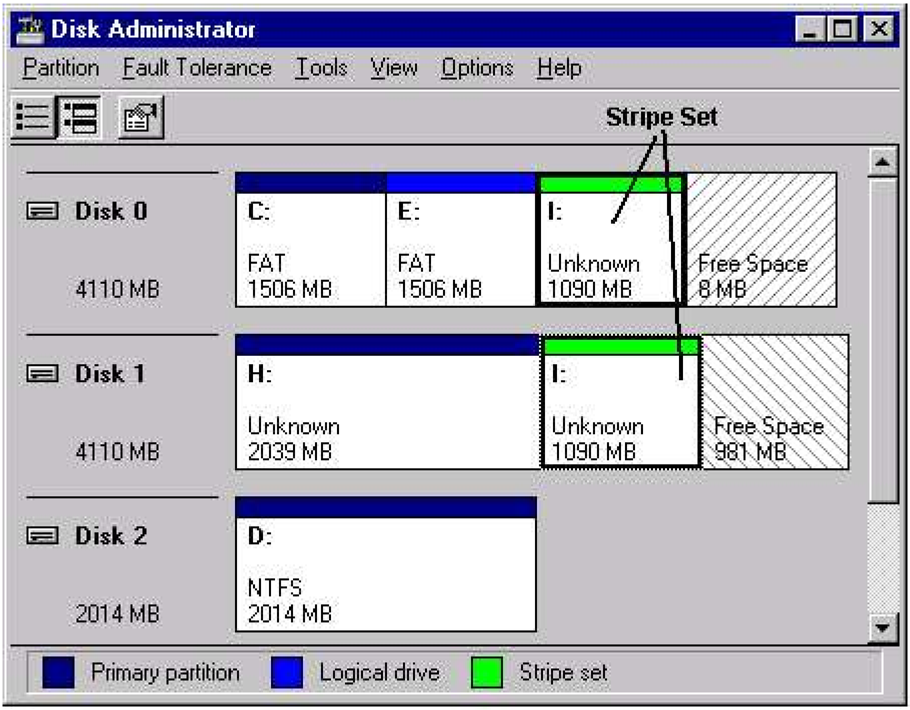


Fig 6.17 Disk Administrator after creating Stripe Set

MIRRORING - RAID 1

The RAID 1 fault-tolerance, Mirroring enables you to create an exact mirror of one disk onto another disk. It requires atleast two drives to create the mirror of one onto other. The hard disks need not to be identical but mirrored drive should be as large as drive to be mirrored.

To create a mirror drive, you must first create a standard formatted volume, and then create the mirror drive. Mirroring creates a formatted volume of the same size as the new standard volume, but on another physical drive.

To create a mirror, select the standard volume, whose mirror you want to create. Now, hold down **Ctrl** key and click on the free space where you want to create the mirror. Now select **Fault-tolerance ➢ Establish Mirror** option to create the mirror.

Select **Partition ➢ Commit Changes Now**. Windows NT Server creates the mirror set and assigns the drive letter of the first drive of the set (D in fig. 6.18).

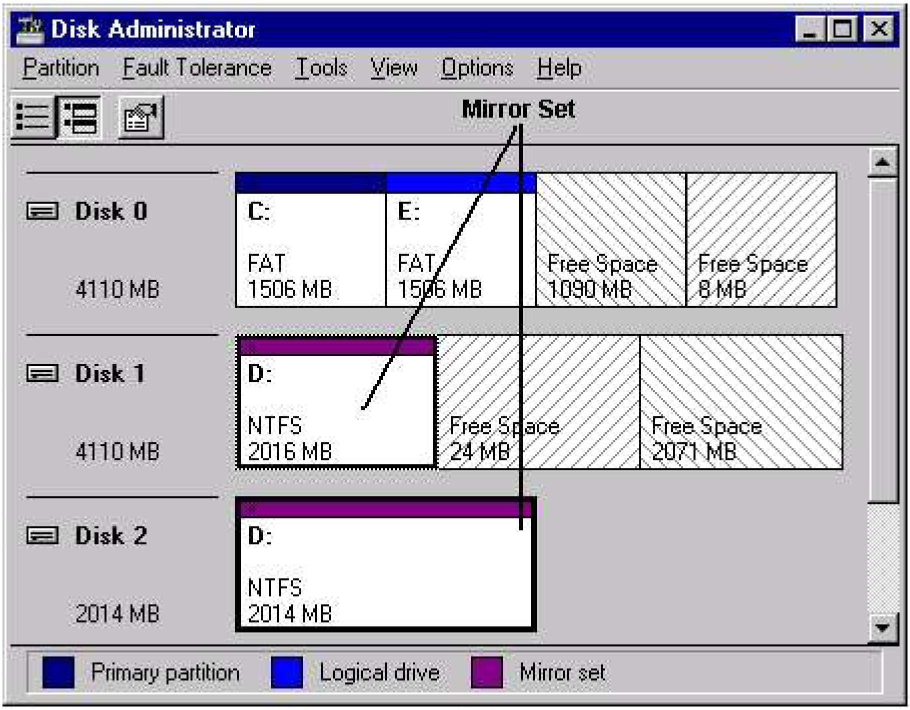
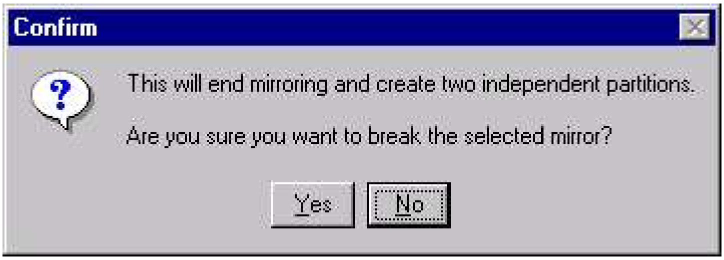


Fig 6.18 Disk Administrator after creating Mirror Set

Whenever you want to reclaim disk space, remove a hard drive, or rearrange your partitions, you need to break a mirror. To break a mirror, select the partition you would like to no longer mirror (or select its mirror) and choose **Fault Tolerance ➢ Break Mirror**. As shown in Figure 6.19, you will first be warned that breaking the mirror will result in a two separate partitions.



Confirm

This will end mirroring and create two independent partitions.

Are you sure you want to break the selected mirror?

Fig 6.19 Breaking Mirror Set

Click **Yes** to confirm the mirror break. Now both the partitions are assigned different drive letters. Mirrored partition retains the same data it had while it was part of the mirror set.

DUPLEXING

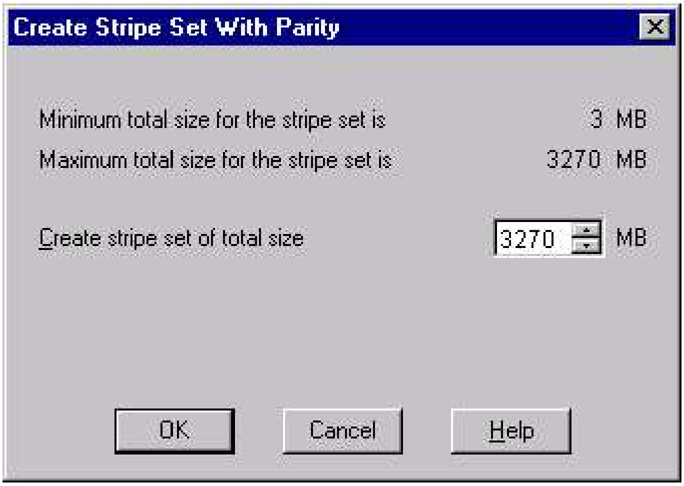
In mirroring, both the hard disk were on the same controller, thus if controller failure occurs, both disk will stop working. In duplexing the two disk drives of similar size are on two disk controllers. The advantage of Duplexing is that even if one of controller fails, only one of the drives is affected, the other controller continues to function and hence the disk drive.

STRIPPING WITH PARITY - RAID 5

Disk stripping with Parity - a RAID 5 fault-tolerance is also supported by Windows NT Server. Windows NT Server allows as many as 32 drives in a striping set. Whereas data from the stripe set without parity is unrecoverable, the data from the stripe set with parity is generally recoverable. If more than one disk of the 3 to 32 hard disk drives fail, you will not be able to recover your data. But striping with parity has a greater initial cost than Disk Mirroring because it requires a minimum of three disks.

The process of creating a stripe set with parity is very similar to that used to create a RAID 0 stripe set. While a RAID 0 stripe set can be created on only two physical drives, a RAID 5 stripe set with parity requires a minimum of three drives-one for parity information.

To create a stripe set with parity, select free space on a disk drive and select two more free space using the Ctrl key. Now choose **Fault-tolerance ➢ Create Stripe set with parity**. This brings the Create stripe with parity dialog box. (Fig 6.20)


Create Stripe Set With Parity

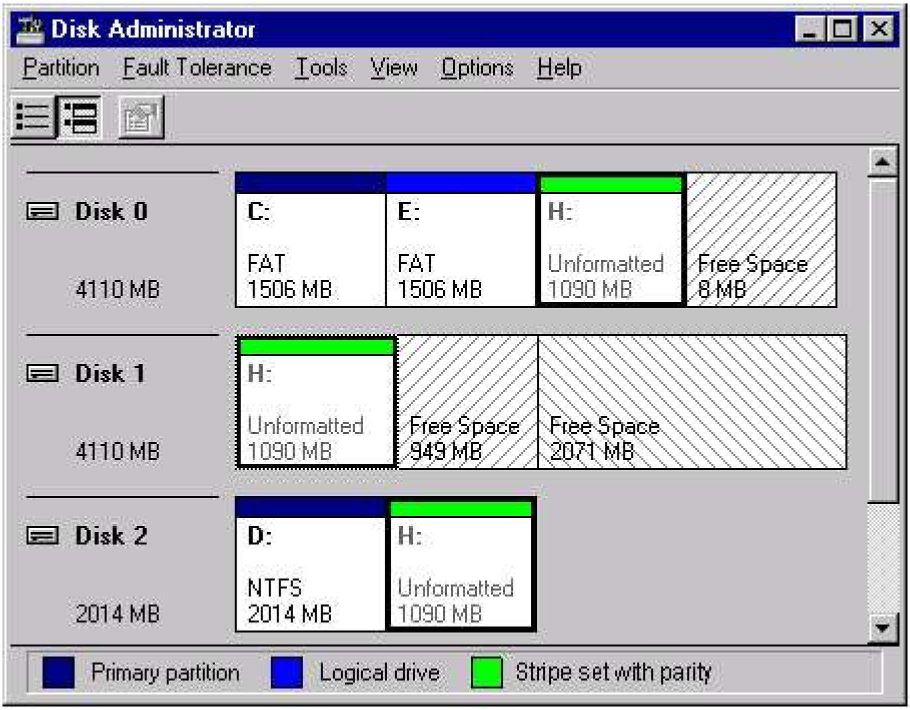
Minimum total size for the stripe set is 3 MB

Maximum total size for the stripe set is 3270 MB

Create stripe set of total size 3270 MB

Fig 6.20 Creating Stripe Set with Parity

Here the maximum size of Stripe set is 3(no. of disk) x 1090 (The minimum space available on any disk) as shown in Fig 6.21.


Disk Administrator

Disk 0 4110 MB: C: FAT 1506 MB | E: FAT 1506 MB | H: Unformatted 1090 MB | Free Space 8 MB

Disk 1 4110 MB: H: Unformatted 1090 MB | Free Space 949 MB | Free Space 2071 MB

Disk 2 2014 MB: D: NTFS 2014 MB | H: Unformatted 1090 MB

■ Primary partition 🟦 Logical drive 🟩 Stripe set with parity

Fig 6.21 Disk Administrator after creating Stripe Set

RECOVERING FROM HARD DISK FAILURES

FAILED MIRROR SET

If one half of the mirror set gets destroyed, you need to break the mirror set to get the good data that you've backed up. Once mirror set broken, the good half of the mirror set is assigned the drive letter that belonged to the earlier mirror set. The half that is crashed is now called an orphan and is set aside by the fault tolerance system so that no one attempts to write to that part of the disk. When you reboot, the dead disk disappears.

FAILED STRIPE SET

If striped set with parity is damaged, you can regenerate the information stored there from the parity information stored in the rest of the set. You can even do this if one of the member hard disks has been low level formatted. To recover the data, install a new disk and reboot the system so that the system can see the new disk. Then go to the Disk Administrator and select the stripe set that you want to fix and a new piece of free space that is equal in size to the other members of the stripe set. Choose **Regenerate** from the fault tolerance menu, quit the Disk Administrator and restart the computer.

When you restart the computer, the fault tolerance driver collects the information from the stripes on the other member disks and then recreates it onto the new member of the stripe set.

EXERCISE

Fill in the Blanks:

1. __________ is one of the fields in the MFT for each file record.
2. NTFS creates _______ of ______ size if the file attributes increases.
3. ____________ command is used to convert FAT to NTFS.
4. RAID level 0 is called as _____________
5. RAID stands for ______________________
6. The process by which server maintains a copy of other servers data is called as _______.
7. Windows NT allows upto _______ partition on the hard disk.
8. Mirroring is RAID ____ level.
9. RAID 0 is ___% redundancy where as RAID 1 is ____% redundancy.

State True or False:

1. NTFS partition is recognized by MS-DOS
2. You can convert NTFS partition to FAT partition.
3. CDFS provides supports for CD-ROM file system.
4. Volume View of Disk Administrator displays the free space on each partition.
5. Logical Drive is the part of extended partition.
6. Windows Nt allows to change the drive letter.
7. In Duplexing the two drives are on two different controllers.
8. Mirroring requires three drives.
9. RAID 5 increases the writing and reading speed.
10. The data in RAID 5 is equally distributed among the drives.

Answer the following:

1. Why NTFS is termed as recoverable File System?
2. What is Master File Table?
3. Discuss the advantages & disadvantages of various file system supported on Windows NT.
4. Compare FAT & NTFS.
5. Discuss various type of partition you can make on the disk.
6. What do you understand by the Fault Tolerance System?
7. What is the need for having a backup? Differentiate between Full Backup and incremental backup?
8. What is the difference between Data replication and Data Backup?
9. How you determine the size of the Volume Set?
10. What do understand by RAID? Discuss various RAID levels.

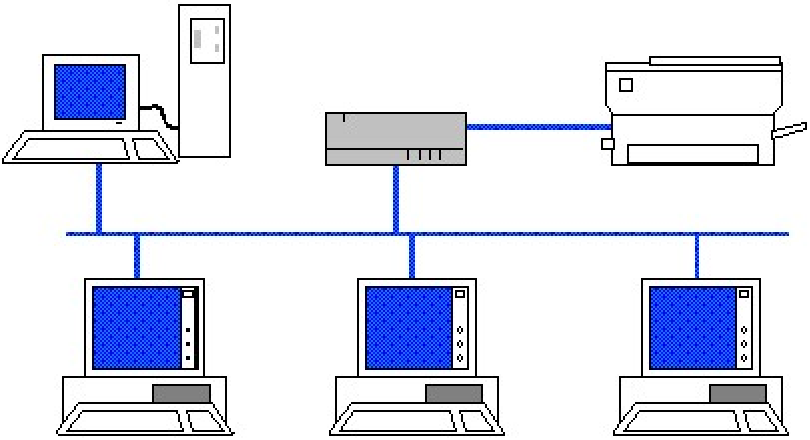
11. If you create a stripe set using three disk - Disk1 has 850 MB space, Disk 2 has 825 MB space and Disk three has also 825 MB of space, what will be the minimum and maximum size of the stripe set.

Practice the following:

1. Connect three hard drives to your system and create a Volume set using these drives, using Disk Administrator tools of Windows NT.
2. Now create a Mirror. Can you mirror a smaller capacity disk to larger capacity one or do they have to be the same size? Format one partition with DOS and one with NTFS.
3. You have to create a stripe set with parity, how many disks will you use? Can a stripe set be made with two disks?

CHAPTER 7

The Control Panel



SETTING UP CONTROL PANEL

To see the Control Panel, choose **Start ➢ Settings ➢ Control Panel**. The icons in the Control Panel window may include these programs, depending on what Windows NT components and other software you have installed:

Accessibility Options The Accessibility Properties dialog box lets you configure Windows NT's keyboard, sound, display, mouse, and other options, for people with disabilities.

Add/Remove Programs The Add/Remove Programs Properties dialog box helps you install new programs or uninstall programs you no longer use.

Console Console is a Control Panel program that enables you to configure the default appearance of character-based windows (consoles) and Command Prompt windows.

Date/Time The Date/Time Properties dialog box lets you set the date, time, and time zone where you are located.

Devices Used to stop and start devices.

Dialup Monitor Display dial-up connection statistics, when you connect using modem etc.

Display The Display Properties dialog box controls the appearance, resolution, screen saver, and other settings for your display.

Find Fast Find Fast builds indexes to speed up finding documents from the Open dialog box in Microsoft Office programs and from Microsoft Outlook.

Fonts The Fonts window lets you install new screen and printer fonts.

Internet The Internet Properties dialog box contains settings for your Web browser and Internet connection.

Keyboard The Keyboard Properties dialog box contains settings that control your keyboard and the cursor.

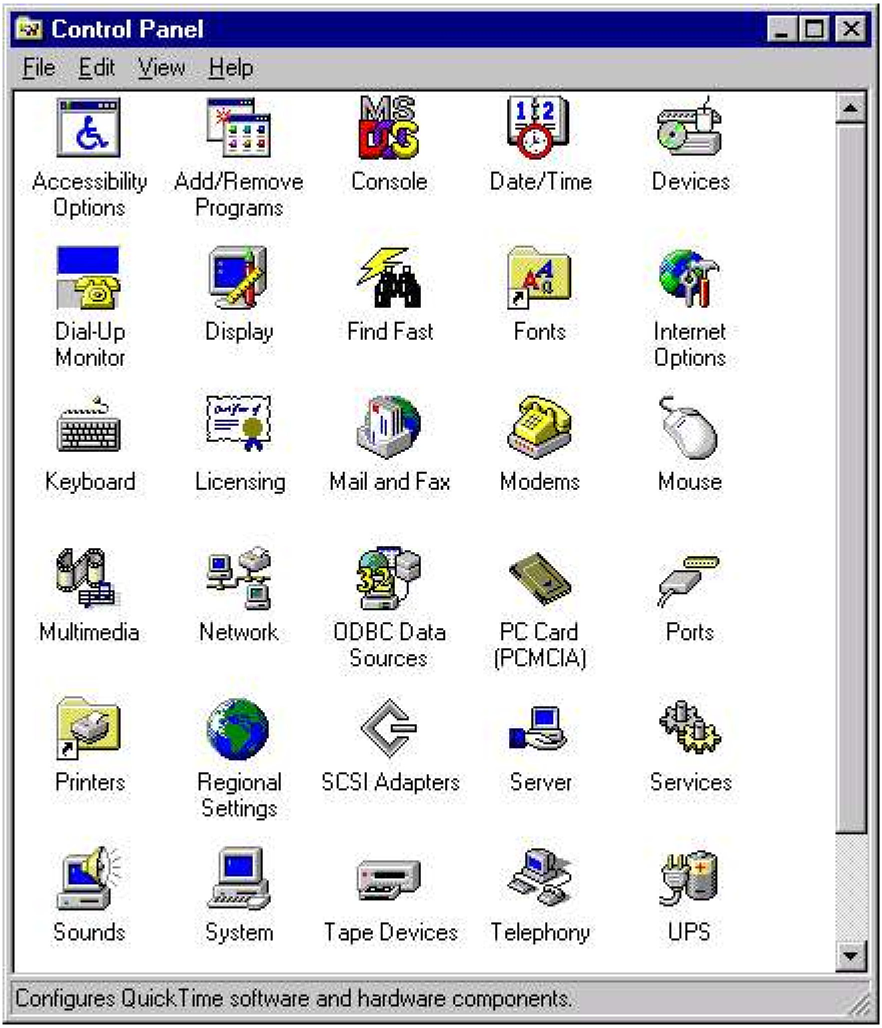
Licensing The Licensing application (available with Windows NT Server only) is used to manage licensing on your Windows NT Server computer.

Modems The Modems Properties dialog box contains settings for how your modem works, and helps you diagnose problems.

Mouse The Mouse Properties dialog box lets you define the buttons on your mouse, and lets you choose how fast you need to double-click, what your mouse pointer looks like on-screen, and whether moving the mouse leaves a trail.

Multimedia The Multimedia Properties dialog box contains settings for the audio, video, MIDI, and audio CD settings of your computer.

Network The Network dialog box contains settings you use when configuring a local area network.



Configures QuickTime software and hardware components.

Fig. 7.1 Control Panel Folder

ODBC Data Source

An ODBC user data source stores information, about how to connect to the indicated data provider. A user data source is only visible to you and can only be used on current machine.

Ports Enables you to specify the communications settings for a selected serial (COM) port.

Printers The Printers dialog box includes icons for each printer to which you have access, as well as an icon for adding a new printer.

Regional Settings The Regional Setting Properties dialog box lets you tell Windows NT the time zone, currency, number format, and date format you prefer to use. Not all programs follow the settings you choose, but many do.

SCSI Adapter The SCSI Adapters application is used to install, configure, and manage SCSI adapters.

Server Used to view and manage the server properties of this computer.

Services This lets you start, stop, pause, or continue each of the services available on the computer, and to pass startup parameters to the service.

Sounds The Sounds dialog box lets you assign a sound to each Windows event, or events in other programs. For example, you can set your computer to play a fanfare when your e-mail program receives new messages.

System The System Properties dialog box lets you use the Device Manager to change advanced settings for each hardware component of your computer. You can also optimize the performance of your computer.

Tape Drive The Tape Devices application is used to install drivers for tape backup devices and to view the status of tape backup devices connected to your computer.

Telephony The Dialing Properties dialog box contains settings that control how Windows NT dials the phone using your modem.

UPS The UPS application is used to install, configure, and manage an uninterruptible power supply.

ACCESSIBILITY OPTIONS

Windows NT includes the accessibility options for people who have difficulty in typing, reading the screen, hearing noises the computer makes, or using a mouse.

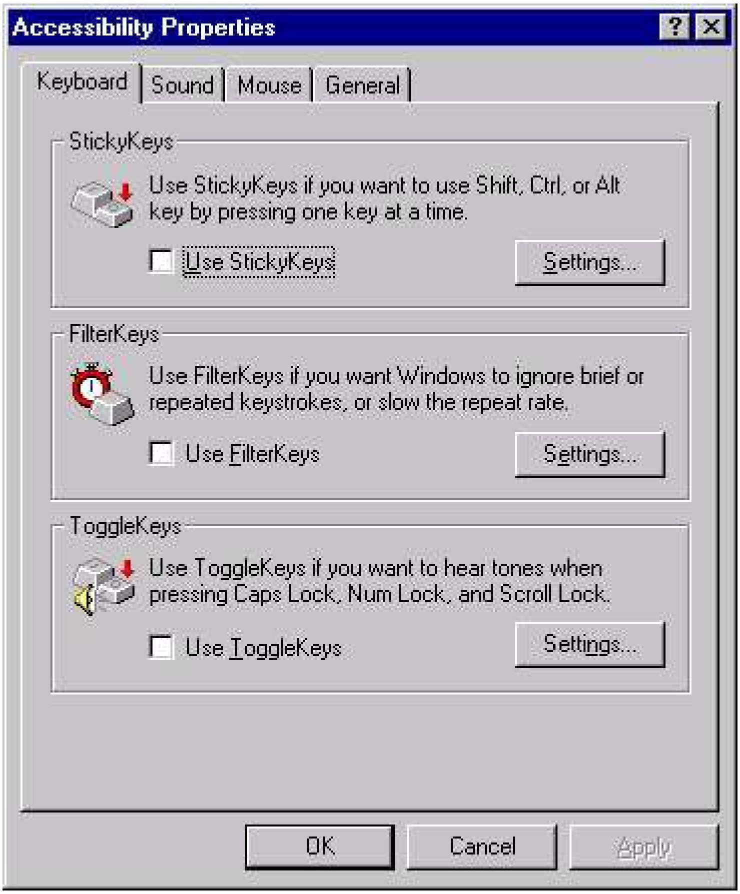
Keyboard aids for those who have difficulty in typing include:

StickyKeys Lets you avoid pressing multiple keys by making keys like the CTRL, SHIFT, and ALT keys “sticky”

- they stay in effect even after they have been released.

FilterKeys “Filters out” repeated keystrokes. Good for typists who have trouble pressing a key once briefly.

ToggleKeys Sounds a tone when the CAPS LOCK, SCROLL LOCK, and NUM LOCK keys are activated.



Use StickyKeys if you want to use Shift, Ctrl, or Alt key by pressing one key at a time.

□ Use StickyKeys

Use FilterKeys if you want Windows to ignore brief or repeated keystrokes, or slow the repeat rate.

□ Use FilterKeys

Use ToggleKeys if you want to hear tones when pressing Caps Lock, Num Lock, and Scroll Lock.

□ Use ToggleKeys

Fig. 7.2 Accessibility Properties dialog box

Visual translation of sounds for those who have difficulty hearing include:

SoundSentry Displays a visual warning when the computer makes a sound.

ShowSounds Displays a caption when the computer makes a sound.

Mouse options for those who dislike or have trouble using a mouse or trackball include:

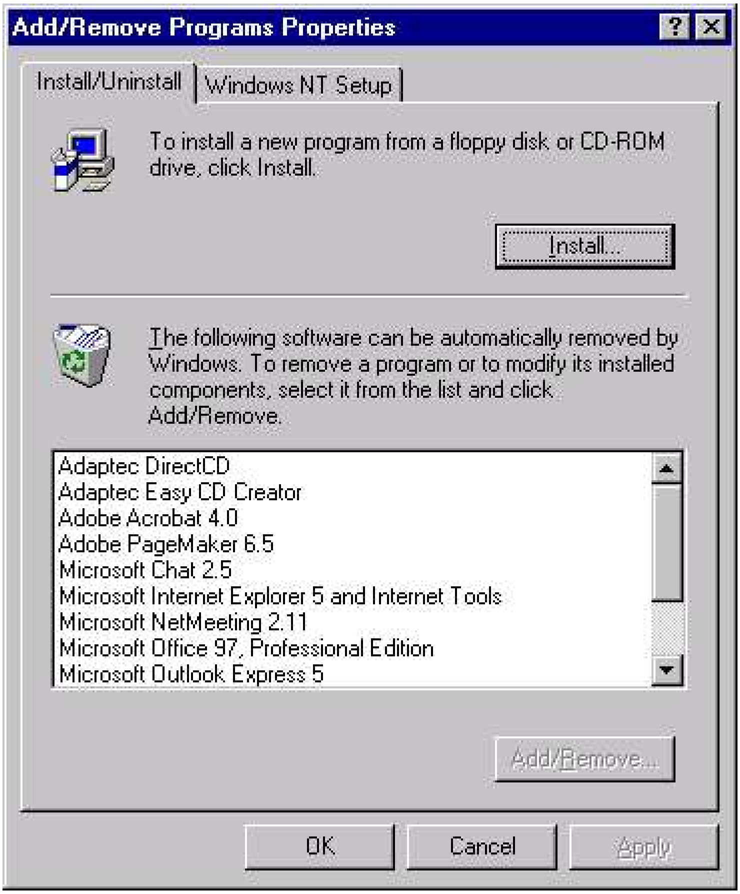
MouseKeys Allows you to use the numeric keypad to control the pointer.

SerialKey Turns on support for alternate input devices attached to the serial port.

To choose **Start ➢ Settings ➢ Control Panel**, run the Accessibility Options program, and click the required tab. (Fig 7.2)

USING THE ADD/REMOVE PROGRAMS

Using Add/Remove Programs to install a program is a good idea, because Windows NT adds the program to the list of programs you've installed, making it easier to uninstall the program later.



To install a new program from a floppy disk or CD-ROM drive, click Install.

The following software can be automatically removed by Windows. To remove a program or to modify its installed components, select it from the list and click Add/Remove.

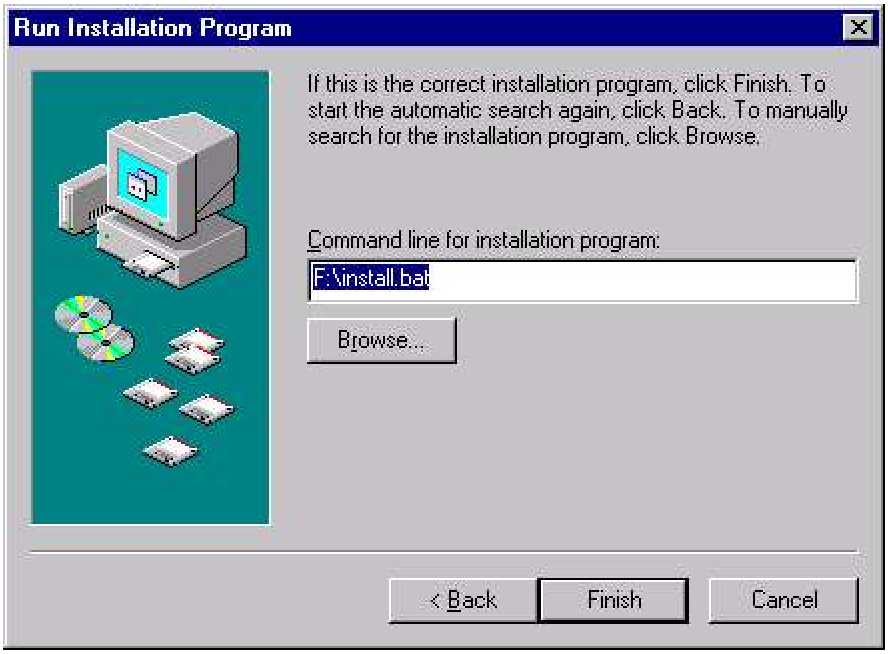
Adaptec DirectCD
Adaptec Easy CD Creator
Adobe Acrobat 4.0
Adobe PageMaker 6.5
Microsoft Chat 2.5
Microsoft Internet Explorer 5 and Internet Tools
Microsoft NetMeeting 2.11
Microsoft Office 97, Professional Edition
Microsoft Outlook Express 5

Fig. 7.3 Adding/removing a Program

Follow these steps to use the Add/Remove Programs command to help you install a program:

- Choose **Start ➢ Settings ➢ Control Panel**. You see the Control Panel window.

- Run the Add/Remove Programs program. If the icons are underlined, your desktop is configured in Web style, so click the icon once. If the icons are not underlined, your desktop is configured in Classic style, so double-click the icon. You can control whether you need to single- or double-click icons to run programs.
- You see the Add/Remove Programs Properties dialog box, shown in Figure 7.3. If the Install/Uninstall tab isn't selected, click it. The box in the lower half of the window lists the programs you have already installed on your system.
- Click the **Install** button. If you are installing a program from a floppy disk or CD-ROM, insert the disk or CD-ROM into its respective drive and click **Next**. If you are installing a program from a file on your hard disk or on a network drive, just click **Next**.
- Windows NT looks on any floppy disk or CD-ROM in your drives for an installation program (that is, a program named Setup.exe or Install.exe). If Windows NT finds an installation program, you can skip to step 8. If Windows NT doesn't find an installation program, you see the Run Installation Program dialog box (Fig 7.4).



Run Installation Program

If this is the correct installation program, click Finish. To start the automatic search again, click Back. To manually search for the installation program, click Browse.

Command line for installation program: F:\install.bat

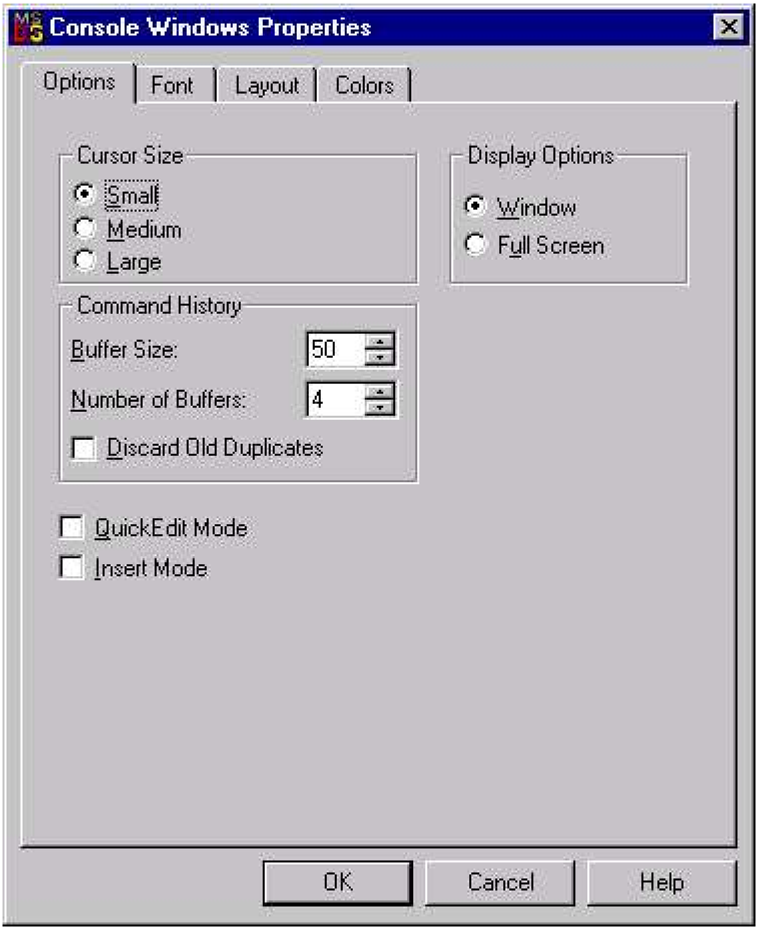
Fig. 7.4 Adding a new Program

- Click the **Browse** button and specify the installation file you want to run in the Browse window.
- When the path name of the installation program appears in the Command Line. For Installation Program box, click the

Finish button. The installation program runs. Follow the instructions on the screen to install the program.

CONSOLE

Console enables you to configure the appearance of character-based windows (consoles) and Command Prompt windows. You can also configure the properties for a specific Command Prompt application or shortcut.



Cursor Size
● Small
○ Medium
○ Large

Display Options
● Window
○ Full Screen

Command History
Buffer Size: 50
Number of Buffers: 4
□ Discard Old Duplicates

□ QuickEdit Mode
□ Insert Mode

Fig 7.5 Setting Console Windows Properties

The settings you configure using Console apply to all newly-created console windows. The settings you configure using command prompt properties apply only to the selected Command Prompt window or to windows invoked from the same icon.

- Cursor Size
- Command History

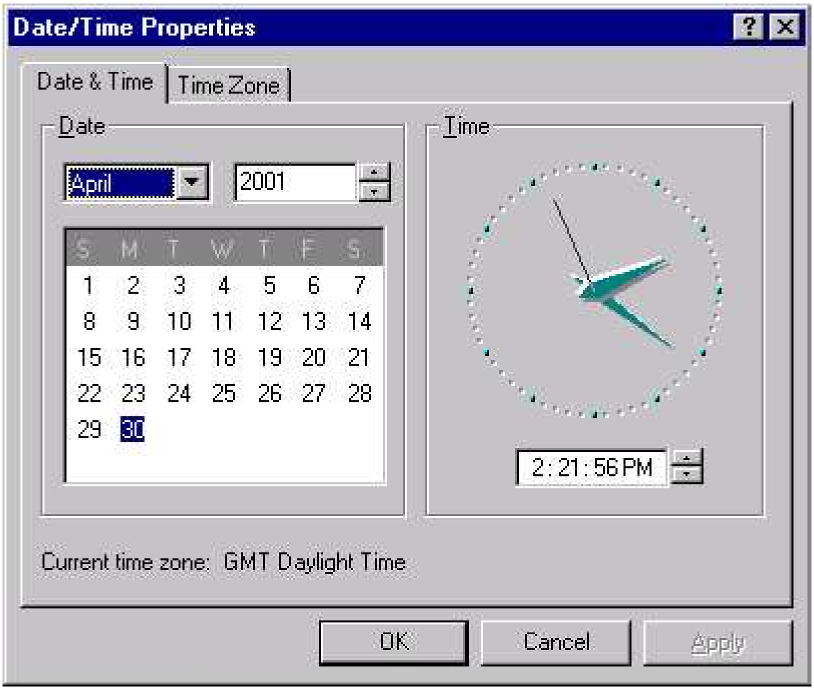
- Quick Edit Mode
- Insert Mode
- Display Options

SETTING THE CURRENT DATE AND TIME

Windows is good at keeping its clock and calendar correct. It knows about U.S. daylight-savings time and leap years.

But depending on where you live, and the accuracy of your computer's internal clock, you may need to reset Windows' clock or calendar from time to time.

To display the Date/Time Properties dialog box, shown in Fig 7.6, double-click the time on the **Taskbar** (usually displayed at the right end of the Taskbar). Alternatively, you can choose **Start ➢ Settings ➢ Control Panel**. In the Control Panel window, run the Date/Time program.



Date

April 2001

S	M	T	W	T	F	S
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30					

Time

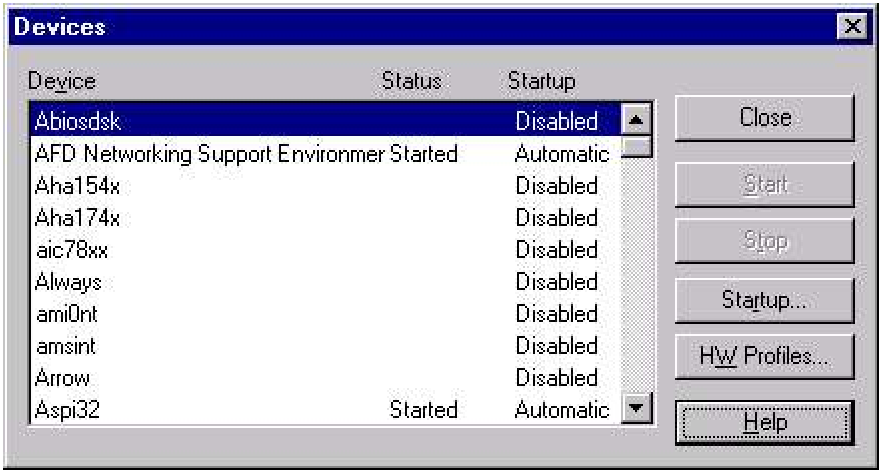
2:21:56 PM

Current time zone: GMT Daylight Time

Fig. 7.6 Setting current date or time

DEVICES

The Devices application is used to start and stop device drivers, to configure the startup behavior of device drivers, to view the status of a device driver, and to enable or disable a device driver within a hardware profile. The dialog box (Fig 7.7) lists all the available devices. After you select a device, you can stop or start it, configure its startup type, or enable or disable it in a hardware profile.

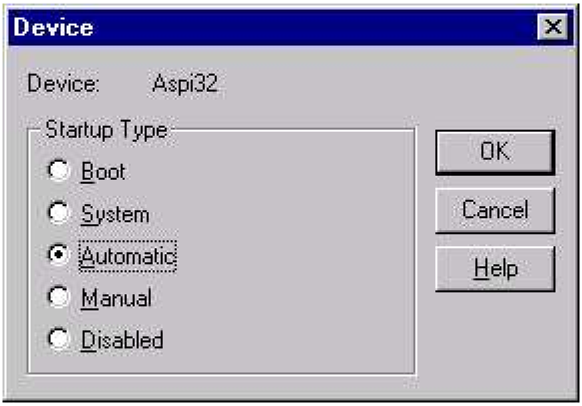


Devices

Device	Status	Startup
Abiosdsk		Disabled
AFD Networking Support Environmer	Started	Automatic
Aha154x		Disabled
Aha174x		Disabled
aic78xx		Disabled
Always		Disabled
ami0nt		Disabled
amsint		Disabled
Arrow		Disabled
Aspi32	Started	Automatic

Fig 7.7 Displaying Devices

To configure the startup type, click on the **Startup** button and select the required option.



Device

Device: Aspi32

Startup Type

○ Boot
○ System
● Automatic
○ Manual
○ Disabled

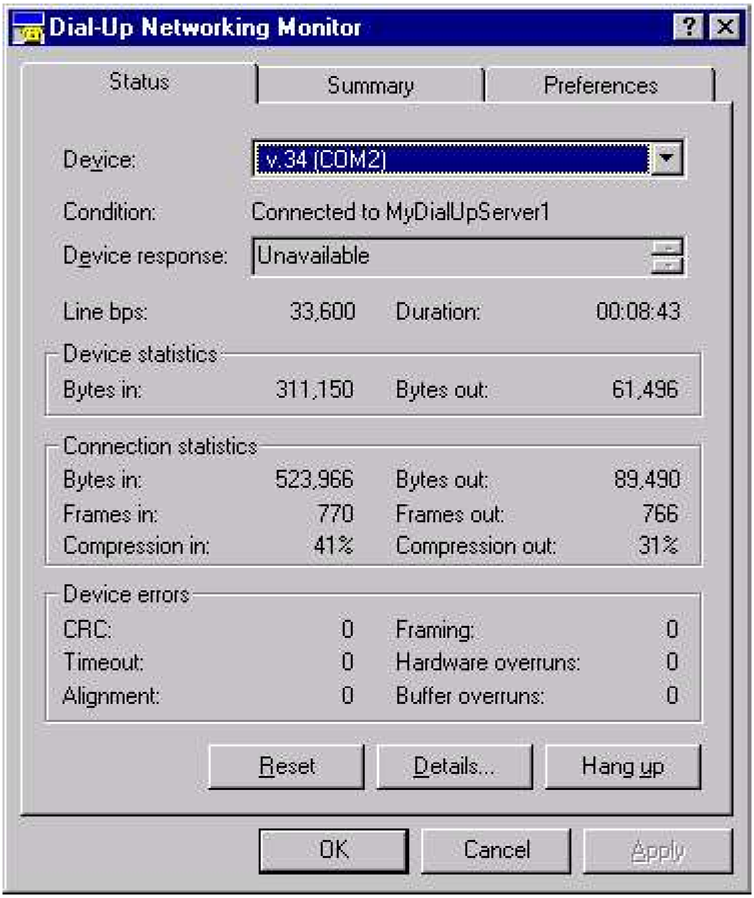
Fig 7.8 Defining Startup type of Device

- Boot, System, or Automatic indicates that the device is started automatically every time the system starts.
- Manual allows the device to be started by a user or a dependent device.
- Disabled prevents the device from being started by a user.

DIAL-UP MONITOR

Display the Dial-up status when you connect to the remote computer, to gain access to shared information, even if your computer is not on a network. The Networking Monitor shows the devices, the connection speed, received and sent bytes besides other statistical data.

The Summary tab displays the total time for which the dial-up is being used.



Device: v.34 (COM2)

Condition: Connected to MyDialUpServer1

Device response: Unavailable

Line bps: 33,600 Duration: 00:08:43

Device statistics

Bytes in: 311,150 Bytes out: 61,496

Connection statistics

Bytes in: 523,966 Bytes out: 89,490

Frames in: 770 Frames out: 766

Compression in: 41% Compression out: 31%

Device errors

CRC: 0 Framing: 0

Timeout: 0 Hardware overruns: 0

Alignment: 0 Buffer overruns: 0

Fig 7.9 The Dial-up Networking

DISPLAY SETTINGS

The command center for anything having to do with your monitor or desktop is the Display Properties dialog box, shown in Figure 7.10. You can access it from the Control Panel, or by right-clicking any unoccupied spot on the desktop and choosing Properties from the menu.

This Display Properties dialog box has six tabs (possibly more if your system has any special display software). Following table lists the tabs and the purpose of each tab. You can change the settings on most of these tabs to change the way your desktop looks and acts.

Tab	What It Controls
Background	Wallpaper and background patterns
Screen Saver	Screen savers and automatic settings for turning off your monitor
Appearance	Color, size, and font of every standard type of object Windows uses
Plus!	Customization of icons and visual effects
Settings	Size of desktop (in pixels), number of colors displayed, and monitor performance

WALLPAPER

Putting wallpaper on your desktop is a bit of a mixed metaphor - perhaps contact paper would be better. Wallpaper is the background pattern behind all the windows, icons, and menus on your desktop. Any image file can be used as wallpaper. The image can be centered on the screen, or it can fill the screen by being repeated as tiles. If you choose not to have wallpaper, the desktop can have either a solid background color or a two-tone repeating pattern.

SELECTING WALLPAPER FROM THE WALLPAPER LIST

Select your wallpaper from the Background tab of the Display Properties dialog box, shown in Figure 7.10. The Wallpaper window of that tab lists all the available wallpapers. Click a name in this list to see the wallpaper pattern displayed on the Desktop Preview - the monitor-like graphic just above the list.

Patterns

Patterns are simple 64-pixel, two-color images that interlock to give your background a textured appearance. The two colors are the background color and black. To choose or change your background pattern, follow these steps:

- Click the **Background tab** of the Display Properties dialog box.
- If the tile option is selected in the Wallpaper, your current wallpaper covers the entire background, making a background pattern irrelevant. Either choose **Center** from the Wallpaper section or set your wallpaper choice to None to reactivate the Pattern button.
- Click the name of a pattern on the Pattern list to see what it looks like in the Pattern Preview window.
- When you find a pattern you like, click **OK**. Then close the Display Properties dialog box.

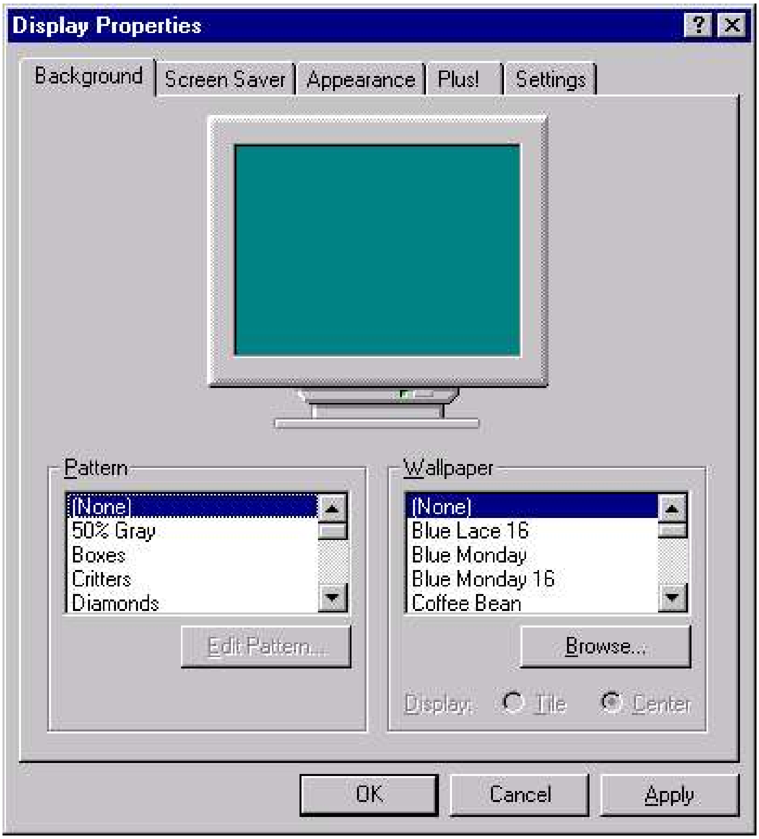


Fig. 7.10 Setting wallpaper on Desktop

EDITING A BACKGROUND PATTERN

When none of the listed patterns is exactly what you want, you can create a new pattern by editing an existing one. Follow the instructions from the previous section until the Pattern dialog box appears in step 4. Then follow these steps:

- Select the pattern you want to edit by clicking its name on the drop-down list.
- Click the **Edit Pattern** button. The Pattern Editor dialog box appears, as shown in Figure 7.11. The box labeled Pattern is an 8x8 grid of pixels, each of which is either black or the background color.
- Click any pixel to change it from one color to the other. As you change the pattern, the Sample box changes to preview how the new pattern will look on your screen.
- When you have the pattern the way you want it, click **Done**, and then OK in the confirmation dialog box. The edited pattern is saved under the original name.

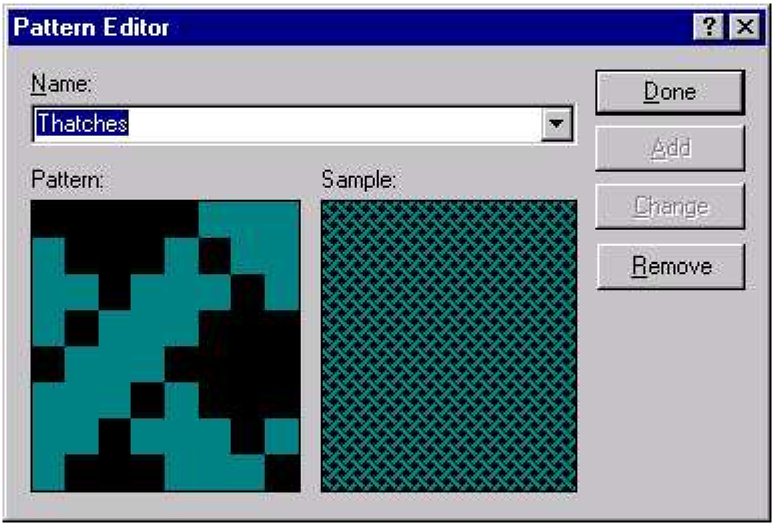


Fig. 7.11 Editing the selected Pattern for Wallpaper

If, instead, you decide you prefer the original pattern, click **No** in the confirmation dialog box. The original pattern is retained and you return to the Pattern dialog box.

SCREEN SAVER

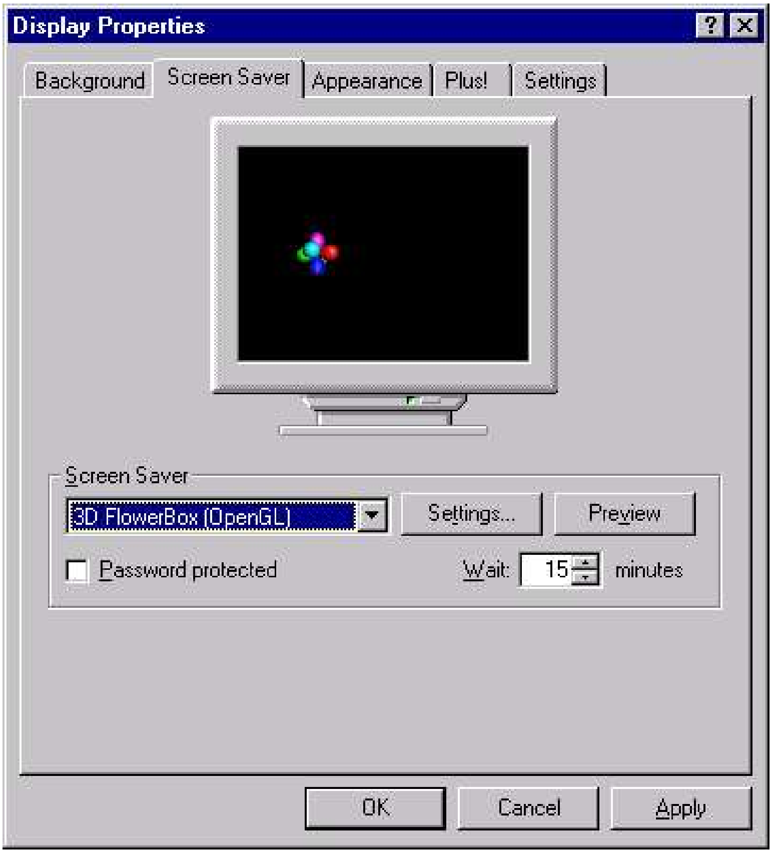
When you are not working on your computer, a screen saver can display something far more engaging and attractive than your desktop or your unfinished documents.

To choose a screen saver:

- Click the **Screen Saver tab** of the Display Properties dialog box, shown in Figure 7.12.
- Select a screen saver from the drop-down list. The previewer shows you a miniaturized version of what the screen saver displays. Or you can click the **Preview** button and see a full-size preview. When you find a screen saver you like, click either the **Apply** or **OK** button.

While you have the Screen Saver tab selected, you can make a number of choices about how your screen saver functions:

- Change the settings by clicking the **Settings** button. Each screen saver has its own list of settings; some let you change a handful of parameters, while some have an entire screen full of choices for you to make.
- Change the wait time for your screen saver by entering a new number of minutes into the Wait box. The wait time is the length of time that your system must be inactive before the screen saver starts up. Windows NT waits this long for keyboard or mouse input before starting the screen saver.



Screen Saver: 3D FlowerBox (OpenGL)

□ Password protected

Wait: 15 minutes

Fig. 7.12 Selecting a Screen saver

- Add a password to your screen saver by checking the Password Protected box. Remove password protection by unchecking the box. Change your password by clicking the **Change** button. If you have never established a screen saver password before, click **Change** to choose one.

DESKTOP SCHEME

Windows NT provides you the ability to select any conceivable color, size, or font for every single type of object on the desktop.

Choosing Sizes, Colors, and Fonts of Desktop Elements

You can choose much more than just the color of your background. In Windows NT, the color and font of almost anything is configurable - title bars, active windows, inactive windows, message boxes, you name it.

You can make all these choices one-by-one, choose a scheme pre-selected by Microsoft's desktop decorators, or start with one of

Microsoft's schemes and redefine one or two things. The focus of all this power is the Appearance tab of the Display Properties dialog box

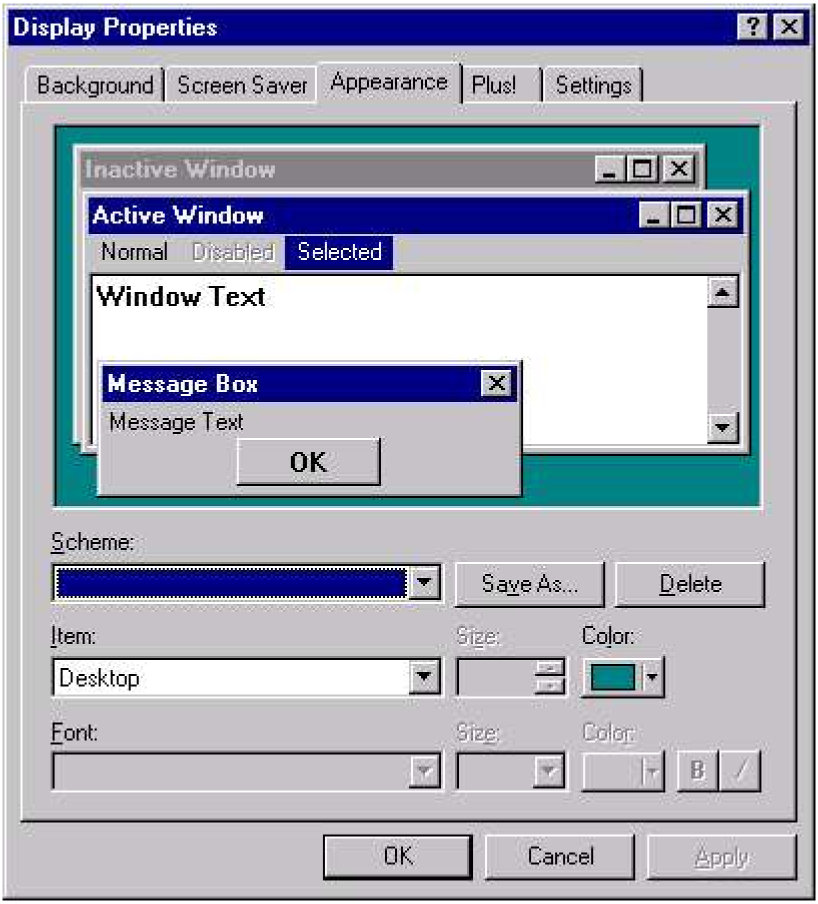


Fig. 7.13 Setting appearance of the Desktop

FONT SUPPORT IN WINDOWS NT

Fonts are used to print text, display text on screen, and send text to other output devices. Windows NT provides a set of Win32-based functions that developers can use to install, select, and query different fonts.

UNDERSTANDING FONTS

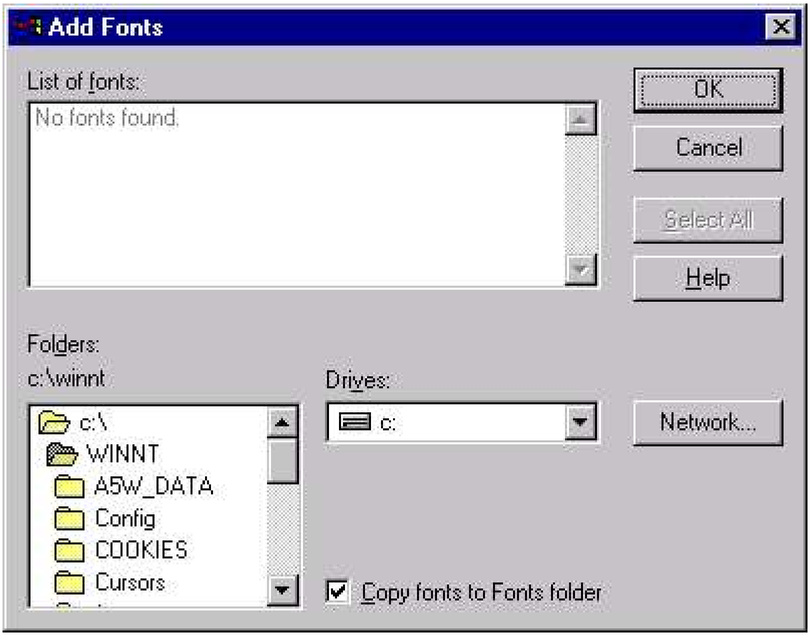
Windows NT provides four basic kinds of fonts, which are categorized according to how the fonts are rendered for screen or print output:

- TrueType fonts are stored as mathematical models that define the outline of each character. They are much easier to work with than vector fonts because they appear the same on the screen as they do on the printed page. TrueType fonts can be scaled and rotated.

- Raster fonts are stored in files as bitmaps and are rendered as an array of dots for displaying on the screen and printing on paper. Raster fonts cannot be cleanly scaled or rotated.
- Vector fonts are rendered from a mathematical model, in which each character is defined as a set of lines drawn between points. Vector fonts can be scaled to any size or aspect ratio. Windows NT provides one vector font (Modern.fon) to ensure backward compatibility with plotter devices. It is installed in the \Windows\Fonts folder as a hidden file.
- OpenType fonts can be used with PostScript outlines only if you have installed Adobe Type Manager (ATM) on your computer.

To install new fonts from a diskette or network, follow these steps:

- View the C:\Windows\Fonts folder in a Folder window or in Windows Explorer.
- Choose **File ➢ Install New Font**, and the Add Fonts dialog box, shown in Fig 7.14, appears.



List of fonts: No fonts found.

Folders: c:\winnt

Drives: c:

☑ Copy fonts to Fonts folder

Fig. 7.14 Installing new Fonts

- In the Drives and Folders boxes, select the drive and folder where the files are located for the new font or fonts. Click the **Network** button if the font files are on a network drive that is not mapped to a drive letter on your computer. Windows displays the fonts it finds.
- In the List of Fonts box, select the font(s) you want to install.

- Normally, Windows copies the font files into its font folder (C:\Windows\Fonts). If you are installing fonts from a networked folder, you can uncheck Copy Fonts To Fonts Folder to use the fonts where they are located, which saves space in exchange for some loss in speed.
- Click OK, and Windows installs the fonts you want.

DELETING FONTS

To delete a font or fonts, display the C:\Windows\Fonts folder in a Folder window or Windows Explorer window. Then select the fonts you want to get rid of and choose **File ➢ Delete**.

KEYBOARD

The Keyboard application is used to configure specific keyboard features, including speed of character repeat and cursor blink rate, input locale (including keyboard layout), and keyboard type. The default input locale is English/United States.

LICENSING

The Licensing application (available with Windows NT Server only) is used to manage licensing on your Windows NT Server computer. Normally, a licensing mode (Per Server or Per Seat - as discussed in Chapter 3) is chosen and the number of client access licenses is configured during the installation of Windows NT Server. However, if you purchase additional client licenses, or decide after installation to change your licensing mode, you can use the Licensing application to accomplish this. In addition, you can use the Licensing application to replicate licensing information to a centrally located (enterprise) server on your network.

USING A MODEM

A modem is a communications tool that enables a computer to transmit information over a standard telephone line. With Windows NT, you can install a modem in one of four ways:

- Using the Modems option in Control Panel.
- Running a communication application that causes Windows NT to prompt you to install a modem.
- Adding a modem through the Add New Hardware option in Control Panel.
- Plugging in your Plug and Play modem and letting Windows NT connect to it.

To install a modem by using the Modems option in Control Panel

- In Control Panel, double-click Modems.

- If no modem is currently installed on your computer, the Install New Modem Wizard starts automatically to lead you through the steps for installing a modem. Follow the online instructions. If you are installing a second modem, click **Add** to start the Install New Modem Wizard.

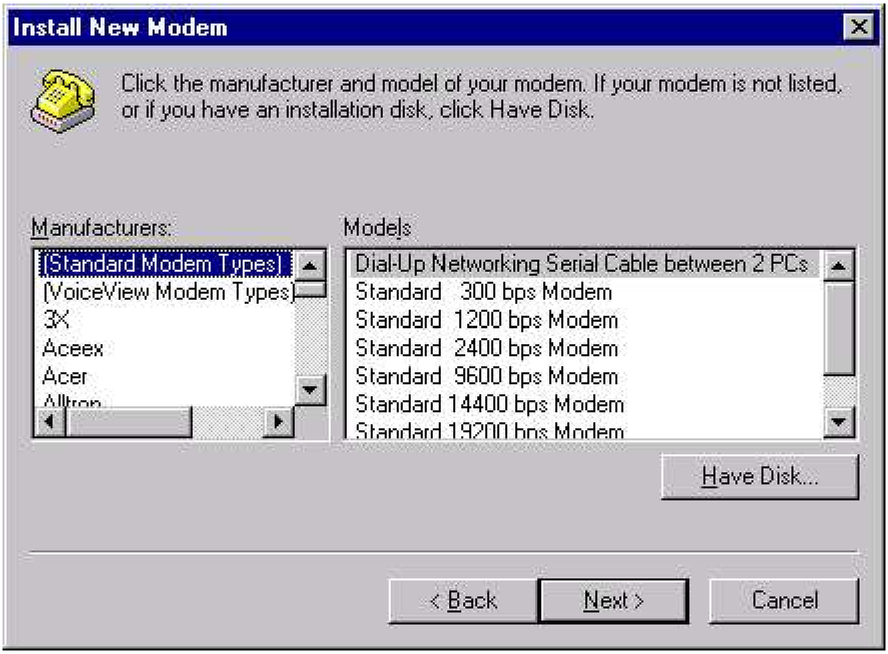


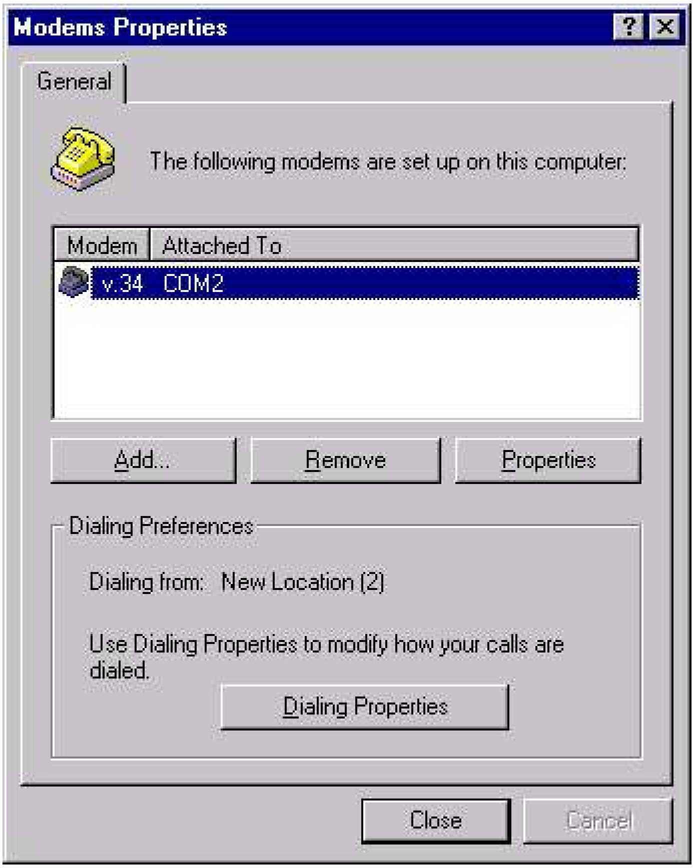
Fig. 7.15 Installing a new Modem

- The wizard shows you a list of modem manufacturers and modem models. Select one each from Manufacturers (use Standard Modem Types if you don't know the manufacturer) and from Models (use a standard or generic type if you don't know the specific model, or the nearest model if yours isn't listed). Then click **Next** to go to the next step. (Have the disk with the driver software available in case Windows asks for it).

SETTING MODEM PROPERTIES

In the Modems option in Control Panel, you can change default modem settings.

- To view General properties for a modem, double-click Modems, click a **modem**, and then click the **Properties** button, in Control Panel to bring Modem Property dialog box. (Fig 7.16).
- View the default settings for the modem that will be used by all applications created for Windows NT.


Modems Properties

General

The following modems are set up on this computer:

Modem	Attached To
v.34	COM2

Dialing Preferences

Dialing from: New Location (2)

Use Dialing Properties to modify how your calls are dialed.

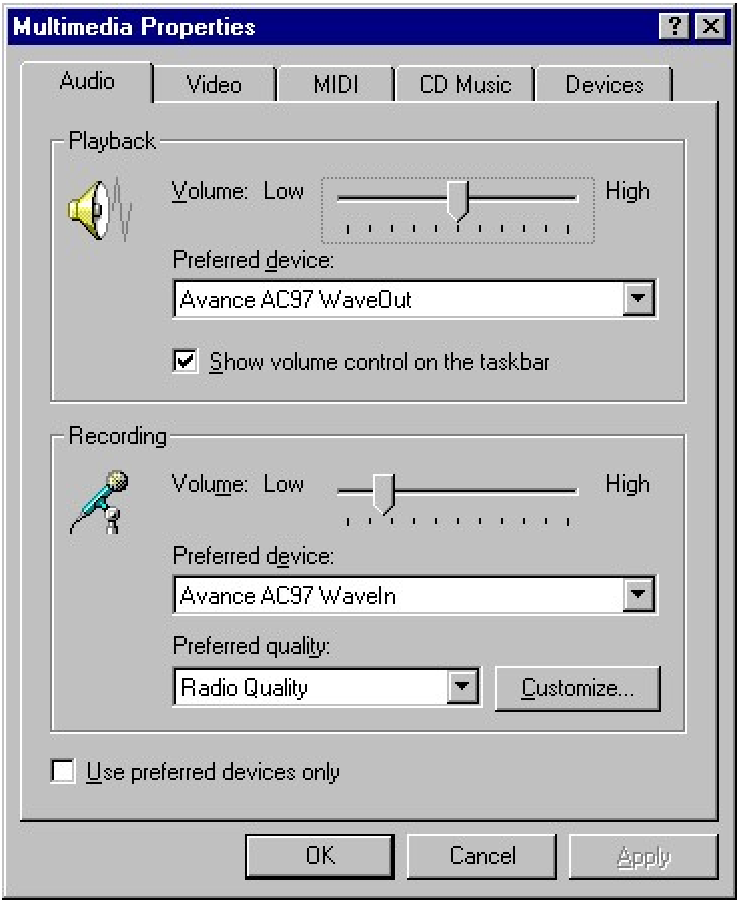
Fig. 7.16 Setting Modem Properties

MULTIMEDIA

The Multimedia application is used to install and configure audio/ visual devices. (Fig 7.17) You can specify audio record and playback devices, MIDI output configuration, and how a video is shown on your computer's display. The devices that you can install with this application include sound cards, MIDI devices and instruments, joysticks, video capture devices, and so on.

NETWORKING

The Network application is used to control all aspects of networking services on the Windows NT computer, including changing the computer/domain/workgroup name, installing and configuring protocols and services, configuring bindings and network access order, and configuring network adapters. The Network application can also be accessed by right-clicking the **Network Neighborhood** icon and selecting Properties from the menu that appears. The details about networking will be discussed in detail in coming chapters.



Playback

Volume: Low High

Preferred device: Avance AC97 WaveOut

☑ Show volume control on the taskbar

Recording

Volume: Low High

Preferred device: Avance AC97 WaveIn

Preferred quality: Radio Quality

Customize...

□ Use preferred devices only

Fig. 7.17 Configuring Multimedia Properties

PORTS

The Ports application is used to add, configure, and manage the serial communication ports (COM ports) in a computer (Fig 7.18). You can use the Ports application to configure settings for your serial ports, including baud rate, data bits, I/O port address, and interrupt.

WINDOWS' REGIONAL SETTINGS

Windows comes with predefined regional settings for most of the countries in the world. Regional settings affect the format of numbers, currency, dates, and times. For example, if you choose the regional settings for Germany, Windows knows to display numbers with dots between the thousands and a comma as the decimal point, to use Deutschmarks as the currency, and to display dates with the day preceding the month.

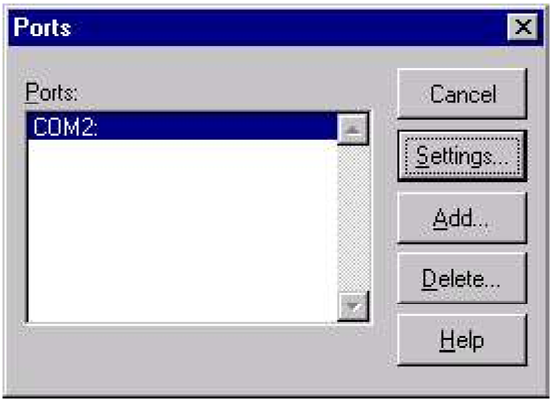
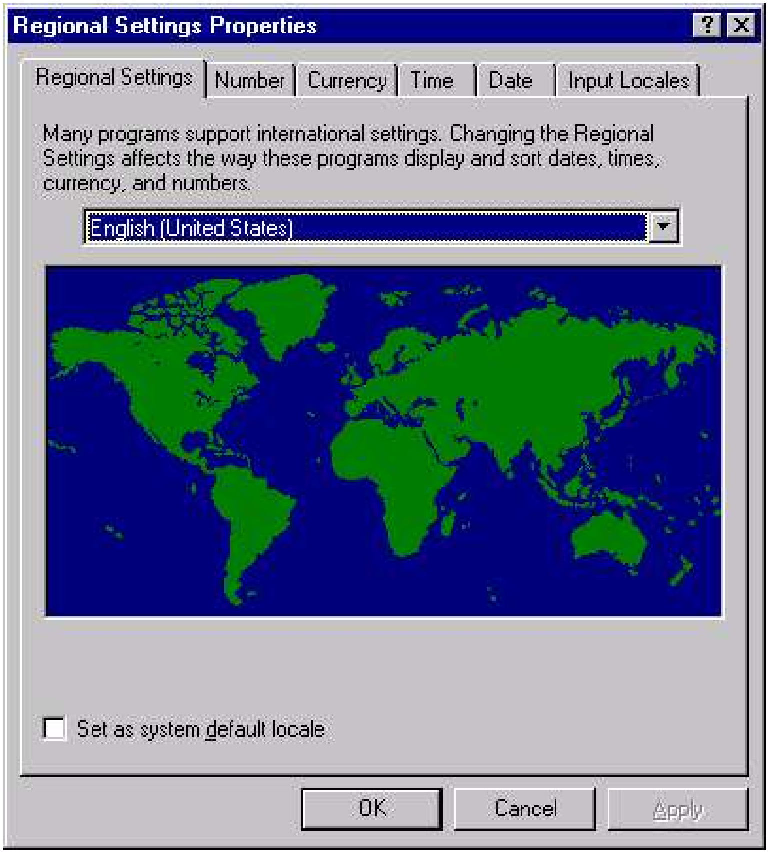


Fig 7.18 Setting Ports

To see or change your settings, choose **Start** ➢ **Settings** ➢ **Control Panel**. In the Control Panel window, run the Regional Settings program. You see the Regional Settings Properties dialog box, shown in Fig 7.19.



Many programs support international settings. Changing the Regional Settings affects the way these programs display and sort dates, times, currency, and numbers.

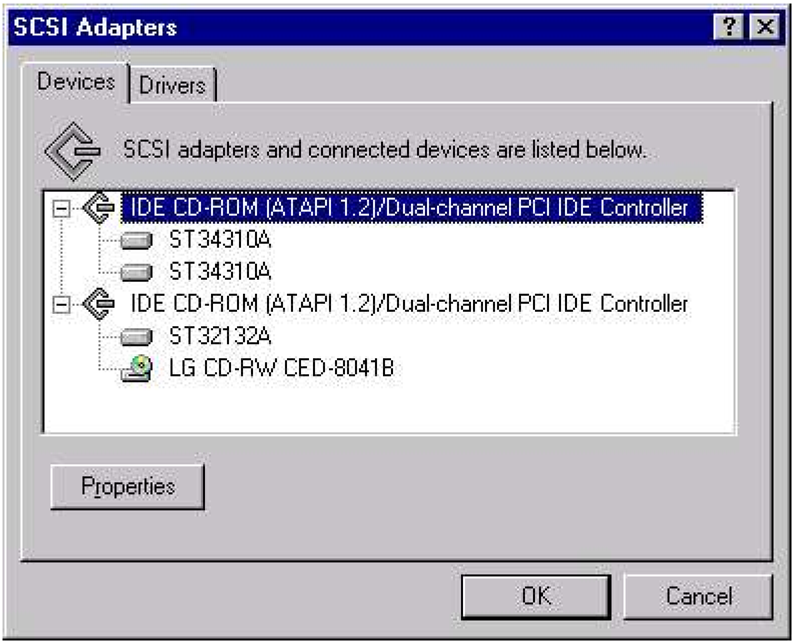
English (United States)

□ Set as system default locale

Fig. 7.19 Changing Regional Setting

SCSI ADAPTER

The SCSI Adapters application is used to install, configure, and manage SCSI adapters. SCSI adapter drivers are usually installed and configured during the installation of Windows NT. The SCSI Adapters application, however, is a convenient tool to add additional SCSI adapters after installation, and to view the operational status, configuration, and resources used by your SCSI adapters. Figure 7.20 shows the two SCSI adapters installed in desktop computer and the devices connected to each adapter. After you click the **Properties** button in the SCSI Adapters dialog box, the IDE CD-ROM dialog box is displayed, which shows the driver status and other information about the IDE controller.



SCSI adapters and connected devices are listed below.

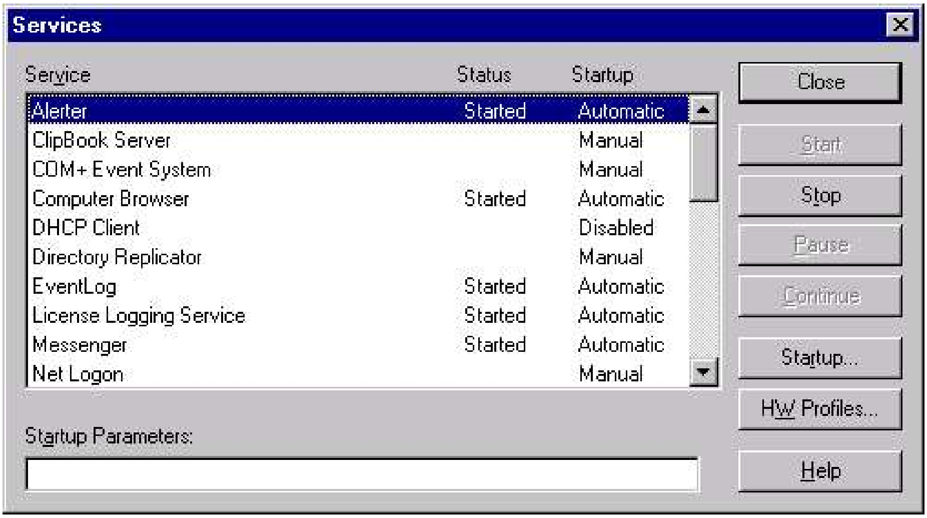
- IDE CD-ROM (ATAPI 1.2)/Dual-channel PCI IDE Controller
  - ST34310A
  - ST34310A
- IDE CD-ROM (ATAPI 1.2)/Dual-channel PCI IDE Controller
  - ST32132A
  - LG CD-RW CED-8041B

Fig 7.20 SCSI Adapter dialog box

SERVICES

The Services application is used to start and stop services, to configure the startup type of services, to view the status of a service, and to enable or disable a service within a hardware profile. (Fig 7.21)

The stop option stops a service that is running. If another service is dependent on the service you stop, you will be warned before the action completes. When you stop the Server service, all users who are connected over the network to the computer are disconnected; therefore, it is a good idea to warn connected users before stopping the Server service.

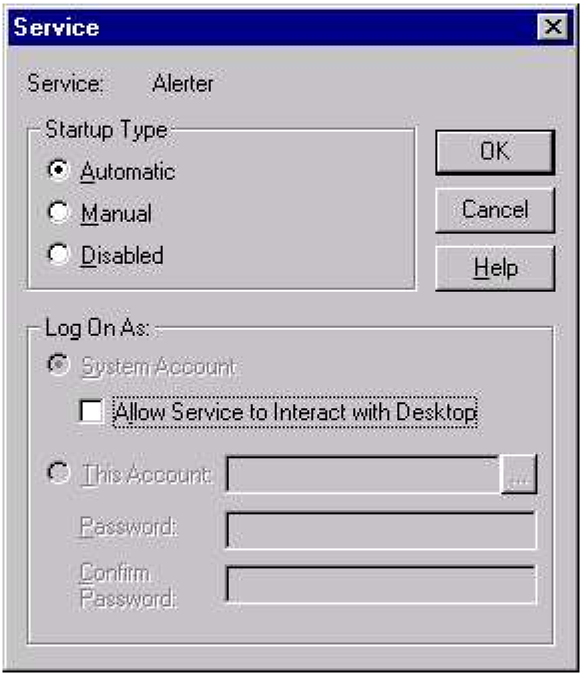


Services

Service	Status	Startup
Alerter	Started	Automatic
ClipBook Server		Manual
COM+ Event System		Manual
Computer Browser	Started	Automatic
DHCP Client		Disabled
Directory Replicator		Manual
EventLog	Started	Automatic
License Logging Service	Started	Automatic
Messenger	Started	Automatic
Net Logon		Manual

Fig 7.21 Displaying Services

The startup option passes startup parameters to a service. To configure service startup, you must be logged on to a user account that has membership in the Administrators local group. (Fig 7.22)



Service

Service: Alerter

Startup Type

● Automatic

○ Manual

○ Disabled

Log On As:

● System Account

□ Allow Service to Interact with Desktop

○ This Account:

Password:

Confirm Password:

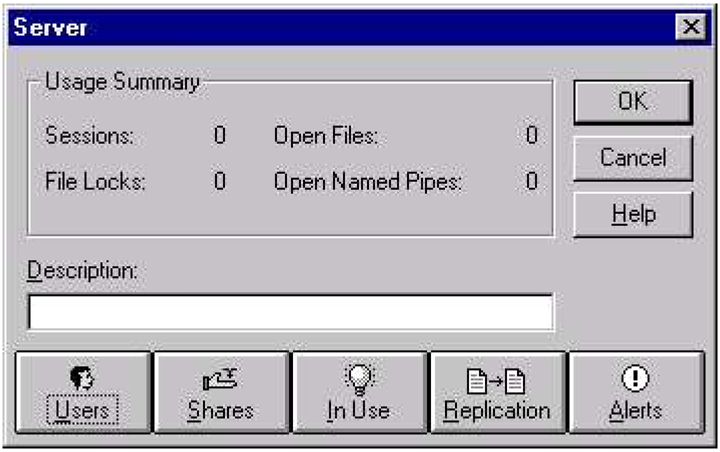
Fig 7.22 Configuring Services

The startup types available in this application include automatic, manual, and disabled. If you choose **automatic**, Windows NT starts the service automatically every time the computer is booted. If you choose **manual**, a user must start the service. If you select disabled, the service can't be started by a user.

SERVER

The Server application is used to view user sessions (including the resources that users are accessing), disconnect users from the computer, view the status of shared resources, configure directory replication, and configure administrative alerts. The Server application is included with both NT Workstation and NT Server.

Most of the functions within the Server application are fairly intuitive and straight forward, but directory replication deserves an in-depth discussion. Configuring Directory Replication Directory replication was designed to copy logon scripts from a central location (usually the primary domain controller [PDC]) to all domain controllers, thus enabling all users to execute their own logon scripts no matter which domain controller validates their logon. Directory replication is also used extensively by Microsoft Systems Management Server.



Server

Usage Summary

Sessions: 0 Open Files: 0

File Locks: 0 Open Named Pipes: 0

Description:

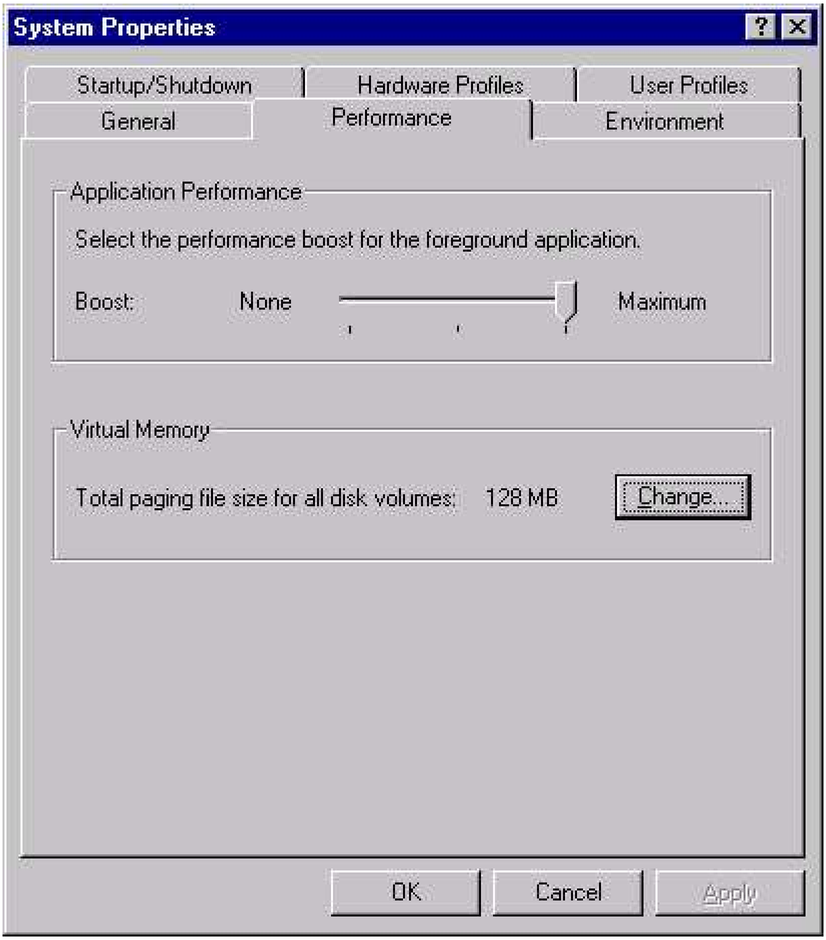
Fig 7.23 Configuring Server

SYSTEM

The System application is used to configure foreground application performance, virtual memory, system and user environment variables, startup and shutdown behavior, hardware profiles, and user profiles. Each of these topics is discussed in the following section.

APPLICATION PERFORMANCE AND VIRTUAL MEMORY

You can use the System application to set the performance boost for the foreground application and to configure your virtual memory paging file(s). Application performance Foreground application performance involves giving a higher priority to the application running in the foreground than to other applications. The purpose of assigning a higher priority is to make the foreground application more responsive to the user. To configure the foreground application priority, double-click the **System** icon in the Control Panel, and select the **Performance** tab. Adjust the slide bar for the amount of performance boost you want.



Application Performance

Select the performance boost for the foreground application.

Boost: None — Maximum

Virtual Memory

Total paging file size for all disk volumes: 128 MB

Fig 7.24 Configuring System Properties

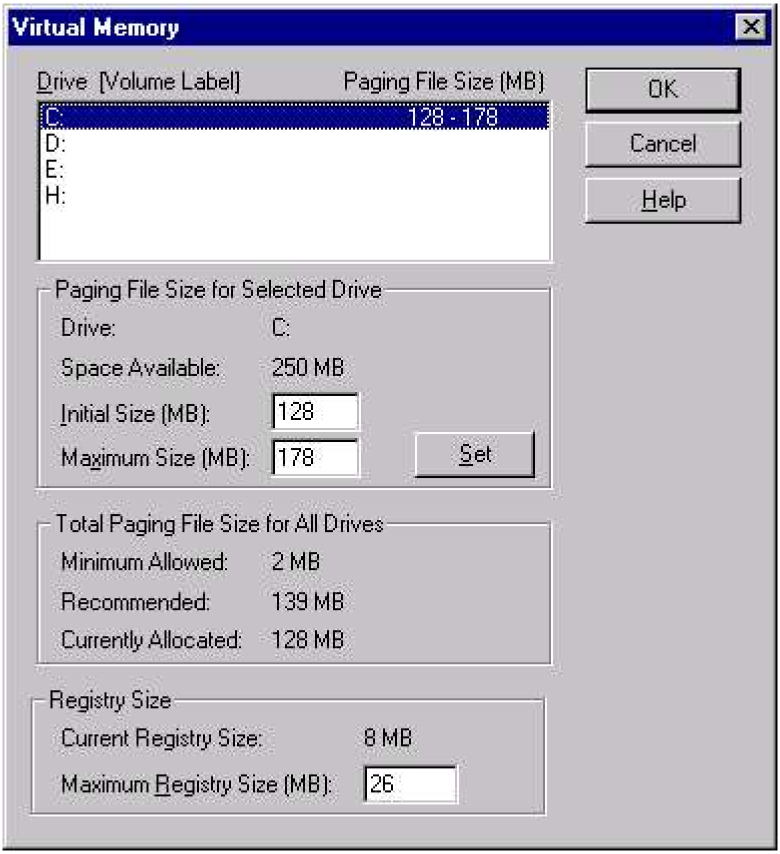
VIRTUAL MEMORY

Virtual memory is implemented in Windows NT by the use of paging files. You should consider both performance and recoverability when configuring virtual memory paging files.

If you want to configure your system for maximum paging file performance, you should put a small paging file on each physical disk, except on the disk that contains the Windows NT boot partition. This will provide the highest performance for virtual memory.

If you want to configure your system for optimum system recovery, you must put a paging file on the Windows NT boot partition that is at least as large as the amount of RAM in your computer. This paging file is used by Windows NT as a normal paging file, and, additionally, this paging file is required to enable Windows NT to write a memory.dmp file when the operating system crashes. It's up to you to consider the tradeoffs between performance and recoverability, and then to determine the best configuration for your paging files.

You can configure virtual memory paging files by using the System application. On the Performance tab, click the **Change** command button in the Virtual Memory section. Then configure paging files on each drive as desired.



Drive [Volume Label] Paging File Size (MB)

C: 128 - 178
D:
E:
H:

Paging File Size for Selected Drive

Drive: C:

Space Available: 250 MB

Initial Size (MB): 128

Maximum Size (MB): 178

Total Paging File Size for All Drives

Minimum Allowed: 2 MB

Recommended: 139 MB

Currently Allocated: 128 MB

Registry Size

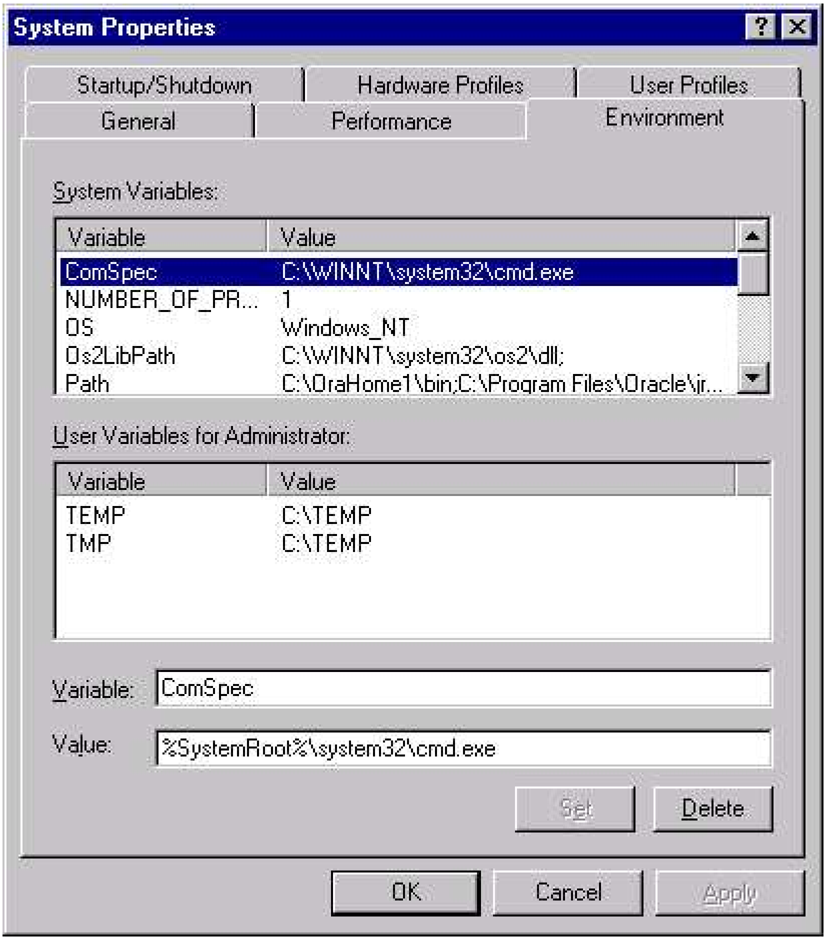
Current Registry Size: 8 MB

Maximum Registry Size (MB): 26

Fig 7.25 Setting Virtual Memory

ENVIRONMENT VARIABLES

You can use the System application to configure system and user environment variables. System environment variables apply to all users and to the operating system. User environment variables apply only to a specific user. To modify a system environment variable, you must be logged on as a user that is a member of the Administrators local group. To modify a user environment variable, you must be logged on as the user whose variable you want to modify. To configure system and user environment variables, start the System application from the Control Panel, and then select the **Environment** tab. Highlight the variable you want to modify in the appropriate list box (System or User), edit the value of this variable in the Value text box near the bottom of the dialog box, and then click the **Set** command button.



System Variables:

Variable	Value
ComSpec	C:\WINNT\system32\cmd.exe
NUMBER_OF_PR...	1
OS	Windows_NT
Os2LibPath	C:\WINNT\system32\os2\dll;
Path	C:\OraHome1\bin;C:\Program Files\Oracle\jr...

User Variables for Administrator:

Variable	Value
TEMP	C:\TEMP
TMP	C:\TEMP

Variable: ComSpec

Value: %SystemRoot%\system32\cmd.exe

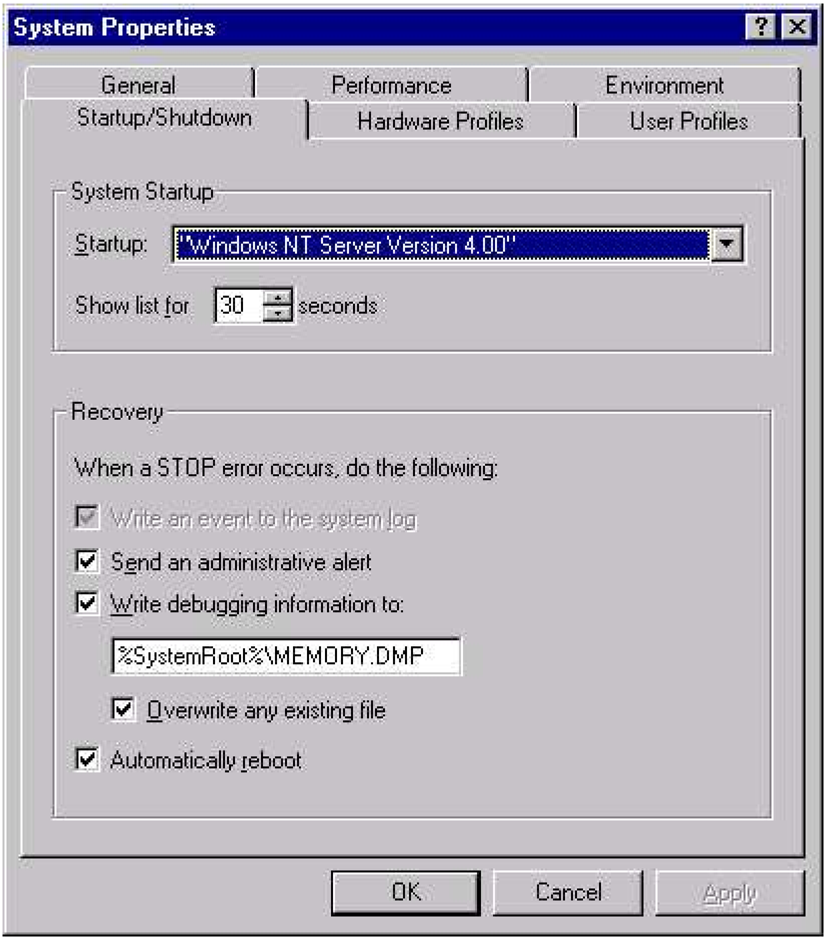
Fig 7.26 Setting System Environment

To add a new system or user environment variable, highlight any variable in the appropriate list box (System or User), and then type in a new variable name and value in the Variable and Value text boxes near the bottom of the dialog box. Then click the **Set** command button to create the new variable. Fig. 7.26 shows the layout of the

Environment tab within the System application. Notice that the Variable and Value text boxes are located near the bottom of the dialog box.

STARTUP/SHUTDOWN

You can use the System application to configure startup and shutdown behavior of Windows NT. Fig 7.27 illustrates the Startup/Shutdown tab within the System application. Notice the System Startup and Recovery options that can be configured.



System Startup

Startup: "Windows NT Server Version 4.00"

Show list for 30 seconds

Recovery

When a STOP error occurs, do the following:

☑ Write an event to the system log

☑ Send an administrative alert

☑ Write debugging information to:

%SystemRoot%\MEMORY.DMP

☑ Overwrite any existing file

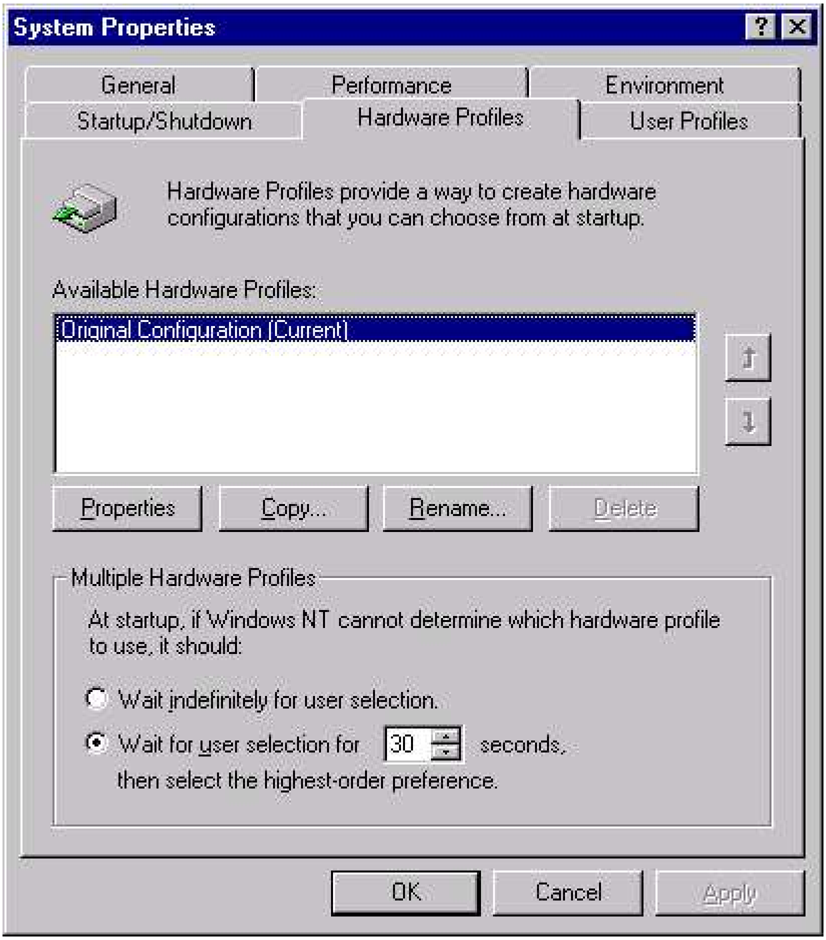
☑ Automatically reboot

Fig 7.27 Setting Startup/Shutdown options

In the System Startup section of the Startup/Shutdown tab you can configure which operating system will boot by default if no other selection is made from the boot loader menu. You can also configure the length of time the boot loader menu is displayed. In the Recovery section of the Startup/Shutdown tab you can configure the actions Windows NT takes when a STOP error occurs. A STOP error is an error from which Windows NT cannot recover (in other words, a system crash). The two most important options you can configure in the Recovery section are the Write debugging information to check box and the Automatically reboot check box.

HARDWARE PROFILES

You can use the System application to create and configure hardware profiles. Windows NT creates an initial hardware profile during installation.



Hardware Profiles provide a way to create hardware configurations that you can choose from at startup.

Available Hardware Profiles:

Original Configuration (Current)

Multiple Hardware Profiles

At startup, if Windows NT cannot determine which hardware profile to use, it should:

○ Wait indefinitely for user selection.

● Wait for user selection for 30 seconds, then select the highest-order preference.

Fig 7.28 Setting Properties for Hardware Profiles

The primary reason for creating hardware profiles is to manage the different hardware configurations of laptop computers. (A laptop computer that is used at the office in a docking station has a different hardware configuration than the same laptop computer when it is used at home or on the road without a docking station.) Hardware profiles enable you to create custom configurations for the same laptop computer that is used both with and without a docking station. Fig 7.29 shows the Hardware Profiles tab within the System application. Note that you can use the arrows on the right hand side to move profiles up or down in the Available Hardware Profiles list box. Windows NT uses the first profile in this list when no other selection is made during the boot process.

To create a new hardware profile, start the System application from Control Panel, and select the **Hardware Profiles** tab. Highlight any profile in the Available Hardware Profiles list box, and click the **Copy** command button. A Copy Profile dialog appears, enabling you to type in a name for your new hardware profile.

The new hardware profile now has the same properties as the profile you highlighted and copied. You can configure this new profile as necessary. To configure a new or existing hardware profile, highlight the profile in the Available Hardware Profiles list box and click the **Properties** command button. Then select the docking status for this hardware profile, and specify whether this is a network disabled profile. You can also use the Services and Devices applications to enable and disable services and device drivers within each hardware profile.

Once you have created multiple profiles, Windows NT displays the Hardware Profile/Configuration Recovery menu after the boot loader menu when your computer boots to Windows NT. This menu enables you to select the hardware profile you want Windows NT to use. You can configure the length of time this menu is displayed in the Multiple Hardware Profiles section on the Hardware Profiles tab.

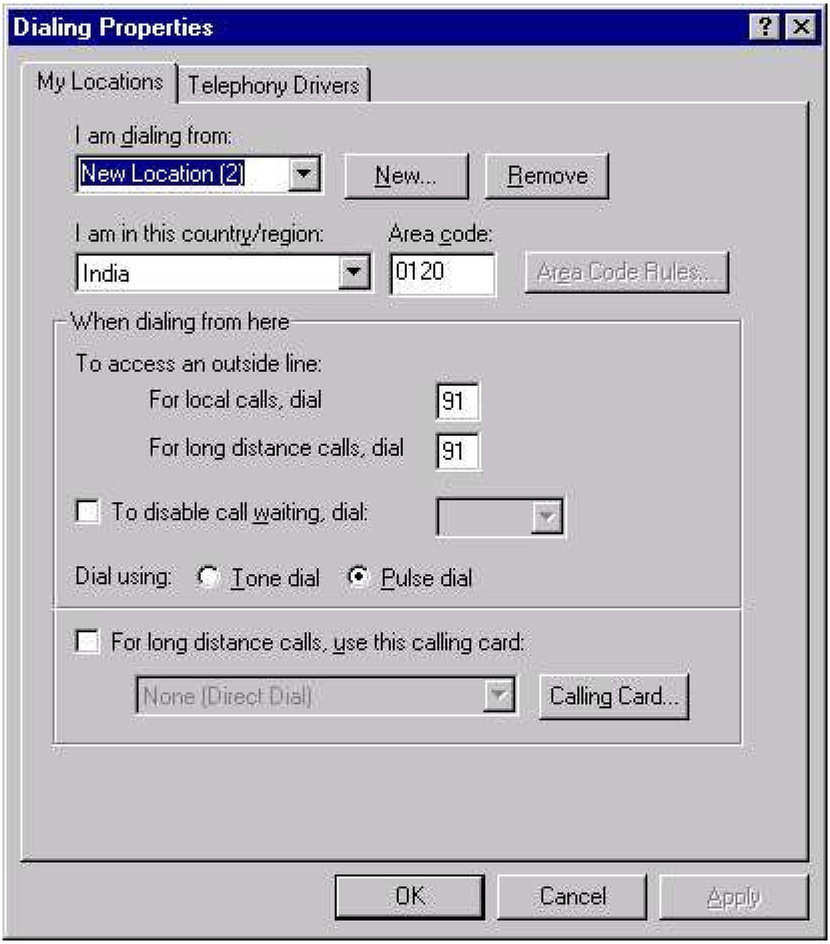
TAPE DEVICES

The Tape Devices application is used to install drivers for tape backup devices and to view the status of tape backup devices connected to your computer. This application functions much like the PC Card (PCMCIA) and SCSI Adapters applications. You must install a driver for your tape backup device before you can access it in the Windows NT Backup application.

TELEPHONY

The Telephony application is used to configure dialing properties for your computer, such as the area code you are calling from, the country you are in, special instructions on how to access an outside line, whether or not to dial using a calling card, instructions on how to disable call waiting, and to specify tone or pulse dialing. In addition, you can use this application to install, configure, and remove telephony drivers.

You can turn off call waiting while you're making data or fax calls from your computer. Also you can specify pulse dialing only if this is the only type your phone line supports.



Dialing Properties

I am dialing from: New Location (2)

I am in this country/region: India

Area code: 0120

When dialing from here

To access an outside line:

For local calls, dial 91

For long distance calls, dial 91

□ To disable call waiting, dial:

Dial using: ○ Tone dial ● Pulse dial

□ For long distance calls, use this calling card: None (Direct Dial)

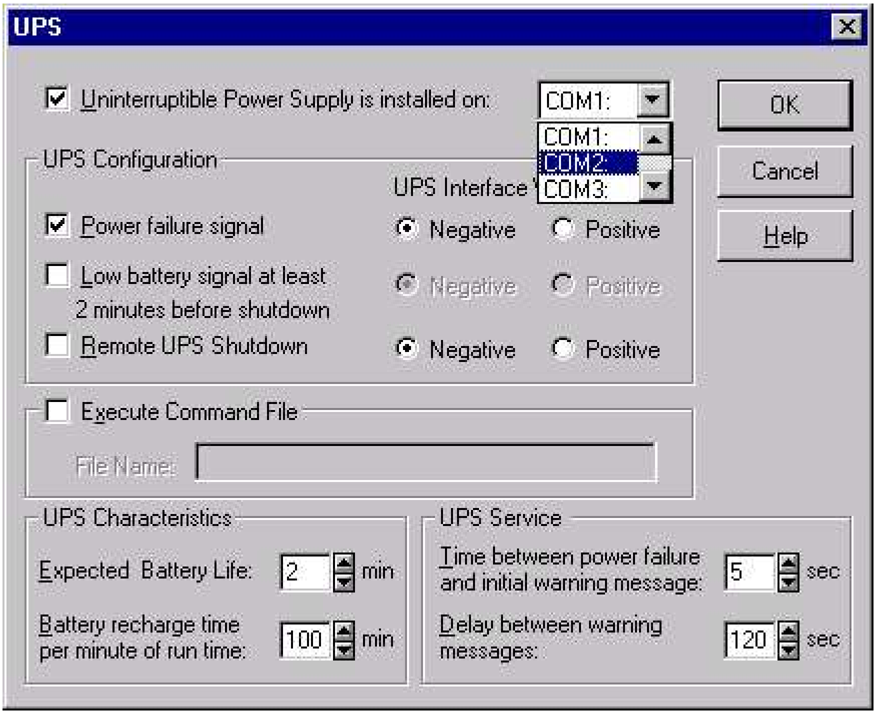
Fig 7.29 Setting Dialing Properties

USER PROFILES

You can use the User Profiles tab within the System application to copy, delete, and change the type of user profiles. The System application is the only application in Windows NT that can copy user profiles. You can’t copy user profiles by using Windows NT Explorer.

UPS

The UPS application is used to install, configure, and manage an uninterruptible power supply. The Windows NT UPS application is adequate for managing an inexpensive UPS that does not include Windows NT-compatible UPS application software.



UPS

☑ Uninterruptible Power Supply is installed on: COM1:

COM1:
COM2:
COM3:

UPS Configuration

UPS Interface Voltages

☑ Power failure signal ● Negative ○ Positive

□ Low battery signal at least 2 minutes before shutdown ● Negative ○ Positive

□ Remote UPS Shutdown ● Negative ○ Positive

□ Execute Command File

File Name:

UPS Characteristics

Expected Battery Life: 2 min

Battery recharge time per minute of run time: 100 min

UPS Service

Time between power failure and initial warning message: 5 sec

Delay between warning messages: 120 sec

Fig 7.30 Setting UPS Properties

Fig 7.30 shows the configuration options available in the Windows NT UPS application. Note that you can configure the UPS interface voltages, expected battery life, the name of an executable program to run thirty seconds before shutdown, and other settings.

EXERCISE

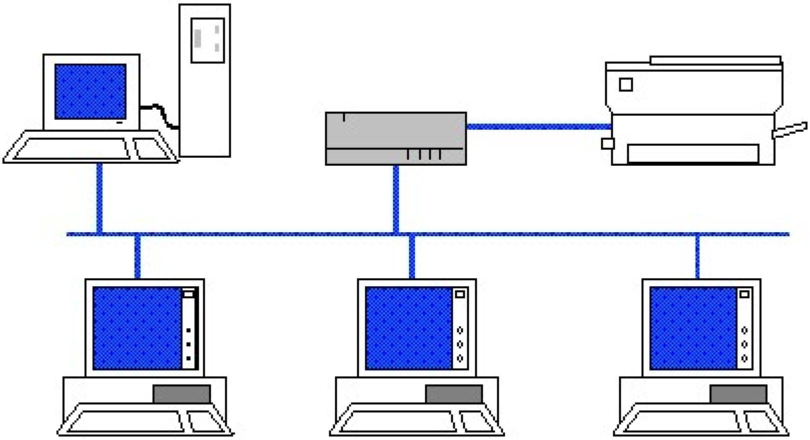
Answer the following questions:

1. Discuss the importance of Control Panel.
2. How you can install new applications in Windows NT? What will you do if you want to remove the paint application (default) from your computer?
3. What is the significance of Dial-up Monitor?
4. Can you change your display cards through the Display Settings ? If yes, how?
5. Can you use Hindi Fonts on your computer? If yes, how to install them.
6. Configure a telephone line with your computer so that you can use the application Phone Dialer in the Accessories.

CHAPTER 8

Users Administration

USER & GROUPS
WORKING WITH ACCOUNTS AND GROUPS
CREATING & MANAGING USER ACCOUNT
CREATING & MANAGING GROUPS
RIGHTS & PERMISSIONS
TRUST RELATIONSHIPS
MANAGING ACCOUNT POLICY
AUDITNG WINDOWS NT



USER & GROUPS

The fundamental purpose of a network operating system (NOS) is to create a productive environment for users while maintaining a high level of security. Windows NT Server 4.0 qualifies as an advanced NOS as it provides all the tools for access and proper management of users and the groups to which they belong.

NT has a powerful and flexible tool, User Manager for Domains, for managing the users of a network. User Manager for Domains lets you, as a network administrators, create and manage individual user accounts and user groups, and manage the security policies that affect the user accounts and groups.

WORKING WITH ACCOUNTS AND GROUPS

DOMAIN

A domain is a network concept that defines group of workstations and servers that share a common Security Accounts Manager (SAM) database and allow a user to log on to any resource in the domain with a single user ID and password. These resources could be file and application servers, printers, CD-ROM drives, modems, and other devices-that are centrally managed.

USER ACCOUNTS

The heart of system management in Windows NT is the user account. Whether you use the workgroup model or the domain model, creating and managing user accounts is a task you'll perform most often. Windows NT brings account control under one interface (called User Manager for Domains), which greatly simplifies the process of creating and managing the user accounts.

A user account defines all the information necessary for the user to connect to the Windows NT network. The user account includes the user name and password required to log on to the network. An account also defines the rights and permissions to access system resources granted to the user beside containing additional information, such as the user environment profile, a list of log on workstations, and a schedule of log on hours.

USER GROUPS

A User groups define the rights and privileges that are assigned to the users in those groups. Placing the User Accounts in groups not only simplifies general management, but also makes it easier and faster to grant multiple users access to a network resource. Groups could be divided into two categories - global groups and local groups. A global group is depicted with a world globe in the background. A local group is depicted with a workstation in the background.

Local Group

Local groups are primarily used to control access to resources. In a typical Windows NT configuration, a local group is assigned permissions to a specific resource, such as a shared folder or a shared printer. Individual user accounts and global groups (discussed in next section) are made members of this local group. The result is that all members of the local group now have permissions to the resource. Using local groups simplifies the administration of resources, because permissions can be assigned once, to a local group, instead of separately to each user account.

In Windows NT, all domain controllers (within a single domain) maintain identical copies of the same directory database, while each non-domain controller maintains its own separate directory database. All user accounts and group accounts are stored in the directory database in which they are created.

Local groups can be created on any Windows NT computer. A local group in the directory database on a domain controller can be assigned permissions to resources on any domain controller in the domain. However, a local group in the directory database on a domain controller cannot be assigned permissions to resources on any non-domain controller. (Remember that non-domain controllers include stand-alone servers, member servers, and all Windows NT Workstation computers.) A local group, in the directory database on a non-domain controller, can be assigned permissions to resources only on that computer.

A local group can contain various user accounts and global groups, depending on whether the local group is located in the directory database on a domain controller, on a non-domain controller that is a member of a domain, or on a non-domain controller that is not a member of a domain.

A local group in the directory database on a domain controller can contain individual user accounts and global groups from the domain directory database, and can also contain user accounts and global groups from the directory database of any trusted domain. A trusted domain is a domain whose users can access resources in the domain that “trusts” it.

Global Group

A global group is a collection of user accounts within a single domain. Global groups are primarily used to organize users that perform similar tasks or have similar network access requirements. In a typical Windows NT configuration, user accounts are placed in a global group, the global group is made a member of one or more local groups, and each local group is assigned permissions to a resource. The advantage of using global groups is ease of administration - the network administrator can manage large numbers of users by placing them in global groups.

A global group can't contain other groups and can include only user accounts from the domain in which the group was created. Thus a global group can only be created on a domain controller, and can only contain individual user accounts from the domain directory database that contains the global group. Global groups can't contain local groups, other global groups, or user accounts from other domains.

Working with Built-In Groups

Windows NT has a number of built-in groups.

Local Groups

The domain controllers have these built-in local groups:

Administrators Members of the Administrators group have almost complete access to - as well as authority over - the domain, server, or workstation containing the group.

Backup Operators This local group is designed to enable users to perform backup functions. Users in the Backup Operators group can back up and restore files (even if they lack read/write permission to the directories they're backing up), log on to the system locally, and shut down the system.

Account Operators Users in this group can create and manage user accounts in the domain. They can create and modify user accounts and groups but cannot assign user rights.

Guests Members of the Guests group on a domain have rights similar to Users. They can log on through a network client and access domain resources.

Print Operators The Print Operators group can log on to servers locally; shut down a server; and share, unshare, and manage printers on a Windows NT server.

Replicator The Replicator group is a special group to facilitate file and directory replication. There are no default members of this group, though the group exists on all servers and workstations.

Server Operators The Server Operators group enables its members to manage servers. This group only exists in a Windows NT server that is acting as a domain controller.

Users The most common group is Users. Members of this group can log on locally to a workstation, member server, or domain, but not to a PDC or BDC.

Global Groups

The domain controllers have these domain (global) groups:

Domain Admins Every domain includes a global group named Domain Admins, which is automatically added to the local Administrators group. Therefore, all members of Domain Admins are domain administrators.

Domain Guests The Guest user account typically is included in the Domain Guests group, which is a member of the local Guests group.

Domain Users All user accounts in a domain automatically become members of the Domain Users group.

Windows NT workstations and Windows NT servers without domain controller security have these built-in groups:

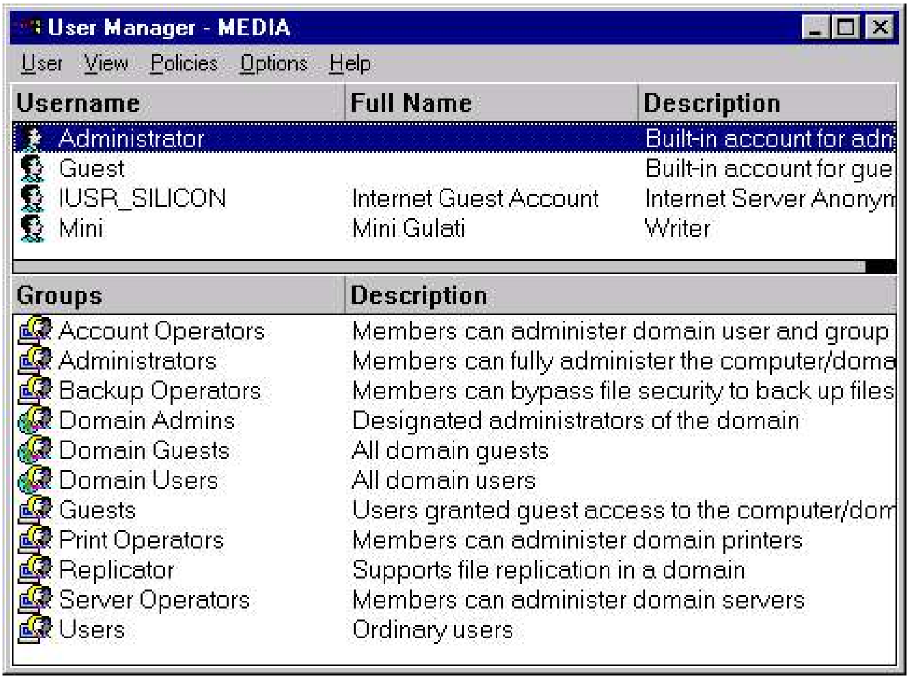
Administrators	See Above
Backup Operators	See Above
Power Users	Power Users are like Users with some administrative rights. Power Users can create and modify those user accounts that they create.
Guests	See Above
Replicator	See Above
Users	See Above

STARTING THE USER MANAGER FOR DOMAINS

You can start User Manager for Domains from the Start menu. To start User Manager click **Start** ➢ **Programs** ➢ **Administrative Tools** ➢ **User Manager** for Domains to open User Manager's window. By default, information for the domain where your user account is defined appears in the window. (Fig 8.1)

You can also type **usrmgr** in run dialog box to open User Manager in the domain. You can also start User Manager in specific domain or for a specific server. To start User Manager for specific domain (say SILICON) type command **usrmgr silicon** in the Run dialog box. To start User Manager for specific computer MNG, type **usrmgr \\mng** in the Run dialog box.

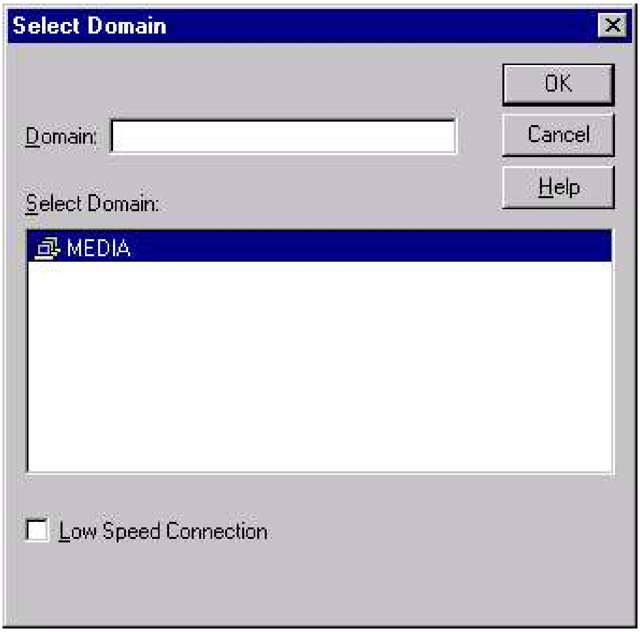
You can open many instance of User Manager for different domain or computer. If you want to change the domain for same instance of User Manager, click **User** ➢ **Select Domain** to bring up the Select Domain dialog box (Fig 8.2).



Username	Full Name	Description
Administrator		Built-in account for adm
Guest		Built-in account for gue
IUSR_SILICON	Internet Guest Account	Internet Server Anonym
Mini	Mini Gulati	Writer

Groups	Description
Account Operators	Members can administer domain user and group
Administrators	Members can fully administer the computer/doma
Backup Operators	Members can bypass file security to back up files
Domain Admins	Designated administrators of the domain
Domain Guests	All domain guests
Domain Users	All domain users
Guests	Users granted guest access to the computer/dom
Print Operators	Members can administer domain printers
Replicator	Supports file replication in a domain
Server Operators	Members can administer domain servers
Users	Ordinary users

Fig 8.1 The User manager



Domain:

Select Domain:

MEDIA

□ Low Speed Connection

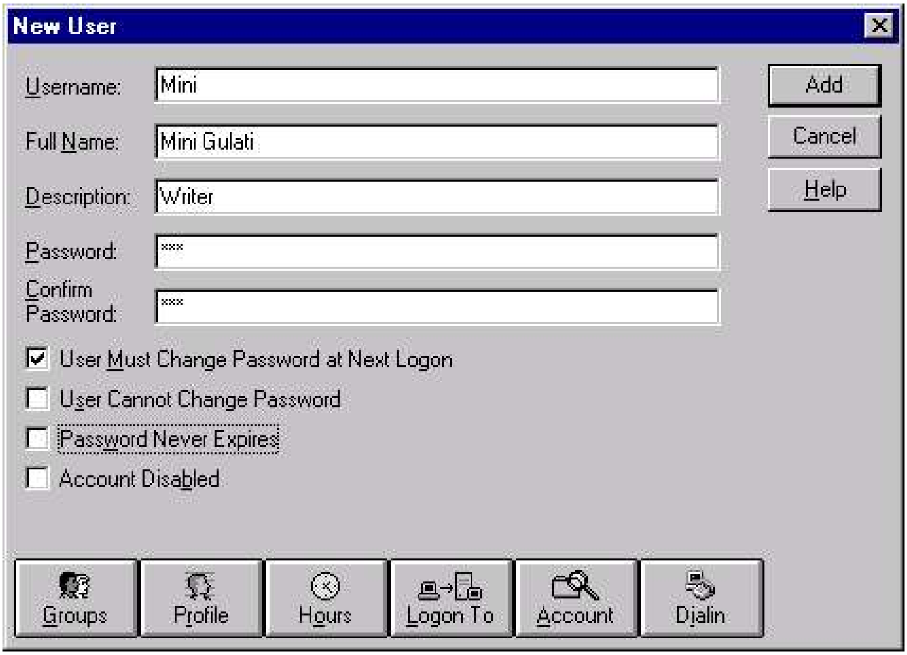
Fig 8.2 Selecting Domain

CREATING & MANAGING USER ACCOUNT

Every user of a Windows NT Server network must have a user account, which consist of all the information that defines a user to the Windows NT network. The user account defines the resources on Windows NT computers and domains that can be accessed by the user. A user account consists of following control features:

- User account and password
- User group membership
- Account policies
- User rights
- User profile
- User home directory
- User login script
- User logon times
- User logon capabilities
- Remote Access Service capabilities
- Access to applications

To add a new user select **User ➤ New User**. To add a new user account, fill in the dialog's text boxes, mark the appropriate security check boxes, and click the **Add** button to create the user account.



Username: Mini

Full Name: Mini Gulati

Description: Writer

Password: ***

Confirm Password: ***

☑ User Must Change Password at Next Logon

□ User Cannot Change Password

□ Password Never Expires

□ Account Disabled

Fig 8.3 Creating New User

To start with, type in a unique user name in the *Username box*. The username can have up to 20 characters, either uppercase or lowercase, and can't include the following characters:

“ / \ [ ] ; | = , + * ? < >

Blanks are acceptable but it is recommended to avoid them, because they make it necessary to surround user names with quotes when executing the commands.

In the full name and description boxes, type in the user's full name and a short description of the user or the user account. Both these entries are optional, but recommended.

Next, type in the password in both password and confirm password boxes. Passwords are case-sensitive. After you have entered and confirmed a password, select or clear the check boxes that determine whether or not user can or must change the password at the next logon. All of the options in this series of check boxes are described below :

Change Password At Next Logon

The default value is Yes. It forces the user to change the password the next time that he / she logs on; this value is set to No afterwards

User cannot Change Password

If set to yes, prevents the user from changing the account password. This is useful for shared accounts.

Password never Expires

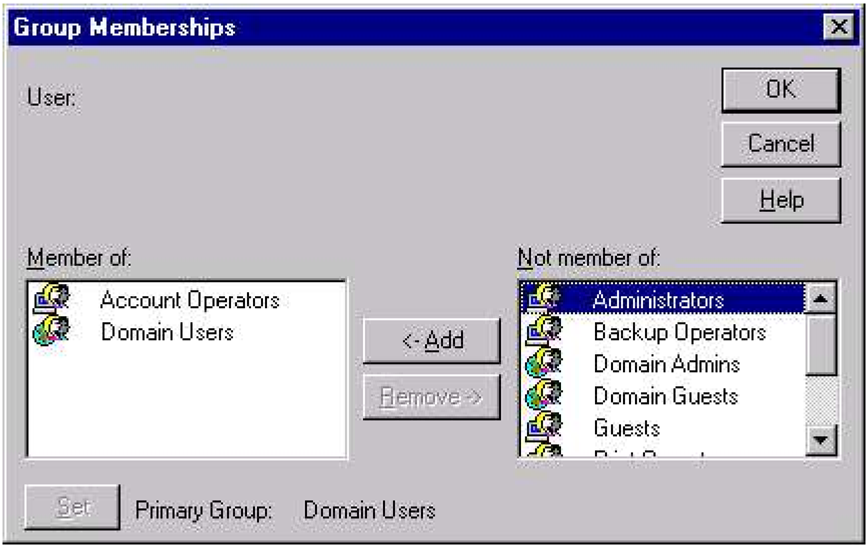
If set to yes, the user account ignores the password expiration policy, and the password for the account never expires. This is useful for accounts that represent services (such as the Replicator accounts) and accounts for which you want a permanent password (such as the Guest accounts).

Account Disabled

If set to yes, the account is disabled and none can log on to it until it is enabled (it is not, however, removed from the database). This is useful for accounts that are used as templates.

At the bottom of the *New User* dialog box are five buttons: *Groups*, *Profile*, *Hours*, *Logon To*, *Account and Dialin*. These buttons help to define the properties of the user account. In workstation only Groups, Profile, and Dialin appear.

- A user account is assigned to group membership by clicking the **Groups** button to display the Group Memberships dialog. This dialog allows the account administrator to assign and revoke group membership privileges (discussed in previous section).



User:

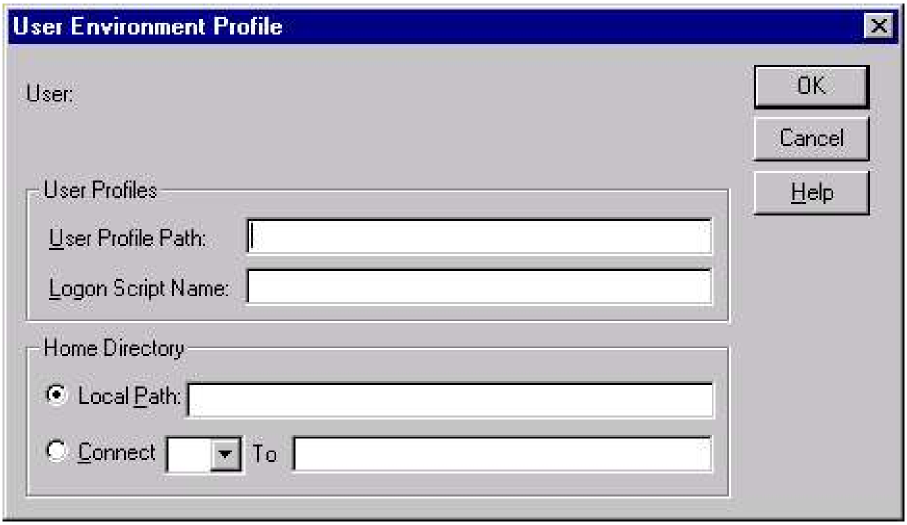
Member of:
Account Operators
Domain Users

Not member of:
Administrators
Backup Operators
Domain Admins
Domain Guests
Guests

Primary Group: Domain Users

Fig 8.4 Allotting Group Membership

- The Profile button lets you select custom settings for one or more users.



User:

User Profile Path:

Logon Script Name:

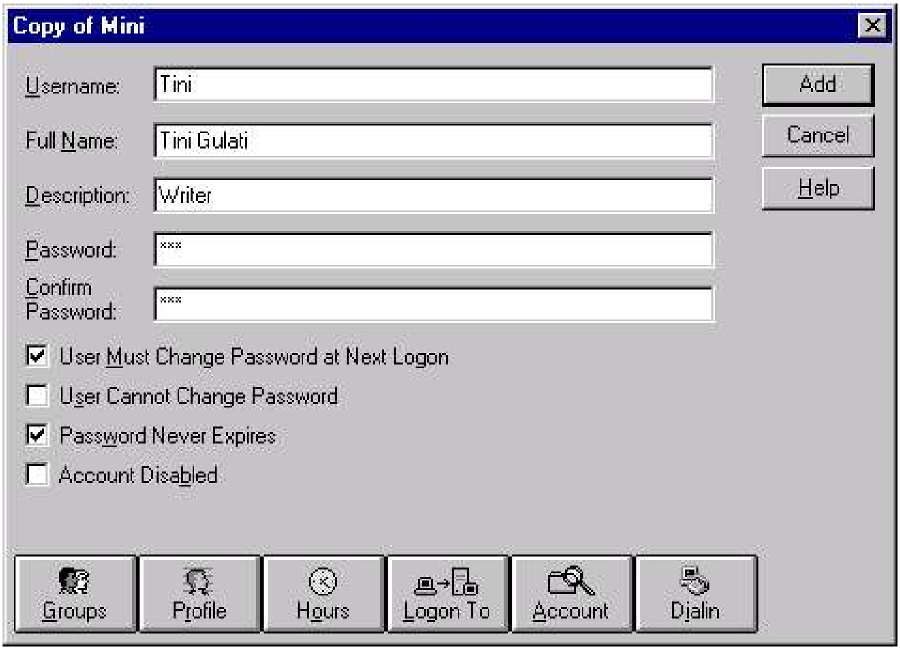
● Local Path:

○ Connect To

Fig 8.5 Specifying User Environment Profile

COPYING A USER ACCOUNT

User Manager allows you to copy an existing user account as a template to create a new account. If you are handling a large network, this option ease your job allot. You could, as a system administrator, create the template account containing all the attributes for all the departments. When you have to create a new user account, you can copy the appropriate template account to reflect the details pertinent to the new user. To copy an user account, select the user account, whose copy you want to create and click **User ➢ Copy**.



Copy of Mini

Username: Tini

Full Name: Tini Gulati

Description: Writer

Password: ***

Confirm Password: ***

☑ User Must Change Password at Next Logon

☐ User Cannot Change Password

☑ Password Never Expires

☐ Account Disabled

Fig 8.6 Copying User

MODIFYING USER ACCOUNT

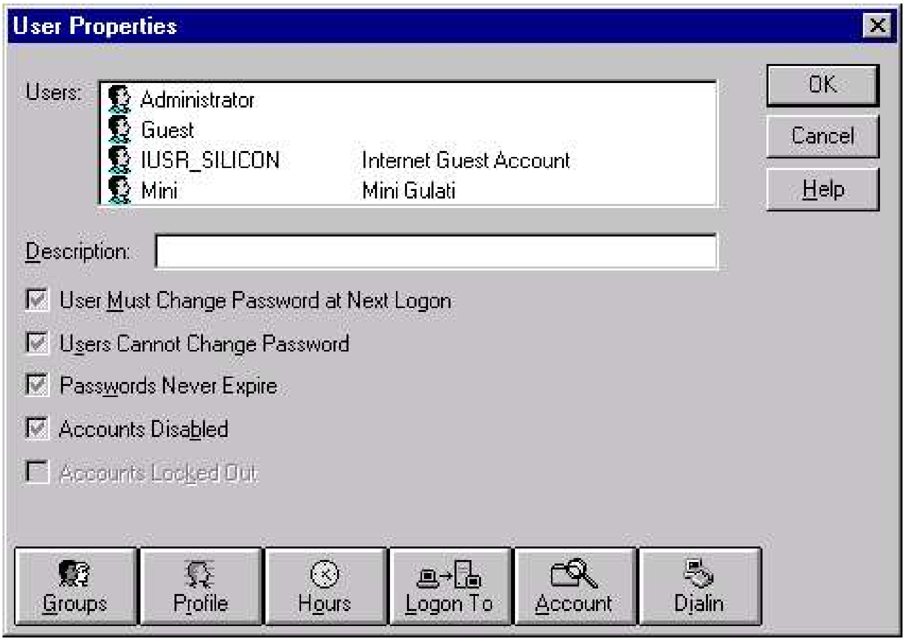
You could also delete the user account. To delete the particular user account, select the user and press **Del**. NT asks you for confirmation.

To modify the user account, double click on the user account and press Enter or select **User ➢ Properties**. This brings the User Property Sheet. You could also select the multiple user and press Enter to bring up combined User property sheet.

To select multiple user, press Ctrl while clicking on the users to be selected or press Shift and click on the first and last user to select all the user in between. Now if you select **User ➢ Properties**, the User Property Sheet appear as shown in Fig 8.7.

You can select all members of a particular group within a domain with the **Select Users** command in the User menu. This brings up the Select User dialog box (Fig 8.8). Now select the group, whose members you want to select for modification.

When modifying multiple accounts, only the options common to all the users are displayed. The additional account property buttons located at the bottom of the dialog allow the administrator to assign common attributes to all the selected user accounts.



Users:

Administrator	
Guest	
IUSR_SILICON	Internet Guest Account
Mini	Mini Gulati

Description:

☑ User Must Change Password at Next Logon

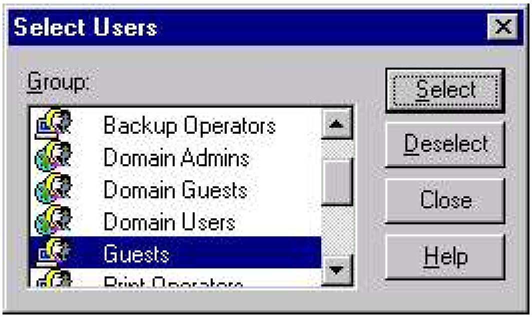
☑ Users Cannot Change Password

☑ Passwords Never Expire

☑ Accounts Disabled

□ Accounts Locked Out

Fig 8.7 Editing User Properties

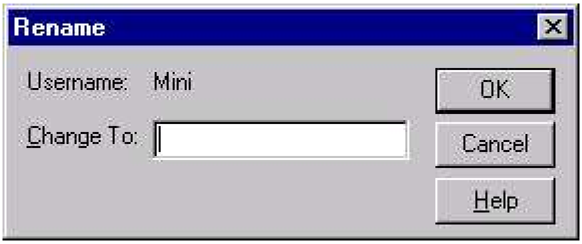


Group:

- Backup Operators
- Domain Admins
- Domain Guests
- Domain Users
- Guests
- Print Operators

Fig 8.8 Selecting User

You can also rename any user account in Windows NT, including the Administrator and Guest default accounts, with User Manager. Select **User ➢ Rename** to bring up the rename dialog box. (Fig 8.9)



Username: Mini

Change To:

Fig 8.9 Renaming User

CREATING & MANAGING GROUPS

LOCAL GROUP

To create a new local group, Select **Start ➢Programs ➢ Administrative Tools (Common)➢User Manager**. Now select **User ➢ New Local Group**. This brings the New Local Group dialog box. (Fig 8.10)

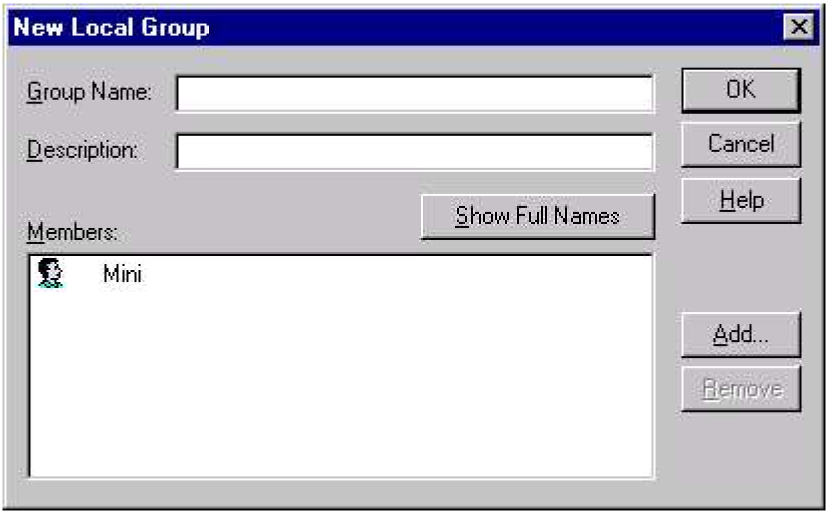


Fig 8.10 Creating Local Group

In the Group Name text box, type the name you want to give the new group. You can use any combination of uppercase and lowercase letters but not the following characters:

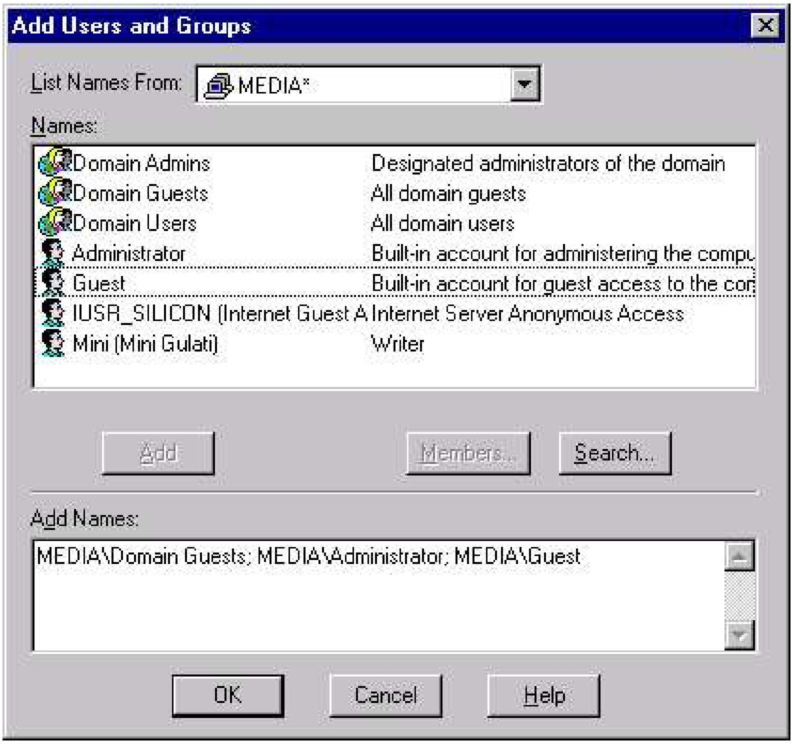
" / \ [ ] : ; | = , + * ? < >

In the Description text box, type an optional description for the group.

Next, you can begin assigning users to the group, or you can leave that task for later. To do it later, just click **OK**. Now to make members of the new local group, click the **Add** command button to bring up the Add dialog box. (Fig 8.11).

From the Names list, select all the groups and users you want to add to the new group; then choose **Add**. If you want to view the members of a listed group, select the group and choose the **Members** button. To delete a user or group from the group, click in the **Add Names** text box, highlight the name(s) to be deleted, and then press Delete. To search for a name or group locally or in a specific domain, click **Search**.

Click **OK**. The User Manager dialog box reappears. The new local group appears in the Groups list box.



Add Users and Groups

List Names From: MEDIA*

Names:

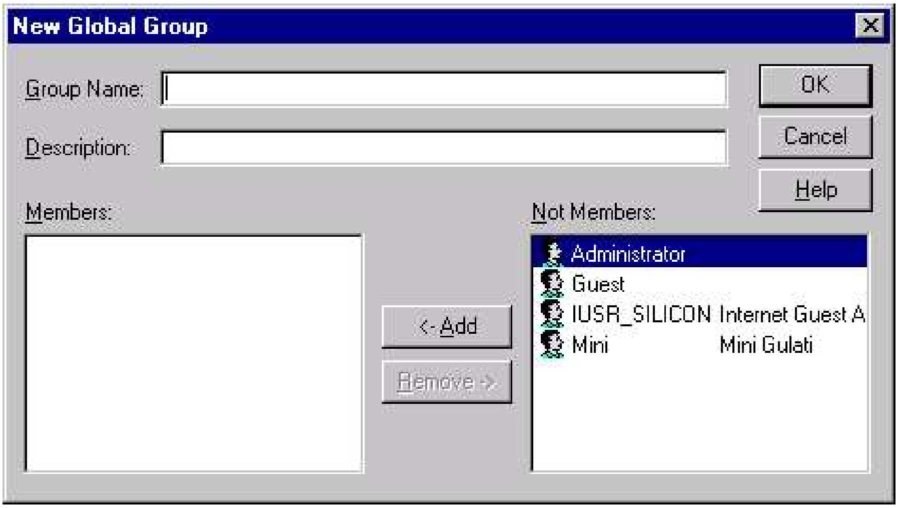
Domain Admins	Designated administrators of the domain
Domain Guests	All domain guests
Domain Users	All domain users
Administrator	Built-in account for administering the compu
Guest	Built-in account for guest access to the cor
IUSR_SILICON (Internet Guest A	Internet Server Anonymous Access
Mini (Mini Gulati)	Writer

Add Names: MEDIA\Domain Guests; MEDIA\Administrator; MEDIA\Guest

Fig 8.11 Adding User & Groups

GLOBAL GROUP

To create a new global group, select **Start ➤ Programs➤ Administrative Tools (Common) ➤ User Manager for Domains**. Now select **User ➤ New Global Group**.



New Global Group

Group Name:

Description:

Members:

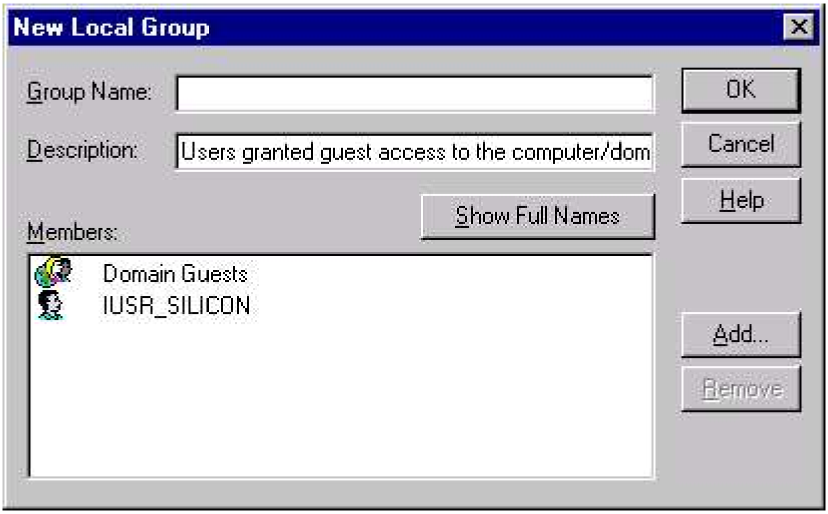
Not Members:

Administrator	
Guest	
IUSR_SILICON	Internet Guest A
Mini	Mini Gulati

Fig 8.12 Adding New Global Group

COPYING A GROUP

User Manager allows you to copy an existing group so that the new group created has the same rights and members as the other group. To copy a group, select the group whose copy you want to create. Select **User ➤ Copy** to bring the Add New Local Group or Add New Global Group dialog appears, depending the type of group you selected. (Fig 8.13)



New Local Group

Group Name:

Description: Users granted guest access to the computer/dom

Members:

Domain Guests

IUSR_SILICON

Fig 8.13 Adding New Local Group

Type a new name and description for the group and select **OK**. You can also modify the group membership at this point.

DELETING GROUPS

Windows NT allows you to delete only user-defined groups. The built-in groups of Windows NT Server 4.0 can't be deleted. To delete a group (local or global) select the group to be deleted. Now choose **User ➤ Delete**. You must remember that each group you create receives a unique security identifier (SID). When you delete a group and recreate a group with the identical name, the new group receives a different SID and doesn't inherit the original group's attributes.

RIGHTS & PERMISSIONS

Each user's capabilities are determined by the rights and privileges assigned to the user. A user's rights refer to system-wide objects and tasks, and permissions apply to specific objects such as files and printers.

When you create a user account on a Windows NT network, you'll frequently place that user into one or more of the built-in groups. As a member of a built-in group, a user "inherits" rights from the group.

If a user is a member of more than one group, the user inherits all the rights from all the groups to which the user belongs.

PERMISSIONS

Permissions assigned to a user refer to the specific files, folders, and hardware devices that are accessible to a user. They are the access parameters associated with a resource. In other words, permissions define the rules by which particular resource is used. These permissions can be set as either object permissions or share permissions.

Object Permission

In Windows NT, each object can have associated with it its own set of permissions, often called object permissions, which limit local access to the resource. e.g. you can set read-only permission for a folder for Guest group. Then anyone who logs on locally will be restricted to only read that folder.

Share Permission

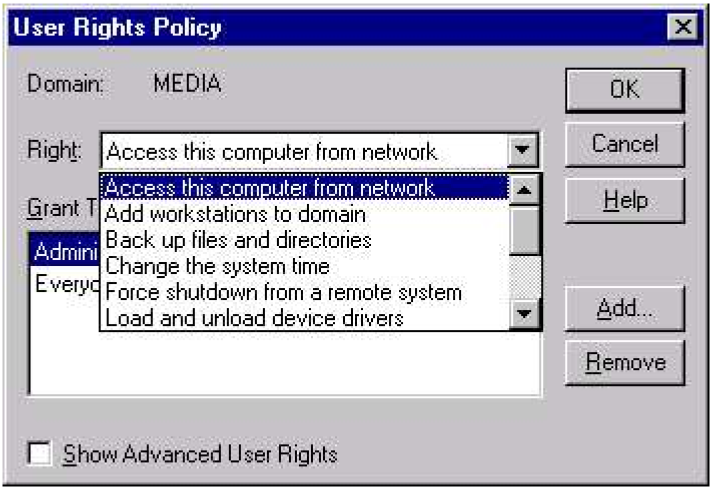
You can also attach share permissions to resources shared on a computer. These permissions determine the level of access remote users across the network have to the shared resource. e.g. in above case instead of assigning read-only object permission to a folder, you could share the folder and then assign a set of share permissions different from the local object permissions. This way, any member of the Guests group could have one set of permissions for the folder when they log on locally to the workstation and a different set of permissions when they access the resource from across the network.

USER RIGHTS

A right gives group members (or individual users) the authority to perform various actions across the network. All rights are assigned by User Manager. The rights assigned to a user directly affect the tasks that a user can perform on the network.

User rights are assigned in the User Rights Policy dialog box in User Manager or User Manager for Domains. To access the User Rights Policy dialog box, start User Manager for domains. In the User Manager dialog box, select **Policies ➢ User Rights**. (Fig 8.14).

A Windows NT network has two categories of rights: basic and advanced. The default configuration of User Right dialog box displays only basic user rights. To view the advance user rights, click on the **Show advance User rights** button. Following section lists and describes each of the Windows NT basic user rights.



User Rights Policy

Domain: MEDIA

Right: Access this computer from network

Access this computer from network
Add workstations to domain
Back up files and directories
Change the system time
Force shutdown from a remote system
Load and unload device drivers
Grant T
Admini
Everyo
OK
Cancel
Help
Add...
Remove
Show Advanced User Rights

☐ Show Advanced User Rights

Fig 8.14 Specifying User Right Policy

Access This Computer from Network

Authorizes a user to access a computer over the network.

Add workstations to domain

Authorizes a user to cause workstation computers to join the domain.

Back up files and directories

Authorizes a user to back up files and folders. This right supersedes permissions on files and folders.

Change the system time

Authorizes a user to change the time on the Windows NT computer's internal clock.

Force shutdown from a remote system

This right is not currently implemented. It is reserved for future use.

Load and unload device drivers

Allows a user to dynamically load and unload device drivers.

Log on locally

Allows a user to log on at the computer.

Manage auditing and security log

Allows a user to manage the auditing of files, directories, and other objects. A user with this right can use the Security tab in the Properties dialog box to specify auditing options for the selected objects, users and groups, and types of access.

Restore files and directories

Allows a user to restore files and directories of the computer. This right supersedes files and directory permissions.

Shut down the system

Allows a user at the computer to shut down a computer running Windows NT Workstation or Windows NT Server.

Take ownership of files or other objects

Allows a user to take ownership of files, directories, and other objects of the computer.

TRUST RELATIONSHIPS

To manage the interaction between multiple domains, Trust Relationships are necessary. Trust Relationships enable users from one domain to access shared resources located in other domains. Without Trust Relationships, the benefits of single user account logon and centralized administration would not be possible. If no trust relationship exists between two domains, users would have to have user accounts (and passwords) in both domains to access shared resources in both domains.

Two primary terms are used to refer to a trust relationship between two domains: trusting domain and trusted domain.

The trusting domain is the domain that has resources to share with user accounts in the trusted domain. The trusting domain trusts the trusted domain.

The trusted domain is the domain that contains the user accounts that want to access resources in the trusting domain. The trusted domain is trusted by the trusting domain.

Let us consider an example. MEDIA and RGC are two domains. If you want to access the resources of MEDIA domain, while logging on to RGC domain, then RGC is the trusted domain (domain being trusted by other domain) and MEDIA is the trusting domain (domain trusting the other domain to let the other domain use its resources)(Fig 8.15).

To establish a one-way trust relationship (a trust relationship where users of one domain - RGC - will be able to share the resources of other domain - MEDIA - but the users of other domain- MEDIA - will not be able to share the resources of RGC), you require to perform two different steps in two different domains:

- The domain that will be the trusted domain adds a domain to its list of trusting domains. (On RGC, MEDIA is added as trusting domain)
- The trusting domain must add the first domain to the list of trusted domains. (On MEDIA, RGC is added as trusted domain)

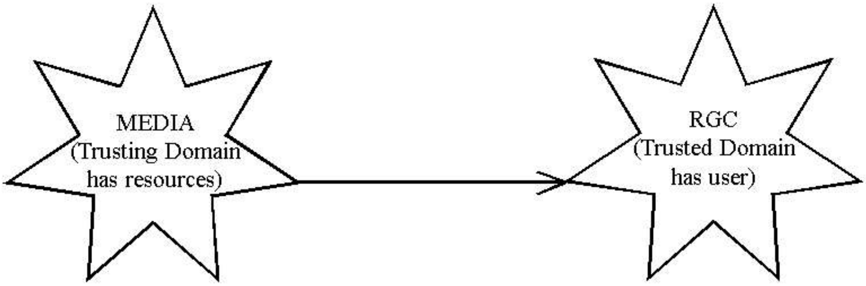
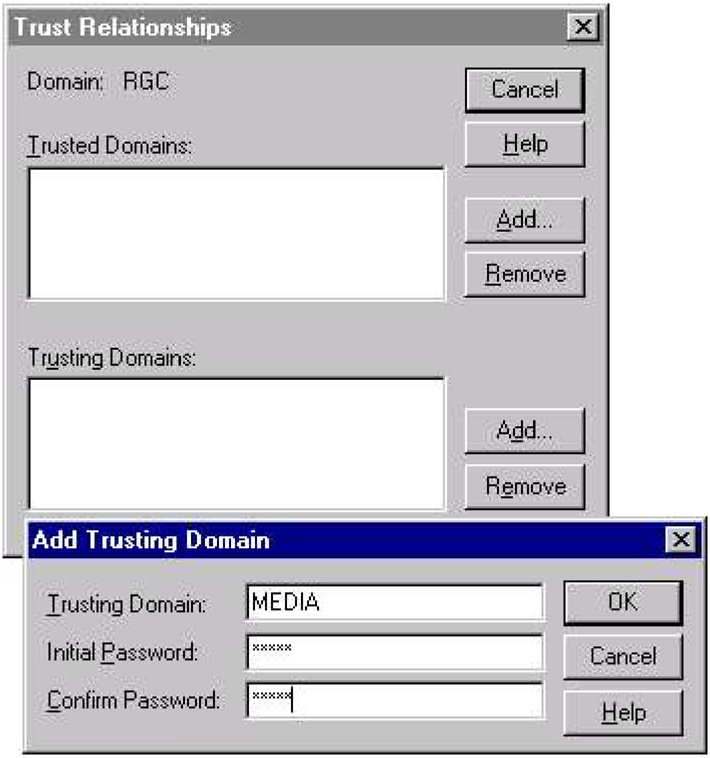


Fig 8.15 Trust Relationship

Thus for step 1, Start User Manager on RGC domain and select **Policies ➢ Trust Relationship** to bring Trust Relationship dialog box. Now Click on **Add** button in trusting domain section to bring up Add trusting domain dialog box. Now add MEDIA as the trusting domain and give a password. Reconfirm the password as press OK.



Domain: RGC

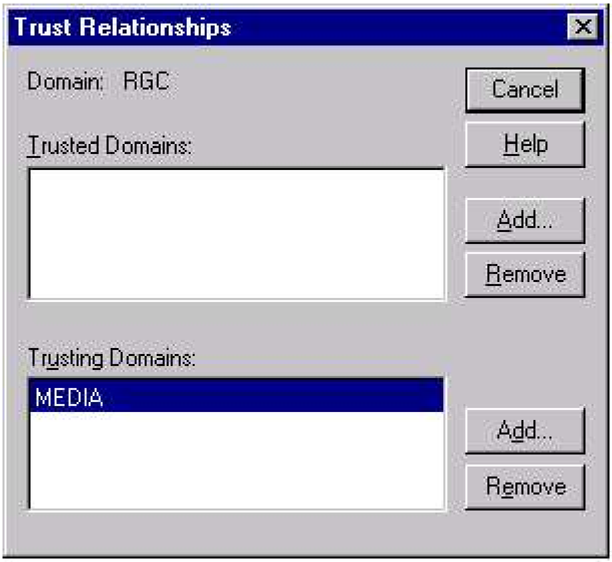
Trusting Domain: MEDIA

Initial Password: *****

Confirm Password: *****

Fig 8.16 Adding Trusting Domain

Thus MEDIA appears as trusting domain for RGC. (Fig 8.17)



Trust Relationships

Domain: RGC

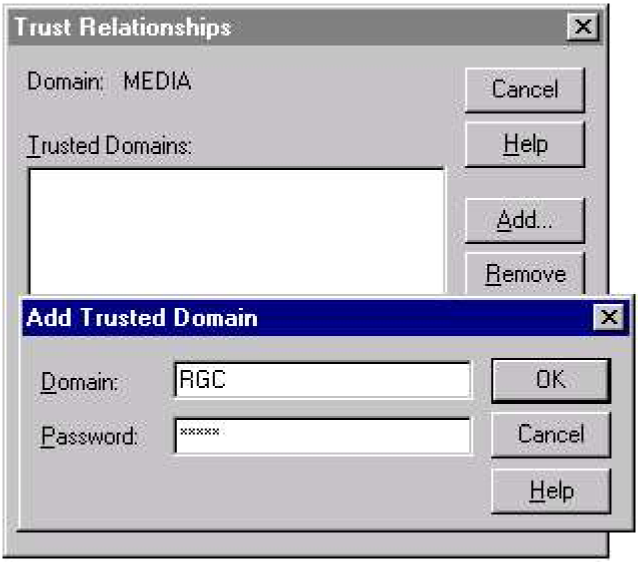
Trusted Domains:

Trusting Domains:

MEDIA

Fig 8.17 After Adding Trusting Domain

Now in Step 2, log on to MEDIA domain and start User Manager. Select **Policies** ➤ **Trust Relationship** to bring Trust Relationship dialog box. Now Click on **Add** button in trusted domain section to bring up Add trusted domain dialog box. Now add RGC as the trusted domain and give the same password as given in step 1. (Fig 8.18)



Trust Relationships

Domain: MEDIA

Trusted Domains:

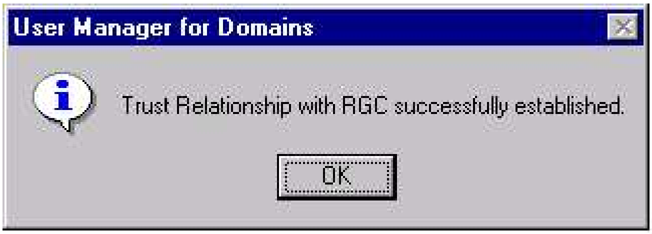
Add Trusted Domain

Domain: RGC

Password: *****

Fig 8.18 Adding Trusted Domain

After a moment, a dialog box appears declaring the success of trust relationship (Fig 8.19).



User Manager for Domains

Trust Relationship with RGC successfully established.

Fig 8.19 The confirmation for Trust Relationship

The Trust Relationship dialog box appears and displays RGC as the trusted domain

MANAGING ACCOUNT POLICY

This chapter focuses on the Policies menu in User Manager. The Policies menu provides three main configurable options: Account Policies, User Rights and Auditing.

The Account Policy lets you configure two things : one enables you to configure password restrictions, and another enables you to set the account lockout policy.

To configure Account policy, start User Manager (or User Manager for Domains). In the User Manager dialog box, select **Policies ➤ Account**. The Account Policy dialog box appears, as shown in Fig 8.20.

Settings in the Account Policy dialog box apply to all users in the domain (or to all users on a computer, if it is not a domain controller). You can’t set individual account policies.

Password restrictions

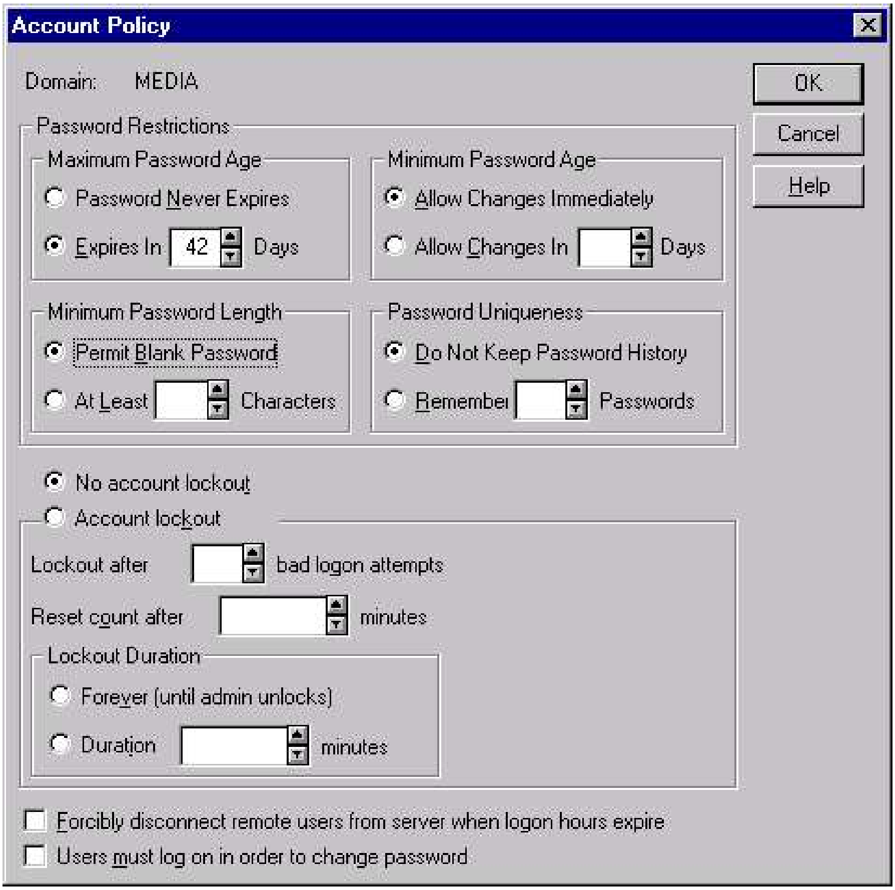
The Password Restrictions section of the Account Policy dialog box has four configurable options: Maximum Password Age, Minimum Password Age, Minimum Password Length and Password Uniqueness.

Maximum password age

Maximum Password Age determines the maximum number of days a user may use the same password. Two selections are available in this section: Password Never Expires, or Expires in defined number of Days.

Minimum Password Age

Minimum Password Age determines the minimum number of days a user must keep the same password. Two selections are available in this section: Allow Changes Immediately, or Allow Changes in xx Days. The default setting is Allow Changes Immediately.



Account Policy

Domain: MEDIA

Password Restrictions

Maximum Password Age

○ Password Never Expires

● Expires In 42 Days

Minimum Password Age

● Allow Changes Immediately

○ Allow Changes In Days

Minimum Password Length

● Permit Blank Password

○ At Least Characters

Password Uniqueness

● Do Not Keep Password History

○ Remember Passwords

● No account lockout

○ Account lockout

Lockout after bad logon attempts

Reset count after minutes

Lockout Duration

○ Forever (until admin unlocks)

○ Duration minutes

□ Forcibly disconnect remote users from server when logon hours expire

□ Users must log on in order to change password

Fig 8.20 Specifying Account Policy

Minimum Password Length

Minimum Password Length specifies the minimum number of characters required in users' passwords. Two selections are possible in this section: Permit Blank Password, or atleast xx Characters.

Account lockout

The Account lockout section of the Account Policy dialog box specifies how Windows NT treats user accounts after several successive unsuccessful logon attempts have occurred.

Select **Forcibly disconnect remote users from server when logon hours expire** option to disconnect users from the domain controllers in the domain, whose logon hours has expired.

Select **Users must log on in order to change password**, to stop user to logon if password has expired. In such case only the administrator must change the user's password.

AUDITING WINDOWS NT

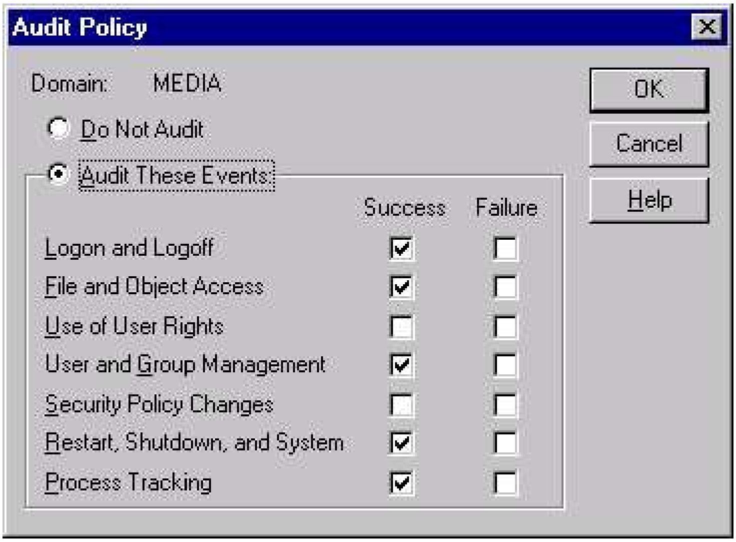
Windows NT enables you to monitor a fairly large number of events that can occur in your system. Many a times, when the applications crash, it is required to record the progress of the application so that you can trace the progress to determine where the problems occurred. This is where Auditing comes in picture. Auditing also enables you to detect and potentially stop the hackers from destroying your server.

Windows NT has the right kind of auditing plan to meet the wide range of challenges and also enable the users to pick from various forms of auditing to suit their individual needs.

When enabled, Windows NT auditing produces a log of specified events and activities that occur on a Windows NT computer. Audited events are written to the security log in Event Viewer. Windows NT auditing is divided into two areas: system access and object access. System access auditing is configured by using User Manager or User Manager for Domains. Object access auditing is configured in the properties dialog boxes for files, folders, and printers. By default, auditing is turned off.

To access the Audit Policy dialog box and to enable auditing, start User Manager for Domains. In the User Manager dialog box, select **Policies ➢ Audit**. This brings the Audit Policy dialog box. (Fig 8.21)

Here you can see that default setting is Do not Audit. To enable auditing, select the radio button next to Audit These Events, and select at least one Success or Failure check box. Click **OK**.



Domain: MEDIA

○ Do Not Audit

● Audit These Events:

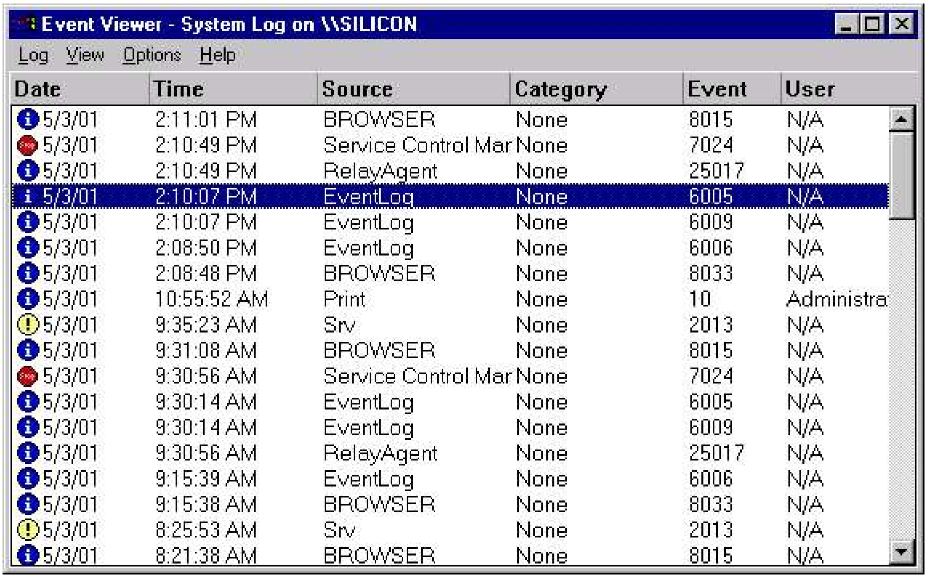
	Success	Failure
Logon and Logoff	☑	□
File and Object Access	☑	□
Use of User Rights	□	□
User and Group Management	☑	□
Security Policy Changes	□	□
Restart, Shutdown, and System	☑	□
Process Tracking	☑	□

Fig 8.21 Specifying Audit Policy

When a Success check box is selected, Windows NT generates an audit event each time a user successfully performs the audited task. When a Failure check box is selected, Windows NT generates an audit event each time a user attempts to perform an audited task but fails.

EVENT VIEWER

The heart of auditing under Windows NT lies in the Event Viewer. You access the Event Viewer through the **Start ➢ Administrative Tools (Common) ➢ Event Viewer** (Fig 8.22). The Event Viewer both displays auditing results and enables you to perform most of the control functions for NT auditing. This is a clean, data-driven interface that focuses on the actual logged information. The control functions are located on the menu across the top.



Date	Time	Source	Category	Event	User
ℹ 5/3/01	2:11:01 PM	BROWSER	None	8015	N/A
⛔ 5/3/01	2:10:49 PM	Service Control Mar	None	7024	N/A
ℹ 5/3/01	2:10:49 PM	RelayAgent	None	25017	N/A
ℹ 5/3/01	2:10:07 PM	EventLog	None	6005	N/A
ℹ 5/3/01	2:10:07 PM	EventLog	None	6009	N/A
ℹ 5/3/01	2:08:50 PM	EventLog	None	6006	N/A
ℹ 5/3/01	2:08:48 PM	BROWSER	None	8033	N/A
ℹ 5/3/01	10:55:52 AM	Print	None	10	Administra
⚠ 5/3/01	9:35:23 AM	Srv	None	2013	N/A
ℹ 5/3/01	9:31:08 AM	BROWSER	None	8015	N/A
⛔ 5/3/01	9:30:56 AM	Service Control Mar	None	7024	N/A
ℹ 5/3/01	9:30:14 AM	EventLog	None	6005	N/A
ℹ 5/3/01	9:30:14 AM	EventLog	None	6009	N/A
ℹ 5/3/01	9:30:56 AM	RelayAgent	None	25017	N/A
ℹ 5/3/01	9:15:39 AM	EventLog	None	6006	N/A
ℹ 5/3/01	9:15:38 AM	BROWSER	None	8033	N/A
⚠ 5/3/01	8:25:53 AM	Srv	None	2013	N/A
ℹ 5/3/01	8:21:38 AM	BROWSER	None	8015	N/A

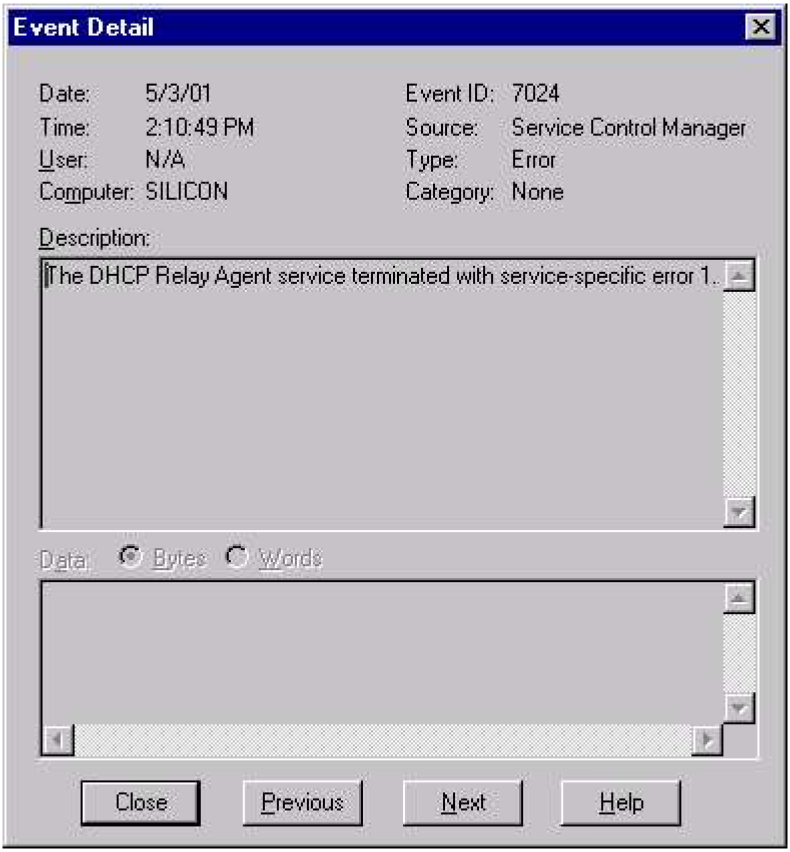
Fig 8.22 Event Viewer

The event viewer captures following information:

- Date of the event
- Time of the event
- Source of the event
- Category of the event
- Event number (a code you can reference)
- User ID that caused this event
- Computer identifier that caused the event
- Domain in which the event occurred
- A reason for the event
- Additional information specific to the event

- Type of event. This is not a text column; instead, the type of event is conveyed by an icon picture. The types of events you might see include errors, warnings, information, success audits, and failure audits.

Although these columns provides useful summary information, they don't really provide details to solve a nasty problem. To get the full details about a particular event, double-click that event. This brings a detailed display dialog, as shown in Fig 8.23.



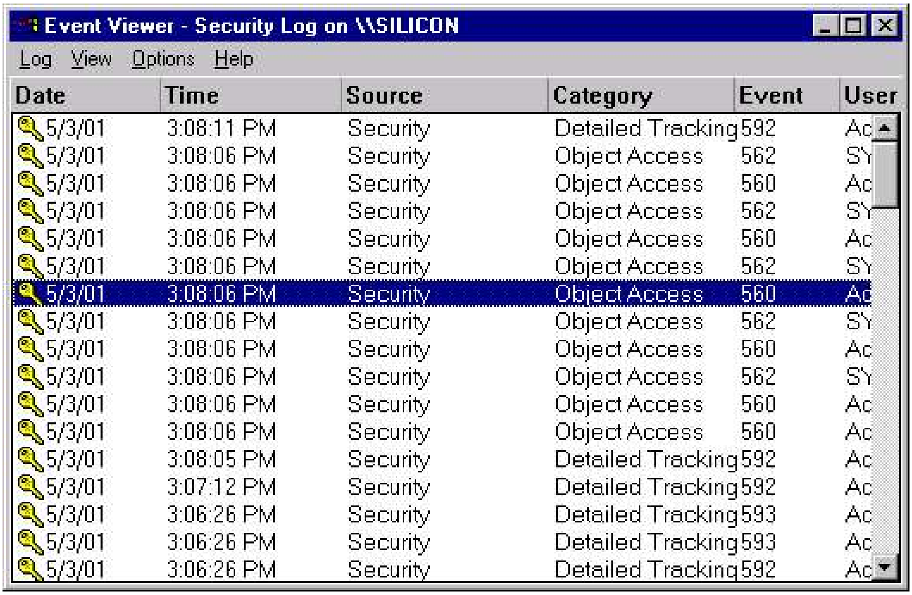
Date: 5/3/01
Time: 2:10:49 PM
User: N/A
Computer: SILICON
Event ID: 7024
Source: Service Control Manager
Type: Error
Category: None
Description:
The DHCP Relay Agent service terminated with service-specific error 1..

Fig 8.23 Event Details

This Event detail dialog box gives the information contained on the summary display, along with several other useful bits of information.

The Event Viewer can displays all three types of Windows NT audit records: system events, security events, and application events. You select which of these event types is displayed using the Log menu.

To display security log, select **Log ➢ Security**. Fig 8.24 shows a security log in Event Viewer. Notice that events are marked with keys (these designate success events). The unsuccessful events are designated with locks. Double-click an event you want to view in greater detail.



Date	Time	Source	Category	Event	User
5/3/01	3:08:11 PM	Security	Detailed Tracking	592	Ac
5/3/01	3:08:06 PM	Security	Object Access	562	SY
5/3/01	3:08:06 PM	Security	Object Access	560	Ac
5/3/01	3:08:06 PM	Security	Object Access	562	SY
5/3/01	3:08:06 PM	Security	Object Access	560	Ac
5/3/01	3:08:06 PM	Security	Object Access	562	SY
5/3/01	3:08:06 PM	Security	Object Access	560	Ac
5/3/01	3:08:06 PM	Security	Object Access	562	SY
5/3/01	3:08:06 PM	Security	Object Access	560	Ac
5/3/01	3:08:06 PM	Security	Object Access	562	SY
5/3/01	3:08:06 PM	Security	Object Access	560	Ac
5/3/01	3:08:06 PM	Security	Object Access	560	Ac
5/3/01	3:08:05 PM	Security	Detailed Tracking	592	Ac
5/3/01	3:07:12 PM	Security	Detailed Tracking	592	Ac
5/3/01	3:06:26 PM	Security	Detailed Tracking	593	Ac
5/3/01	3:06:26 PM	Security	Detailed Tracking	593	Ac
5/3/01	3:06:26 PM	Security	Detailed Tracking	592	Ac

Fig 8.24 Security Log of Event Viewer

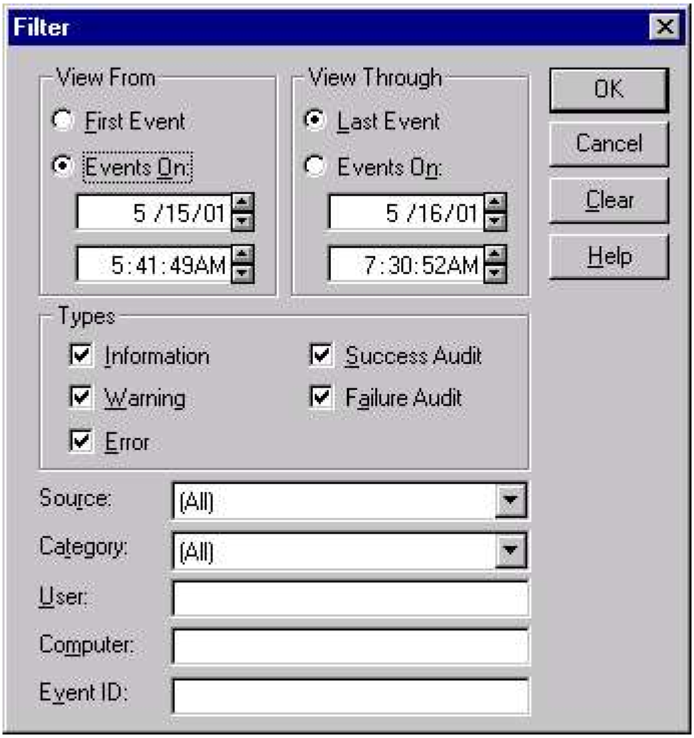
Filtering an Event

In Windows NT, so many events occur at a time, that some times, it becomes difficult and time consuming to locate the problem area. Event Viewer provides the facility to filter events on the basis of various factors to minimize the amount of data overload.

To filter events, select **View ➤ Filter** events to display the Filter dialog box. (Fig (8.25)

- In the View From section, select the Events On radio button. Then specify a date and time from which you want to display events in Event Viewer.
- In the View Through section, select the Events On radio button. Then specify a date and time upto which you want to display events in Event Viewer.
- The Event Viewer divides the events into five types - Information, Warning, Error, Success Audit & Failure Audit. In the Types section, select the type of event to report.
- In the Source drop-down list box, select the event source to view. This limits the report to a specific application, system service, or device driver to determine how often the error has occurred.
- You can further limit the report to a particular category by selecting it from the Category drop-down list box. Normally

there will be only security-related categories, or possibly no subcategories.



Filter

View From
○ First Event
● Events On:
5 /15/01
5:41:49AM

View Through
● Last Event
○ Events On:
5 /16/01
7:30:52AM

Types
☑ Information
☑ Success Audit
☑ Warning
☑ Failure Audit
☑ Error

Source: (All)
Category: (All)
User:
Computer:
Event ID:

Fig 8.25 Filtering Events

- In the User field, enter the user account you want to use to further limit the report.
- Enter the computer name in the Computer field to filter events that have occurred on the specific computer.
- If you are looking for a specific event, enter the event number in the Event ID field.

Once you enter the filtering characteristics, click **OK** to display the filtered events. Note that the title bar of the Event Viewer changes to include the word Filtered.

LOGGING ON

When a user logs on to a Windows NT computer or domain, the logon process is managed by the NetLogon Service. This Service is installed automatically during the installation of Windows NT. The service is configured, by default, to start automatically every time Windows NT is booted. The NetLogon Service in Windows NT is responsible for managing the logon process, pass-through authentication, and synchronization of the backup domain controllers (BDCs) with the primary domain controller (PDC) within a domain.

If you set up a domain, users who log onto Windows 3.x, Windows 95, and Windows NT systems can be made to use a logon script. These scripts are batch files, stored on the domain controllers and can be used to perform such actions as connect drive and printer assignments, or even to run programs such as running a virus scanning program.

THE LOGON PROCESS

To understand the NT logon process, it's better to have an understanding of the Windows NT Security Accounts Manager (SAM) database. Windows NT assigns every user account, group account, and computer account a unique security identifier (SID). All account information, including user names, passwords, group memberships, and SIDs are stored in a domain database called the SAM database. This database is created originally on the domain's PDC (and on each local Windows NT computer that is a non-domain controller). The SAM is stored in the <winntroot>\System32\Config folder.

When you begin the logon process by pressing Ctrl + Alt + Delete, the Logon Information dialog box appears, prompting you to enter a user name and password.

If the Windows NT Workstation computer is a member of a domain, an additional Domain drop-down list box is displayed. In the Domain drop-down list box, you can choose to log on using a user account from the domain or using a user account on the local computer. In this example, you are logging on using a user account on the local computer.

When you click **OK** in the Logon Information dialog box, Windows NT provides your logon information (user name, password, and domain/ local computer name) to the NetLogon Service. The NetLogon Service determines whether you are logging on using a user account on the local computer or a user account from the domain. In this example, you are logging on using a user account on the local computer. The NetLogon Service queries the local SAM to determine if your user account and password is valid. If your user name and password are validated, the NetLogon Service retrieves your user account's SID, and the SIDs for each group of which you are a member. The NetLogon Service combines your user and group SIDs to create an access token.

The NetLogon Services completes the logon process for you. For the rest of the logon session, Windows NT uses your access token to determine whether you can access resources. Every time you attempt to access a resource (such as a folder or a printer), Windows NT compares the SIDs in your access token to the SIDs contained in the access control list (ACL) for the resource you want to access. If the SIDs in your access token are listed in the ACL for the resource, you are granted access to the resource.Anytime a user logs on to a Windows NT computer using a user account that is not contained in the local computer's SAM, pass-through authentication is used to validate the user.

PASS-THROUGH AUTHENTICATION

Pass-through authentication enables a user to log on to a Windows NT computer by using a user account from the domain or from a trusted domain. Without pass-through authentication, the single user account logon/single password feature of Directory Services would not be possible.

Pass-through authentication occurs when a user account can't be validated by the NetLogon Service on the local computer. The NetLogon Service on the local computer forwards (passes-through) the logon request (and logon information) to the NetLogon Service on a Windows NT Server domain controller for validation. The domain controller validates the user account and passes the appropriate SIDs back to the NetLogon Service on the local computer to which the user is logging on. The NetLogon Service on the local computer completes the user's logon and creates the user's access token.

EXERCISE

Fill in the Blanks:

1. _______ is the main tool used to create and manage user accounts.
2. The ________ domain is trusted by the __________ domain.
3. _____________ determines the minimum number of days a user must keep the same password.
4. By default, Auditing is turned ____.
5. Event Viewer can displays three types of Windows NT audit records: ___________, ___________ and __________.
6. Event Viewer divides the events into five types - ________, _______, ______, __________ & ___________.

State True or False:

1. Guest is a Built-in Global Group.
2. A global group can include only user accounts from the domain in which the group was created.
3. A local group can contain various user accounts and global groups.
4. Auditing, when enabled, produces a log of only failed events.
5. One-way trust relationship can be established by configuring on one of the domain only.

Answer the following question:

1. When should a user account be disabled?
2. What are the two types of groups available in Windows NT? Differentiate between them.
3. List down the various built-in groups available.
4. Discuss various types of rights in Windows NT network.
5. What do you understand by trust relationship?
6. Define auditing. What is its advantage?
7. What do you understand by the logon script?
8. Differentiate between logon scripts and user profiles.

Try the following practicals:

1. Assume that an organization has different departments – PRODUCTION, MARKETING, SALES, FINANCE. Create five users in each domain, ensuring that their usernames reflect the department they work in.
2. Create New Local User “SILICON”, in the Dialog box. Then check the “User Must Change Password at Next Logon”. Select Properties of this user and assign the right to log on locally from policies – User rights tab associated with User Rights Policy. Now try to log on using user name as SILICON.

3. Ensure that you are in a network with atleast two domains. Try to establist one-way trust relationship between two domains. Extend it to Two-way trust relationship.

4. You are required to audit Successful and Failed logons in Windows NT using User Manager. Verify by successfully logging and attempt unsuccessful logons.

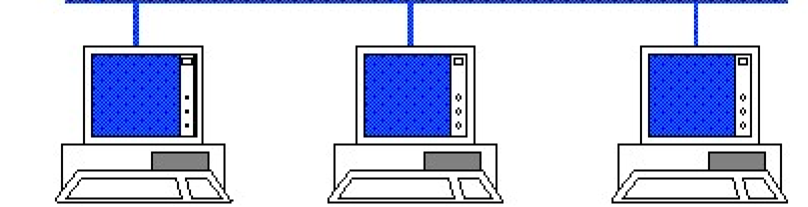
5. Use the Event Viewer to filter out application events that taken place over a period of last 15 days from today's date.

6. Select Application in the Log menu, Here the events that have been logged are shown. Select Clear All Events in the log menu.

CHAPTER 9

Printing Administration

PRINTING SUPPORT IN WINDOWS NT
CONFIGURING PRINT SERVER PROPERTIES
CONFIGURING PRINTERS



PRINTING SUPPORT IN WINDOWS NT

In Windows NT, the term printer does not represent a physical device that produces printed output. Rather, a printer is the software interface between the Windows NT operating system and the device that produces printed output. In Windows NT, the term print device refers to the physical device that produces printed output, what is more commonly referred to as a “printer.”

There are two ways to install and configure a printer in Windows NT: you can either create a printer, or you can connect to a shared network printer. Creating a printer involves installing and configuring all of the drivers needed to use a locally managed print device. Connecting to a shared network printer involves installing and configuring all of the drivers needed to use a print device that is managed by another computer on the network. You can either connect to a shared network printer by using the Add Printer Wizard in the Printers folder, or you can use drag-and-drop printing to connect to a shared network printer.

Both creating a printer and connecting to a printer are called “adding a printer,” because both processes use the Add Printer Wizard.

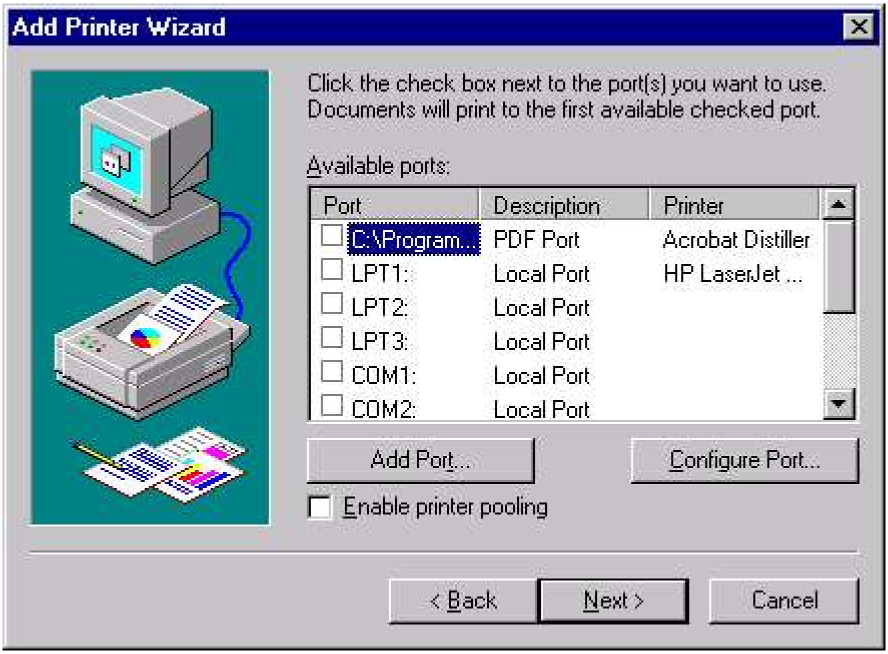
USING THE ADD PRINTER WIZARD

Windows NT provides the Add Printer Wizard to simplify installing printers, and - the Printers folder - for running the wizard and for managing printing processes. You can open the Printers folder in the following ways:

- From the Start menu, point to Settings, and then click **Printers** or in My Computer, double-click **Printers** or in Control Panel, double-click **Printers**.

To install a printer with the Add Printer Wizard.

- In the Printers folder, double-click **Add Printer**. The Add Printer Wizard leads you through the process of setting up and configuring a printer.
- The only difference between installing a network printer and a local printer with the Add Printer Wizard is that you must specify the path to the network printer or browse to find its network location. If you select the My Computer option, the wizard offers you various ports on which you want to install the printer.
- Select a port in the Available Ports list box (Fig 9.1). If the port you want to use is not listed, click the **Add Port** command button and follow the directions given. Click **Next**.



Click the check box next to the port(s) you want to use. Documents will print to the first available checked port.

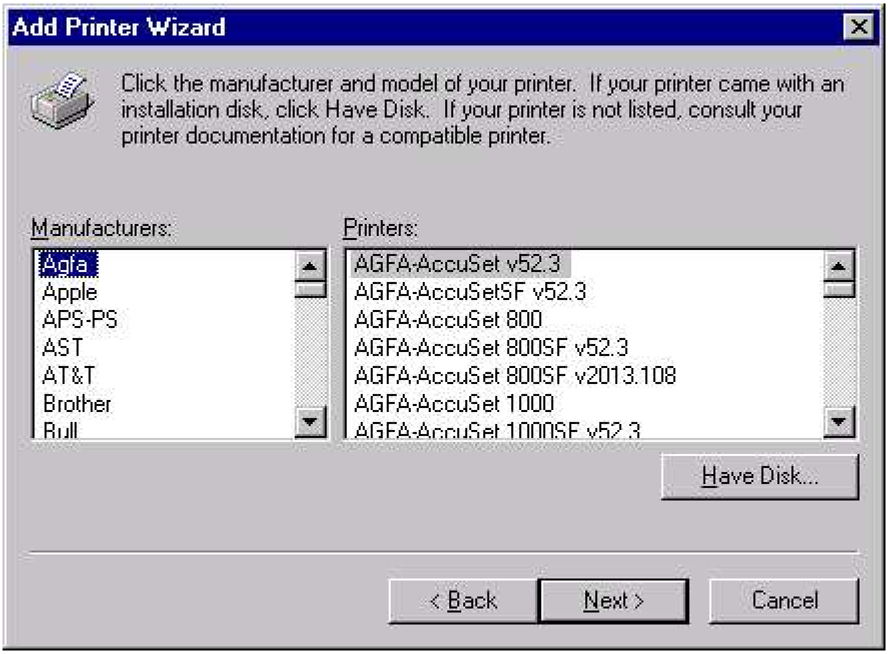
Available ports:

Port	Description	Printer
□ C:\Program...	PDF Port	Acrobat Distiller
□ LPT1:	Local Port	HP LaserJet ...
□ LPT2:	Local Port	
□ LPT3:	Local Port	
□ COM1:	Local Port	
□ COM2:	Local Port	

□ Enable printer pooling

Fig. 9.1 Specifying Port for Printer

- Click **Next** to select the appropriate manufacturer and print device model. (Fig 9.2)



Click the manufacturer and model of your printer. If your printer came with an installation disk, click Have Disk. If your printer is not listed, consult your printer documentation for a compatible printer.

Manufacturers:

Agfa
Apple
APS-PS
AST
AT&T
Brother
Bull

Printers:

AGFA-AccuSet v52.3
AGFA-AccuSetSF v52.3
AGFA-AccuSet 800
AGFA-AccuSet 800SF v52.3
AGFA-AccuSet 800SF v2013.108
AGFA-AccuSet 1000
AGFA-AccuSet 1000SF v52.3

Fig. 9.2 Adding a New Printer

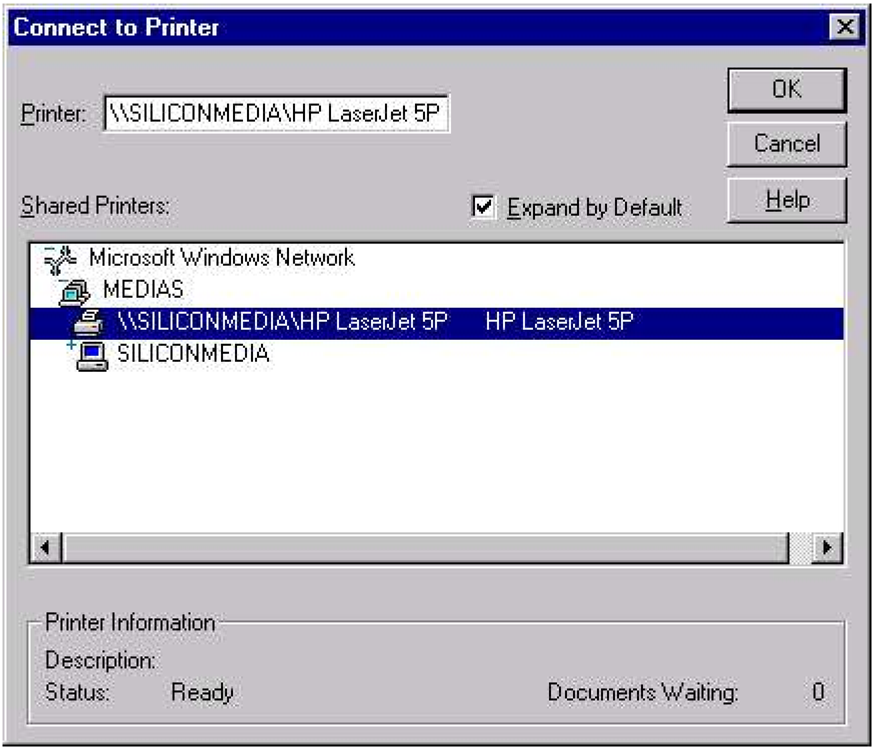
- Type a printer name, or accept the default. Click **Next**.
- Choose whether to share the printer. You can share or stop sharing the printer later by using Printers properties. Click **Next**.
- Choose whether to print a test page. Click **Finish**.

You can modify a printer's properties any time after the printer is created by right-clicking the printer's icon (in the Printers folder), and then selecting Properties from the menu that appears.

CONNECTING TO NETWORK PRINTER

To connect to a Windows NT shared network printer, open the Printers folder and double-click the **Add Printers** icon. In the Add Printer Wizard dialog box select **Network Printer Server**, and click **Next** to bring the Connect to Printer dialog box.

In the Printer text box, type in a complete path to the network printer to which you want to connect, in the form of \\server_name\printer_name. Or, use the browse list in the Shared Printers list box to select the network printer to which you want to connect. Then click **OK**.



Printer: \\SILICONMEDIA\HP LaserJet 5P

Shared Printers: ☑ Expand by Default

Microsoft Windows Network
MEDIAS
\\SILICONMEDIA\HP LaserJet 5P HP LaserJet 5P
SILICONMEDIA

Printer Information
Description:
Status: Ready Documents Waiting: 0

Fig 9.3 Connecting to Printer

Choose whether you want this printer to be your default printer. Click **Next** to Finish. You are now connected to a shared network printer.

PRINTING FROM THE ACTIVE DESKTOP

Once you have installed a printer, you can create a shortcut to it on your Active Desktop. This enables you to quickly print a document by simply dragging it onto the shortcut you create.

To print a document from the Active Desktop

- On the Start menu, point to Settings, and then click **Printers**.
- Right-click the printer's icon and drag it onto the Active Desktop.
- Click **Create Shortcut(s) Here**.
- Drag a document from My Documents, Windows Explorer, or My Computer onto the printer shortcut on your Active Desktop.

DELETING A PRINTER

If you want to remove an installed printer, just drag the printer's icon from the Printer window into the Recycle Bin.

CONFIGURING PRINT SERVER PROPERTIES

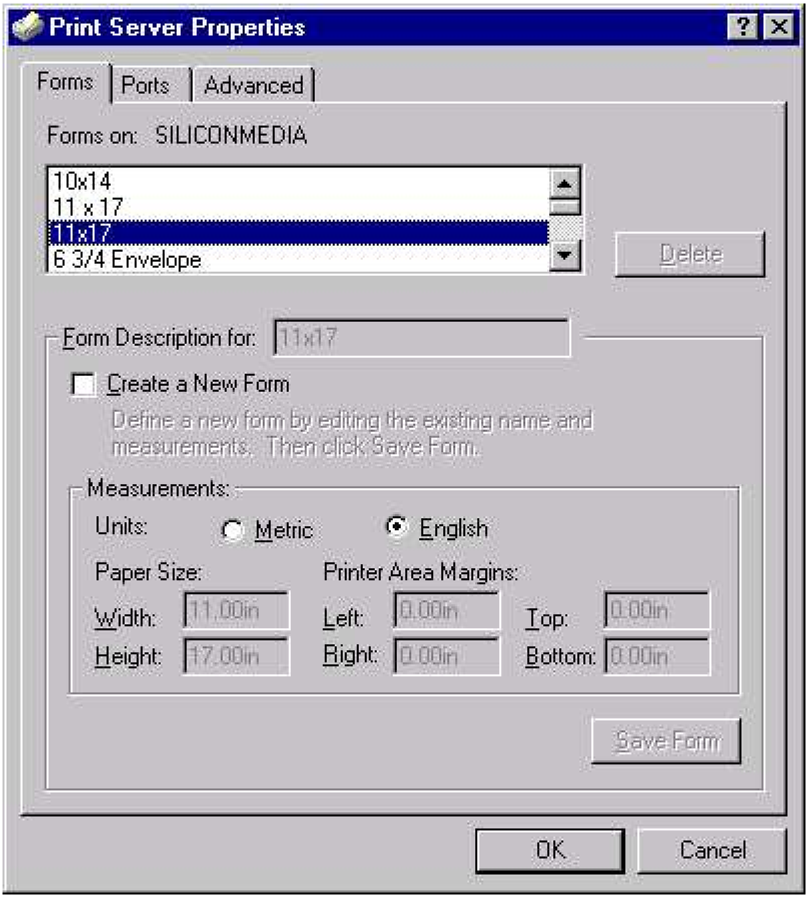
A print server is a computer (or network device) that manages print jobs and print devices. The Windows NT Spooler service performs many of the functions of a print server. You can configure several of the Spooler service's properties (which Windows NT calls print server properties) including the spool folder, forms, and ports. To access the print server properties, select **Start ➤ Settings ➤ Printers** and then select **File ➤ Server Properties**. (Fig 9.4)

Creating Forms

Forms Tab lets you create forms by specifying form name, paper size, and printer area margins. To create a form, highlight any existing form in the Forms list box, select the check box next to **Create a New Form**, and then edit the name of the form, as well as the paper size and printer area margins to meet your new form's specifications. Then click the **Save Form** command button. The new form is added to the Forms list box, and the old form is not changed or deleted.

Managing Ports

You can use the Ports tab in the Print Server Properties dialog box to add, delete, and configure ports. The capabilities of the Ports tab in the Print Server Properties dialog box are identical to those in the Add Printer Wizard with one exception: ports can only be deleted from the Ports tab in the Print Server Properties dialog box.



Print Server Properties

Forms | Ports | Advanced

Forms on: SILICONMEDIA

- 10x14
- 11 x 17
- 11x17
- 6 3/4 Envelope

Delete

Form Description for: 11x17

□ Create a New Form

Define a new form by editing the existing name and measurements. Then click Save Form.

Measurements:

Units: ○ Metric ● English

Paper Size:
Width: 11.00in
Height: 17.00in

Printer Area Margins:
Left: 0.00in
Right: 0.00in
Top: 0.00in
Bottom: 0.00in

Save Form

OK | Cancel

Fig 9.4 Specifying Printer Server Properties

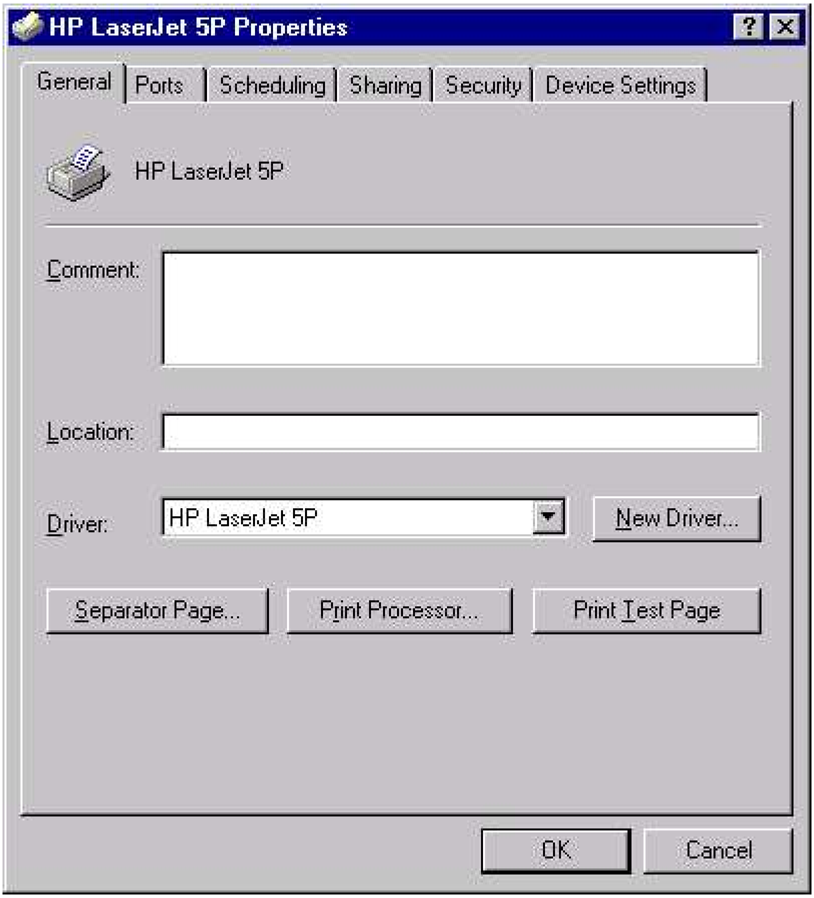
Spool Folder

The spool folder is used by the Windows NT Spooler service as a temporary storage area for print jobs waiting to be sent to a print device. The default location for the spool folder is <winntroot>\System32\Spool\Printers. If the partition that contains the spool folder does not have enough free space to store print jobs, you may experience print job failures. If you experience print job failures due to a lack of free space for your spool folder, you can specify a different folder on another partition, to be used as your spool folder. To change your spool folder, click the **Advanced** tab in the Print Server Properties dialog box. Then, edit the contents of the Spool Folder text box. You can specify any folder in any partition as your spool folder, in the format of Drive_letter:\Folder\Subfolder.

CONFIGURING PRINTERS

After you install your printer or printers, you configure the driver to match your printer's setup. Some simple printers have little or no setup, while laser printers have a variety of hardware and software options.

To configure a printer, open the Printers folder by choosing **Start** ➢ **Settings** ➢ **Printers**. Right-click the printer of interest and select **Properties** from the menu that appears. You see the Properties dialog box for the printer, as shown in Fig 9.5.



HP LaserJet 5P

Comment:

Location:

Driver: HP LaserJet 5P

Fig. 9.5 Configuring printers

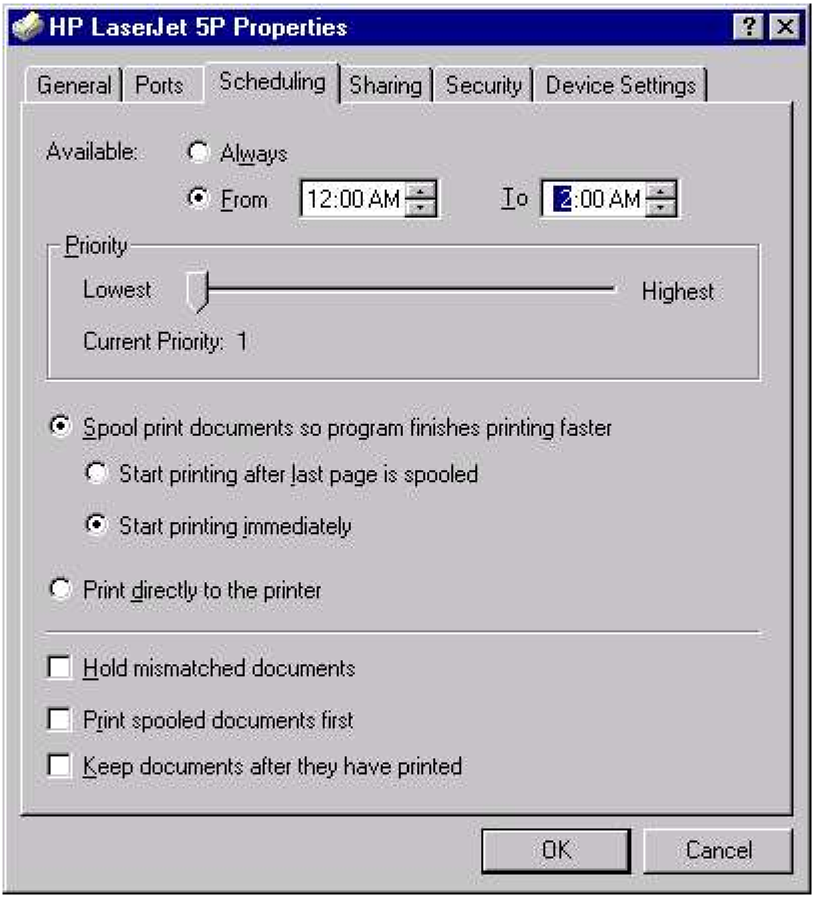
Printer Pools

When a printer has multiple ports (and multiple print devices) assigned to it, this is called a printer pool. Users print to a single printer, and the printer load-balances its print jobs between the print devices assigned to it. A printer pool is a useful tool when All print devices assigned to the printer pool use the same print device driver and are located physically close to each other.

To configure multiple ports as a printer pool, click the check box next to **Enable printer pooling** in the Ports tab in the Printer property dialog box. Then select at least one additional port from the Port list box. When a user prints to a printer pool, the print job is sent to the first listed print device in the Port list that is not busy printing another print job. The entire print job is sent to the same port (print device).

Scheduling printers

Scheduling printer means assigning the hours to a specific print device for use by a specific printer. When scheduling a printer, the hours of availability apply only to the print device, not to the printer. This means that users can print to the printer at any time during the day, and the printer then spools the jobs to the hard disk. However, the print jobs are only sent to the print device during the print device's hours of availability.



Available: ○ Always ● From 12:00 AM To 2:00 AM

Priority
Lowest Highest
Current Priority: 1

● Spool print documents so program finishes printing faster
○ Start printing after last page is spooled
● Start printing immediately
○ Print directly to the printer

□ Hold mismatched documents
□ Print spooled documents first
□ Keep documents after they have printed

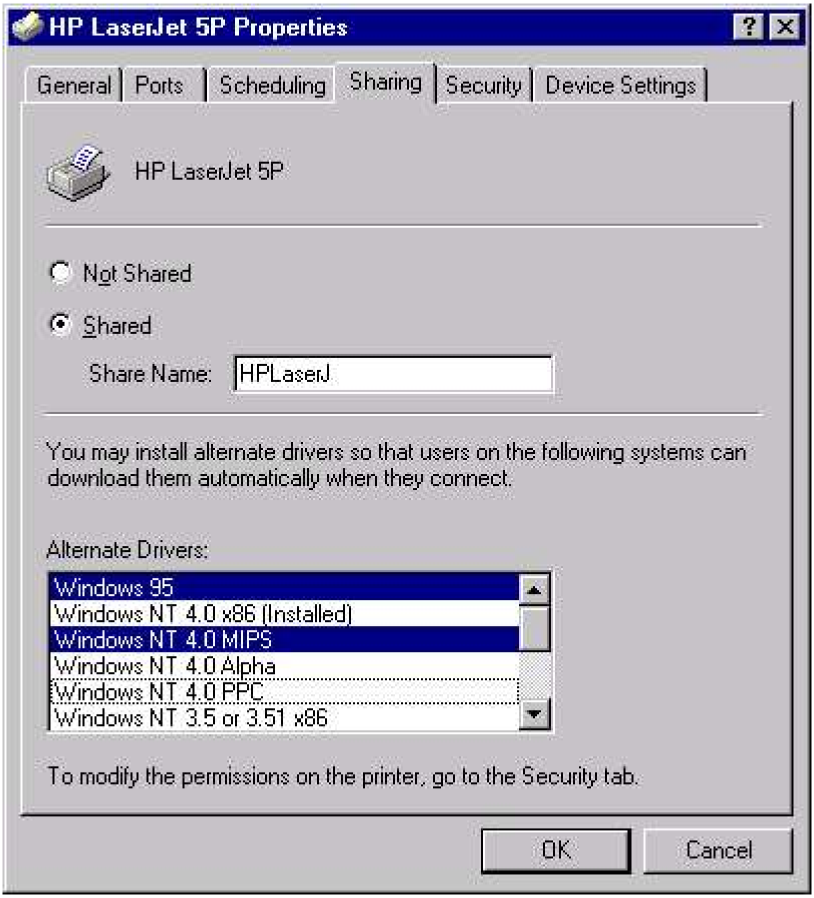
Fig 9.6 Scheduling the Printer

Using scheduling, you can schedule you long and not so important print jobs to print during nonbusiness hours, thereby increasing the productivity.

To schedule a printer, you must create a second copy of the same printer by using the Add Printer wizard. Now right-click this printer in the Printers folder and select **Properties** from the menu that is displayed. Select the **Scheduling** tab and set the available hours by clicking the radio button next to **From** and set the times in the spin boxes next to From and To. (Fig 9.6)

Sharing a Printer

The purpose of sharing a printer on a Windows NT computer is to enable users of other computers on the network to connect to and to send print jobs to the shared printer. The computer that hosts the shared printer is called a print server. The print server performs all of the spooling, print job management, scheduling, and sending of the final print jobs to the print device.



HP LaserJet 5P

○ Not Shared

● Shared

Share Name: HPLaserJ

You may install alternate drivers so that users on the following systems can download them automatically when they connect.

Alternate Drivers:

- Windows 95
- Windows NT 4.0 x86 (Installed)
- Windows NT 4.0 MIPS
- Windows NT 4.0 Alpha
- Windows NT 4.0 PPC
- Windows NT 3.5 or 3.51 x86

To modify the permissions on the printer, go to the Security tab.

Fig 9.7 Sharing the Printer

When you share a printer on your Windows NT computer, the types of computers on the network that can access your shared printer are somewhat dependent upon the protocols and services installed in your computer. When you install Windows NT, Microsoft Windows Networking is installed by default. If you have not installed any other services and you share a printer on your computer, only computers that support Microsoft Windows Networking can access the shared printer.

When you share a printer on a Windows NT computer, Windows NT enables you to install alternate printer drivers for other versions of Windows NT and Windows 95. You can also install alternate printer drivers for other Windows NT hardware platforms, such as MIPS R4000, PowerPC, and DEC Alpha.

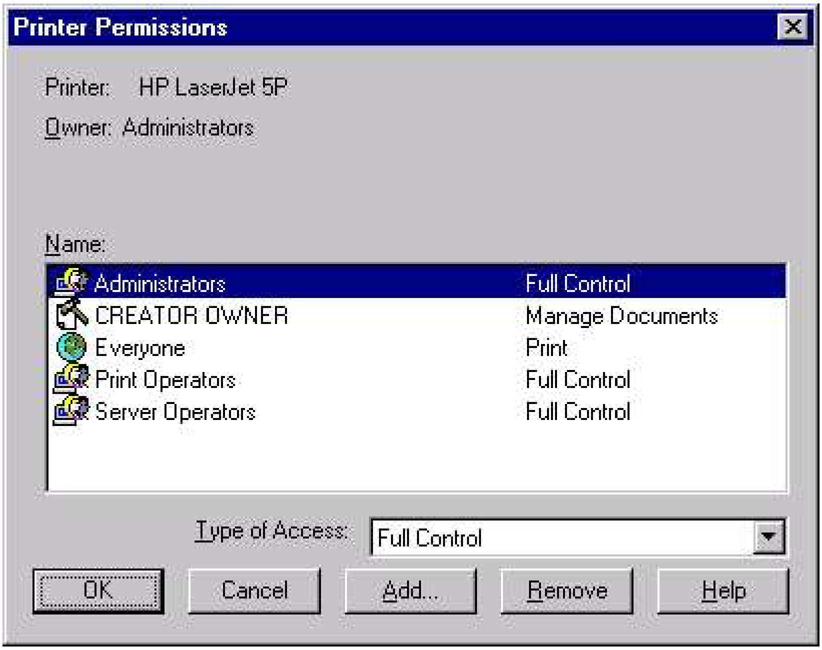
To share a printer, select the **Sharing tab** from the Printer Properties dialog box and click the radio button next to **Shared**. Give a shared name for the printer and install the alternate drivers, if required.

Printer Security

You can use Windows NT printer security to control access to a printer by assigning printer permissions to users and groups. Printer security is configured on the Security tab in a printer's Properties dialog box. In addition, you can take ownership of a printer and configure Windows NT to audit printer usage in this dialog box.

Printer Permissions

Printer permissions control which tasks a user can perform on a specific printer.



Printer: HP LaserJet 5P

Owner: Administrators

Name:

Administrators	Full Control
CREATOR OWNER	Manage Documents
Everyone	Print
Print Operators	Full Control
Server Operators	Full Control

Type of Access: Full Control

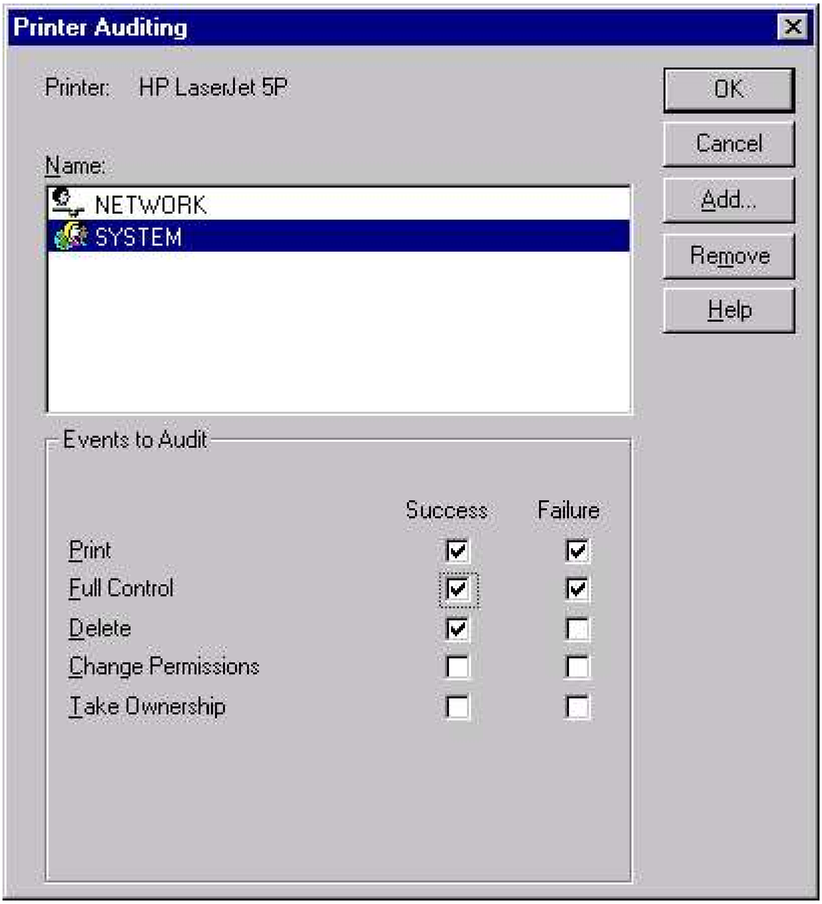
Fig 9.8 Specifying Printer Permission

You can assign printer permissions to users and groups. User and group permissions are additive. In other words, if a user has the Print permission, and a group that the user is a member of has Full Control, then the user has Full Control.

To assign printer permissions to users and groups, click the **Permissions** command button on the Security tab in the Properties dialog box for the printer you want to configure. (Fig 9.8) Note that by default the Everyone group has the Print permission, which effectively enables all users to create and delete their own print jobs on this printer.

Printer Auditing

You can use your printer's Properties dialog box to configure Windows NT to audit a user or group's usage (and/or attempted usage) of a printer. Only members of the Administrators group can configure auditing on a Windows NT computer.



Printer Auditing

Printer: HP LaserJet 5P

Name:
- NETWORK
- SYSTEM

Events to Audit

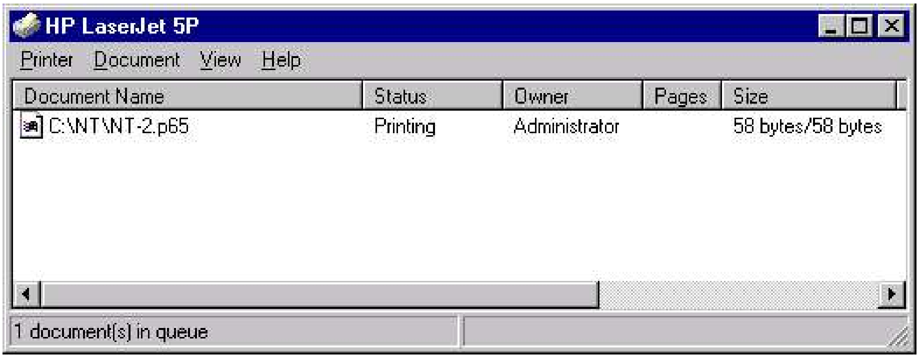
	Success	Failure
Print	☑	☑
Full Control	☑	☑
Delete	☑	□
Change Permissions	□	□
Take Ownership	□	□

Fig 9.9 Specifying Printer Auditing

When auditing is enabled, Windows NT adds an entry to the security log in Event Viewer every time an audited user or group exercises (and/or attempts to exercise) an audited permission on a specific printer.

MANAGING PRINT JOBS

Each printer has a window that shows the activity for that printer. The printer control window lists the print jobs waiting to be printed, and the one that is currently printing. Open the Printers folder by choosing **Start** ➢ **Settings** ➢ **Printers**, and then double click the printer's icon in the Printers window.



Document Name	Status	Owner	Pages	Size
C:\NT\NT-2.p65	Printing	Administrator		58 bytes/58 bytes

1 document(s) in queue

Fig. 9.10 Printer status dialog box

Changing the Printing Order

Select and drag the file to its new position in print queue, and release the mouse button or select the file, press and hold down CTRL, and press the UP arrow or DOWN arrow key to move the file to its new position. Then release CTRL and arrow key. The file information in the print queue changes to reflect the new positions of the files.

Pausing & Resuming Printing

To temporarily interrupt printing, select the printer for print queue, or select the individual file to be paused and choose the pauses button or press Alt+P. The information displayed for printer or file now indicates that printing has paused.

To resume printing, select the printer for the print queue, or select the individual file you want to continue, and choose the **Resume** Button or Press Alt+R. The information displayed for printer or file changes to indicate that printing has resumed.

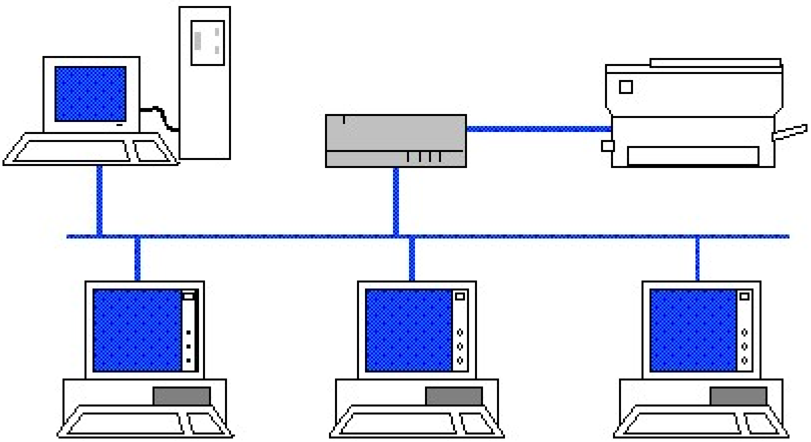
EXERCISE

1. _____ _________ are special storage areas where print jobs are stored and then sent to the printer in an organized fashion.
2. What is print server and how is it configured?
3. What is printer pool?
4. How scheduling printer helps in managing the print work?
5. Explain in brief what is a Network Printer?
6. Verify whether the machine you are working on has a printer installed? If not then install a network printer.
7. Create a user PRN-A and PRN-B and assign the right to Manage Document to PRN-A and Full control to PRN-B. Choose a default printer and go through the Properties > Security > Permissions. Can the permissions be changed? Can PRN-A user purge the documents?

CHAPTER 10

Managing Files & Folders

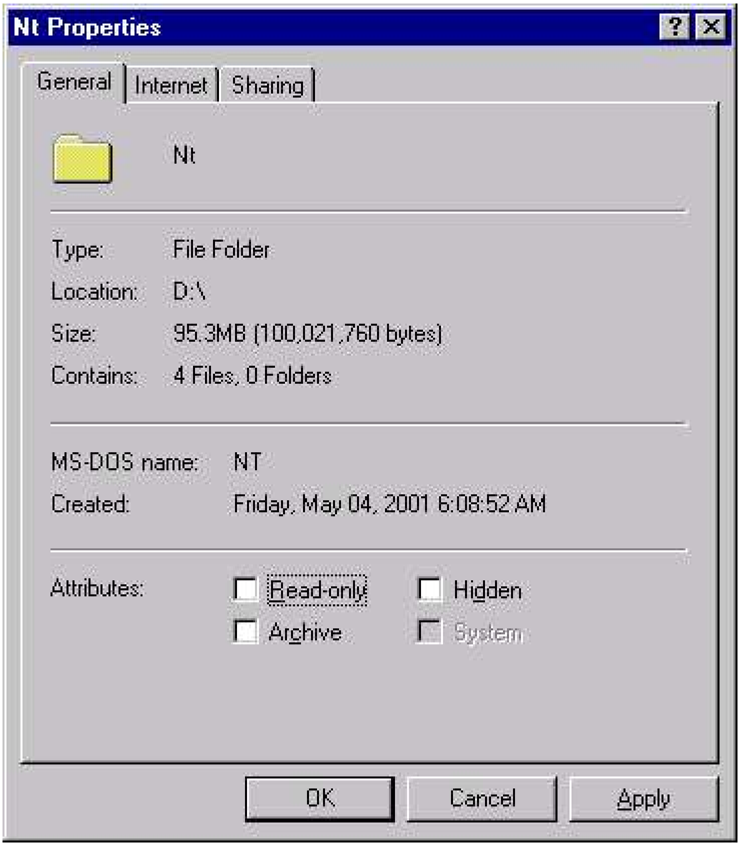
FILES & FOLDERS ATTRIBUTES
SHARING A FOLDER
SETTING PERMISSION
NTFS FILES & FOLDERS PERMISSION
AUDITING FILES AND FOLDERS
OWNERSHIP OF FILES AND FOLDERS



FILES & FOLDERS ATTRIBUTES

Windows NT files and folders have various attributes, some of which the Administrator can use to provide a limited amount of data protection. File attributes can be used on both FAT and NTFS partitions, with the exception of the Compress attribute, which is only available on NTFS partitions.

To change or assign file or folder attributes, start Windows NT Explorer by selecting **Start ➢ Programs ➢ Windows NT Explorer**. In the Exploring dialog box, highlight the file or folder on which you want to change attributes or to which you want to assign attributes. Now select **File ➢ Properties** or you can right-click the file or folder, and select **Properties** from the menu that appears to bring the File_name or Folder_name property dialog box.



Nt

Type: File Folder

Location: D:\

Size: 95.3MB (100,021,760 bytes)

Contains: 4 Files, 0 Folders

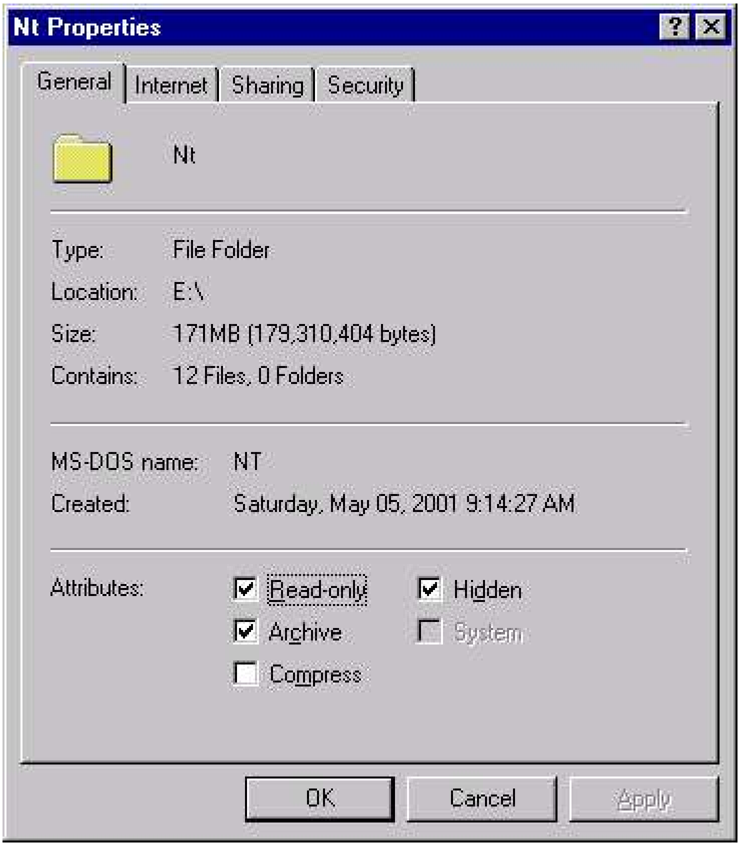
MS-DOS name: NT

Created: Friday, May 04, 2001 6:08:52 AM

Attributes: □ Read-only □ Hidden □ Archive □ System

Fig 10.1 Setting Folder Properties on FAT

Notice the System attribute is grayed out and can't be changed using this interface. You can change only three attributes in FAT partition - Read-only, Archive and Hidden (Fig 10.1) whereas you can change four attributes in NTFS partition - Read-only, Archive, Compress and Hidden (Fig 10.2). Select the check boxes next to the attributes you want to assign and click **OK**. Exit Windows NT Explorer.



Nt

Type: File Folder
Location: E:\
Size: 171MB (179,310,404 bytes)
Contains: 12 Files, 0 Folders

MS-DOS name: NT
Created: Saturday, May 05, 2001 9:14:27 AM

Attributes: ☑ Read-only ☑ Hidden
☑ Archive □ System
□ Compress

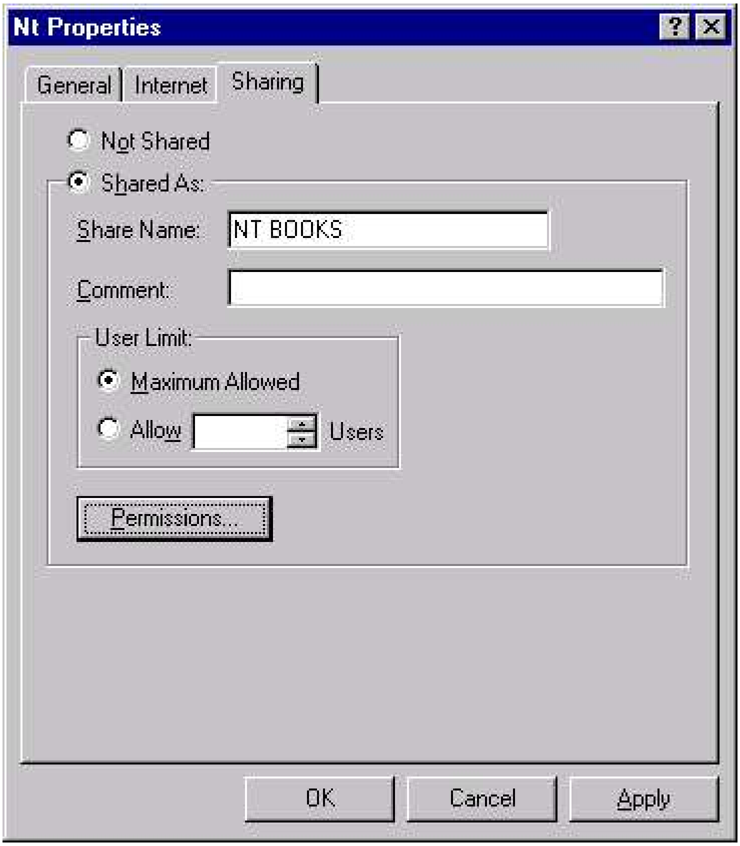
Fig 10.2 Setting Folder properties on NTFS

In the Properties dialog box, you may note the difference in properties for FAT and NTFS by comparing Fig 10.1 (FAT) and Fig 10.2 (NTFS). In NTFS, the security tab is also provided which gives you finer level of control over shared files and folders.

SHARING A FOLDER

USING WINDOWS NT EXPLORER (FAT PARTITION)

In Windows NT, folders are shared to enable users to access network resources. A folder can't be accessed by users across the network until it is shared or placed within another folder that is shared. A shared folder appears in Windows NT Explorer and My Computer as a folder with a hand under it. Only members of the Administrators, Server Operators, and Power Users built-in local groups can share folders. When a folder is shared, its entire contents (including all files and subfolders) are available to users who have the appropriate permissions to the share.



○ Not Shared

● Shared As:

Share Name: NT BOOKS

Comment:

User Limit:

● Maximum Allowed

○ Allow Users

Fig 10.3 Sharing Folder on FAT

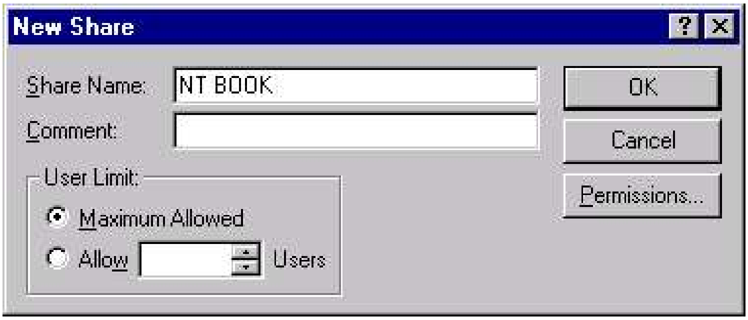
When sharing a folder, it's a good idea to assign it a share name that is easily recognized by users, and one that appropriately describes the resources contained in the folder. Share names in Windows NT can be as long as eighty characters. (But you can give share name according to the client computer - 8.3 for MS-DOS format or 12 character for Windows 95 format).

To share a folder using Windows NT explorer, start Windows NT Explorer by selecting **Start ➢ Programs ➢ Windows NT Explorer**. In the Exploring dialog box, highlight the file or folder on which you want to share. Now select **File ➢ Properties** or you can right-click the folder, and select **Properties** from the menu that appears to bring the Folder Property dialog box. Select the **Sharing** tab in the property dialog box. Either accept the default name in the Share Name text box or type in the name you want to use for the share.

You can add a descriptive comment about the share in the Comment text box if you so choose. If you want to limit the number of users who can connect to this share simultaneously. The default User Limit setting is Maximum Allowed. Click **OK** to bring the Explorer. A hand appears under the folder you shared, indicating that it is a shared folder.

USING WINDOWS NT EXPLORER (NTFS PARTITION)

In NTFS, the Sharing tab is similar except the fact that the share name can't be typed directly. Instead, the folder name appear as default share name. To change the shared name and give a more appropriate name for the user, click on the **New Share** button to display New Share dialog box. Give a new share name. Notice that the new share name appears in the drop down list of Share name in the Properties dialog box.



New Share

Share Name: NT BOOK

Comment:

User Limit:

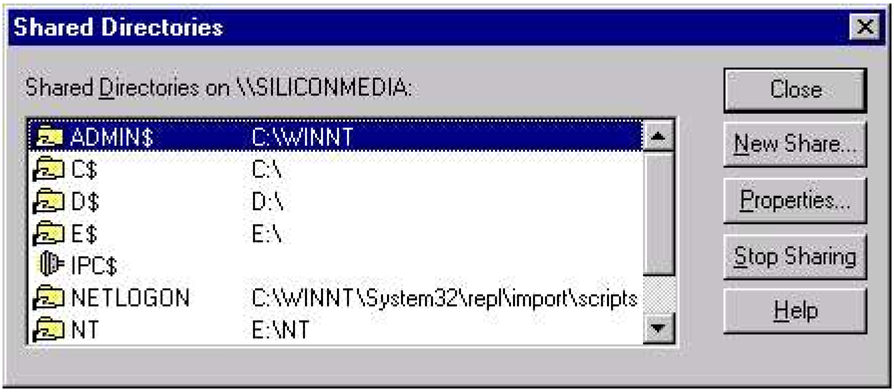
● Maximum Allowed

○ Allow Users

Fig 10.4 Defining Share name on NTFS

USING SERVER MANAGER

To share a folder using Server Manager, Select **Start ➤ Programs ➤ Administrative Tools (Common) ➤ Server Manager**. In the Server Manager dialog box, highlight the computer that contains the folder you want to share. Select **Computer ➤ Shared Directories** to display shared directory dialog box. Here all the directories that are shared are listed. (Fig 10.5).



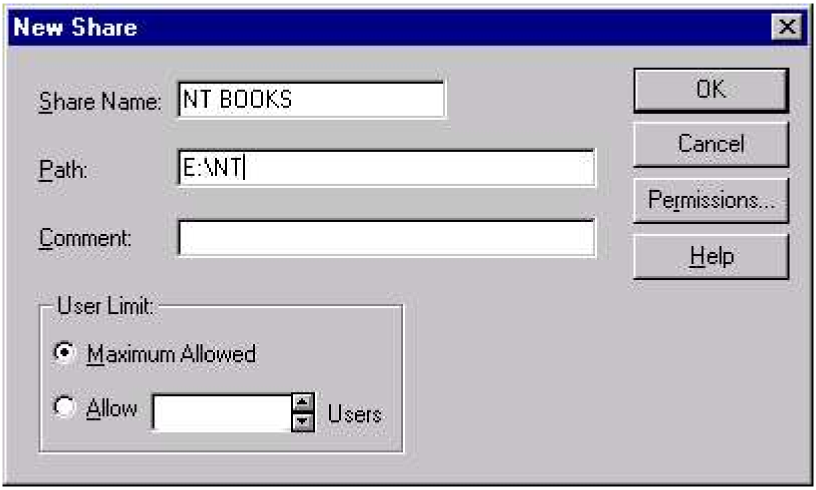
Shared Directories

Shared Directories on \\SILICONMEDIA:

```
ADMIN$      C:\WINNT
C$          C:\
D$          D:\
E$          E:\
IPC$
NETLOGON    C:\WINNT\System32\repl\import\scripts
NT          E:\NT
```

Fig 10.5 Sharing Folder through Server Manager

In the Shared Directories dialog box, click the **New Share** command button. (Fig 10.6)



New Share

Share Name: NT BOOKS

Path: E:\NT

Comment:

User Limit:

● Maximum Allowed

○ Allow Users

Fig 10.6 Defining New Share

In the Share Name text box, type in the name you want to assign to the new share. Then, in the Path text box, type in the full path to the share, in the form of *Drive_letter:**Folder**subfolder*\... If you want to limit the number of users that can connect to this share simultaneously you can configure the User Limit section. Click **OK**.

SETTING PERMISSION

SHARED FOLDER PERMISSIONS FOR FAT

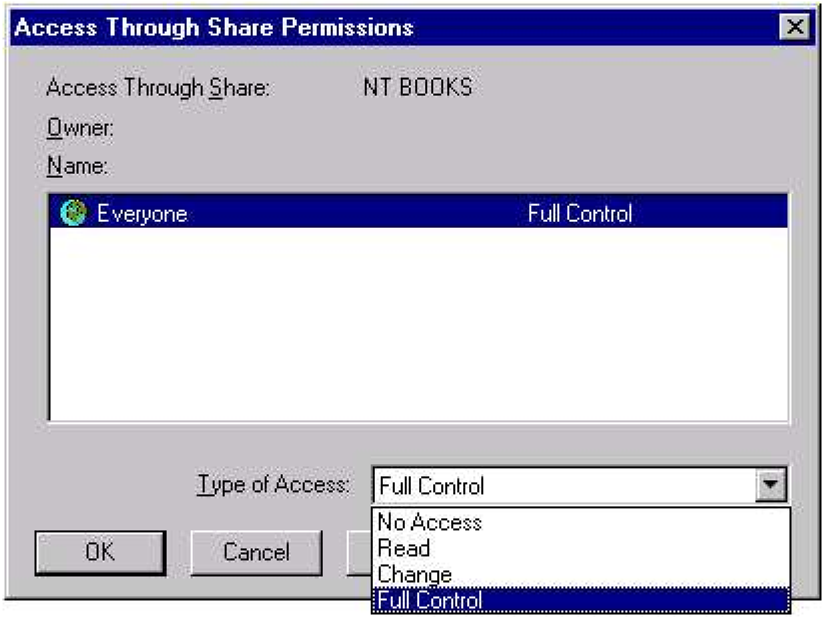
Shared folder permissions control user access to shared folders. Shared folder permissions only apply when users connect to the folder over the network and not when users access the folder from the local computer.

Shared folder permissions (commonly called share permissions) apply to the shared folder, its files, and subfolders. Share permissions are the only folder and file security available on a FAT partition (with the exception of file attributes), and control only over-the-network access to the share - local access is totally unrestricted on a FAT partition.

You can set the following permissions for files and directories through a shared directory:

No Access (None) Prevents any access to the shared directory, its subdirectories, and its files.

Read It allows viewing filenames and subdirectory names, changing to the subdirectories of the shared directory and viewing data in files and running application files.



Access Through Share Permissions

Access Through Share: NT BOOKS

Owner:

Name:

Everyone Full Control

Type of Access: Full Control

Fig 10.7 Shared Folder Permission for FAT

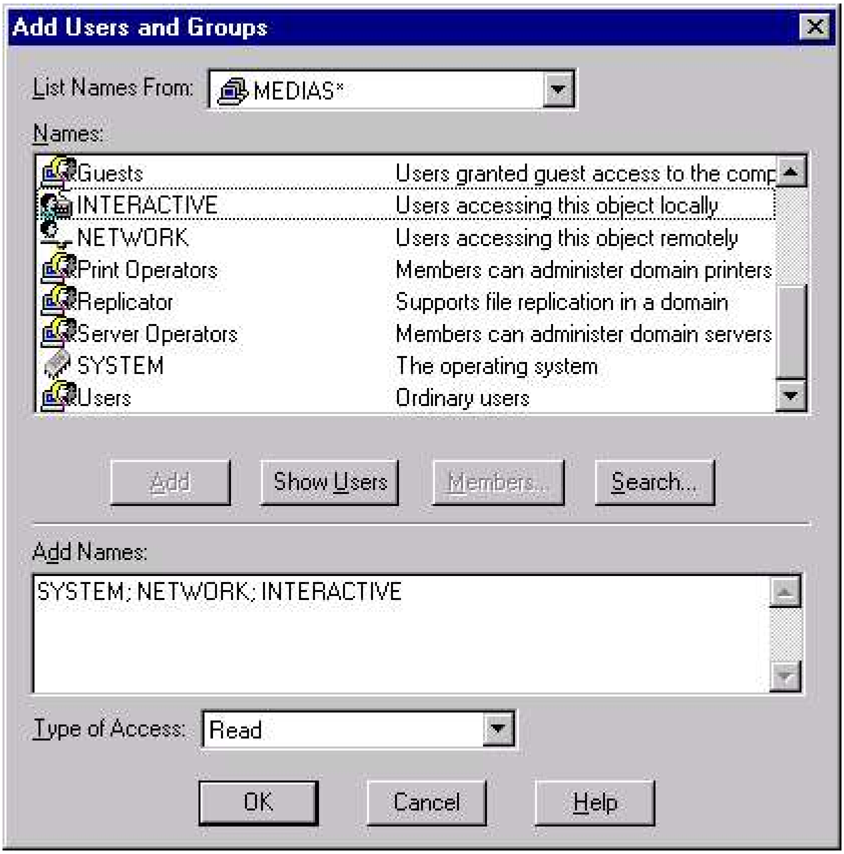
Change — It permits all the options of Read only with adding files and subdirectories to the shared directory, changing data in files and deleting subdirectories and files.

Full Control (All) — It allows all the options of Change alongwith changing permissions (NTFS files and directories only) and taking ownership (NTFS files and directories only).

To assign share permissions by using Windows NT explorer, start Windows NT Explorer. In the Exploring dialog box, highlight the shared folder to which you want to assign permissions and select **File ➤ Properties**. Select the **Sharing** tab in Properties dialog box and click the **Permissions** command button to display the "Access Through Share Permissions" dialog box. By default, the Everyone group has Full Control. (Fig 10.7)

To add user and groups for share permission, click on the **Add** button to display the Add Users and Groups dialog box, as shown in Fig 10.8.

Notice that only group names from the MEDIAS domain appear in the Names list box. If you want to add global groups and users from other trusted domains, click the arrow in the **List Names From** drop-down list box and select the domain you want. If you want to add individual users, click the **Show Users** command button. Double-click the group or user you want to add to the permissions list for the share. Then select the appropriate permission from the Type of Access drop-down list box. Click **OK**.



Add Users and Groups

List Names From: MEDIAS*

Names:

Guests	Users granted guest access to the comp
INTERACTIVE	Users accessing this object locally
NETWORK	Users accessing this object remotely
Print Operators	Members can administer domain printers
Replicator	Supports file replication in a domain
Server Operators	Members can administer domain servers
SYSTEM	The operating system
Users	Ordinary users

Add Names:

SYSTEM; NETWORK; INTERACTIVE

Type of Access: Read

Fig 10.8 Adding Users & Groups

ADMINISTRATIVE SHARES

If you use Server Manager to display the Shared directories (Fig 10.4 of Server Manager), you will realize that your server's shared drives are named as C$, D$, E$ etc. These are the administrative shares (used by Administrators to perform administrative tasks) which NT creates automatically, every time you start Windows NT on a computer. These are hidden shares that only members of the Administrators group have permission to access.

One administrative share for the root of each hard disk partition on the computer and a share named Admin$, which corresponds to the folder in which NT is installed (<*winntroot*>), are created by Windows

NT. The $ at the end of each administrative share causes the share to be hidden from users when they browse the network.

Administrative shares make it possible for an Administrator to connect to any hard drive on a computer and access all of its files and folders, regardless of whether regular shares exist on that hard drive. In this way an Administrator can perform backup, restore, and other administrative functions on a Windows NT computer. Any share can be configured as a hidden share by placing a $ at the end of its share name. However, hiding a share by appending a $ to the share name does not limit user access to the share. The hidden share retains its assigned share permissions. Only access to the hidden administrative shares is restricted, by default, to Administrators only.

NTFS FILES & FOLDERS PERMISSION

When files and folders are stored on an NTFS volume, NTFS permissions can be assigned to provide a greater level of security than share permissions on FAT. This is possible because of following reasons:

- NTFS permissions, unlike share permissions, can be assigned to individual files as well as folders. This gives an Administrator a much finer level of control over shared files and folders than is possible by using only share permissions.
- NTFS permissions apply to local users as well as to users who connect to a shared folder over the network. This fills the large security loophole left when files and folders on FAT partitions are secured only by share permissions.

NTFS permissions, which can only be assigned to files and folders on NTFS volumes, protect data from authorized access when users connect to the share locally or over the network. To make the assignment of NTFS permissions easier, Microsoft has created a set of standard directory (folder) permissions, and a set of standard file permissions. These standard permissions consist of the most commonly used combinations of NTFS permissions.

Standard permissions are used in most situations. Individual NTFS permissions are typically only used when a unique combination of permissions must be assigned. The individual NTFS permissions are sometimes referred to as Special Access Directory permissions and Special Access File permissions. The permissions specified within the first set of parentheses following the permission name apply to the folder, and the permissions specified within the second set of parentheses following the permission name apply to files within the folder.

Assigning NTFS Permissions to Files and Folders

A user can assign NTFS permissions to a file or folder only if one or more of the following criteria are met:

- The user is the owner of the file or folder.
- The user has the Change Permissions NTFS permission to the file or folder.
- The user has the Full Control NTFS permission to the file or folder.

SETTING FILE PERMISSIONS

Setting permissions on a file specifies the access that a group or user has to it. When a file is created in a directory, it inherits its permissions from the directory.

Permissions are cumulative except that the No Access permission overrides all other permissions. For example, if a user is a member of a group with Read permission and a member of a group with Change permission, the user will have Change permission.

When you set a standard permission, a set of individual permissions is displayed next to it. For example, when you set Read permission on a file, you see (RX), signifying Read and Execute permissions on the file. Similarly you have W for Write permission and D for Delete permission, P for Change permission and O for taking Ownership.

You can set file permissions only on drives formatted to use the Windows NT file system (NTFS).

To assign NTFS permissions to a file, select **Start ➢ Programs ➢ Windows NT Explorer**. In the Exploring dialog box, highlight the file to which you want to assign NTFS permissions and select **File ➢ Properties** to bring the Properties dialog box. Click the **Security** tab in the Properties dialog box. On the Security tab, click the **Permissions** command button to display File Permission dialog box. (Fig 10.9)

Click the **Add** command button to display the Add Users and Groups dialog box. To add users or groups from trusted domains, click the arrow in the List Names From drop-down list box, and select the appropriate domain from the list. To add individual users, click the **Show Users** command button to display individual users, as well as groups, in the Names list box. Select the NTFS folder permission you want to assign from the Type of Access drop-down list box and click **OK**.

The File Permissions dialog box reappears. If you want to assign individual (Special Access) NTFS files permissions then Highlight the user(s) or group(s) to which you want to assign the individual NTFS permissions. Select **Special File Access** from the Type of Access drop-down list box. (Fig 10.10).

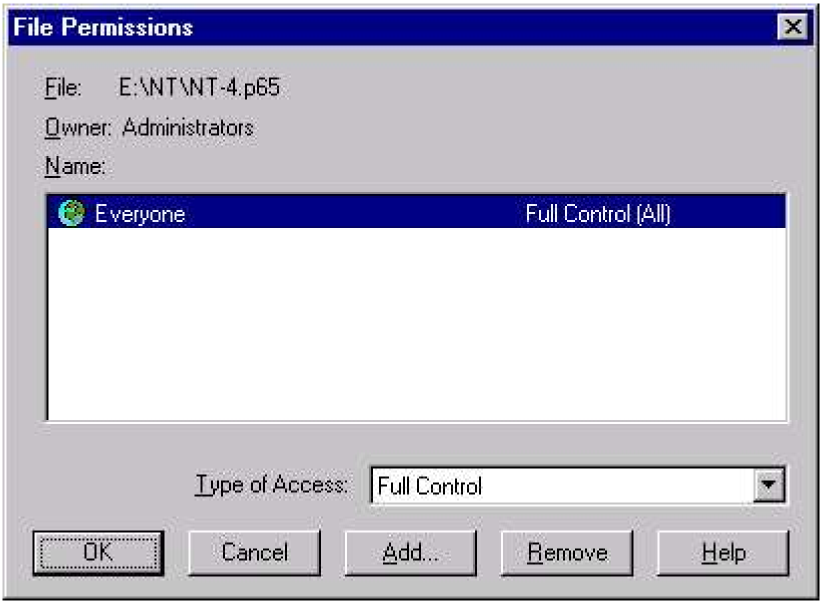


Fig 10.9 Specifying File Permission

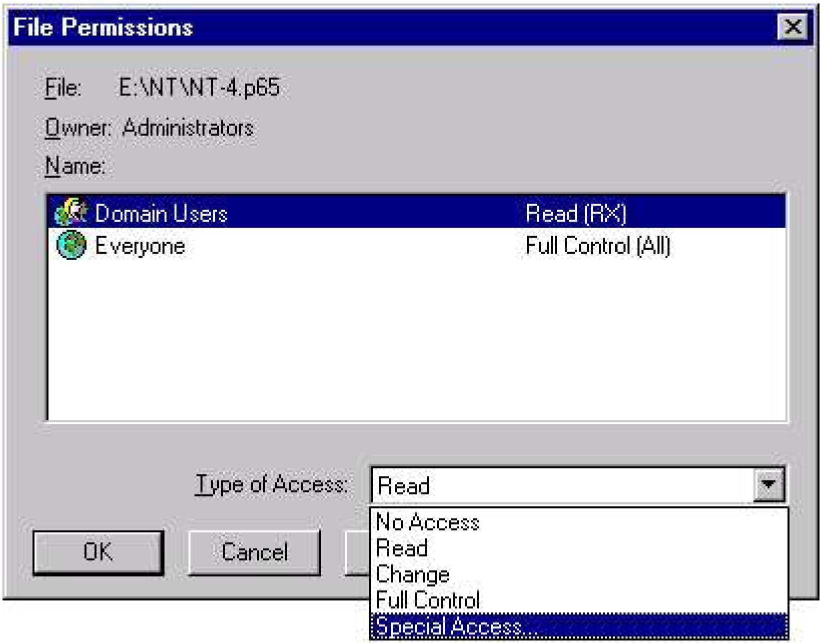
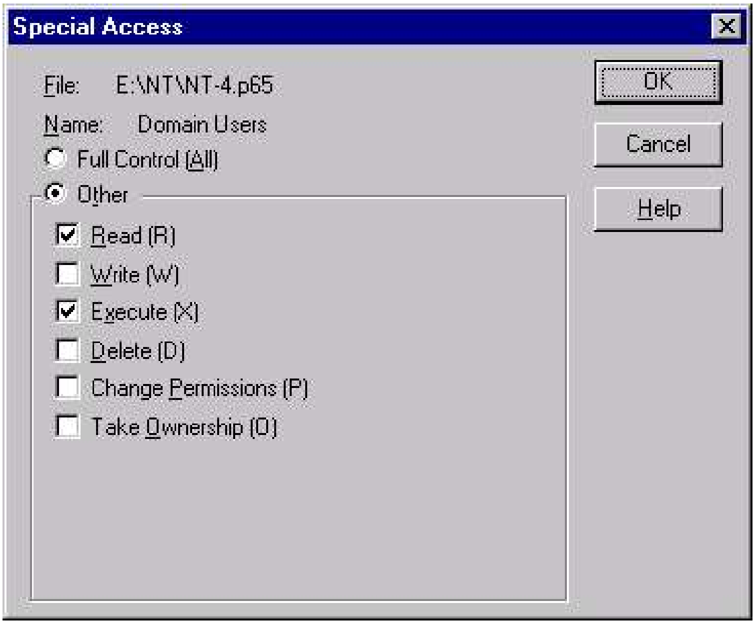


Fig 10.10 Specifying Type of Access

The Special Access dialog box appears (Fig 10.11). Select the radio button next to **Other**. Then check the check box next to the individual NTFS permission(s) you want to assign and click **OK**.



Special Access

File: E:\NT\NT-4.p65

Name: Domain Users

○ Full Control (All)

● Other

☑ Read (R)

□ Write (W)

☑ Execute (X)

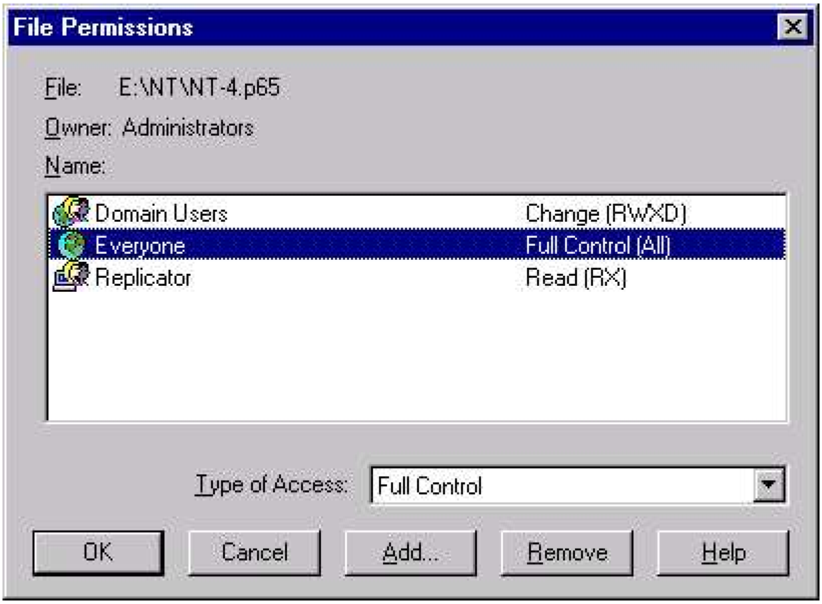
□ Delete (D)

□ Change Permissions (P)

□ Take Ownership (O)

Fig 10.11 Specifying Special Access

Figure 10.12 shows the File Permissions dialog box after NTFS permissions have been assigned. Notice the various NTFS permissions assigned, and how they appear in the Name list box. Click **OK**.



File Permissions

File: E:\NT\NT-4.p65

Owner: Administrators

Name:

Domain Users	Change (RWXD)
Everyone	Full Control (All)
Replicator	Read (RX)

Type of Access: Full Control

Fig 10.12 File after specifying Special Access

SETTING DIRECTORY PERMISSIONS

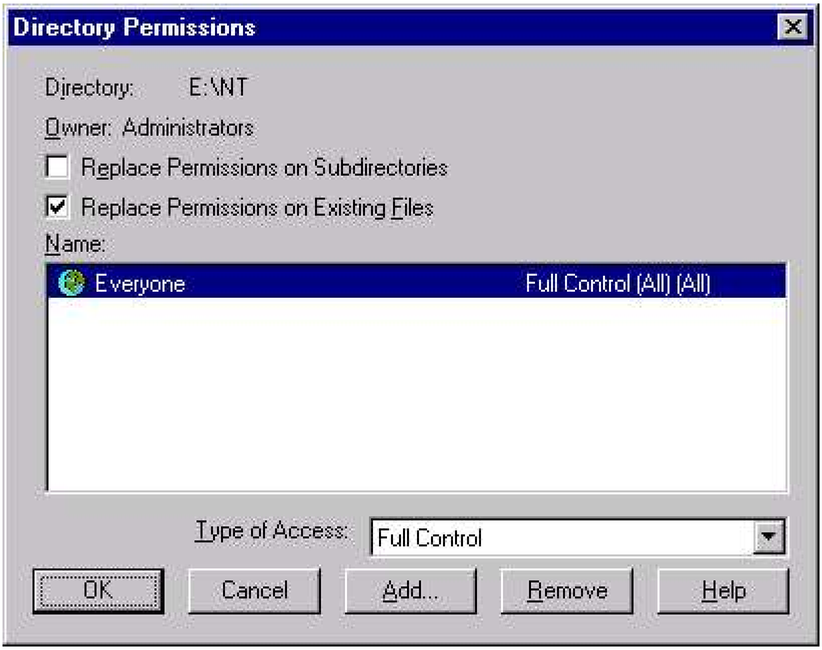
Setting permissions on a directory specifies the access that a group or user has to the directory and, by default, its files. Existing subdirectories and their files are not changed unless you specify to change them. However, when you create new files and subdirectories in the directory, they inherit their permissions from the directory.

Permissions are cumulative except that the No Access permission overrides all other permissions. For example, if a user is a member of a group with Read permission and a member of a group with Change permission, the user will have Change permission.

You can set directory permissions only on drives formatted to use the Windows NT file system (NTFS).

To assign NTFS permissions to a directory, select **Start** ➢ **Programs** ➢ **Windows NT Explorer**. In the Exploring dialog box, highlight the folder to which you want to assign NTFS permissions and select **File** ➢ **Properties** to bring the Properties dialog box. Click the **Security** tab in the Properties dialog box. On the Security tab, click the **Permissions** command button to display Directory Permission dialog box. (Fig 10.13)

Note the two check boxes available. Also note that the check box next to Replace Permissions on Existing Files is selected by default. Click the **Add** command button to display the Add Users and Groups dialog box.



Directory: E:\NT

Owner: Administrators

□ Replace Permissions on Subdirectories

☑ Replace Permissions on Existing Files

Name:

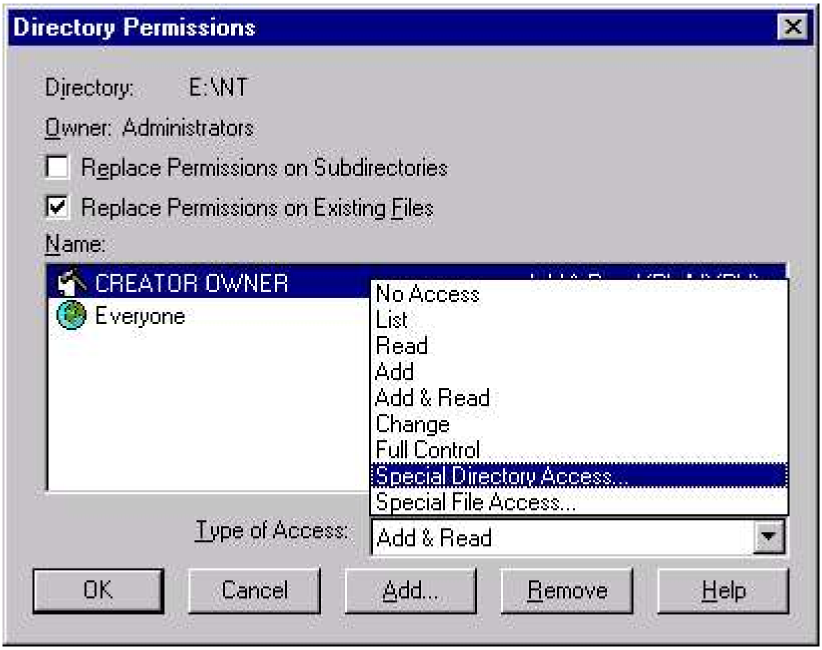
Everyone Full Control (All) (All)

Type of Access: Full Control

Fig 10.13 Specifying Directory Permission

To add users or groups from trusted domains, click the arrow in the **List Names From** drop-down list box, and select the appropriate domain from the list. To add individual users, click the **Show Users** command button to display individual users, as well as groups, in the Names list box. Select the NTFS folder permission you want to assign from the Type of Access drop-down list box and click **OK**.

The Directory Permissions dialog box reappears. If you want to assign individual (Special Access) NTFS folder permissions then Highlight the user(s) or group(s) to which you want to assign the individual NTFS permissions. Select **Special Directory Access** from the Type of Access drop-down list box. (Fig 10.14)


Directory Permissions

Directory: E:\NT

Owner: Administrators

□ Replace Permissions on Subdirectories

☑ Replace Permissions on Existing Files

Name:

CREATOR OWNER

Everyone

Type of Access: Add & Read

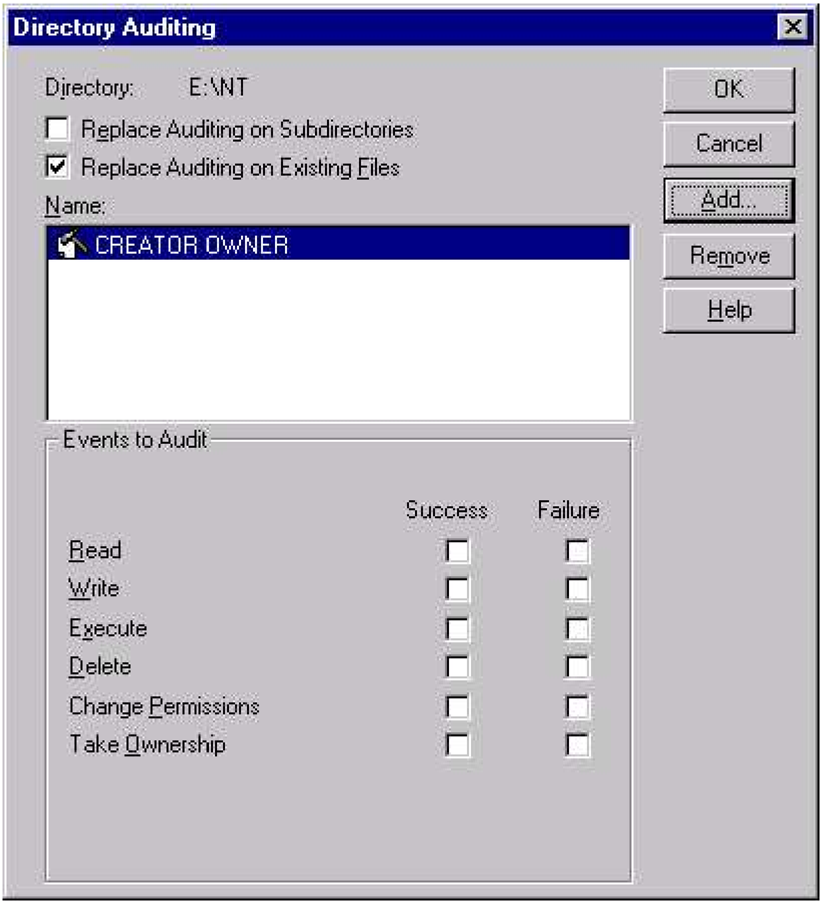
Fig 10.14 Specifying Type of Access

The Special Directory Access dialog box appears which is more or less similar to the Special File Access dialog box (Fig 10.11). Select the radio button next to **Other**. Then check the check box next to the individual NTFS permission(s) you want to assign and click **OK**.

In the Directory Permissions dialog box, select the check box next to **Replace Permissions** on Subdirectories if you want these NTFS permissions assigned to all subfolders. Clear the check box next to Replace Permissions on Existing Files if you do not want these NTFS permissions assigned to each existing file within the folder. If both check boxes are selected, these NTFS permissions will be assigned to all files within the folder, all subfolders, and their files. If both check boxes are cleared, these NTFS permissions will be assigned only to the folder and to new files created in the folder. Existing subfolders and the files they contain will not be affected.

AUDITING FILES AND FOLDERS

Windows NT auditing makes it possible for you to determine whether unauthorized users have accessed or attempted to access sensitive data. Windows NT auditing is only available on NTFS partitions. You can't audit files or folders that are located on FAT partitions. Because auditing generates a large amount of data, it's important that you determine what is really necessary to audit. Not only does auditing data take up space in the security log, it also takes administrative time to review the events in the log. In general, if you won't use the information obtained by auditing a given event, you probably shouldn't choose to audit it.



Directory: E:\NT

□ Replace Auditing on Subdirectories

☑ Replace Auditing on Existing Files

Name: CREATOR OWNER

Events to Audit

	Success	Failure
Read	□	□
Write	□	□
Execute	□	□
Delete	□	□
Change Permissions	□	□
Take Ownership	□	□

Fig 10.15 Auditing Files & Folders

To audit a file or directory, select the file or directory in the Window NT Explorer. From the Security menu, choose **Auditing**. If you are setting auditing on a directory, two check boxes allow you to control how auditing changes apply to existing files and subdirectories. By default, the Replace Auditing On Existing Files check box is selected, so the changes you make to auditing apply to the directory and its files only.

Set auditing for each group or user in the list by selecting the name of a group or user, and then selecting the events to audit for that group or user. If no group is being displayed, click on **Add** button to add different groups and users where auditing is required.

OWNERSHIP OF FILES AND FOLDERS

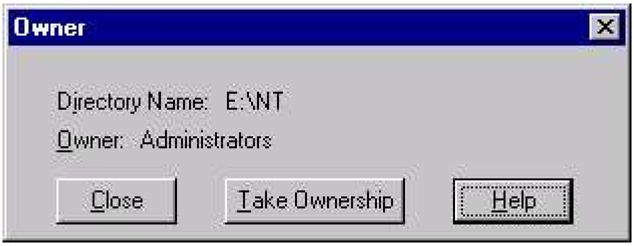
The creator of a file or folder is its owner. The owner of a file or folder can always assign permissions to that file or folder. Only files and folders on NTFS partitions have owners.

Occasionally, you may need to change or assign permissions to a file or folder, but not have the Change Permissions NTFS permission to the file or folder. Without being the owner of the file or folder or having the Change Permissions NTFS permission, the only way you can accomplish changing or assigning permissions to the file or folder is to take ownership of the file or folder.

To change the permissions on the folder, the Administrator must first take ownership of it. A user can take ownership of a file or folder only if one or more of the following criteria are met:

- The user is a member of the Administrators group.
- The user has the Take Ownership NTFS permission to the file or folder.
- The user has the “Take ownership of files or other objects” user right.

To take ownership of a file or directory, select the file or directory in the Windows NT Explorer. You can select more than one file or directory at a time. From the Security menu, choose **Owner** to display the Owner dialog box.



Directory Name: E:\NT

Owner: Administrators

Fig 10.16 Specifying Ownership

Choose the **Take Ownership** button. If you have selected one or more directories, Explorer asks whether you want to take ownership of all files and subdirectories in the trees of the selected directories. Choose **Yes** if you want to do so.

EXERCISE

Fill in the Blanks

1. Compress Attribute is available only in _________ partition.
2. Share Name in Windows NT can have ______ characters.
3. The ______ permission allows making changes to the subdirectories in the directory.
4. The _______ permission allows changing data in the files.

State True or False:

1. In NTFS partition, the share name can be typed directly.
2. NTFS permissions can be assigned to individual files as well as folders.
3. A hand appears below the shared folder.
4. In FAT, shared permissions apply only to the shared folder and not to its subfolders.
5. Auditing & Ownership is available for both NTFS and FAT files & folders.
6. Server Manager can define shares only for NTFS partition.
7. A user can assign NTFS permissions to a file or folder only if user is the owner of the file or folder.

Answer the following questions :

1. What is share permission and what is difference between FAT & NTFS share permission.
2. What are administrative shares.
3. What does symbol R, X, W and D stand for?
4. What is the difference between File permission and Folder Permission in NTFS.
5. What purpose does Auditing solve?

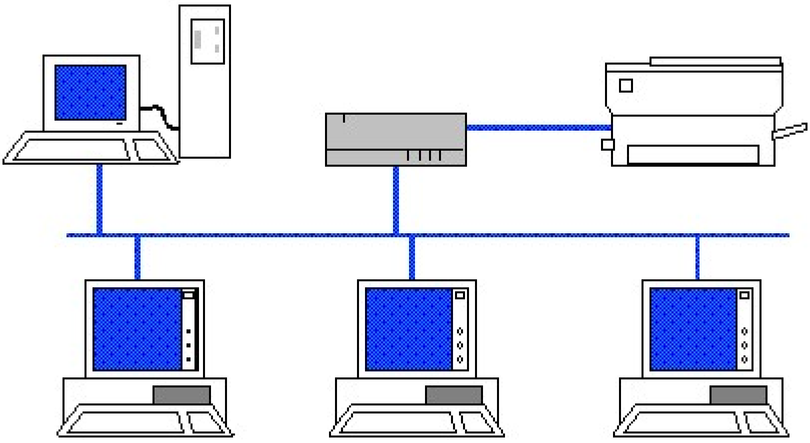
Try the following exercise:

1. Create Shared Directory in drive C and call it SILICON and in the permissions tab give it only read permission. Try copying a file in to the folder SILICON. Discuss observation?

CHAPTER 11

Windows NT Networking

WINDOWS NT NETWORKING
IDENTIFICATION
SERVICES
THE NETWORK PROTOCOLS
TCP/IP
INSTALLING TCP/IP
CONFIGURING TCP/IP



WINDOWS NT NETWORKING

Windows NT Server is a Network Operating System (NOS). As a NOS, it must support a variety of network clients over a range of protocols. And NT Server qualifies as an advanced NOS as it supports a broad range of protocols that can be used to service all types of clients - Windows NT Server supports native Microsoft clients (DOS, Windows, Windows for Workgroups, Windows 95, and of course, Windows NT Workstation), Macintosh clients, UNIX workstations, and others.

To take maximum usage of the Windows NT in real life network environment, you must understand the protocols supported by Windows NT and the services that these protocols can use.

CONFIGURING PROTOCOLS & SERVICES

Windows NT has built-in networking as an integrated part of the operating system. The networking hierarchy of Windows NT could be divided into three components- Adapter, Protocol & Service as shown in Fig 11.1.

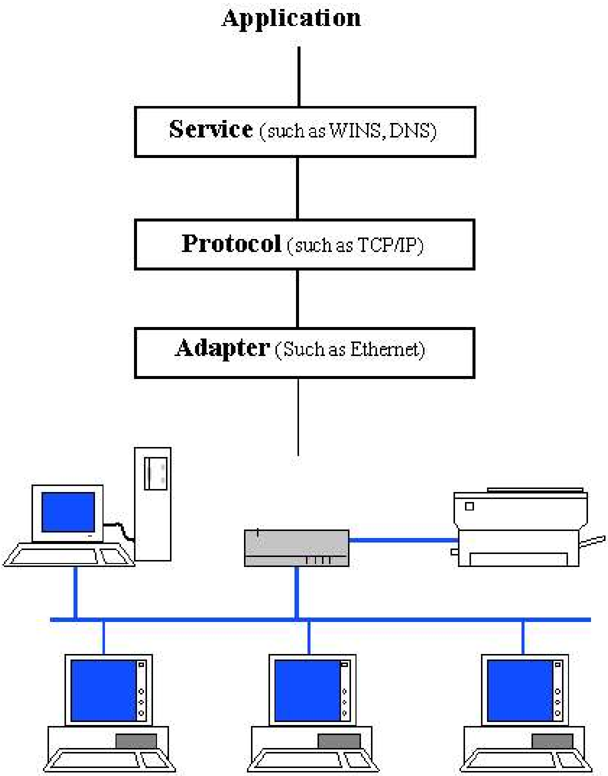
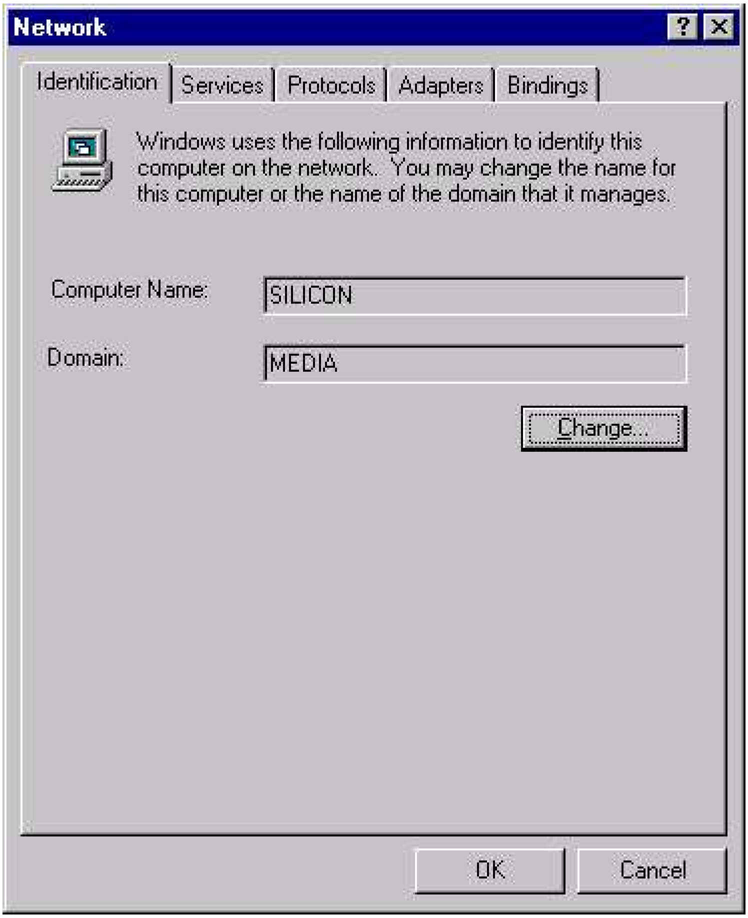

Application
Service (such as WINS, DNS)
Protocol (such as TCP/IP)
Adapter (Such as Ethernet)

Fig 11.1 Networking Hierarchy of Windows NT

As discussed in Chapter 7, the networking protocols and services are configured through Control Panel. Select the **Network** option from the Control Panel. This brings the Network dialog box (Fig 11.2).



Windows uses the following information to identify this computer on the network. You may change the name for this computer or the name of the domain that it manages.

Computer Name: SILICON

Domain: MEDIA

Fig 11.2 The Network dialog box

The dialog box defines five major areas of configuration, including the three area of networking hierarchy. The other two are Identification and Binding.

Identification Defines the logical name of the system and name of the workgroup or domain.

Services This layer is a series of services that handle the high-level functions that users and applications require. Here you could configure the services that can be used in conjunction with the protocol sets.

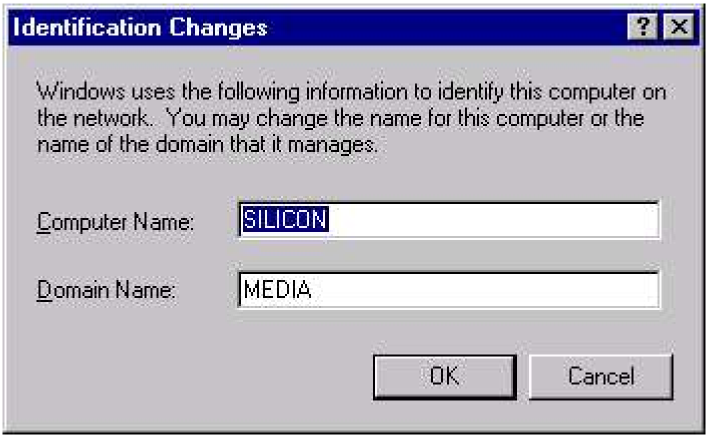
Protocols This is the language and format of the communication signals. You can define which protocols (for example, NetBEUI, IPX, and TCP/IP) are supported and how those protocols are configured

Adapter This is the device that connects the logical signals that you formed in the protocol portion of the hierarchy to the physical wires. Here you could defines which network adapters are physically installed in the system.

Binding Defines the exact associations between services, protocols, and the available network adapter(s).

IDENTIFICATION

The identification tab (Fig 11.2) sets the identity of your computer in the network. The key components are the Computer Name and Domain/Workgroup name. The computer name is the unique identifier for the computer that should make sense to everyone else in your workgroup or domain. The workgroup/domain is your workgroup or domain name. The workgroup and domain names are names made up by administrators to refer to a particular group of computers. You can change the name of the computer and domain by clicking on the **Change** button. This brings up the Change dialog box (Fig 11.3).



Identification Changes

Windows uses the following information to identify this computer on the network. You may change the name for this computer or the name of the domain that it manages.

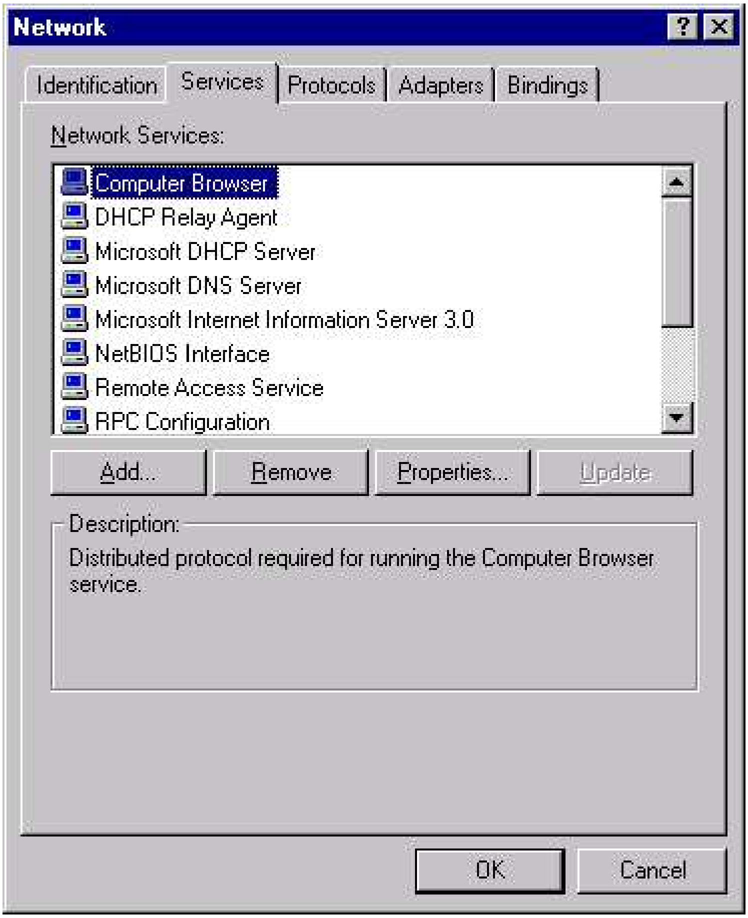
Computer Name: SILICON

Domain Name: MEDIA

Fig 11.3 Changing Identification

SERVICES

Windows NT Server supports a wide variety of network services - services for file sharing, printer sharing, network management, Web access, and more. Services are added using the Services tab in the Network option in Control Panel. (Fig 11.4). Generally the services could be divided into three categories



Network Services:

- Computer Browser
- DHCP Relay Agent
- Microsoft DHCP Server
- Microsoft DNS Server
- Microsoft Internet Information Server 3.0
- NetBIOS Interface
- Remote Access Service
- RPC Configuration

Description:
Distributed protocol required for running the Computer Browser service.

Fig 11.4 Service Tab of Network

Native Microsoft services

These are the services Microsoft has historically used for file sharing, print sharing, and program-to-program communications.

Computer Browser : For browsing the list of computers that are available on the network.

NetBIOS Interface : It provides basic interface to the Network Basic Internal Operating System.

Server : Converts your system to network server.

Workstation : This provides the services that you will need when using your server as a workstation.

BOOTP Relay Agent : Predecessor of DHCP; helps to locate the computer in the network.

FTP Server : File Transfer Protocol Server - lets other computers, which are using this protocol, to access its files.

TCP/IP services

These services, found in many non-Microsoft environments, enable Web access, file transfer, network management, and other important services.

The TCP/IP services are added via the Services tab on the Network option in Control Panel. The services that fall into this category are:

DHCP Relay Agent : Enables the Windows NT server to forward the DHCP information to remote DHCP server.

DHCP Server : Allows your computer to act as a master repository for IP addresses thus saving you from assigning them manually to each computer.

DNS Server : Lets your computer to act as a TCP/IP domain name server.

Internet Information Server 2.0 :

Enables you computer to act as Information Server.

TCP/IP Printing : Enables your computer to use UNIX TCP/IP print job transfer services (LPR/LPD).

RIP for Internet Protocol : Enables routing of TCP/IP traffic between segments on your network.

Simple TCP/IP Services : Enables your computer to participate in a TCP/IP network

Simple Network Monitoring Protocols Service :

Using various monitoring packages, it provides your computer with information on load, availability, etc.

WINS Server : Windows Internet Name Service - enables your server to resolve IP addresses for clients on your network.

Miscellaneous services

Connectivity to Macintosh clients and Novell NetWare servers is provided via separate services. The services included in this category are:

Gateway (and Client) Services for NetWare :

Enter to the world Novell Netware. Using this service you can use file sharing, print sharing, and other common Novell services.

Network Monitor Agent: Enables you to monitor your network.

Network Monitor Tools and Agent :

Using this you can monitor the network via the Simple Network Monitoring Protocol (SNMP).

Remote Access Service : Using this service you can dial -in to any server using modem interface.

Remoteboot Service : Lets remote computer to use your server as boot server.

RIP for NWLink IPX/SPX compatible transport

Enables you to locate the routes for IPX/SPX (Novell) traffic on your network.

RPC Configuration : Remote Procedure Calls - this allows you to execute remote procedure calls.

RPC Support for Banyan : Connects you to the computers using Banyan networks.

SAP Agent : Service Advertising Protocol - allows remote computers to determine the network access points on your computer.

Services for Macintosh : Connects you to the computers using Macintosh Appletalk networks.

Most of these services are installed as you install Windows NT. There are no configuration chores that you have to perform on them. The service which require configuration are discussed in the next chapter.

THE NETWORK PROTOCOLS

A **protocol** is an agreed-upon format for transmitting data between two devices. The data that is exchanged between the computers can be in the form of messages, commands, codes indicating errors or can be the contents of the file etc.

The communication protocol defines the packet structure, the networking system in use and defines the frames structure for the bit-stream transmission. Apart form this any communication protocol also determines the type of error checking to be used, Data compression method, indication by sending device after a message has been sent and indication by receiving device after it receives the message.

Communication protocols are either **connection-oriented** or **connectionless**. In the **connection-oriented communication**, the connection is maintained until the time the packet is delivered at the destination. In the **Connectionless communication**, the network does not need to do anything. It just sends the packet to the destination without any prior contact with the hope that the message would not be lost on the way and would reach its destination.

WORKING OF THE PROTOCOLS

Network protocol is a set of instructions that both computers (senders and receiver) must perform in the right order. When one computer sent the message to another computer, the sender computer performs the following instructions:

- Breaks data into small sections called packets.
- Add destination computers address to the packets..
- Deliver the data to the network card for transmission over the network.

The receiving computer must perform the same instructions in the reverse order to receive the data i.e. Accept the data, remove the address and reassemble the packets to produce the original message.

Now these small carriers of data, called packet hold small information of data (say 512 bytes) and it takes many packets to transfer a large file over the network. A typical package consist of three main parts : Header, Data & Trailer.

- The header contains information regarding source and destination address and control information to handle address.
- The data part contains the actual data being sent. It could vary from 48 bytes to 4 KB.
- The trailer contains CRC (Cyclic Redundancy Check) to determine the damage to the packet in transmission.

PROTOCOL STACKS

Protocols that work together to provide a layer or layers of the OSI model is known as a **protocol stack**, or **suite**. Protocol stack can also be defined as a set of network protocol layers that work together. It defines how communication between the hardware and the software interoperate at various levels.

Another common phrase is **binding** a stack, which refers to linking a set of network protocols to a network interface card. The **binding process** lets you install different network interface cards on the computers so that different protocol stacks can perform network functions.

Windows NT supports seven protocols in all, three of which (NetBEUI, IPX/SPX, TCP/IP) are used for major services like, file sharing, print sharing, client/server administration etc., where as other four are used to access various other platforms like Macintosh, IBM etc. To add or modify a protocol to your server, click on the **Protocol** tab of Network dialog box (Fig 11.5).

NetBIOS Extended User Interface (NetBEUI)

Typically used in small LAN implementations of 50 nodes or less, NetBEUI is a non-routeable protocol, impractical for larger installations. It supports NetBIOS connectivity. NetBEUI is the least efficient of all the core protocols supported by Windows NT Server; however, it is often implemented for backward compatibility with LAN Manager and WFW (Windows for Workgroups).

IPX/SPX compatible protocol

This is Microsoft's implementation of Novell's IPX/SPX (Internetwork Packet Exchange/Sequenced Packet Exchange) protocol. This protocol is routable and can accommodate a larger LAN than NetBEUI while still supporting NetBIOS connectivity. IPX is a connectionless protocol with no guaranteed delivery, and SPX is a connection-oriented protocol with guaranteed delivery.

Transfer Control Protocol/Internet Protocol (TCP/IP)

This is quickly becoming the most popular protocol, providing connectivity to the Internet and is used mostly in large LAN/MAN/WAN implementations. Provides connectivity to UNIX and mainframe boxes running TCP/IP.

TCP/IP is actually a suite of protocols that includes TCP, IP, the User Datagram Protocol (UDP), and several other service protocols. TCP is a connection-oriented protocol with guaranteed delivery, and UDP is a connectionless protocol with no guarantees.

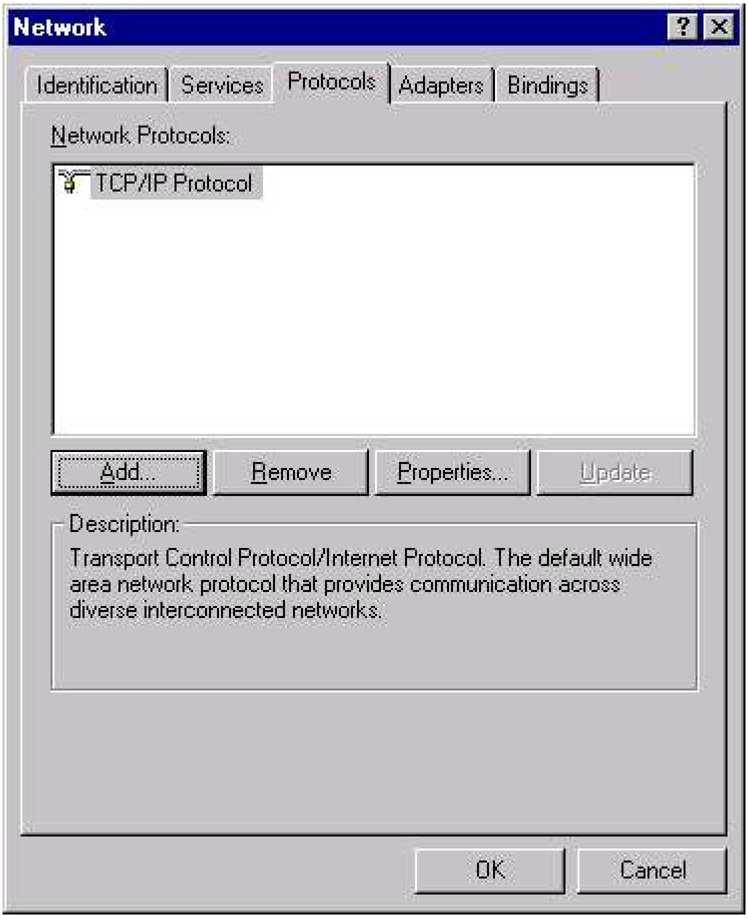
Windows NT offers additional tools that help manage an IP network. Dynamic Host Configuration Protocol (DHCP) is used to dynamically assign IP addresses to clients.

Data Link Protocol (DLC)

This is widely used for IBM mainframe connectivity. Another use of DLC is network connection to Hewlett Packard network printers. DLC is a low-level protocol used in IBM SNA LANs to establish end-to-end connections. DLC is a LAN-based implementation of the connection component found in the wide-area network.

Point-to-Point Tunneling Protocol (PPTP)

Provides a secure connection over the Internet. This protocol enables private virtual networks to exist over the Internet.



Network Protocols:

TCP/IP Protocol

Description:

Transport Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

Fig 11.5 Protocols Tab of Network

PPTP is a high-level protocol used to transport native Microsoft network services through a public TCP/IP network, such as the Internet. PPTP works in conjunction with Remote Access Service (RAS).

Streams

These provides specific connectivity with UNIX machines. Adds porting protocols to the Windows NT environment. The streams interface provides a general-purpose interface used by third-party protocols. Streams offers a raw data pipe between the network and programs-it does not include any transport level services such as TCP or UDP.

AppleTalk

AppleTalk is the protocol used in Apple Macintosh LANs for file sharing, print sharing, and client/server communications. AppleTalk cannot be installed on its own - it is installed automatically when Services for Macintosh is installed.

TCP/IP

The Transmission Control Protocol/Internet Protocol (TCP/IP) is a widely used transport protocol that provides robust capabilities for Windows NT networking. TCP/IP is a fast, routable enterprise protocol that is used on the Internet. TCP/IP is supported by many other operating systems, including Windows 95, Macintosh, UNIX, MS-DOS, and IBM mainframes. TCP/IP is typically the recommended protocol for large, heterogeneous networks.

IP ADDRESS

An IP Address is a 32-bit binary number, broken into four 8-bit sections (often called octets), that uniquely identifies a computer or other network device on a network that uses TCP/IP. Each computer in the network must have a unique IP address (IP stands for Internet Protocol). If two computers have the same IP Address, one or both of the computers may be unable to communicate over the network.

An IP address identifies the host on the network so that IP data packets can be properly routed to the host. IP data packets are simply data encapsulated in IP format for transmission by using TCP/IP.

Although an *IP Address* is a 32-bit binary number, it is normally represented in a dotted decimal format. Each 8-bit octet is represented by a whole number between 0 and 255. e.g. 192.168.511.5

An IP Address contains two important identifiers: a network ID and a host ID. One portion of each IP Address identifies the network segment on which a computer (or other network device) is located.

The second portion of each IP Address identifies the individual computer or network device. This portion is called the host ID. Each computer or other network device on a given network segment must have a unique host ID.

You could arbitrarily assign your own IP network address for your network as long as you are not connected to Internet. But if you are connected to Internet, you must assure that unique IP Addresses are used. To assure uniqueness of network addresses, a governing organization known as InterNIC (Internet Network Information Center) -www.networksolutions.com - is responsible for assigning and maintaining IP addresses.

SUBNET MASKS

A subnet mask specifies which portion of an IP Address represents the network ID and which portion represents the host ID. A subnet mask allows TCP/IP to determine whether network traffic destined for a given IP Address should be transmitted on the local subnet, or whether it should be routed to a remote subnet. A subnet mask should be the same for all computers and other network devices on a given network segment.

Subnet mask is a 32-bit binary number, broken into four 8-bit sections (octets), that is normally represented in a dotted decimal format. Each 8-bit section is represented by a whole number between 0 and 255. A common subnet mask is 255.255.255.0.

If subnet masks are incorrectly configured, network communications problems due to routing errors may occur. For example, TCP/IP may incorrectly determine that a computer on the local subnet is located on a remote subnet and attempt to route a packet to the remote subnet. In this instance, the computer on the local subnet would never receive the packet intended for it.

DEFAULT GATEWAY ADDRESSES

A default gateway address specifies the IP Address of a router on the local network segment. When a computer that uses TCP/IP determines that the computer it wants to communicate with is located on a remote subnet, it sends all network messages intended for the remote computer to the default gateway address, instead of directly to the destination computer. Then the router on the local sub-net specified by the default gateway address forwards the messages to the destination computer on the remote subnet, either directly or via other routers.

DOMAINS AND NAME RESOLUTION

Computers have no problems using IP addresses to locate other networks and hosts. However, these dotted-decimal addresses could be replaced by Domain names and computer names. This make the process of specifying the addresses or other networks or hosts much easier.

A domain name is a unique name formatted similar to an IP address, except that the domain name uses words rather than numbers. The domain name identifies your network and is associated with your network's IP address. For example, the sales department of organization - siliconmedia - may have an domain name like sales.siliconmedia.org, where sales, identifies the subnet, siliconmedia, identifies your corporate network and org , specifies the type of organization. There could be different type of organizations.

Identifier	**Meaning**
com	Commercial entity
gov	Government entity
net	Networking organization
org	General organization

edu	Education
mil	Military

As domain name has to be unique, its management is done by a company InterNIC (www.solutionnetwork.com). You can also check with InterNIC about your domain name.

A computer name specifies a host on the subnet. Your host computer name is combined with your domain to derive your Internet address. By default, Windows NT uses as your host name the NetBIOS computer name you specify during setup, but you can specify a different name when you configure TCP/IP.

DOMAIN NAME SERVICE (DNS)

DNS is a distributed database system that enables a computer to look up a computer name and resolve the name to an IP address. A DNS name server maintains the database of domain names and their corresponding IP addresses. The DNS name server stores records that describe all hosts in the name server's zone.

You can specify the IP address of one or more DNS servers in your TCP/IP configuration, so that whenever workstation needs to resolve a name into an IP address, it queries the DNS servers. If the server doesn't have an entry for the specified name, the name server returns a list of other name servers that might contain the entry. The workstation then can query these additional name servers to resolve the name.

WINDOWS INTERNET NAME SERVICE (WINS)

WINS provides a dynamic database for managing name resolution. WINS relies on a Windows NT server to act as a WINS server. When you install TCP/IP on your workstation, the client software necessary to connect to a WINS server is installed automatically.

One of the main advantage of using WINS is that it's dynamic, and not static like DNS. In DNS, you specify the IP address, and every time computer is moved to some other network, you have to update the DNS entry manually. If you use DHCP to assign network addresses, WINS automatically updates the name database to incorporate DHCP IP address assignments. As computers move from one place (and address) to another on the network, the WINS server automatically updates and maintains their addresses.

When you configure TCP/IP in Windows NT, you can specify the IP addresses of up to two WINS servers to handle name resolution. If your network uses DHCP, you can configure your workstation to resolve the addresses of WINS servers dynamically by using DHCP.

Moreover, WINS includes NetBIOS name space also, which enables it to resolve NetBIOS names into IP addresses.

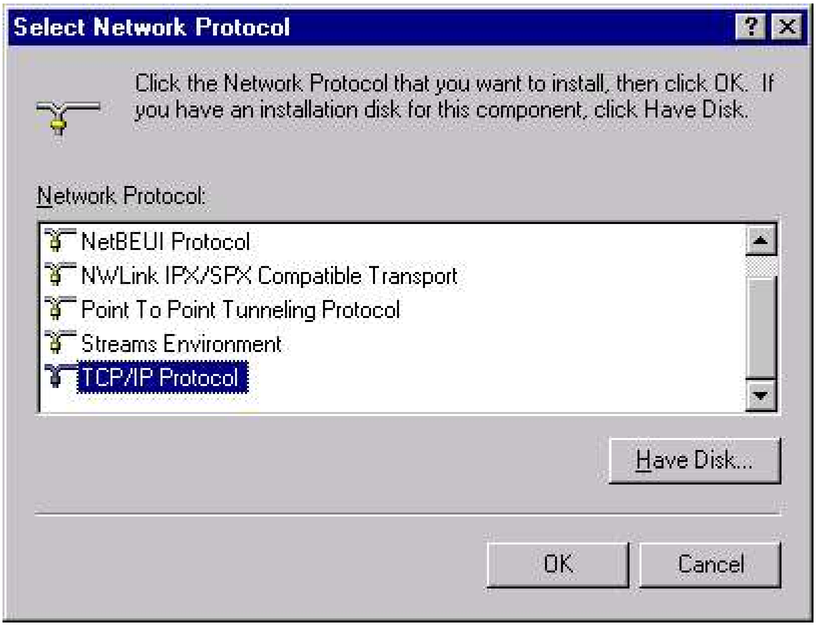
Using HOSTS and LMHOSTS Files

DNS name servers provides in the host domain format to IP addresses. A WINS server can resolve IP host.domain names to IP addresses, and it also can resolve a computer's NetBIOS name into its address name.

At times, it is possible that the DNS or WINS name server is not available to you. In such a case, Windows NT provides two methods for resolving names to IP addresses locally. The first of these files, HOSTS (check the sample file HOSTS.SAM), resolves DNS-formatted names, and works with or in place of DNS. The second file, LMHOSTS (Sample file LMHOSTS.SAM), resolves NetBIOS names into IP addresses, and works with or in place of WINS.

INSTALLING TCP/IP

Windows NT TCP/IP installs like any other network transport protocol - through the Control Panel. To install TCP/IP, open the Network Properties dialog box; click **Add** on the Protocols tab to display the Select **Network Protocol** dialog box (Fig 11.6) and then select **TCP/IP Protocol** from the list.



Select Network Protocol

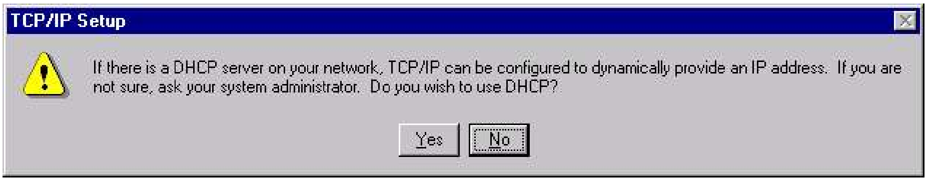
Click the Network Protocol that you want to install, then click OK. If you have an installation disk for this component, click Have Disk.

Network Protocol:

- NetBEUI Protocol
- NWLink IPX/SPX Compatible Transport
- Point To Point Tunneling Protocol
- Streams Environment
- TCP/IP Protocol

Fig 11.6 Adding TCP/IP

After you close this dialog box, Windows NT prompts you to specify whether you want to use DHCP to assign your IP address. Choose **Yes** to use DHCP, or No to assign an IP address manually. (Fig 11.7)



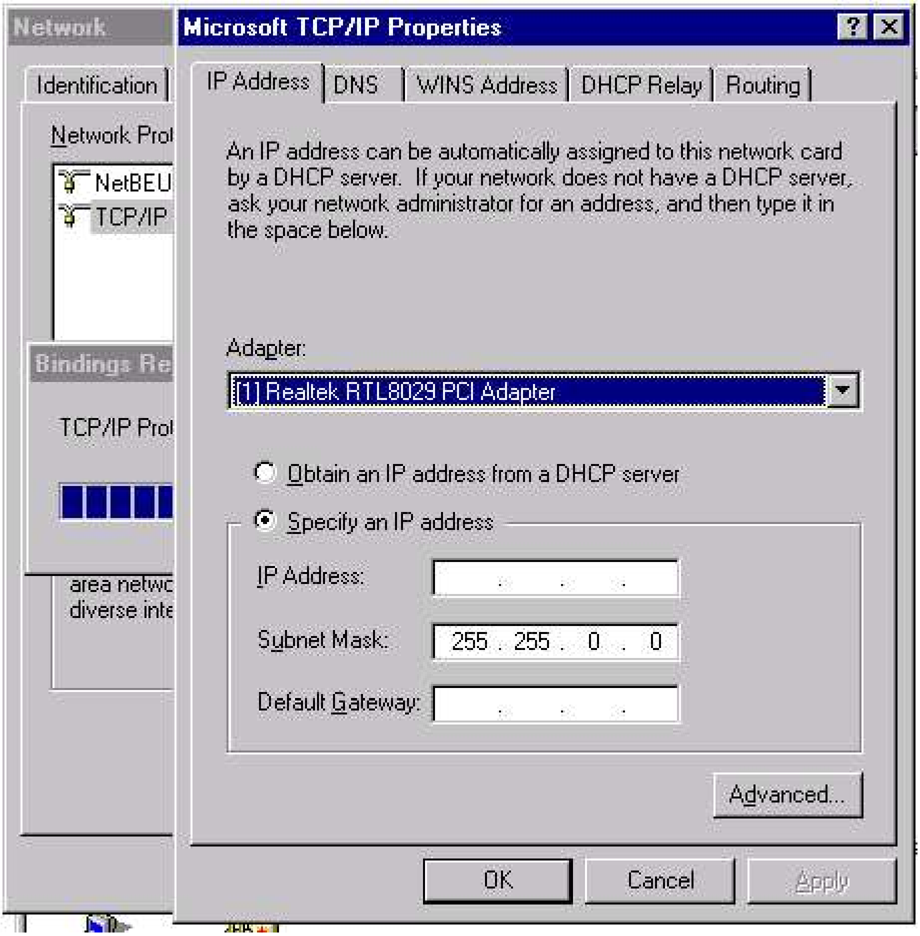
TCP/IP Setup

If there is a DHCP server on your network, TCP/IP can be configured to dynamically provide an IP address. If you are not sure, ask your system administrator. Do you wish to use DHCP?

Fig 11.7 Confirmation for dynamically configuring TCP/IP

Now Windows NT asks about the location of Windows NT source files. When you specify the location, NT installs TCP/IP in your computer. If you are using a local CD-ROM, indicate the drive letter and path. NT will copy files from the distribution media to the local system directory.

You will be returned to the Protocols tab of the Network window. You should see TCP/IP Protocol listed in the Network Protocols list. Click the **Close** button at the bottom of the Network window.



An IP address can be automatically assigned to this network card by a DHCP server. If your network does not have a DHCP server, ask your network administrator for an address, and then type it in the space below.

Adapter: [1] Realtek RTL8029 PCI Adapter

○ Obtain an IP address from a DHCP server

● Specify an IP address

IP Address: . . .

Subnet Mask: 255 . 255 . 0 . 0

Default Gateway: . . .

Fig 11.8 Specifying static IP Address

NT will go through an automatic process to review the bindings on the network adapter. NT will display the Microsoft TCP/IP Properties window so you can provide specific TCP/IP configuration information, which is necessary to complete the binding. (Fig 11.8)

Enter the IP address, subnet mask, and default gateway for your network card into the appropriate text boxes, if you want to configure it manually. Windows NT provides automatic way to locate the IP address using DHCP server (DHCP will be discussed in more detail in next chapter. For now, you may specify an IP address manually).

This is the minimal amount of information you need to provide to get your system up and running with TCP/IP. Click **OK** at the bottom of the Microsoft TCP/IP properties window. NT will complete the adapter binding process and tell you that you need to restart your computer before your changes can take effect.

CONFIGURING TCP/IP

IP ADDRESS

IP Addresses must be configured on each computer when TCP/IP is installed. You can assign an IP Address to a Windows NT computer in one of two ways: by configuring a computer to obtain an IP Address automatically from a DHCP server, or by manually specifying a computer's IP Address configuration. IP Addresses are assigned to Windows NT computers in the Microsoft TCP/IP Properties dialog box.

As stated earlier, DHCP will be taken up in the next chapter. For now, IP address will be configured manually.

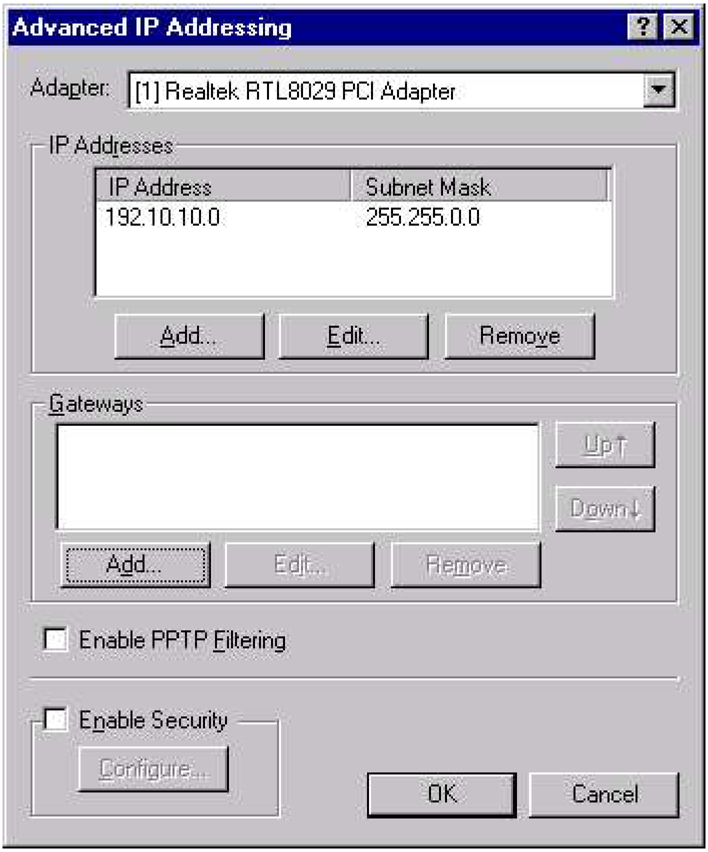
To configure the IP Address, logon as administrator and select **Control Panel ➢ Network** to display the Network dialog box. Click the **Protocols** tab and then double-click **TCP/IP Protocol**. This will display the Microsoft TCP/IP Properties window. Now, click the **Advanced** button located in the bottom-right corner of the windows. This will display the Advanced IP Addressing window. (Fig 11.9)

Logically Multihomed Adapter

Windows NT allows you to assign up to five IP addresses to a single network adapter. This is known as a logically multihomed network adapter. To select an adapter from multiple physical network adapters, you can use the Adapter pick list to choose the adapter you want to configure.

IP Addresses

You can use TCP/IP to communicate with a computer outside of your subnet. Such communication needs to be done through an IP gateway. To specify the IP address for such communication, click on **IP address** tab.



Advanced IP Addressing

Adapter: [1] Realtek RTL8029 PCI Adapter

IP Addresses

IP Address	Subnet Mask
192.10.10.0	255.255.0.0

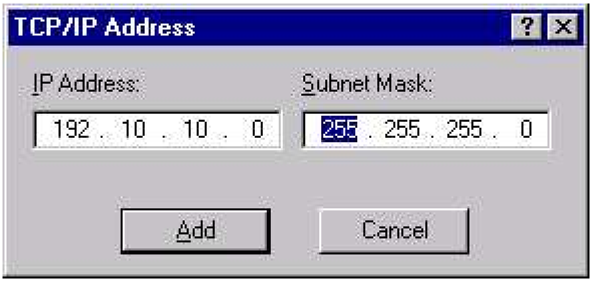
Gateways

☐ Enable PPTP Filtering

☐ Enable Security

Fig 11.9 Specifying Advance IP Address

the add button in the IP Addresses window to add additional IP address and subnet mask pairs for the current network adapter. (Fig 11.10)



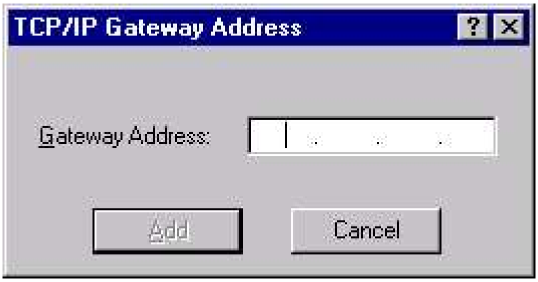
TCP/IP Address

IP Address: 192 . 10 . 10 . 0

Subnet Mask: 255 . 255 . 255 . 0

Fig 11.10 Adding TCP/IP address

If your network is connected to multiple gateways, you can specify as many gateways as necessary to allow for fault tolerance if one gateway becomes unavailable. To add a gateway, click the **Add** button in Gateway section. To change the search order for the gateways, use the Up and Down buttons on the Advanced IP Addressing dialog box to change the order of the gateways in the list.



TCP/IP Gateway Address

Gateway Address: . . .

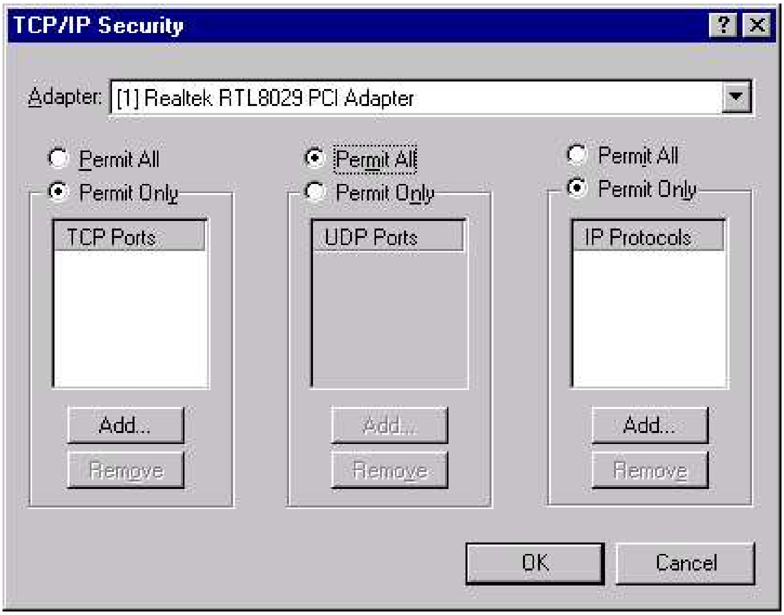
Fig 11.11 Adding Gateway address

PPTP

Point-to-Point Tunneling Protocol (PPTP) allows you to create multiprotocol virtual private networks (VPNs). If you enable the PPTP Filtering, your NT Server will only communicate with machines on its VPNs. Select the Enable PPTP Filtering option to restrict network access to PPTP.

TCP/IP Security

Windows NT has the ability to filter network traffic by TCP or UDP port number, as well as IP protocol value. Using such filter you can have greater control over the type of TCP/IP traffic that your server will respond to, thus providing a higher level of security.



TCP/IP Security

Adapter: [1] Realtek RTL8029 PCI Adapter

○ Permit All
● Permit Only
TCP Ports

● Permit All
○ Permit Only
UDP Ports

○ Permit All
● Permit Only
IP Protocols

Fig 11.12 Specifying TCP/IP security

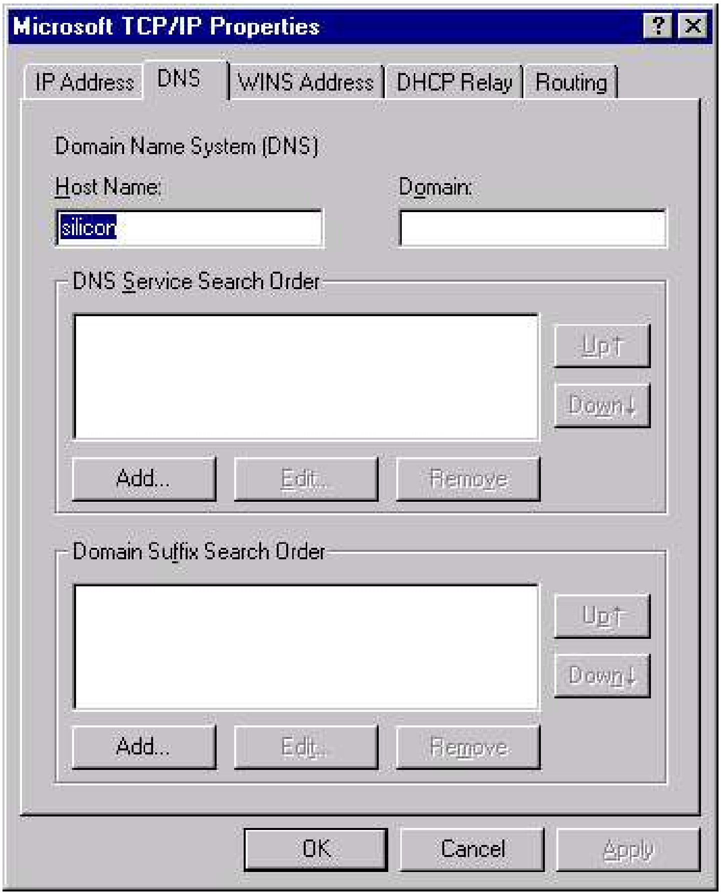
Select the **Enable Security** option to enable IP or port-level filtering and then click the **Configure** button. This will bring up the TCP/IP Security Window as shown in Fig 11.12.

To enable only certain TCP or UDP ports, select the **Permit Only** option above the appropriate field, then click the **Add** button to add the TCP or UDP port addresses you want to allow.

USING DNS

You can configure your Windows NT to use an existing DNS server to resolve the domain names. Whenever the workstation require to resolve a domain name, it will query the DNS server.

To configure DNS for TCP/IP, logon as administrator and select **Control Panel ➢ Network** to display the Network dialog box. Click the **Protocols** tab and then double-click **TCP/IP Protocol**. This will display the Microsoft TCP/IP Properties window. Now, click the **DNS** tab to display the DNS configuration options. (Fig 11.13)



Host Name: silicon

Domain:

Fig 11.13 Configuring DNS for TCP/IP

Specifying DNS Server IP Addresses

If you do not use DHCP to define IP addresses, you must provide the IP addresses of the DNS servers you use. If you do use DHCP, the DHCP server can automatically provide the IP addresses of the DNS servers. You can specify DNS server addresses in the DNS Service Search Order group of controls. Click on **Add** button to add an IP address of DNS Server.

Adding Domain Suffix Entries

Normally, DNS appends the domain name specified in the Domain text box to your host name to resolve the domain name of your computer. You can specify up to five additional domain suffixes that DNS can use if it can't resolve the complete domain name by using the default domain name.

USING WINS

If your network includes one or more Windows NT servers configured as WINS servers, or access to WINS servers, you can configure your Windows NT TCP/IP stack to use WINS to resolve names. WINS offers numerous advantages over DNS.

To configure WINS, logon as administrator and select **Control Panel ➢ Network** to display the Network dialog box. Click the **Protocols** tab and then double-click TCP/IP Protocol. This will display the Microsoft TCP/IP Properties window. Now, click the **WINS** tab to display the WINS configuration options. (Fig 11.14)

You can specify a primary and a secondary WINS server by entering their IP addresses in the fields provided for that purpose on the property page. If your computer uses DHCP to resolve names, however, you can leave the IP address fields blank, and Windows NT queries the DHCP server for the WINS server addresses.

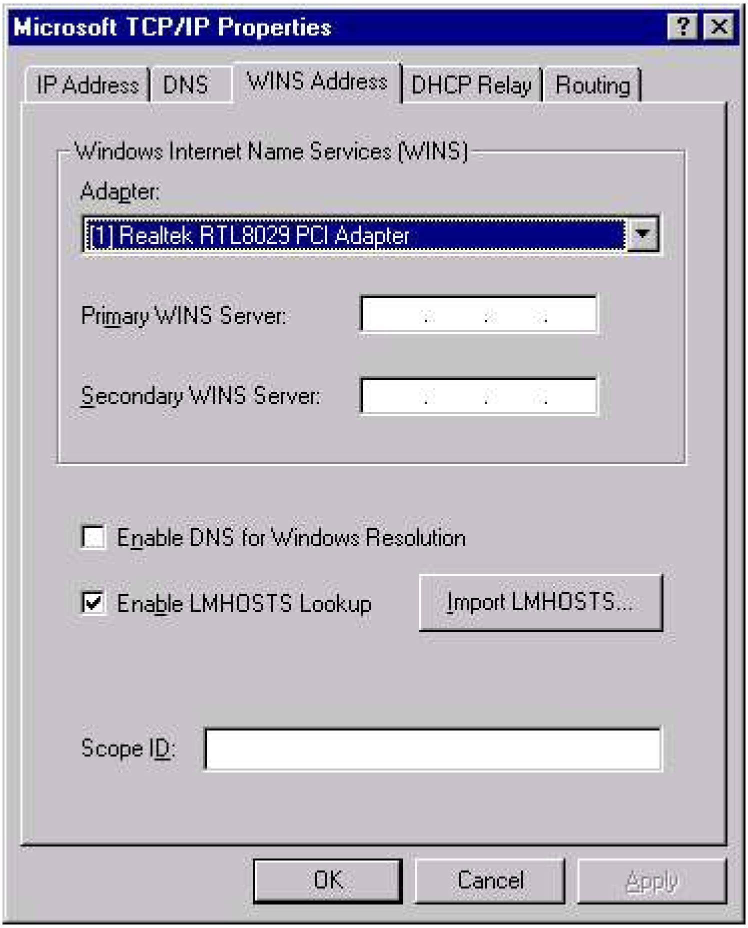
If you want to allow your system to act as a WINS proxy, check the Enable WINS Proxy Agent.

Check the Enable DNS for Windows Name Resolution box if you want to use a DNS server to provide resolution for NetBIOS names.

If you want to use an LMHOSTS file for Windows name resolution, check the box Enable LMHOSTS lookup.

DHCP RELAY

The setting of this tab will be discussed in next chapter.



Microsoft TCP/IP Properties

Windows Internet Name Services (WINS)

Adapter: [1] Realtek RTL8029 PCI Adapter

Primary WINS Server: . . .

Secondary WINS Server: . . .

□ Enable DNS for Windows Resolution

☑ Enable LMHOSTS Lookup

Scope ID:

Fig 11.14 Specifying WINS for TCP/IP

IP ROUTING

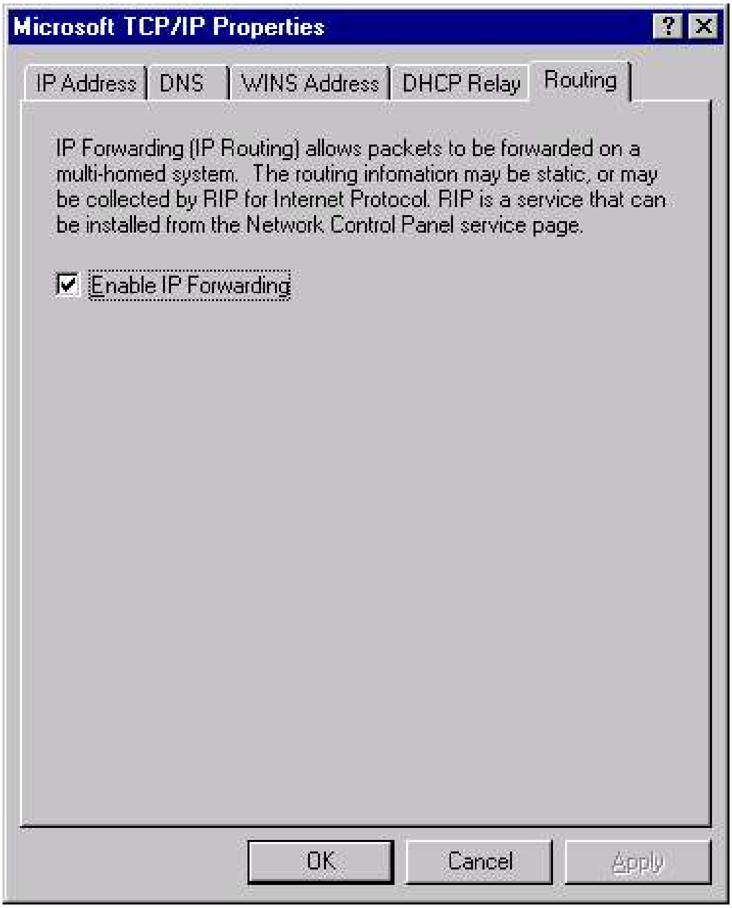
IP routing is a function of the Internet Protocol (IP) that uses IP Address information to send data packets from a source computer on one network segment across one or more routers to a destination computer on another network segment. Hardware devices that perform routing are called routers. Windows NT (servers only) computers that have multiple network adapters (sometimes called multihomed computers) can function as IP routers. IP routers are occasionally referred to as Internet routers.

Two primary types of routing exist: static and dynamic.

Static Routing

In static routing, no additional software is necessary to implement Static Routing in multihomed Windows NT computers. Static routers are not capable of automatically building a routing table. A routing table contains a list of network IDs, each of which is associated with the IP Address of the router on the network that can forward data packets over the shortest path to the specified destination computer. In a Static Routing environment, administrators must manually configure the routing table on each individual router.

To configure Routing, logon as administrator and select **Control Panel ➢ Network** to display the Network dialog box. Click the **Protocols** tab and then double-click **TCP/IP Protocol**. This will display the Microsoft TCP/IP Properties window. Now, click the **Routing** tab to display the Routing configuration options. (Fig 11.15)



IP Forwarding (IP Routing) allows packets to be forwarded on a multi-homed system. The routing infomation may be static, or may be collected by RIP for Internet Protocol. RIP is a service that can be installed from the Network Control Panel service page.

☑ Enable IP Forwarding

Fig 11.15 Configuring Routing

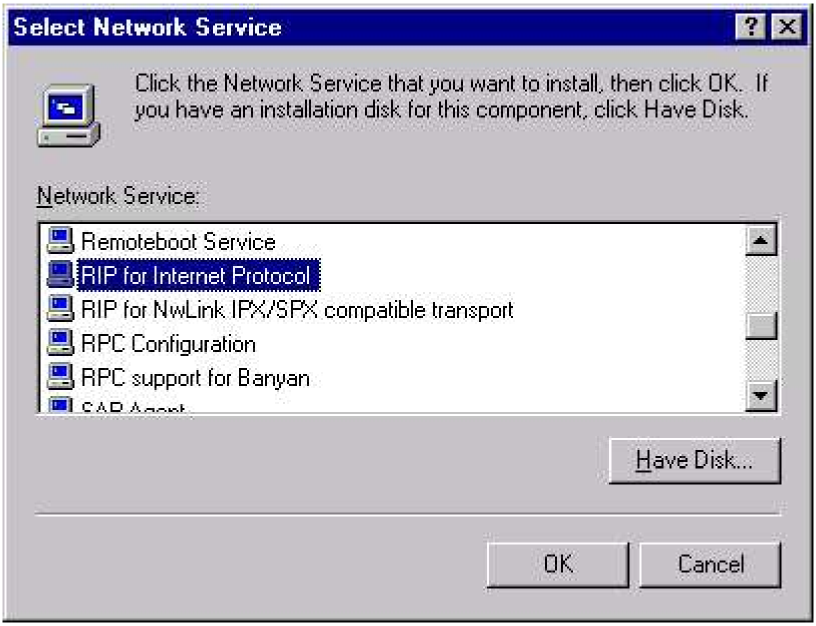
Here select the **Enable IP Forwarding** check box and press **OK**. Select **Close** in the Network dialog box. A Network Settings Change dialog box appears. Click **Yes** to restart the computer and implement the changes you made. After the computer restarts, Static Routing will be enabled. To configure the routing table manually on a Windows NT computer that is configured as a static router, use the Route.exe command-line utility.

Dynamic Routing

Dynamic routing is intelligent IP routing. Dynamic routing requires the use of additional software in multihomed Windows NT Server computers. A dynamic router is capable of automatically building and updating a routing table. In a Dynamic routing environment, administrators needn't configure the routing table on each individual router manually. As changes are made to the network, dynamic routers automatically adjust their routing tables to reflect these changes.

By installing RIP(Route Information Protocol) for Internet Protocol, multihomed Windows NT Server computers can be configured to function as dynamic routers. Routing Information Protocol (RIP) is the software that allows Windows NT Server computers to share their routing tables dynamically. Dynamic routers that use RIP to share their routing tables are sometimes called RIP routers.

To configure DNS for TCP/IP, logon as administrator and select **Control Panel ➢ Network** to display the Network dialog box. Select the **Service** tab. Click on the **Add** button. Select the **RIP for Internal Protocol** and click **OK**. (Fig 11.16)



Click the Network Service that you want to install, then click OK. If you have an installation disk for this component, click Have Disk.

Network Service:

- Remoteboot Service
- RIP for Internet Protocol
- RIP for NwLink IPX/SPX compatible transport
- RPC Configuration
- RPC support for Banyan
- SAP Agent

Fig 11.16 Installing Route Information Protocol

A Windows NT Setup dialog box appears asking for Windows NT Server source files. Insert the CD-ROM and click the **Continue** command button. The Network dialog box reappears. Windows NT, in the process of installing RIP for Internet Protocol, has automatically enabled IP forwarding. Click the **Close** command button.

Windows NT performs various bindings operations. A Network Settings Change dialog box appears. Click **Yes** to restart the computer and implement the changes you made. After the computer restarts, dynamic (RIP) routing will be enabled.

EXERCISE

Fill in the Blanks:

1. When data is sent from one computer to another computer, it is broken into small sections called _______.
2. A packet is consist of three parts ______, ________ and _______.
3. An IP address is consist of ______ 8-bits sections called _______.
4. The governing organization for uniqueness of IP address is known as __________.
5. __________ file resolves DNS-formatted names, and works with or in place of DNS.
6. __________ file resolves NetBIOS names into IP addresses, and works with or in place of WINS.
7. Up to _____ IP addresses can be assigned to a single network adapter. Such Adapters are known as ________.

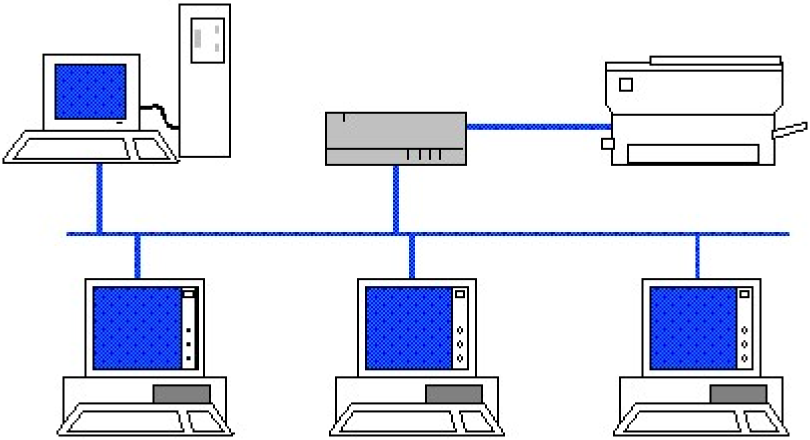
Answer the following Questions:

1. Define protocols. What are the various types of protocols available?
2. What do you understand by binding process?
3. What is the significance of Subnet mask and Gateway addresses.
4. What is the utility of DNS & WINS?
5. On your machine, locate for the protocol that has been installed on it. If it is TCP/IP remove it.
6. Discuss the services supported by Windows NT.
7. What do you understand by the following terms:
   a) PPTP
   b) RIP
   c) Static & Dynamic routing
   d) DHCP
   e) IPX/SPX
   f) DLC
8. Install TCP/IP on your machine if it has been uninstalled. While installing, do not try to obtain IP address from the DHCP server option. After the configuration, manually change the IP Address to 192.10.10.6 and Subnet Mask to 255.255.255.0.

CHAPTER 12

DHCP, WINS and DNS

USING DHCP SERVER
INSTALLING DHCP SERVER
CONFIGURING DHCP SERVER
WINDOWS INTERNET NAME SERVICE (WINS)
INSTALLING WINS SERVICE
CONFIGURING WINS SERVICE
DOMAIN NAME SYSTEN (DNS) SERVER
INSTALLING WINS SERVICE
DNS MANAGER



USING DHCP SERVER

Till now, we have seen how IP addresses could be configured manually. But if one system in the network changes its IP address due to one reason or the other. In such case, administrator has to update this IP address at different places in the network, which becomes a tedious task in a large network. Dynamic Host Configuration Protocol (DHCP) resolve this problem. In DHCP, each of the computers is configured to obtain its IP Address from a Dynamic Host Configuration Protocol (DHCP) server.

The Dynamic Host Configuration Protocol (DHCP) is actually an extension to the BOOTP protocol, which had been the standard for assigning dynamic IP addresses and remote-booting diskless workstations. Because DHCP is a client/server system, to have a fully functioning system, you must have at least one machine running the DHCP server service, and one machine with a DHCP-capable TCP/IP stack.

Advantages of using a DHCP server

Assigning IP Addresses by using a DHCP server is the preferred method because:

- Using a DHCP server makes it possible for you to manage IP Addresses centrally, thus assuring addresses are valid and not duplicated.
- It reduces the amount of administration time required to manage and maintain IP Addresses for each computer on the network.
- It reduces the likelihood of human error when IP Addresses are assigned because no need exists to enter an IP Address manually on every individual computer.
- It also enables you to regain the use of an IP Address no longer assigned to a host when the DHCP lease period for this IP Address expires.

There are four phases to IP assignment with DHCP:

- The client makes a request for an IP address. This is called IP lease request. The request is made through **DHCP discover** packet, which is sent to to the local subnet broadcast address of 255.255.255.255.
- A DHCP server offers an IP address, called IP lease Offer. Any available DHCP servers with IP addresses to offer respond to the client request with a **DHCP Offer** packet.
- The client selects an DHCP Offer, regardless of which subnet the DHCP server is located on. This is called IP lease selection. The client then sends a **DHCP request** message, requesting a lease.
- The DHCP server selected assigns an IP to the client through DHCP Acknowledge. while any other DHCP servers

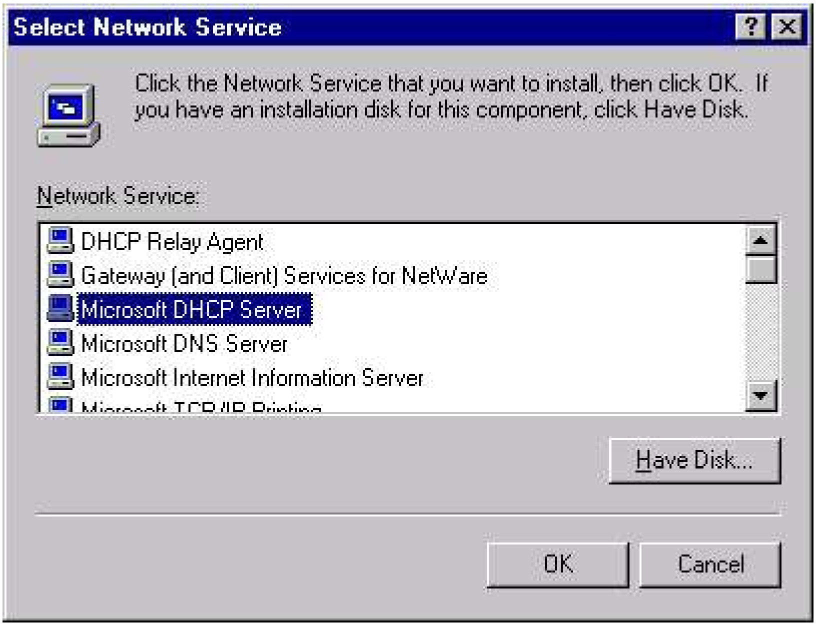
that made an offer withdraw. The IP information is assigned to the client and the protocol is bound.

Before you can assign an IP Address to a Windows NT computer by using a DHCP server, you must first install and configure a DHCP server on your network.

INSTALLING DHCP SERVER

Microsoft includes a DHCP server product with Windows NT Server. Microsoft DHCP Server is an NT Server service that provides centralized management of IP Address assignment. Microsoft DHCP Server can be installed on any Windows NT Server computer that has a manually configured IP Address for each network adapter installed in it.

To install Microsoft DHCP server on a Windows NT server computer, select **Start ➤ Settings ➤ Control Panel** and click on the Network icon. In the Network dialog box, click the **Services** tab and Click the **Add** button on it. This brings the Select **Network Service** dialog box. (Fig 12.1)


Select Network Service

Click the Network Service that you want to install, then click OK. If you have an installation disk for this component, click Have Disk.

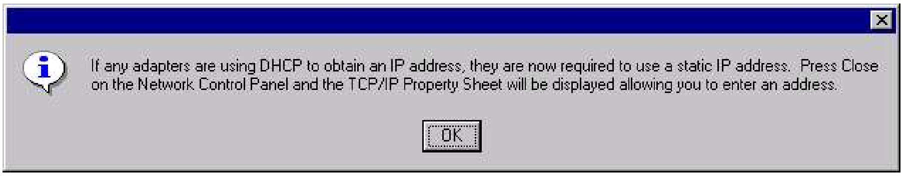
Network Service:

DHCP Relay Agent
Gateway (and Client) Services for NetWare
Microsoft DHCP Server
Microsoft DNS Server
Microsoft Internet Information Server
Microsoft TCP/IP Printing

Fig 12.1 Installing DHCP Server

In the Select **Network Service** dialog box, highlight Microsoft DHCP Server. Click **OK**.

Now Windows NT asks about the location of Windows NT source files. When you specify the location, NT installs TCP/IP in your computer. If you are using a local CD-ROM, indicate the drive letter and path. NT will copy files from the distribution media to the local system directory. An informational dialog box appears, indicating all network adapters in this computer must have manually configured IP Addresses.



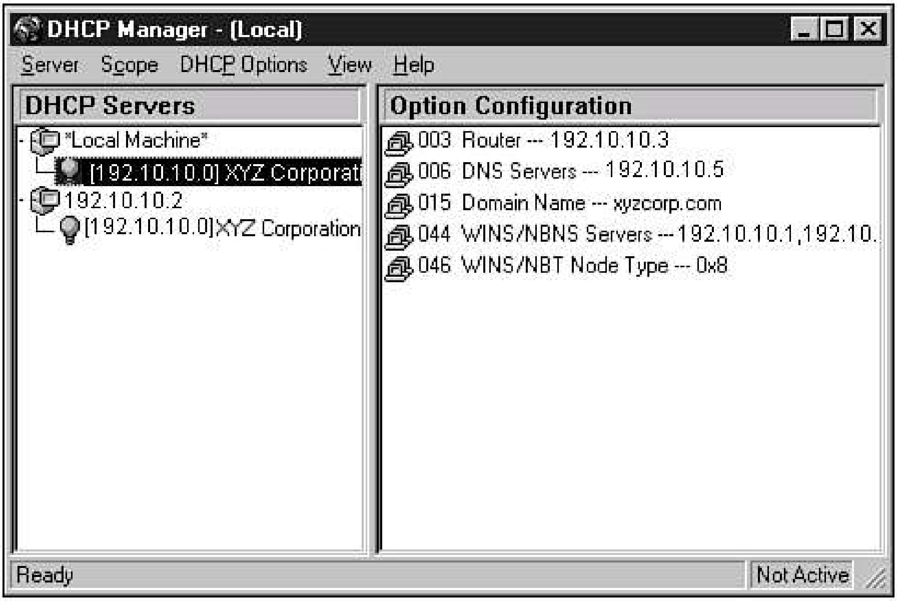
If any adapters are using DHCP to obtain an IP address, they are now required to use a static IP address. Press Close on the Network Control Panel and the TCP/IP Property Sheet will be displayed allowing you to enter an address.

Fig 12.2 Informational dialog box

Click **OK**. The Network dialog box reappears. Click the **Close** command button. NT will complete the binding process and tell you that you need to restart your computer before your changes can take effect.

CONFIGURING DHCP SERVER

To configure Microsoft DHCP server on a Windows NT server computer, log on as Administrator. and Select **Start ➢ Programs ➢ Administrative Tools (Common) ➢ DHCP Manager**. The DHCP Manager dialog box appears.

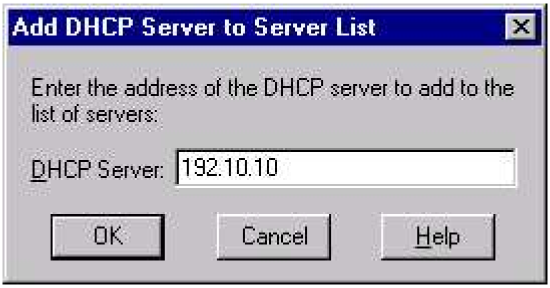


Local Machine
[192.10.10.0] XYZ Corporat
192.10.10.2
[192.10.10.0]XYZ Corporation

003 Router --- 192.10.10.3
006 DNS Servers --- 192.10.10.5
015 Domain Name --- xyzcorp.com
044 WINS/NBNS Servers ---192.10.10.1,192.10.
046 WINS/NBT Node Type --- 0x8

Fig 12.3 DHCP Manager

Select **Server ➢ Add** or press Ctrl+A to display the Add DHCP Server to Server List dialog box. Enter the IP address of the DHCP Server in the DHCP Server field and click the **OK** button. The IP address appears in the DHCP Server window.



Enter the address of the DHCP server to add to the list of servers:

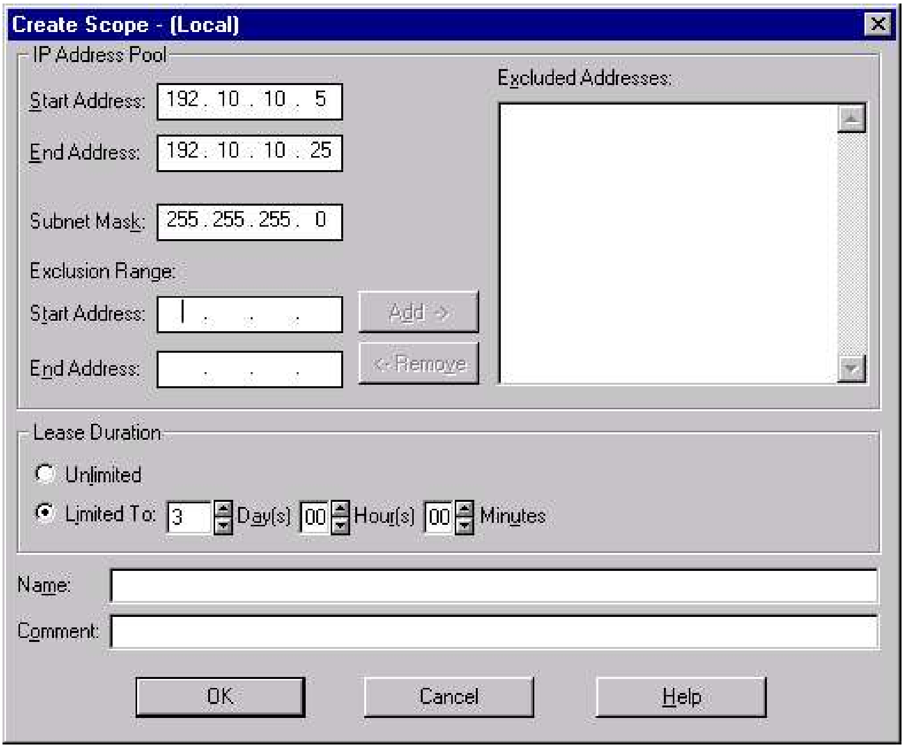
DHCP Server: 192.10.10

Fig 12.4 Adding DHCP server to Server List

DHCP Scope

To activate a DHCP server, a scope must be created. A scope is a logical grouping of DHCP clients. Each subnet must have a scope, and it defines the parameters for that subnet.

DHCP Manager gives you options to create, activate and delete the scope. To create a scope, choose **Scope ➤ Create** in DHCP Manager. The Create Scope dialog box appears, enabling you to configure the DHCP server. Configure the scope by creating an IP address pool and subnet mask, as shown in Fig 12.5.



Start Address: 192 . 10 . 10 . 5

End Address: 192 . 10 . 10 . 25

Subnet Mask: 255 . 255 . 255 . 0

Start Address: . . .

End Address: . . .

○ Unlimited

● Limited To: 3 Day(s) 00 Hour(s) 00 Minutes

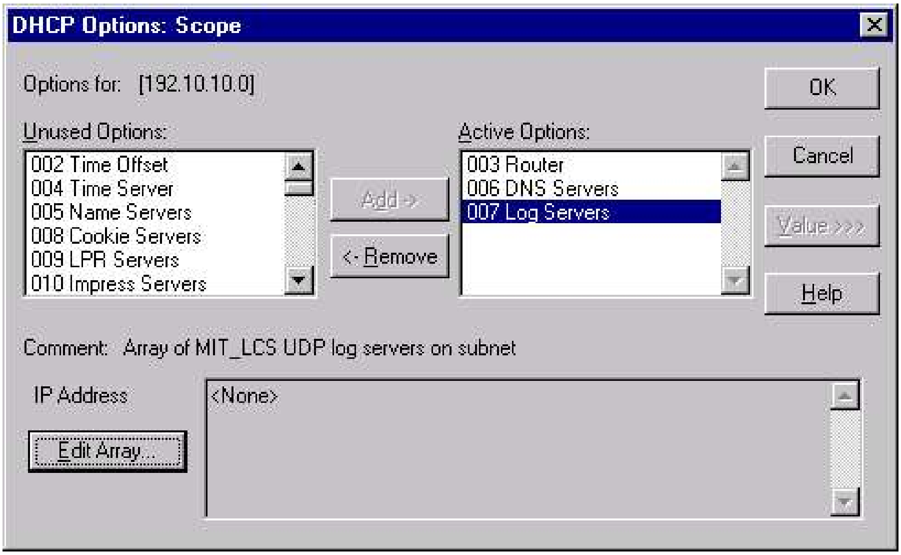
Name:

Comment:

Fig 12.5 Creating Scope

Scope options are of two type: You can have a global scope setting, which applies to all scopes for the DHCP Server, or a local scope setting, which applies only to a specific scope. Local scope properties override globally defined scope properties.

To configure local scope options including router IP addresses, DNS servers, and WINS servers options, first select the desired scope, and then choose **DHCP Options ➤ Scope**. Add the desired options by selecting an **option** and clicking **Add**. (Fig 12.6)



DHCP Options: Scope

Options for: [192.10.10.0]

Unused Options:
002 Time Offset
004 Time Server
005 Name Servers
008 Cookie Servers
009 LPR Servers
010 Impress Servers

Active Options:
003 Router
006 DNS Servers
007 Log Servers

Comment: Array of MIT_LCS UDP log servers on subnet

IP Address <None>

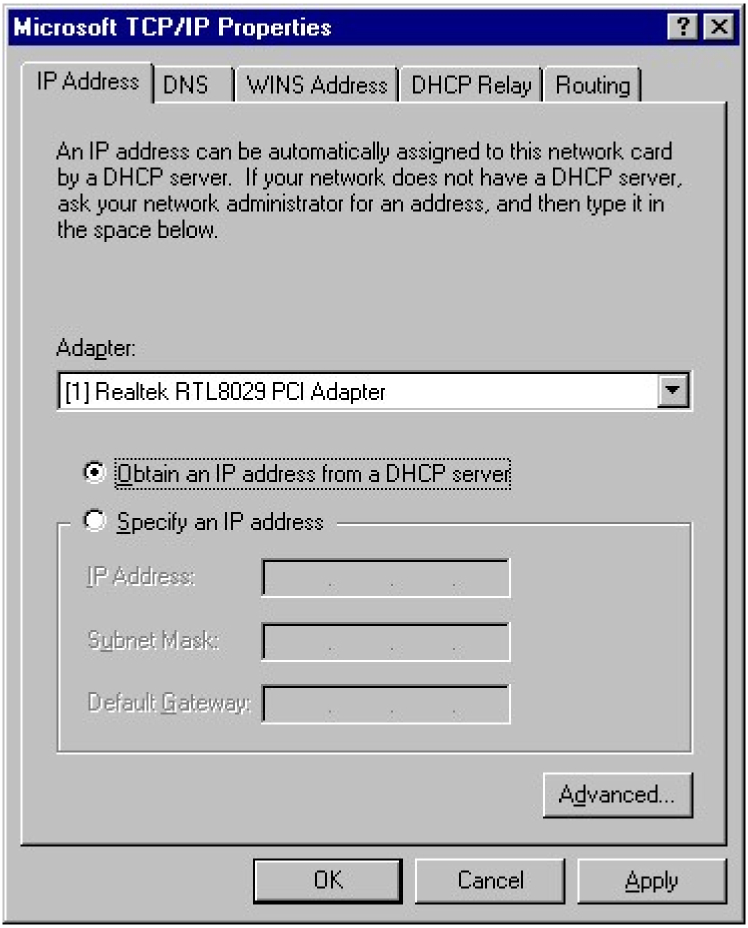
Fig 12.6 Configuring local scope

To set additional configuration options for each active option, select the option you want to configure, and click **Edit Array**. Type in the IP Address of the router you want assigned as the default gateway address in the New IP Address text box. Click the **Add** command button. Click **OK**.

Locating IP using DHCP

To configure a Windows NT client computer to obtain an IP Address from a DHCP server, select **Start ➤ Settings ➤ Control Panel**. In the Control Panel dialog box, double-click **Network** and click the **Protocols** tab in Network dialog box. Select the **TCP/IP Protocol** and click the Properties command button.

This brings the Microsoft TCP/IP Properties dialog box. Ensure the radio button next to “Obtain an IP Address from a DHCP server” is selected. (Fig 12.7).



Microsoft TCP/IP Properties

An IP address can be automatically assigned to this network card by a DHCP server. If your network does not have a DHCP server, ask your network administrator for an address, and then type it in the space below.

Adapter: [1] Realtek RTL8029 PCI Adapter

● Obtain an IP address from a DHCP server

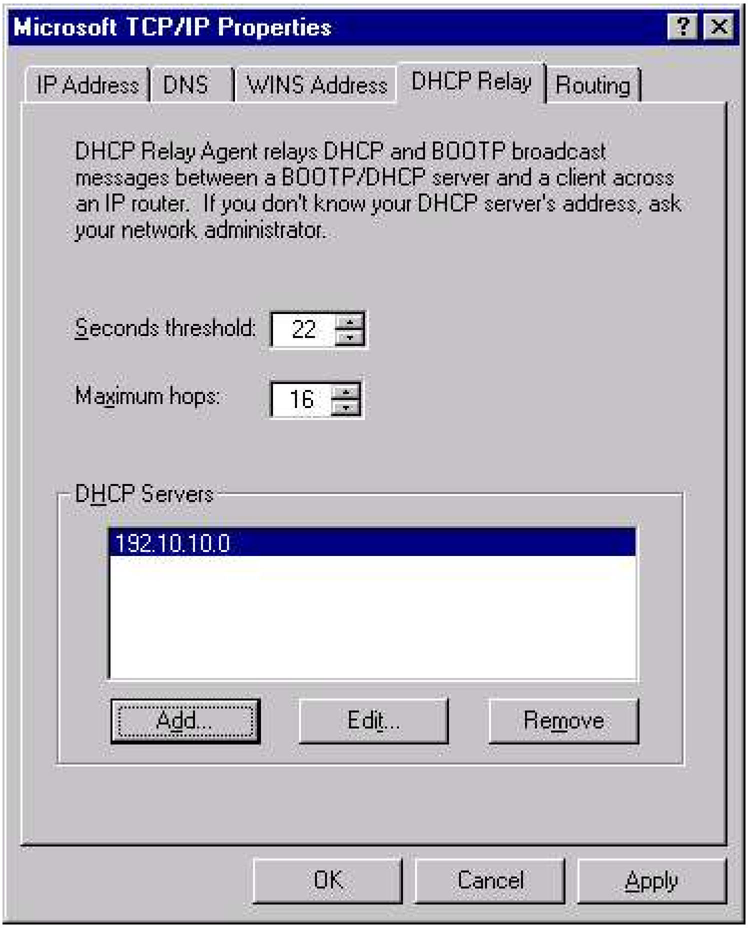
○ Specify an IP address

Fig 12.7 Locating IP using DHCP

DHCP Relay Agent

The DHCP Relay Agent is a Windows NT Server service that forwards client DHCP configuration requests to a DHCP server on another network segment or remote DHCP server. It allows computers on one subnet to receive IP Addresses from a DHCP server located on a different subnet and can be installed only on multihomed Windows NT Server computers. The DHCP Relay Agent is normally installed on Windows NT Server computers configured to function as static or dynamic routers.

To install the DHCP Relay Agent service, log as a member of local Administrator group and Click **Start** ➤ **Settings** ➤ **Control Panel** and click on the Network icon. Select the **Services** tab and click **Add**, and select **DHCP Relay Agent**. Now, Select the **Protocols** tab, and select **TCP/IP** properties. On the TCP/IP Properties sheet, select the **DHCP Relay** tab (Fig 12.8), and add the IP of your DHCP server or servers.



DHCP Relay Agent relays DHCP and BOOTP broadcast messages between a BOOTP/DHCP server and a client across an IP router. If you don't know your DHCP server's address, ask your network administrator.

Seconds threshold: 22

Maximum hops: 16

192.10.10.0

Fig 12.7 DHCP Relay Agent

WINDOWS INTERNET NAME SERVICE (WINS)

Windows Internet Name Service (WINS) is a Windows NT Server service that provides NetBIOS name resolution services to client computers. A single WINS server can handle about 10,000 name resolution requests an hour.

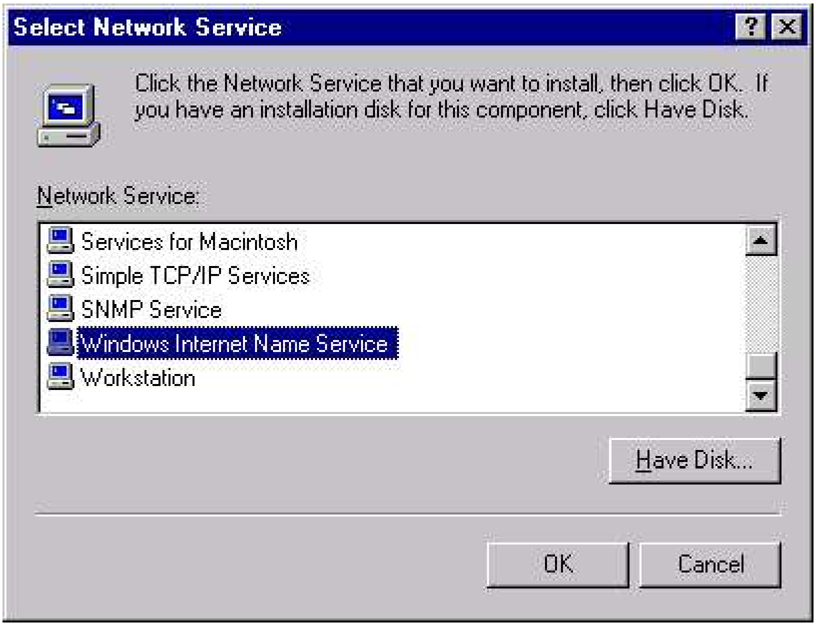
A Windows NT Server computer that has WINS installed on it is called a WINS server. A NetBIOS name is the computer name assigned during the installation of Windows NT. A NetBIOS name can be up to 15 characters in length. NetBIOS names are used to connect to resources located on other computers when a user browses the network, maps to a network drive, or uses the Net use command from the command prompt.

When a user attempts to connect to a computer selected from a browse list by the remote computer's NetBIOS name, the user's computer must first obtain the IP Address associated with the remote computer's NetBIOS name. This process is called **NetBIOS name resolution**. Once the user's computer has resolved the remote computer's NetBIOS name to its IP Address, it can then establish TCP/IP network communications with the remote computer.

The WINS server dynamically updates its NetBIOS name to IP Address tables whenever computers are added to or removed from the network. WINS maintains a database on the WINS server. This database provides a computer name to IP address mapping, enabling other computers on the network to connect to it simply by supplying a machine name.

INSTALLING WINS SERVICE

WINS Service can be installed on any Windows NT Server computer. To install WINS server on a Windows NT server computer, select **Start ➢ Settings ➢ Control Panel** and click on the **Network** icon. In the Network dialog box, click the **Services** tab and Click the **Add** button on it. This brings the Select **Network Service** dialog box. (Fig 12.8)



Select Network Service

Click the Network Service that you want to install, then click OK. If you have an installation disk for this component, click Have Disk.

Network Service:

- Services for Macintosh
- Simple TCP/IP Services
- SNMP Service
- Windows Internet Name Service
- Workstation

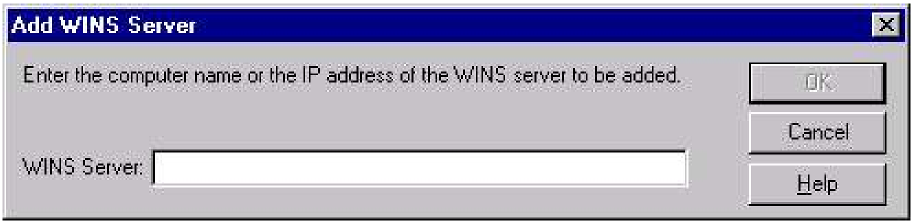
Fig 12.8 Installing WINS

In the Select **Network Service** dialog box, highlight Windows Internet Name Server. Click **OK**.

Now Windows NT asks about the location of Windows NT source files. When you specify the location, NT installs TCP/IP in your computer. If you are using a local CD-ROM, indicate the drive letter and path. NT will copy files from the distribution media to the local system directory. Click **OK**. The Network dialog box reappears. Click the **Close** command button. NT will complete the binding process and tell you that you need to restart your computer before your changes can take effect.

CONFIGURING WINS SERVICE

All configuration options for WINS can be set through the WINS Manager tool. To start WINS Manager, click **Start ➤ Programs ➤ Administrative Tools (Common) ➤ WINS Manager**. In the beginning, it displays the WINS Server on the local computer. To add WINS Server to WINS manager, Choose **Server ➤ Add WINS Server**.



Add WINS Server

Enter the computer name or the IP address of the WINS server to be added.

WINS Server:

Fig 12.9 Adding WINS Server

Add the IP address or computer name in the Add WINS Server dialog box. After adding your WINS Servers to the local WINS Manager, you can configure the local WINS Server for optimal performance. This includes setting your WINS Server configuration, replication partners, and preferences etc.

To configure the WINS server, select **Server ➤ Configuration** to display WINS Server Configuration dialog box.

Renewal Interval

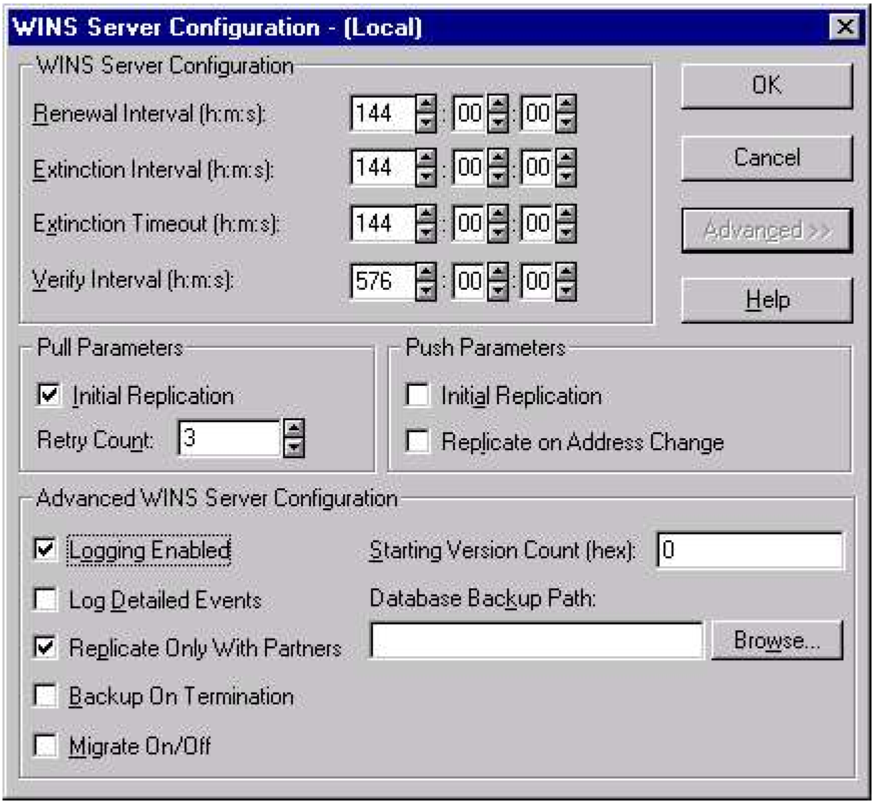
This value specifies how often a WINS client needs to register its name with the WINS Server. The default is 6 days. If a client does not reregister successfully by the Renewal Interval time, the registration in the WINS database for that client will be marked released.

Extinction Interval

Sets how long it is between the time the record is marked released and when it's marked extinct. An extinct records can removed from the database. The default and maximum time is 6 days.

Extinction Timeout

Specifies the interval between when an entry is marked extinct and when the entry is finally removed from the database. The default and maximum time is 6 days and minimum is 1 day.



WINS Server Configuration - (Local)

WINS Server Configuration

Renewal Interval (h:m:s): 144 : 00 : 00

Extinction Interval (h:m:s): 144 : 00 : 00

Extinction Timeout (h:m:s): 144 : 00 : 00

Verify Interval (h:m:s): 576 : 00 : 00

Pull Parameters

☑ Initial Replication

Retry Count: 3

Push Parameters

□ Initial Replication

□ Replicate on Address Change

Advanced WINS Server Configuration

☑ Logging Enabled

□ Log Detailed Events

☑ Replicate Only With Partners

□ Backup On Termination

□ Migrate On/Off

Starting Version Count (hex): 0

Database Backup Path:

Fig 12.10 WINS Server Configuration

Verify Interval

Specifies the interval after which the WINS server must verify that old names owned by another WINS Server are still valid. The default is dependent on the extinction interval. The minimum allowable value is 24 days.

Pull Parameters

If you want the replication to be triggered when the system is initialized or when a replication-related parameter changes, enable the Initial Replication checkbox and specify a number in the Retry Count list box.

Push Parameters

To inform partners of the database status when the system is initialized, click **Initial Replication** in the Push Parameters group.

If Replicate On Address Change is enabled, push partners are informed whenever an address changes or when a new entry is added.

Click on the **Advanced** button to expand the WINS Server Configuration dialog box and Set any Advanced WINS Server Configuration options.

Logging Enabled Specifies whether to log database changes in the Jet.log file.

Log Detailed Events This item, when enabled, provides a more detailed event record in the Windows NT Event Log. This requires considerable system resources and should be turned off if you are tuning for performance.

Replicate Only With Partners Specifies that replication will be done only with WINS pull or push partners. If this feature is not enabled, you can replicate with this server from any other WINS server, regardless of whether it has explicitly defined the partner or not.

Backup On Termination This automatically backs up the WINS database whenever the WINS Server Service is stopped, except shut down.

Migrate On/Off This enables or disables the treatment of static unique and multihomed records as dynamic whenever they conflict with a new registration or replica. By default, this option is not selected.

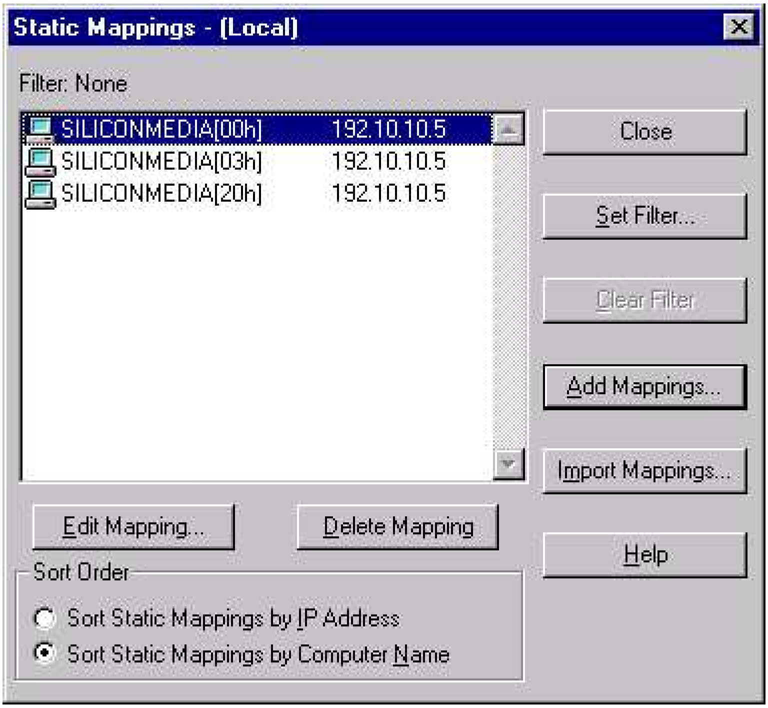
Starting Version Count This feature enables you to reset the starting version number, in hex notation, of WINS database records on this WINS server. Change this value to a higher value if the database becomes corrupted and needs to start fresh. This guarantees that all replication partners to this WINS server will have out-of-date values for the records owned by this server, and will re-replicate the new records.

Database Backup Path Specifies the path to the folder where the backup copies of the database are to be stored.

STATIC MAPPINGS

Normally, records are created in the WINS database when devices dynamically register themselves with the WINS server. However, there might be certain machines you want to ensure are always present in the database. You can ensure this using Static Mapping.

To access the static mappings feature, start WINS Manager, and choose **Mappings ➢ Static Mappings**. (Fig 12.11)


Static Mappings - (Local)

Filter: None

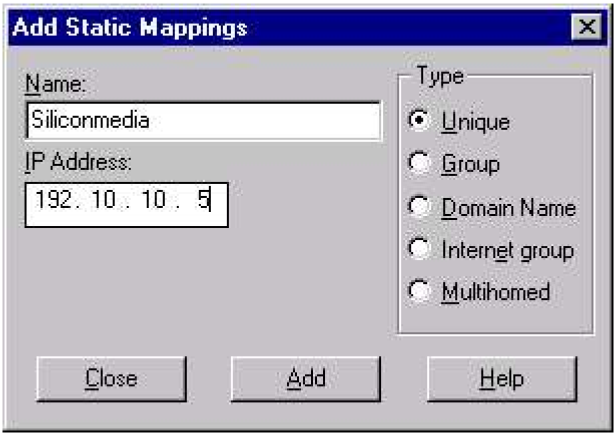
```
SILICONMEDIA[00h]      192.10.10.5
SILICONMEDIA[03h]      192.10.10.5
SILICONMEDIA[20h]      192.10.10.5
```

Sort Order

○ Sort Static Mappings by IP Address
● Sort Static Mappings by Computer Name

Fig 12.11 Static Local mapping

You can add the static mappings manually by clicking the **Add Mappings** button, and the Add Static Mappings dialog box appears.


Add Static Mappings

Name: Siliconmedia

IP Address: 192. 10 . 10 . 5

Type

● Unique
○ Group
○ Domain Name
○ Internet group
○ Multihomed

Fig 12.12 Adding Static mapping

Specify the name & IP address of the Computer, you want to add for static mapping. Select a radio button from the Type section.

Name Allows you to specify the computer name of the system for which you are adding a static mapping.

IP Address Allows you to specify the address for the computer.

Unique Allows you to specify a unique name in the database, with one address per name.

Group Allows you to specify a normal group, where addresses of individual members are not stored. The client broadcasts name packets to normal groups.

Domain Name Allows you to specify a group with NetBIOS names that have 0x1C as the 16th bytes. A domain name group stores up to 25 addresses for members.

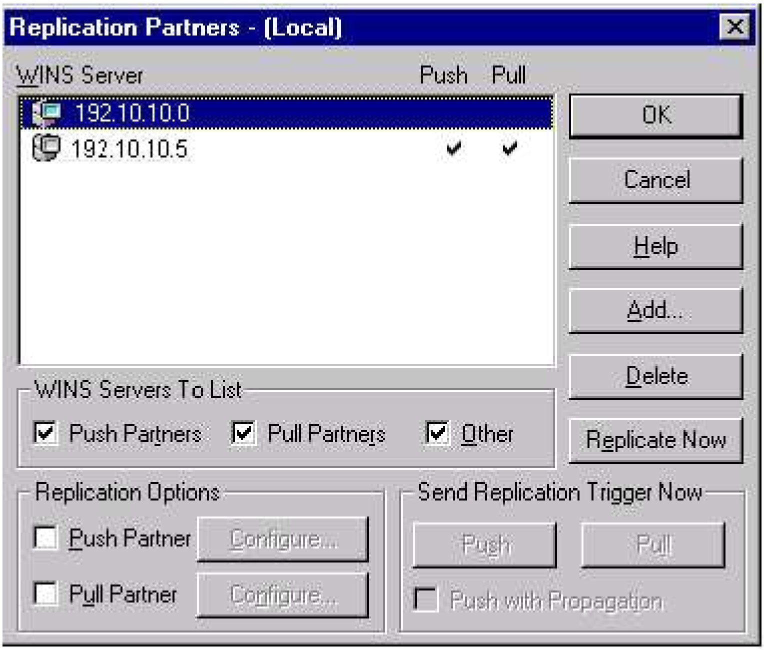
Internet Group Internet groups are user-defined, special groups that store up to 25 addresses for members. Click this option to specify your own group of NetBIOS names and IP addresses.

Multihomed Allows you to specify a unique name that can have more than one address.

REPLICATION

WINS replication is the process by which multiple WINS servers share their database of registered machine, user, and domain information. If you want multiple WINS servers to share the database so that all WINS-capable clients are able to resolve all machine names, then you need to replicate the database. To set the replication settings for the local WINS Server by choosing **Server ➤ Replication Partners**. (Fig 12.13).

- If the partner's IP address with which you want to establish replication is already in the list, select that entry. If not, click **Add** to add a new IP address.
- From the Replication Options frame, mark both the Push Partner and Pull Partner check boxes. This activates the configure buttons for each.
- To configure the push update count, click **Configure**. The Push Partner Properties dialog box appears. Enter a value that represents how many changes can occur in the WINS database before a push trigger is sent.
- To configure the pull frequency, click **Configure**. The Pull Partner Properties dialog box appears. In the Start Time box, enter a time to start the pull replication cycle. Enter the time in hh:mm:ss AM format.
- To force a replication immediately, select the WINS server you want to replicate with from the Replication Partners dialog box, and choose **Replicate Now** to replicate databases between the two partners.



Replication Partners - (Local)

WINS Server	Push	Pull
192.10.10.0		
192.10.10.5	✓	✓

WINS Servers To List

☑ Push Partners ☑ Pull Partners ☑ Other

Replication Options

□ Push Partner

□ Pull Partner

Send Replication Trigger Now

□ Push with Propagation

Fig 12.13 Replicating Partners

Once you install WINS servers in your environment, you need to configure your client machines to take advantage of those servers to perform NetBIOS name resolution. This has already been discussed how to add WINS Server on the client Computer. Refer to Chapter 9 - Using WINS. (Fig 11.14).

WINS MAINTENANCE

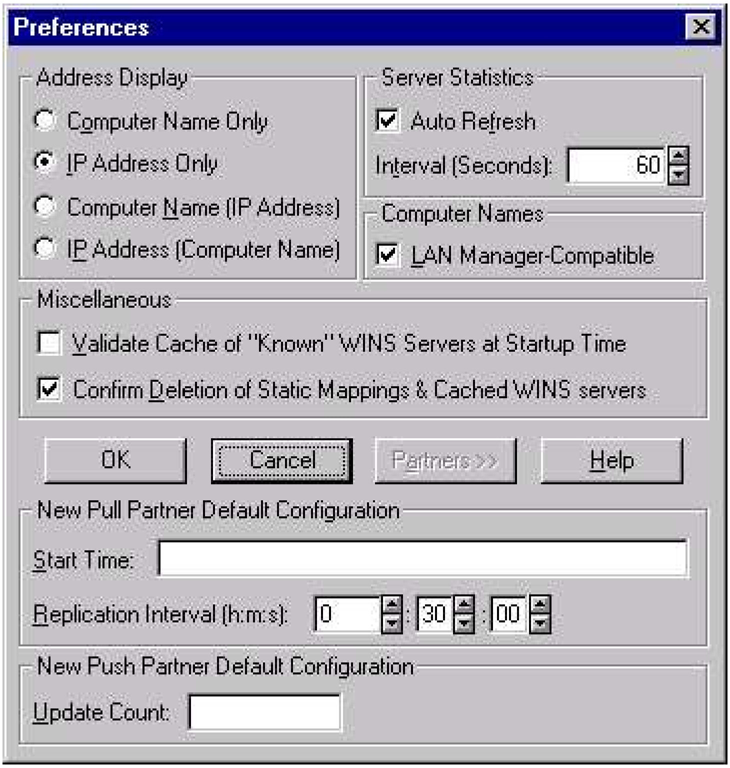
If you have a number of WINS servers spread across a WAN environment and you have to manage each of them remotely, then you can use the WINS Manager. Start WINS Manager and choose **Options ➤ Preferences** to view the configuration screen shown in Fig 12.14.

Address Display

Specifies the method and mechanism to be used for address information displayed throughout WINS Manager.

Computer Name Only	To display only the computer name
IP Address Only	To display only the address
Computer Name(IP Address)	To display the computer name first, with the address to the right of the name

IP Address(Computer Name) To display the address first, with the computer name to the right of the address.



Preferences

Address Display

○ Computer Name Only

● IP Address Only

○ Computer Name (IP Address)

○ IP Address (Computer Name)

Server Statistics

☑ Auto Refresh

Interval (Seconds): 60

Computer Names

☑ LAN Manager-Compatible

Miscellaneous

□ Validate Cache of "Known" WINS Servers at Startup Time

☑ Confirm Deletion of Static Mappings & Cached WINS servers

New Pull Partner Default Configuration

Start Time:

Replication Interval (h:m:s): 0 : 30 : 00

New Push Partner Default Configuration

Update Count:

Fig 12.14 Configuring WINS Manager

Server Statistics

Allows you to specify refresh interval for updating the statistics in WINS Manager window. Specify the number of seconds between automatic screen refreshes in the Interval (Secs) box.

Computer Names

Specifies whether computer names will adhere to the LAN Manager naming convention of 15 characters or to 16-character NetBIOS names used by other sources. If you use other applications that require a 16-byte NetBIOS name, such as Lotus Notes, this option should be disabled.

Miscellaneous

Click **Validate Cache Of Known WINS Servers At Startup Time** to enable WINS Manager to attempts to connect to all WINS Servers you have added. Click **Confirm Deletion of Static Mappings And Cached WINS Servers** to prompt you with a message box whenever you attempt to remove a static mapping or cached WINS Server.

New Pull Partner Default Configuration

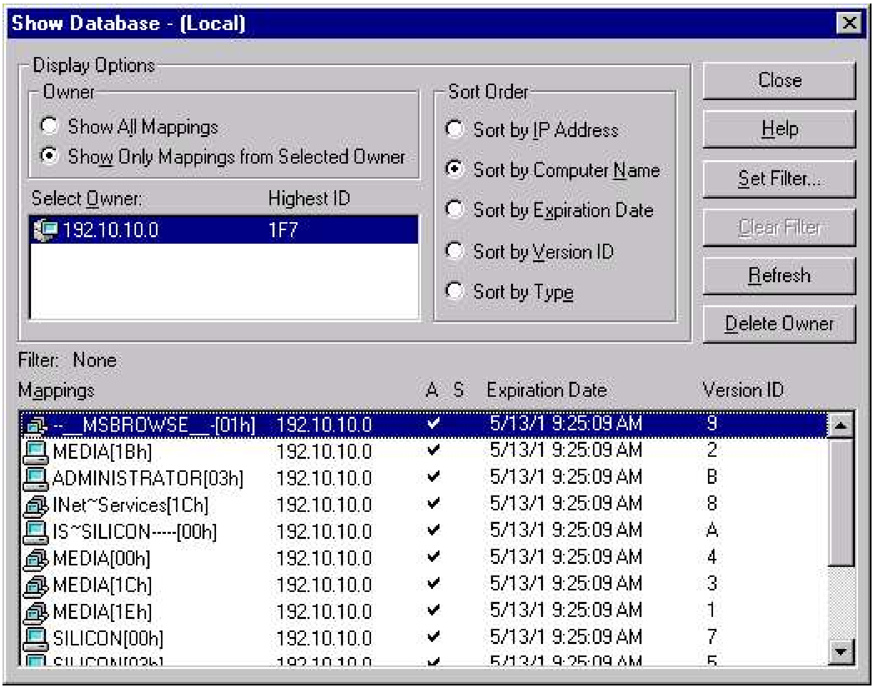
Specifies default replication settings for new pull partners for this WINS server.

New Push Partner Default Configuration

Specifies default value for configuring new push partners for this WINS server. The value specifies the number of changes that must occur in the WINS Server database a replication trigger is sent by this server as a push partner.

WINS DATABASE

The WINS database and associated files are stored on your server's system partition in %systemroot%\system32\wins. You can view the entire WINS database and its constituent owners from WINS Manager by choosing **Mappings ➤ Show Database**.



Display Options

Owner

○ Show All Mappings

● Show Only Mappings from Selected Owner

Sort Order

○ Sort by IP Address

● Sort by Computer Name

○ Sort by Expiration Date

○ Sort by Version ID

○ Sort by Type

Select Owner:	Highest ID
192.10.10.0	1F7

Filter: None

Mappings		A	S	Expiration Date	Version ID
--__MSBROWSE__-[01h]	192.10.10.0	✓		5/13/1 9:25:09 AM	9
MEDIA[1Bh]	192.10.10.0	✓		5/13/1 9:25:09 AM	2
ADMINISTRATOR[03h]	192.10.10.0	✓		5/13/1 9:25:09 AM	B
INet~Services[1Ch]	192.10.10.0	✓		5/13/1 9:25:09 AM	8
IS~SILICON-----[00h]	192.10.10.0	✓		5/13/1 9:25:09 AM	A
MEDIA[00h]	192.10.10.0	✓		5/13/1 9:25:09 AM	4
MEDIA[1Ch]	192.10.10.0	✓		5/13/1 9:25:09 AM	3
MEDIA[1Eh]	192.10.10.0	✓		5/13/1 9:25:09 AM	1
SILICON[00h]	192.10.10.0	✓		5/13/1 9:25:09 AM	7
SILICON[03h]	192.10.10.0	✓		5/13/1 9:25:09 AM	5

Fig 12.15 The WINS Database

The files used by WINS and their functions are described, as follows:

wins.mdb The main WINS database file in Microsoft Access format.

winstmp.mdb A temporary working file used by wins.mdb.

system.mdb A file that holds information about the structure of the WINS database.

j50.log and j50.chk Transaction logs that keep track of all changes made to the WINS database.

The WINS Manager provides backup tools so that you can back up and restore the WINS database. After you specify a backup folder for the database, WINS performs complete database backups every three hours, using the specified folder.

- To back up a WINS database, On the Mappings menu, click **Backup Database**. Type or enter the location for saving the backup files, and then click **OK**.
- To restore a WINS database, On the Mappings menu, click **Restore Database**. Type or enter the location where the backup files are stored, and then click **OK**.

DOMAIN NAME SYSTEN (DNS) SERVER

DNS is to basically used to supply friendly computer names instead of an IP address to locate a resource. The TCP/IP protocol must be installed prior to installing the DNS service. Although WINS also provides similar kind of service of names resolution as DNS, but they have numerous differences, in both the scope of their jobs and their actual implementation. The major differences can be outlined as follows:

- WINS provides dynamic name resolution, DNS is based on static configuration files.
- DNS allows hierarchical naming, whereas WINS, because of its ties to NetBIOS, only provides for a flat filename space.
- WINS provides only name registration and resolution, whereas DNS also provides other services, such as mail exchange information to route the electronic mail properly for the entire domain.

Another advantage of using a DNS server is that it provides additional name resolution capabilities that WINS cannot. It includes e-mail name resolution by supporting the MX record type, which associates an e-mail address with a hostname. And when a DNS server cannot resolve a name locally, it will refer the name query to another DNS server higher up the chain in a effort to resolve it.

TERMINOLOGY

Domain

All or part of a hierarchical name space. For example com is the root or top level domain for all commercial subdomains, edu is top level domain for all education subdomains and so on.

Zone

A specific kind of DNS configuration file. A zone file can include one or more domains, and provides the configuration information for those domains, e.g siliconmedia.org have a zone file siliconmedia.org.dns which have all the information of subdomains of siliconmedia.org.

Host

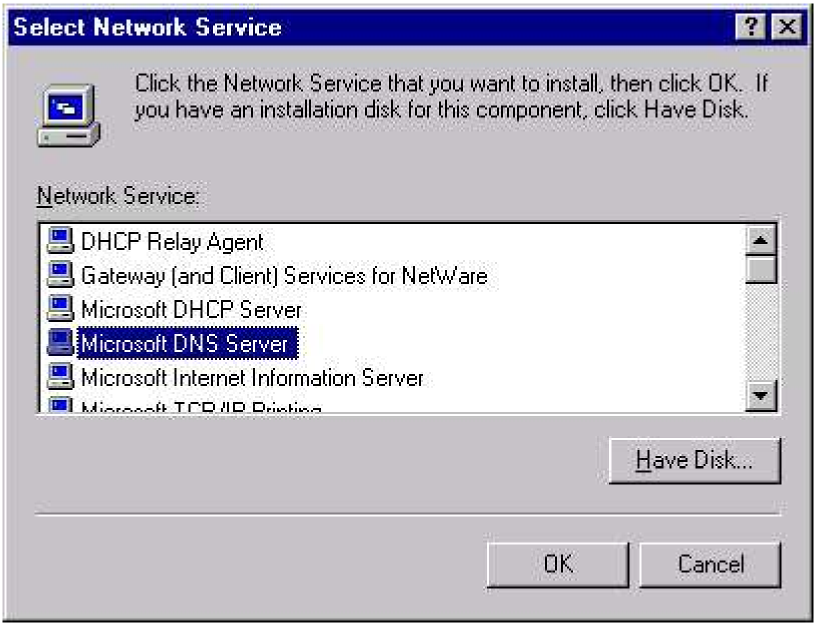
A machine name with a corresponding IP address. When you create zones that represent a domain, you enter host information for machines that reside with that domain, e.g. you add a host name abc with IP address 2011.240.27.121 for siliconmedia.org.

Reverse Lookup

When a client queries DNS, it finds the IP address of a particular host name. There are some applications, which finds the host name for IP address. This is called reversed lookup.

INSTALLING WINS SERVICE

WINS Service can be installed on any Windows NT Server computer. To install Microsoft DNS server on a Windows NT server computer, select **Start** ➢ **Settings** ➢ **Control Panel** and click on the Network icon. In the Network dialog box, click the **Services** tab and click the **Add** button on it. This brings the Select **Network Service** dialog box. (Fig 12.16)


Select Network Service

Click the Network Service that you want to install, then click OK. If you have an installation disk for this component, click Have Disk.

Network Service:

- DHCP Relay Agent
- Gateway (and Client) Services for NetWare
- Microsoft DHCP Server
- Microsoft DNS Server
- Microsoft Internet Information Server
- Microsoft TCP/IP Printing

Fig 12.16 Installing DNS Server

In the Select **Network Service** dialog box, highlight Microsoft DNS Server. Click **OK**.

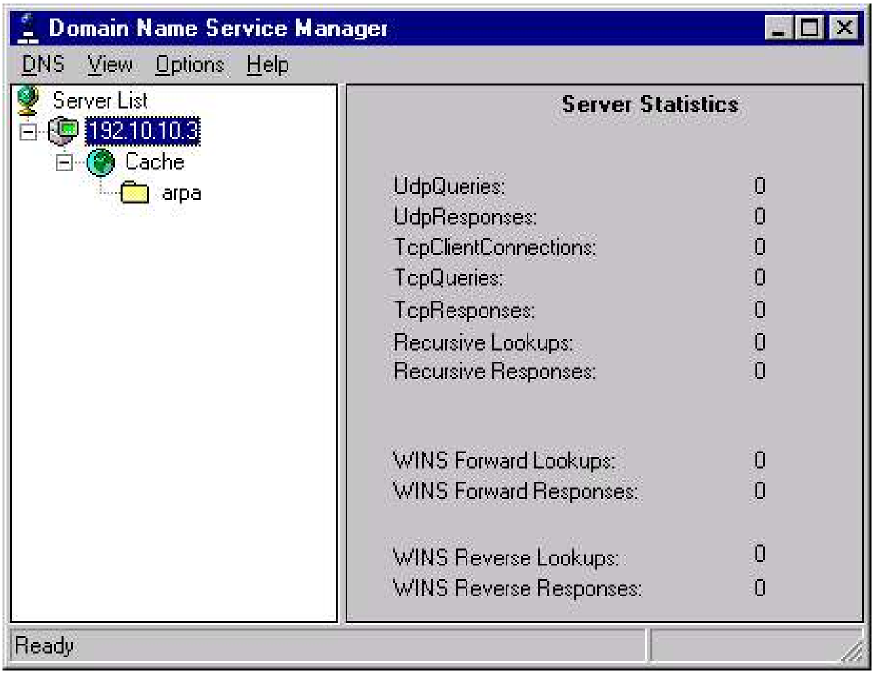
Now Windows NT asks about the location of Windows NT source files. When you specify the location, NT installs TCP/IP in your computer. If you are using a local CD-ROM, indicate the drive letter and path. NT will copy files from the distribution media to the local system directory. Click **OK**. The Network dialog box reappears. Click the **Close** command button. NT will complete the binding process and tell you that you need to restart your computer before your changes can take effect.

DNS MANAGER

Your interface to managing the DNS Service is the DNS Manager. It is installed in the Administrative Tools program group when you install the DNS service. The DNS Manager enables you to work with the DNS zones, the administrative unit in the DNS.

The first and most basic operation you'll want to perform is the creation of a domain. You've installed the DNS service on your server, and you want to build a domain for your company. To start DNS Manager, choose **Start ➤ Programs ➤ Administrative Tools (Common) ➤ DNS Manager**.

From DNS Manager, if no DNS servers are listed, you can add the new server by choosing **DNS ➤ New Server**, and entering the IP address of your DNS server. Then click **OK**. The DNS Manager tool looks like as shown in Fig. 12.17

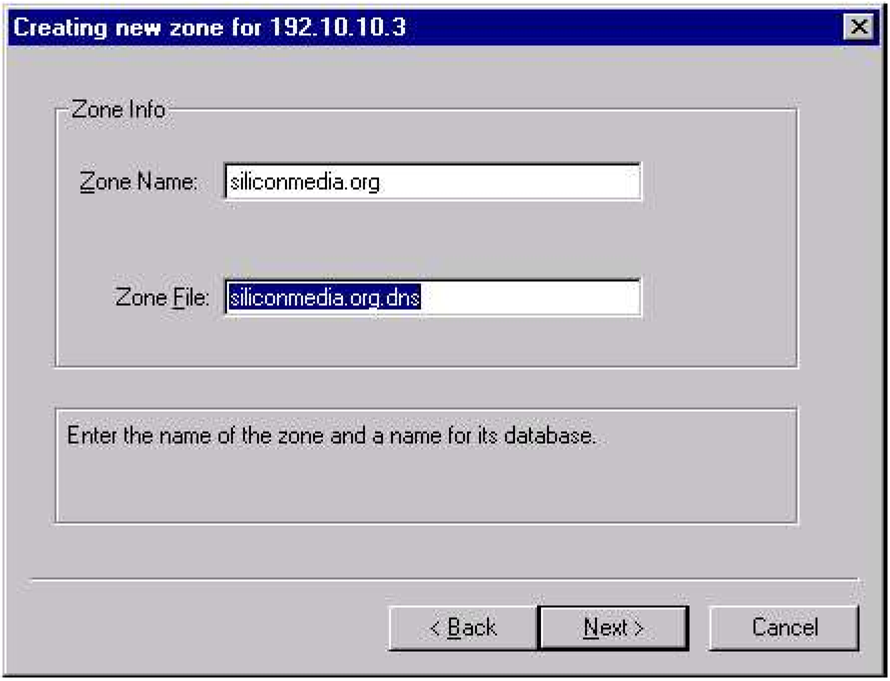


```
Server Statistics

UdpQueries:                  0
UdpResponses:                0
TcpClientConnections:        0
TcpQueries:                  0
TcpResponses:                0
Recursive Lookups:           0
Recursive Responses:         0


WINS Forward Lookups:        0
WINS Forward Responses:      0

WINS Reverse Lookups:        0
WINS Reverse Responses:      0
```

Fig 12.17 Domain Name Service manager

To add a new domain, either choose **DNS ➢ New Zone** or right-click the server and choose **New Zone**. This brings the Creating New Zone dialog box. If this is a zone file for a new domain, it has to be a primary. Select the **Primary** button, and click **Next**.

Enter the zone information. In the Zone Name box, enter the name of the domain you want to create. The zone file name is automatically added for you. (Fig 12.18)


Creating new zone for 192.10.10.3

Zone Info

Zone Name: siliconmedia.org

Zone File: siliconmedia.org.dns

Enter the name of the zone and a name for its database.

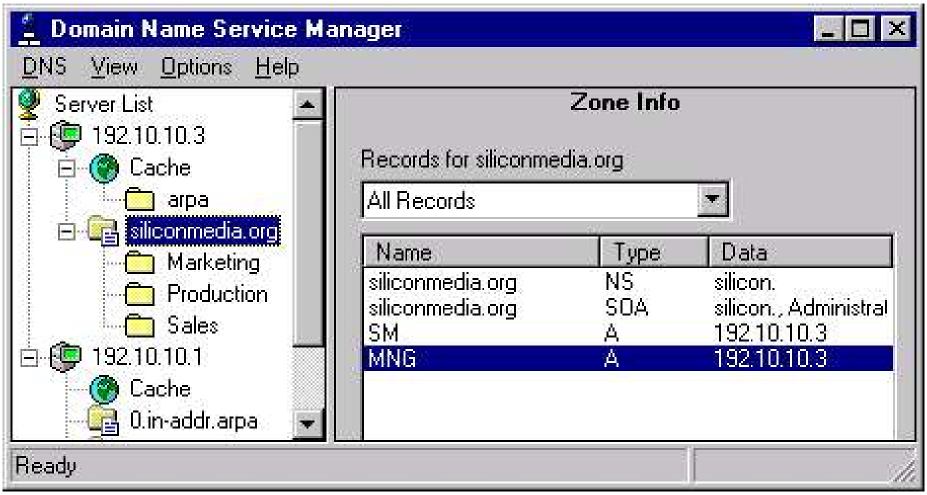
Fig 12.18 Creating New Zone

Click **Finish** to complete the creation of the zone file and the new domain. From DNS Manager, you can see the new domain appear in the list. If you highlight the domain, you can see that three records were created for you in the domain - an NS (Name Server record is used to indicate all the DNS servers for a given domain), an SOA (Start of Authority record indicates that the information in this zone is the definitive source), and an A (Address). (Fig 12.19)

Creating Subdomains

As discussed earlier, the DNS is a hierarchical naming system. This means that you can create nested domains to divide the network into administrative units.

To divide domains into subdomains, repeat the process of creating domain but create new domains while selecting the domain. This will create new subdomains inside the domains.



Records for siliconmedia.org

All Records

Name	Type	Data
siliconmedia.org	NS	silicon.
siliconmedia.org	SOA	silicon., Administral
SM	A	192.10.10.3
MNG	A	192.10.10.3

Fig 12.19 Displaying Zone Information

To view the properties of the domain siliconmedia.org, right-click the domain name , and choose **Properties**. The Zone Properties dialog box appears and shows a number of properties. (Fig 12.20)

General — Gives general information about this zone, including the name of its zone file and whether it is a primary or secondary server.

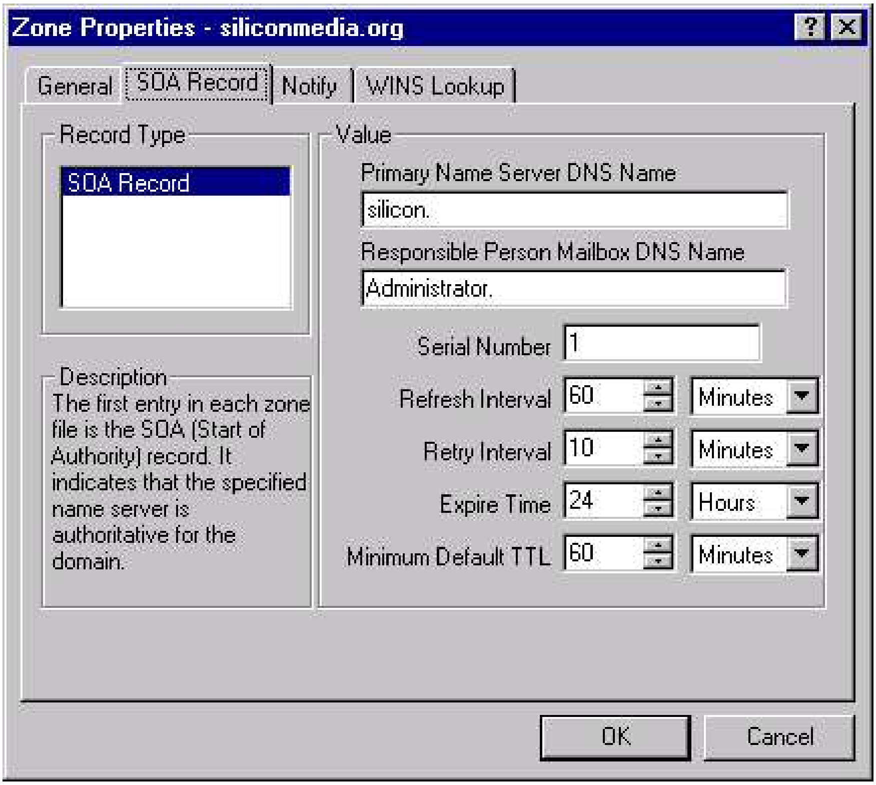
SOA — Gives information related to the SOA record for this zone. The SOA records contain a number of parameters related to the zone.

Notify — Enables you to have a list of secondaries if records change.

WINS Lookup — Enables you to create a WINS RR for this zone. Here, you can specify the IP addresses of multiple WINS servers, and they will automatically be added to your zone file. You can enable WINS resolution on a zone-by-zone basis. When the DNS is asked to resolve a DNS name and it can't find an entry for the name anywhere in the DNS database, the NT DNS service takes the left-most part of the hostname.

ADDING HOST

To add a host, click the domain (zone) or subdomain where you want the host to reside, such as siliconmedia.org, choose **New Host** from the DNS menu. Enter the hostname and IP address, such as media and 192.12.12.1.



Zone Properties - siliconmedia.org

Record Type

SOA Record

Description

The first entry in each zone file is the SOA (Start of Authority) record. It indicates that the specified name server is authoritative for the domain.

Value

Primary Name Server DNS Name: silicon.

Responsible Person Mailbox DNS Name: Administrator.

Serial Number: 1

Refresh Interval: 60 Minutes

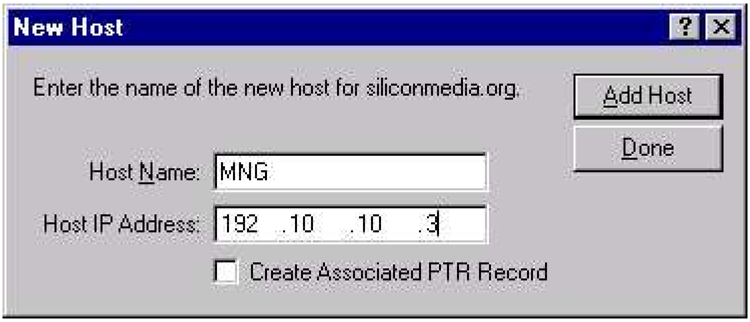
Retry Interval: 10 Minutes

Expire Time: 24 Hours

Minimum Default TTL: 60 Minutes

Fig 12.20 Specifying Zone Properties

To create an associated PTR record, click the **Create Associated PTR Record** button. Click the **Add Host** button, then click the **Done** button. A new record of type A is created for the host.



New Host

Enter the name of the new host for siliconmedia.org.

Host Name: MNG

Host IP Address: 192 .10 .10 .3

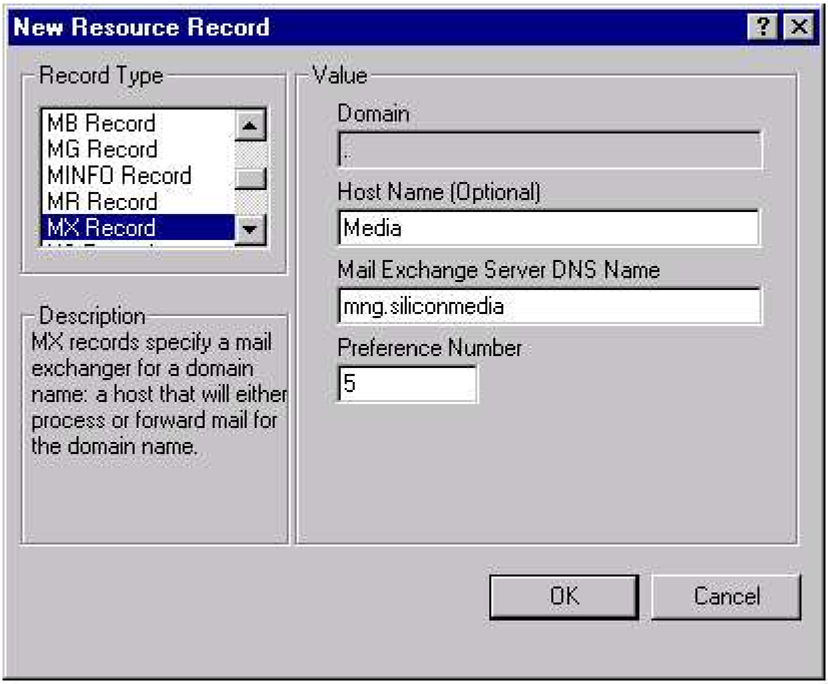
□ Create Associated PTR Record

Fig 12.21 Adding New Host

ADDING RECORDS

Microsoft's DNS Manager makes it simple to create A, PTR(Pointer record is specific to reverse mappings), MX (Mail Exchange record enables you to specify a host name for a given domain that is the mail server responsible for either forwarding or processing SMTP mail) and CNAME (Canonical Name records enable you to create aliases to a given A record) records in a given zone.

To add records to the domain, click the zone or subdomain where you want to create the new record. Choose **DNS ➤ New Record** to bring the New Resource Record dialog box.



Description
MX records specify a mail exchanger for a domain name: a host that will either process or forward mail for the domain name.

Value

Domain: .

Host Name (Optional): Media

Mail Exchange Server DNS Name: mng.siliconmedia

Preference Number: 5

Fig 12.22 Adding New Resource Record

EXERCISE

Fill in the Blanks:

1. DHCP is an extension of ________
2. DHCP relay agent relays DHCP and BOOTP broadcast messages between a _________ server and a client across an ________.
3. Logical grouping of DHCP clients is called ________.
4. Scope Properties are of the types _______ and ________. The ______ scope setting overrides the ________ scope settings.
5. WINS can be configured using __________.
6. _________ is the main WINS database file in ________ format.
7. ________ is a machine name with a corresponding IP address.

Answer the following questions:

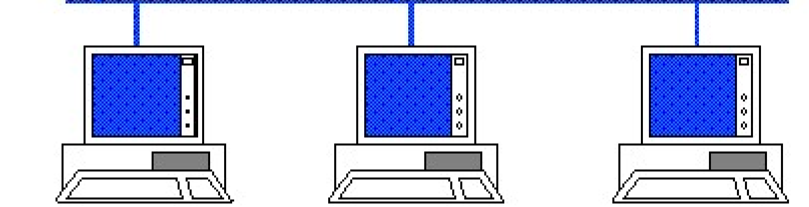
1. Discuss the advantages of using DHCP Server. Also discuss the process of IP assignment using DHCP server.
2. Install the DHCP server from the Server CD or from the main server. Restart the computer after that.
3. Check for the status of the DHCP related services running currently. Create a Scope, with lease duration limited to 4 days. Find out the implications of this kind of Scope.
4. What is the significance of WINS? Discuss the NetBIOS name resolution process.
5. Explain the following terms

   Renewal Interval
   Extinction Timeout
   Pull Parameters
   CNAME
   MX
   Extinction Interval
   Verify Interval
   Push Parameters
   SMTP
   DHCP Offer
6. What is replication?
7. Install WINS on your machine. Configure the DHCP server to automatically assign WINS server Addresses.
8. Differentiate between WINS & DNS.
9. What is DNS zone and how you create DNS host in it?
10. Install the DNS Services. Configure the DNS Service search order.
11. Create a Primary zone for the same giving the name of the zone as “Siliconmedia” and the server name as “New Delhi”. Specify the IP Addresses on your own.

CHAPTER 13

Remote Access Server

REMOTE ACCESS SERVER
DIAL UP NETWORKING
INSTALLING RAS
INSTALLING DIAL-UP NETWORKING
RAS MONITOR



REMOTE ACCESS SERVER

The Remote Access Services of Windows NT enables a user to dial into an NT Server through a telephone connection and establish a basic connection to the network. Using RAS you can connect to your workplace computer and use the same procedures to connect to network drives, printers, and other resources, as if you actually had a network card installed and were hooked up to the network. Of course, if you're using a modem you will notice one major difference that the RAS speed is far slower than a direct connection.

All three major network protocols namely IPX, TCP/IP, and NetBEUI, are supported by RAS. RAS connections can support all three of these protocols on a single connection or any combination of them. Though these are the actual network protocols through which applications communicate, RAS uses two transport protocols to carry these network protocols over an asynchronous modem connection (a connection that is not rigidly controlled by timed packet transmissions): PPP (Point to Point Protocol) and SLIP (Serial Line Interface Protocol). Unlike the network protocols supported by RAS, only one type of transport protocol can be used over a connection.

An NT RAS server does not have to be an isolated server on the network. The PDC (primary domain controller) of the network can serve as the RAS server provided it has the computing strength to do so. The method of connection can also be something other than modems. ISDN, X.25, and full digital lines can also be used to connect to a RAS server, provided that the client side can interface with such lines.

DIAL UP NETWORKING

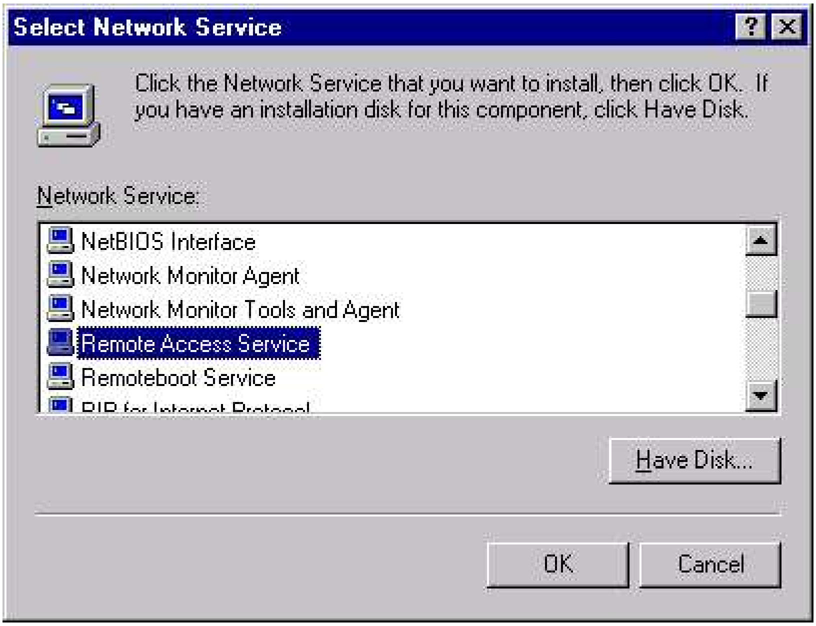
Dial up networking is a component of RAS, which can be used to dial out to other RAS servers. Both NT Server and Workstations can use the Dial-Up Networking components of RAS to dial out to other RAS Servers.

The RAS that was supplied with versions of Windows NT prior to version 4.0 had a single GUI application that you could use to administer both the dial-in and dial-out services. In Windows NT 4.0, an attempt was made to provide the user with an interface that is similar to the one provided with Windows 95. Thus, you can use the Dial-Up Network icon (found in My Computer desktop folder) to establish outgoing RAS communication sessions.

INSTALLING RAS

RAS service is installed via the network applet in Control Panel. To install WINS server on a Windows NT server computer, select **Start ➢ Settings ➢ Control Panel** and click on the Network icon. In the

Network dialog box, click the **Services** tab and Click the **Add** button on it. This brings the Select **Network Service** dialog box. (Fig 13.1)



Select Network Service

Click the Network Service that you want to install, then click OK. If you have an installation disk for this component, click Have Disk.

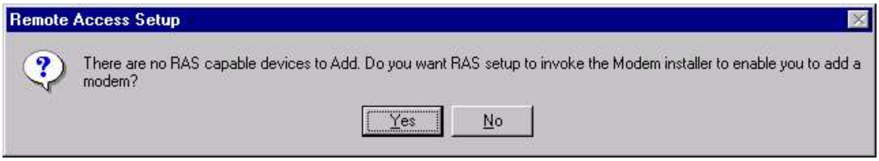
Network Service:

- NetBIOS Interface
- Network Monitor Agent
- Network Monitor Tools and Agent
- Remote Access Service
- Remoteboot Service
- RIP for Internet Protocol

Fig 13.1 Adding Remote Access Service

In the Select **Network Service** dialog box, highlight Windows Internet Name Server. Click **OK**.

Now Windows NT asks about the location of Windows NT source files. When you specify the location, NT installs RAS in your computer. If you are using a local CD-ROM, indicate the drive letter and path. NT will copy files from the distribution media to the local system directory. If you have not installed a modem or other communication port the setup program will prompt you to setup a modem.

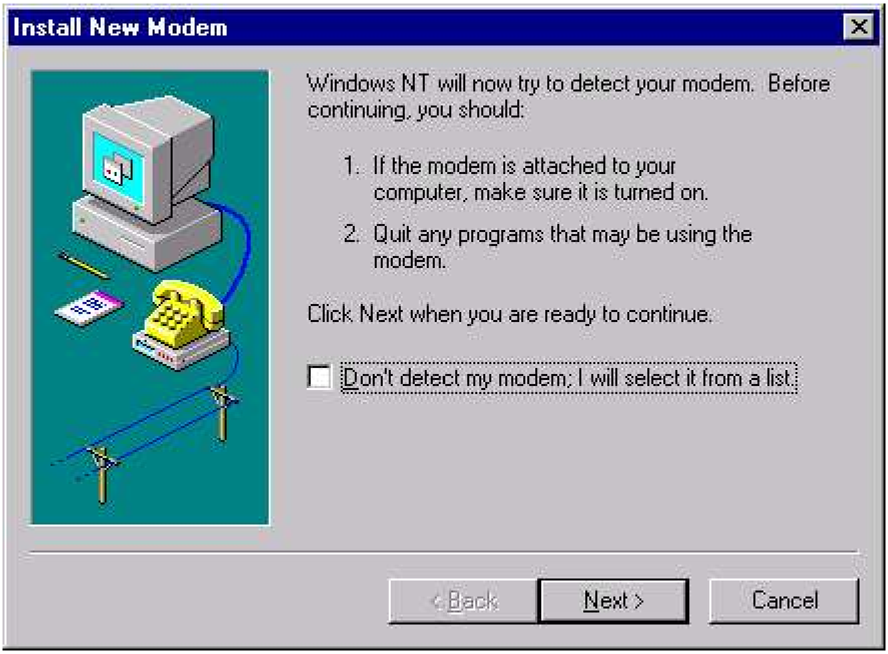


Remote Access Setup

There are no RAS capable devices to Add. Do you want RAS setup to invoke the Modem installer to enable you to add a modem?

Fig 13.2 RAS invoking Modem installer

Click **Yes**. It invokes the modem installation dialog. The Install New Modem Wizard starts automatically to lead you through the steps for installing a modem. Follow the online instructions. If you are installing a second modem, click **Add** to start the Install New Modem Wizard.



Install New Modem

Windows NT will now try to detect your modem. Before continuing, you should:

1. If the modem is attached to your computer, make sure it is turned on.
2. Quit any programs that may be using the modem.

Click Next when you are ready to continue.

□ Don't detect my modem; I will select it from a list.

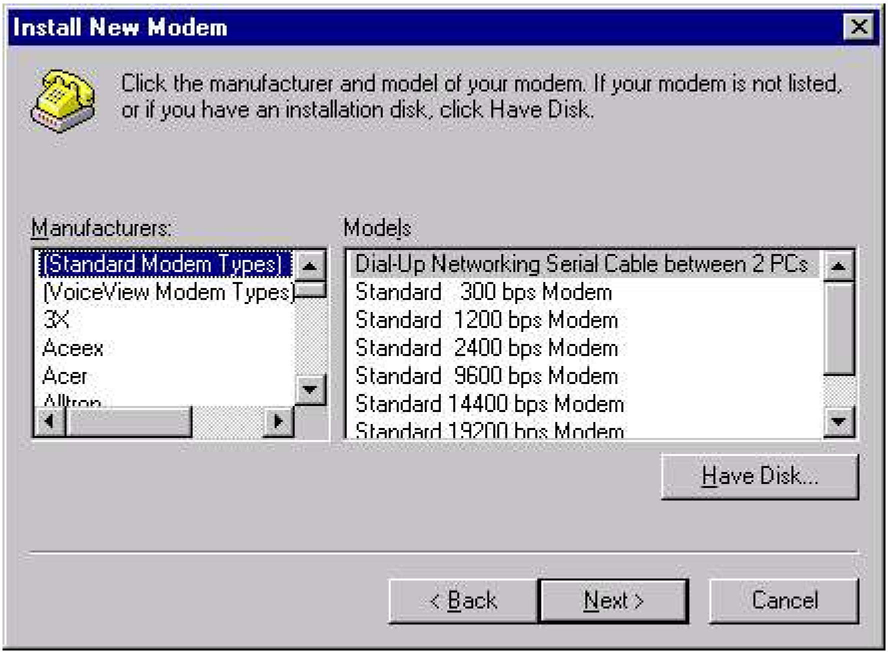
Fig 13.3 Installing New Modem

Windows NT will attempt to detect what type of modem is connected to your system. Windows NT checks the selected COM port, looking for the modem. If Windows NT finds your modem, it displays the Install New Modem Wizard. Click **Next** to select the ports on which to install the modem; when finished, click **Next**. If the dialog box notifies you that your modem has set up successfully, click **Finish** to complete the modem installation.

If Windows NT does not detect your modem, the wizard show you a list of modem manufacturers and modem models.(Fig 13.4) Select one each from Manufacturers (use Standard Modem Types if you don't know the manufacturer) and from Models (use a standard or generic type if you don't know the specific model, or the nearest model if yours isn't listed). Then click **Next** to go to the next step. (Have the disk with the driver software available in case Windows asks for it). Click **Finish**.

Once modem is installed you are returned to the Add RAS Device dialog box (Fig 13.5). Select the modem that you just installed from the RAS Compatible Devices list, and click **OK** to return to the Remote Access Setup dialog box. (Fig 13.6)

Here select **OK** to add the currently selected communication device to RAS.



Install New Modem

Click the manufacturer and model of your modem. If your modem is not listed, or if you have an installation disk, click Have Disk.

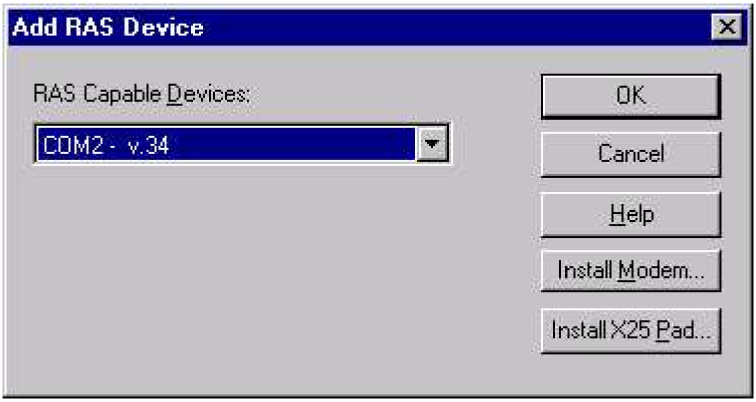
Manufacturers:

- (Standard Modem Types)
- (VoiceView Modem Types)
- 3X
- Aceex
- Acer
- Alltron

Models

- Dial-Up Networking Serial Cable between 2 PCs
- Standard 300 bps Modem
- Standard 1200 bps Modem
- Standard 2400 bps Modem
- Standard 9600 bps Modem
- Standard 14400 bps Modem
- Standard 19200 bps Modem

Fig 13.4 Step - Installing Modem



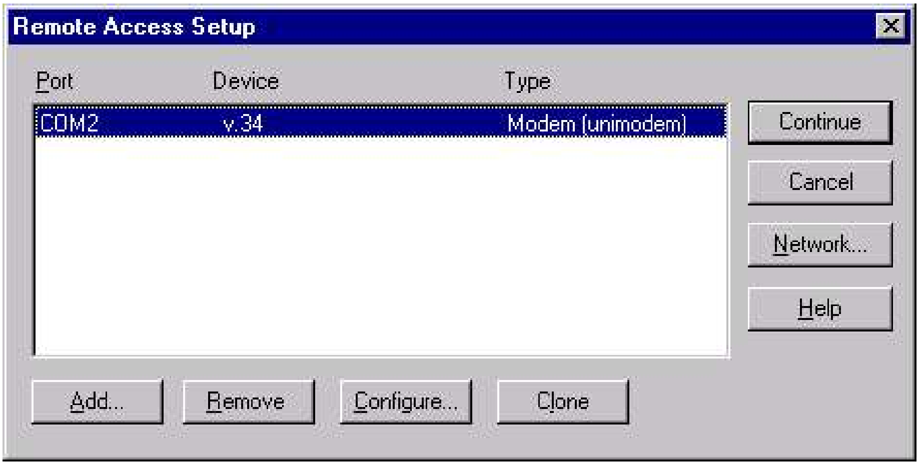
Add RAS Device

RAS Capable Devices: COM2 - v.34

Fig 13.5 Selecting RAS Device

You can also select **Install Modem** button to start the modem installation Wizard, which can also be accessed through the Modems icon in Control Panel.

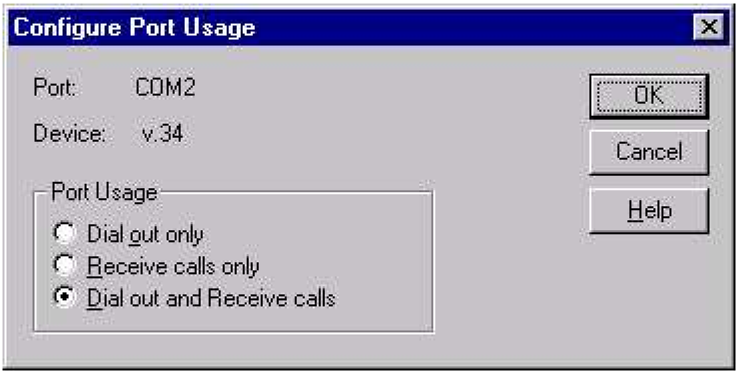
Click on **Install X.25 Pad** button to enable you to add any X.25 Pads that may be attached to the server to RAS. The X.25 Pads must already be installed and configured correctly before they can be added to RAS.



Port	Device	Type
COM2	v.34	Modem (unimodem)

Fig 13.6 Configuring Remote Access Setup

Select the port, and click **Configure** to display the Configure Port Usage dialog box. (Fig 13.7)



Port: COM2

Device: v.34

Port Usage

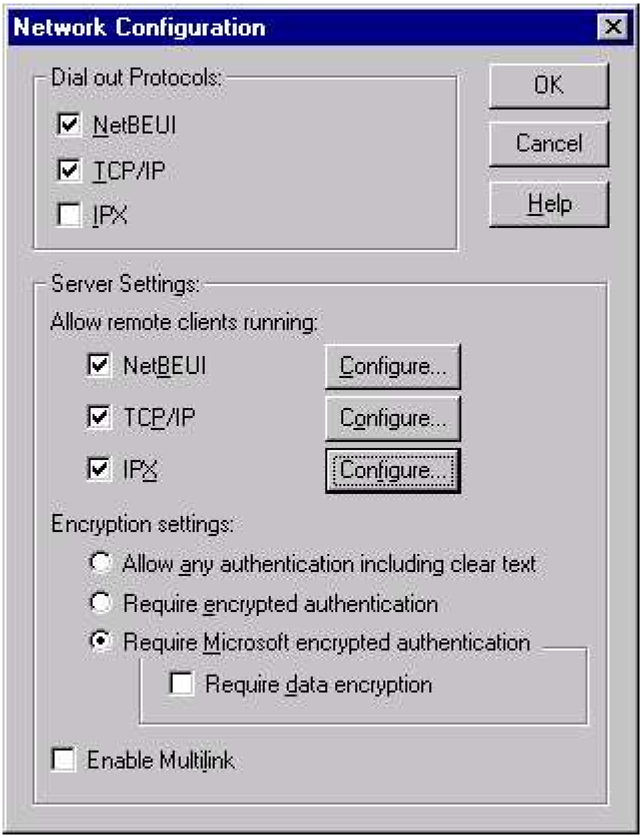
- ○ Dial out only
- ○ Receive calls only
- ● Dial out and Receive calls

Fig 13.7 Configuring Port Usage

You can use this dialog box to configure the modem port for one of the three type of access: Dial out only, Receive calls only, or Dial out and Receive calls.

Click **OK**. The Remote Access Setup dialog box reappears.

Now click **Network** to open the Network Configuration dialog box. The Network Configuration for RAS is pretty straightforward. Select the protocols that can be used for dial-out. Normally, all the protocols you have installed are selected here so that any protocol can be used to dial another network.



Network Configuration

Dial out Protocols:

☑ NetBEUI

☑ TCP/IP

□ IPX

Server Settings:

Allow remote clients running:

☑ NetBEUI Configure...

☑ TCP/IP Configure...

☑ IPX Configure...

Encryption settings:

○ Allow any authentication including clear text

○ Require encrypted authentication

● Require Microsoft encrypted authentication

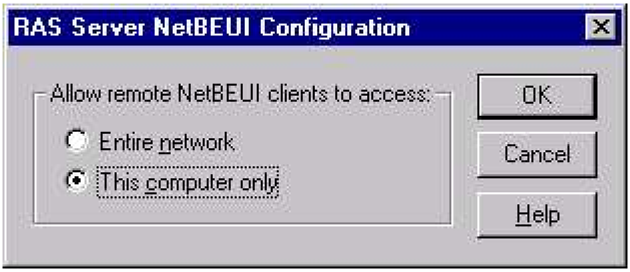
□ Require data encryption

□ Enable Multilink

Fig 13.8 Specifying Network Configuration

The upper areas of this dialog box enable you to indicate the protocols you want to permit during RAS sessions for both outbound and inbound calls. By default, all the protocols you have installed will be checked.

- Select the protocols to be used for dial-in access. If you select NetBEUI for dial-in, click the NetBEUI configuration button to show the RAS Server NetBEUI Configuration dialog box.



RAS Server NetBEUI Configuration

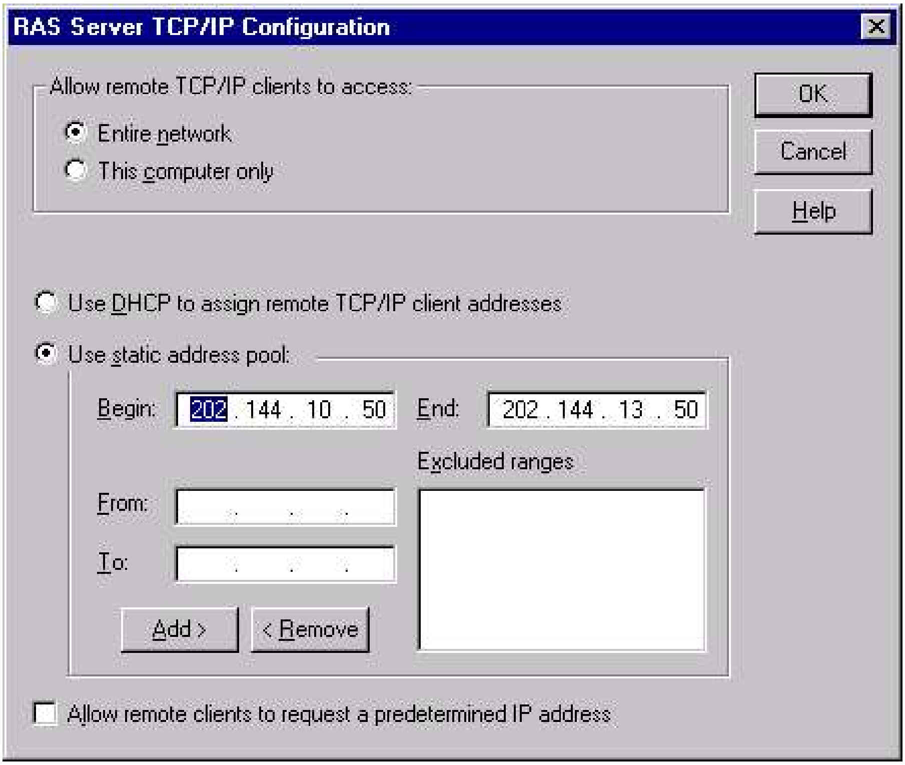
Allow remote NetBEUI clients to access:

○ Entire network

● This computer only

Fig 13.9 Specifying NetBEUI Configuration

- Select the appropriate option i.e. **Entire Network** or **This Computer Only**. When finished, click **OK** to return to the Network Configuration dialog box.
- To configure TCP/IP, click the **TCP/IP configuration** button to show the RAS Server TCP/IP Configuration dialog box. TCP/IP options are little more complex.
  - Select whether the TCP/IP client should be enabled to access the Entire Network or This Computer Only.


RAS Server TCP/IP Configuration

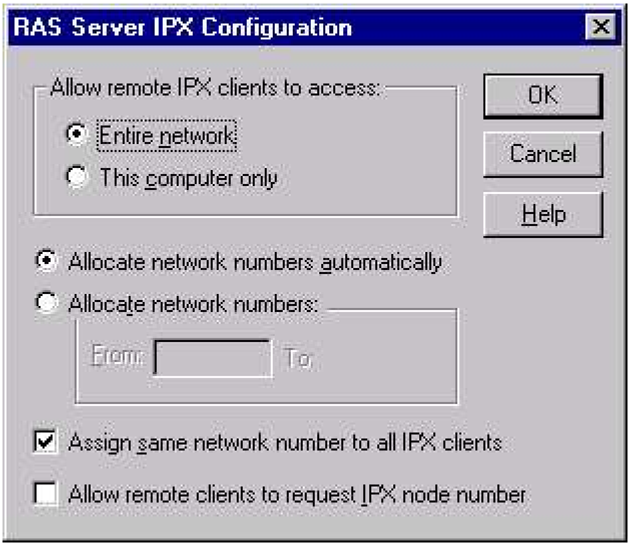
Allow remote TCP/IP clients to access:
● Entire network
○ This computer only

○ Use DHCP to assign remote TCP/IP client addresses
● Use static address pool:
Begin: 202 . 144 . 10 . 50 End: 202 . 144 . 13 . 50
Excluded ranges
From: . . .
To: . . .

☐ Allow remote clients to request a predetermined IP address

Fig 13.10 RAS Server TCP/IP Configuration

  - Determine the method of assigning IP addresses to clients. If you are not using DHCP to assign remote addresses, then give the static pool of addresses for RAS to use.
  - Check Allow Remote Clients to Request a Predetermined IP Address if you want the remote client to be able to keep the IP address it wants to use.
- Click the **IPX configuration** button to show the RAS Server IPX Configuration dialog box.



RAS Server IPX Configuration

Allow remote IPX clients to access:

● Entire network

○ This computer only

● Allocate network numbers automatically

○ Allocate network numbers:

From: To:

☑ Assign same network number to all IPX clients

☐ Allow remote clients to request IPX node number

Fig 13.11 RAS Server IPX Configuration

- Select whether the IPX client should be enabled to access the Entire Network or This Computer Only.
- Determine whether you want Windows NT Server to allocate network numbers for each remote client automatically or from a range of network numbers.

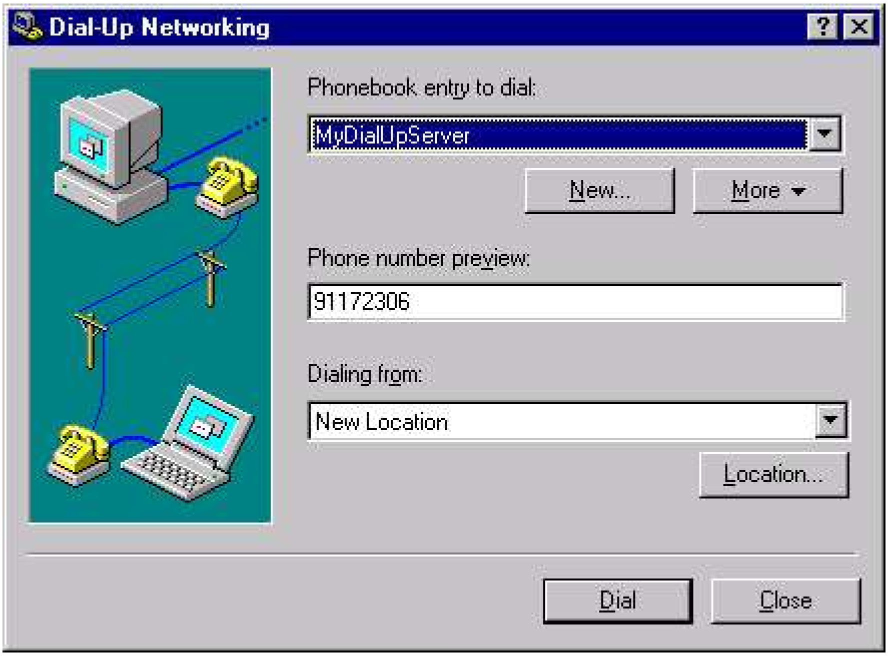
Close the Network Configuration, Remote Access Setup, and Network dialog boxes. NT will complete the binding process and tell you that you need to restart your computer before your changes can take effect.

INSTALLING DIAL-UP NETWORKING

Once you install RAS, you must create a dial-up entry in the workstation phone book to tell the workstation how to connect with the server. To add a new dial-up entry, select **Dial-up Networking** Icon from the My Computer or select **Start ➢ Programs ➢ Accessories➢ Dial-Up Networking**.

If an entry exist, the entry is displayed in the Dial-up Networking dialog box (Fig 13.12). Here you could create new entry, modify the existing entry and change the phone numbers and location.

To create a new entry, click on the **New** button to display New Phone Book Entry Wizard. (Fig 13.13)



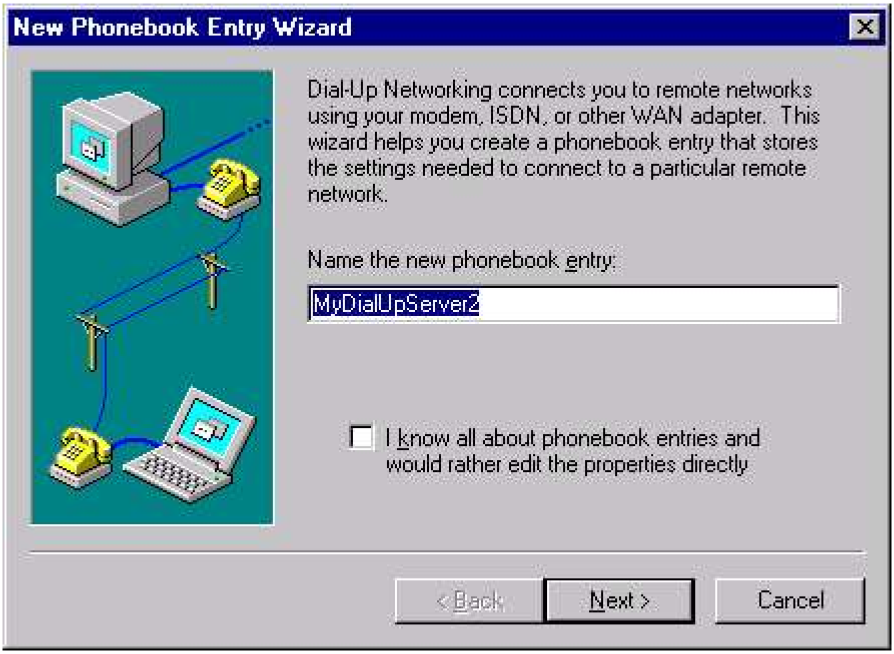
Dial-Up Networking

Phonebook entry to dial: MyDialUpServer

Phone number preview: 91172306

Dialing from: New Location

Fig 13.12 Installing Dial-up Networking



New Phonebook Entry Wizard

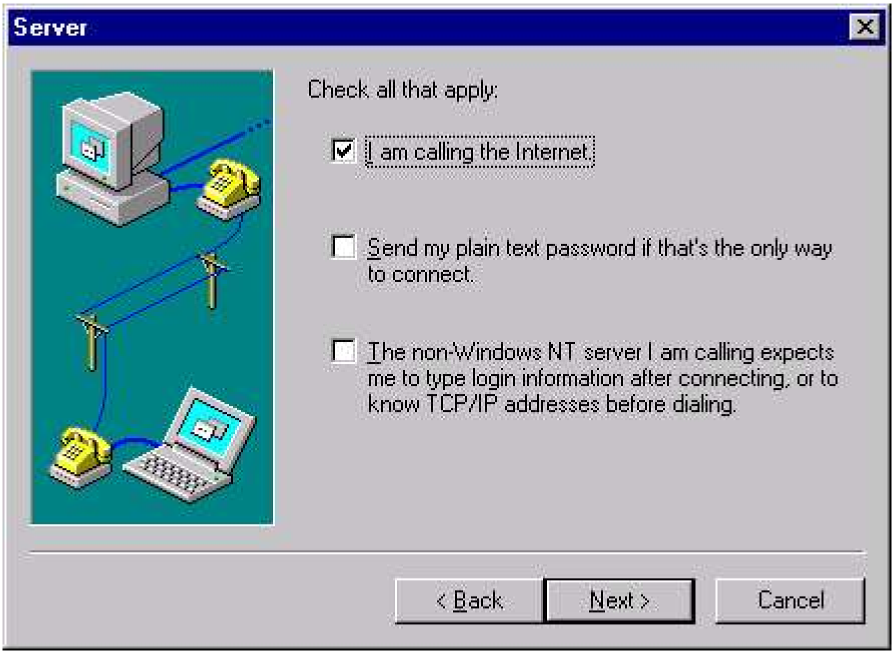
Dial-Up Networking connects you to remote networks using your modem, ISDN, or other WAN adapter. This wizard helps you create a phonebook entry that stores the settings needed to connect to a particular remote network.

Name the new phonebook entry: MyDialUpServer2

□ I know all about phonebook entries and would rather edit the properties directly

Fig 13.13 Step 1 - Creating New Phone Book

Enter the name of the phone book entry and click **Next** to bring up the Server dialog box (Fig 13.14). Select the appropriate options given in Server dialog box and click **Next** to select the modem port. When you click **next**, the Phone number dialog box appears. Give the detailed information about the Location and phone numbers and click **Next** to Finish the dial-up networking configuration.



Server

Check all that apply:

☑ I am calling the Internet.

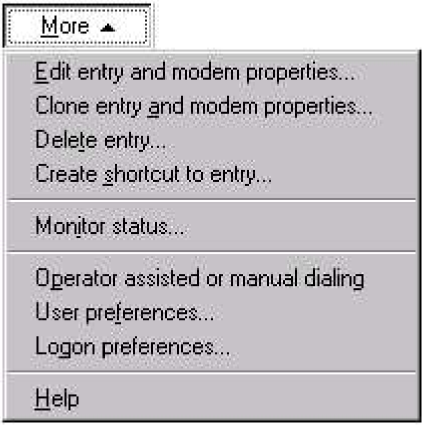
□ Send my plain text password if that's the only way to connect.

□ The non-Windows NT server I am calling expects me to type login information after connecting, or to know TCP/IP addresses before dialing.

Fig 13.14 Step 2 - Specifying Server

Clone Entry and Modem Properties

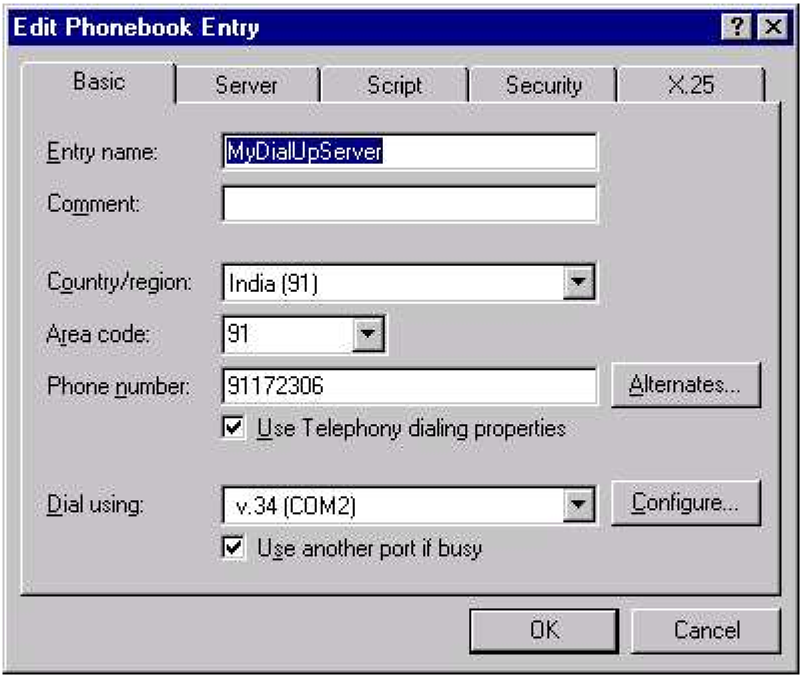
To Edit the Properties of the phone book entry, click on the **More** button in the Dial-up Networking dialog box to display the options (Fig 13.15).



More ▲
Edit entry and modem properties...
Clone entry and modem properties...
Delete entry...
Create shortcut to entry...
Monitor status...
Operator assisted or manual dialing
User preferences...
Logon preferences...
Help

Fig 13.15 Modifying Properties

Select **Edit Entry** and **Modem Properties** to show the Edit Phonebook Entry dialog box (Fig 13.16). The Edit Phonebook Entry dialog box is exactly the same as the New Phonebook Entry dialog box. (This dialog box appears as New Phone Books entry dialog box if you click the option **I know all about phonebook entries....** in the Fig 13.13 and click **Next**).



Entry name: MyDialUpServer

Comment:

Country/region: India (91)

Area code: 91

Phone number: 91172306

☑ Use Telephony dialing properties

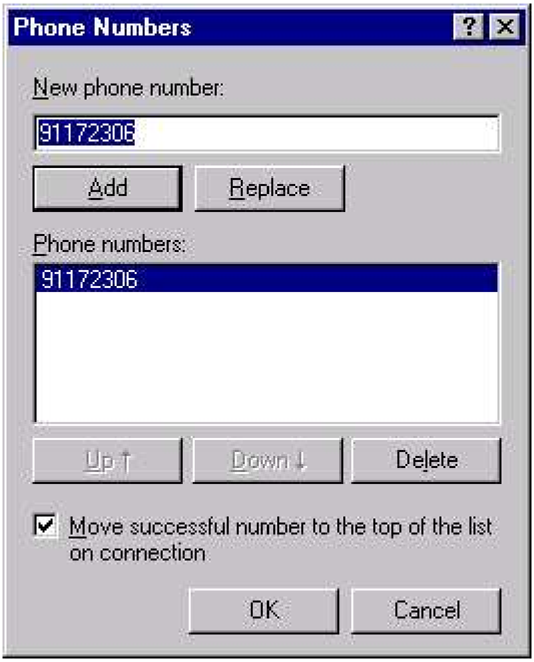
Dial using: v.34 (COM2)

☑ Use another port if busy

Fig 13.16 Editing Phonebook

- The Basic tab contains all the basic entries that are common to every dial-up entry - name, phone number, and modem.

  Click on the **Alternate** button to specify the multiple numbers, you want to dial. (Fig 13.17)
- The server tab controls Windows NT connection to the remote server. It could be PPP, SLIP or Windows NT 3.1.
- If the server doesn't support Windows NT's normal connection method, then it enables you to connect to these servers manually or automatically, even if they can't understand Windows NT's logon sequence.
- The Security tab enables you to choose which form of encryption RAS will use when trying to log into a host.
- If you need to connect Windows NT to an X.25 packet network, you can define in this tab. X.25 packet switching networks provide low-speed—normally 9,600 baud—connections that do not have a distance charge, but rather a charge for each packet sent.



New phone number: 91172306

Phone numbers:
91172306

☑ Move successful number to the top of the list on connection

Fig 13.17 Specifying Alternate numbers

Clone Entry and Modem Properties

This option creates a clone of the current entry then immediately enables you to edit it in any way necessary.

Delete Entry

This option deletes the currently selected entry after confirmation.

Create Shortcut to Entry

if you want to create a shortcut to the entry in the Desktop, Network Neighborhood, or My Briefcase, click here.

Monitor Status

This option starts the RAS monitor discussed in the next section.

Operated Assisted or Manual Dialing

This option lets you manually dial the phone to make the connection to the host.

User Preferences

This option enables you to set user-related RAS preferences.

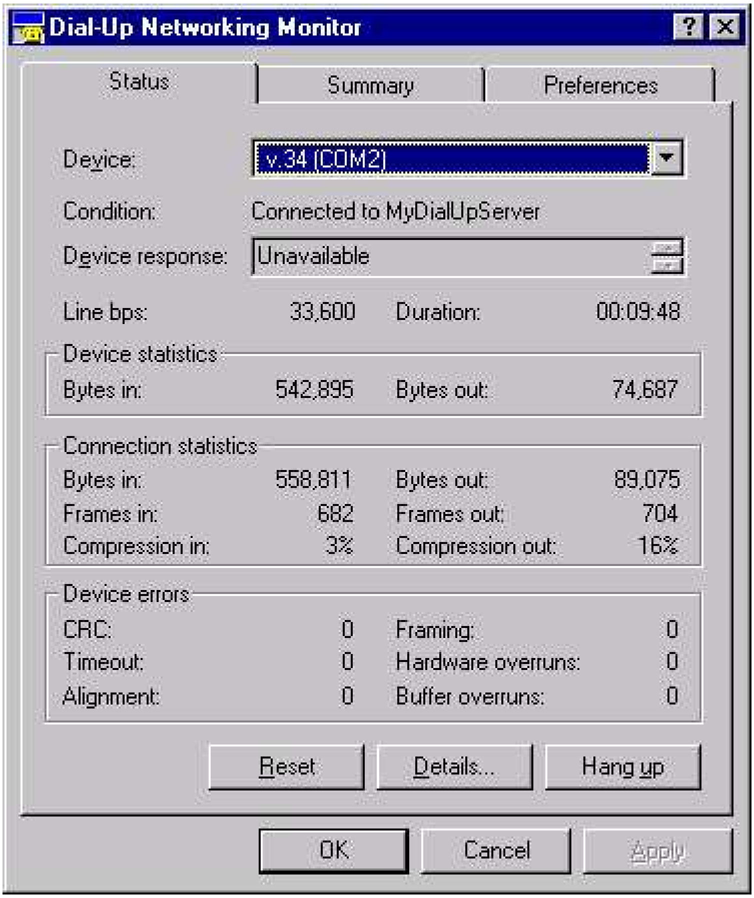
Logon Preferences

This option lets you set preferences when a user selects “**Login Using Dial-Up Networking**” at the **Ctrl+Alt+Del** login prompt NT presents at bootup.

When all the Settings are complete, you can dial using Dial-up Networking icon in My Computer. This brings Dial-up Networking dialog box (Refer Fig 13.12), which enables you to select the specific phone book entry from the drop down menu.

RAS MONITOR

When you are connected to Remote Access Server, a small icon ☎ appears in the system tray. This icon blinks, which indicated that the system is connected to RAS. Also using this icon you can find out the status of your dial-up connection. To bring up the Dial-up Networking Monitor (Fig 13.18), double-click on the icon.



Device: v.34 (COM2)

Condition: Connected to MyDialUpServer

Device response: Unavailable

Line bps: 33,600 Duration: 00:09:48

Device statistics

Bytes in: 542,895 Bytes out: 74,687

Connection statistics

Bytes in: 558,811 Bytes out: 89,075
Frames in: 682 Frames out: 704
Compression in: 3% Compression out: 16%

Device errors

CRC: 0 Framing: 0
Timeout: 0 Hardware overruns: 0
Alignment: 0 Buffer overruns: 0

Fig 13.18 Monitoring RAS

- The first tab displays statistics of RAS ports (Fig 13.18). The drop-down box enables you to browse through all local RAS ports. It also displays connection statistics and Device errors.
- The Summary tab shows you information on multilink sessions.
- The Preferences tab enables you to configure some basic options for RAS : On Connection, On Disconnect, On Transmission, and On Line Error.

EXERCISE

Fil in the Blanks:

1. RAS speed is ________ than direct connection.
2. The two transport protocol used by RAS to carry network protocols over modem are _______ and ________.
3. ______, _______ and _______ could also be used to connect to RAS server.

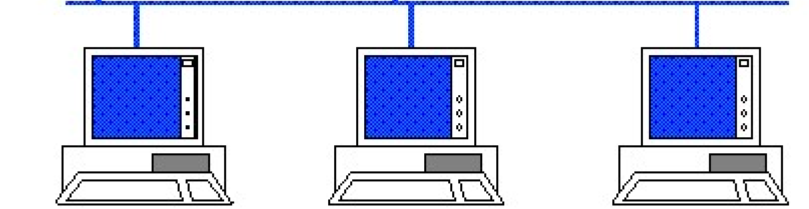
Try the following exercise:

1. Install the Remote Access Service.
2. Configure the modem and the port for both dial out and receive.
3. Install the necessary protocols, which are supported by Remote Access Service.

CHAPTER 14

Administrating Server

ADMINISTRATING SERVER
SERVER MANAGER
BACKING UP
REPAIR DISK UTILITY



ADMINISTRATING SERVER

As a network administrator, you are a person responsible for setting up and managing domain controllers or local computers and their user and group accounts, assigning passwords and permissions, taking backups, maintaining security of the server and troubleshooting all sorts of problems.

In Windows NT Server, you can manage domains with an application called Server Manager, used to view and administer domains, workgroups, and computers.

Also you can ensure that your system is as reliable as possible, by using a number of features that, when used properly, can help increase reliability and guarantee the integrity of your system. These features include Fault-tolerant hard disk driver , Built-in backup support, Integrated UPS support. Here in this chapter we will discuss the last two features. The first feature - Fault tolerance, has already been discussed in the Chapter 4 and UPS configuration has been discussed in Chapter 5.

And in the event of system failure, you can use Repair Disk utility (RDISK.EXE) to recover the server.

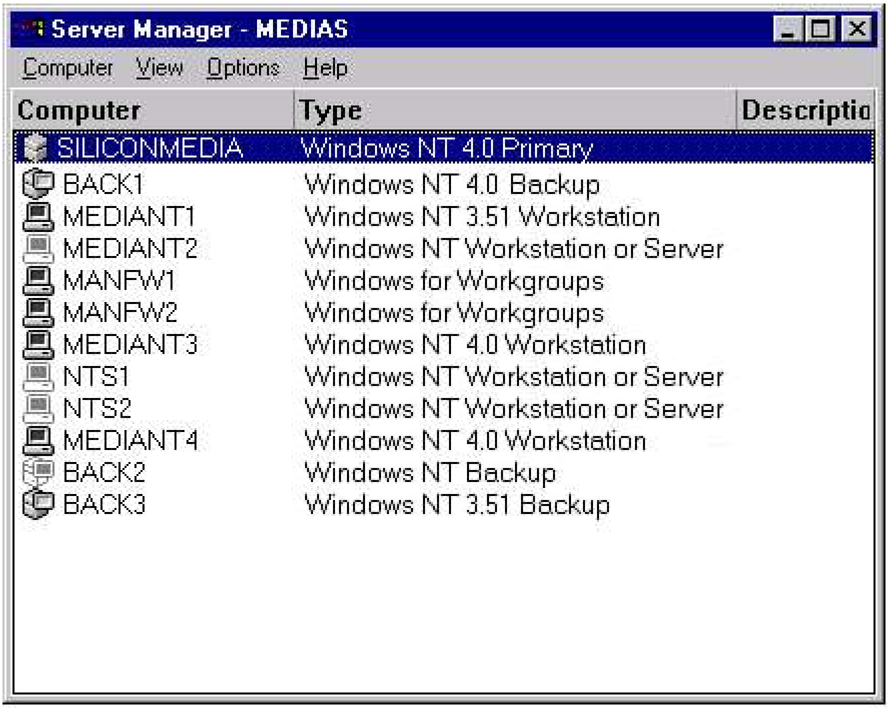
SERVER MANAGER

You can use Server Manager to administer domains and computers. With Server Manager, you can manage your network client (Windows NT only) computer's shared resources and even determine which shared resources your other network clients are using.

You can also use this tool to create computer accounts and to synchronize your backup domain controller's database with your primary domain controller. And you can perform all this from your own server or workstation. The Server Manager is installed in the Administrative Tools program group by default.

To use Server Manager, you must be logged on to a user account that is a member of the Administrators, Domain Admins, or Server Operators group for that domain. Members of the Account Operators group can also use Server Manager, but only for the purpose of adding computers to the domain. Now select **Start ➢ Programs ➢ Administrative Tools (Common) ➢ Server Manager**.

In most cases, when Server Manager is first started it displays your logon domain. The Server Manager title bar shows the domain name, and the body of the Server Manager window lists the computers of that domain. You can select a computer from this list and then use commands on the Computer menu be to manage it. (Fig 14.1)



Computer	Type	Descriptio
SILICONMEDIA	Windows NT 4.0 Primary	
BACK1	Windows NT 4.0 Backup	
MEDIANT1	Windows NT 3.51 Workstation	
MEDIANT2	Windows NT Workstation or Server	
MANFW1	Windows for Workgroups	
MANFW2	Windows for Workgroups	
MEDIANT3	Windows NT 4.0 Workstation	
NTS1	Windows NT Workstation or Server	
NTS2	Windows NT Workstation or Server	
MEDIANT4	Windows NT 4.0 Workstation	
BACK2	Windows NT Backup	
BACK3	Windows NT 3.51 Backup	

Fig 14.1 The Server Manager

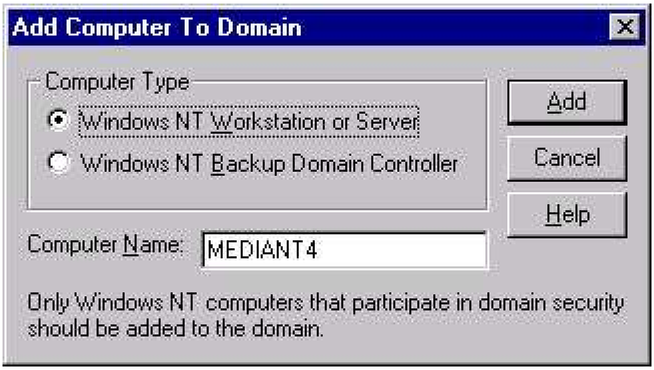
Each entry listed in the Server Manager is associated with an icon that lets you know at a glance what role the computer plays in the domain structure. The three icons are for the primary domain controller- (PDC), the backup domain controller (BDC)- and a workstation .

COMPUTER ACCOUNTS

One of the most important tasks of administrator is to create computer accounts. A computer account must be the same as the computer name of a client computer. A client can be a Windows NT Server backup domain controller (BDC), a Windows NT Server configured as a member server, or a Windows NT Workstation. This component is used to establish the trusted connection between your domain controller and your client. This trusted connection is the beginning of the network authentication process for domain members.

Before a computer running Windows NT can be a domain member and participate in domain security, it must be added to the domain. Computers that are added to a domain are given accounts in the domain directory database.

To add a computer to a domain, start Server Manager and select **Computer ➤ Add to Domain** to bring up the Add Computer dialog box.



Add Computer To Domain

Computer Type

● Windows NT Workstation or Server

○ Windows NT Backup Domain Controller

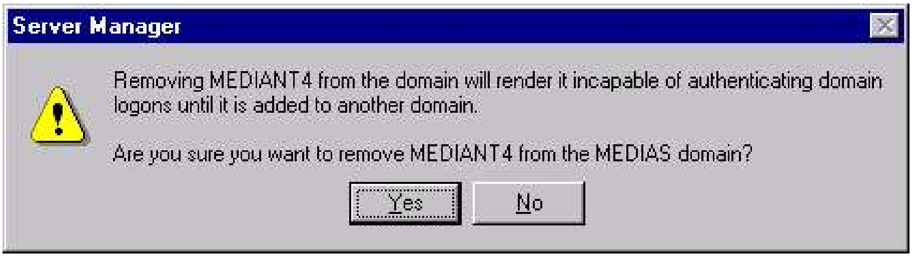
Computer Name: MEDIANT4

Only Windows NT computers that participate in domain security should be added to the domain.

Fig 14.2 Adding Computer to Domain

In the Add Computer to Domain dialog box, select either Windows NT Workstation or Server or Windows NT Primary or Backup and type the computer name in Computer Name, and click **Add**. An account for that computer name is added to the domain directory database.

To delete an account from the Server Manager, simply select the computer account and press Del of select **Computer ➤ Remove** from Domain.



Server Manager

Removing MEDIANT4 from the domain will render it incapable of authenticating domain logons until it is added to another domain.

Are you sure you want to remove MEDIANT4 from the MEDIAS domain?

Fig 14.3 Removing domain from Server Manager

SYNCHRONIZING A BDC

Any changes to master domain database in Primary Domain Controller (PDC) are reflected to Backup Domain Controller (BDC) as defined by a setting in registry. This is called synchronizing a BDC with PDC.

Although Synchronization is usually done automatically by the system, but if the domain directory database on a computer running Windows NT Server becomes unsynchronized or if a backup domain controller is unable to establish network connections due to password failure, you can manually Synchronize the BDC using **Computer ➢ Synchronize with Primary domain controller**. As you Synchronize only the BDC, this command is available only when a backup domain controller is selected.

To synchronize a backup domain controller with the primary domain controller, select the server from the list in the Server Manager window and then select **Computer ➢ Synchronize with Primary Domain Controller**.

To synchronize all the backup domain controllers (BDCs) of the domain, select the primary domain controller on the list in the Server Manager window and then select **Computer ➢ Synchronize Entire Domain**.

PROMOTING BDC

If the PDC fails and goes off line, you cannot make any account modifications as all the user accounts and computer accounts are created on PDC database. In such cases, you can promote a BDC to PDC to make account modification.

If a PDC is available and you promote a server to PDC, the previous primary domain controller is automatically demoted to backup domain-controller status.

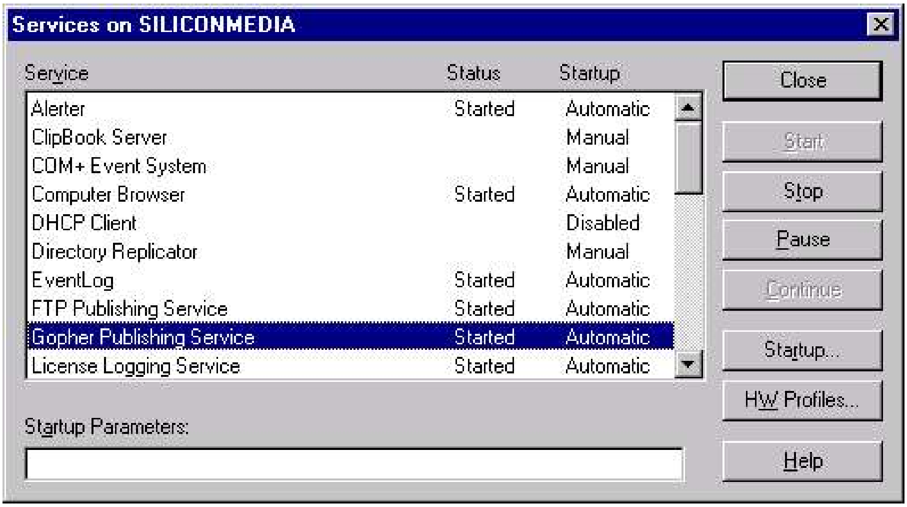
To promote a backup domain controller to primary domain controller, select a backup domain controller from the list of computers in the Server Manager window and select **Computer ➢ Promote To Primary Domain Controller**.

MANAGING SERVICES

Using Server Manager you can manage your local or remote computer resources. With Server Manager, you can stop, start, pause, continue, or configure system services on a remote computer running Windows NT Workstation or NT Server. On the local computer, you can perform the same task by selecting **Control Panel ➢ Services**. But Server Manager lets you perform the same task on the remote computer also.

To start, stop, pause, or continue a service, select a computer in the list in the Server Manager window, and then on the Computer menu click **Services**. In the Services dialog box, select the service you want to Start, Stop, Pause, or Continue. (Fig 14.4)

You can also configure the service on the remote computer. To configure startup for a service, select a computer from the list in the Server Manager window, and then click **Services** on the Computer menu. In the Services dialog box, select the service and click **Startup** to bring up the Service Startup dialog box. (Fig 14.5) In the Service Startup dialog box, click a startup type: Automatic, Manual, or Disabled. To specify the user account the service will use to log on, click **System Account** or **This Account**. If you select **This Account**, click the gray button to the right of the text box and select a user account in the Add User dialog box, and then click **OK**.

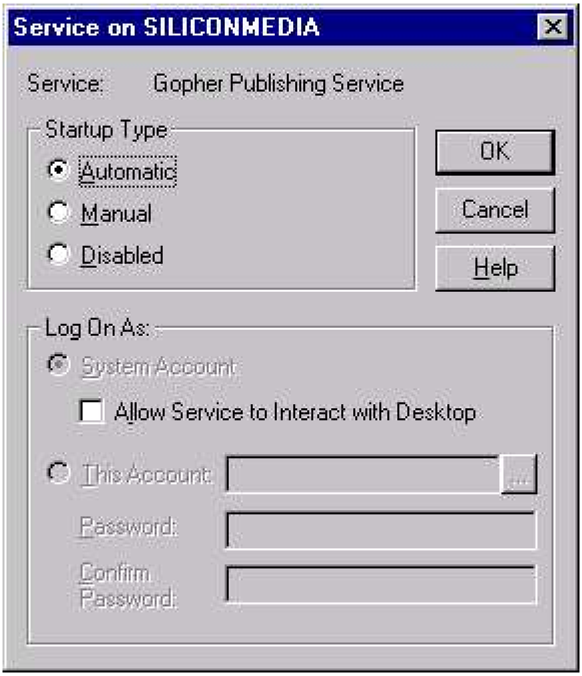


Services on SILICONMEDIA

Service	Status	Startup
Alerter	Started	Automatic
ClipBook Server		Manual
COM+ Event System		Manual
Computer Browser	Started	Automatic
DHCP Client		Disabled
Directory Replicator		Manual
EventLog	Started	Automatic
FTP Publishing Service	Started	Automatic
Gopher Publishing Service	Started	Automatic
License Logging Service	Started	Automatic

Startup Parameters:

Fig 14.4 Services on the Domain



Service on SILICONMEDIA

Service: Gopher Publishing Service

Startup Type
● Automatic
○ Manual
○ Disabled

Log On As:
● System Account
□ Allow Service to Interact with Desktop
○ This Account:
Password:
Confirm Password:

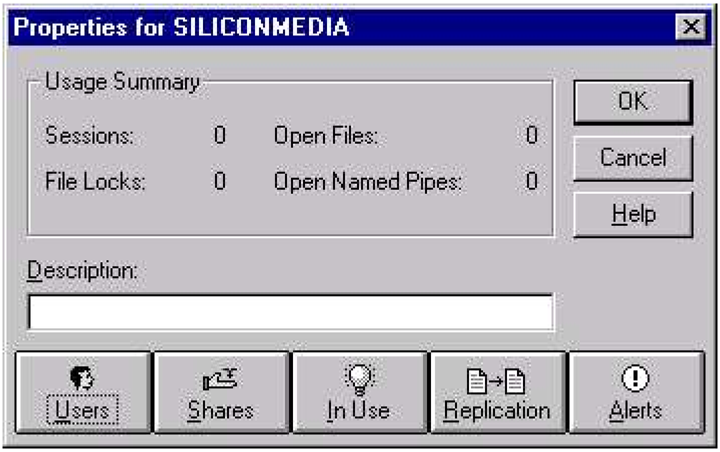
Fig 14.5 Configuring Services

MANAGING SHARES

Similar to services, the shares can also be managed for a remote computer's network using the Server Manager. To share a directory/folder, select a computer from the list, and then click **Shared Directories** on the Computer menu in the Server Manager window. (Refer Chapter 10 - Sharing a Folder)

SERVER PROPERTIES

Server Properties lets you determine the users connected to a computer, the network shares available on a computer, or the shares in use on a remote computer. You can bring up Server property dialog box by double-clicking a specific computer listed in the Server Manager's main window, or selecting a computer in the main window and then choosing Properties from the Computer menu.



Properties for SILICONMEDIA

Usage Summary

Sessions: 0 Open Files: 0

File Locks: 0 Open Named Pipes: 0

Description:

Fig 14.6 Specifying Server Properties

Usage Summary This lists the number of sessions, file locks, open files, and named pipes in use on a computer.

Users Determines which users are connected to the computer and what resources they are using.

Shares Lists the shares by name, number of connections, physical path of the shared directory, the connected users, total connection time, and whether the connection currently is active.

In Use Here the resources that currently are open, such as files, named pipe connections, print jobs, and links to LAN Manager communication devices are listed.

Replicator It lets you copy directories and files from a Windows NT Server to another server or workstation. The service consists of an export component specifying the root directory to export and an import component used to specify directories and files to copy from the export server.

Alerts You can use alerts to notify an administrator of a serious problem that has occurred on a Windows NT computer.

BACKING UP

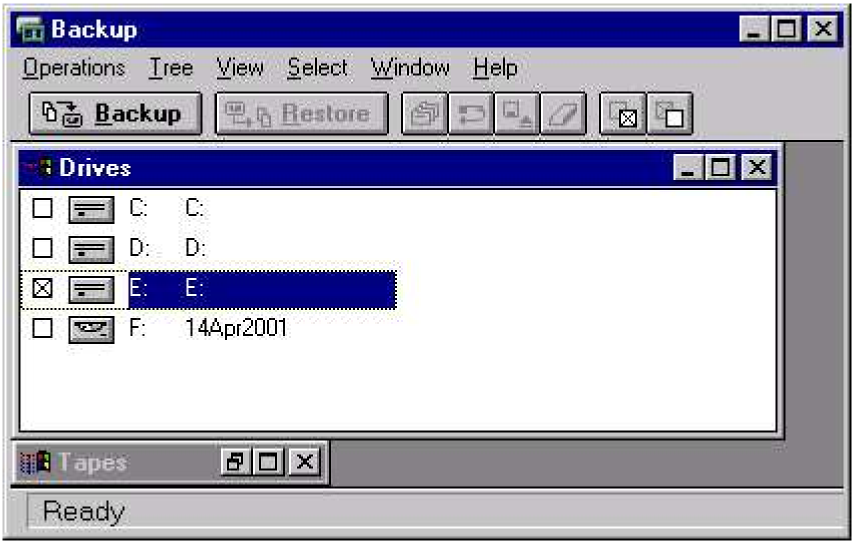
Windows NT Backup is a graphical tool for protecting data from accidental loss or hardware and media failures. The damage caused by either failed hardware or accidental deletion ranges from minor nuisance to major catastrophe. Backup makes it easy for you to use a tape drive to back up and restore your important files on either the Windows NT file system (NTFS) or file allocation table (FAT) file system.

NT Backup is a simple but elegant graphical backup solution that serves the needs of most smaller LANs. You can use the NT Backup to perform following selective backups and restores to protect your data:

- You can back up and restore both local and remote files on NTFS or FAT volumes from your own computer using an attached tape drive.
- You can select files for backing up or restoring by volume, directory, or individual filename, and view detailed file information, such as size or modification date.
- You can select an optional verification pass to ensure reliable backups or restorations.
- You can also perform any of the following common backup operations: Normal, Copy, Incremental, Differential, and Daily Copy.

As the Backup is possible only on the tape drive, you must load the tape drive before taking the backup. To load a tape driver, double-click **Tape Devices** in Control Panel. Click **Detect** and when prompted, click **OK** to install the driver detected by Tape Devices.

Once tape drive is installed, start the Backup by selecting **Start ➢ Programs ➢ Administrative Tools (Common) ➢ Backup**. This brings the Backup Windows (Fig 14.7). This window will show *all* local volumes, including CD-ROMs, as well as any current network connections. Placing a check mark in the box next to any volume, tells NT Backup that you want to backup the entire contents of that volume. Place a check mark next to any volume you want to backup.



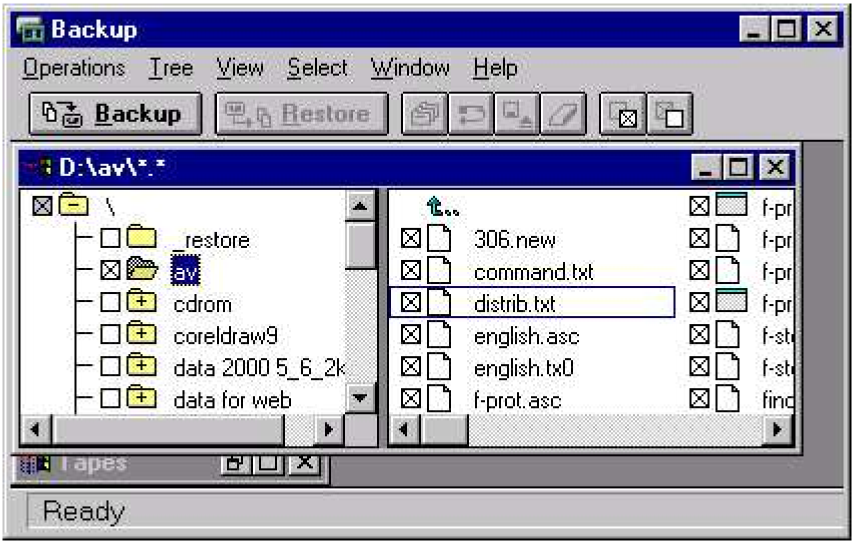
□ C: C:
□ D: D:
☒ E: E:
□ F: 14Apr2001

Fig 14.7 Backing Up data

To back up all the files on a disk, select the drive that you want to back up in the Drives window. On the Select menu, click **Check**. Now select **Operations ➤ Backup** to start backup.

To back up individual files, double-click the drive in which the files are located in the Drives window. Select all the individual files you want to back up, using the any of the following method:

- To select contiguous files, click the first filename, hold down SHIFT, and click the last contiguous filename.



☒ \
□ _restore
☒ av
□ cdrom
□ coreldraw9
□ data 2000 5_6_2k
□ data for web

t..
☒ 306.new
☒ command.txt
☒ distrib.txt
☒ english.asc
☒ english.tx0
☒ f-prot.asc

☒ f-pr
☒ f-pr
☒ f-pr
☒ f-pr
☒ f-st
☒ f-st
☒ finc

Fig 14.8 Selecting Files for Backing up

- To select noncontiguous files, click a filename, hold down CTRL, and click each filename.

On the Select menu, click **Check** to specify the selected files for backing up to display a check mark in the check box beside each selected file. Now select **Operations ➢ Backup** to start backup.

REPAIR DISK UTILITY

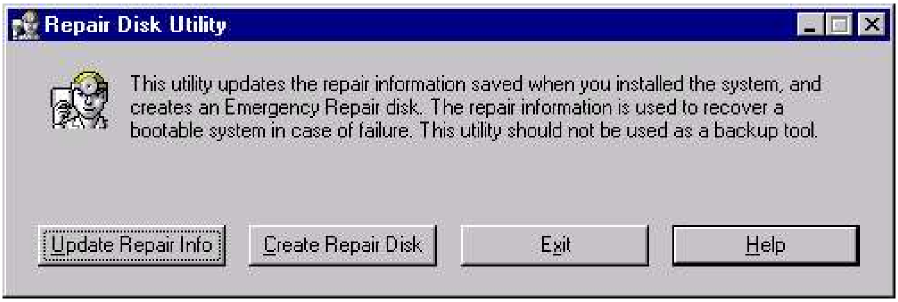
The Repair Disk Utility (RDISK.EXE) is used for creating and updating your system's Emergency Repair Disk (ERD). An icon is not automatically created for this utility when you install Windows NT.

You can then use this disk to restore your computer if files become damaged. You should create and update an ERD every time you make significant changes to your hardware or software setup. This saves you from unexpected problems you could face after making the modifications.

The repair information on your hard disk or your Emergency Repair Disk can be used to reconstruct your Windows NT system files, system configuration, and startup environment variables if they become damaged. The Repair Disk utility should not be used as a backup tool.

The ERD is also useful for restoring the Registry when you make a mistake with the Registry Editor or install some software that prevents your system from functioning properly. If you have a recent copy of the repair disk, you can back out of the changes to your system just by running through the repair process and be up and running in minutes.

You can create a Repair Disk shortcut in the Programs menu. The file associated with Repair disk utility is Rdisk.exe. You can also run this file using the Run command. Using any method, when you run the Repair Disk Utility, you are presented with Repair Disk Utility dialog box.



This utility updates the repair information saved when you installed the system, and creates an Emergency Repair disk. The repair information is used to recover a bootable system in case of failure. This utility should not be used as a backup tool.

Fig 14.9 Running Repair Disk Utility

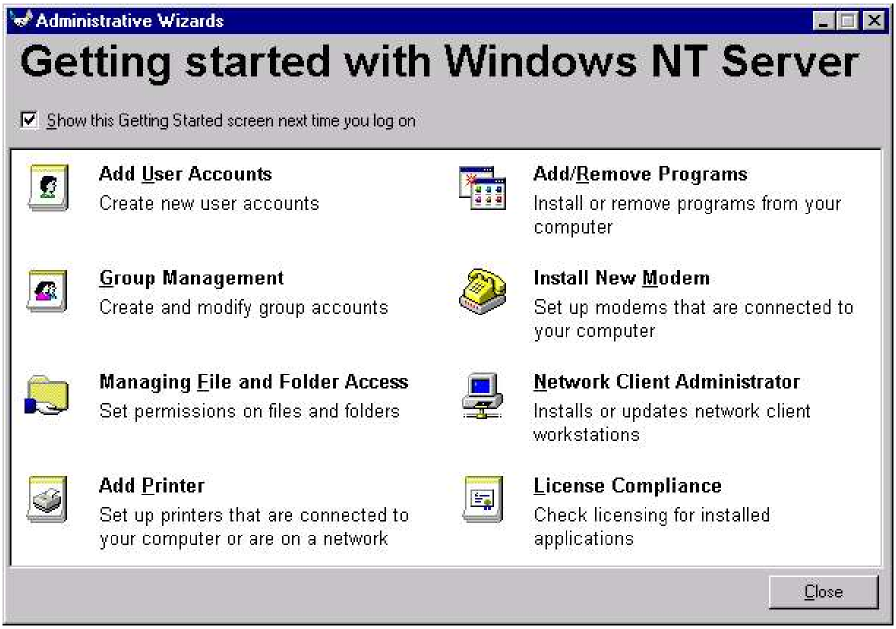
Update Repair Info You can use this option to updates the Registry information contained in the

%SystemRoot%\Repair directory. After you click this button, you are asked whether you want to create a new repair disk. The Repair Disk utility replaces some of the files saved in the \Repair directory with new files that contain updated information about the system configuration.

Create Repair Disk You can use this option to format a high-density floppy disk and copy the same repair information as described for the Update Repair Info button. This repair disk is used by the repair process to restore your Registry.

ADMINISTRATIVE WIZARDS

Windows NT Server 4 now has Administrative wizards to assist you with many network management chores. To access these new wizards, click the **Start** button and select **Programs ➢ Administrative Tools ➢ Administrative Wizards**. These new wizards streamline many commonly used administrative tasks like adding new users, adding and changing group accounts, setting permissions on folders and files, adding network printers, and more. (Fig 14.10) If you are new to Windows NT, the Administrative wizards can prove especially helpful.



Administrative Wizards

Getting started with Windows NT Server

☑ Show this Getting Started screen next time you log on

Add User Accounts
Create new user accounts

Add/Remove Programs
Install or remove programs from your computer

Group Management
Create and modify group accounts

Install New Modem
Set up modems that are connected to your computer

Managing File and Folder Access
Set permissions on files and folders

Network Client Administrator
Installs or updates network client workstations

Add Printer
Set up printers that are connected to your computer or are on a network

License Compliance
Check licensing for installed applications

Close

Fig 14.10 Administrative Wizards

EXERCISE

State True or False:

1. You can use Server Manager to synchronize your backup domain controller's database with your primary domain controller.
2. A BDC can never be promoted to PDC.
3. Synchronization is done automatically and can't be done manually.
4. Backup can only be taken into Tape Drives.
5. You can back up files on NTFS or FAT volumes.
6. Repair Disk utility repairs your hard disk.
7. ERD contains the backup of files and folders also.

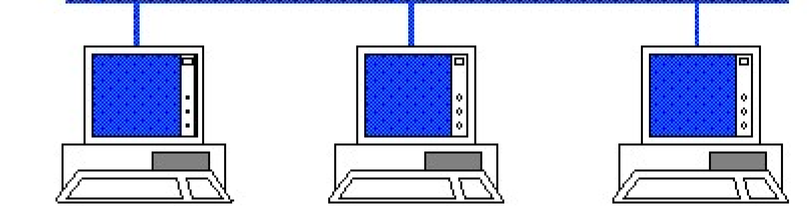
Answer the following:

1. What is the need for having a backup? Differentiate between Full Backup and incremental backup?
2. What is the difference between Data replication and Data Backup?

CHAPTER 15

Internet & NT

INTRODUCTION
GENESIS OF INTERNET
GROWTH OF INTERNET
WHO CONTROLS THE INTERNET?
INTERNET ADDRESSING SCHEME
INTERNET SERVICE PROVIDER (ISP)
INTERNET TOOLS PROVIDED WITH NT SERVER
INTERNET SERVICE MANAGER



INTRODUCTION

The Internet is a worldwide conglomeration of computer networks, including networks located in government offices, universities, businesses, and so on. Thus, the Internet offers access to a vast collection of world knowledge. The Internet is a public place, and it is not owned and operated by any one company.

Most of the networks prevailing at the birth of Internet were of proprietary nature. These networks could/some times not talk to each other till some times back. By adopting a universal standard of communication, Internet has made it possible even for these networks to talk to each other.

The World Wide Web (usually just referred to as “the Web”) is a collection of millions of files stored on thousands of computers (called web servers) all over the world. These files represent text documents, pictures, video, sounds, programs, interactive environments, and just about any other kind of information that has ever been recorded in computer files. It is probably the largest and most diverse collection of information ever assembled.

All Internet transactions take place between one server and at least one client. A client makes a request for information. The server’s job is merely to respond with either the information that was requested or some form of “No”.

GENESIS OF INTERNET

Like computers, Internet owes its birth to the US Defence Department. As the role of information gained importance, a need was felt to develop a network, which could bear the enemy’s attack in the event of war. Moreover it was also thought, even if the network comes under direct attack of enemy, it should not collapse fully, it must work partially and each of its nodes should be able to work independently. With these ideas, US Defence started a network project called ARPANET (Advance Research Project Agency Network). ARPA’s goal was not to create a network the way the present Internet has taken its shape, but to create a data network, which could survive a nuclear attack. It was in 1960’s.

By 1970’s ARPA helped in the development of new protocol for transferring data between the networks. A new standard transmission protocol TCP/IP was evaluated and adopted.

Initially 5 major universities centers were connected in early 70’s. Gradually Defence related research centers and educational institutions from around the world linked to this network forming a global network.

Initially most common application was that of sending simple messages, this evolved into a major application on the Internet namely Electronic Mail (E-mail). E-mail was important enough for many universities who want a connection for just this capability.

The next development was that of search engines such as Archie, Gopher, Veronica etc. which permitted access to information available elsewhere on the net. World Wide Web is the next logical development in the process of making information easily accessible.

GROWTH OF INTERNET

Though the Internet is there for more than 2 decades, the real growth has been in the last three years or so.

The most important factor is that of penetration of Personal Computers (PCs) into all walks of life. The availability of low cost hardware with improved communications and advances in MODEM technology fueled the growth of Internet.

The second important factor was the development of the World Wide Web at CERN. This permitted access to information using a Graphical User Interface (GUI) metaphor and the use of Hyper Text Links to access information across the network without being a computer scientist and without knowing the exact physical location.

Another important factor was the acceptance of the Internet model over the much-touted ISO-OSI model. Acceptance of TCP/IP and HTML standards meant that any computer, which complied with these standards, could connect to the Internet.

As Internet grew so did the quality, quantity and variety of information grow. So much so that Internet today is a repository of every consumable type of information from mating of ants to the design of a functional atom bomb.

WHO CONTROLS THE INTERNET?

Though started in USA, no single agency controls the Internet. Like a phone, we use the network, but we do not own the network. There are groups which may be called Network Operation Centers (NOC) and these NOCs talk to each other through GATEWAYs and make it possible to the residents of one NOC to talk with the resident of other NOCs.

The Internet Society (ISOC) is a voluntary membership organization, which is formed to promote Internet. There is an Internet Architecture Board, a group of invited volunteers who are involved in choosing the standards for Internet. And then there is Internet Engineer Task Force, again another volunteer agency which look after the technical operational details of the Internet.

Internet is there as a network. If someone wants to connect its own network to it, the standards set by Internet have to be followed, otherwise remain out of the domain of Internet.

INTERNET ADDRESSING SCHEME

How to identify a machine on the Internet? Where it is located? How to find a person on the Internet? How to locate resources on the Internet? These few questions will be answered in the following chapters. All these fall under the category of Internet Addressing scheme. Without defining a standardized way, it will be impossible to work on the Internet.

To ensure that our mail reaches into the right hands, we put the address of the receiver very carefully. Similarly, in the Internet to send a mail or to receive information or to download a file, we must know the addresses of the receiver and the host computer. What are these addresses called? How are these addresses allotted? What are different classes of these addresses? These topics will be explained in the subsequent paragraphs.

MACHINE ADDRESSES (IP ADDRESSES)

Internet is a global network of networks of computers, which is available 24 hours a day. The host machine, router and gateway form the entire Internet. A machine, which is supposed to become a part of the Internet, must have an address. Almost all the servers over the network handle the traffic automatically without any human intervention. This has been made possible by designing a concept of IP Addresses. Each host connected onto the Internet must have an IP address.

Further it is also very necessary that each node on the Internet must have a unique IP address so that the IP packet are delivered correctly. The IP Addresses are registered and issued by the following organization

DDN Network Information Centre
14200 Park Meadow Dr., Suite 200
Chantilly, VA 22021
USA.

To identify a machine on the Internet, an arrangement of numbers have been devised so that each machine on the Internet is identified uniquely, globally and in a standardized manner. This arrangement of number allocated to each machine is called Internet Protocol (IP) address of the machine.

The IP address on the Internet is 32 bits long. It consists of 4 - bytes of 8 bits. One portion of these 4 bytes identifies the network address and the second portion identifies the host machine address.

The network portion of the address is allocated by the InterNIC under the authority of Internet Assigned Number Authority to the Internet Service Provider. This is the part of the address of the network available on the Internet. The host portion address is allocated by the Internet Service Provider who provides connection to an individual user. This part identifies the machine on the Internet.

Each section of the IP address contains a number, which may vary from 0 to 255. Further each IP address has been classified into a number of classes which are explained in the following slides.

CLASSES OF IP ADDRESSES

To utilize the resources such as gateways and routers, optimally, the IP addresses have been classified into a number of classes. This is done so that the routers can extract the network portion of the address quickly and efficiently. This was absolutely necessary for a smooth management of the network traffic.

Class A IP Address

Class A of the IP address consists of one byte long address for the network portion and 3 bytes long address for the host portion.

Out of 8-bit address for the network portion, one bit i.e. the highest order bit is always set to zero (o). As a result of this there cannot be more than 127 Class A IP addresses. Again out of these, the address number 127 is kept as reserved / special address. So at the most, there will be 126 Class A addresses i.e. the number will vary from 1 to 126.

The remaining 24 bits are used to identify the host machines. Thus on a single Class A address, we can address upto 255*255*255 i.e. more than 16 millions hosts on each Class A network.

Class B IP Address

A Class B IP address consists of 2-bytes long network address and 2-bytes long host portion address.

In Class A, one highest order bit was set to zero, here two highest order bits are set to 10, which reduces the length of network portion to 14 bits only. With Class B IP address we can configure 64*255 i.e. approximately 16,000 networks. Class B IP address value varies from 128 to 191.

The host portion address on the Class B address is 16-bit long and in this way we can configure 255*255 i.e. approximately 65000 hosts on each Class B network.

Class C IP Address

A Class C IP address consists of 3-bytes long network address and 1-byte long host portion address.

In Class B, two highest order bits were set to 10, here three highest order bits are set to 110, which reduces the length of network portion to 21 bits only. With Class C IP address we can configure 32*255*255 i.e. approximately 2 millions networks. Class C IP Address value varies from 192 to 223.

The host portion address on the Class C address is 8-bit long and in this way we can configure 254 hosts on a single Class C address.

Special/Reserved IP Addresses

Then there are special/reserved addresses, which are kept for research and development and for special purposes.

Network addresses are always kept separately from the addresses allocated to the nodes connected on the network e.g. in Class A network, 58.0.0.0 is the Class A network whereas 58.10.20.30 is the address of a host connected onto a Class A Network.

To facilitate the process of broadcast over the network, the addresses in the host portion is set to all ones e.g. in Class B Network, a packet with a broadcast address 178.48.1.1 will reach every node of the Class B network 178.48.0.0.

Then there are loopback and reserved addresses, which are kept for future and special purposes.

DOMAIN NAME SYSTEM

Domain Names are easier to remember than a combination of 4 level digital numbers of an IP address. Almost all the computers on the Internet have a unique and meaningful domain name. To make such facility available to the users, there are special computers/systems, which are called Domain Name Servers (DNS). The main function of these servers is to lookup the IP Address table and match the domain name given by the user with the digital IP Address and route the traffic accordingly.

A naming convention has been adopted while defining the domain names. It varies from country to country e.g. domain name for VSNL, the Indian Internet Service provider is vsnl.net.in and for National Informatics Centre is nic.in.

The digital IP Address is always read from right to left i.e. the address of lowest entity i.e. of the host machine comes at the rightmost position and then it travels up to the network and to the address of the ISP.

The domain name system is always read from left to right i.e. the name of the person/machine comes first and then it travels up.

INTERNET SERVICE PROVIDER (ISP)

The Internet is a network of computers, one talking to another, then another. In order to “jump on” the Internet, you must do so through a direct connection, or host computer. The Internet Service Provider (ISP) acts as that host computer. It is a company that provides the gateway for you to access the Internet. BSNL (Bharat Sanchar Nigam Limited), Satyamonline, Mantronline are few such ISP. ISPs come in different flavors, offering different levels of service.

INDIRECT ACCESS

You can get indirect access to the Internet through an online service, such as MSN, CompuServe, or America Online. You must be a member of an online service to use its features. In India few ISP have come up with such services such as Mantra Online and Satyam Online

- America Online (AOL) The world’s most popular online service, with a wide range of AOL-only chat rooms.
- CompuServe One of the oldest online services, with an excellent selection of proprietary technical- and business-oriented discussion groups. CompuServe was purchased by America Online, so the two services may merge. CompuServe has access phone numbers in dozens of countries.
- Microsoft Network (MSN) Microsoft’s online service.

DIAL UP CONNECTION

Another way to access the Internet is through a dial up (modem) connection. The ISP acts as your gateway to the Internet, but does not provide any services beyond Internet email and Internet access. With such an ISP, you dial into their server, start your Web browser and surf the net.

You use the Dial-Up Networking program to connect to an Internet PPP, CSLIP, or SLIP account. Dial-Up Networking uses the Windows 98 Dial-Up Adapter to communicate with Internet accounts by using TCP/IP, the communication protocol used on the Internet.

PERSISTENT CONNECTION

The third way to connect to the Internet is through a persistent connection, such as your company’s network. In such a case, the network is connected directly to the Internet through the network’s gateway. You don’t dial into your connection; instead, after you log on to the network you are able to access the Internet.

PROTOCOLS

The following protocols have become popular and accepted on the Internet. This acceptance means that if you use them, you can get at information. If you do not want to use them, you can get your information somewhere else. The most common standard services follow:

World Wide Web (WWW)

This is the hot topic in most information systems magazines. It is a graphical interface that enables you to read and download information people have stored in the standard WWW format.

FTP Server

This is a way for Administrators to export part of their disk storage system for access by users over the Internet.

Internet mail

This is a standard set of protocols that allow dissimilar electronic mail systems (Microsoft Mail and Lotus cc:Mail, for example) to exchange information over the Internet.

Newsgroups

If you have a complaint about life in general or need technical data on installing an Adaptec 2940 SCSI controller on an NT 4.0 Server, there are newsgroups for you. Imagine a huge number of bulletin boards that you can use to discuss various topics, ranging from technology to philosophy. The Internet newsgroups are a way of relaying topic-based questions and comments around the planet.

Telnet server

For those who need to allow remote users to log into their server to run programs, the Telnet service facilitates this across the Internet.

Gopher/WAIS

Servers that use gopher protocol present their content in the form of submenus. You pick items from menus, each menu item can be another menu, a program or a file of some kind. The special strength of gopher is that any menu item may actually be on a gopher server that is different from the one that presented the menu to you in the first place.

Domain Name Server

It is much easier to remember standard character patterns such as siliconmedia.org rather than number associated with it. Realizing this, the Internet community has developed domain name servers, which store synchronized lists of official text addresses (assigned by the various Internet governing bodies) along with their official Internet addresses (290.240.27.121, for example). You get to enter the easy-to-remember text name, and the name server translates this into the address needed to communicate with the remote machine.

INTERNET TOOLS PROVIDED WITH NT SERVER

Windows NT server provides products and services that support Internet technology. Two of the major services that support Internet technology are **Internet Explorer** and the **Internet Information Server** (IIS).

The Internet Explorer is a client Web browser and IIS is a Web server. The two services are complimentary to each other. For example, any user who would like to visit any web site would be the client. The user would use the Internet Explore to access the Internet and contact the server of that particular Web site. The destination server would be running IIS.

IIS is made up of three service protocols. They are HyperText Transfer Protocol (HTTP), File Transfer Protocol (FTP) and the Gopher service. The main aim of these services protocols is to provide publishing services for Intranet or the Internet. Once the IIS has been installed, anyone with an Internet connection can access Web pages or interactive applications that have been published.

You can also install Gopher only if you have a number of users who would rely on this service. You can probably install the ODBC access only if you plan to derive portions of the Web page content from the database or store some of the responses from your Internet server in your database.

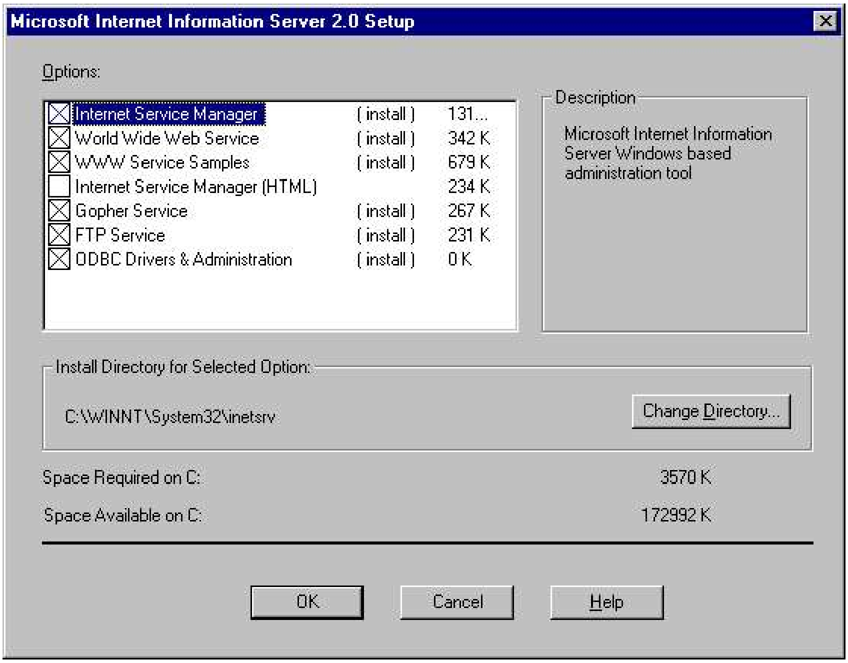
INSTALLING INTERNET INFORMATION SERVER

While Windows NT is being installed, the IIS can be installed along with it. However, if it hasn't been installed at that time, you can install it later also.

To install IIS, select **Control Panel ➢ Network ➢ Services tab**. Or click on the right mouse button on the Network Neighborhood icon on the desktop and select **Properties**. Select **Add** from the window. The user will be presented with a list of services. Select the **Internet Information Server**.

Now Windows NT asks about the location of Windows NT source files. When you specify the location, NT installs IIS in your computer. If you are using a local CD-ROM, indicate the drive letter and path.

A menu listing of all the service components appears (15.1). Click on the adjacent box to select each of the desired components. Select the Help only if the online help is needed. Then click on **OK** to continue. A list of directories is presented for the locations of World Wide Web, FTP and Gopher Publishing. This is the path of the root directory for each service being installed. It is upto the user whether he wants to



Microsoft Internet Information Server 2.0 Setup

Options:

☒ Internet Service Manager (install) 131...
☒ World Wide Web Service (install) 342 K
☒ WWW Service Samples (install) 679 K
□ Internet Service Manager (HTML) 234 K
☒ Gopher Service (install) 267 K
☒ FTP Service (install) 231 K
☒ ODBC Drivers & Administration (install) 0 K

Description: Microsoft Internet Information Server Windows based administration tool

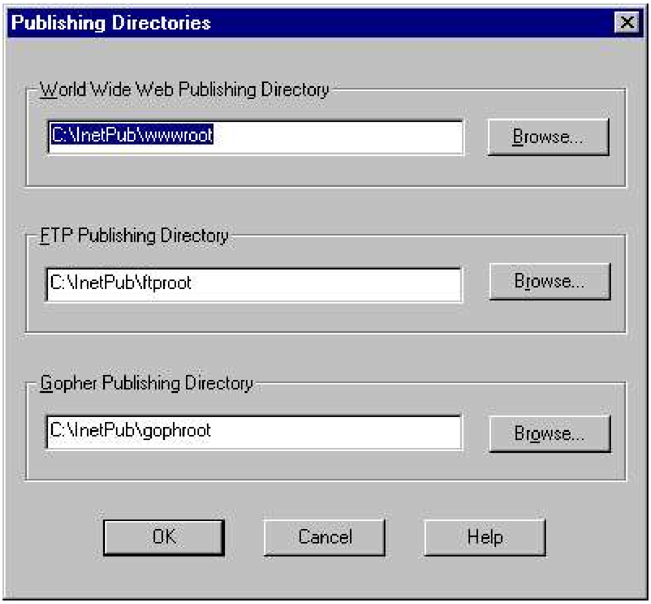
Install Directory for Selected Option: C:\WINNT\System32\inetsrv

Space Required on C: 3570 K

Space Available on C: 172992 K

Fig 15.1

accept the default directory and place all the files to be published in that directory. When you click **OK**, another dialog box appears asking the user if it is **OK** to create directories. Choose **Yes**.



Publishing Directories

World Wide Web Publishing Directory: C:\InetPub\wwwroot

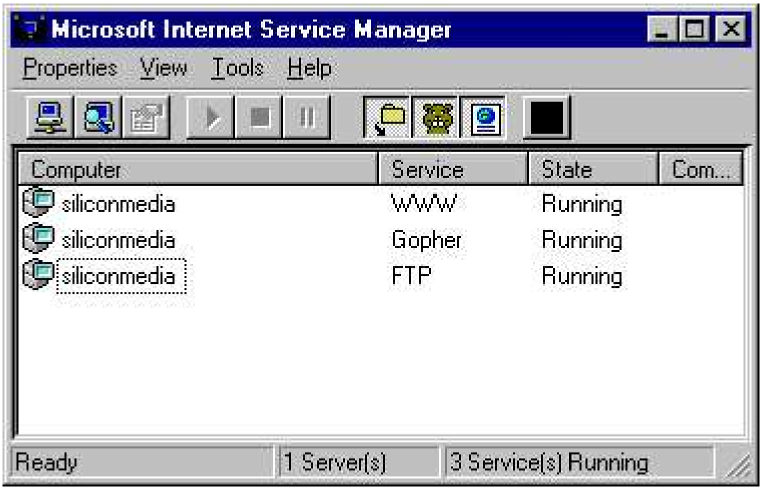
FTP Publishing Directory: C:\InetPub\ftproot

Gopher Publishing Directory: C:\InetPub\gophroot

Fig 15.2

INTERNET SERVICE MANAGER

The Internet Service Manager is the utility that customizes and administers the Internet services. You can start Internet Service Manager by selecting **Start ➢ Programs ➢ Microsoft Internet Server (Common) ➢ Internet Service Manager**. The Internet services you installed are displayed, along with their status (normally, Running). To take action on any of these services, you need to highlight the service you want and then click one of the items on the button bar or right-click the mouse and select **properties** to change the settings for the service.



Computer	Service	State	Com...
siliconmedia	WWW	Running	
siliconmedia	Gopher	Running	
siliconmedia	FTP	Running	

Fig 15.3

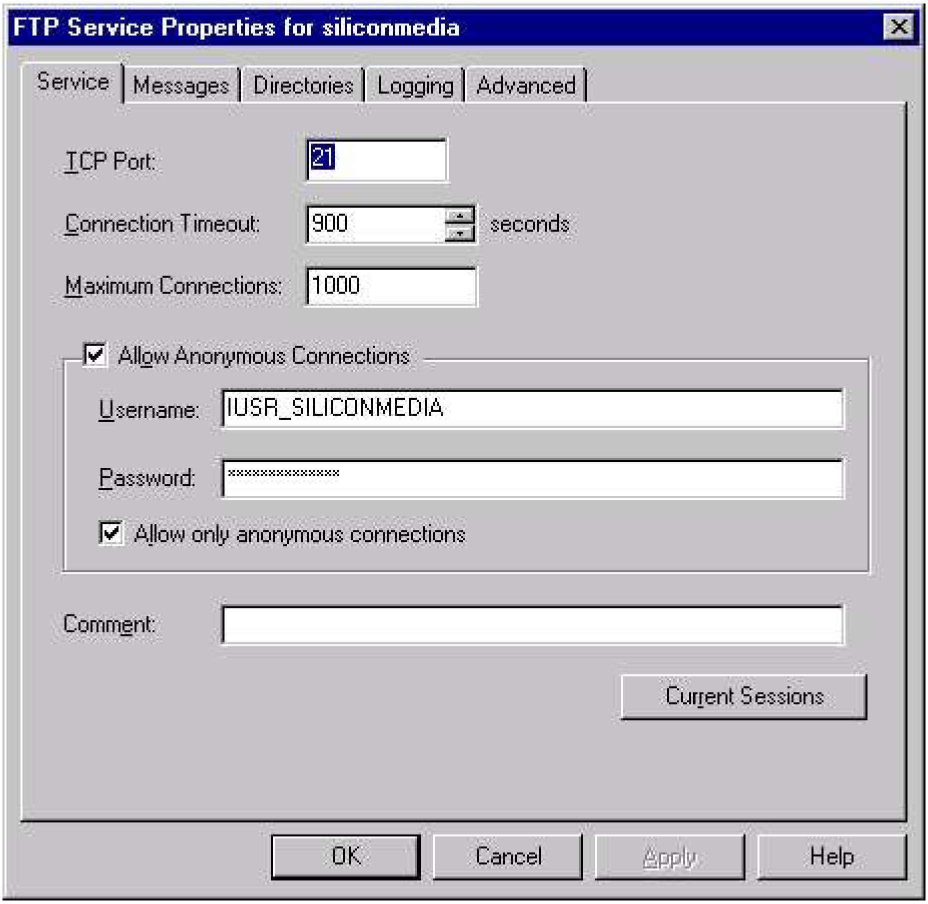
Internet Information Server is designed to assist in the configuration and enhancement of the internetwork services. By using a single program to manage Internet services, it is possible to manage all the Internet services running on any Windows NT system in a streamlined manner. Depending on the number of systems running the internetwork services it is possible to choose from the three control view formats found in the Internet Services Manager menu.

MANAGING IIS

The Internet services you installed are displayed, along with their status. To take action on any of these services, you need to highlight the service you want and then click one of the items on the button bar or right-click the mouse and select **properties** to change the settings for the service. IIS contains five property page tabs for the FTP server and four for the other ones. FTP has one additional Message Tab.

Service Tab Use this tab to control the time-out setting and the number of connections supported.

Message Tab Use this tab to enter text for messages that will be displayed to people who connect to your FTP site.



TCP Port: 21

Connection Timeout: 900 seconds

Maximum Connections: 1000

☑ Allow Anonymous Connections

Username: IUSR_SILICONMEDIA

Password: ***************

☑ Allow only anonymous connections

Comment:

Fig 15.4

Directories tab Displays the directories set up to work with your Internet server. When you ran Setup, you specified a single directory for each of the World Wide Web, Gopher, and FTP services. In a larger Internet site, you might want to have different directories for different groups of users.

Logging tab Controls the logs kept on your Internet server.

Advance tab Use this tab to limit access to only a certain group of computers.

Networking & Windows NT

Everything you wanted to know about.....

About the Author

Munishwar Gulati is a graduate from IIT-Roorkee (Formerly University of Roorkee) and has about 13 years of experience in Computer Industry. He has written many computer based titles from DOS to Windows NT , to COBOL, to desktop publishing, to Visual Studio, to Web designing and many more, for various training centres all over India.

Co-Author Mini Gulati is also a graduate in Computer Science and has rich experience in analyzing systems and developing solutions. She is also co-authoring many of the upcoming titles.

Other Titles in Everything.... Series

- Introduction to Computers (including MS-DOS)
- Windows 98 & Information Technology
- Word 2000
- Excel 2000
- Powerpoint 2000
- Access 2000
- Foxpro 2.6 for Windows
- Business System & Tally 5.4
- Programming in C
- UNIX/Linux
- System Analysis & Design
- Adobe Photoshop 6.0
- HTML 4
- VBScript
- Oracle 8i
- Core Java
- Information Technology Fundamentals
- Basic Electronics
- Visual Basic 6.0

ISBN-81-87870-10-9

Silicon Media PRESS

SILICON MEDIA PRESS

www.siliconmedia.org