INDEX

Chapter No.	**Description**	**Page No.**
1	Introduction to Windows NT	3
2	Introduction to Windows 2000 Server and its installation	5
3	Upgrading a member server to a domain controller	13
4	Automating Windows 2000 Server installation	16
5	Configuring Windows 2000 Server	32
6	Managing local users and groups	40
7	Managing active directory users and groups	54
8	Managing security settings	62
9	Managing disk	77
10	Managing dynamic storage	98
11	Recovering from disk failure	103
12	Managing data compression, disk quota,	106

	encryption and decryption	
13	Accessing files and folders	119
14	Managing network services	134
15	DNS server	146
16	WINS server	154
17	DHCP server	157
18	NW link IPX/SPX/NETBIOS	162
19	Web Server	164
20	Windows 2000 boot process	172
21	Advanced startup options	182
22	Startup and recovery options	184
23	Setup boot disk and backup	187
24	RAS Server & VPN Server	196
25	Proxy server / setting up cyber café	203

CHAPTER 1

INTRODUCTION TO WINDOWS NT

1.1. **Introduction**

Microsoft Company developed Windows NT in 1993. NT stands for New (Network) Technology. Windows NT has two products namely Server and Client. This was developed from the scratch and has nothing to do with the earlier versions of OSs from Microsoft.

1.2. **Features of NT**

NT has the following major features:

- Adaptability/Portability: It can run on different hardware platforms with minimal change. *It can run on Intel x86 machines as well as on other computers manufactured by DEC Alpha AXP, MIPS R4400 and Motorola Power PC.*
- Security: It is locked down through software passwords.
- Pre-emptive Multitasking: There are two major types of multitasking namely Co-operative and Pre-emptive.
    - In co-operative multitasking, the operating system gives the control of the system to a particular application. *In this if any of the application does not work properly, then it may hang the system. This is supported by Windows 3.x and Apple's Mac operating system.*
    - In pre-emptive multitasking, OS always maintains the control over the system. It gives specific slices of time to each of the applications.
- No More DOS: Windows NT does not contain DOS codes in the coding. Everything is done through emulation of standard DOS calls. *Although there is no DOS, Windows NT will still be able to run the vast*

majority of DOS programs by creating a virtual DOS environment called the NT Virtual DOS Machine (NTVDM).

Exercise - 1

Q.1 Fill in the blanks:

(i) In Windows NT, NT stands for__________.(New Technology)

(ii) Windows NT was developed in__________. (1993)

(iii) In pre-emptive multi-tasking, __________ always maintains the control of the system. (OS)

Q.2 Write short Notes:

(i) Multi-tasking

(ii) Cooperative Multi-tasking

(iii) Pre-emptive Multi-tasking

(iv) Features of Windows NT

CHAPTER 2

INTRODUCTION TO WINDOWS 2000 SERVER AND ITS INSTALLATION

2.1. **Introduction**

Windows 2000 Server is a product of Microsoft Company. This is an advanced version of Windows NT 4.0 Server.

2.2. **Features of Windows 2000**

- Active directory, which provides scalable network architecture that can be used to support a single server with a few objects or thousands of servers with millions of objects.
- An administrative console called Microsoft Management Console (MMC) provides administrative tools.
- Improved hardware support, including plug and play.
- High level security.
- A high level support for Internet connections through Internet Information Services (IIS).
- Supports up to 4 GB of memory.
- Support for two processors on a new installation.
- Supports Dynamic Disk.

2.3. **Logical Organisation of Active Directory**

The logical structure of the active directory consists of containers, domains and organizational units (OUs).

- A container is an active directory object that contains other active directory objects ie. Domains and OUs.

- A domain is the main logical unit of organization in the active directory. Objects in a domain share common security and account information. Each domain must have at least one domain controller (DC) which stores the complete domain database.
- Each domain can consist multiple OUs organized in a hierarchical structure. OUs may contain users, groups, security policies, computers, printers, file shares etc.
- Domains are connected to one another through logical structure relationships.
- *A domain tree is a hierarchical organization of domains in a single, contiguous namespace, in the active directory, a tree is a hierarchy of domains that are connected to each other through a series of trust relationships (logical links that combine two or more domains into a single administrative unit) the advantage of using trust relationships between domains is that they allow users in one domain to access resources in another domain, assuming the users have the proper access rights.*
- *A domain forest is a set of trees that does not form a contiguous namespace. For example, you might have a forest if your company merged with another company. With a forest, you could easily maintain a separate corporate identity through your namespace but share information across the active directory.*

2.4. <u>Minimum Hardware Requirement</u>

- Processor -133 MHz
- Memory (RAM)-128 MB
- Disk Space -2 GB.
- Display Adapter -VGA

2.5. <u>Different Versions of Windows 2000</u>

- <u>Windows 2000 Professional</u>: This is for stand alone machine and can act as client.

- Windows 2000 Server: This is for small and medium companies.
- Windows 2000 Advanced Server: This for medium and large companies, for example ISP (Internet Service Provider)
- Windows 2000 Datacenter Server: This is used for large-scale networks.

2.6. **File Systems Used by Windows 2000**

Windows 2000 supports three types of file systems which are as follows:

(i) File Allocation Table (FAT16)

- FAT keeps the track of location of files and directory entries.
- FAT16 is the 16-bit file system widely used by MSDOS.
- Supports up to 2GB disk partition.

(ii) FAT32

- It is 32-bit version of FAT introduced in 1996 with Windows 95 OEM (Original Equipment Manufacturer). *OEM is a version of Windows 95.*
- Supports up to 2 TB (Terabytes) disk.

(iii). New Technology File System (NTFS)

- NTFS provides local security on files and folders.
- The flexibility to assign disk quotas.
- The option to encrypt files which offers an additional level of security.

2.7. **Multi Booting**

Dual booting or Multi booting allows your computer to boot by multiple OSs. Your computer will be automatically configured for dual booting if there was a supported OS on your computer prior to the Windows 2000 Server installation. You should choose FAT16 or FAT32 file systems to dual boot because these file systems are backward compatible.

Important points for multi booting:

- Install the simplest OS before 2000 Server ie. install DOS or window 9.x first.
- Do not convert your file system to NTFS.
- Never upgrade to windows 2000 dynamic disk. Any other OS including Windows NT does not recognize dynamic disks.

2.8. Licensing Mode

Microsoft has two choices of licensing modes, which are as follows:

- Per Server: Per server specifies the number of network connections that can be made to a server at a time.
- Per Seat: Per seat specifies that each client will be licensed separately.

2.9. Membership in a Domain or Workgroup

When you are installing a server, choose workgroup or domain. If you are installing Windows 2000 Server on a non-net work computer, then choose Workgroup and if any Windows 2000 Server on your network is configured as Domain Controller (DC) with active directory installed, then choose Domain. *To join a domain you must specify the name of valid domain and user who has rights to add a computer to the domain.*

2.10. Language and Locale

Language and locale settings are used to determine the language that computer will use. Locale settings are used to configure the locality of items such as numbers, currencies, times and dates.

2.11. **Installation Methods**

To install Windows 2000 from CD, follow one of the following procedures:

(i) You can boot the system by another OS and access CD ROM drive and then run winnt.exe (in case of DOS) or winnt32.exe (in case of Windows 95, 98, NT).

(ii) If your computer can boot by CD, then insert Windows 2000 Server CD into its CDROM drive and restart your computer.

(iii) If your computer has no OS installed and does not support booting from the CDROM drive, then use the Windows 2000 Server set up boot disks.

2.12. **Creating Set Up Boot Disks**

To create set up boot disks, take four 1.44 MB floppies labelled as Windows 2000 Server set-up disk 1, 2, 3 and 4.

The command/utility to create boot disks from Windows 2000, Windows NT or Windows 9.x is MAKEBT32.EXE and to make a disk from 16-bit OS is MAKEBOOT.EXE.

SMARTDRV

Smartdrv is a disk-caching program that speeds up process of copying files. With smartdrv it takes a few minutes to copy the files and without smartdrv it takes hour.

2.13. **Steps for Installation**

Main steps are as follows:

- Choose one of the installation procedures. If you boot from DOS or Windows 9.x, the set up program will be DOS based. If you boot from Windows NT, the set up program will be GUI based.
- Run the set-up wizard.
- Install windows 2000 networking.
- Upgrade the server to a domain controller *(If this is a domain controller rather than a member server).*

2.14. **Running Set Up Program**

- Go to i386 folder and run Winnt32.Exe or Winnt.Exe.

- First it will copy the files.
- A dialog box will appear. Press Enter to set up or press R to repair or press F3 to quit set up.
- Windows 2000 license agreement dialog box appears. Press F8 to accept or press Esc to disagree.
- Set partition in which you want to install.
- Computer will restart automatically.

2.15. **Windows Set Up Wizard**

This wizard will ask following informations:

- Regional setting *(Regional setting dialog box appears, in which set locale and keyboard settings.)*
- Personal information *(Personalize dialog box appears, in which fill name and organisation.)*
- Product key *(The product key dialog box appears in which enter the product key number).*
- Licensing modes *(The licensing modes dialog box appears, in which select per seat or per server.)*

- Computer name and Administrator password *(The computer name and administrator password dialog box appears).* Your computer name can be up to 15 characters.
- Modem information *(If you have plug and play modem, then a modem dialog box will appear)*.
- Date and time *(The date and time dialog box appear in which set your date and time)*.
- Network setting *(The network setting dialog box appears which specifies how you want to connect to other computer and Internet, select typical).*
- Workgroup or Domain, select one of them.
- Computer will perform some final tasks including installing start menu items, registering computers, saving settings and removing temporary files. This will take several minutes.
- Remove the CD and click Finish button to restart the computer.

2.16. **Network Identification Wizard**

Network identification wizard is responsible for the network component installation.

- Enter user name and password, which is compulsory.
- Network identification wizard prompts you to finish the wizard.
- Enter the valid Windows 2000 user name and password. At this point, administrator and user name which you have entered for identification are enabled and at the last you will be greeted with the Windows 2000 Server.

Practical

Installation of Windows 2000 Server.

Exercise - 2

Q.1 Fill in the blanks:

(i) Windows 2000 Server is an advanced version of Windows--------------. (NT 4.0 Server)

(ii) MMC stands for-----------. (Microsoft Management Console)

(iii) Windows 2000 supports memory upto--------------. (4 GB)

(iv) Logical structure of Active Directory consists of--------------. (Containers, Domains and OUs)

(v) Minimum memory required for Windows 2000 installation is-----------. (128 MB)

(vi) Minimum disk space required for Windows 2000 installation is-----------. (2 GB)

(vii) FAT-32 was introduced with----------- version of Windows 95. (OEM)

(viii) OEM stands for --------------. (Original Equipment Manufacturer)

(ix) FAT-32 supports upto ----------- disk. (2TB)

(x) NTFS stands for ------------. (New Technology File System)

(xi) Utilities for creating Setup boot disks are ------------. (Makeboot and Makebt32)

Q.2 Write short Notes:

(i) Features of Windows 20000

(ii) Logical Organisation of AD

(iii) Minimum Hardware requirement for Windows 2000

(iv) Versions of Windows 2000

(v) File Systems used by Windows 2000

(vi) NTFS

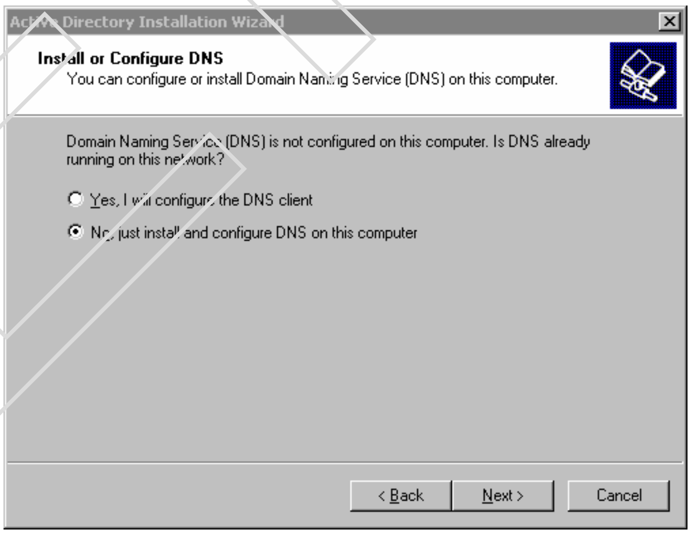
(vii) Multi Booting

(viii) Licensing Modes

CHAPTER 3

UPGRADING A MEMBER SERVER TO A DOMAIN CONTROLLER

- Click Start → Run, type DCPROMO & click OK button.
- Active Directory Installation wizard starts. Click Next button.
- Domain Controller Type dialog box appears, in which select "Domain controller for a new domain" option and click Next.
- Create Tree or Child domain dialog box appears. In this select "Create a new domain tree" option and click Next button. *(If you had the active directory installed on your network and you wanted to create a new child domain in the existing domain tree, you would select create a new domain child in an existing domain tree option).*
- Create or Join Forest dialog box appears. Select "Create a new forest of domain trees" option and click Next. *(If you already had the active directory installed on your network and wanted the domain tree to be installed as a part of an existing forest, you would select the place 'This new domain tree is an existing forest option'.*
- Install or Configure DNS dialogue box appears. Select "No, just install and configure DNS on this computer" and click Next.



Install or Configure DNS

You can configure or install Domain Naming Service (DNS) on this computer.

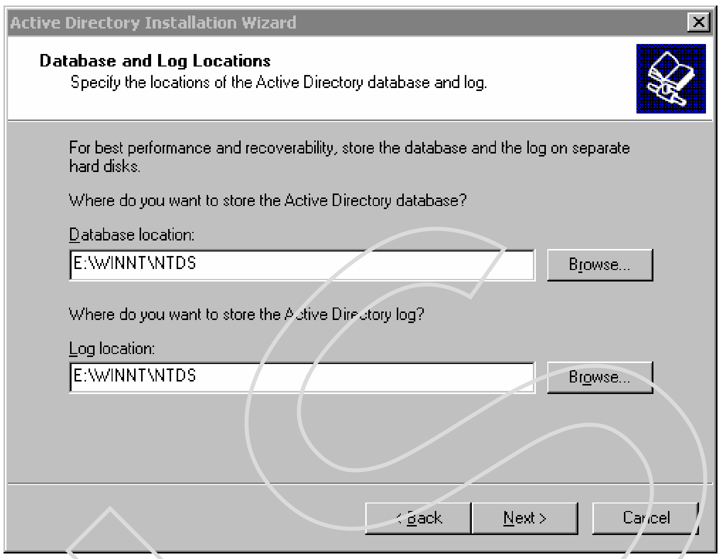
Domain Naming Service (DNS) is not configured on this computer. Is DNS already running on this network?

○ Yes, I will configure the DNS client

● No, just install and configure DNS on this computer

- New Domain Name dialog box appears. Specify the full DNS name for the new domain such as NITS.COM & click Next. *(Usually, DNS is configured for network before you create a domain controller).*

- NetBIOS Domain Name dialog box appears. NetBIOS domain names are used for compatibility with Windows NT client. NetBIOS domain name is same as DNS name. You can change or accept the default and click Next.
- Data Base and Log Locations dialog box appears to specify the locations of the Active Directory database and database log files. Accept the default and click Next.



Database and Log Locations
Specify the locations of the Active Directory database and log.

For best performance and recoverability, store the database and the log on separate hard disks.

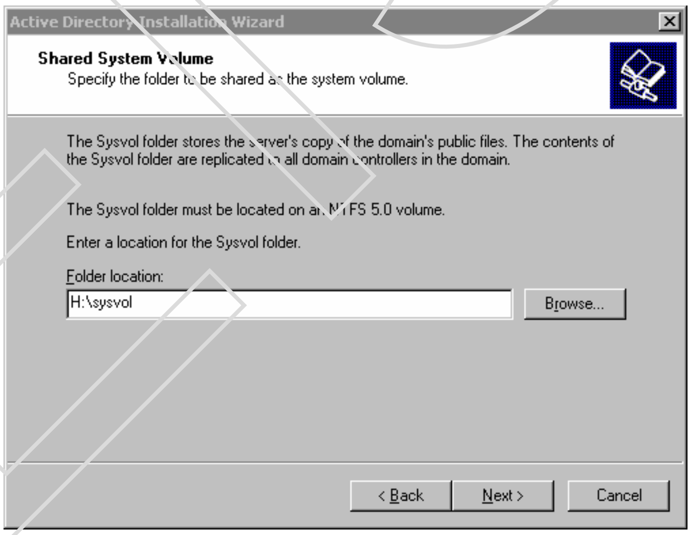
Where do you want to store the Active Directory database?

Database location: E:\WINNT\NTDS

Where do you want to store the Active Directory log?

Log location: E:\WINNT\NTDS

- Shared System Volume dialog box appears. This volume must be on NTFS. You can accept the default and click Next button. *(If the partition is not NTFS, you will see an error message indicating the file system must be converted). If the DNS has not been configured, message appears stating DNS server cannot locate, click OK.*



Shared System Volume
Specify the folder to be shared as the system volume.

The Sysvol folder stores the server's copy of the domain's public files. The contents of the Sysvol folder are replicated to all domain controllers in the domain.

The Sysvol folder must be located on an NTFS 5.0 volume.

Enter a location for the Sysvol folder.

Folder location: H:\sysvol

- Permission dialog box appears. To run server programs of earlier version of windows, select permissions compatible with pre-windows 2000 servers. Otherwise, select permissions compatible only with windows 2000 server.

- Directory Services Mode Administrator Password dialog box appears. Specify the password that can be used if the server needs to be restarted in the directory service restore mode. Enter and confirm the password and click Next button.
- Summary dialog box appears. Confirm all the selections and click Next.
- Configuring Active Directory dialog box appears. *(You will be asked to insert windows 2000 server CD, so that additional files may be copied thus completing the AD installation wizard)*. Click the Finish button. If asks to configure DNS, select "Skip DNS Configuration".
- Click Finish.
- Restart the Windows 2000 Server.
- After creating Domain Logon screen appears

User name-------------

Password---------------

Logon to --------------

Logon using dialup connections.

Practical
Upgrading a member server to a DC.

Exercise - 3
Q.1 Fill in the blanks:

(i) A member server can be upgraded to DC by using ________ utility. (DCPROMO)

(ii) Main difference between a member server and a Domain Controller is ________. (AD)

(iii) For upgrading a DC, one partition must be formatted by ________. (NTFS)

CHAPTER 4

AUTOMATING WINDOWS 2000 SERVER INSTALLATION

4.1. **Automated Installation**

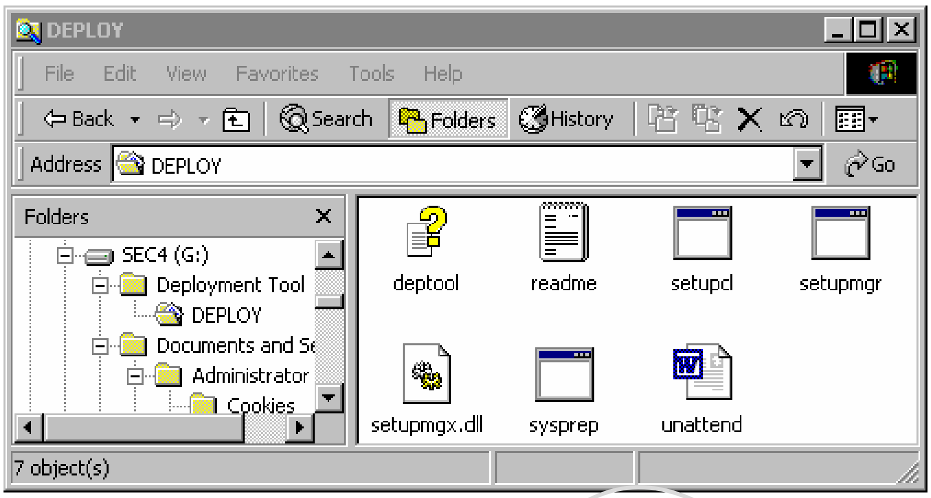
Automated installation is done through the use of disk imaging or by using the unattended installation method, when installing on multiple computers, which saves the time and makes easier.

The utilities used for automating the installation are included in the Deployment Tools folder while extracting the Deployment Tools. The utilities are as follows:

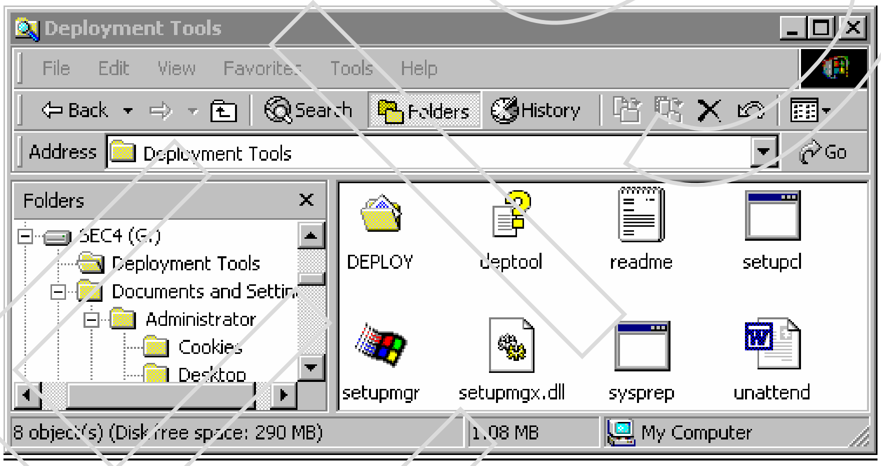
- The system preparation tool ie. Sysprep utility is used for preparing disk image.
- The set up manager ie. Setupmgr utility is used for creating unattended answer files. You have to extract these utilities before use.

4.2. **Extracting the Deployment Tools**

- Log on as Administrator.
- Create DEPLOYMENT TOOLS folder under C: or any other drive.
- Insert the Windows 2000 Server CD.
- Copy SUPPORT\TOOLS\DEPLOY.CAB file of CD to DEPLOYMENT TOOLS folder.
- Double-click the DEPLOY.CAB file to display its contents.



- ➢ Select Edit → Select All.
- ➢ Then select File → Extract.
- ➢ Browse for Folder dialog box appears. Select DEPLOYMENT TOOLS folder.



Note: There should be eight items including DEPLOY.CAB file

4.3. **Disk Imaging**

Disk imaging or disk duplication is the process of creating a reference computer for the automated deployment. The reference or source computer has Windows 2000 Server installed and is configured with the settings and applications that should be installed on the target computers.

4.4. Points to Remember for Disk Duplication

In order to use a disk image, the source and target computers must meet the following requirements:

(i) The hard disk interface (SCSI or IDE) must be of the same type.

(ii) The HAL (Hardware Abstraction Layer) must be of the same type. *(This means that the processor type must be the same).*

(iii) The size of the destination computer's hard drive must be at least as large as the source computer's hard drive.

(iv) Plug-and-Play devices on the source and destination computers need not to match, as long as the drivers for the Plug-and-Play devices are available.

(v) Non-Plug-and-Plug devices must be same.

4.5. System Preparation Tool (Sysprep)

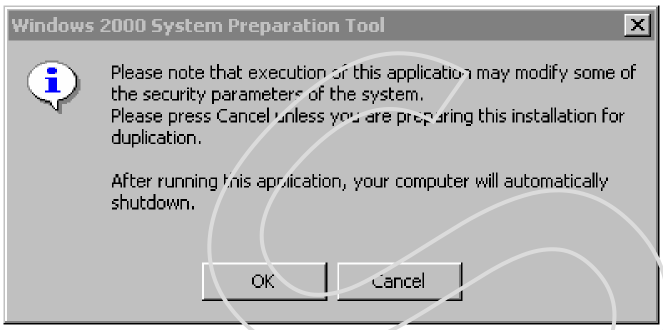
The System Preparation Tool (Sysprep) is included in the Windows 2000 Server CD in the DEPLOY.CAB file under Support\Tools folder. After you extract this tool, you can run Sysprep on the source computer. Sysprep prepares the disk image, stripping out information from the master copy that must be unique for each computer, such as the Security ID (SID).

After installing the copied image on the target computer, a Mini-Setup Wizard starts. This Wizard automatically creates a unique computer SID and then prompts the user for computer-specific information, such as the product ID, regional settings, and network configuration. The information that is required can also be supplied through an unattended answer file. One of the command switches can be used to customize how Sysprep works.

4.6. Creating a Disk Image

(i) Double click the Sysprep, which is under the Deployment Tools folder and click OK button.

(ii) Windows 2000 System Preparation Tools dialog box appears, giving warning that this program will modify some of the security parameters of the computer and click OK button.



Please note that execution of this application may modify some of the security parameters of the system.
Please press Cancel unless you are preparing this installation for duplication.

After running this application, your computer will automatically shutdown.

(iii) Automatically the computer will turn off. Restart the computer. Mini installation wizard will start.

4.7. Copying and Installing From a Disk Image

After running Sysrep on the source computer, you can copy the image and can then install it on the target computer.

You can create a duplicate disk image using a disk duplicator (a special device) or using special software.

If you are using a disk duplicator, shut down the source computer and remove the disk. Copy the disk with the help disk duplicator and install the copied disk into the target computer. If you are using special software, copy the disk image as per the software vendor’s instructions.

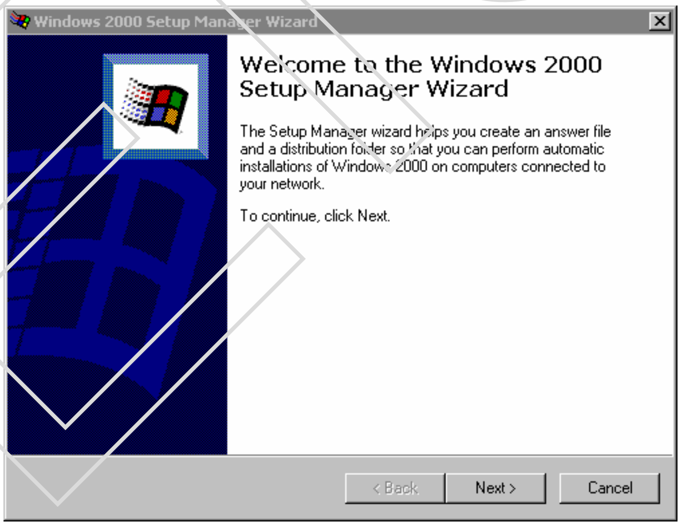
After the image is copied, turn on the destination computer. Mini Setup Wizard starts and asks some questions, if you have not configured answer file.

4.8. **Creating Answer Files**

Answer files are used for automated installations, which are used to answer the questions that appear during Windows 2000 Server installation.

The procedure to create answer files is as follows:

1. Double click the SETUPMGR program, which is under DEPLOYMENT TOOLS folder.
2. Windows 2000 Setup Manager Wizard starts. Click the Next button.

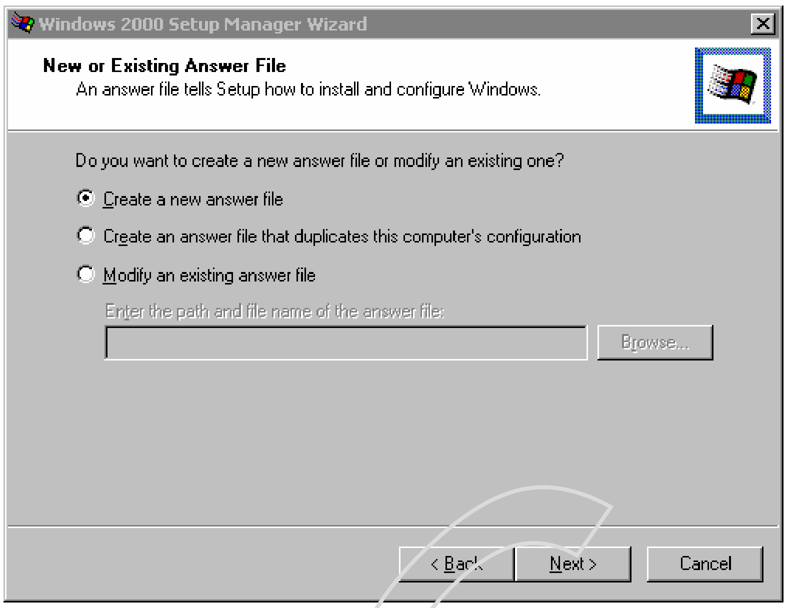


Welcome to the Windows 2000 Setup Manager Wizard

The Setup Manager wizard helps you create an answer file and a distribution folder so that you can perform automatic installations of Windows 2000 on computers connected to your network.

To continue, click Next.

3. New or Existing Answer File dialog box appears. *This dialog box provides choices for creating a new answer file, creating an answer file that duplicates this computer’s configuration, or modifying an existing answer file.* Select Create a new answer file option and click the Next button.



Windows 2000 Setup Manager Wizard

New or Existing Answer File
An answer file tells Setup how to install and configure Windows.

Do you want to create a new answer file or modify an existing one?

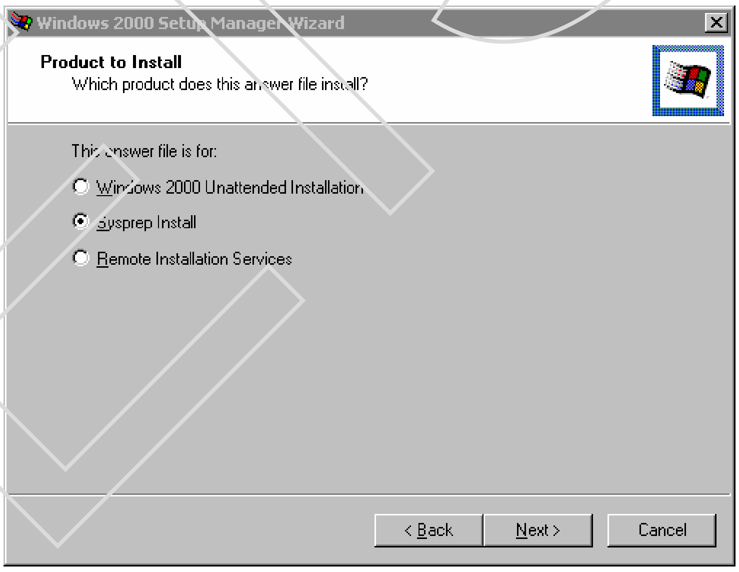
● Create a new answer file

○ Create an answer file that duplicates this computer's configuration

○ Modify an existing answer file

Enter the path and file name of the answer file:

4. Product to Install dialog box appears. You can select Windows 2000 Unattended Installation or Sysprep Install or Remote Installation Services. Select Sysprep Install and click the Next button.



Windows 2000 Setup Manager Wizard

Product to Install
Which product does this answer file install?

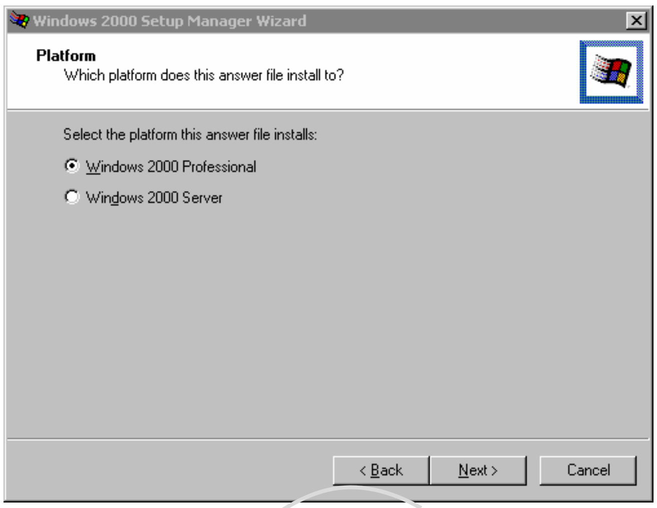
This answer file is for:

○ Windows 2000 Unattended Installation

● Sysprep Install

○ Remote Installation Services

5. Platform dialog box appears. You can choose to create answer files for the Windows 2000 Professional platform or the Windows 2000 Server platform. Select Windows 2000 Professional and click the Next button.



Windows 2000 Setup Manager Wizard

Platform

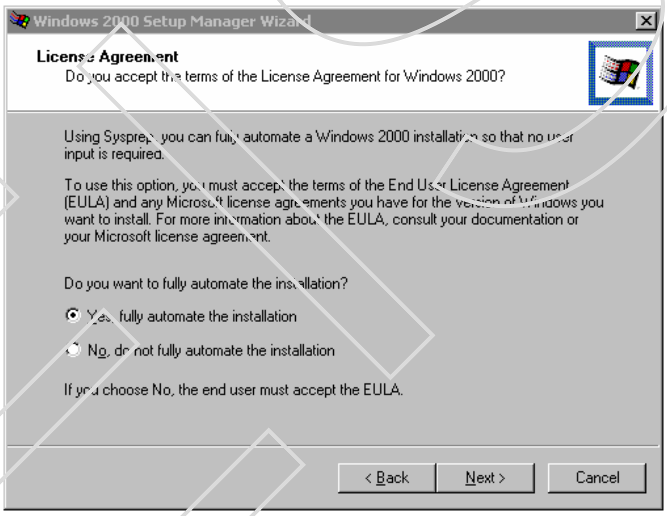
Which platform does this answer file install to?

Select the platform this answer file installs:

● Windows 2000 Professional

○ Windows 2000 Server

6. License Agreement dialog box appears. Choose "Yes Fully Automate the Installation", so that the installation is fully automated and click the Next button.



Windows 2000 Setup Manager Wizard

License Agreement

Do you accept the terms of the License Agreement for Windows 2000?

Using Sysprep, you can fully automate a Windows 2000 installation so that no user input is required.

To use this option, you must accept the terms of the End User License Agreement (EULA) and any Microsoft license agreements you have for the version of Windows you want to install. For more information about the EULA, consult your documentation or your Microsoft license agreement.

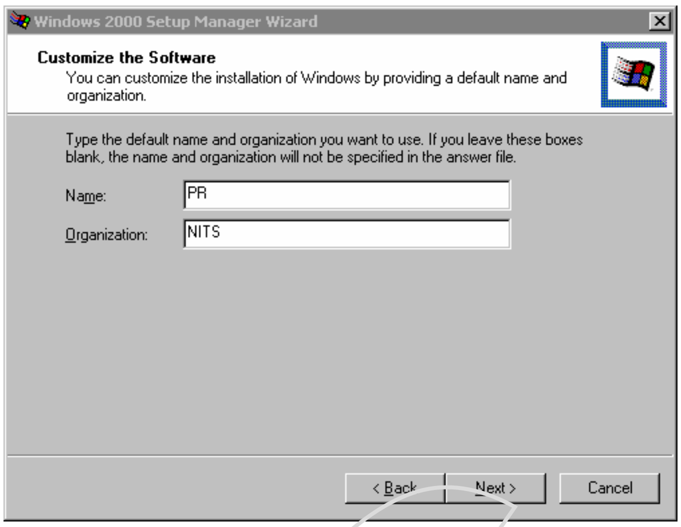
Do you want to fully automate the installation?

● Yes, fully automate the installation

○ No, do not fully automate the installation

If you choose No, the end user must accept the EULA.

7. Customize the Software dialog box appears, which allows you to specify the name and organization that will be used for licensing information. After you enter this information, click the Next button.



Customize the Software

You can customize the installation of Windows by providing a default name and organization.

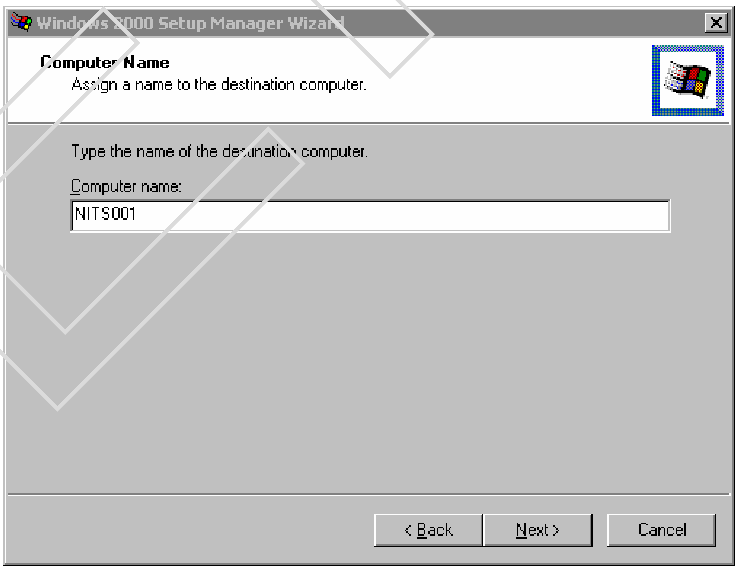
Type the default name and organization you want to use. If you leave these boxes blank, the name and organization will not be specified in the answer file.

Name: PR

Organization: NITS

8. Licensing Mode dialog box appears .You can choose Per Server or Per Seat. *In this dialog box, you specify whether you will license the server by concurrent connections (Per Server) or by seat (Per Seat). If you select Per Server, you can also set the number of concurrent connections allowed. (See Chapter 1 for more information about the Per Server and Per Seat licensing modes.) After you make your selection, click the Next button.*

9. Computer Name dialog box appears. Type the name of the destination computer and click the Next button.



Computer Name

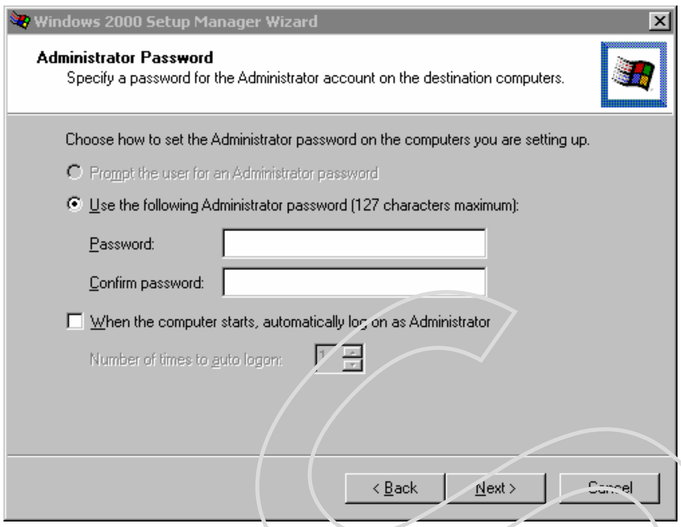
Assign a name to the destination computer.

Type the name of the destination computer.

Computer name: NITS001

10. Administrator Password dialog box appears in which you can enter the Administrator password upto 127 characters, then

click the Next button. *You can also specify that when the computer starts, the Administrator will automatically be logged on for x number of times. Enter and confirm an Administrator password*.



Windows 2000 Setup Manager Wizard

Administrator Password

Specify a password for the Administrator account on the destination computers.

Choose how to set the Administrator password on the computers you are setting up.

○ Prompt the user for an Administrator password

● Use the following Administrator password (127 characters maximum):

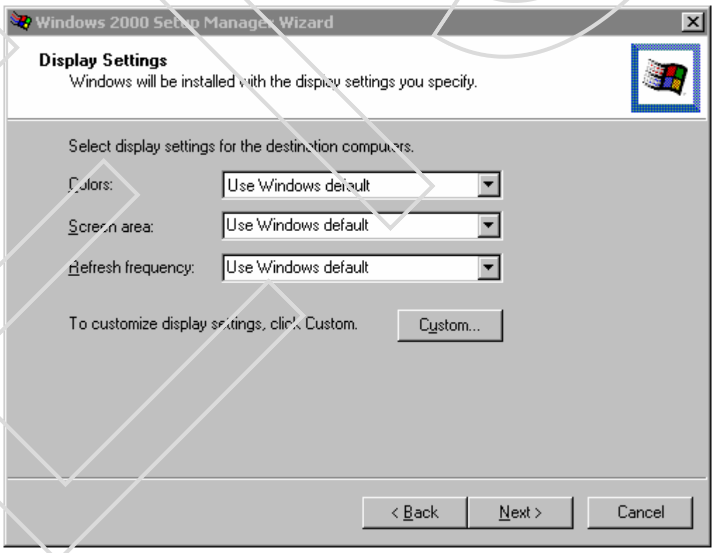
Password:

Confirm password:

□ When the computer starts, automatically log on as Administrator

Number of times to auto logon: 1

11. Display Settings dialog box appears in which change the settings or click Next to accept the default settings.



Windows 2000 Setup Manager Wizard

Display Settings

Windows will be installed with the display settings you specify.

Select display settings for the destination computers.

Colors: Use Windows default

Screen area: Use Windows default

Refresh frequency: Use Windows default

To customize display settings, click Custom.

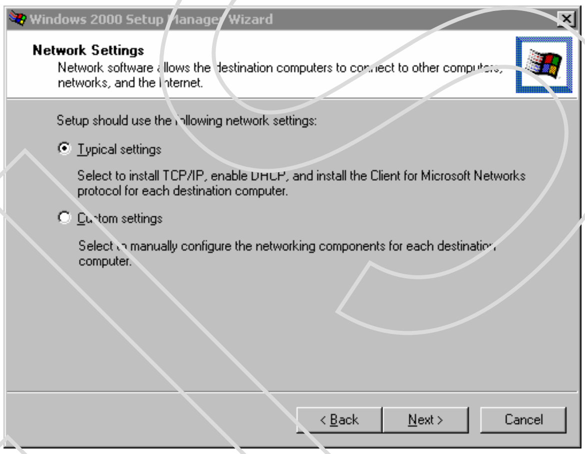
(i) *The Colors option allows you to set the display color to the Windows default, 16 colors, 256 colors high color (16 bit), true color (24 bit), or true color(32 bit).*

(ii) *The Screen Area option allows you to set the screen area to the Windows default, 640*480, 800*600, 1024*768, or 1280*1024,or 1600*1200.*

(iii) *The Refresh Frequency option (the number of times the screen is updated) allows you to set the refresh frequency to the Windows default, 60Hz, 70Hz, 72Hz, 75Hz,or 85Hz.*

(iv) *The custom button displays a dialog box that allows you to further customize display settings for the color, screen area, and refresh frequency.*

12. Network Settings dialog box appears, in which choose Typical Settings *(installs TCP/IP, enables DHCP, and installs Client for Microsoft Networks)* or Custom Settings *(allows you to customize the computer's network settings)* and click the Next button.



Network Settings

Network software allows the destination computers to connect to other computers, networks, and the Internet.

Setup should use the following network settings:

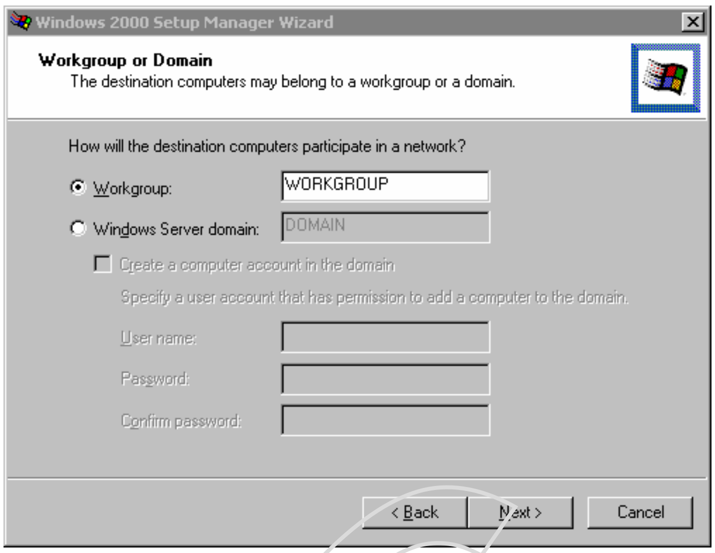
● Typical settings

Select to install TCP/IP, enable DHCP, and install the Client for Microsoft Networks protocol for each destination computer.

○ Custom settings

Select to manually configure the networking components for each destination computer.

13. Workgroup or Domain dialog box appears. Select the Workgroup or Windows Server domain and click the Next button.



Workgroup or Domain
The destination computers may belong to a workgroup or a domain.

How will the destination computers participate in a network?

● Workgroup: WORKGROUP

○ Windows Server domain: DOMAIN

□ Create a computer account in the domain

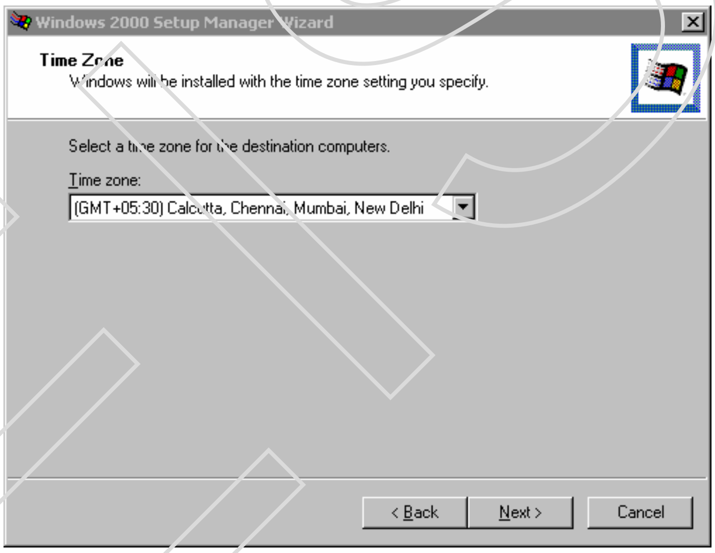
Specify a user account that has permission to add a computer to the domain.

User name:

Password:

Confirm password:

14. Time Zone dialog box appears. Select your computer's time zone from the drop-down list and click the Next button.



Time Zone
Windows will be installed with the time zone setting you specify.

Select a time zone for the destination computers.

Time zone: (GMT+05:30) Calcutta, Chennai, Mumbai, New Delhi

15. Additional Settings dialog box appears. Select No, do not edit the additional settings option and click the Next button to accept the default selection *If you select Yes, edit the additional settings, you can configure the following options:*

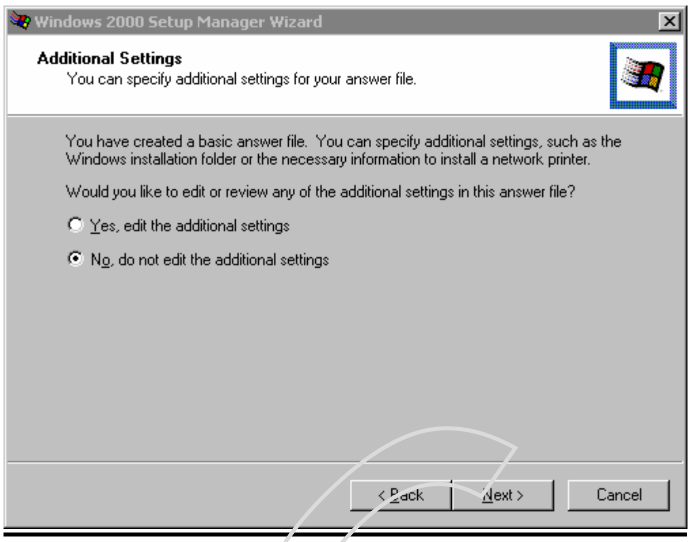
(i) Telephony settings

(ii) Regional settings

(iii) Languages

(iv) Install printers

(v) A command that will run once the first time a user logs on.



Windows 2000 Setup Manager Wizard

Additional Settings
You can specify additional settings for your answer file.

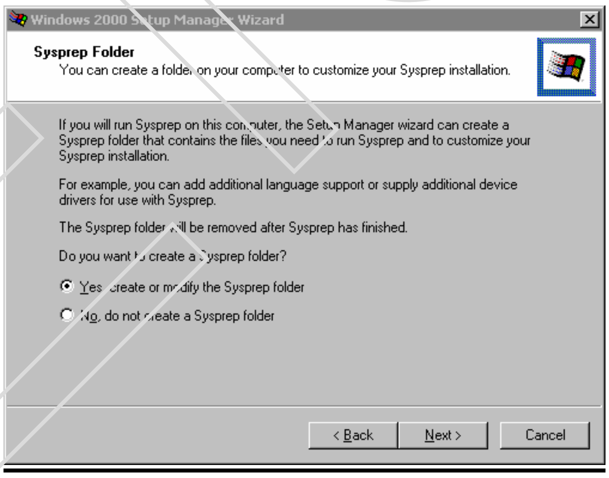
You have created a basic answer file. You can specify additional settings, such as the Windows installation folder or the necessary information to install a network printer.

Would you like to edit or review any of the additional settings in this answer file?

○ Yes, edit the additional settings

● No, do not edit the additional settings

16. Sysprep Folder dialog box appears which allows you to create a Sysprep folder that will be used during the Sysprep installation. Select "Yes, create or modify the Sysprep folder" and click Next.



Windows 2000 Setup Manager Wizard

Sysprep Folder
You can create a folder on your computer to customize your Sysprep installation.

If you will run Sysprep on this computer, the Setup Manager wizard can create a Sysprep folder that contains the files you need to run Sysprep and to customize your Sysprep installation.

For example, you can add additional language support or supply additional device drivers for use with Sysprep.

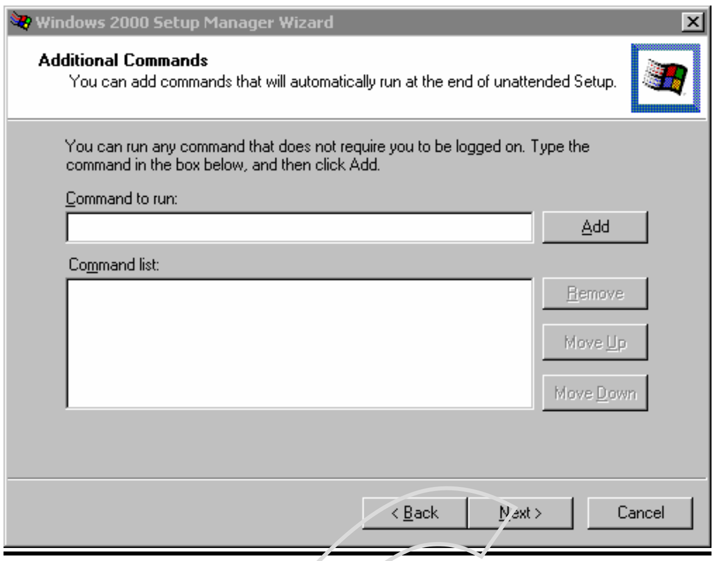
The Sysprep folder will be removed after Sysprep has finished.

Do you want to create a Sysprep folder?

● Yes, create or modify the Sysprep folder

○ No, do not create a Sysprep folder

17. Additional Commands dialog box appears, which allows you to run commands at the end of the automated installation. *You can specify any command that does not require a user to be logged on*. After you add any additional commands, click the Next button.



Windows 2000 Setup Manager Wizard

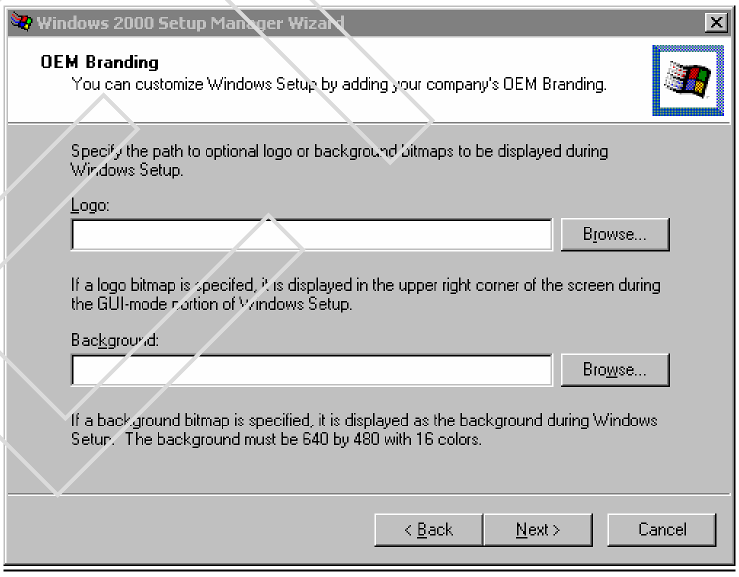
Additional Commands
You can add commands that will automatically run at the end of unattended Setup.

You can run any command that does not require you to be logged on. Type the command in the box below, and then click Add.

Command to run:

Command list:

18. OEM Branding dialog box appears, which allows you to configure an optional logo *(Logo or background that can be used to display Original Equipment Manufacturer (OEM) information, called OEM branding).* If you want to use a logo and / or a background, specify the path to the appropriate files. Then click the Next button.



Windows 2000 Setup Manager Wizard

OEM Branding
You can customize Windows Setup by adding your company's OEM Branding.

Specify the path to optional logo or background bitmaps to be displayed during Windows Setup.

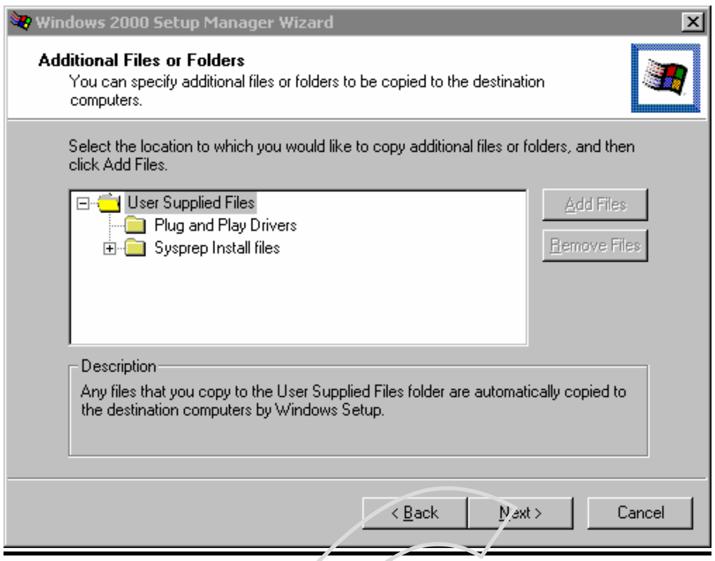
Logo:

If a logo bitmap is specifed, it is displayed in the upper right corner of the screen during the GUI-mode portion of Windows Setup.

Background:

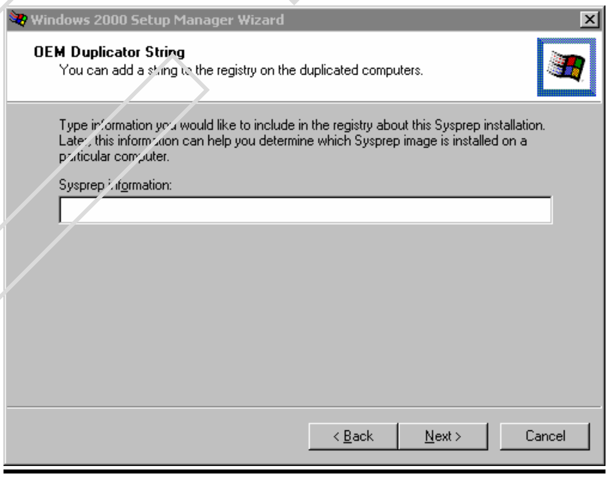
If a background bitmap is specified, it is displayed as the background during Windows Setup. The background must be 640 by 480 with 16 colors.

19. Additional Files or Folders dialog box appears, which allows you to specify any additional files or folders that should be automatically copied on the destination computers. After adding files, click the Next button.


Windows 2000 Setup Manager Wizard
Additional Files or Folders
You can specify additional files or folders to be copied to the destination computers.
Select the location to which you would like to copy additional files or folders, and then click Add Files.
User Supplied Files
Plug and Play Drivers
Sysprep Install files
Add Files
Remove Files
Description
Any files that you copy to the User Supplied Files folder are automatically copied to the destination computers by Windows Setup.
< Back
Next >
Cancel

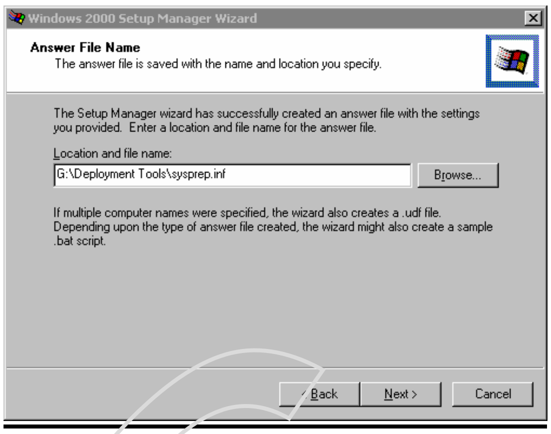
20. A message box appears, in which specify the location of the Sysprep.Exe file. Specify the location (for example, C:\Deployment Tools) and click the OK button.

21. OEM Duplicator String dialog box appears, which allows you to add information about the Sysprep installation that will be included in the computer's Registry. *This information can be used to determine which Sysprep image is installed on the specific computer.* After the information is added, click the Next button.


Windows 2000 Setup Manager Wizard
OEM Duplicator String
You can add a string to the registry on the duplicated computers.
Type information you would like to include in the registry about this Sysprep installation. Later, this information can help you determine which Sysprep image is installed on a particular computer.
Sysprep information:
< Back
Next >
Cancel

22. Answer File Name dialog box appears. The Setup Manager Wizard will create a file in the folder that the Sysprep command will run from. This file is named as Sysprep.Inf by default. You

can edit the location and accept the default and click the Next button.



Answer File Name

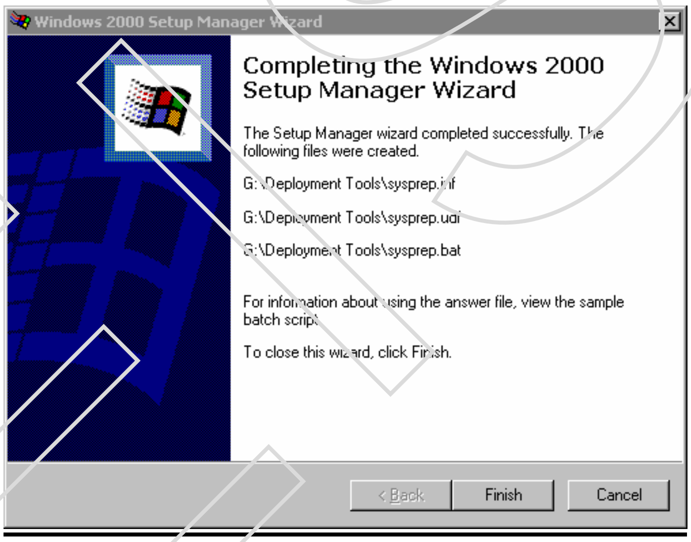
The answer file is saved with the name and location you specify.

The Setup Manager wizard has successfully created an answer file with the settings you provided. Enter a location and file name for the answer file.

Location and file name:
G:\Deployment Tools\sysprep.inf

If multiple computer names were specified, the wizard also creates a .udf file. Depending upon the type of answer file created, the wizard might also create a sample .bat script.

23. Completing the Windows 2000 Setup Manager Wizard dialog box appears. Click the Finish button.



Completing the Windows 2000 Setup Manager Wizard

The Setup Manager wizard completed successfully. The following files were created.

G:\Deployment Tools\sysprep.inf

G:\Deployment Tools\sysprep.udf

G:\Deployment Tools\sysprep.bat

For information about using the answer file, view the sample batch script.

To close this wizard, click Finish.

Practical

i) Extracting the Deployment Tools.
ii) Creating a disk image.
iii) Creating Answer Files.

Exercise - 4

Q.1 Fill in the blanks:

i) Automated installation is done when -----------. (installing on multiple computers)

ii) Utilities used for automated installation are ------------. (Sysprep and Setupmgr)

iii) Deployment Tools are stored in ------------. (Support\Tools\Deploy.Cab)

iv) Sysprep is used for ---------------. (creating disk image)

v) Setupmgr is used for -------------. (creating unattended answer files)

vi) HAL stands for -------------. (Hardware Abstraction Layer)

Q.2 Write short Notes:

(i) Automated Installation

(ii) Extracting Deployment Tools

(iii) Sysprep

(iv) Setupmgr

(v) Disk Image

(vi) Answer Files

CHAPTER 5

CONFIGURING WINDOWS 2000 SERVER

5.1. Introduction

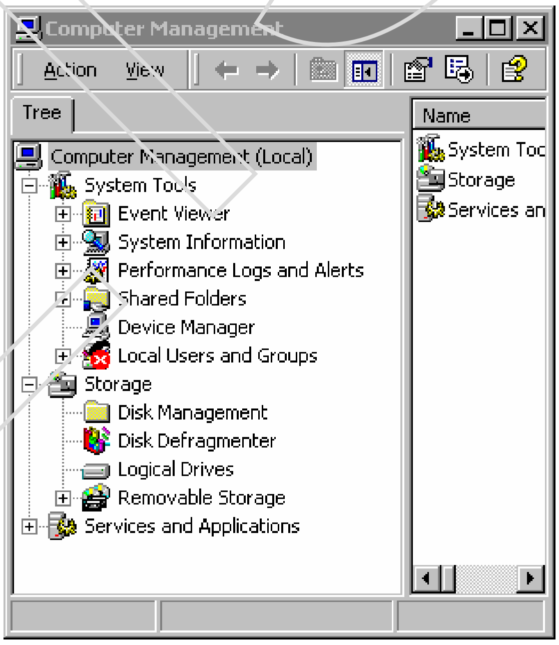
You can configure the system using Control Panel, Computer Management, Microsoft Management Console (MMC) and Registry.

5.2. Control Panel

You can access Control Panel by selecting Start → Settings → Control Panel or by opening My Computer and selecting Control Panel. The control panel provides different icons to configure the system.

5.3. Computer Management

To access Computer Management, right click on My Computer and select Manage from the pop-up menu. Computer Management interface appears, which is organised into three main areas. These are System Tools, Storage and Services & Applications.



1. System Tools: It includes the following utilities:

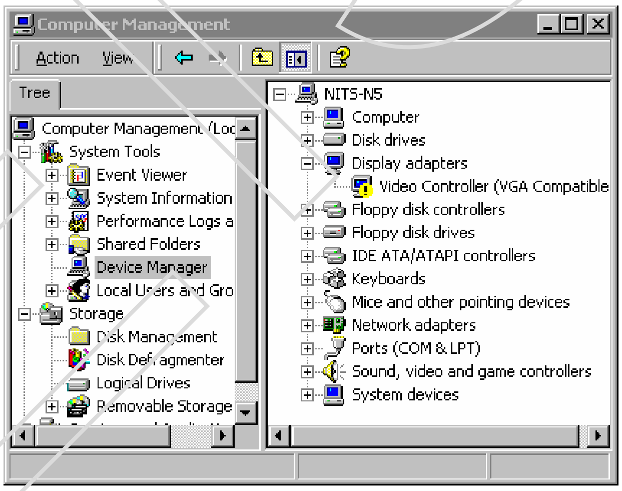
(i) Event Viewer: It tracks information about your event's success or failure, for example logon failure or success.

(ii) System Information: It is used to collect and display information about the computer's current configuration. Information is organised into six categories. These are System Summary, Hardware Resources, Components, Software Environment, Internet Explorer 5 and Applications.

(iii) Performance Logs and Alerts: It is keeping the log files, for example Disk Quota.

(iv) Shared Folders: It is used to create and manage shared folders.

(v) Device Manager: It provides information about all of the devices that your computer currently recognizes. Through device manager you can load, unload and update device drivers. In the right pane of the Device Manager window, double click the specific device you wish to manage.



(vi) Local Users and Groups: It is used to manage users and groups on a Windows 2000 Server running as a member server and not on a DC.

2. Storage: It is used to manage the computer's storage facilities, which includes Disk Management, Disk Defragmenter, Logical Drives and Removable Storage.

3. Services and Applications: You can manage all of the services like Telephony, IIS etc. installed on your computer.

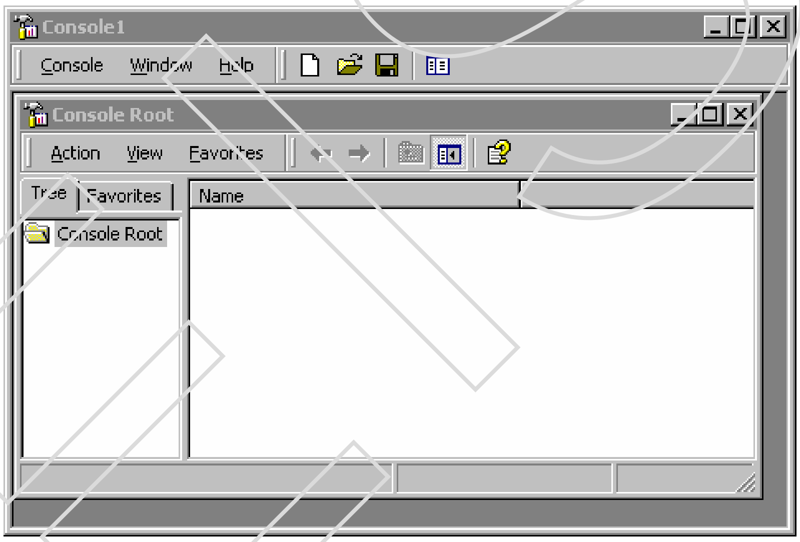
5.4. **Microsoft Management Console (MMC)**

MMC is the console frame for management. MMC offers the following benefits:

- MMC is highly customisable.
- MMC console can be saved and shared with other administrators.
- You can configure permissions for MMC, which an administrator can manage.

On a Windows 2000 Server computer, there is no item created for the MMC by default.

To open the MMC, click Start → Run and type MMC and then click OK.



Adding Snap-In

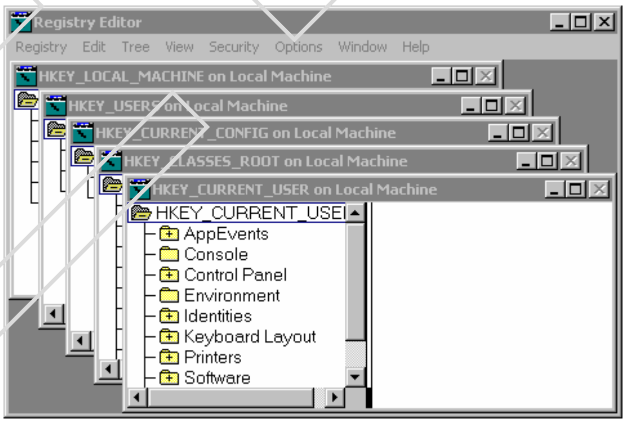
1. From the main Console window, select Console → Add/Remove Snap-in.
2. Add/Remove Snap-in dialog box appears. Click Add button.
3. Add Standalone Snap-in dialog box appears. Select the snap-in you wish to add and click Add button.

4. If prompted, specify whether the snap-in will be used to manage the local computer or the remote computer, select any one and click Finish.
5. Repeat steps 3 and 4 to add each snap-in you want to include in your console.
6. When finished click Close button.
7. Click OK to return to the main window.
8. Save by clicking Console → Save As and entering a name for the console.

5.5. **Registry Editor**

Registry is a database that is used to store information about the system configuration. The registry editor program is used to edit the registry. *When you make changes to your configuration, you use other utilities, such as control panel.* Windows 2000 has two Registry Editor utilities which are as follows:

(i) REGEDT32: It supports full editing of the Registry. To use REGEDT32, select Start → Run, type REGEDT32 and click OK.


Registry Editor
Registry Edit Tree View Security Options Window Help
HKEY_LOCAL_MACHINE on Local Machine
HKEY_USERS on Local Machine
HKEY_CURRENT_CONFIG on Local Machine
HKEY_CLASSES_ROOT on Local Machine
HKEY_CURRENT_USER on Local Machine
HKEY_CURRENT_USEI
AppEvents
Console
Control Panel
Environment
Identities
Keyboard Layout
Printers
Software

(ii) REGEDIT: It is lacking some of the options that are available with REGEDT32. For example, you cann't set security for Registry keys through REGEDIT. To use REGEDIT, select Start → Run, type REGEDIT and click OK.

It has the following hierarchical keys:

REGISTRY KEYS

HKEY_CURRENT_USER	Information for the users who is currently logged on.
HKEY_USERS	Information for all users of the computer.
HKEY_LOCAL_MACHINE	Contains computer hardware and software information.
HKEY_CLASSES_ROOT	Contains configuration information.
HKEY_CURRENT_CONFIG	Contains the configuration of the hardware profile that is used during start up.

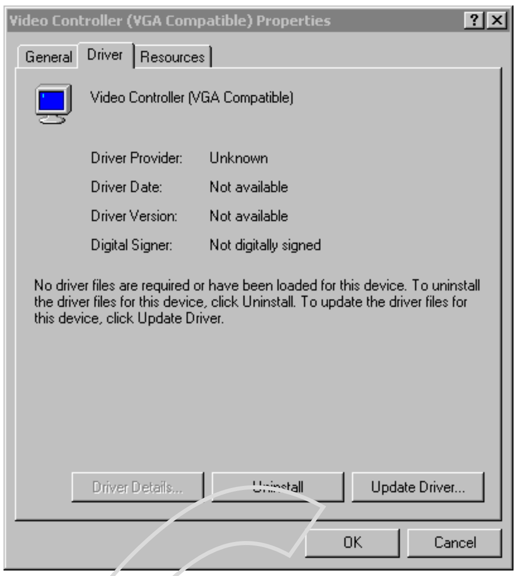
5.6. **Managing Hardware Devices Through Device Manager**

In the Computer Management window, select System Tools and then select Device Manager. In the right pane of the Device Manager window, double click the category of the device you wish to manage. It will display the list of devices which have been recognised by your computer. Double click the specific device you wish to manage.

5.7. **Configuring Video Adapters**

To configure video adapter steps are as follows:

- ➢ Click the Display adapters from the list of devices.
- ➢ Double click the Video Controller.
- ➢ Video Controller Properties dialog box appears.
- ➢ Click Driver tab and click Update driver button.
- ➢ Update Device Driver Wizard starts and click Next.



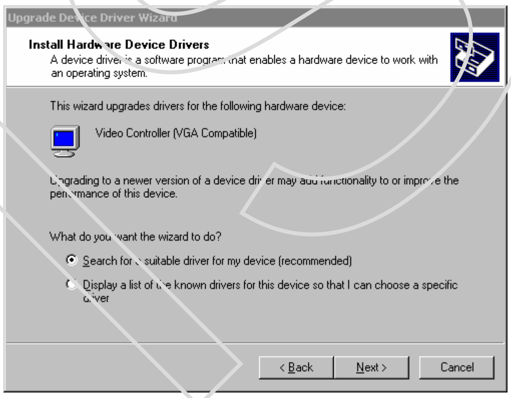
Video Controller (VGA Compatible) Properties

Video Controller (VGA Compatible)

Driver Provider: Unknown
Driver Date: Not available
Driver Version: Not available
Digital Signer: Not digitally signed

No driver files are required or have been loaded for this device. To uninstall the driver files for this device, click Uninstall. To update the driver files for this device, click Update Driver.

- Select “Display a list of known divers for this device so that I can choose a specific driver” or other option and click Next.



Upgrade Device Driver Wizard

Install Hardware Device Drivers
A device driver is a software program that enables a hardware device to work with an operating system.

This wizard upgrades drivers for the following hardware device:

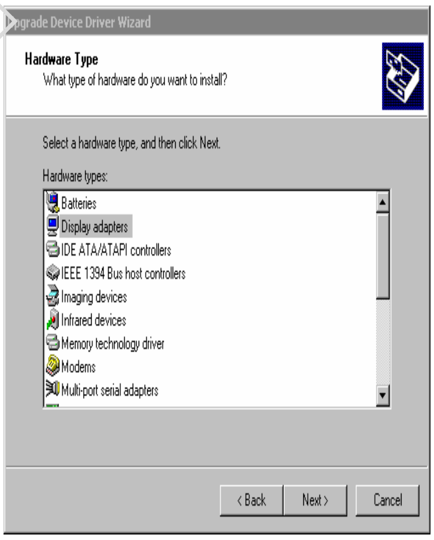
Video Controller (VGA Compatible)

Upgrading to a newer version of a device driver may add functionality to or improve the performance of this device.

What do you want the wizard to do?

● Search for a suitable driver for my device (recommended)
○ Display a list of the known drivers for this device so that I can choose a specific driver

- Select Display adapters and click Next.



Upgrade Device Driver Wizard

Hardware Type
What type of hardware do you want to install?

Select a hardware type, and then click Next.

Hardware types:

- Batteries
- Display adapters
- IDE ATA/ATAPI controllers
- IEEE 1394 Bus host controllers
- Imaging devices
- Infrared devices
- Memory technology driver
- Modems
- Multi-port serial adapters

- Click Have Disk button and select appropriate driver using Browse and Apply.

5.8. **Managing Device Drivers**

Updating Drivers

- Double click the device whose driver you want to update.
- Device Driver Properties dialog box appears. Click the Driver tab.
- Click the Update driver command button.
- Update Device Driver Wizard starts. Click Next button.
- Choose Search or Specific Driver from the list and click Next.
- In Search, it will locate the driver automatically and in Specific Driver, it will ask to mention the path of the driver. Give the path and click Next and click Finish.

Practical

i) Adding Snaps-in to MMC.

ii) Managing Device Drivers through Device Manager.

Exercise - 5

Q.1 Fill in the blanks:

i) System can be configured using __________. (Control Panel, Computer Management, MMC and Registry)

ii) You can access Computer Management by __________. (Right clicking on My Computer and selecting Manage)

iii) Three main areas of Computer Management are ________. System Tools, Storage and Services & Applications)

iv) Device Manager is used to ________. (provide information regarding all of the devices that the computer recognises and is used to load, unload and update device drivers)

v) MMC stands for ________. (Microsoft Management Console)

vi) You can open the MMC window by ________. (Start-→ Run, type MMC and click OK)

vii) Utilities used for editing Registry are ________. (REGEDIT and REGEDT32)

Q.2 Write short Notes:

i) Configuring System

ii) Computer Management

iii) System Tools

iv) Device Manager

v) MMC

vi) Adding Snaps-in to MMC

vii) Registry Editor

CHAPTER 6

MANAGING LOCAL USERS AND GROUPS

6.1. <u>An Overview of User Accounts</u>

Windows 2000 supports two kinds of users: local users and active directory (domain) users. *A computer that is running as Windows 2000 Professional or Windows 2000 Server (configured as a member server) has the ability to store its own user accounts database.* The users that are stored at the local computer are known as local users.

6.2. <u>Built-in User Accounts</u>

Built in user	**Description**	**Environment**
Administrator	The administrator has full control over the computer. *You provide a password for this account during windows 2000 installation. The administrator account can perform all tasks, such as creating users and groups, managing the file system printing.*	Local and domain
Guest	It has limited privileges. *The guest account allows users to access the computer even if they do not have a unique username and password. Because of the inherent security risks associated with this type of user, this account is disabled by default.*	Local and domain

ILS_Anonymous_ User	*It supports telephony applications that use features such as caller ID, video conferencing. In order to use ILS, internet information services (IIS) must be installed.*	*Domain*
IUSR_Computer_ name	*It is used for anonymous access for IIS on a computer that has IIS installed.*	*Local and domain*
IWAM-computer-name	*It is used for IIS to start from process applications on a computer that has IIS installed.*	*Local and domain*
Krbtgt	*It is used by the key distribution center service.*	*Domain*
TSlnternetUser	*It is used by terminal services.*	*Domain*

By default, the name administrator is given to the account with full control over the computer. You can increase the computer's security by renaming the administrator account and then creating an account named administrator without any permissions. This way even if a hacker is able to log on as administrator, the intruder won't be able to access any system resources.

6.3. **An Overview of Group Accounts**

Windows 2000 member server has local groups whereas Windows 2000 domain controller has security groups and distribution groups.

A security group is a logical group of users who need to access specific resources.

A distribution group is a logical group of users who have common characteristics.

Windows 2000 domain controller also allows you to select group scope, which can be as follows:

- Domain local groups are used to assign permissions to resources. Local groups can contain user accounts, universal groups and global groups.
- Global groups are used to organize users who have similar network access requirements.

- <u>Universal groups</u> are used to logically organize users from anywhere in the domain tree or forest.

6.4. **<u>Built in Group Accounts</u>**

<u>Built-in-Group</u>	<u>Description</u>	<u>Environment</u>
Account operators	Can create domain user and group accounts, but can only manage the users and groups created by self.	Domain
Administrators	Have full rights and privileges.	Local and Domain
Backup operators	Have rights to back up and restore the file system. *Even if the file system is NTFS and they have not been assigned permissions to the file of backup operators and only access the file system through the backup utility*	Local and Domain
Guests	Has limited access to the computer	Local and Domain

Power users	Can create users and groups, but can only mange the users and groups created by self. They can also create network shares and printers.	Local
Print operator	Can administer domain printers.	Domain
Replicator	Replicator supports directory replication, which is a feature used by domain servers. *Only domain users who will start the replication service should be assigned to this group*	Local and Domain
Server operators	Can administer domain servers.	Domain
User	Have very limited system access. By default, all users who have been created on the computer except guest are members of this group.	Local and Domain
DHCP Administrators	Has rights to manage DHCP	Domain
DHCP Users	Has rights to use DHCP services	Domain
DnsAdmins	Have rights to manage DNS.	Domain
DnsUpdateProxy	Has permission that allows DNS clients to perform dynamic updates on behalf of other clients, such as DHCP servers.	Global
Domain Admins	Has complete administrative rights over the domain	Global
Domain computers	Contains all of the workstations and servers that are a part of the domain.	Global
Domain controllers	Contains all of the domain controllers in the domain.	Global
Domain guests	Has limited access to the domain.	Global

Enterprise Admins	Have computer administrative rights over the enterprise. This group has the highest level of permissions of all groups.	Global
Group Policy Creator Owner	Has permissions to modify group policy for the domain	Global
RAS and IAS Server	Servers in this group can access remote access properties of users.	Domain
Schema Admins	Has permission to modify the schema of the active directory.	Global
WINS users	Has permissions to view information on the Windows Internet Name Service (WINS) server.	Domain

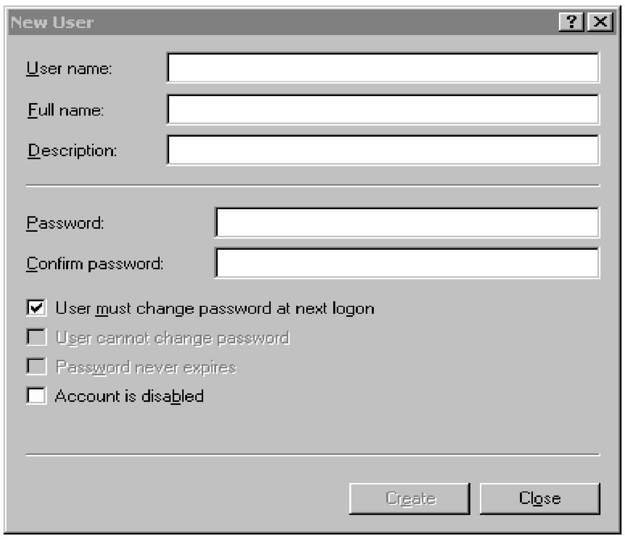
6.5. Creating New Users

To create a user you must be a member of the Administrators group or the Power Users group.

Username Rules and Conventions:

- ✓ A username must be between 1 and 20 characters.
- ✓ The username must be unique to the users. *Different from all other user and group names stored within the specified computer.*
- ✓ The username cannot contain special characters like * / \ [ ] : ; | = , + ? , > “.
- ✓ A username cannot contain periods (.) or spaces.

To create a new user, open the Local Users and Groups



New User

User name:

Full name:

Description:

Password:

Confirm password:

☑ User must change password at next logon

□ User cannot change password

□ Password never expires

□ Account is disabled

utility, highlight the Users folder and select Action → New User. This opens the New User dialog box.

The new user dialog box options are as follows:

Option	Description
User name	Defines the user name for the new account. User names are not case sensitive.
Full name	Allow you to provide detailed information about this user.
Description	Allow you to provide additional information.
Password	Assigns the initial password for the user. Passwords can be up to 127 characters and are case sensitive.
Confirm password	To verify that you have entered the password correctly.
User must change password at next logon	If selected, forces the user to change the password at first log on.

User cannot change password	If selected, prevents a user from changing the password. *It is useful for accounts like guest and those that are shared by default. This option is not selected.*
Password never expires	If selected, specifies that the password will never expire. *Even if a password policy has been specified.*
Account is disabled	If selected, user can not log on.

6.6. **Disabling a User Account**

1. Open the MMC and expand the Local Users and Groups snap in.
2. Open the Users folder. Double click the user to open the User Properties dialog box.
3. In the general tab, check the "Account is disabled" box and click the OK button.

6.7. **Deleting a User**

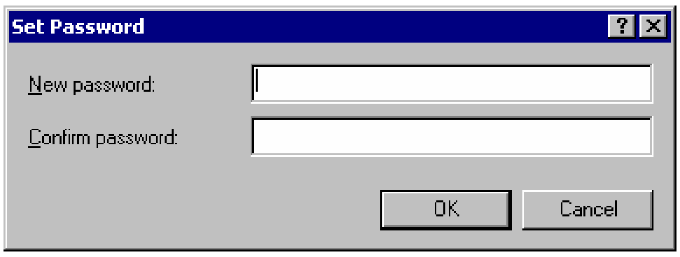
- Select the user you wish to delete.
- Click Action and then click Delete.
- Click Yes to confirm.

6.8. **Renaming a User**

- Select the user you wish to rename.
- Click Action and then click Rename and type the new name.

6.9. Changing a User’s Password

- Select the user whose password you wish to change.
- Click Action and then click Set Password.
- Set Password dialog box appears. Enter the new password and then confirm the password.

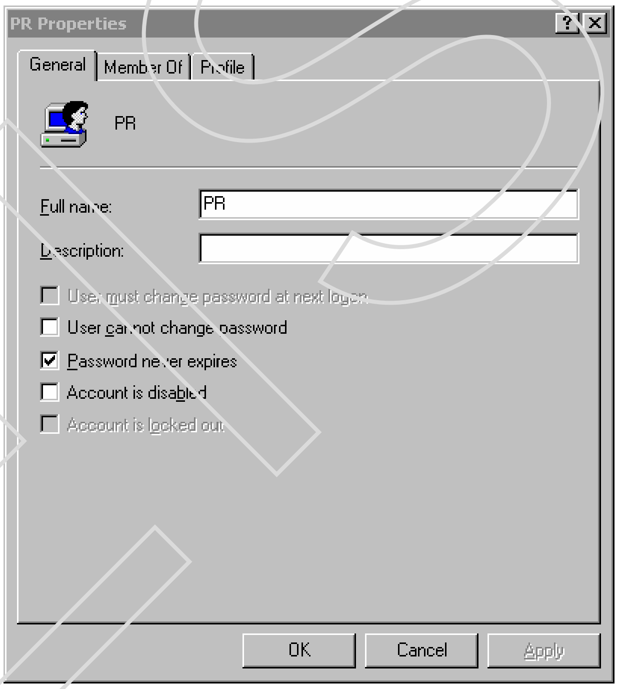


New password:

Confirm password:

6.10. Managing Local User Properties

To open the User Properties dialog box, double click the user account. User Properties dialog box has three tabs which are General, Member of and Profile.



Full name: PR

Description:

□ User must change password at next logon
□ User cannot change password
☑ Password never expires
□ Account is disabled
□ Account is locked out

- General tab contains the information that you supplied when you set up the new user account
- Member Of tab is used to manage the user’s membership in groups. To add a user to a group, follow the following procedure:
  - Click Add button.
  - Select the group, for example Power Users.
  - Click Add.
  - Click OK.

- Profile tab is used to set properties to customize the user's environment. You can specify the following items for the user:
  - Profile path
  - Logon script
  - Home folder

User profiles contain information about the Windows 2000 environment for a particular user, for example, the desktop arrangement, screen colours etc.

If the configuration option is a personal preference, it is most likely a part of the user profile. Configuration options that relate to the computer are not a part of the user profile. For example, the mouse driver is not a part of a user profile. Pointer, and mouse button settings are the user's personal preferences and are a part of a user profile.

By default, when a user logs on, a profile is opened for a user. A folder that matches the user's logon name is created for the user in the DOCUMENTS AND SETTINGS FOLDER when the user logs off and logs on.

The user profile folder holds subfolders that contain directory links to the user's desktop items.

Any changes that the user makes to the desktop are stored on the local computer when the user logs off. *For example, suppose that user PR logs on, picks his wallpaper, creates shortcuts, and customizes the desktop to his personal preference. When he logs off, his profile is stored locally.*

i) Profile path

This is used to point another location for the profile files other than the default local location. *This allows users to access profiles that have been stored on a shared network folder. This way, profiles can be used for an individual user or shared between a group of users. To specify a path, just type it in the profile path text box.*

ii) Logon script:

Logon scripts are the files that run every time when a user logs on to the network. They are usually batch files, but they can be any type of executable files.

You might use logon scripts to set up drive mappings or to run a specific executable file each time a user logs on to the computer. For example, you could run an inventory management file that collects information about the computer's configuration and sends that data to a central management database. Logon scripts are useful for compatibility with non-windows 2000 clients, not commonly used in windows 2000 networks. Windows 2000 automates much of the user's configuration. In older net ware environments, for example, this isn't the case, and administrators use logon scripts to configure the users, environment.

iii) Home folder:

Users normally store their personal files and information in a private folder called a home folder. *In the profile tab of the user properties dialog box you can specify the location of a home folder as a local folder or a network folder.*

To specify a local path folder, choose the local path option and type the path in the text box next to that option. To specify a network path for a folder, choose the connect option and specify a network path using a UNC (Universal Naming Convention) path. In this case, a network folder should already be created and shared.

6.11. Assigning a Home Folder to User

1. Open the User Properties dialog box.
2. Select the Profile tab and click Local path.
3. Specify the home folder path by typing C:/USERS /FOLDER NAME in the text box for the local path and then click the OK button.

6.12 **Managing Local Groups**

Groups are an important part of network management. Efficient administrators are able to accomplish the majority of their management tasks through the use of groups; they rarely assign permissions to individual users.

To set up and manage local groups, Local Users and Groups utility is used. With this utility, you can create, assign members to, rename and delete groups.

6.13. **Creating New Local Groups**

In order to create a group, you must be logged on as a member of the Administrators group or the Power Users group. The administrators group has full permission to manage users and groups. The members of the power users group can manage only the groups that they have created.

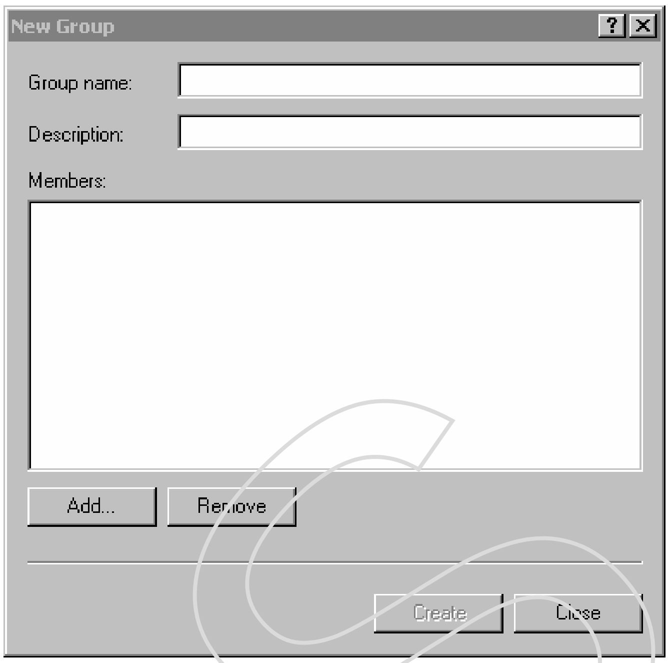
If possible you should add users to the built in local groups rather than creating new groups from scratch. This makes your job easier, because the built in groups already have the appropriate permissions. All you need to do is add the users you want to be members of the group.

Guidelines to Create a Local Group:

- The group name should be descriptive. *(For example, accounting data users).*
- The group name must be unique to the computer. *(Different from all of the other group names and usernames tat exist on that computer).*
- Group names can be up to 256 characters. The special characters are not allowed.

Creating a Local Group

1. Open the MMC and expand the Local Users and Groups snap-in.
2. Right click the Groups folder and select the New Group.
3. Type group name and click Create button.
4. Click Close button.



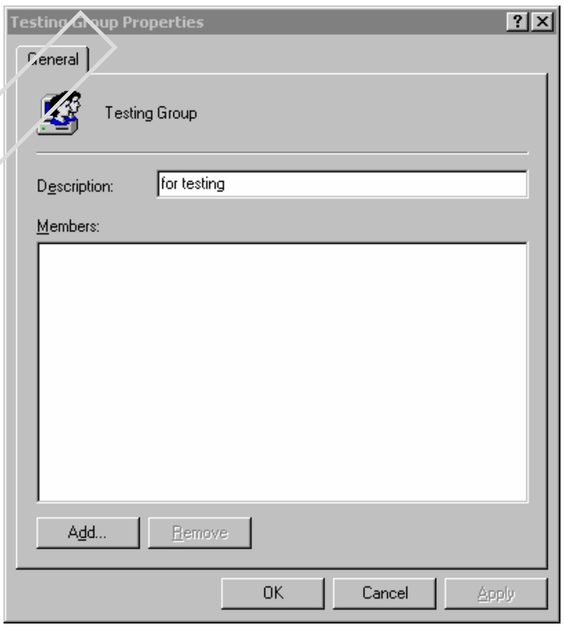
6.14. Managing Local Group Properties

After creating a group, you can add members to it. A user can belong to multiple groups.

You can easily add and remove users through the Group Properties dialog box. To access the Group Properties dialog box double click the group you want to manage.

From the Group Properties dialog box, you can change the group's description and add or remove group members. When you click the Add button to add members, the Select Users or Groups dialog box appears. In this dialog box, you select the user account you wish to add and click the Add button. Click the OK button to add the users to the group.

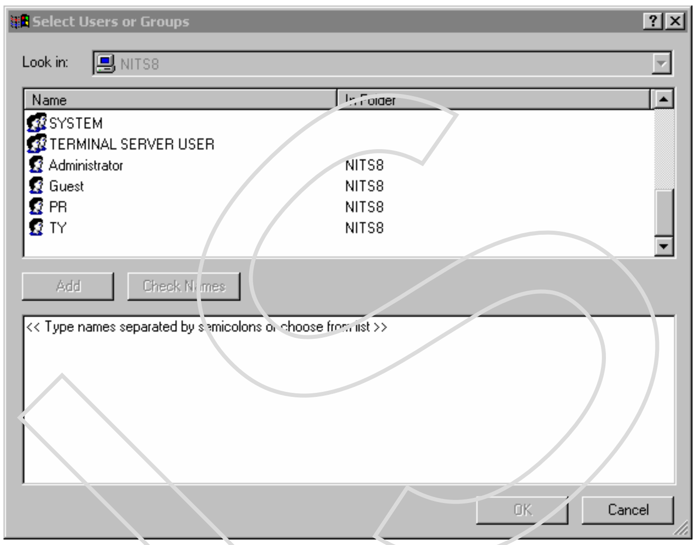
To remove a member from the group, select the member in the Group Properties dialog box from members list and click the Remove button.



Description: for testing

6.15. Adding User to Local Groups

1. Go to Group Properties dialog box. Click the Add button.
2. Select Users or Groups dialog box appears. Select the user and click Add button and then click OK.
3. In the Group Properties dialog box, you will see that the user has been added to the group. Click OK to close the Group Properties dialog box.



Look in: NITS8

Name	In Folder
SYSTEM	
TERMINAL SERVER USER	
Administrator	NITS8
Guest	NITS8
PR	NITS8
TY	NITS8

<< Type names separated by semicolons or choose from list >>

6.16. **Renaming Groups**

To rename a group, right click the group and choose the Rename option from the pop-up menu. Type the new name of the group and press Enter.

6.17. **Deleting Group**

To delete a group, right click the group and choose the Delete option from the pop-up menu. A dialog box appears, which warns you that a group will be deleted. Click Yes to delete.

Practical

i) Creating Local Users.
ii) Managing Local Users.
iii) Creating Local Groups.

iv) Managing Local Groups.

Exercise - 6

Q.1 Fill in the blanks:

i) The users stored on a member server are called ------------. (Local Users)

ii) The users stored on a DC are called ------------. (AD/ Domain Users)

iii) The group other than Administrators group on a member server that can create its own users is -----------. (Power Users)

iv) Path to Local Users and Groups utility is ------------. (Right click on My Computer-→ Manage-→ Tools)

v) Local user is created by using ---------------- utility. (Local Users and Groups)

vi) Number of tabs available in Local User Properties dialog box are --------------. (3)

vii) Local group is created by using ------------- utility. (Local Users and Groups)

Q.2 Short Notes:

i) Built in Group Accounts

ii) Creating New User

iii) Deleting User

iv) Managing Local Users Properties

v) Creating New Local Group

vi) Adding User to Local groups

CHAPTER 7
MANAGING ACTIVE DIRECTORY USERS AND GROUPS

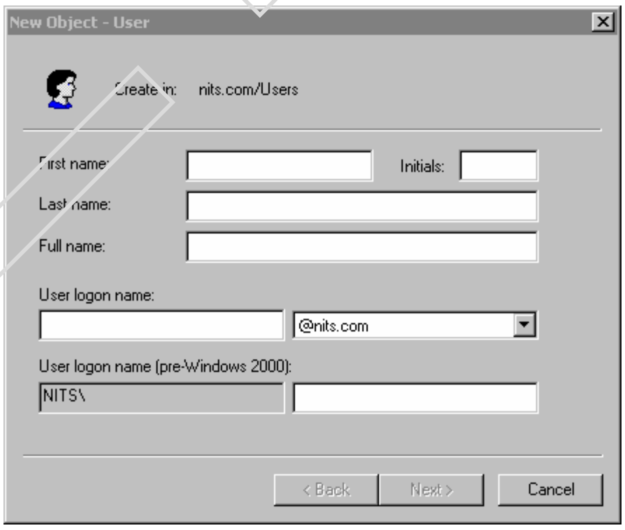
7.1. <u>Introduction</u>

To create domain accounts for users, you use the Active Directory Users and Computers utility. With this utility, you can add users to a domain in the active directory.

7.2. <u>Creating Active Directory Users</u>

You can create Active Directory users by the Active Directory Users and Computers utility. The procedure is as follows:

1. Select Start → Programs → Administrative Tools → Active Directory Users and Computers.
2. Active Directory Users and Computers window appears. Right click Users folder and select New from the pop up menu and then select User.
3. New Object - User dialog box appears. Type the user's first name, initials, last name, and logon name and then click Next. *The full name and pre windows 2000 logon name (for clients logging in from non windows 2000 operating systems) will be filled in automatically when you enter the other information, but you can change them if desired. Click the next button.*


New Object - User

Create in: nits.com/Users

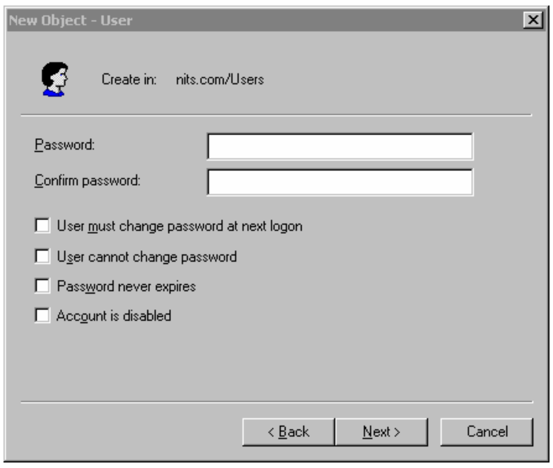
User logon name: @nits.com

User logon name (pre-Windows 2000): NITS\

4. Second dialog box appears in which type and confirm the user's password. Check the required check boxes and click Next. *The*

check boxes in this dialog box allow you to specify that the user must change the password when the user logs on, the user cannot change the password, the password never expires, or the account is disabled. Click the Next button.

5. Click the Finish button.



Create in: nits.com/Users

Password:

Confirm password:

□ User must change password at next logon

□ User cannot change password

□ Password never expires

□ Account is disabled

7.3. Managing Active Directory User Properties

- To access the properties dialog box for an active directory user, open the Active Directory Users and Computers utility *(By selecting Start, Programs, Administrative Tools, Active Directory User and Computers)*
- Open the Users folder and double click the user account.
- Active Directory User Properties dialog box appears. It has twelve main categories of properties which are as follows:

✓ General

✓ Address

✓ Account

✓ Profile

✓ Telephones

✓ Organization

✓ Member of

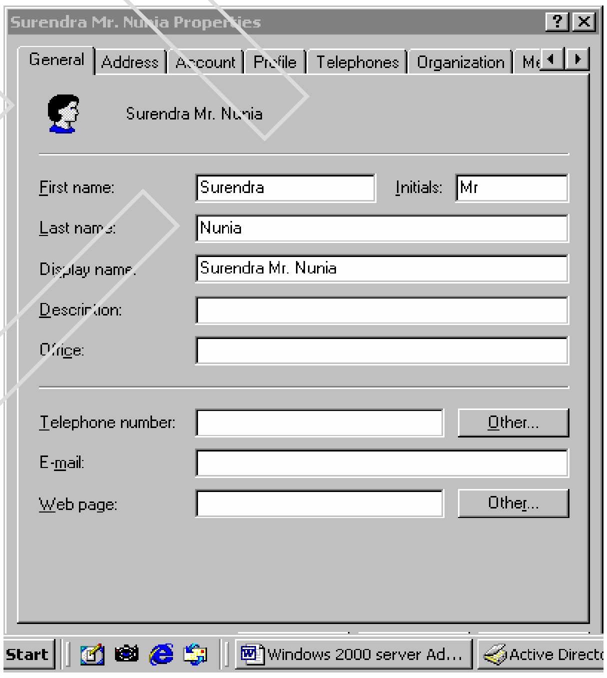
✓ Dial in

✓ Environment

✓ Sessions

✓ Remote control

✓ Terminal services profile



Surendra Mr. Nunia

First name: Surendra Initials: Mr

Last name: Nunia

Display name: Surendra Mr. Nunia

Description:

Office:

Telephone number: Other...

E-mail:

Web page: Other...

i) Configuring General Active Directory User Properties:

General tab contains the information that you supplied when you set up the new user account. *You can add information in the Description and Office text boxes. You can also enter contact information for the user, including a Telephone number, E-mail address and Web page URL.*

ii) Adding Active Directory User Address Information:

Address tab is used to provide the address information for the user. *This tab has text boxes for the User's street address. Post office box number, City, State or Province and Zip code. You can also select a Country or Region identifier from the country region drop down list.*

iii) Controlling Active Directory Users Accounts:

Account tab is used to control the user's account. *This tab shows the Logon name information that you supplied when you set up the New user account and allows you to configure the following settings:*

- *The logon hours for the user*
- *The computers that the user is allowed to log on from*
- *Account policies that apply to the user*
- *When the account expires*

a) Controlling Logon hours: You can control the logon hours by clicking Logon hours command button. *When you click the logon hours button, you see the logon hours dialog box, by default, users are allowed to log on 24 hours a day, seven days a week., logon hours are typically restricted during computer backups. You might also want to restrict logon hours for security reasons. A blue box indicates that logon is permitted. A white box indicates that logon is not permitted. You can change logon hours by selecting the hours you want to modify and clicking the logon permitted radio button or the logon denied radio button.*

b) *Controlling Computer Access:*

You can specify to logon from a particular workstation using Logon button. By default user can logon from any workstation. *When you click the Log on to button, you see the logon workstations dialog box, this dialog box allows you to* *specify that the user can log on to all the computers in the network or limit the user to logging on to specific computers in the network. For example, if the administrator works in a secure environment, you might limit the administrator account to only log on from a specific computer. You configure the computers that the user can log on from based on the computer's name. You add the computers that are allowed by typing in the computer name and clicking the add button.*

c) *Setting Account Options:*

- *User must change password at next logon.*
- *User cannot change password.*
- *Password never expires.*
- *Store password using reversible encryption.*

The account options are similar to the password policies that you can set for local user accounts.

d) Setting Account Expiration:

You can specify a specific date by Account expiration button. *The end of radio button at the bottom of the account tab lets you set account expiration for a specific date. By default, accounts do not expire. You might want to set an expiration date. This option is also useful in academic environments where students need user accounts. but their accounts should be disabled at the end of the academic period.*

iv) Setting up the Active Directory User Profile:

Profile tab allows you to set up user profiles, logon scripts and home folders. *These options are configured in the same way as they are for local user accounts. See the setting up the local user environment section earlier in this chapter for details on using the options in the profile tab.*

v) Adding Active Directory User Telephone Information:

Telephone tab, allows you to configure the user’s telephone numbers for home, pager, mobile and fax. *You can also add notes such as don’t call home after 10:00 PM.*

vi) Adding Active Directory Organization Information:

Organization tab allows you to provide information about the users role in your organization. *You can enter the user’s title department, company, and manager. You can also specify to whom the user directly reports.*

vii) Managing Active Directory User Group Membership:

Member Of tab displays the groups that the user belongs to us. You can add the user to an existing group by clicking the add button. It is used to manage a user’s group membership. *To remove the user form a group listed on this tab, highlight the group and click the remove button.*

viii) Configuring Dial in Properties:

Through Dial in tab, you can configure the user’s remote access permissions for dial in (covered later).

ix) Configuring Terminal Services Properties:

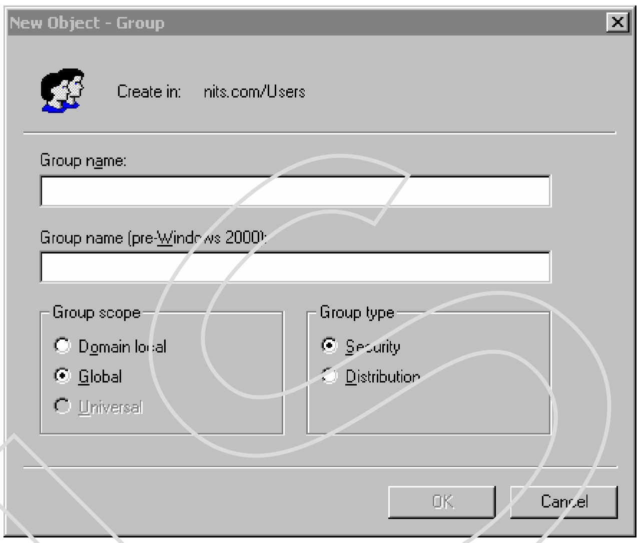
Four of the tabs in the active directory user properties dialog box contain properties that relate the Terminal Services; Environment, Sessions, Remote control and Terminal services profile (covered later).

7.4. **Creating Active Directory Groups**:

Groups are an important part of network management. Efficient administrators are able to accomplish the majority of their management tasks through the use of groups; they rarely assign permissions to individual users.

You can create and manage Active Directory Groups through the Active Directory Users and Computers utility. Active Directory Groups are created on a Domain Controller (DC). Procedure to create AD Groups is as follows:

1. Click Start → Programs → Administrative Tools → Active Directory Users and Computers.
2. Right click the Users folder, select New from the pop-up menu and then select Group.
3. New Object-Group dialog box appears. Type the name of the group in the Group name for windows 2000. Pre-Windows 2000 group name will be filled automatically but you can change it if desired.



Create in: nits.com/Users

Group name:

Group name (pre-Windows 2000):

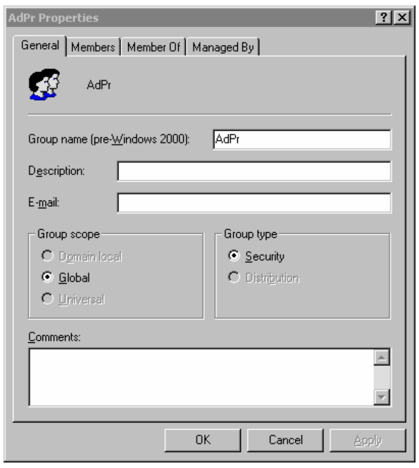
Group scope: ○ Domain local ● Global ○ Universal

Group type: ● Security ○ Distribution

4. In the Group scope section, select the scope for the group (Domain Local, Global or Universal).
5. In the Group type section, select the type of group that you want to create (Security or Distribution).
6. Click OK.

7.5. Managing Active Directory Group Properties

- Double click the group or right click the group and then select Properties.



AdPr

Group name (pre-Windows 2000): AdPr

Description:

E-mail:

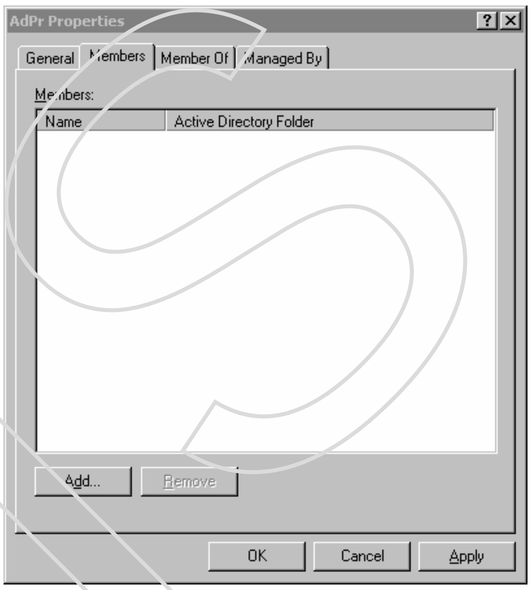
Group scope: ○ Domain local ● Global ○ Universal

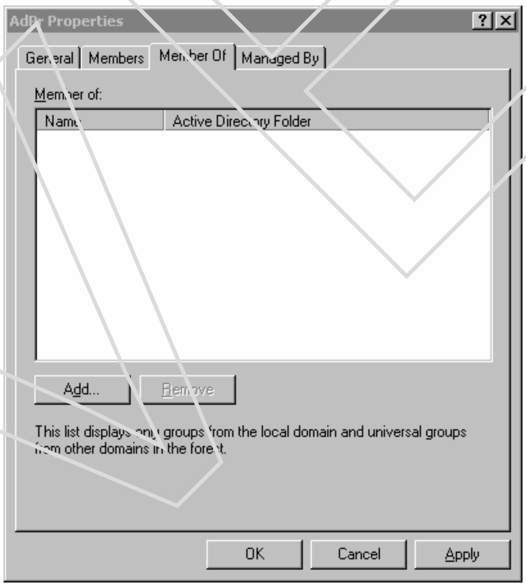
Group type: ● Security ○ Distribution

Comments:

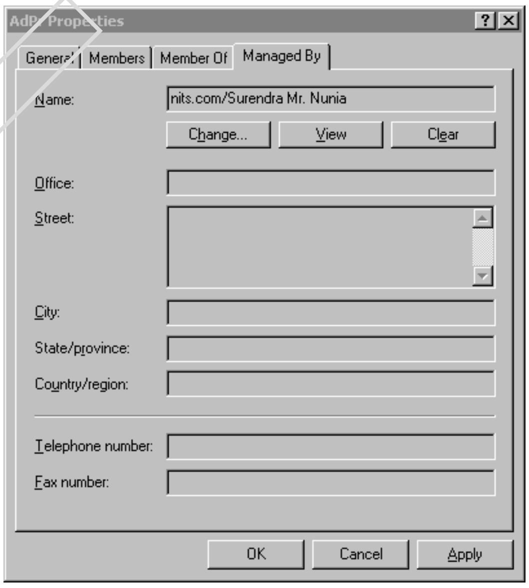
- Group Properties dialog box appears. The dialog box has four tabs with options. These are as follows:

- General Tab: Allows you to view and change the Pre-Windows 2000 group name, description and E-mail address. You can view the Group scope and Group type but you cann't change these entries.
- Members Tab: Allows you to view and change group membership.
- Member Of Tab: Allows you to view, add groups to or remove groups from other groups, if the group type allows group nesting (one group contained within another group).
- Managed By Tab: Allows you to view and change the user who manages the group.





This list displays only groups from the local domain and universal groups from other domains in the forest.



Name: nits.com/Surendra Mr. Nunia

Practical

i) Creating AD Users.
ii) Managing AD Users.
iii) Creating AD Groups.
iv) Managing AD Groups.

Exercise - 7

Q.1 Fill in the blanks:

i) AD users and Groups are created by ----------- utility. (AD Users and Computers)

ii) AD Users and Computers utility is accessed by-------------. (Clicking Start-→ Programs-→Administrative Tools)

iii) AD User Properties dialog box has ---------- tabs. (12)

iv) Account tab in AD User Properties dialog box is used to manage -----------------. (Logon hours for the user, the computers that the user is allowed to logon from, account policies that applies to the user and when the account should expire)

v) AD Group Properties dialog box has ----------------- tabs. (4)

Q.2 Write short Notes:

i) Creating AD Users
ii) Managing Account Properties of AD User
iii) Creating AD Groups

CHAPTER 8
MANAGING SECURITY SETTINGS

8.1. <u>Introduction</u>

Windows 2000 Server allows you to manage security settings at the local level, for a particular computer or at a domain level. Any domain security policies you define will override the local policies of a computer.

- To manage local policies, you use Group Policy with the local computer Group Policy object.
- To manage domain polices, you use Group Policy with the domain controller Group Policy object.

  To facilitate your policy management tasks, you can add the Local Computer Policy and Domain Controller Security Policy snap-ins to the Microsoft Management Console (MMC). You can also access the Account Policies and Local Policies by selecting Start- Programs- Administrative Tools- Domain Security Policy or Local Security Policy.

8.2. <u>Creating Management Console For Security Settings</u>

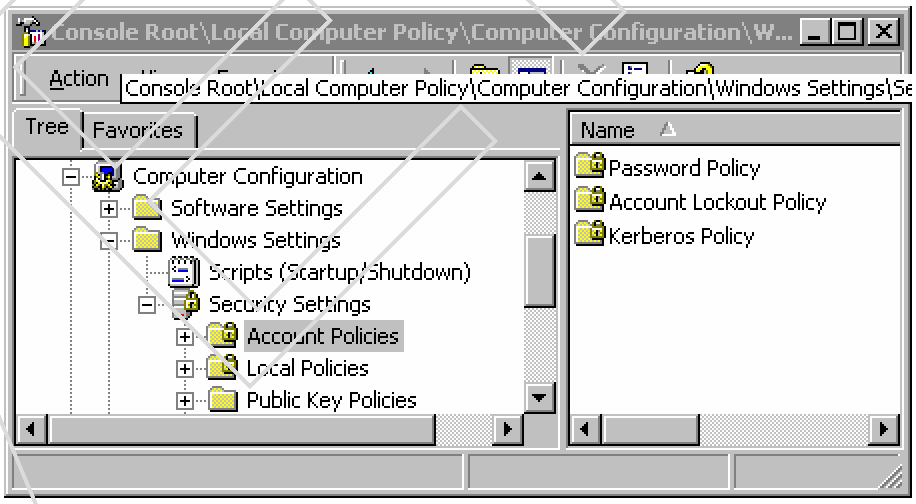
1. Click Start → Run, type MMC in the Run dialog box and click the OK button to open the MMC window.
2. From the main menu, select Console → Add/Remove Snap-in.
3. Add/Remove Snap in dialog box appears. Click the Add button.
4. Highlight the Group Policy option and click the Add button. Local Computer Policy is added in the MMC.
5. The group policy object specifies local computer by default. Click the Finish button and then click the Close button.
6. In the Add/Remove Snap-in dialog box, click the OK button.
7. From the main menu, select Console → Add/Remove Snap-in.
8. Add/Remove Snap-in dialog box appears. Click the Add button.
9. Highlight the Event Viewer option and click the Add button.

10. Select computer dialog box appears with local computer selected by default. Click the Finish button and then click the Close button.
11. In the Add/Remove Snap in dialog box, click the OK button.
12. Click Console → Save As. It saves the console *(any name)* in the Administrative Tools folder which is the default location and click the Save button.

    You can also access this console by selecting Start → Programs → Administrative Tools → Local Security Policy.

8.3. **Using Account Policies**

Account policies are used to specify the user account properties that relate to the logon process. *They allow you to configure computer security settings for passwords, account lockout specifications, and kerberos authentication within a domain. After you have loaded the Group Policy snap-in in the MMC, you will see an option for Local Computer Policy.* To access the Account Policies folder, expand the Local Computer Policy-→ Computer Configuration-→ Windows Settings-→ Security Settings-→ Account Policies.



If you are on a Windows 2000 member server, you will see two folders namely Password Policy and Account Lockout Policy. If you are on a

Windows 2000 Server computer that is configured as a Domain Controller (DC), you will see three folders namely Password Policy, Account Lockout Policy and Kerberos Policy. *The Account Policies available for member servers and domain controllers are described in the following sections.*

8.4. **Setting Password Policies**

Password policies ensure that the security requirements are enforced on the computer. It is important to note that the password policy is set on per computer basis and it cannot be configured for specific users.

The password policies, which are defined on Windows 2000 member servers are as follows:

Password Policy Options

Policy	Description	Default	Minimum	Maximum
Enforce Password History	Keeps track of user's password history	Remember 0 passwords	Same as default	Remember 24 passwords
Maximum Password Age	Maximum number of days user can keep valid password	Keep password for 42 days	Keep password 1 day	Keep password for up to 999 days.
Minimum Password Age	How long password must be kept before it can be changed.	0 days *(password can be changed immediately)*	Same as default	999 days
Minimum Password Length	Minimum number of characters password must	0 characters *(no password required)*	Same as default	14 characters

	contain			
Password must meet complexity requirements	*Allows you to install password filter*	*Disable*	*Same as default*	*Enabled*
Store pass word using reversible encryption for all user in the domain	*Specifies higher level of encryption for stored user password*	*Disabled*	*Same as default*	*Enabled*

Password Policies are used as follows:

- Enforce Password History option is used so that user can not use the same password. Users must create a new password when their password expires or is changed.
- Maximum Password Age option is used so that after the maximum password age is exceeded, users are forced to change their password.
- Minimum Password Age option is used to prevent users from changing their passwords several times in rapid succession in order to defeat the purpose of the enforce password history policy.
- Minimum Password Length option is used to ensure that the users create a password as well as to specify that it meet the length requirement. If this option isn't set, users are not required to create a password.
- Password Must Meet Complexity option is used to prevent users form using as passwords items found in a dictionary of common names.
- Store Password Using reversible encryption for all users in the domain option is used to provide a higher level of security for user passwords.

Procedure for Setting Password Policies is as follows:

1. Select Start → Programs → Administrative Tools → Local Security Policy OR

2. Expand the Local Computer Policy snap-in in the MMC.
3. Expand the folders as follows: Computer Configuration, Windows Settings, Security Settings, Account Policies and Password Policy.
4. Open the Enforce Password History policy. In the effective policy setting field, specify 5 passwords remembered and click the OK button.
5. Open the Maximum Password Age policy. In the local policy setting field, specify that the password expire in 60 days and click the OK button.

8.5. **Setting Account Lockout Policies**

The account lockout polices are as follows:

Policy	Description	Default	Minimum	Maximum
Account Lockout Threshold	Specifies number of invalid attempts allowed before account is locked out.	0 *(disabled account will not be locked out)*	Same as default	999 attempts
Account Lockout Duration	Specifies how long account will remain locked if Account Lockout Threshold is exceeded.	0; *but if account threshold is enabled, 30 minutes*	Same as default	99,999 minutes
Reset Account Lockout Counter After	Specifies how long counter will remember unsuccessful logon attempts.	0; *but if account threshold is enabled, 5 minutes*	Same as default	99,999 minutes

8.6. **Setting Kerberos Policies** *(Only for Domain Controllers)*

Kerberos version 5 is a security protocol that is used in Windows 2000 Server to authenticate users and network service. This is used for dual verification.

When a Windows 2000 Server is installed as a domain controller (DC), it automatically becomes a Key Distribution Center (KDC). The KDC is responsible for holding all of the client passwords and account information. Kerberos services are also installed on each of the Windows 2000 client and server.

The kerberos authentication involves the followings steps:

1. *The client requests authentication from the KDC using a password or smart card.*
2. *The KDC issues the client a Ticket Granting Ticket (TGT). The client can use the TGT to access the Ticket Granting Service (TGS), which allows the user to authenticate or services within the domain. The TGS issues service tickets to the clients.*
3. *The client presents the service ticket to the requested network service. This service ticket authenticates the user to the service and the service to the user, for mutual authentication.*

Kerberos Policy Options:

Policy	*Description*	*Default local setting*	*Effective setting*
Enforce user logon restrictions	*Specifies that any logon restrictions will be enforced*	*Not definer*	*Enabled*
Maximum life time for service ticket	*Specifies the maximum age of a service ticket before in must be renewed*	*Not defined*	*600 minutes*
Maximum life time for user ticket	*Specifies the maximum age for a user ticket before it must be renewed*	*Not defined*	*10 hours*
Maximum life time for user ticket renewal	*Specifies how long a ticket may be renewed before it*	*Not defined*	*7 days*

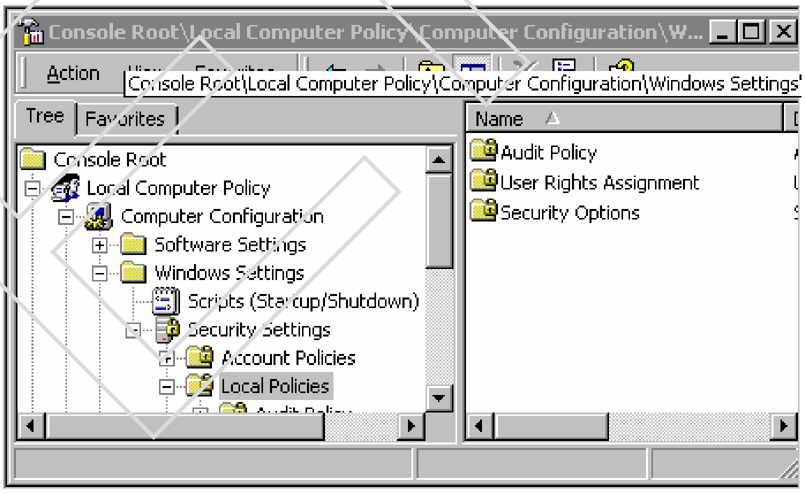
	must be regenerated		
Maximum tolerance for computer clock synchronization	*Specifies the maximum clock synchronization between the client and the KDC*	*Not defined*	*5 minutes*

8.7. **Using Local Policies**

Account Policies are used to control logon procedures and Local Policies are used to control that a user can do after logging on. *With local policies, you can implement auditing, specify user rights, and set security options*.

To use Local Policies, first add the Local Computer Policy snap-in to the MMC. Then, from MMC, to access the Local Policies folder, click Local Computer Policy, Computer Configuration, Windows Settings, Security Settings and Local Policies.

There are three folders under Local Policies: Audit Policy, User Rights Assignment and Security Options.



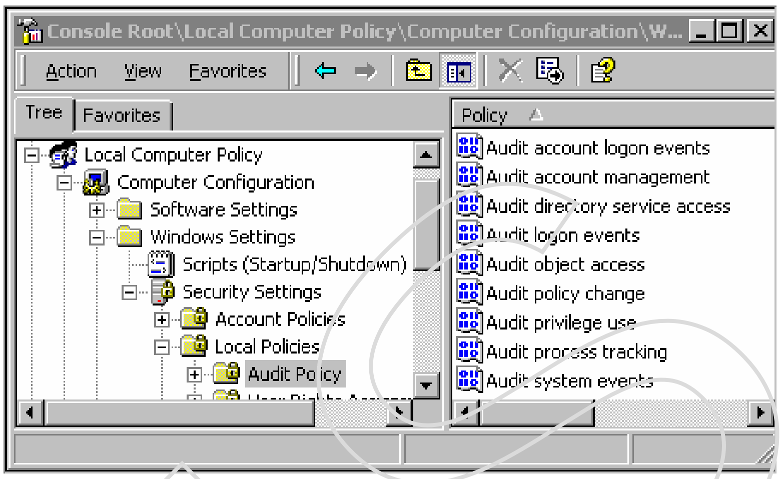
8.8. **Setting Audit Policies**:

By implementing auditing you can watch what users are doing.

You audit events that relate to user management through the audit policies. By tracking certain events, you can create a history of specific tasks, such as user creation and successful or unsuccessful logon attempts. You can also identify security violations that arise when attempt to access system management tasks that they do not have permission to access.

When you define an audit policy, you can choose to audit success or failure of specific events. The success of an event means that the task was successfully accomplished. The failure of an event means that the task was not successful accomplished.

By default, auditing is not enabled, and it must be manually configured. Once auditing has been configured, you can see the results of the audit through the event viewer utility. (The event viewer utility is covered later).



- <u>Setting Audit Polices</u>:

1. Go to the Local Computer Policy snap-in in the MMC.
2. Expand the folders as follows: Computer Configuration → Windows Settings → Security Settings → Local Policies → Audit Policy.
3. Open the Audit Account Logon Events event’s policy. In the local policy setting field, audit the attempts. Check the boxes for Success and Failure and Click the OK button.
4. Open the Audit Account Management policy. In the local policy-setting field check the boxes for success and failure and Click the OK button.
5. Log off as Administrator. Attempt to log on as different user, which does not exists. *(Means logon will fail).*
6. Log on as Administrator. Open the MMC and expand the Event Viewer snap-in.

7. From Event Viewer, open the security log. You should see the audited events listed in this log.

Audit Policy Options

Policy	**Description**
Audit Account Logon Events	Tracks when a user logs on, logs off or make a network connection.
Audit Account Management	Tracks user and group account creation, deletion and management actions.
Audit Object Access	Audits access to files, folders and printers.

8.9. **Assigning User Rights**:

The user right policies determine the rights that a user or a group has on the computer. User rights apply to the system. *They are not the same as permissions, which apply to a specific object.*

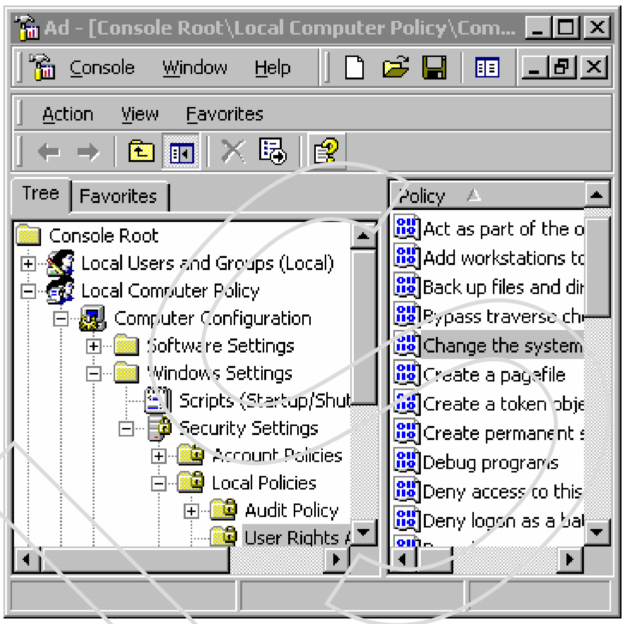
An example of a user right is the back up files and directories right. This right allows a user to back up files and folders, even if the user does not have permissions through the file system. The other user rights are similar in that they deal with system access as opposed to resource access.

User Rights Assignment Policy Options:

Right	**Description**
Access this computer from the network	*Allows a user to access the computer from the network*
Change the system time	*Allows a user to change the internal time of the computer*
Shut down the system.	*Allows a user to shut down the local windows 2000 computer.*
Log On Locally	*Allows a user to log on at the computer where the user account has been defined.*

Setting Local User Rights:

1. Go to the Local Computer Policy snap-in in the MMC.
2. Expand the folders as follows: Computer Configuration → Windows Settings → Security Settings → Local Policies → User Rights Assignment.
3. Open "Change the System Time" user right.
4. Local Security Policy Setting dialog box appears. Click the Add button.
5. Select Users or Groups dialog box appears. Select the user to whom you would like to assign right. Click the Add button and then click the OK button.



8.10. **Defining Security Options**:

Security options are used to configure security for the computer. Unlike User Rights policies, which are applied to a user or group, Security Option policies apply to the computer.

Security Options:

Option	**Description**	**Default**
Disable CTRL+ALT+DEL requirement for logon	*Allows the Ctrl + Alt + Delete requirement for logon to be disabled*	Not defined

Do not display last user name in logon screen	*Prevents the last user name in the logon screen from being displayed*	Disabled
Prompt user to change password before expiration	*Prompts the user to change the password before expiration*	14 days before password expiration.

<u>Defining Security Options</u>:

1. Go to the Local Computer Policy snap-in in the MMC.
2. Expand the folder as follows: Computer Configuration, Windows Settings, Security Settings, Local Policies, Security Options.
3. Open the policy “Do not display last user name in logon screen”. In the Local Policy Setting click Enabled.
4. Log off and log on to see the effect.

If security policy is not taking effect, then go to the Command Prompt by clicking Start-→ Programs-→ Accessories → Command Prompt and type **Secedit / refreshpolicy machine_policy** and press Enter. *It may be because the group policies are only applied periodically.*

8.11. <u>**System Policies**</u>

Through the system policies, you can control the computer’s system configuration and the user’s work environment. You can set the system policies for specific users, groups and computers, as well as for all users and all computers.

System policies are commonly associated with Windows NT 4.0. In Windows 2000 it is recommended that you use Group Policy to manage user’s Desktop settings.

System policies are configured only on domain controller and to configure on Professional computer, install AIDMINPAK utility.

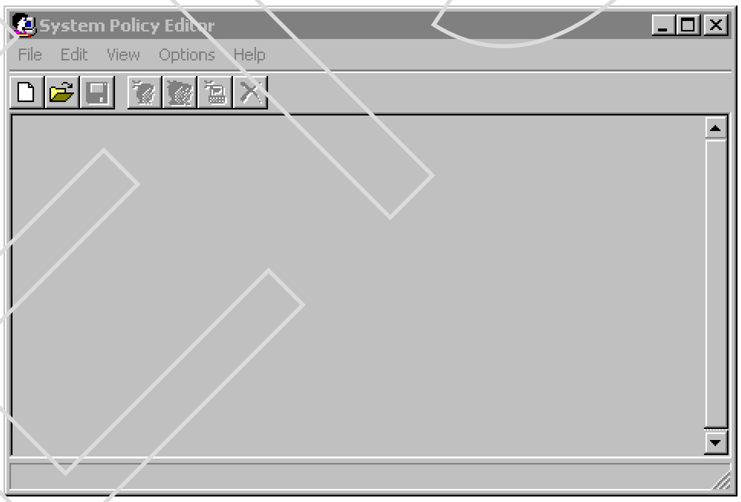
User and Group System Policy Options

Policy	*Options*
Control Panel	*Allow you to specify display settings such as hiding the screen saver.*
Desktop	*Allow you to configure wallpaper and color scheme.*
Shell	*Allow you to configure restrictions such as hiding drives.*
System	*Allow you to set restrictions such as disabling the registry editing tools.*
Windows NT Shell	*Allow you to configure Windows NT custom folders.*
Windows NT system	*Allow you to specify whether or not to parse autoexec.bat and logon scripts.*

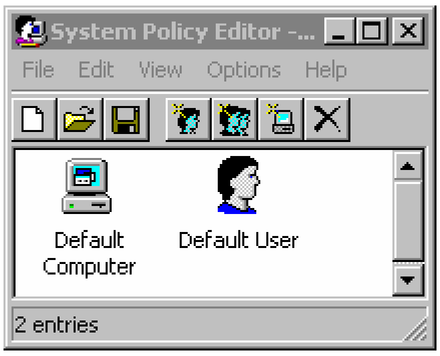
Creating a System Policy for a User or Group

To configure a system policy for a user or group, take the following steps:

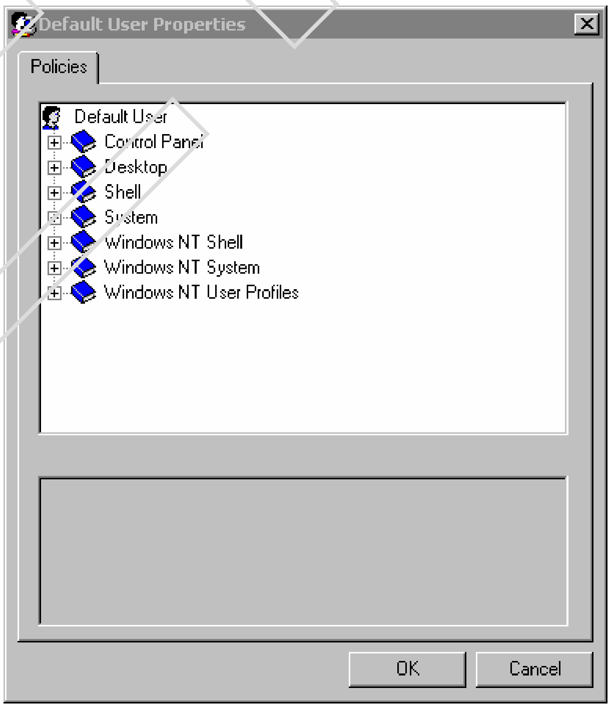
1. Select Start → Run, type POLEDIT and click the OK button.
2. System Policy Editor window opens.



3. Select File → New Policy.
4. System Policy Editor displays icons for Default Computer and Default User.



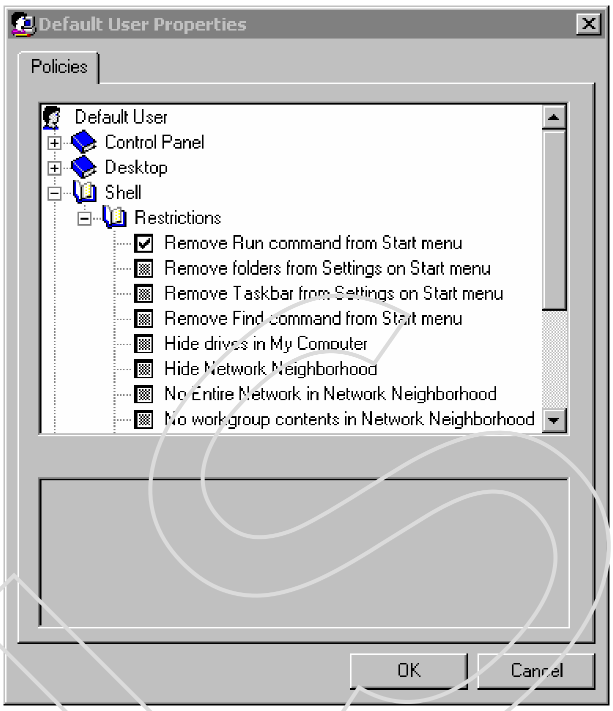
5. Select Edit → Add User (or Add Group).
6. To Add User (or Add Group) dialog box appears. You can type the name or click the browse button to select from a list of available users or groups. After adding the user or group, click the OK button.
7. *The user (or group) you selected appears in the System Policy Editor window*. To edit or view the user's or group's policy settings, double click the user or group.
8. The policies are listed under the Policies tab of the User Properties dialog box. Click an option that you want to configure.



9. List of all policies that can be defined are displayed. Check the check box to apply a policy.

You can configure each option as follows:

- *A grayed-out box indicates that no policy is applied.*
- *A check in the check box indicates that the policy should be applied.*
- *A blank (or white) check box indicates that the policy should not be applied.*



- Default User
  - Control Panel
  - Desktop
  - Shell
    - Restrictions
      - ☑ Remove Run command from Start menu
      - ▨ Remove folders from Settings on Start menu
      - ▨ Remove Taskbar from Settings on Start menu
      - ▨ Remove Find command from Start menu
      - ▨ Hide drives in My Computer
      - ▨ Hide Network Neighborhood
      - ▨ No Entire Network in Network Neighborhood
      - ▨ No workgroup contents in Network Neighborhood

10. After you have finished editing all the policies, save the policies by selecting File → Save. The policies will be saved under C:\Winnt\Sysvol|Yourdomain\Scripts\Ntconfig.Pol.

Practical

i) Crating MMC for Security Settings.

ii) Using Account Policies (Setting Password Policies and Setting Account Lockout Policies).

iii) Using Local Policies (Setting Audit Policies, Assigning User Rights and Defining Security Options).

iv) Configuring System Policies.

Exercise - 8

Q.1 Fill in the blanks:

i) The local policy, which is only available on the DC is _________. (Kerberos Policy)

ii) KDC stands for _________. (Key Distribution Centre)

iii) Account policies are used to _________. (Control logon procedures)

iv) Local policies are used to control _________. (that a user can do after logging on)

v) System policies are used to control _________. (computer's system configuration and the user's work environment)

vi) Utility used for creating System Policies is _________. (POLEDIT)

vii) You can configure System Policies on a Professional computer using _________utility. (AIDMINPAK)

Q.2 Write short Notes:

i) Accessing Local Computer Policy

ii) Account Policies

iii) Local Policies

iv) System Policies

CHAPTER 9

MANAGING DISK

9.1. **Introduction**

Through Windows 200 Server Disk Management utility, you can configure the followings:

i) File system. *(Conversion from FAT16 or FAT32 partition to NTFS).*

ii) Physical drives. *(Conversion from basic storage to dynamic storage).*

9.2. **Configuring File System**

File systems are used to store and locate the files you save on your hard disk drive.

Windows 2000 supports the FAT16, FAT32 and NTFS file systems.

You should choose NTFS to take the advantage of features such as local security, file compression and file encryption.

(i) File System Capabilities

Feature	FAT16	FAT32	NTFS
Operating system support	Most	Windows 95, 98, 2000 & OS2	Windows NT and 2000
Long filename support?	Yes	Yes	Yes
Efficient use of disk space?	No	Yes	Yes
Compression support?	No	No	Yes
Quota support?	No	No	Yes
Encryption support?	No	No	Yes

Local security support?	No	No	Yes
Network security support?	Yes	Yes	Yes
Maximum volume size	2 GB	32 GB	2 TB

Windows 2000 Server also supports CDFS (Compact Disk File System) and UDF (Universal Disk Format). However, CDFS cannot be managed. It is only used to mount and read CDs. UDF is used to read DVDs (Digital Versatile Disk).

Note: HPFS (High Performance File System) is used on Windows NT 4.0 and earlier versions.

(ii) **Converting a FAT Partition to NTFS**:

Windows 2000 provides the Convert command line utility for converting a FAT 16 or FAT 32 partition to NTFS. The syntax for the Convert command is:

```
Convert [drive:] /fs:ntfs
```

After the conversion process is completed, close the command prompt dialog box. If the conversion doesn't occur immediately, specify that the conversion should take place, next time when the computer is restarted.

9.3. Configuring Disk Storage

Windows 2000 Server supports two types of disk storage:

(i) Basic Storage- Basic storage is backward compatible with other operating systems.

(ii) Dynamic Storage- Dynamic storage is a new system that is configured as volumes.

<u>Basic storage</u>

Basic storage is backward compatible with other operating system and consists of primary and extended partitions.

The first partition that is created on a hard drive is called a primary partition. The primary partition uses all of the space that is allocated to the partition. With extended partitions you can allocate the space however you like. For example, a 500MB extended partition could have a 250MB d: partition and a 250 MB e: partition.

An advantage of using a partition on a single physical disk is that you can allocate the space however you want. For example, if you had a 1 GB physical drive and you created a single primary partition, you could allocate the space on the drive as needed. On the other hand, if you created two 500 MB partitions called C: and D:, and C: was full and D: had space left, you could not take space from the d: drive without deleting the partition first.

One of the advantages of using multiple partitions on a single physical hard drive is that each partition can have a different file system. For example, the C: drive might be fat32 and the D: drive might be NTFS. Multiple –partitions also make it easier to manage security requirements.

<u>Dynamic storage</u>:

Dynamic storage is a new feature of Windows 2000 that consists of a dynamic disk divided into dynamic volumes. *Dynamic volumes cannot contain partitions or logical drives, and they are only accessible through windows 2000 systems.*

9.4. <u>**Different Volumes of Dynamic Storage**</u>

Windows 2000 Server dynamic storage supports following types of dynamic volumes:

(i) Simple volumes

(ii) Spanned volumes

(iii) Striped volumes

(iv) Mirrored volumes

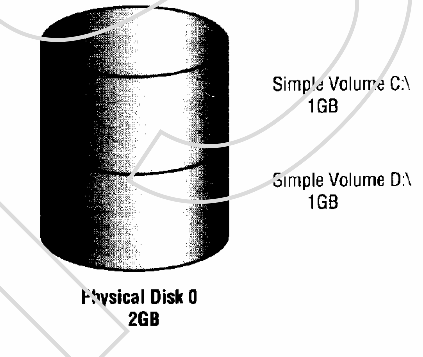
(v) RAID 5 volumes

When you install or upgrade to Windows 2000, you are using basic storage, and you cann't add volume sets, but you can upgrade from basic storage to dynamic storage.

To set up dynamic storage, you create or upgrade a disk to a dynamic disk. Then you create dynamic volumes within the dynamic disk. You create dynamic storage with the Windows 2000 Disk Management utility.

(i) Simple volumes

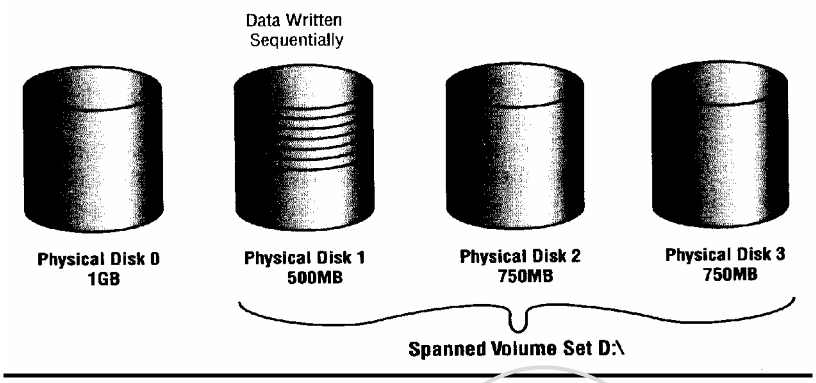
A simple volume contains space from a single dynamic drive. It can be formatted with FAT, FAT 32 or NTFS. *The space from the single drive can be contiguous (adjacent or neighbour) or non-contiguous. Simple volumes are used when you have enough disk space on a single drive to hold your entire volume.*



(ii) Spanned volumes:

Spanned volumes consist of disk space on two or more dynamic disks. Up to 32 dynamic disks can be used in a spanned volume configuration. When you create spanned volumes, the data is written sequentially, filling space on the first physical disk before writing on the next physical disk in the spanned volume set. Capacity of all the disks should be the same. *Typically, administrators use spanned volumes when they are running out of disk space on a volume and want to dynamically extend the volume with space from another hard drive. You do not need to allocate the same amount of space to the volume set on each physical drive.*

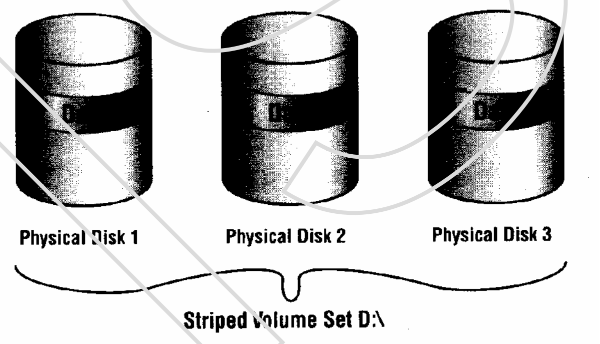
Data is written sequentially, you do not see any performance enhancement with spanned volumes.



(iii) Striped volumes

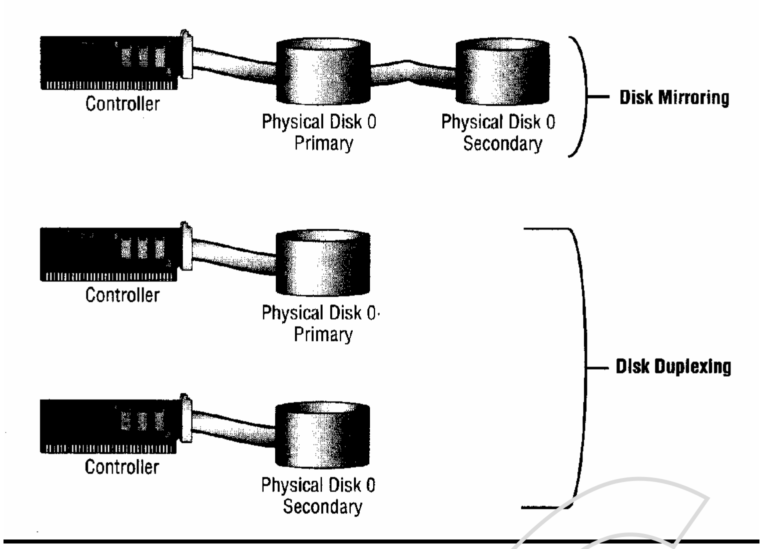
Striped volumes store data in equal stripes between two or more (up to 32) dynamic disks. Data is written sequentially in the stripes.

The main disadvantage of striped volumes in that if any drive in the striped volumes set fails, you lose access to all of the data in the striped set.



(iv) **Mirrored volumes**

Mirrored volumes are copies of two simple volumes stored on two separate physical disks. Suppose you have a primary disk and a secondary disk, the data written to the primary disk is mirrored to the secondary disk. *Mirrored volumes provide fault tolerance if one drive in the mirrored volume fails, the other drive still works with out any interruption in service or loss of data.*



(v) RAID-5 Volumes

RAID stands for Redundant Array of Inexpensive Disks. RAID-5 volumes are similar to the striped volumes. In addition, RAID-5 volumes place a parity stripe across the volume. RAID-5 volumes require at least three physical disks (up to a maximum of 32 disks), using an equal size of free space on all of the disks. *(Parity is a mathematical calculation performed on the data that provides information that can be used to rebuild data on failed drives).* If a single disk within the volume set fails, the parity information stored on the other disks can be used to rebuild the data on the failed disk.

Advantages of RAID-5

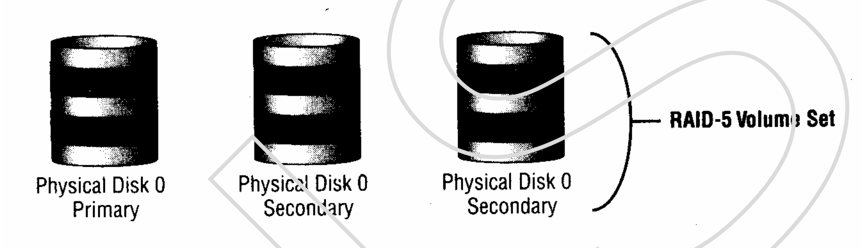
(i) Fault tolerant

(ii) Provide good performance because of multiple channels I/O.

(iii) Occupy less space for fault tolerant than mirrored volumes.

The main advantage of RAID-5 volumes is that they are fault tolerant and provide good performance because this configuration used multiple disk I/O channels. The other advantage of raid 5 volumes is that they require less disk space for fault *tolerance than mirrored volumes need. A mirrored volume set used half of the volume set to store the mirror. A RAID-5 volume set requires only the storage space of one drive in the volume set to use to store the parity information. For example, if you have three 5GB drives in a RAID-5 volume set, 5 GB of the volume set is used to store parity information, and the remaining 10 GB can store data. If your volume set contained five 5GB drives, you could use 20 GB for data and 5 GB for storing parity information.*

The main disadvantage of a RAID-5 volume is that once a drive fails. System performance suffers until you rebuild the RAID-5 volume. This is because the parity information suffers until you rebuild the RAID-5 volume. This is because the parity information must be recalculated through memory to reconstruct the missing drive. If more that one drive fails, the RAID-5 volume becomes inaccessible. At that point, you must restore your data from your backup media.



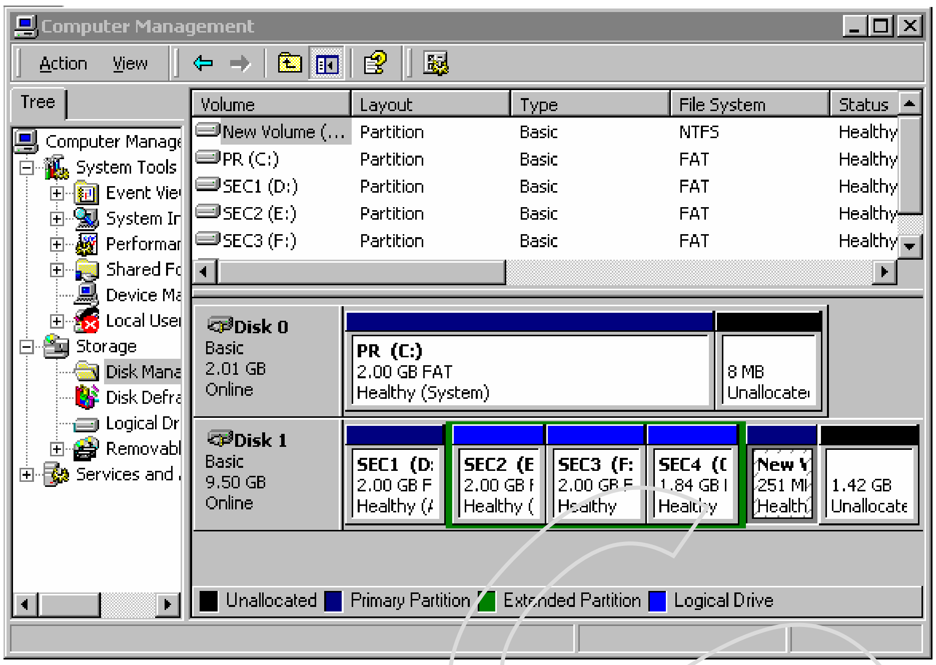
Note: In order to have full permissions to use the disk management utility, you should be logged on with administrative privileges.

9.5. **Disk Management**

The Disk Management utility is a graphical tool for managing disks and volumes. To access this utility procedure is as follows:

(i) Click Start-→ Settings-→ Control Panel-→ Administrative Tools-→ Computer Management-→Storage-→ Disk Management. OR

(ii) You can also access by right clicking My Computer, selecting Manage and expanding Computer Management, Storage and Disk Management.



Volume	Layout	Type	File System	Status
New Volume (…	Partition	Basic	NTFS	Healthy
PR (C:)	Partition	Basic	FAT	Healthy
SEC1 (D:)	Partition	Basic	FAT	Healthy
SEC2 (E:)	Partition	Basic	FAT	Healthy
SEC3 (F:)	Partition	Basic	FAT	Healthy

The main window, shows the following information:

- The volumes that are recognized by the computer.
- The type of partition, either basic or dynamic.
- The type of file system used by each partition.
- The status of the partition and whether or not the partition contains the system or boot partition.
- The capacity, or amount of space, allocated to the partition.
- The amount of free space remaining on the partition.
- The amount of overhead associated with the partition.

9.6. Managing Basic Tasks

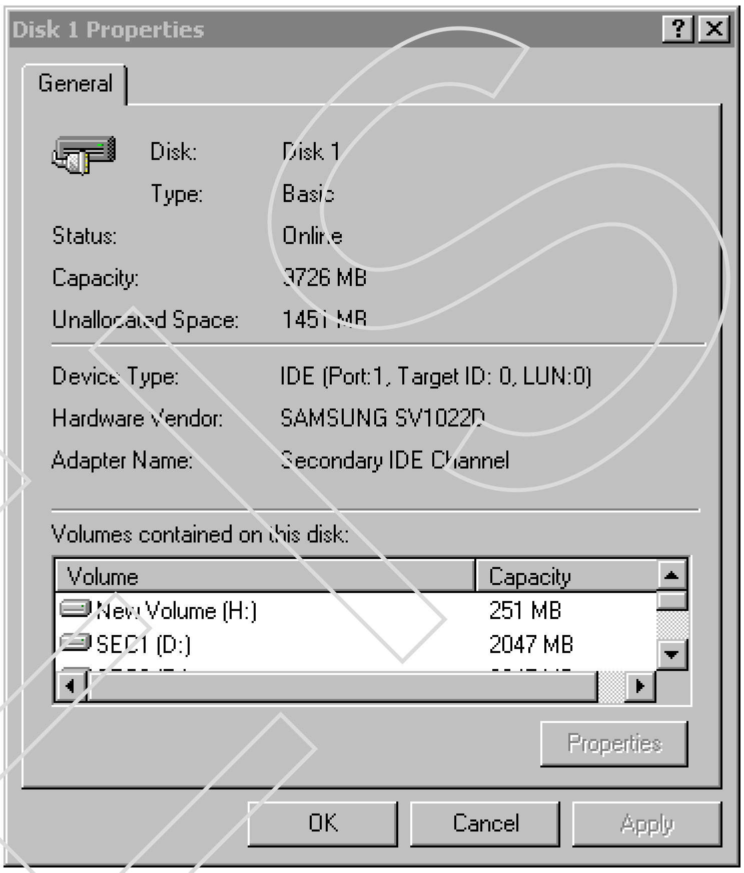
You can perform the following basic tasks:

- View disk and volume properties.
- Add a new disk.
- Create partitions and volumes.
- Upgrade a basic disk to a dynamic disk.

- Change a drive letter.
- Delete partitions and volumes.

9.7. **Disk Properties**

To view the properties of a disk, right click the disk and choose Properties from the pop up menu. This brings up the Disk Properties dialog box.



Disk: Disk 1
Type: Basic
Status: Online
Capacity: 3726 MB
Unallocated Space: 1451 MB

Device Type: IDE (Port:1, Target ID: 0, LUN:0)
Hardware Vendor: SAMSUNG SV1022D
Adapter Name: Secondary IDE Channel

Volumes contained on this disk:

Volume	Capacity
New Volume (H:)	251 MB
SEC1 (D:)	2047 MB

This dialog box displays the following disk properties:

- The Disk Number.
- The type of disk (Basic, dynamic, CD ROM, removable, DVD, or unknown)
- The status of the disk (online or offline)
- The capacity of the disk.
- The amount of unallocated space on the disk.

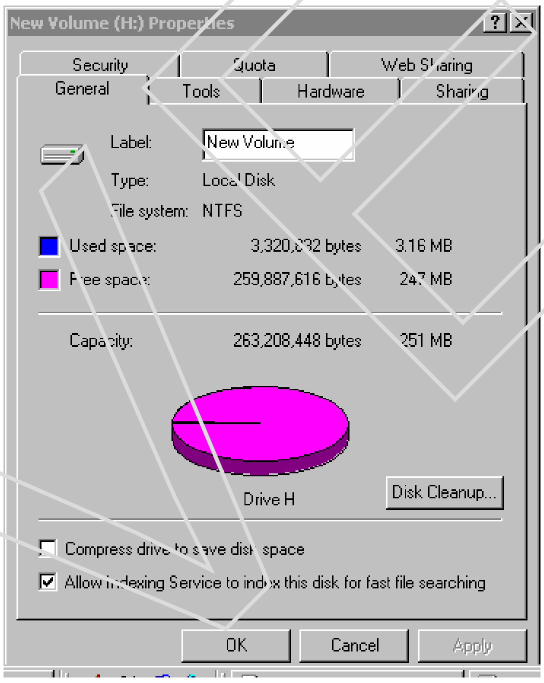
- The hardware vendor who produced the drive.
- The hardware device type
- The adapter name
- The logical volumes that have been defined on the physical drive.

9.8. Volume and Logical Disk Properties

On a dynamic disk, you manage volume properties and on a basic disk, you manage logical disk properties. Volumes and logical disks perform the same function.

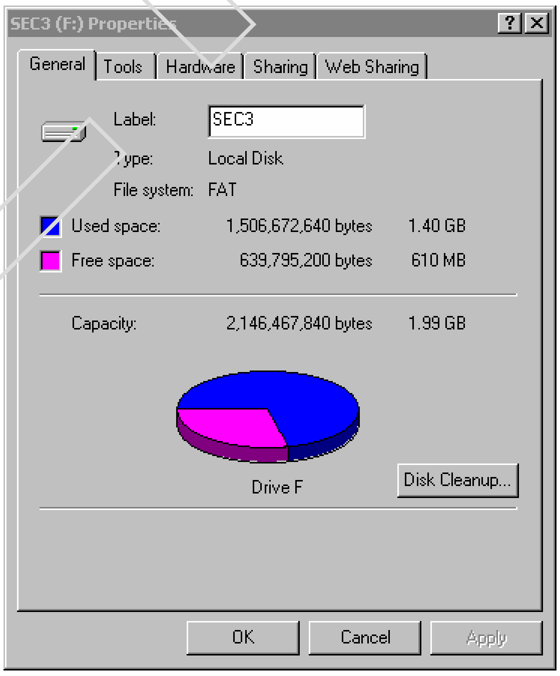
To view the properties of a logical drive, right click the logical drive and choose Properties from the pop up menu. Volume properties are organized in seven tabs for NTFS and five tabs for FAT. These are General, Tools, Hardware, Sharing, Security, Quota and Web Sharing. The Security and Quota tabs appear only for NTFS volume.

(i) General Tab: This shows the label, file system type, used and free space and capacity of


New Volume (H:) Properties

Label: New Volume
Type: Local Disk
File system: NTFS
Used space: 3,320,832 bytes 3.16 MB
Free space: 259,887,616 bytes 247 MB
Capacity: 263,208,448 bytes 251 MB

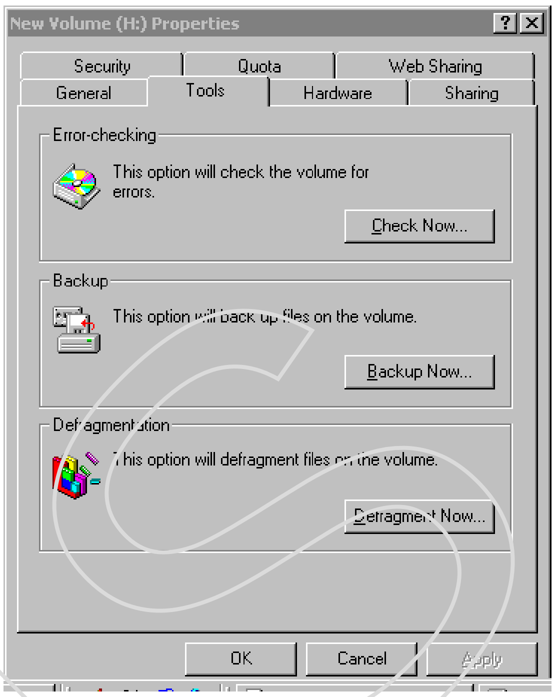
□ Compress drive to save disk space
☑ Allow Indexing Service to index this disk for fast file searching


SEC3 (F:) Properties

Label: SEC3
Type: Local Disk
File system: FAT
Used space: 1,506,672,640 bytes 1.40 GB
Free space: 639,795,200 bytes 610 MB
Capacity: 2,146,467,840 bytes 1.99 GB

the volume.

(ii) <u>Tools Tab</u>: Tools tab has three tools:



Error-checking

This option will check the volume for errors.

Backup

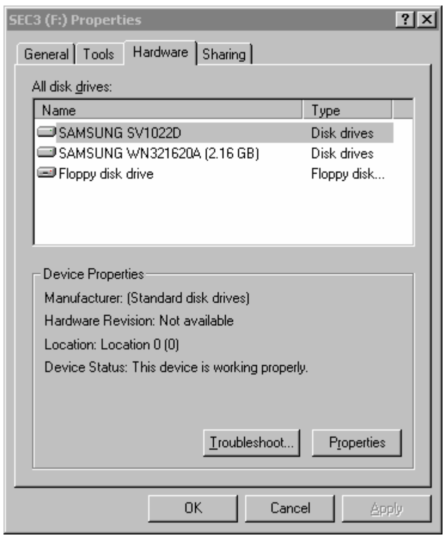
This option will back up files on the volume.

Defragmentation

This option will defragment files on the volume.

- **Error Checking** - Check the disk for errors.
- **Backup** - This backs up the files on the disk. *(Backup procedures are covered later in, "performing system recovery functions").*
- **Defragmentation** - Defragments files on the disk. *Defragmentation is covered in detail later in the "defragmenting disks" section.*

(iii) <u>Hardware Tab</u>: Displays the hardware associated with the disk drives. *For more details about a hardware item, highlight it and click the properties*



All disk drives:

Name	Type
SAMSUNG SV1022D	Disk drives
SAMSUNG WN321620A (2.16 GB)	Disk drives
Floppy disk drive	Floppy disk...

Device Properties

Manufacturer: (Standard disk drives)

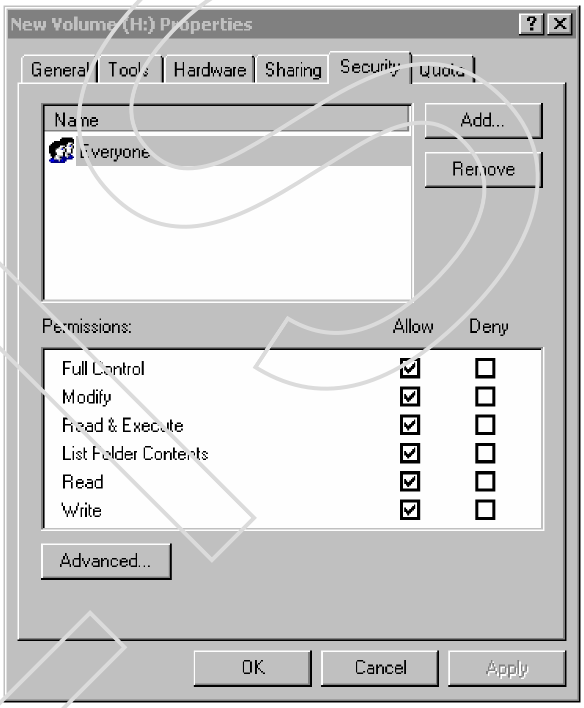
Hardware Revision: Not available

Location: Location 0 (0)

Device Status: This device is working properly.

(iv) <u>Sharing Tab</u>: Allows you to specify whether to share or not to share the disk. By default, all volumes are shared. The share name is the drive letter followed by a $ (dollar sign). The $ indicates that the share is hidden. *From this dialog box, you can set the user limit, permissions, and caching for the share. Sharing in covered in “accessing files and folders.*

(v) <u>Security Tab</u>: *The security tab of the volume properties dialog box appears only if the volume is NTFS.* The security tab is used to set the NTFS permissions for the volume. By default, Everyone group allow full control permissions at the root of the volume. *(Managing file system security is covered in later Chapter).*



Name
Everyone

Permissions:	Allow	Deny
Full Control	☑	□
Modify	☑	□
Read & Execute	☑	□
List Folder Contents	☑	□
Read	☑	□
Write	☑	□

(vi) <u>Quota Tab</u>: *The quota tab of the volume properties dialog box appears only if the volume is NTFS.* Through this tab, you can limit the amount of space for users to use within the volume. *(Quotas are covered in detail later in this chapter in the “setting disk quotas” section).*

(vii) <u>Web Sharing Tab</u>: *By default, Internet Information Services (IIS) is installed and started on a windows 2000 server computer.* If Internet Information Services (IIS) is running, you will see a tab for web sharing. *(The* *web-sharing tab is used to configure folder sharing for IIS. IIS is covered in chapter, " managing web services.")*

9.9. **Adding a New Disk**

Adding a disk depends on whether your computer supports hot swapping of drives or not.

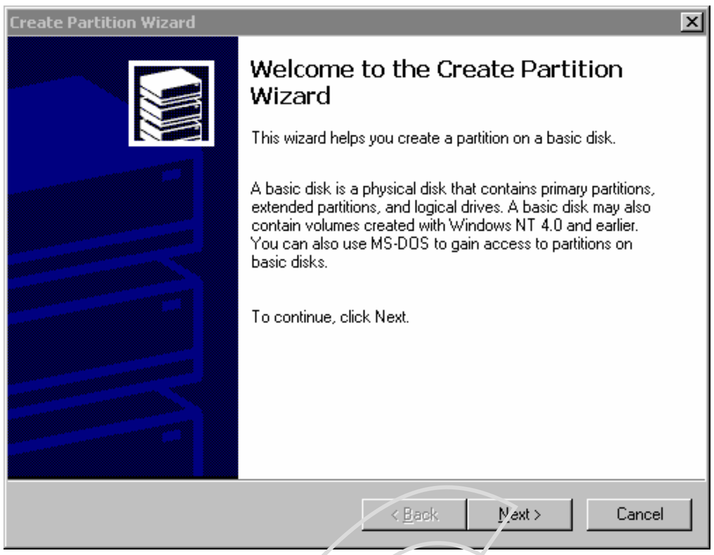
(i) Computer doesn't support hot swap: If your computer does not support hot swapping, shut down the computer and then add the disk. When you're finished, restart the computer. As soon as you will start the Disk Management utility, you will be prompted to write a signature to the disk so that Windows 2000 Server will recognize it. *By default, the new drive will be configured as a dynamic disk.*

(ii) Computer supports hot swap: If your computer supports hot swapping, you need not to turn off your computer and add the disk according to the manufacturer's directions. Then, open the Disk Management utility and select Action → Rescan disks. The new drive will appear in the Disk Management utility.

9.10. **Creating Partition**

To create a partition from unallocated space on a basic disk, use the Create Partition Wizard, which will guide you through the following steps:

1. Right click on unallocated area and choose the Create Partition Drive option from the pop up menu.



Create Partition Wizard

Welcome to the Create Partition Wizard

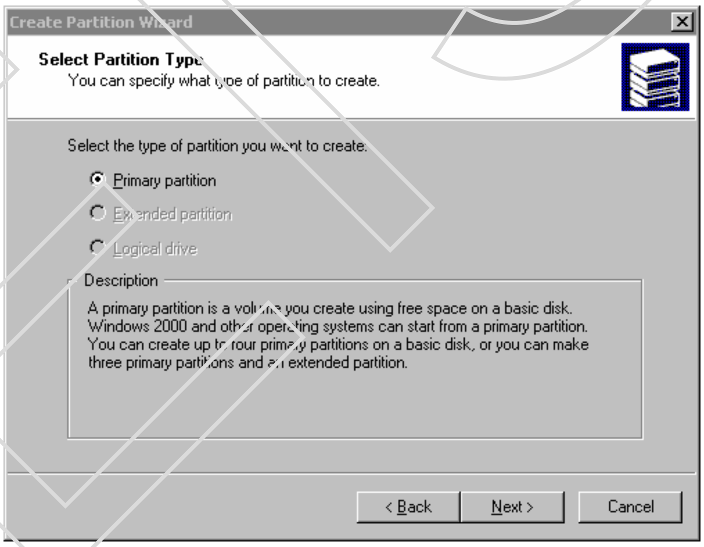
This wizard helps you create a partition on a basic disk.

A basic disk is a physical disk that contains primary partitions, extended partitions, and logical drives. A basic disk may also contain volumes created with Windows NT 4.0 and earlier. You can also use MS-DOS to gain access to partitions on basic disks.

To continue, click Next.

2. Welcome to the Create Partition Wizard dialog box appears. Click the Next button to continue.

3. Select Partition Type dialog box appears. Select the type of partition you want to create and click Next.



Create Partition Wizard

Select Partition Type

You can specify what type of partition to create.

Select the type of partition you want to create:

● Primary partition

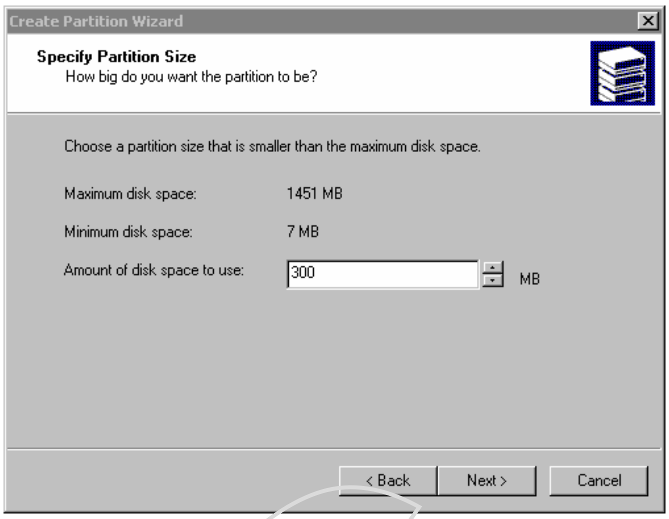
○ Extended partition

○ Logical drive

Description

A primary partition is a volume you create using free space on a basic disk. Windows 2000 and other operating systems can start from a primary partition. You can create up to four primary partitions on a basic disk, or you can make three primary partitions and an extended partition.

4. Specify Partition Size dialog box appears. Specify the partition size and click the Next button.



Create Partition Wizard

Specify Partition Size
How big do you want the partition to be?

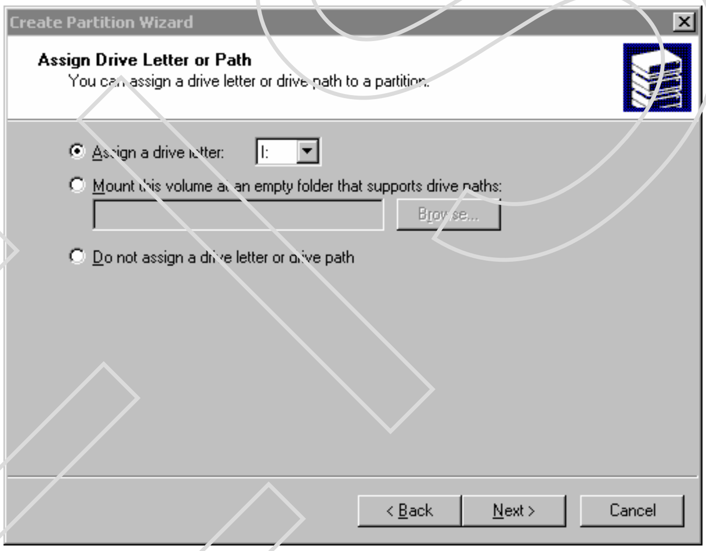
Choose a partition size that is smaller than the maximum disk space.

Maximum disk space: 1451 MB

Minimum disk space: 7 MB

Amount of disk space to use: 300 MB

5. Assign Drive Letter or Path dialog box appears. Assign the drive letter and click the Next Button.



Create Partition Wizard

Assign Drive Letter or Path
You can assign a drive letter or drive path to a partition.

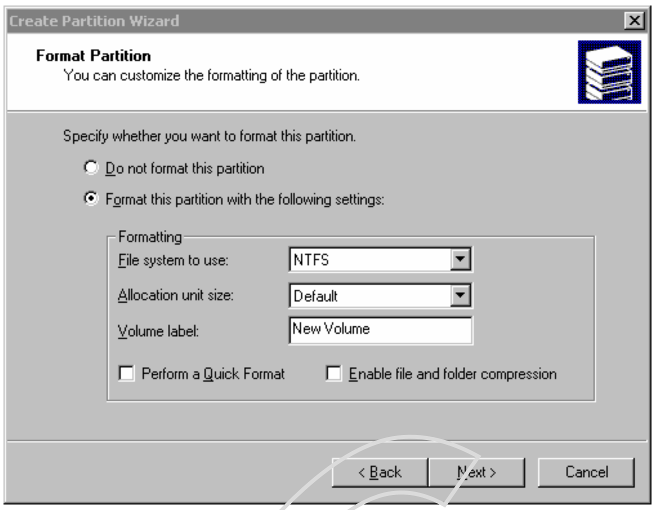
● Assign a drive letter: I:

○ Mount this volume at an empty folder that supports drive paths:

○ Do not assign a drive letter or drive path

6. Format Partition dialog box appears. Choose the file system to use (FAT, FAT 32 or NTFS) and click the Next button. *You can also select the allocation unit size, enter a volume label (for informative purposes), specify a quick format, or choose to enable file and folder compression. Specifying a quick*

format is risky, because it will not scan the disk for bad sectors (which is done in a normal format operation).



Create Partition Wizard

Format Partition

You can customize the formatting of the partition.

Specify whether you want to format this partition.

○ Do not format this partition

● Format this partition with the following settings:

Formatting

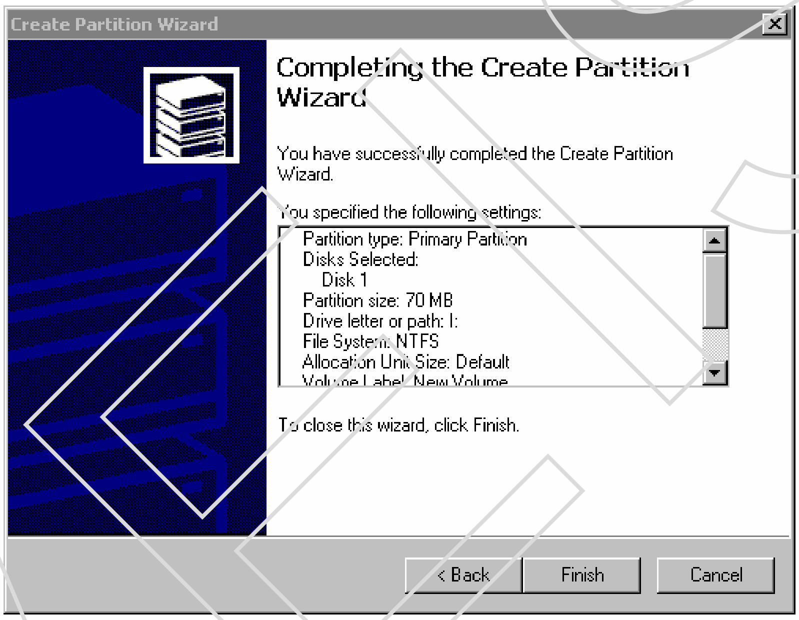
File system to use: NTFS

Allocation unit size: Default

Volume label: New Volume

□ Perform a Quick Format □ Enable file and folder compression

7. Completing the Create Partition Wizard dialog box appears. Verify the selections and click Finish.



Create Partition Wizard

Completing the Create Partition Wizard

You have successfully completed the Create Partition Wizard.

You specified the following settings:

```
Partition type: Primary Partition
Disks Selected:
  Disk 1
Partition size: 70 MB
Drive letter or path: I:
File System: NTFS
Allocation Unit Size: Default
Volume Label: New Volume
```

To close this wizard, click Finish.

9.11 **Creating Volume**

The procedure to create a volume on a dynamic disk is same as creating a partition on a basic disk. The procedure is as follows:

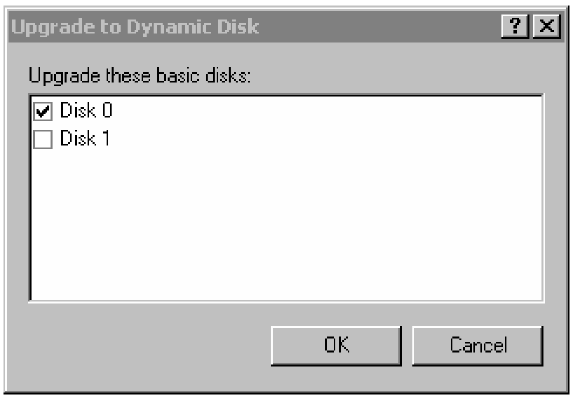
- Select Volume Type dialog box allows you to select the type of volume you want to create. *(Options include simple volume, spanned volume, striped volume, mirrored volume, or RAID-5 volume.)*
- Select Disks dialog box allows you to select the disks and the size of the volume that is being created.
- Assign Drive Letter or Path dialog box allows you to assign a drive letter or a drive path. *There is also an option to not assign a drive letter or path, but if you choose this option, users will not be able to access the volume.*
- Format Volume dialog box appears, in which specify whether or not format the volume. *If you choose to format the volume, you can select the file system, allocation unit size, and the volume label. You can also choose to perform a quick format and to enable file and folder compression.*

9.12. **Upgrading a Basic Disk to a Dynamic Disk**

Upgrading basic disk to dynamic disks is a one-way process. If you decide to revert to a basic disk, you must first delete all volumes associated with the drive. This operation is dangerous. Before you do this (or make any major change to your drives or volumes). Create a new backup of the drive or volume and verify that you can successfully restore the backup.

To upgrade to dynamic disk, the procedure is as follows:

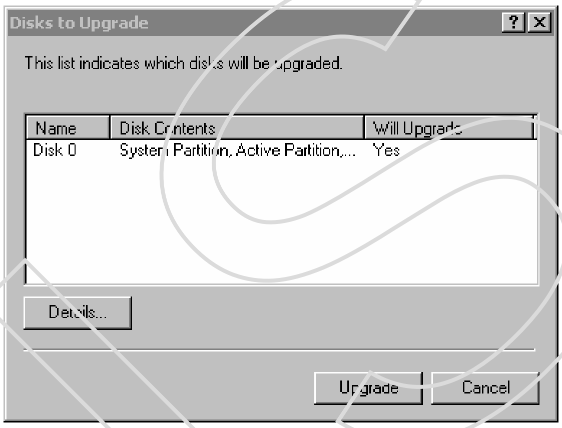
1. In the Disk Management utility, right click the physical disk you want to convert and select Upgrade to Dynamic Disk option from the pop-up menu.
2. Upgrade to Dynamic Disk dialog box appears. Select the disk that you want to upgrade and click the OK button.



Upgrade these basic disks:

☑ Disk 0
□ Disk 1

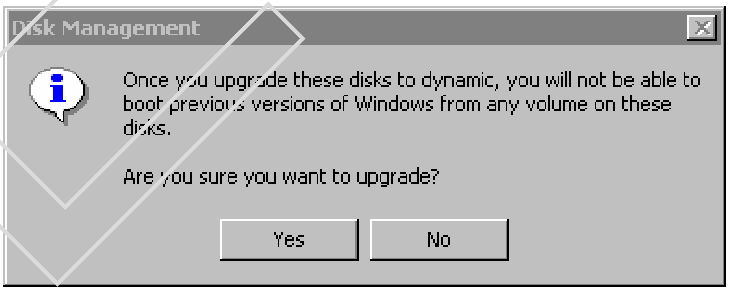
3. Disks to Upgrade dialog box appears. Click the Upgrade button.



This list indicates which disks will be upgraded.

Name	Disk Contents	Will Upgrade
Disk 0	System Partition, Active Partition,...	Yes

4. A Confirmation dialog box warns you that you will not be able to boot from previous versions of windows from this disk. Click the Yes button to continue.



Once you upgrade these disks to dynamic, you will not be able to boot previous versions of Windows from any volume on these disks.

Are you sure you want to upgrade?

5. Another Confirmation dialog box warns you that all the file systems mounted on the disk will be dismounted. Click the Yes button to continue.

6. An Information dialog box tells you that a reboot is required to complete the upgrade. Click the OK button. Your computer will restart and the disk upgrade process will be completed.

9.13. **Changing the Drive Letter**

Suppose that you have drive C: assigned as your first partition and drive D: assigned as your CD d rive. You add a new drive and partition it as a new volume. By default, the new partition is assigned as drive E: if you want your logical drives to appear before the CD drive, you can use the disk management utility's change drive letter and path option to rearrange your drive letters.

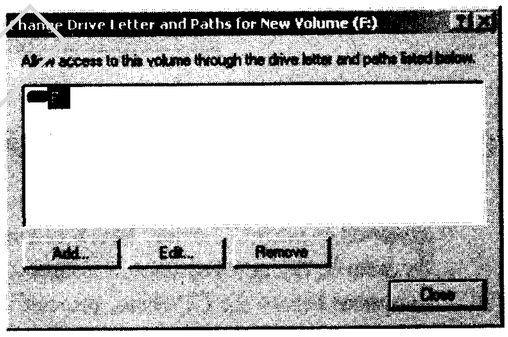
To reassign/change the drive letters proceed as follows:

(i) Go to the Disk Management utility.

(ii) Right click the drive, for which you want to change the drive letter.

(iii) Choose, Change Drive Letter and Path option from the pop-up menu.

(iv) Change Drive Letter and Path dialog box appears. Click the Edit button.



Change Drive Letter and Paths for New Volume (F:)

Allow access to this volume through the drive letter and paths listed below.

(v) Edit Drive Letter or Path dialog box appears. Use the drop down list to assign a drive letter. Select the drive letter you want to assign to the volume and finally, confirm the change when prompted.

Note: You cannot change the drive letter for boot partition.

9.14. **Deleting Partitions and Volumes**

You would delete a partition or volume if you wanted to reorganize your disk or make sure that data would not be accessed. Once you delete a partition or volume, it is gone forever.

To delete a partition or volume, in the Disk Management window, right click the partition or volume and choose the Delete volume or Delete partition option from the pop-up menu. *You will see a dialog box warming you that all the data on the partition or volume will be lost, click yes to confirm that you want to delete the volume or partition.*

Practical

(i) Converting FAT or FAT 32 to NTFS.

(ii) Creating partition.

(iii) Changing the drive letter.

(iv) Deleting the partition.

Exercise - 9

Q.1 Fill in the blanks:

i) CDFS stands for ________. (Compact Disk File System)

ii) UDF stands for ________. (Universal Disk Format)

iii) DVD stands for ________. (Digital Versatile Disk)

iv) Windows 2000 supports ________ file systems. (FAT, FAT 32, NTFS, CDFS and UDF)

v) FAT is converted to NTFS by ________ utility. (Convert)

vi) Two types of disk storage supported by Windows 2000 are ________. (Basic storage and Dynamic storage)

vii) Different volumes of dynamic storage are ________. (Simple, Spanned, Stripped, Mirrored and RAID-5)

viii) RAID stands for ________. (Redundant Array of Inexpensive Disks)

ix) Disk Management utility can be accessed by ________. (Clicking Start-→ Programs-→ Administrative Tools-→ Computer Management-→ Storage)

x) Two tabs, which are available only on the NTFS partitions are ________. (Quota and Security)

Q.2 Write short Notes.

i) Different volumes of Dynamic Storage

ii) RAID-5

iii) Disk Management

iv) Converting FAT partition to NTFS

v) File System capabilities

vi) File systems supported by Windows 2000

vii) UDF

CHAPTER 10

MANAGING DYNAMIC STORAGE

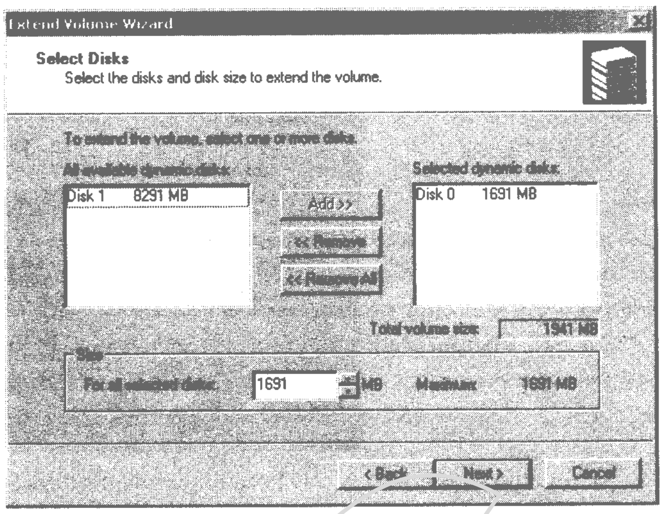
10.1. **Managing Dynamic Storage**

The disk management utility offers limited support for managing basic storage. You can create, delete and format partitions on basic drives. Most other disk management tasks require dynamic disks.

Dynamic disk overcomes the partition limitation which is in the basic disk. A dynamic disk can contain simple, spanned, stripped, mirrored or RAID-5 volumes. Through the disk management utility, you can create volumes of each type. You can also create an extended volume by the process of adding disk space to a single simple volume.

10.2. **Creating Extended Volumes**

When you create an extended volume, you are adding more disk space to the volume from the free space that exists on the same physical hard disk. When the volume is extended, it is displayed as a single drive letter. In order to extend a volume, the simple volume must be formatted as NTFS. You cannot extend a system or boot partition and the volumes that were originally created as basic disk partition and then converted to dynamic disk.



Extend Volume Wizard

Select Disks

Select the disks and disk size to extend the volume.

To extend the volume, select one or more disks.

All available dynamic disks: Disk 1 8291 MB

Selected dynamic disks: Disk 0 1691 MB

Total volume size: 1941 MB

Size

For all selected disks: 1691 MB Maximum: 1691 MB

The steps are as follows to create extended volumes:

(i) In the Disk Management utility, right click the volume you want to extend and choose the Extend Volume option from the pop-up menu.

(ii) Extend Volume Wizard starts. Click the Next button.

(iii) Select Disks dialog box appears. Select the disk that you want to use for the extended volume and click the Next button.

(iv) Completing the Extend Volume Wizard dialog box appears. Click the Finish button.

10.3. **Creating Spanned Volumes**

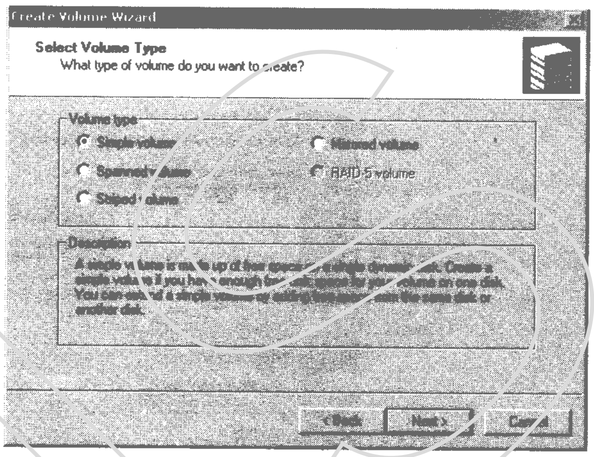
When you create a spanned volume, you are forming a new volume form scratch that includes space from two or more physical drives, up to a maximum of 32 drives. You can create spanned volumes that are formatted as FAT, FAT32 or NTFS. In order to create a spanned volume, you must have at least two d rives installed on your computer and each drive must contain unallocated space.

The steps are as follows:

(i) In the Disk Management utility, right-click an area of unallocated space on the disk and select Create Volume option from the pop-up menu.

(ii) Create Volume Wizard starts. Click the Next button.

(iii) Select Volume Type dialog box appears. Select the Spanned Volume radio button and click the Next button.



Create Volume Wizard

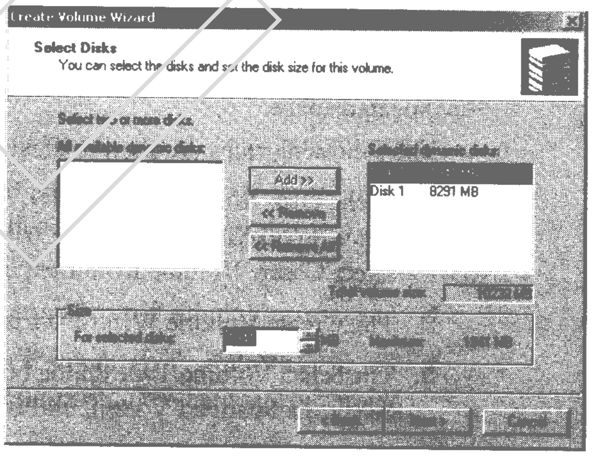
Select Volume Type

What type of volume do you want to create?

Description

A simple volume is made up of free space on a single dynamic disk. Create a simple volume if you have enough free disk space for your volume on one disk. You can extend a simple volume by adding free space from the same disk or another disk.

(iv) Select Disks dialog box appears. By default, the disk that you originally selected to create the spanned volume is selected. You need to select at least one other dynamic disk by highlighting the disk and clicking the Add button. The disks that you select appear in the selected dynamic disks list box. When you have added all of the disks that will make the spanned volume, click the Next button.



Create Volume Wizard

Select Disks

You can select the disks and set the disk size for this volume.

Select two or more disks.

Selected dynamic disks:

Disk 1 8291 MB

(v) Assign Drive Letter or Path dialog box appears. Specify a drive letter, mount the volume at an empty folder that supports drive paths or choose Not to assign a drive letter or drive path and then click the Next button.

(vi) Format Partition dialog box appears. You can choose whether or not you will format the partition and if so what file system will be used. After you’ve made your choices, click the Next button.

(vii) Completing the Create Volume Wizard dialog box appears, offering you the opportunity to verify your selections. If you need to make changes, click the Back button. If the configuration is correct, click the Finish button. *In the disk management window, you will see that the spanned volume consists of two or more drives that share a single drive letter, as in the example notice that in the example, the disks that make up the spanned volume are unequal in size.*

10.4. Creating Striped Volumes

When you create a striped volume, you are forming a new volume that combines free space of 2 to 32 drives into a single logical partition. Data in the striped volume is written across all drives in stripes of 64 KB (Data in spanned and extended volumes is written sequentially). In order to create a striped volume, each drive must contain unallocated space. The free space on all drives must be equal in size.

The procedure for creating striped volume is same as for the spanned volume.

10.5. Creating Mirrored Volumes

When you create a mirrored volume, you are setting up two physical drives that contain volumes that mirror each other. You create mirrored volumes from areas of space on the two drives. To create a mirrored volume, you must have at least two disks installed on your computer and each disk must contain unallocated space. Mirrored volumes require that the space on each disk used for the mirror set must be equal in size.

The procedure for creating mirrored volume is same as for the spanned volume.

Exercise - 10

Q.1 Write short notes

(i) Dynamic disk

(ii) Procedure to create spanned volume

CHAPTER 11

RECOVERING FROM DISK FAILURE

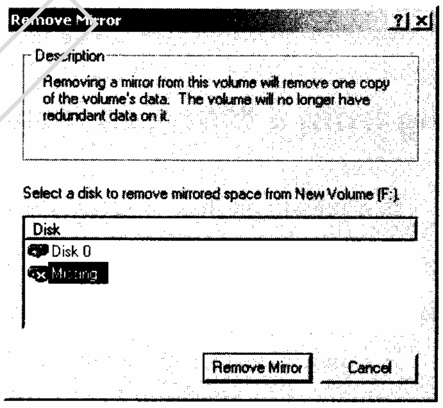
11.1. **Introduction**

If the failure occurs on a simple, extended, spanned or striped volume, you will need to restore your data from your last backup.

You will see a system error and an error in event viewer. Also, in the disk management utility, the failed volume will be indicated by the description-failed redundancy. If the disk that failed was part of a mirrored volume set, you need to remove and recreate the failed volume. If the disk was part of a RAID 5 volume set, you need to repair the volume.

11.2. **Recovering From a Mirrored Volume Failure**

To recover from a mirrored volume failure, remove the volume that failed and then recreate the volume. You can perform these tasks through the Disk Management utility.



Removing a mirror from this volume will remove one copy of the volume's data. The volume will no longer have redundant data on it.

Select a disk to remove mirrored space from New Volume (F:).

Disk
Disk 0
Missing

(a) Recovering From a Mirror Failure on Data Volume

If a drive fails in a mirrored volume set that contains only the data (It does not contain your system or boot partition), follow the following steps:

(i) Go to the Disk Management utility.

(ii) Right click the failed mirrored volume *(marked as failed redundancy)* and choose, Remove Mirror from the pop up menu.

(iii) Remove Mirror dialog box appears. Select the disk that will be removed from the mirrored volume and click the Remove Mirror button.

(iv) Confirmation dialog box appears. Click the Yes button. The remaining disk will become a simple volume.

(v) Remove the failed hard disk from the computer and replace the disk

(vi) Use the Disk Management utility to recreate the mirrored volume.

(b) <u>Recovering from a Mirror Failure on Boot Partition</u>:

If a drive fails in a mirrored volume set that contains the boot partition, you must first determine if the failed drive is the primary drive (the one with the original data) or the secondary drive (the one with the mirrored data) in the set. If the secondary disk fails, you can remove the failed disk and replace it and then recreate the mirrored volume *(As you do to recover from a failed mirrored volume set containing only data).*

If the primary disk fails which contains the boot partition, then boot from the startup disk and recover as for a failed data volume.

If the primary drive fails and it contains the boot partition, then recovery becomes more complex, because the BOOT.INI file, which is used during the windows 2000-boot process, contains the location of the boot partition. If this file points to the failed partition, Windows 2000 Server will not boot. To recover from this type of failure, you will need a windows 2000 server boot disk with a BOOT.INI file that point to the secondary drive in the mirrored set. Then you can follow the same steps as you would to recover from a failed data volume.

11.3. **Recovering From a RAID-5 Volume Failure**

If a drive in a RAID-5 volume set fails, you will still be able to access your volume set; however, your system performance will degrade significantly and you will need to re-crate the missing data through the parity information.

Steps to recover from a RAID-5 volume failure are as follows:

(i) Replace the failed hardware.

(ii) Open the Disk Management utility. Right click the failed RAID-5 volume set (marked as Failed Redundancy) and choose Repair Volume from the pop-up menu.

(iii) Repair RAID-5 Volume dialog box appears. Choose the disk that you have replaced and click the OK button to regenerate the RAID-5 volume set.

Exercise - 11

Q.1 Explain procedure

(i) To recover from mirror volume

(ii) To recover from RAID-5 volume failure.

CHAPTER 12

MANAGING DATA COMPRESSION, DISK QUOTA, ENCRYPTION AND DECRYPTION

12.1. **Data Compression**

Data compression is the process of storing data in a form that takes less space than uncompressed data. With Windows 2000 Server data compression is possible only on the NTFS partitions.

Both files and folders in the NTFS file system can be compressed or uncompressed. Files and folders are managed independently, which means that compressed folder could contain compressed files and an uncompressed folder could contain compressed files.

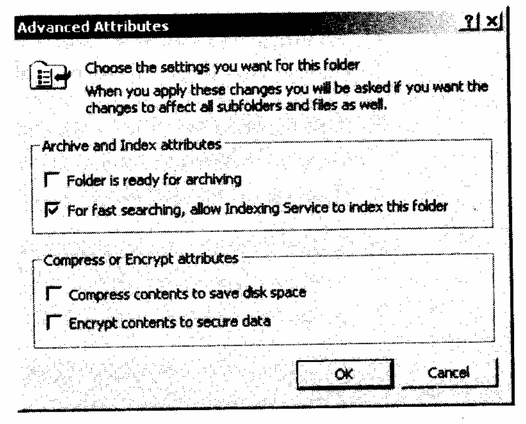
Access to compressed files by DOS or windows applications is transparent. For example, if you access a compressed file through Microsoft word, the file will be uncompressed automatically when it is opened, and then automatically compressed again when it is closed.

Data compression is only available on NTFS partitions. If you copy or move a compressed folder or file to a FAT partition (or a floppy disk) windows 2000 will automatically uncompress the folder or file.

You cannot have a folder or file compressed and encrypted at the same time.

12.2. **Steps to Compress a File or Folder**

1. Right click the folder or file you wish to compress and select Properties form the pop up menu.
2. Properties dialog box appears. Click the Advanced button under the General tab.
3. Advanced Attributes dialog box appears. Check the “Compress contents to save disk space” check box and then click the OK Button.



Choose the settings you want for this folder

When you apply these changes you will be asked if you want the changes to affect all subfolders and files as well.

Archive and Index attributes

□ Folder is ready for archiving

☑ For fast searching, allow Indexing Service to index this folder

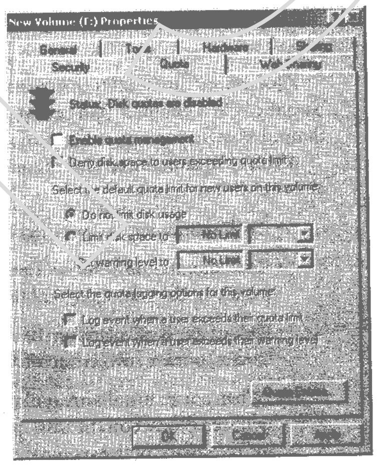
Compress or Encrypt attributes

□ Compress contents to save disk space

□ Encrypt contents to secure data

4. Confirm Attribute Changes dialog box appears. Specify whether you want to apply encryption to this folder only or to its subfolders and files also and click the OK button.

12.3. **Disk Quota**



Status: Disk quotas are disabled

□ Enable quota management

□ Deny disk space to users exceeding quota limit

Select the default quota limit for new users on this volume:

● Do not limit disk usage

○ Limit disk space to No Limit

○ Set warning level to No Limit

Select the quota logging options for this volume:

□ Log event when a user exceeds their quota limit

□ Log event when a user exceeds their warning level

Disk quota is used to specify how much disk space a user is allowed on NTFS volumes. You can specify disk quotas for all users, group of users or individual user.

Before you administer disk quotas, you should be aware of the following points:

- *Disk quotas can be specified only for NTFS volumes.*
- *Disk quotas apply at the volume level, even if the NTFS partitions reside on the same physical hard drive.*

- *Disk usage is calculated on the file and folder ownership. When a user creates, copies or takes ownership of a file, that user is the owner of the file.*
- *When a user installs an application, the free space that the application will see is based on the disk quota availability, not the actual amount of free space on the volume.*
- *Disk quota space used is based on actual file size. There is no mechanism to support or recognize file compression.*

12.4. **Configuring Disk Quotas**

You configure disk quotas through the NTFS volume properties dialog box. You learned that you can access the Volume Properties dialog box in the Disk Management utility by right clicking the drive letter and selecting Properties from the pop up menu. Then click Quota tab.

Another way to access this dialog box is from Windows Explorer – just right click the drive letter in the listing and select Properties. In the Volume Properties dialog box, click the Quota tab to see the dialog box. When you open the quota tab, you will see that disk quotas are disabled by default.

- To assign the disk quota, right click the drive letter and select Properties.
- Volume Properties dialog box appears. Click the Quota tab.

Disk quota configuration options:

Option	**Description**
Enable quota management	Specifies that the quota management is enabled for the volume.
Deny disk space to users exceeding quota limit	Specifies that the users who exceed their disk quota will not be able to override their disk allocation. Those users will receive “out of disk space” message.

Select the default quota limit for new users on this volume	Allow you to specify quota limits and warning level for new users.
Select the quota logging options for this volume	Allows you to record log events.

Notice the traffic light icon in the upper left corner of the quota tab. The traffic light indicates the status of disk quotas, as follows:

- *A red light specifies that disk quota is disabled.*
- *A yellow light specifies that a windows 2000 server is rebuilding disk quota information.*
- *A green light specifies that the disk quota system is enabled and active.*

12.5. **Setting Default Quotas**

When you set default quota limits for new users on a volume, the quotas apply only to the users who have not yet created files on that volume. This means that the users who already own files or folders on the volume will be exempted from the quota policy.

Users who have not created a file on the volume will be bound by the quota policy.

Procedure to Set the Default Quota Limit

(i) Access the Quota tab of the Volume Properties dialog box.

(ii) Check the “Enable quota management” check box.

(iii) Click the “Limit disk space to” radio button and enter the size *[Size number in the first box and in the drop down list in the second box, specify whether disk space is limited by KB (Kilobytes), MB (Megabytes), GB (Gigabytes), TB (Terabytes), PB (Peta bytes), or EB (Exabytes)].* If you choose to limit disk space, you can also set a warning level, so that the users will be warned if they approach close to their quota limit.

(iv) Click Apply and then click OK.

Applying Default Quota Limits

1. Use the Local Users and Groups utility to create a new user: Mahesh. Deselect the “User must change password at next logon” option.
2. Log off as administrator and log on as Mahesh. Drag and drop some folders to NTFS drive.
3. Log on as administrator. Open My Computer.

   or

4. Select Start → Programs → Accessories → Windows Explorer- → My Computer
5. Right click the NTFS drive and select Properties.
6. Local Disk Properties dialog box appears. Select the Quota tab.
7. Check the “Enable quota management” and the “Deny disk space to users exceeding quota limit” check boxes.
8. Click the “Limit disk space to” radio button. Specify 5MB as the limit. Specify the “Set warning level to” a value as 4MB.
9. Click the Apply button and then click the OK button.
10. If you currently have data stored on the volume, you will see a disk quota dialog box specifying that the volume will need to be rescanned. Click the OK button.

11. Log off as administrator and log on as Mahesh. Drag and drop some folders to NTFS drive. If the disk quota limit is exceeded, then it will give a message “out of disk space”.

12. Log off as Mahesh and log on again as administrator.

12.6. **Setting an Individual Quota**

You can also set quotas for individual users. There are several reasons for setting quotas in this way:

- *You can allow a user who routinely updates your applications to have unlimited disk space, while restricting other users.*
- *You can set warning level for a user who routinely exceeds disk space.*
- *You can apply the quota to users who already had files on the volume before the quota was implemented and thus have been granted unlimited disk space.*

Procedure to Set an Individual Quota Limit

(i) Click the Quota entries button under the Quota tab in the Volume Properties dialog box *in the bottom right corner under the quota tab.*

(ii) Quota Entries dialog box appears. Click Quota on menu bar and select New Quota Entry option.

(iii) Select Users dialog box appears. Select the user from the list and click the Add button and then click OK button.

(iv) Add New Quota Entry dialog box appears. You can specify whether or not the user disk space should be limited. Set the quota limit and the warning level and then click OK.

Note*: You can also modify the quotas of several users at once by CTRL + CLICKING to highlight several users and selecting quota properties.*

Modifying Individual User's Quota Limit:

(iii) Click the Quota entries button under the Quota tab in the Volume Properties dialog box *in the bottom right corner under the quota tab.*

(iv) Quota Entries dialog box appears. Double click the user whose quota you want to modify.

(v) Quota Settings dialog box appears. You can specify whether or not the user disk space should be limited. Set the quota limit and the warning level and then click OK.

Applying Individual Quota Limits

1. Open My Computer.

   or

2. Select Start → Programs → Accessories → Windows Explorer.
3. Right click the NTFS drive and select Properties.
4. Local Disk Properties dialog box appears. Select the Quota tab and then click the Quota entries button.
5. Quota Entries dialog box appears. Click Quota on the menu bar and select New Quota Entry option.
6. Select Users dialog box appears. Select the user from the list and click the Add button and then click the OK button.
7. Add New Quota Entry dialog box appears. Set the quota limit and the warning level and then click OK button.

12.7. **Monitoring Disk Quota**

You can monitor the disk quotas through the Quota Entries dialog box, which appears when you click the Quota entries button under the Quota tab of the Volume Properties dialog box. Quota Entries dialog box shows the following information:

i) The status of the user's disk quota. Status icon includes:

- Green arrow which indicates that the status is OK.

- Yellow triangle which indicates that the warning threshold has been exceeded.

- Red circle which indicates that the user threshold has been exceeded.

ii) The name and logon name of the user who has stored the files on the volume.

iii) The amount of disk space that the user has used on the volume.

iv) The user's quota limit.

v) The user's warning level.

vi) The percent of disk space that the user has used in relation to their disk quota.

12.8. **Managing Data Encryption with EFS (Encrypting File System)**

Data encryption increases the data security. Encryption translates the data into code that is not easily accessible. Encryption is possible on NTFS file system only.

Once data has been encrypted, you must have a password or key to decrypt the data. Unencrypted data is known as plain text and encrypted data is known as cipher text.

The Encrypting File System (EFS) is the windows 2000 technology that is used to store encrypted files on NTFS partitions. Encrypted files add an extra layer of security to your file system. A user with the proper key can transparently access encrypted files. A user without the proper key is denied access. There is a recovery agent that can be used by the administrator if the owner is unavailable to provide the proper key to decrypt folders or files. You can encrypt and decrypt file through the volume properties dialog box or by using the cipher utility.

12.9. **Encrypting and Decrypting Folders or Files**

To use EFS, a user specifies that a folder or file on an NTFS partition should be encrypted. The encryption is transparent to the user, who has access to the file. However, when other users try to access the file, they will not be able to unencrypt the file – even if those users have full control NTFS permissions. Instead, they will receive an error message.

To encrypt a folder or a file proceed as follows:

1. Right click the folder or file you wish to encrypt and select Properties.
2. Folder Properties dialog box appears. Under General tab click the Advanced button.
3. Advanced Attributes dialog box appears. Check the “Encrypt contents to secure data” check box and click the OK button.
4. Confirm Attribute Changes dialog box appears. Specify whether you want to apply encryption to this folder only or to its subfolders and files also and click the OK button.

To decrypt folders and files, repeat the same steps as stated above, but uncheck “Encrypt contents to secure data” check box in the Advanced Attributes dialog box.

12.10. **Using the CIPHER Utility**

CIPHER is a command line utility that can be used to encrypt and decrypt files or folders on NTFS volumes.

Syntax: CIPHER [Options] [Folder]

/e – For encrypting files and folders

/d – For decrypting files and folders

Parameter	***Description***
/e	*Specifies that files or folders should be encrypted.*
/d	*Specifies that files or folders should be decrypted*
/s:dir	*Specifies that subfolders of the target folder should also be encrypted or decrypted based on the option specified.*
/I	*Causes any errors that occur to be ignored. By default, the CIHPHER utility stops whenever an error occurs.*
/f	*Forces all files and folders to be encrypted or decrypted, regardless of their current state.*
/q	*Runs in a quiet mode and displays only the most important information.*

12.11. **Disk Defragmenter Utility**

This utility is used to bring the scattered pieces of files together.

To access this utility, select Start → Programs → Accessories → System Tools → Disk Defragmenter.

Data is normally stored sequentially on the disk where ever space is available. Fragmentation occurs naturally as users create, delete and modify files. The access of non-contiguous data is transparent to the user. However, when data is stored in this manner, the operating system must search through the disk drive to access all of the pieces of a file. This slows down data access.

12.12. **Analyzing Disk**

To analyze a disk open the Disk Defragmenter utility, select the drive to be analyzed and click the Analyze button on the bottom left side of the window. When you analyze a disk the disk defragmenter utility checks for fragmented files, contiguous files, system files and free space. The results of the analysis are shown in the analysis display bar, which is color coded as follows:

Fragmented file	Red
Contiguous file	Blue
System file	Green
Free space	White

Even though you can't see the colors you can get an idea of what this analysis bar looks like.

The disk analysis also produces a report, which is displayed when you click the view report button. The report contains the following information:

- *Whether or not the volume needs defragmenting.*
- *Volume information that includes general volume statistics, volume fragmentation, file fragmentation, page file fragmentation, directory fragmentation, and master file table (MTF) fragmentation*
- *A list of the most fragmented files.*

12.13. **Defragmenting Disks**

To defragment a disk, open the Disk Defragmenter utility, select the drive to be defragmented and click the defragment button (to the right of the analyze button at the bottom of the window). Defragmenting causes all files to be stored more efficiently in contiguous space. When defragmentation is complete, you can view a report of the defragmentation process.

12.14. **Disk Cleanup Utility**

This utility identifies areas of disk space that can be deleted to free up the hard disk space. It identifies temporary files, Internet cache files and unnecessary program files.

To access this utility, select Start → Programs → Accessories → System Tools → Disk Cleanup.

Practical

i) Compressing a file or folder.
ii) Configuring Disk Quotas.
iii) Setting Default Quotas.
iv) Setting an Individual Quota.
v) Modifying an Individual User's Quota.
vi) Monitoring Disk Quota.
vii) Encrypting file or folder.
viii) Encrypting and Decrypting file or folder using CIPHER utility.

Exercise - 12

Q.1 Fill in the blanks:

i) Data compression is possible only on _______ partitions. (NTFS)

ii) Data compression is the process of storing data that occupies _______. (less space than the uncompressed)

iii) Utility used for encrypting and decrypting files or folders is _______. (CIPHER)

Q.2 Write short Notes:

i) Data Compression

ii) Disk Quota

iii) Setting Default Quota Limit

iv) Setting an Individual Quota Limit

v) Modifying an Individual User’s Quota

vi) Monitoring Disk Quota

vii) CIPHER utility

CHAPTER 13

ACCESSING FILES AND FOLDERS

13.1. **Managing Local Access**

FAT *(which includes FAT16 and FAT32)* partitions do not support local security but the NTFS partitions support local security. You can allow or deny NTFS permissions to users and groups.

This means that if the file system on the partition that users access is configured as a FAT partition, you cannot specify any security for the file system once a user has logged on. However, if the partition is NTFS, you can specify the access each user has to specific folders on the partition, based on the user's based on the user's logon name and group associations.

Normally, NTFS permissions are cumulative (collective), based on group memberships. However, if the user had been denied access through user or group membership, those permissions override allowed permission.

13.2. **NTFS Permissions**

Windows 2000 Server offers following NTFS permissions:

i) Read – When applied to a file, a user is able to view the file contents, attributes and permissions.

ii) Read and Execute – Performs all actions included in the Read permission and can also execute files if the files are executable.

iii) List Folder Contents – Performs all actions included in the Read and Execute permission but is applicable to folders only.

iv) Write – User can append data to the file, change the file attributes and can also create files and sub-folders.

v) Modify – Performs all functions included in Read & Execute and Write permissions. In addition user can delete the files and folders.

vi) Full Control – Performs all actions included in the Modify permissions. In addition user can change permissions.

13.3. **Applying NTFS Permissions**

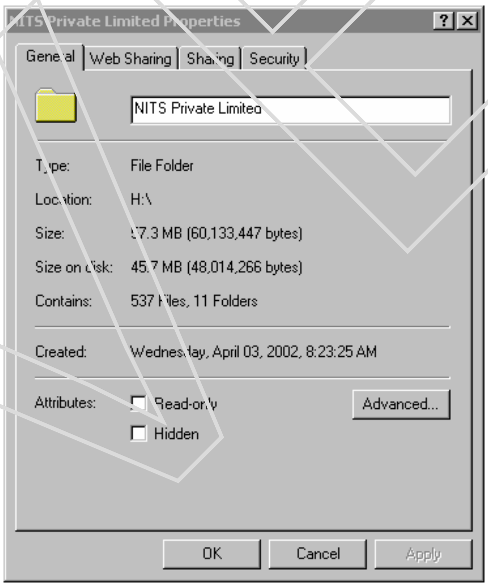
You apply NTFS permissions through Windows Explorer. Right click the file or folder that you want to control access to and select Properties form the pop up menu. This brings up the folder or file Properties dialog box. A folder properties dialog box.

The tabs in file or folder properties dialog box depend on the options that have been configured for your computer. For files and folders on NTFS partitions, the dialog box will contain a security tab, which is where you configure NTFS permissions. The security tab lists the users and groups that have been assigned permissions to the folder (or file)

When you click a user or group, you see the permissions that have been allowed or denied for that user or group

Steps to Apply NTFS Permissions:

1. Right click the folder or file and select Properties.



NITS Private Limited

Type: File Folder

Location: H:\

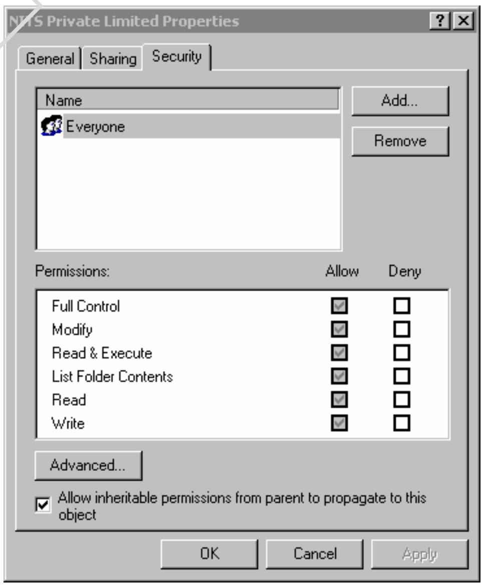
Size: 57.3 MB (60,133,447 bytes)

Size on disk: 45.7 MB (48,014,266 bytes)

Contains: 537 Files, 11 Folders

Created: Wednesday, April 03, 2002, 8:23:25 AM

Attributes: □ Read-only □ Hidden



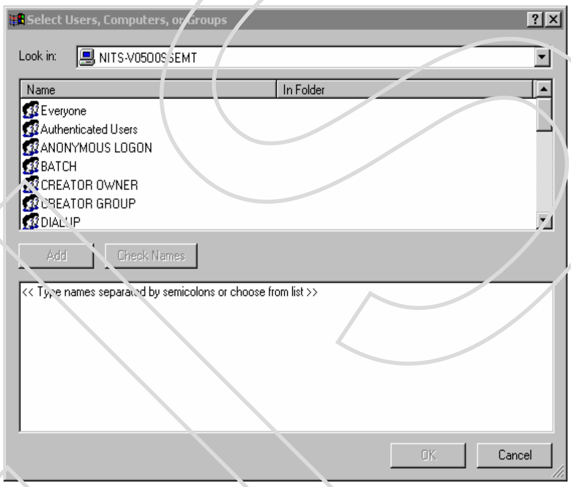
Name
Everyone

Permissions:	Allow	Deny
Full Control	☑	□
Modify	☑	□
Read & Execute	☑	□
List Folder Contents	☑	□
Read	☑	□
Write	☑	□

☑ Allow inheritable permissions from parent to propagate to this object

2. Folder Properties dialog box appears. Click the Security tab and then click the Add button.

3. Select Users, Computers or Groups dialog box appears. Select the user, computer or group that you wish to add and click the Add button and then click the OK button. *The user, computer, or group appears in the bottom list box. Use CTRL+CLICK to select non-contiguous users, computers, or groups or SHIFT+CLICK to select contiguous users, computers, or groups*



4. Specify the NTFS permissions that should be applied. When you are finished, click the OK button.

   To remove the NTFS permissions for a user, computer, or group, high light the user computer, or group you wish to remove in the security tab and click the remove button. Note that if the permissions are being inherited, you must first uncheck allow inheritable permissions from parent to propagate to this object check box before removing the permissions. Be careful when you remove NTFS permissions.

<u>Configuring NTFS Permissions;</u>

1. *Using the local users and groups utility, create two users: Mahesh and Yogesh.*

2. *Using the local users and groups utility. Create four groups: Accounting, Execs, Sales, and Temps. Add Mahesh to the accounting and execs groups, and add Yogesh to the sales and temps groups.*
3. *Select Start → Programs → Accessories → Windows Explorer.*
4. *Create a folder NITS and go to its properties, and click the security tab.*
5. *In the security tab of the folder properties dialog box, highlight everyone group and click the remove button. You see a dialog box telling you that you cannot remove everyone because this group is inheriting permissions from a higher level. Click the OK button.*
6. *In the security tab, deselect Allow inheritable permission from parent to propagate to this object. In the dialog box that appears, click the remove button.*
7. *Configure NTFS permission for the accounting group by clicking the add button. In the select user, computers, or groups dialog box, highlight the accounting group and click the add button. SHIFT + CLICK to select the excess, sales, and temps groups and click the Add button then click OK.*
8. *In the security tab, highlight each group and check the allow or deny check boxes to add permissions as follows:*
   - *For accounting, allow read & execute (list folder contents and read will automatically be allowed) and write.*
   - *For execs, allow read. Z*
   - *For sales, allow modify (read & execute, list folder contents, read, and write will automatically be allowed.*
   - *For temps, deny write.*
9. *Click the ok button to close the folder properties dialog box.*
10. *You will see a security dialog box cautioning you about the deny entry. Click the Yes button to continue.*
11. *Log off as Administrator and log on as Mahesh. Access the d:/NITS/TRAINING file, make changes, and then save the changes. Mahesh's permissions should allow these actions.*

12. *Log off as Mahesh and log on as Yogesh. Access the d:/NITS/TRAINING file, make changes, and then save the changes. Yogesh's permissions should allow you to open the file but not to save any changes.*
13. *Log off as Yogesh and log on as Administrator.*

You may want to remove permissions from everyone group to test how the permissions of other groups combine. If you decide to do this, adding the administrators group with full control permission will make it easier or troubleshoot any problems that arise.

13.4. **NTFS Permissions for Copied or Moved Files**

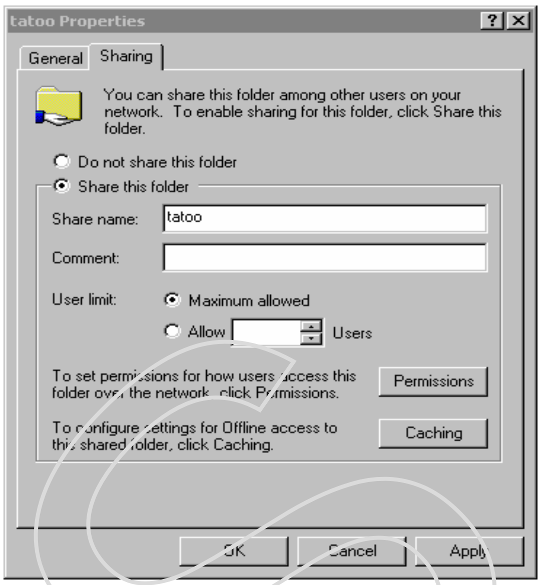
When you copy or move NTFS files, the permissions that have been set for those files might change. These changes are applied in the following manner:

- If you move a file from one folder to another folder on the same NTFS volume, the file will retain the original NTFS permissions.
- If you move a file from one folder to another folder on a different NTFS volume, the file will have the same permissions as the destination folder.
- If you copy or move a folder or file to a FAT partition, it will not retain any NTFS permissions.

13.5. **Sharing Folders**

Sharing means allowing network users to access a shared folder. To share a folder logon as Administrators or Power Users group on a Windows 2000 member server and Administrators or Server Operators group on a Domain Controller.

- To share a folder right click the folder and click the Sharing option from the pop up menu.
- Folder Properties dialog box appears. Select the Sharing tab. The following options appear:



tatoo Properties

You can share this folder among other users on your network. To enable sharing for this folder, click Share this folder.

○ Do not share this folder

● Share this folder

Share name: tatoo

Comment:

User limit: ● Maximum allowed

○ Allow Users

To set permissions for how users access this folder over the network, click Permissions.

To configure settings for Offline access to this shared folder, click Caching.

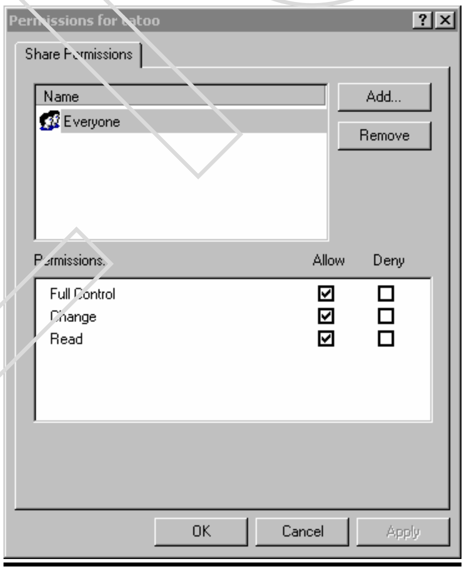
<u>Option</u>	<u>Description</u>
Do not share this folder	Folder is only available through local access.
Share this folder	Folder is available through local access and network access
Share name	A name by which users will access the folder.
Comment	Allows you to enter more information about the share (optional)
User limit	Allow you to specify the maximum number of connections to the share at a time.
Permissions	Allows you to configure how users will access the folder over the network
Caching	Specifies how folders are cached when the folder is offline.

If you share a folder and then decide that you do not want to share it, just select do not share this folder radio button under the Sharing tab of the folder properties dialog box.

13.6. **Configuring Share Permissions**

You can control user's access to a shared folder by assigning share permissions to a particular group or a user. *Share permissions are less complex than NTFS permissions and can be applied only to folders (unlike NTFS permission, which can be applied to folders and files).*

- To assign share permissions, right click the folder and select Sharing from the pop-up menu.
- Folder Properties dialog box appears. Select the Security tab and then click Permissions button. This brings up the Share Permissions dialog box.



Name

Everyone

Permissions:	Allow	Deny
Full Control	☑	□
Change	☑	□
Read	☑	□

You can assign three types of share permissions:

- <u>Full Control</u> - share permission allows full access.

- Change - share permission allows users to change data in a file or to delete files.
- Read - share permission allows a user to view and execute file in the shared folder.

Full control is the default permission on shared folders for the everyone group. When the Full Control permission is assigned, the Change and Read permissions are automatically checked.

13.7. **Managing Shares With the Shared Folders Utility**

Shared Folders utility is used for creating and managing the shared folders on the computer. *The shared folders windows displays all of the shares that have been created on the computer, the user sessions that are open on each share, and the files that are currently open, listed by user.*

To access the Shared Folders utility steps are as follows:

1. Right click My Computer and select Manage from the pop up menu.
2. Computer Management window appears. Expand System Tools and then expand Shared Folders.

   Note: You can add the shared folders utility as an MMC snap in.

Shared Folders utility has the following folders:

(i) Shares

(ii) Sessions

(iii) Open Files

(i) Shares:

Shares folder is used to display all of the shares that have been configured on the computer and can also be used to create new shares.

Along with the shares that you have specifically configured, you will also see the windows 2000 special shares, which are shares created by the system automatically to facilitate system administration.

A share that is followed by a dollar sign ($) indicates that the share is hidden. The user cannot view the hidden shares when users access through My Network Places.

The following special shares may appear on your windows 2000 server computer, depending upon how the computer is configured:

- *The drive letter $ share is the share for the root of the drive. By default, the root of every drive is shared. For example, the c: drive is shared as c$.*

On windows 2000 member servers and windows professional computers, only members of the administrators and backup operators group can access the drive letter $ share. On windows 2000 domain controllers, members of the administrators, backup operators, and server operators group can access this share.

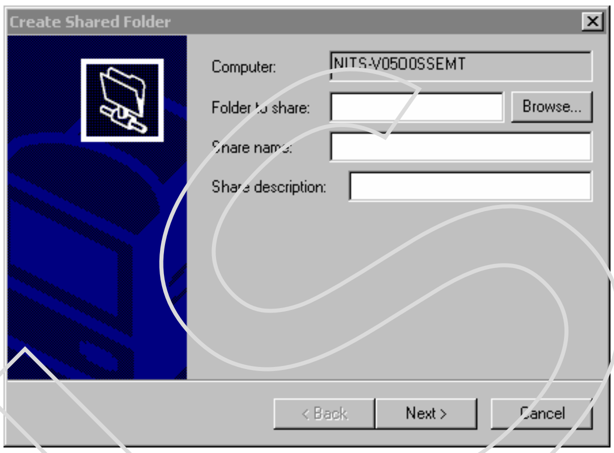
- *The Admin$ share points to the windows 2000 system root (for example, C:/WINNT).*
- *The IPC$ share allows remote administration of a computer and is used to view a computer's shared resources. (IPC stands for Inter Process Communication).*
- *The PRINT$ share is used for remote printer administration.*
- *The FAX$ share is used by fax clients to cache fax cover sheets and documents that are in the process of being faxed.*

<u>Creating New Shares</u>

Under Shared Folders, you can create new shares through the following steps:

(a) Right click the Shares folder and select “New File Share” from the pop up menu.

(b) Create Shared Folder wizard starts. Specify the folder that you want to share *(You can use the browse button to select the folder)* and provide a share name and description. Click the Next button.



Create Shared Folder

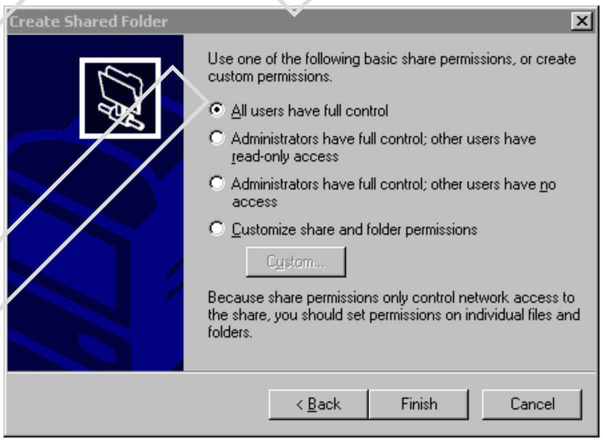
Computer: NITS-V0500SSEMT

Folder to share:

Share name:

Share description:

(c) Then assign the share permissions and click the Finish button. *(Assign permissions from one of the predefined permissions or customize the share permissions)*.



Create Shared Folder

Use one of the following basic share permissions, or create custom permissions.

● All users have full control

○ Administrators have full control; other users have read-only access

○ Administrators have full control; other users have no access

○ Customize share and folder permissions

Because share permissions only control network access to the share, you should set permissions on individual files and folders.

(d) Click the Yes button to create another shared folder or No button if you do not want to create.

You can stop sharing a folder by right clicking the shared folder and selecting Stop Sharing from the pop up menu. *You will be asked to confirm that you want to stop sharing the folder.*

(ii) <u>Sessions</u>:

Sessions folder is used to display all of the users who are currently accessing the shared folders on the computer.

The sessions listing includes the following information:

- *The username that has connected to the share*
- *The computer name that the user has connected form*
- *The client operating system that is used by the connecting computer*
- *The number of files that the user has open*
- *The amount of time that the user has been connected*
- *The amount of idle time for the connection*
- *Whether or not the user has connected through guest access*

(iii) <u>Open Files</u>:

Open Files folder is used to display a list of files that are currently being opened from the shared folders.

The open files listing includes the following information:

- *The path and files those are currently open.*
- *The username that is accessing the file.*
- *The operating system that the user who is accessing the file is using.*
- *Whether or not any file locks have been applied (file locks are used to prevent two users form opening the same file and editing it at the same time)*
- *The open mode that is being used (such as read or write).*

13.8. **Providing Access to Shared Resources**

The methods to access shared resources are as follows:

(i) Through My Network Places.

(ii) By Mapping as a Network drive.

(iii) Through the NET USE command line utility.

(i) Through My Network Places:

The advantage of mapping a network location through my network places is that you do not use a drive letter. This is useful if you have already exceeded the limit of 26 drive letters.

The steps are as follows:

(i) Double click My Network Places icon on the desktop.

(ii) Double click Add Network Place.

(iii) Welcome to the Add Network Place Wizard dialog box appears. Type the location of the shared folder and click the Next button. (*This can be a UNC path to a shred network folder, an HTTP path to a web folder, or an FTP path to an FTP site. If you are unsure of the path, you can use the browse button to search for your path. After specifying the path).*

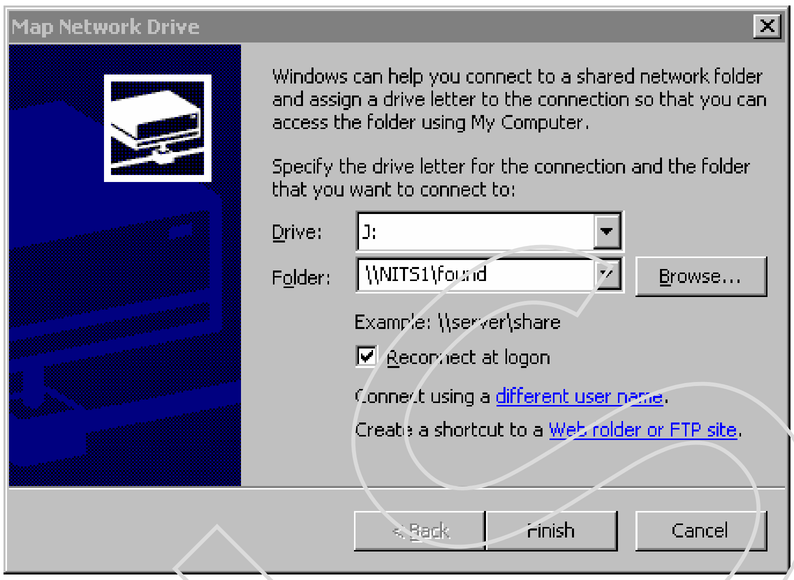
(iv) Completing the Add Network Place Wizard dialog box appears. Enter the name that you want to use for the network location. This name will appear in the computer's My Network Places listing.

(ii) By Mapping a Network Drive:

Through Windows Explorer, you can map a folder as a drive that will appear in My Computer.

The steps are as follows:

1. Open Windows Explorer.
2. Select Tools → Map Network Drive.



Map Network Drive

Windows can help you connect to a shared network folder and assign a drive letter to the connection so that you can access the folder using My Computer.

Specify the drive letter for the connection and the folder that you want to connect to:

Drive: J:

Folder: \\NITS1\found

Example: \\server\share

☑ Reconnect at logon

Connect using a different user name.

Create a shortcut to a Web folder or FTP site.

3. Choose the network drive letter.
4. Choose the shared network folder that you want to map as network drive.
5. Click Finish.

(iii) <u>Using the NET USE Command Line Utility</u>:

Syntax:

NET USE [Drive:] \\COMPUTER NAME \SHARE NAME

For example, NET USE G: \\NITS\DATA command maps drive G to a share, named DATA on computer named NITS.

<u>Accessing network resources:</u>

1. *Log on as user Mahesh. Double click the My Network Places icon on the desktop.*

2. *Double click Add Network places. When the add network place wizard starts. Click the browse button.*
3. *Select the workgroup or domain that your computer is installed in. click your computer name. Select TEST shared folder and click the OK button. Click the Next Button.*
4. *Enter the name that you want to use for the network location. This name will appear in the computer's my network places listing.*
5. *Accept the default name for the network place and click the Finish button.*
6. *The folder opens automatically. Close the folder. You will see the new folder in My Network Places.*
7. *Log off as Mahesh and log on as Yogesh.*
8. *Double click my network places. You will not see the network place that you created as user Mahesh.*

Practical

i) Applying NTFS permissions.

ii) Sharing a folder.

iii) Configuring Share permissions.

iv) Managing shares with Shared Folder utility.

v) Accessing through My Network Places.

vi) Mapping a network drive.

vii) Using NET USE utility.

Exercise - 13

Q.1 Fill in the blanks:

i) Local security of files is possible only on ________ partitions. (NTFS)

ii) If you move/copy a file from one folder to another folder between different NTFS volumes, the file will have the ________. (same permissions as the destination folder)

iii) There are ________ permissions. (6)

iv) There are ________ types of share permissions. (3)

v) Methods to access shared resources are ________. (My Network Places, Mapping as network drive and NET USE utility)

Q.2 Write short Notes

i) NTFS Permissions

ii) Determining NTFS permissions for copied files

iii) Sharing a folder

iv) Accessing Shared Folders utility

v) Methods to access shared resources

CHAPTER 14

MANAGING NETWORK SERVICES

14.1. **Introduction**

Network connections require the proper network protocols. The three primary protocols that are used by the Windows 2000 Server are TCP/IP, NW Link IPX/SPX/Net BIOS and NetBEUI.

Network services provide IP address management and address resolution functions. The main services used for Windows 2000 network are as follows:

(i) Dynamic Host Configuration Protocol (DHCP)

(ii) Domain Name System (DNS)

(iii) Windows Internet Name Service (WINS).

14.2. **Installing Network Adapter**

Network adapters are hardwares used to connect computers (or other devices) to the network. Network adapters are responsible for providing the physical connection to the network and the physical address of the computers. Like all other hardware devices, network adapters need a driver in order to communicate with the Windows 2000 operating system.

Connect the network adapter and install the driver for that adapter, if the adapter is not plug and play then add the network adapter through Add/Remove Hardware icon in Control Panel.

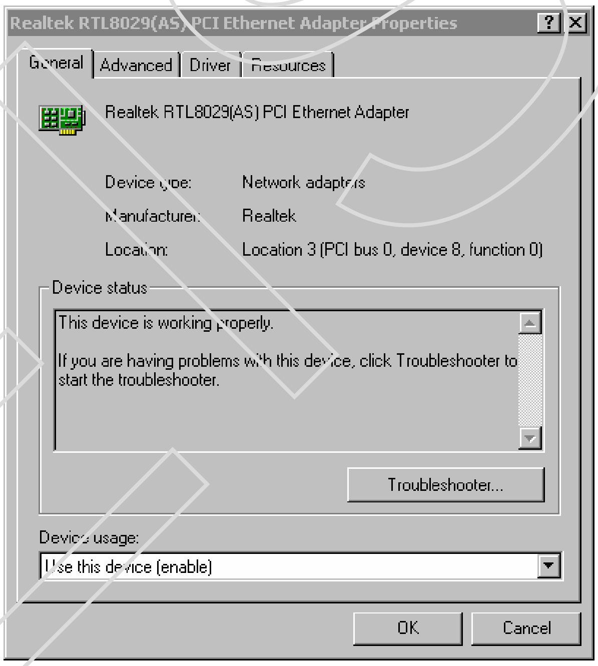
14.3. **Configuring a Network Adapter**

After installing a network adapter, you can configure it through its Properties dialog box. To access this dialog box proceed as follows:

(i) Go to the Control Panel and double click the Network and Dial-up Connections icon.

(ii) Network and Dial-up Connections dialog box appears. Right click the Local Area Connection and select Properties from the pop-up menu.

(iii) Local Area Connection Properties dialog box appears. Click Configure command button.



Realtek RTL8029(AS) PCI Ethernet Adapter Properties

Realtek RTL8029(AS) PCI Ethernet Adapter

Device type: Network adapters
Manufacturer: Realtek
Location: Location 3 (PCI bus 0, device 8, function 0)

Device status

This device is working properly.

If you are having problems with this device, click Troubleshooter to start the troubleshooter.

Device usage:
Use this device (enable)

(iv) Adapter Properties dialog box appears in which properties are grouped in four tabs: General, Advanced, Driver and Resources.

<u>General Tab</u>: This tab shows the name of the adapter, device type, manufacturer, location and status box. *The device status box shows whether or not the device is working properly. If the device is not working properly, you can click the troubles shooter button to have windows 2000 display some general*

troubleshooting tips. You can also enable or disable the device through the device usage drop down list options.

Advanced Tab: Its contents vary depending on the network adapter and driver that you are using.

Driver Tab: It provides the information about driver manufacturer, date that the driver was released and the driver version. *(It is useful in determining if you have latest driver installed).*

The digital signer (The company that provides the digital signature for driver signing).

Resources Tab: *Each device installed on a computer uses computer resources.* Resources include Interrupt Request (IRQ), memory and I/O settings. *The resources tab of the network adapter properties dialog box lists the resource setting for your network adapter, this information is important for troubleshooting, because if other device are trying to use the same resource settings, your devices will not work properly. The conflicting device list box at the bottom of the resources tab shows if any conflicts exist.*

14.4. **Protocols Supported by Windows 2000**

Windows 2000 server supports the following protocols:

- TCP/IP- It is installed on Windows 2000 Server computer by default
- NW Link IPX/SPX/Net BIOS - These are used to connect to Novell Netware Networks. IPX stands for Internet Packet Exchange and SPX stands for Sequenced Packet Exchange.
- NetBEUI- It is a non-routable protocol, useful for small networks.
- Apple Talk- It is used to support Apple Macintosh computers. *(It is a fully functional, routable protocol)*.

- DLC (Data Link Control)- It is used for old HP printers and IBM mainframe computers.

14.5. **TCP/IP**

TCP/IP (Transmission Control Protocol / Internet Protocol) was developed in 1970s to connect dissimilar networks as it is supported by all operating systems. It provides routing service in large networks.

One the most commonly used network protocols. TCP/IP was originally developed in the 1970s for the department of defense (DoD) as a way of connecting dissimilar networks. Since, TCP/IP has become an industry standard. On a clean installation of windows 2000 server, TCP/IP is installed by default.

TCP/IP has the following benefits:

- It is supported by almost all network operating system.
- It is scalable *(Can be used for small and large Networks)* and provides routing services.
- It is fault tolerant and is able to dynamically reroute the packets if network links become unavailable *(assuming alternate paths exist).*

TCP/IP requires an IP Address and a Subnet Mask.

(i) <u>IP Address</u>

The IP address uniquely identifies your computer on the network. The IP address is a four-field, 32 bit address, separated by periods. Part of the address is used to identify the network address and part of the address is used to identify the host (or local computer) computer's address.

(ii) <u>Classes of IP Addresses</u>

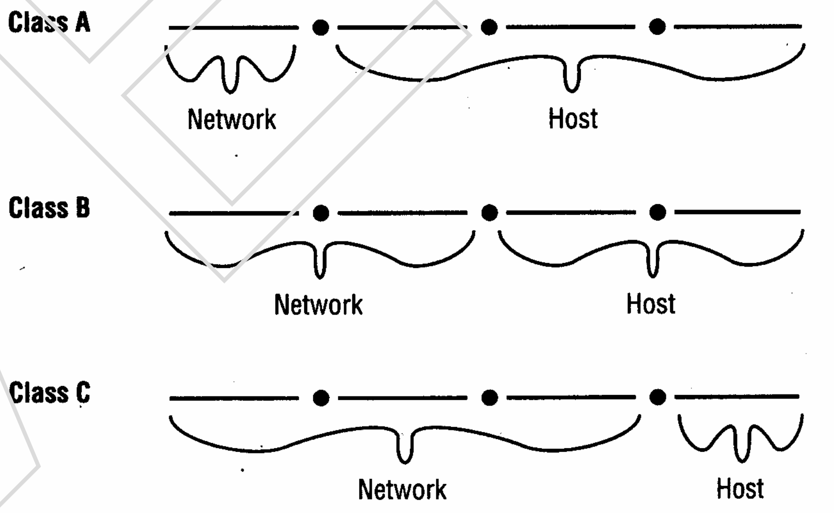
IP address is a 32-bit address means 32-bit binary number divided into 4 octets. There are three main classes of IP addresses. These are class A, class B and class C. Depending on the class you use, different parts of the address show the Network address and the Host address.

In class A, the first bit of the first octet is always zero (0). The first octet is used for the Network ID and the last three for the Host ID. For the same network, Network ID is same but the Host ID for computer is unique. In class A type of network, 2^7-2= 126 networks are possible and 2^{24}-2 hosts can be connected. It is suitable for big networks as it can have 126 different networks with 2^2 -2 computers in a single network.

In class B, the first 2 bits are always 10 (one zero). First 2 octets form the Network ID and last two form the Host ID.

In class C, first 3 bits are always 110. First 3 octets form the Network ID and last octet form the Host ID.

All zeros (0.0.0.0) and all (255.255.255.255) are not possible because these are used for broadcast purpose. In class A, IP addresses 127.0.0.1 is used for the loop back.



Network Class	Address Range of first field.	Number of networks available	Number of host nodes supported
A	1-126	126= (2^7-2)	16,777,214=(2^{24} – 2)
B	128-191	16,384= (2^{14}-2)	65,534= (2^{16} –2)
C	192-223	2,097,152= (2^{21}-2)	254= (2^8 – 2)

Note: IP addresses are also available in class D and E for future use.

(iii) Subnet Mask

The subnet mask is used to specify which part of the IP address is the Network address and which part of the address is the Host address. By default following subnet mask are applied:

Class A – 255.0.0.0

Class B – 255.255.0.0

Class C – 255.255.255.0

255 are used to identify the network address. For example, in the class B network address 167.147.1.2. The 167.147 is the Network address and 1.2 is the Host address.

14.6. Default Gateway

You configure a default gateway if the network contains routers. A router is a device that connects two or more network segments together. Routers function at the Network layer of the OSI model.

You can configure a Windows 2000 Server to act as a router by installing two or more network cards in the server, attaching each network card to a different network segment and then configuring each network card for the segment that it will attach to. *You can also use third party routers, which typically offer more features than windows 2000 server configured as routers*.

As an example, suppose that your network is configured. Network A uses the IP network address 131.1.0.0. Network B uses the IP network address 131.2.0.0. In this case, each network card in the router should be configured with an IP address from the segment that the network card is addressed to.

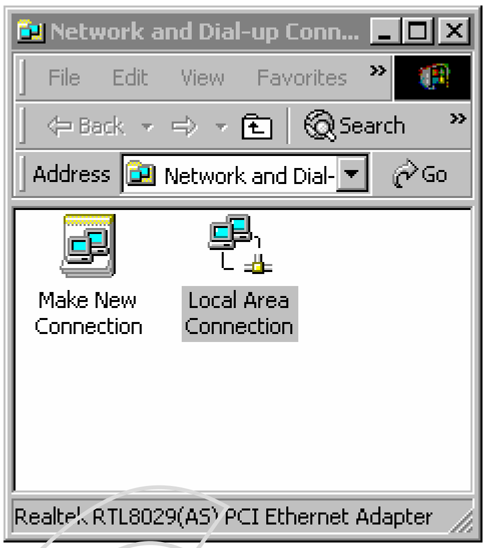
For example, the Computer NITS1 is attached to Network A. The default gateway would be configured for this computer is 131.1.0.10. The Computer NITS2 is attached to Network B. The default gateway would be configured for this computer is 131.2.0.10.

14.7. **Manual IP Configuration**

You can manually configure IP if you know your IP address and Subnet mask. If you are using optional components such as a default gateway or a DNS server, you need to know the IP addresses of the computers that host these services as well.

To manually configure IP, follow the following steps:

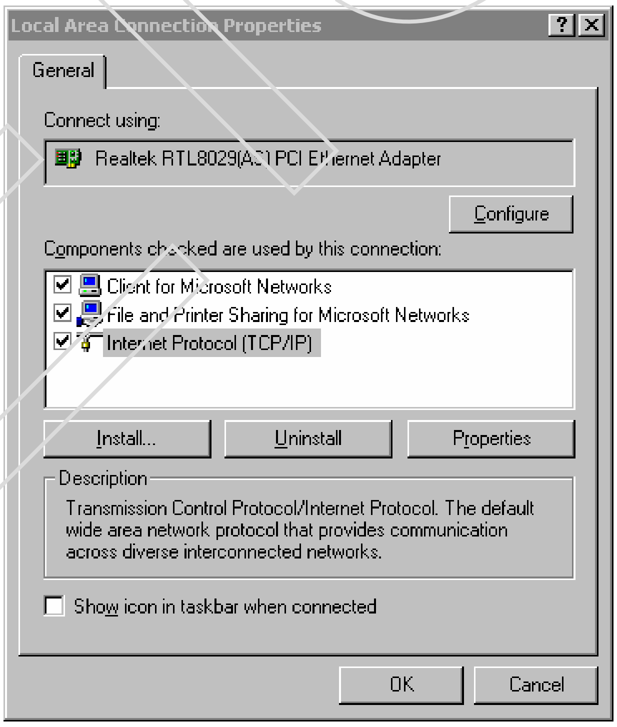
1. Right click My Network Places and choose Properties from the pop-up menu.



Realtek RTL8029(AS) PCI Ethernet Adapter

2. Network and Dial-up Connections dialog box appears. Right click Local Area Connection and choose Properties from the pop-up menu.

3. Local Area Connection Properties dialog box appears. Select Internet Protocol (TCP/IP) and click the Properties button.



Connect using:

Realtek RTL8029(AS) PCI Ethernet Adapter

Components checked are used by this connection:

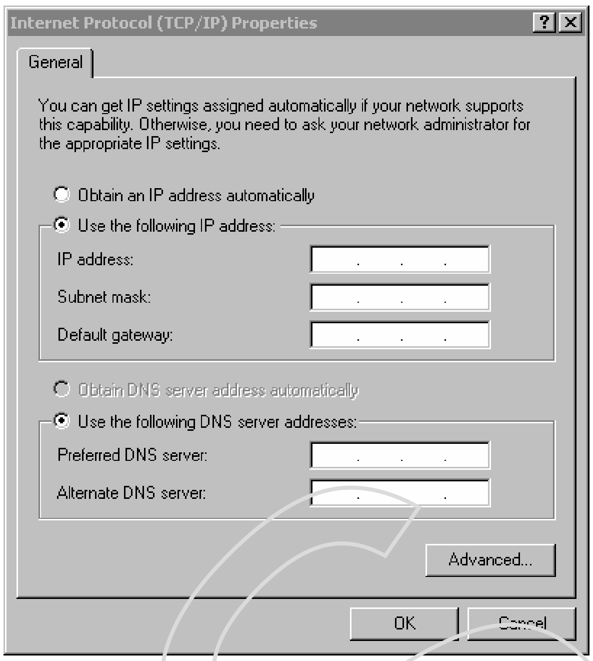
☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ Internet Protocol (TCP/IP)

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

☐ Show icon in taskbar when connected

4. Internet Protocol (TCP/IP) Properties dialog box appears. Select “Use the following IP address” radio button.



Internet Protocol (TCP/IP) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

5. Specify the IP address, Subnet mask and Default Gateway (optional) that you want to use.
6. Optionally, specify a Preferred and Alternate DNS server in the corresponding text boxes.
7. Click the OK button to save your settings and close the dialog box.

14.8. <u>Testing IP Configuration</u>

After configuring IP, you can test the IP configuration by using IPCONFIG and PING commands.

(i) <u>IPCONFIG Command</u>

IPCONFIG command displays your IP configuration.

Syntax:

IPCONFIG [Options]

/All – Shows all information about your IP configuration.

Switch	**Description**
/All	Shows information about your IP configuration. *(Such as your computer's physical address, the DNS server you are using, and whether you are using DHCP).*
/Release	*Releases an address that has been assigned through DHCP.*
/Renew	*Renews an address through DHCP*

Using the IPCONFIG Command:

1. *Select start → Programs → Accessories → Command Prompt.*
2. *In the command prompt dialog box, type IPCONFIG and press enter. Note the IP address, which should be the address that you configured when the computer was installed.*
3. *In the command prompt dialog box, type IPCONFIG / All and press inter. You now see more information.*
4. *Type exit and press enter.*

(ii) PING Command

PING command is used to send an Internet Control Message Protocol (ICMP) echo request and echo reply to verify that IP address is configured properly or not.

Syntax:

PING IP Address

For example if your IP address is 131.200.2.30, type the following command: PING 131.200.2.30

PING is useful for verifying connectivity between two hosts. For example, if you were having trouble connecting to a host on another network, you would use PING to verify that a valid communication path existed by pinging the following addresses:

- *The loop back address, 127.0.0.1*
- *The local router's computer's IP address (You can verify this with IPCONFIG)*
- *The local router's (default gateway's) IP address*
- *The remote computer's IP address*

If PING failed to get a reply from any of these addresses, you would have a starting point for troubleshooting the connection error.

Practical

i) Configuring Network Adapter.

ii) Manual IP Configuration.

iii) Testing IP Configuration using PING and IPCONFIG.

EXERCISE

Q.1 Fill in the blanks:

i) Three primary protocols used by Windows 2000 Server are ________. (TCP/IP, NW Link IPX/SPX/Net BIOS and Net BEUI)

ii) Network services provide ________functions. (IP address management and address resolution)

iii) DHCP stands for ________. (Dynamic Host Configuration Protocol)

iv) DNS stands for ________. (Domain Name System)

v) WINS stands for ________. (Windows Internet Name Service)

vi) IPX stands for ________. (Internet Packet Exchange)

vii) SPX stands for ________. (Sequenced Packet Exchange)

viii) DLC stands for ________. (Data Link Control)

ix) TCP/IP address requires ________ and ________. (IP address, Subnet mask)

x) IP configuration can be tested by using ________ and ________. (PING, IPCONFIG)

Q.2 Write short Notes:

i) Network Services

ii) Protocols supported by Windows 2000 Server

iii) TCP/IP

iv) IP address

v) Subnet mask

vi) PING and IPCONFIG

Q.3 Explain TCP/IP and different classes of IP addresses.

+++

DNS SERVER

15.1. DNS Server

DNS servers are used to resolve (decide) host names to IP addresses. This makes easier for the people to access domain hosts.

Do you know what the IP address is for the white house? It's 198.137.240.91. Do you know the host name of the white house? It's www.whitehouse.gov you can understand why many people might not know the IP address but would know the host name.

When you access the internet and type in www.whitehouse.gov , there are DNS servers that resolve the host name to the proper IP address. If you do not have access to properly configured DNS server, you can configure a host file for your computer. A host file contains the mappings of IP addresses to the domain hosts that you need to access.

15.2. Terminologies Used in DNS

(i) Forwarders: This is used to configure the DNS server to use one or more other existing DNS servers on your network as a forwarder. *(You have to specify the IP address of other DNS servers). Select 'Do not use recursion' if forwarders is available to avoid repetition.*

(ii) Recursion: Recursion means repeating a process until a solution is found. This means that a DNS server will contact many other DNS servers.

(iii) Zone: A zone is a storage database for either a DNS domain or for a DNS sub domain. These storage database files are called zone files.

The DNS Server service is not installed by default. Before installing DNS server service, the computer must be configured to use a static IP address on a computer with a primary DNS suffix. *If your computer is to use DHCP to obtain its IP address dynamically, you must reconfigure the computer with a static IP address before you install DNS.*

15.3. Configuring a Primary DNS Suffix

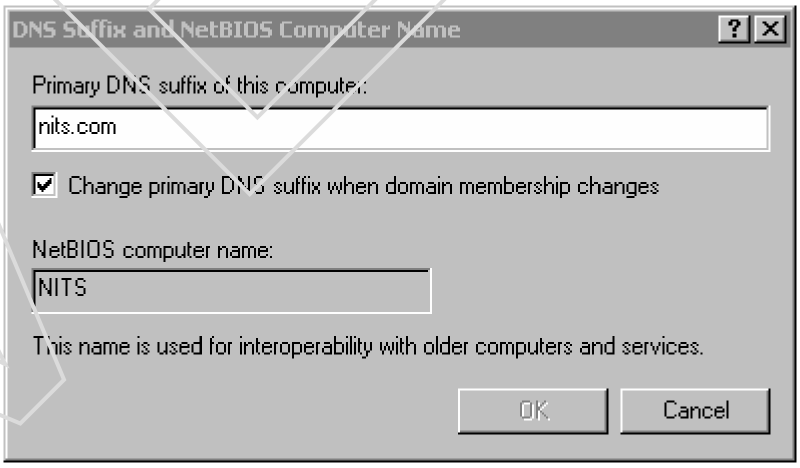
(i) Right click My Computer and select Properties from the pop-up menu.

(ii) System Properties dialog box appears. Click the Network Identification tab.

(iii) Under the Network Identification tab, click the Properties button.

(iv) Identification Changes dialog box appears. Click More button.

(v) DNS suffix and NetBIOS Computer Name dialog box appears. Type the DNS suffix in the "Primary DNS suffix of this computer" text box (NITS.COM) and click OK.



Primary DNS suffix of this computer: nits.com

☑ Change primary DNS suffix when domain membership changes

NetBIOS computer name: NITS

This name is used for interoperability with older computers and services.

(vi) Identification Changes dialog box appears in which full computer name is displayed which includes computer name and DNS suffix (PR1.NITS.COM). Click the OK button.

(vii) In the Network Identification Changes dialog box, click OK.

(viii) Under the Network Identification tab, click OK.

(ix) In the System Settings Change dialog box, click Yes to restart your computer.

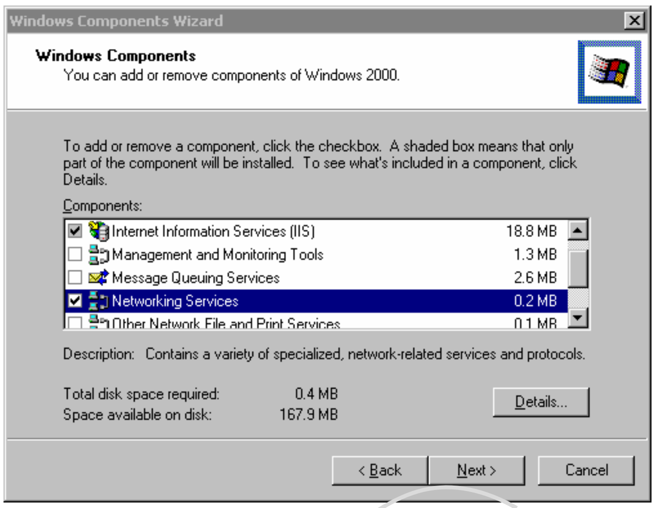
15.4. **Installing the DNS Service**

(i) Click Start → Settings → Control Panel.

(ii) Double click Add/Remove Programs.

(iii) Add/Remove Properties dialog box appears. Click Add/Remove Windows Components.

(iv) Windows Components Wizard starts. In the Windows Components screen, select Networking Services and then click Details.



Windows Components Wizard

Windows Components
You can add or remove components of Windows 2000.

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

Components:

☑	Internet Information Services (IIS)	18.8 MB
□	Management and Monitoring Tools	1.3 MB
□	Message Queuing Services	2.6 MB
☑	Networking Services	0.2 MB
□	Other Network File and Print Services	0.1 MB

Description: Contains a variety of specialized, network-related services and protocols.

Total disk space required: 0.4 MB
Space available on disk: 167.9 MB

(v) In the Networking Services dialog box, select Domain Name System (DNS) and click OK.

(vi) In the Windows Components screen, click Next.

(vii) In the Completing Wizard screen click Finish button.

15.5. **Configuring a DNS Server to Use Itself**

It means that your DNS Server needs to be configured to use itself to perform host name resolution. The steps are as follows:

1. Right click My Network Places and select Properties from the pop-up menu.
2. Network and Dial-up Connections dialog box appears. Right click the Local Area Connection and select Properties.
3. Local Area Connection Properties dialog box appears. Select Internet Protocol (TCP/IP) and click the Properties button.
4. Internet Protocol (TCP/IP) Properties dialog box appears. Ensure that the "Use the following DNS server addresses" option is selected. Then, in the "Preferred DNS server" text box,

type the IP address of this DNS Server and click the Advanced button.

5. Advanced TCP/IP Settings dialog box appears. Click the DNS tab.
6. Under DNS tab type your domain name (i.e. your company name) in the "DNS suffix for the connection" text box. Generally, it is advisable to accept the remaining default settings under this tab and click OK.
7. In the Internet Protocol (TCP/IP) Properties dialog box, click OK.
8. In the Local Area Connection properties dialog box, click OK.
9. Close the Network and Dial-up Connections dialog box.

15.6. **Configuring a Root Server**

If this is the first DNS Server on your network and your network is not connected to the Internet, then you have to configure first server as the root server. To configure root server follow the following steps:

1. Select Start → Programs → Administrative Tools → DNS.
2. In the DNS dialog box, select your computer in the left pane, which will indicate that DNS server has not been configured.
3. Select Action → Configure the server.
4. Configure DNS Server Wizard starts. Click Next.
5. Select 'This is the first DNS server on this network' and click OK. *If you want this DNS server to use an existing root server on your network, select the 'One or more DNS servers are running on this network' option and*

provide IP address of a root server on your network that you want to this server to use.

6. Forward Lookup Zone screen appears. You can choose whether or not to create a forward lookup zone now.

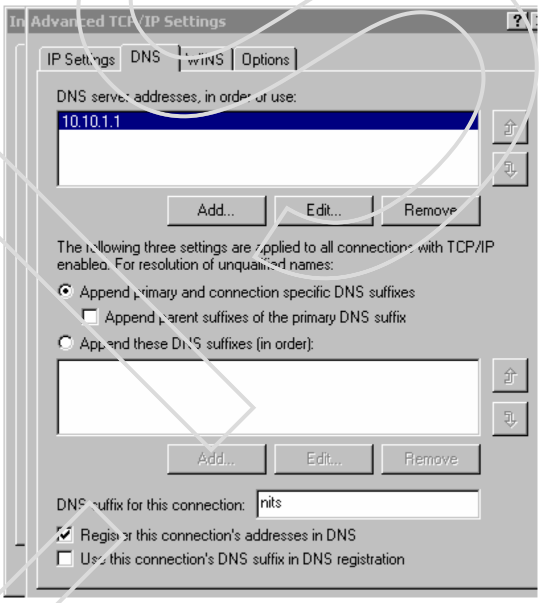
7. Click Finish and close the DNS Server dialog box.

15.7. **<u>Advanced DNS Settings</u>**

To access the DNS Advanced Properties follow the following steps:

- Click Advanced tab in the Internet Protocol (TCP/IP) Properties dialog box.

- Click DNS tab in the Advanced TCP/IP Settings dialog box.



DNS server addresses, in order of use:

10.10.1.1

The following three settings are applied to all connections with TCP/IP enabled. For resolution of unqualified names:

● Append primary and connection specific DNS suffixes

□ Append parent suffixes of the primary DNS suffix

○ Append these DNS suffixes (in order):

DNS suffix for this connection: nits

☑ Register this connection's addresses in DNS

□ Use this connection's DNS suffix in DNS registration

<u>Options in Advanced DNS TCP/IP Settings</u>

<u>Options</u>	<u>Description</u>
DNS Server Addresses, in Order of Use	Specify the DNS servers that are used to resolve DNS queries.
Append Primary and	Specifies how unqualified domain names are resolved

Connection Specific DNS Suffixes	by DNS. *For example, if your primary DNS suffix is nits.com and you type ping tinku, DNS will try to resolve the host name as tinku.nits.com.*
Append Parent Suffixes of the Primary DNS suffix	Specifies whether name resolution includes the parent suffix for the primary domain DNS suffix, upto the second level of the domain name. *For example, if your primary domain DNS suffix is training.nits.com and you type ping nits1, DNS will try to resolve the host name as nits1.training.nits.com. if this does not work, DNS will try to resolve the host name as nits1.nits.com.*
Append These DNS Suffixes	Specifies the DNS suffixes that will be used to attempt to resolve unqualified name. *For example, if your primary DNS suffix is training.com and you type ping nits DNS will try to resolve the host name as nits1.training.com. If you append the additional DNS suffix eg. adpr.com and type ping nits1, DNS will try to resolve the host name as nits1.training.com and nits1.adpr.com.*
DNS Suffix for this connection	Specifies the DNS suffix for the connection. If this value is configured by a DHCP server and you specify a DNS suffix, it will override the value set by DHCP.
Register this connection’s address in DNS	Specifies that the computer will try to register its address dynamically using the computer name *(accessed through the system icon in control panel).*
Use this connection’s DNS suffix in DNS Registration	When the computer registers automatically with the DNS server, it should use the combination of the computer name and the DNS suffix.

Practical

i) Configuring a Primary DNS suffix.

ii) Installing the DNS service.

iii) Configuring a DNS Server to use itself.

iv) Configuring a Root Server.

Exercise - 15

Q.1 Fill in the blanks:

i) DNS server is used to --------------. (resolve host names to IP addresses)

ii) Recursion means ----------------. (repeating a process until solution is found)

iii) DNS service is installed through --------------. (Start → Settings → Control Panel → Add/Remove Programs)

Q.2 Write short Notes:

i) DNS

ii) Installing DNS service

CHAPTER 16

WINS SERVER

16.1. <u>NetBIOS Name Resolution</u>

Windows 2000 uses NetBIOS names in addition to the host names to identify network computers. This is mainly for backward compatibility with Windows NT 4.0. This address resolution can be accomplished by using one of the following methods:

- Through a WINS server.
- Through an LMHOSTS file.

16.2. <u>WINS Server</u>

Windows Internet Name Service (WINS) server dynamically updates its NetBIOS names to IP addresses whenever computers are added to or removed from the network.

16.3. <u>Installing WINS Service</u>

The installation procedure for WINS is same as DNS choose WINS instead of DNS.

1. *Select Start → Settings → Control Panel.*
2. *Double click Add/Remove Programs.*
3. *In the Add/Remove Properties dialog box, click Add/Remove Windows Components.*
4. *The Windows Components wizard starts. In the windows component screen, select **Networking Services** and then click Details.*

5. *In the Networking services dialog box. Select Windows Internet Name Service (WINS) and click OK.*

6. *In the windows components screen, click Next.*

7. *In the completing wizard screen click Finish button.*

16.4. **Advanced WINS Settings**

You can configure the Advanced WINS options through the WINS tab in the Advanced TCP/IP Settings dialog box. The options are as follows:

Option	**Description**
WINS addresses, in order of use	Specify the WINS servers that are used to resolve WINS queries.
Enable LMHOSTS lookup	Specifies whether an LMHOSTS file can be used for name resolution.
Enable net BIOS over TCP/IP	Use this option if your network also includes pre-windows 2000 computers.
Disable Net BIOS over TCP/IP	Use this option only if your network includes only windows 2000 clients.
Use Net BIOS settings from the DHCP server	Specifies when NetBIOS and WINS setting are obtained from the DHCP server.

16.5. **LMHOSTS File**

An lmhosts file is a text file that contains a list that maps the IP addresses to the NetBIOS names on the network.

By default, lmhosts file does not contain any mapping entries. You have to make entries manually. Therefore every time when a computer is added to or removed from network, the lmhosts file is to be amended using notepad or any other text editor.

On Windows 2000 Server, the lmhosts file is stored in systemroot\system32\drivers.

Sample host file

167.147.1.1 NITS1

167.147.1.2 NITS2

167.147.1.3 NITS3

Practical

i) Installing WINS service.

Exercise - 16

Q.1 Fill in the blanks:

i) NetBIOS are used mainly for -------------. (backward compatability with Windows NT 4.0)

ii) Address resolution can be accomplished by ------------- and ----------------. (WINS Server, LMHOSTS file)

iii) WINS stands for --------------. (Windows Internet Name Service)

iv) LMHOSTS file is a text file that maps the IP addresses to the ----------------. (NetBIOS names)

Q.2 Write short Notes:

i) NetBIOS

ii) WINS

CHAPTER 17

DHCP SERVER

17.1. **Dynamic IP Configuration**

DHCP (Dynamic Host Configuration Protocol) is used to assign an IP address dynamically. *By default, when TCP/IP is installed on a windows 2000 server computer, the computer is configured for dynamic IP configuration. If your computer is configured for manual IP configuration and you want to use dynamic IP configuration. The DHCP server provides centralized management of IP address assignment.*

17.2. **Configuring a Computer to Obtain IP Address From a DHCP Server**

1. Right click My Network Places and choose Properties.
2. Right click Local Area Connection and choose Properties.
3. Local Area Connection Properties dialog box appears. Select the Internet Protocol (TCP/IP) and click the Properties button.
4. Internet Protocol (TCP/IP) Properties dialog box appears. Choose “Obtain an IP address automatically”. Then click the OK button.

17.3. **Installing DHCP Service**

Before installing DHCP service, the TCP/IP must be installed and manually configured on the Windows 2000 Server. The installation procedure for the DHCP is same as for the DNS, choose DHCP instead of DNS. The steps are as follows:

Steps

1. Select Start → Settings → Control Panel.
2. Double click Add/Remove Programs.
3. Add/Remove Properties dialog box appears. Click Add/Remove Windows Components.
4. Windows Components Wizard starts. In the Windows Components screen, select Networking Services and then click Details.
5. Networking Services dialog box appears. Select Dynamic Host Configuration Protocol (DHCP) and click OK.
6. In the Windows Components screen, click Next.
7. In the Completing Wizard screen click Finish button.

17.4. **Creating a DHCP Scope**

A DHCP scope is a range of IP addresses on a DHCP Server that can be assigned to the DHCP clients that are available on a single subnet mask. Steps to create a DHCP scope are as follows:

1. Select Start → Programs → Administrative Tools → DHCP.
2. Select the DHCP Server for which you want to create a scope.
3. Select Action → New Scope.
4. In the Scope Name screen, type the Name and Description for the scope and click Next.
5. IP Address Range screen appears. In the “Start IP address” and “End IP address” text boxes enter the range.

6. Enter the subnet mask or the length of the network address. For example Class A has 8 bits, Class B has 16 bits and Class C has 24 bits length.
7. Add Exclusion dialog box appears. In this, add IP address range, which is already in use or reserved.
8. Lease Duration dialog box appears. In this you can specify how long the client will be able to use the IP address before the IP address is returned to the DHCP scope.
9. Configure DHCP dialog box appears. In this choose "Yes, I want to configure these options now". If you want to configure settings for DNS, Router and WINS then select "No, I will configure these options later".
10. Click Finish.

17.5. **Special Kinds of DHCP Scopes**

⇒ Superscope: This type of scope contains range of IP addresses that are spread over several subnet masks.

⇒ Multicast Scope: This type of scope contains a range of class D IP addresses.

17.6. **Authorising a DHCP Server in Active Directory**

If a DHCP Server is a part of Active Directory, then you must authorize the DHCP Server to assign IP addresses to the network computers.

Steps to Authorize DHCP Server

1. Select Start → Programs → Administrative Tools → DHCP.

2. Select the DHCP Server, you want to authorize.

3. Select Action → Authorize.

4. Wait for two minutes and then select Action → Refresh.

5. The DHCP Server is now authorized. *The icon next to the DHCP server now contains a green, upward pointing arrow (instead of a red, downward arrow).*

6. Close DHCP

17.7. **Configuring DHCP for DNS Integration**

By default, all Windows 2000 computers that have TCP/IP installed, automatically register their IP addresses and host names with the DNS Server on the network. Windows NT, Windows 95 and Windows 98 computers are not capable of dynamically registering their IP addresses and host names information with a DNS Server.

If you want that the DNS Server should support dynamic update, then configure the DHCP for DNS integration. The steps are as follows:

1. Select Start → Programs → Administrative Tools → DHCP.

2. Select the DHCP Server you want to configure for integration. Select Action → Properties.

3. In the DHCP Properties dialog box, click the DNS tab.

4. Check “Enable updates for DNS clients that do not support dynamic updates” for Non-Windows 2000 clients and “Always Update DNS” for Windows 2000 clients check boxes.

5. Close DHCP.

Practical

i) Configuring a computer to obtain IP address from a DHCP Server.

ii) Installing the DHCP Server.

iii) Creating a DHCP scope.

iv) Authorising a DHCP Server in Active Directory.

v) Configuring DHCP for DNS integration.

Exercise - 17

Q.1 Fill in the blanks:

i) DHCP stands for ________. (Dynamic Host Configuration Protocol)

ii) DHCP is used to assign ________. (IP address dynamically)

Q.2 Write short Notes:

i) DHCP

ii) Special kinds of DHCP scopes

iii) DHCP scope

CHAPTER 18

NW LINK IPX/SPX/NETBIOS

18.1. **Introduction**

NW Link IPX/SPX/Net BIOS is a routable protocol, which is used to provide connectivity with the Netware servers.

If you want to access Netware file and print services, you need to install NW link and Client Services for NetWare (CSNW) on your windows 2000 client or Gateway Services for NetWare (GSNW) on your windows 2000 server computer. *(CSNW and GSNW are software packages that work at the upper layers of the OSI model to allow access to net ware file and print services).*

18.2. **Installing NW Link IPX/SPX/Net BIOS**

To install NW Link, follow the following steps:

1. Right click My Network Places and choose Properties.
2. Right click Local Area Connection and choose Properties.
3. Local Area Connection Properties dialog box appears. Click the Install button.
4. Select Network Component Type dialog box appears. Select Protocol and click the Add button.
5. Select Network Protocol dialog box appears. Select NW Link IPX/SPX/NetBIOS Compatible Transport Protocol from the list and then click the OK button.

Practical

Installing NW Link IPX/SPX/NetBIOS.

Exercise - 18

Q.1 Fill in the blanks:

i) NW Link IPX/SPX/NetBIOS is used to provide connectivity with ________ servers. (Netware)

Q.2 Write short Notes on NW Link IPX/SPX/NetBIOS

CHAPTER 19

WEB SERVER

19.1. <u>**Introduction**</u>

When IIS is installed on a Windows 2000 computer, then it acts as a Web Server.

19.2. <u>**Installing IIS**</u>

Internet Information Services (IIS) is used to publish multiple web sites on the Internet or on a private intranet. *IIS is a full-featured web server, designed to support heavy Internet usage*.

By default IIS is installed and if not installed you can install IIS through the following steps:

1. Select Start → Settings → Control Panel
2. Double click the Add/ Remove Programs icon.
3. In the Add/Remove Programs window, click the Add/Remove Windows Components.
4. Windows components are displayed in which check the Internet Information Services (IIS) check box and click the Next button.
5. When prompted, insert the Windows 2000 Server CD and click the OK button.
6. After copying all of the files, you will see Completing the Windows Components Wizard. Click the Finish button.
7. Close the Add/Remove Programs window.

19.3. Configuring and Managing IIS

When IIS is installed, you will see the Internet Services Manager program item in Administrative Tools. This is the primary utility used to manage IIS.

The following services are installed as a part of IIS.

- File Transfer Protocol (FTP), which is used to transfer files between two computers using the TCP/IP protocol.
- Hyper Text Transfer Protocol (HTTP), which is used to create contents for web sites as well as to navigate websites.
- Simple Mail Transfer Protocol (SMTP), which is used to transfer mail between two SMTP mail systems.
- Network News Transfer Protocol (NNTP), which is used to provide newsgroup services between NNTP servers and NNTP clients.

19.4. Configuring a Web Site

Once the IIS is installed on Windows 2000 computer, it is called a Web Server. When the web server is installed, it creates a default web site. The contents of the default web site are located in the Drive:**\Inetpub\wwwroot**.

To manage any of the web sites select Start → Programs → Administrative Tools → Internet Services Manager. Internet Services Manager has following items by default:

(i) Default FTP Site

(ii) Default Web Site

(iii) Administration Web Site

(iv) Default SMTP Virtual Server

Note: These default sites and virtual servers are provided to help you get IIS up and running as quickly as possible.

WEB SITE PROPERTIES

To access a web site's properties, right click the web site you want to manage in the IIS windows and select properties from the pop up menu. This brings up the web site properties box.

The Web Site Properties Dialog Box Tabs:

Tab	*Description*
Web site	*Allow you to configure web site identification, connections and logging.*
Operators	*Allows you to configure which users and groups can manage the web site*
Performance	*Allow you to configure performance tuning. Bandwidth throttling, and process throttling*
ISAPI filters	*Allow you to set ISAPI (Internet Server Application Programming Interface) filters.*
Home directory	*Allow you to configure the content location, access permissions. Content control, and application settings*
Documents	*Allow you to specify the default document users will see if they access your web site without specifying a specific document*
Directory security	*Allow you to configure anonymous access and authentication control, IP address and domain name restrictions, and secure communications.*
HTTP headers	*Allows you to configure values that will be returned to web browsers in the hypertext mark up language (HTML) headers of the web pages*
Custom errors	*Allow you to present a customized error message that will appear when there is a web browser error.*

Server extensions	*Allow you to configure publishing controls for frontpage options.*

1. ***Web Site Tab****:*

The web site tab includes options for identifying the web site, controlling connections, and enabling logging.

Web Site Identification*:*

Description: By default, the web site description is the same as the name of the web site. You can change this.

IP Address: If you leave the IP address at the default setting of all unassigned, all of the IP addresses that are assigned to the computer and that have not been assigned to other web sites will be used.

TCP Port: The TCP port specifies the port that will be used to respond to HTTP requests by default. The default TCP port that is used is 80. If you change this value, clients attempting to connect to the web site must specify the correct port value. This option can be used for additional security.

Connections*:*

By this you can allow unlimited connections to the web site, or you can control the number of connections. To specify a connection limit, select the limited to option and enter and enter the maximum number of connections allowed.

The connection timeout is used to specify how long an inactive user can remain connected to the web site before the connection is automatically terminated.

If you select the HTTP keep–Alives enabled option, the client will maintain an open connection with the server, as opposed to opening a new connection for each client request. This enhances client performance, but may degrade server performance.

Logging*:*

Logging is used to enable logging features, which record details of web site access. If logging is enabled, you can select from several log formats that collect information in a specified format. If you want to log user access to the web site, the log visits check box on the home directory tab must also be checked (which is the default setting).

2. ***Operators Tab****:*

You can configure which users and groups are able to manage that web site through the operators tab, by default, the administrators group is assigned operator privileges.

3. ***Performance Tab**:*

This allows you to configure performance tuning, bandwidth throttling, and process throttling.

Performance Tuning:

Performance tuning allows you to tune your web site based on the number of hits your web site is expected to receive each day.

Bandwidth Throttling:

Bandwidth is defined as the total capacity of your transmission media. This can be expressed as bits per second (BPS) or as Hertz (frequency). IIS allows you to specify how much bandwidth can be used in terms of kilobytes per second (KBS).

If the server is used to host other web sites or is used for other purposes, such as hosting an e-mail server, you might want to limit the maximum amount of bandwidth that can be used by your web server. This is called bandwidth throttling. If bandwidth throttling is not enabled, your web server can use the maximum amount of bandwidth throttling is not enabled, your web server can use the maximum amount of bandwidth that is available.

Process Throttling:

When you enable process throttling, you can specify the percentage of CPU processing that can be used by the web site, if you select the enforce limits option, whatever value is for process throttling will be enforced. If this option is not selected, the site will be able to exceed the process throttling settings, and an event will be written to the event log.

4. ***ISAPI filters Tab***

Internet Server Application Programming Interface (ISAPI) filters direct web browser requests for specific URLs, which are then run. ISAPI filters are commonly used to manage customized logon authentication. These filters work by monitoring

HTTP requests and responding to specific events that are defined through the filter. The filters are loaded into the web site's memory.

Through the ISAPI filters tab, you can add ISAPI filters for your web site, the filters are applied in the order they are listed in the list box.

5. ***Home Directory Tab**:*

The home directory tab includes options for the content location, access permissions, content control, and application settings.

Content Location:

The home directory is used to provide web content. The default directory is c:\Inetpub\wwwroot. You have three choices for the location of the home directory.

- *A directory on the local computer*
- *A share on another computer (stored on the local network and identified by a UNC name).*
- *A redirection to a resource using a URL*

***Access Permissions and Content Control**:*

Access permissions define what access users have to the web site. Content control specifies whether logging and indexing are enabled. The access permissions and content control options are described in table 10.2

Option	***Description***
Script source access	*Allows users to access source code for scripts, such as asp (active server pages) applications, if the user has either read or write permissions.*
Read	*Allows users to read or download files located in your home folder. This is used if your folder contains HTML files. If your home folder contains CGI applications or ISAPI applications, you should uncheck this option so that users cant download your application files.*
Write	*Allows users to modify or add your web content. This access should be granted with extreme caution.*

6. ***Document Tab**:*

This allows you to specify the default document users will see if they access your web site without specifying a specific document. You normally set your default document as your web site's home page.

7. ***Directory Security**:*

This tab includes options for anonymous access and authentication control, IP address and domain name restrictions and secure communications.

8. ***HTTP Headers**:*

This tab allows you to configure values that will be returned to web browsers in the HTML headers of the web pages.

9. ***Custom Errors Tab**:*

If the web browser encounters an error it will display an error message.

10. ***Server Extensions**:*

This tab allows you to configure publishing controls for FrontPage options.

PRACTICAL

(i) Installing IIS.

EXERCISE

Q.1 Fill in the blanks:

i) After installing IIS on a Windows 2000 computer, it acts as a --------------------. (Web Server)

ii) IIS stands for --------------. (Internet Information Services)

iii) IIS is used to ---------------. (publish multiple web sites)

iv) IIS is managed through --------------------. (Internet Services Manager which is under Administrative Tools)

v) NNTP stands for ---------------. (Network News Transfer Protocol)

Q.2 Short Notes:

i) Web Server
ii) IIS
iii) Internet Services Manager

CHAPTER 20

WINDOWS 2000 BOOT PROCESS

20.1. <u>**Introduction**</u>

The boot process starts when you turn on your computer and ends when you log on to Windows 2000.

The Windows 2000 boot process consists of following major stages:

- Pre-boot Sequence
- Boot Sequence
- Kernel Loading
- Kernel Initialization
- Logon

20.2. <u>**Pre-Boot Sequence**</u>

A normal boot process begins with the pre-boot sequence, in which your computer starts up and prepares for booting the operating system.

System files reside in system partition and most of the boot process files reside in the root of the boot partition. The default folder for NT files is WINNT. The system partition and boot partition can be on the same partition or on different partitions.

File attributes are used to specify the properties of a file. Examples of the attributes are system (S), Hidden (H), and Read-only (R). This is important to know because, by default, system and hidden files are not listed in windows explorer by selecting tools → folder options and clicking the view tab. In this dialog box, select the show hidden files and folders option, and uncheck the hide file extensions for known file types and hide protected operating system files options.

i) <u>Files Accessed in the Pre-Boot Sequence</u>

During the pre-boot sequence, your computer accesses the NTLDR file. This file is used to control the Windows 2000 boot process until control is passed to the NTOSKRNL file for the boot sequence. The

NTLDR file is located in the root of the system partition. It has the file attributes of System, Hidden and Read only.

ii) <u>Steps in the Pre-Boot Sequence</u>

1. When the computer is powered on, it runs a Power On Self Test (POST) check. *The POST detects the process you are using, how much memory is present, what hardware is recognized, and whether the bios (basic input/output system) is standard or has plug and play capabilities.*
2. The BIOS points to the boot device and the Master Boot Record (MBR) is loaded.
3. The MBR points to the active partition. The active partition is used to specify the partition which should be used to boot the operating system. This is normally the C: drive. Once the MBR locates the active partition, the Boot Sector is loaded into the memory and is executed.
4. The boot sector points to the NTLDR file and this file executes. The NTLDR file is used to initialize and start the Windows 2000 boot process.

iii) <u>Possible Errors During the Pre-Boot Sequence</u>

If you see errors during the pre-boot sequence they are probably not related to the Windows 2000 Server because the operating system has not yet been loaded. The following are some of the common causes for errors during the pre-boot stage:

Improperly configured hard ware	If the POST does not recognize your hard dive, the pre boot stage will fail. *This error is most likely to occur in a computer that is still being initially configured. If everything has been working properly and you have not made any changes to your configuration, a hardware error is unlikely.*
Corrupt MBR	Viruses that are specifically designed to infect the MBR can corrupt it. You can protect your system from this

	type of error by using virus-scanning software. *Also, most virus scanning programs can correct an infected MBR.*
No partition is marked as active	This can happen if you used the FDISK utility for creating partition and did not make a partition active. *If the partition is FAT 16 or FAT 32 and on a basic disk, you can boot the computer to DOS or windows 9x with a boot disk, run mark a partition as active. If you created your partitions as a part of the windows 2000 installation and have dynamic disks, marking an active partition is done for you during installation.*
Corrupt or missing NTLDR file.	If the NTLDR file does not execute, it may have been corrupted or deleted *(by a virus or malicious intent)*. You can restore this file through the ERD (Emergency Repair Disk).
System files run from DOS or Windows 9.x after Windows 2000 installation	The system (system files) has been transferred from DOS or Windows 9.X. If you have done this, the only solution is to reinstall Windows 2000.

20.3. **Boot Sequence**

When the pre-boot sequence is completed, the boot sequence begins. This includes the following phases:

(i) Initial boot loader phase

(ii) Operating system selection phase

(iii) Hardware detection phase.

a) Files Accessed in the Boot Sequence

Along with the NTLDR file, the following files are used during the boot sequence:

- BOOT. INI: This file is used to build the operating system menu choices that are displayed during the boot process. It is also used to specify the location of the boot partition. This file is located in the root of the system partition. It has System and Hidden attributes.
- BOOTSECT.DOS: This file is an optional file that is loaded if you choose to load an operating system other than Windows 2000. It is used only in dual boot or multi boot computer. This file is located in the root of the system partition. It has System and Hidden file attributes.
- NTDETECT.COM: This file is used to detect any hardware that is installed and to add information about the hardware to the registry. This file is located in the root of the system partition. It has System, Hidden and Read only file attributes.
- NTBOOTDD.SYS: This file is an optional file and is used when you have a SCSI (Small Computer System Interface) adapter. *(This option is not commonly implement) this file is located in the root of the system partitions. It has the file attributes of system and hidden.*
- NTOSKRNL.EXE: This file is used to load the Windows 2000 operating system. This file is located in WINNT\SYSTEM32 folder and has no file attributes.

b) Steps in the Boot Sequence

1. For the initial boot loader phase, NTLDR switches the processor from real mode to 32-bit flat memory mode and starts

the appropriate Mini File System Drivers. Mini file system drivers are used to support your computer's file systems.

2. For the operating system selection phase, the computer reads the BOOT.INI file, which builds operating system choices. If you choose an operating system other than Windows 2000, the BOOTSECT.DOS file is used to load the alternate operating system and the Windows 2000 boot process terminates. If you choose a Windows 2000 operating system, the Windows 2000 boot process continues.
3. If you choose Windows 2000 operating system, the NTDETECT.COM file is used to perform hardware detection. Any hardware that is detected is added to the registry, in the HKEY _LOCAL_MACHINE key. Some of the hardwares that NTDETECT.COM will recognize includes communication and parallel ports, the keyboard, the floppy disk drive, the mouse, the SCSI adapter and the video adapter.
4. Control is passed to the NTOSKRNL.EXE to start the kernel loading process.

c) Possible Errors During the Boot Sequence

Missing or corrupt boot files	If any of the NTLDR, BOOT.INI, BOOTSECT.DOS, NTDETECT.COM or NTOSKRNL.EXE is corrupt or missing, *(by a virus or malicious intent,)* the boot sequence will fail. You will see an error message that indicates which file is missing or corrupt. You can restore these files through the ERD.
Improperly	If you have made any changes to your disk

configured BOOT.INI file	configuration and did not make appropriate changes in the BOOT.INI file, then your computer will not start.
Unrecognizable or improperly configured hardware.	If you have serious errors that cause NTDETECT.COM to fail, then you should resolve the hardware problems. *If your computer has a lot of hardware, remove all of the hardware that is not required to boot the computer. Add each piece of hardware one at a time and boot the computer. This will help you identify which piece of hard ware is bad or is confliction for a resource with another device.*

20.4. **Kernel Loading Sequence**

In the kernel load sequence, the Hardware Abstraction Layer (HAL), computer control set and low-level device drivers are loaded.

The kernel loading sequence consists of the following steps:

1. The NTOSKRNL.EXE file is loaded and initialized.
2. The HAL is loaded. This is the HAL that makes Windows 2000 portable to support different platforms such as Intel and Alpha.
3. The computer control set is used to control system configuration, such as list of device drivers that should be loaded.
4. Low-level device drivers, such as disk drivers are loaded.

Note: If you have problems in loading the Windows 2000 kernel, then you will have to reinstall the operating system.

20.5. **Kernel Initialisation Sequence**

In this the HKEY_LOCAL_MACHINE\HARDWARE registry and clone control set are created, device drivers are initialized and high order subsystems and services are loaded.

Steps:

- Once the kernel has been successfully loaded, the registry key HKEY_LOCAL_MACHINE\HARDWARE is created. *This registry key is used to specify the hardware configuration of hardware components when the computer is started.*

- The clone control set is created. The clone control set is an exact copy of the data that is used to configure the computer and does not include changes made by the startup process.

- The device drivers that were loaded during the kernel load phase are initialized.

- Higher order sub systems and services are loaders.

20.6. **Logon Sequence**

In the logon sequence, the user logs on to windows 2000 and any remaining services are loaded.

Steps:

1. After completion of kernel initialization sequence, the Logon to Windows dialog box appears. At this point, you should type in a valid Windows 2000 username and password.

The service controller performs a final scan of HKEY_ LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services to see if there are any remaining service that need to be loaded.

If logon errors occur, they are usually due to an incorrect username or password or the unavailability of a domain controller to authenticate the request.

Error can also occur if a service cannot be loaded. If a service fails to load, you will see a message in event viewer.

20.7. **BOOT.INI File**

BOOT.INI file is located in the active partition and is used to build the boot loader menu and to specify the location of the Windows 2000 boot partition. It also specifies the default operating system that should be loaded. *You can open and edit this file to add switches or options that allow you to control how the operation system is loaded. You can edit a BOOT.INI file in notepad.* It uses ARC naming conventions.

ARC Naming Conventions

ARC stands for Advanced RISC Computing. RISC stands for Reduced Instructions Set Computing. In the BOOT.INI file, the ARC path is used to specify the location of the boot partition within the disk channel.

multi(w) or scsi(w)	Identifies the type of disk controller that is being used by the system. *The multi option is used by IDE controllers and SCSI adapters that use the SCSI BIOS. The scsi option is used by SCSI adapters that do not use the SCSI BIOS.* The letter (w) represents the number of the hardware adapter you are booting from.
disk(x)	Indicates which SCSI adapter you are booting from, if you use the SCSI option. If you use multi, this setting is always 0.
rdisk(y)	Specifies the number of the physical disk to be used, 0 means first disk (Primary) and 1 means second disk (Secondary). *In an IDE environment, it is the ordinal of the disk attached to the controller and will always be a 0 or 1. On a SCSI system, this is the ordinal number of the SCSI drive.*
partition(z)	Specifies the partition number that contains the operating system files. The first partition is always 1.

Example of BOOT.INI file

Multi(0) disk(0) rdisk(0) partition(1)\WINNT= “Microsoft Windows 2000 Server:”

This indicates:

- multi(0) is an IDE controller or a SCSI controller with the BIOS enabled.
- disk(0) is 0 since the multi option has been used.
- rdisk (0) specifies that the first disk on the controller is being used.
- partition (1) specifies that the system partition is on the first partition.
- \WINNT indicates the folder that is used to store the operating system files.
- “Microsoft Windows 2000 Server” is what the user sees in the boot menu.

BOOT.INI Switches

When you edit your BOOT.INI file, you can add switches or options that allow you to control how the operating system is loaded.

Switch	Description
/basevideo	Boots the computer using a standard VGA driver. *This option is used when you change your video driver and then cannot use the new port.*
/maxmem:n	*Specifies the maximum amount of RAM that is recognized. This option is sometimes used in test environments where you want to analyze performance using different amounts of memory.*
/noguiboot	Boots Windows 2000 without loading the GUI. With this option, a command prompt appears after the boot process ends.

Practical

i) Editing BOOT.INI.

EXERCISE

Q.1 Fill in the blanks:

i) NTLDR file is accessed during the ------------ sequence. (Pre-Boot)

ii) HAL stands for -------------. (Hardware Abstraction Layer)

iii) ARC stands for ---------------. (Advanced RISC Computing)

iv) RISC stands for -----------------. (Reduced Instructions Set Computing)

v) Operating system selection choice menu appears in ---------------- file. (BOOT.INI)

vi) BOOT.INI file is located in the -----------------. (root of the system partition)

vii) BOOTSECT.DOS is loaded if you choose ------------. (an OS other than Windows 2000)

viii) NTOSKRNL.EXE file is located in the ---------------. (WINNT\SYSTEM32)

Q.2 Short Notes:

i) Stages of boot process

ii) BOOT.INI

iii) NTOSKRNL.EXE

iv) ARC Naming convention

v) BOOTSECT.DOS

vi) NTDETECT.COM

Q.3 Explain complete boot process in Windows 2000.

CHAPTER 21
ADVANCED STARTUP OPTIONS

21.1. **Advanced Startup Options**

Advanced Startup options are used to troubleshoot the errors which occur during booting. To access Advanced Startup Options, press F8 key when prompted or at the beginning of the Windows 2000 Server boot process. The Advanced Startup options are as follows:

- Safe mode

  In the safe mode, the server loads the minimum device drivers required to boot the system. If your server is able to boot through the safe mode, then you can find out the driver, which is causing the trouble using Control Panel or Device Manager.

- Safe Mode With Networking

  This is the same as the safe mode option, but it adds the networking features.

- Safe Mode With Command Prompt

  This option starts the computer in safe mode but instead of loading the graphical interface, it loads a command prompt.

- Enable Boot Logging

  Boot logging creates a log file that tracks the loading of drivers and services. This allows you to log all the events that take place during a normal boot sequence. This log file is used to troubleshoot the boot process and the log information is stored in **\Winnt\ntbtlog.txt**.

- Enable VGA Mode

  This option loads a standard VGA driver without starting the computer in Safe Mode. *You might use this mode if you changed* *your video driver and, did not test it and tried to boot Windows 2000 with a bad drive that may not allow you to access video.*

- Last Known Good Configuration

  This option boots using the Registry information which was saved last time when the computer was successfully booted.

- Directory Services Restore Mode

  This option is used when the server is configured as Domain Controller to restore the Active Directory.

- Boot Normally

  Boot in the default manner.

Practical

i) Using different Advanced Startup Options.

EXERCISE

Q.1 Explain advanced startup options in Windows 2000.

CHAPTER 22

STARTUP AND RECOVERY OPTIONS

22.1. **Startup and Recovery Options**

These options are used to specify the default operating system that is loaded and the action to be taken in the event of system failure.

To access the Startup and Recovery options proceed as follows:

(i) Right click My Computer and select Properties from the pop up menu.

(ii) Click the Advanced tab and then click the Startup and Recovery button

OR

(i) Select Start → Settings → Control Panel

(ii) Double click the System icon.

(iii) Click the Advanced tab.

(iv) Click the Startup and Recovery button.

22.2. **Different Startup and Recovery Options**

Options that can be specified through the Startup and Recovery are as follows:

Option	Description
Default operating system	Specifies the operating system that should be loaded by default. *If no selection is made the operating system selection menu (If your computer dual boots or multi boots and an operating system selection menu appears during boot up).*
Display list of operating system for x	Specifies how long the operating system selection menu should be available before the default selection is loaded. *(If your computer dual boots or multi boots and an operating system*

seconds	*selection menu appears during boot up). By default, this option is set to 30 seconds.*
Write an event to the system log	Specifies that an entry should be made in the system log whenever a system failure occurs. *By default, this option is enabled, which allows you to track system failures.*
Send an administrative alert	Specifies that a pop up alert message should be sent to the administrator whenever a system failure occurs. *By default, this option is enabled, so the administrator is notified of system failure.*
Automatically reboot	Specifies that the computer should automatically reboot in the event of a system failure. *By default, this option is enabled, so the system restarts after a failure without intervention. You would disable this option if you wanted to see the blue screen for analysis.*
Write debugging information	Specifies that the debugging information (a memory dump) should be written to a file. *You can choose not to create a dump file or to create a small memory dump (64KB) file, a kernel memory dump file, or a complete memory dump file. Complete, memory files require free disk space equivalent to your memory and a page file that is at least as large as your memory with an extra 2MB. The default setting is to write debugging information to a complete memory dump.*
Overwrite any existing file	If you have created any dump files, then it allows you to create a new dump file that will overwrite the old dump file or to keep all the dump files each time a system failure occurs. *This option is selected by default.*

Practical

i) Using Startup and Recovery options.

Exercise - 22

Q.1 Fill in the blanks:

i) Startup and Recovery options are used to specify ________ and ________. (the default operating system, the action to be taken in the event of system failure)

ii) Startup and Recovery options can be accessed by ________. (right clicking My Computer →Properties →Advanced → Startup and Recovery)

Q.2 Short Notes:

i) Startup and Recovery

ii) Accessing Startup and Recovery options

CHAPTER 23

SETUP BOOT DISK AND BACKUP

23.1. **Introduction**

From server boot disks, you can perform the following tasks:

- Reinstall the Windows 2000 Server operating system if you do not have access to the CD-ROM drive.
- Use the Recovery console.
- Use an ERD.

To create the Windows 2000 Server startup disks, you require four high-density floppy disks. Label them as follows:

- Windows 2000 server setup boot disk # 1
- Windows 2000 server setup disk # 2
- Windows 2000 server setup disk #3
- Windows 2000 server setup disk #4

23.2. **Creating a Server Setup Boot Disk**

The command/utility to create setup boot disks from Windows 2000 or Windows 9.x is MAKEBT32.EXE and the command to make setup boot disks from a 16 -bit operating system is MAKEBOOT.EXE.

Steps:

1. Insert the Windows 2000 Server CD into your CD-ROM drive.
2. Select Start → Run → Browse. Select your CD ROM drive in the dialog box that appears. Select BOOTDISK and then select MAKEBT32 and click the OK button.
3. Command Prompt dialog box appears. Specify the floppy drive letter. *This is normally your A: drive.*

4. Insert the disk labelled as Windows 2000 Server Setup Boot Disk # 1, 2, 3 and 4 one after another. The files will be copied.

23.3. **Backup Utility**

The Windows 2000 Backup utility allows you to create and restore backups and to create an Emergency Repair Disk (ERD). Backup protects your data in the event of system failure by storing the data on another medium, such as another hard disk or a tape. If your original data is lost due to corruption, deletion, or media failure, you can restore the data using your backup.

23.4. **Emergency Repair Disk (ERD)**

ERD is used to repair and restart Windows 2000 Server in case your computer does not start or system files have been damaged. ERD can repair the basic system, system files, partition boot sector, startup environment and the registry (return the registry to its original configuration).

23.5. **Creating an Emergency Repair Disk**

1. Select Start → Programs → Accessories → System Tools → Backup.
2. Click the Emergency Repair Disk button.
3. Emergency Repair Disk dialog box appears. Insert a blank, formatted floppy disk into drive A:
4. Check the “Also back up the registry to the repair directory” check box and click OK.
5. The system data will be copied to the ERD.
6. A Confirmation dialog box appears. Click the OK button to close the dialog box.

23.6. **Using an Emergency Repair Disk**

ERD is not a bootable disk and can be accessed only by using the Windows 2000 Server Setup CD or the Windows 20000 Server Setup diskettes that have been created from the CD. Follow the following steps to use an ERD:

1. Restart you computer using the Windows 2000 Server Setup Boot disk #1.
2. When prompted, insert the Windows 2000 Server Setup disks #2, #3 and #4 and press Enter after inserting.
3. Welcome to Setup dialog box appears. To repair a Windows 2000 installation, press the R key.
4. Windows 2000 Repair options menu appears. To repair Windows 2000 using the ERD, press the R key.
5. Press the M key to choose Manual repair or the F key to choose Fast repair. *The manual repair option inspects the startup environment, verify the windows 2000 system files, and inspect the boot sector. The fast repair option doesn't require any user input. It attempts to correct problems that relate to system files, the partition boot sector on the system disk, and the startup environment on dual boot systems.*
6. Insert your Windows 2000 ERD and press Enter. You will see one more dialog box indicating that you should insert your ERD. Press Enter again.
7. Press Enter to examine the drive or press Esc to skip the drive examination.
8. If you choose to examine your computer's drives, you will be asked to insert the Windows 2000 Server CD into your CD ROM drive and press Enter. The emergency repair process will examine the files on your hard disk.

9. When the repair process is complete, you are prompted to remove floppy from your computer. Then your computer will restart automatically.

23.7. **Using Backup Wizard**

Before you start the backup, you should be logged on as Administrator or a member of the Backup Operators group.

Steps:

1. Click Start → Programs → Accessories → System Tools → Backup.
2. Backup [Untitled] dialog box appears.
3. Click the Backup Wizard button under the Welcome tab.
4. Welcome to the Windows 2000 Backup and Recovery Tools dialog box appears. Click the Next button.
5. What to Back Up dialog box appears. This dialog box allows you to select the items you want to back up. You can choose to back up everything or back up just selected files, drives or network data or back up only the system state data and then click the Next button. *System state data includes system configuration information. For this example, select the back up selected files, drives, or network data radio button, then click the next button.*
6. Items to Back Up dialog box appears. Check the items you want to back up and click the Next button.
7. Where to Store the Backup dialog box appears. You can either type the name of the backup media or filename or click the Browse button to locate it. Clicking the Browse button brings up the Open dialog box. Select the drive, give file name to backup *(for example, you might use the date as the file name),* and click the Option button. You

will return to Where to Store the Backup dialog box. When your backup media or filename path is correct, click the Next button.

8. Completing the Backup Wizard dialog box appears. If all of the information is correct, click the Finish button.

<u>*Using the backup wizard*</u>

1. *Create a folder on your D: drive called DATA. Create some small text files in this folder. The size of all of the files combined should not exceed 1MB.*
2. *Select Start → Programs → Accessories → System Tools → Backup.*
3. *In the opening backup windows, click the backup wizard button.*
4. *In the welcome to the windows 2000 backup recovery tools, drives, or network data radio button. Then click the next button.*
5. *In the what to back up dialog box, click the back up selected files, drives, or network data radio button. Then click the next button.*
6. *In the items to back up dialog box, select my computer, expand D:; and check the DATA folder. Click the next button.*
7. *In the where to store the backup dialog box click the brows button in the open dialog box select floppy (A:). For the filename, enter the data (in the mm/dd/yy format) then click the open button.*
8. *In the where to store the backup dialog box, click the next button.*
9. *Verify your selections in the completing the backup wizard dialog box. Then click the finish button.*
10. *When the backup wizard completes click the Report button in the backup progress dialog box. This will show the backup log in a Notepad window. Close this window when you are finished viewing the report.*
11. *Close all to the backup wizard dialog boxes.*

23.8. Managing System State Data

System state data refers to a collection of system specific configuration information. You can manage the availability of system state data by using the Backup utility.

<u>Backing Up System Data</u>

1. Select Start → Programs → Accessories → System Tools → Backup.
2. In the Backup window, click the Backup tab.
3. Under My Computer, check the “System State” check box and select the backup media or file name that will be used for the backup.
4. Click the Start Backup button.
5. When the backup is complete, click the Report button in the Backup Progress dialog box.
6. Backup log appears in a Notepad window. Close this window when you have finished viewing the report.
7. Close all of the backup dialog boxes.

23.9. **Configuring Backup Options**

To access the backup options proceed as follows:

- Click Start → Programs → Accessories → System Tools → Backup.
- Backup [Untitled] dialog box appears. Click the Backup tab.
- From menu bar, click Tools → Options.
- Options dialog box appears which has five tabs with options. These are as follows:
  - General
  - Restore
  - Backup Type
  - Backup Log
  - Exclude Files

General: It contains general information.

Restore: The restore tab options relate, how files are restored when the files already exist on the computer. *These are as follow:*

1. *Do not replace the file on my computer (recommended)*
2. *Replace the file on disk only if the file on the disk is older*
3. *Always replace the file on my computer.*

Backup Type: This tab, specify the backup type.

Option	Description
Normal	Backs up all files and sets the archive bit as marked for each file that is backed up. *Requires only tape for the restore process.*
Copy	Backs up all files and does not set the archive bit as marked for each file that is backed up. *Requires only one tae for the restore process.*
Differential	Backs up only the files that have not been marked as archived and does not set the archive bit for each file that is backed up. *Requires the last normal backup and the last different tape for the restore process.*
Incremental	Backs up only the files that have not been marked as archived and sets the archive bit for each file that is backed up. *Requires the last normal backup and all of the incremental tapes that have been created since the last normal backup for the restore process.*
Daily	Backs up only the files that have been changed today and does not set the archive bit for each file that is backed up. *Requires each daily backup and the last normal backup for the restore process.*

Backup Log: This tab specifies the amount of information that is logged during the backup process.

Excluding Files: This tab allows you to exclude specific files during the backup process.

23.10. **Restoring Data**

1. Click Start → Programs→ Accessories → System Tools → Backup.
2. Backup [Untitled] dialog box appears. Click the Restore Wizard button.
3. Welcome to the Restore Wizard dialog box appears. Click the Next button.
4. What to Restore dialog box appears. Click the filename of the backup session that you want to restore and click the Next button. *After you select the backup you want to restore, you can choose to restore the entire session, or you can selectively restore drives, folders, or files form the backup session.*
5. Completing the Restore Wizard dialog box appears. If all of the configuration information is correct, click the Finish button.
6. Enter Backup File Name dialog box appears. Specify the filename and click the OK button.
7. Wizard displays the Restore Progress dialog box. *Once the restoration process is complete, you can click the report button in this dialog box to see details of the restore session.*

23.11. **Event Viewer**

Event Viewer utility is used to track information about computer's hardware, software and security events. The information that is tracked is stored in the following log files:

- System Log: It tracks the events that are related to the Windows 2000 operating system.

- Security Log: It tracks the events that are related to the Windows 2000 auditing.
- Application Log: It tracks the events that are related to the applications that are running on your computer.

  To access the Event Viewer select Start → Programs → Administrative Tools → Event Viewer

  or

  Right click My Computer, select Manage from the pop-up menu and access Event Viewer under System Tools.

  To display the properties of the event simply click the event.

Practical

i) Creating server setup boot disks.
ii) Creating an ERD.
iii) Using an ERD.
iv) Using Backup wizard.
v) Managing system state data.
vi) Restoring data.

Exercise - 23

Q.1 Fill in the blanks.
i) For creating Windows 2000 server setup disks ________ diskettes are required. (4)
ii) Utilities used for creating boot disks are __________. (MAKEBT32 and MAKEBOOT)
iii) ERD stands for __________. (Emergency Repair Disk)
iv) ERD is created by __________ utility. (Backup)

Q.2 Short Notes
i) Creating a server setup boot disk
ii) Backup utility
iii) ERD

CHAPTER 24
RAS SERVER & VPN SERVER

24.1. <u>Introduction</u>

Remote Access Service (RAS) is used to allow remote computers to access network resources through the routing and remote access service.

24.2. <u>Protocols Supported by RAS</u>

(i) <u>Connection Protocols:</u>

PPP – Point-to-Point Protocol

SLIP – Serial Line Internet Protocol

PPTP – Point-to-Point Tunneling Protocol (VPN)

L2TP – Layer Two Tunneling Protocol (VPN)

(ii) <u>Transport Protocols:</u>

TCP/IP

IPX

NetBEUI

Apple Talk

24.3. <u>Installing RAS</u>

1. Select Start → Programs → Administrative Tools → Routing and Remote Access.
2. Routing and Remote Access window opens. In this, right click the server and select Configure and Enable Routing and Remote Access from the pop up menu.
3. Routing and Remote Access Server Wizard starts. Click the Next button to continue.

4. Common Configurations dialog box appears. Select the “Remote access server” option and click the Next button.
5. Remote Access Server Setup dialog box appears. Select, “Set up an advanced remote access server” and click the Next button.
6. Remote Client Protocols dialog box appears. This dialog box lists the protocols that are installed on your computer. Accept the default (TCP/IP / IPX) or add new and click the Next button.
7. If you specified that the RAS Server should use the TCP/IP protocol, the IP Address Assignment dialog box appears. Choose specified range of IP address or choose Automatically.
8. Managing Multiple Remote Access Servers dialog box appears. Specify RADIUS (Remote Authentication Dial-In User Service) if you have multiple RAS servers otherwise No and click the Next button.
9. Completing the Routing and Remote Access Server Setup Wizard dialog box appears. Click Finish.

24.4. **Configuring Inbound and Outbound Connections**

Inbound connections allow incoming access to the RAS Server. Outbound connections allow users to dial out to the external resources through the RAS Server. Users can connect to the RAS Server though a modem. *(RAS also can use ISDN connection, or direct connection through a null modem cable).*

You can configure inbound and outbound connections through the ports properties dialog box. To access ports properties, expand the computer in the Routing and Remote Access window, right click Ports, and select properties form the pop up menu.

In the ports properties dialog box, select devices tab and click the configure button. This brings up the configure device dialog box, this dialog box allows you to specify if computer will be used for inbound connections (the default setting) or for demand dial routing *connections. Which support both inbound and outbound connections. In addition, you can configure the telephone number that will be used for the device.*

You will configure inbound and outbound connections for the RAS server you installed. Assumes that you have a modem or null modem installed on your server.

1. Select Start → Programs → Administrative Tools → Routing and Remote Access.
2. In the Routing and Remote Access window, expand your computer, right click Ports and select Properties.
3. In the Ports Properties dialog box, select the RAS connection device you want to configure and click the Configure button.
4. In the Configure Device dialog box, select "Remote access connections (inbound only)" and "Demand dial routing connections (inbound and outbound)". Specify the telephone number to be used for outbound connections and then click the OK button.
5. In the Ports Properties dialog box, click the OK button.

24.5. **Managing RAS Server Properties**

To manage the properties of an RAS Server, right click your server in the Routing and Remote Access window and select Properties from the pop up menu. This brings up the RAS Server Properties dialog box. This dialog box contains General, Security, Event Logging and Protocol tabs for each protocol you've installed for remote access connections.

General Tab

This tab allows you to enable the computer as a router or as an RAS Server. *If you enable your computer as a router, you can specify whether the computer will route packets between two or more network segments.*

Security

This tab allows you to select and configure an authentication provider and an accounting provider. Select RADIUS, if multiple servers are there in the network, otherwise select windows authentication. *The authentication provider is the server that will provide authentication services for remote access and the accounting provider server provides the accounting services for the remote access.*

Event Logging

This tab allows you to configure how RAS Server events are to be logged. *You can choose to log errors only, log errors and warnings log the maximum amount of information, or disable event logging.*

You can also specify whether PPP Logging in enabled. If you enable PPP logging, all of the events related to the PPP Connection process will be written to the /windir/Tracing /PPP. Log file.

24.6. **Creating a Dial-up Connection to Access RAS Server**

- Click Start → Settings → Network and Dial-up Connections.
- In this, double click Make New Connection.
- Network Connection Wizard starts. Click Next.
- Network Connection Type dialog box appears. Select, “Dial-up to Private Network” option and click Next.
- Select a Device dialog box appears. In this, select the modem from the list and click Next.
- Phone Number to Dial dialog box appears. Enter the phone number and click Next.
- Connection Availability dialog box appears. Select, “For all users” and click Next.
- Completing the Network Connection Wizard screen appears. Click Finish.

24.7. Assigning Dial- in Permissions to Users

You can assign permissions to users who can access an RAS Server through the User Properties dialog box, in the Local Users and Groups utility on a member server and in the Active Directory Users and Computers utility on a Windows 2000 domain controller. *To open the user properties dialog box, access the appropriate utility, open the users folders, ad double click the user account. Click the dial in tab to see the dialog box.*

To assign Dial-in permissions to the users follow the following steps:

i) Go to the Users Properties.

ii) Click the Dial-in tab.

iii) Select "Allow Access"

Note: If a dial in tab option is not available, that means that your computer is not configured to support RAS.

24.8. Remote Access Policies

You can configure who is authorized to access your RAS Server by defining a remote access policy. *Through a remote access policy, you can create a dial in profile to specify access based on windows 20000 group membership, time of day, day of week, and type of connection. You can also configure settings for option such as maximum session time.*

Modifying an Existing Remote Access Policy

By default, there is a remote access policy called "Allow access, if dial-in permission is enabled". To access and modify this policy follow the following steps:

- Double click Remote Access Policies in the Routing and Remote Access window under RAS Server.
- Double click the policy you want to manage.
- Under Settings tab of the Policy Properties dialog box, specify grant or deny remote access permission.

Note: You can click Edit Profile button to display profile properties.

24.9. Installing a VPN Server

Virtual Private Networks (VPNs) are used to allow VPN clients to access VPN Servers through a private network or through the Internet.

Steps to Install VPN Server:

1. Select Start → Programs → Administrative Tools → Routing and Remote Access.
2. In the Routing and Remote Access window, right click the server and select "Configure and Enable Routing and Remote Access" from the pop up menu.
3. Routing and Remote Access Server Wizard starts. Click the Next button to continue.
4. Common Configurations dialog box appears. Select the "Virtual private network (VPN) server" option and click the Next button.
5. Remote Client Protocols dialog box appears. Accept the default and click the Next button.
6. Internet Connection dialog box appears. Accept the default and click the Next button.
7. IP Address Assignment dialog box appears. Specify to select range or select "Automatically" and click the Next button.
8. Managing Multiple Remote Access Servers dialog box appears. Select "No, I don't want to set up this server to use RADIUS" option and click the Next button.
9. Completing the Routing and Remote Access Server Setup Wizard screen appears. Click the Finish button.

24.10. Creating a Dial-up Connection to Access VPN Server

Steps are same as for “Creating a Dial-up Connection to Access RAS Server” covered under clause 6. of this chapter.

Practical

i) Installing an RAS Server.
ii) Configuring Inbound and Outbound connections.
iii) Managing RAS Server properties.
iv) Creating a Dial-up connection to access RAS Server.
v) Assigning Dial-in permissions to users.
vi) Modifying an existing Remote Access Policy.
vii) Installing a VPN Server.
viii) Creating a Dial-up connection to access VPN Server.

Exercise – 24

Q.1 Fill in the blanks

i) RAS stands for __________. (Remote Access Service)
ii) RADIUS stands for __________. (Remote Authentication Dial In User Service)
iii) PPTP stands for ___________. (Point to Point Tunneling Protocol)
iv) VPN stands for _________. (Virtual Private Network)

Q.2 Write short Notes:

i) RAS Server
ii) Protocols supported by RAS
iii) Managing RAS properties
iv) Assigning Dial-in permissions to users

CHAPTER 25

PROXY SERVER / SETTING UP CYBER CAFE

25.1. **Creating New Connections by Installing Network Adapters**

If you have a network adapter in your computer when you install Windows 2000, Windows 2000 automatically creates a Local Area Connection.

25.2. **Installing Modems**

You can use either the Phone and Modem Options icon or the Add/Remove Hardware icon in Control Panel to install a modem. You must be a member of the Administrators group to add and configure modems.

Installing a Modem Using Phone and Modem Options

1. Select Start → Settings → Control Panel.
2. In the Control Panel dialog box, double click Phone and Modem Options icon.
3. In the Phone and Modem Options dialog box, click the Modems tab.
4. To install a modem, click Add button.
5. Add/Remove Hardware Wizard starts and displays the Install New Modem screen. If you want Windows 2000 to detect your modem automatically, ensure that the check box against "Don't detect my modem, I will select it from a list" is

unchecked. If you want to manually select your modem, check this check box and click the Next button.

6. Follow the instructions presented on screen to complete the installation of your modem.

25.3. **Configuring Modems**

Once you have installed a modem, you can use the Phone and Modem Options icon in Control Panel to configure your modem's properties.

Configuring a Modem Using Phone and Modem Options

1.Select Start → Settings → Control Panel.

2. In the Control Panel dialog box, double click Phone and Modem Options icon.
3. In the Phone and Modem Options dialog box, click the Modems tab.
4. Under the Modems tab, select the modem you want to configure and click the Properties button.
5. Modem's Properties dialog box appears with three tabs namely General, Diagnostics and Advanced.
6. With General tab, you can configure speaker volume, maximum port speed and dial control.
7. With Diagnostics tab, you can " Record a log" of modem connection activity.
8. With Advanced tab, you can specify the "Extra initialisation commands" but generally it is not made use of. Click the OK button.

9. In the Phone and Modem Options dialog box, click OK and close the Control Panel.

25.4. <u>Creating a Dial-up Connection to the Internet on a Proxy Server</u>

1. Click Start → Settings → Network and Dial-up Connections.
2. In the Network and Dial-up Connections folder, double click Make New Connection.
3. Network Connection Wizard starts. Click the Next button.
4. Network Connection Type dialog box appears. Select the "Dial-up to the Internet" option and click the Next button.
5. Internet Connection Wizard starts. Select "I want to set up my Internet connection manually, or I want to connect through a local area network (LAN)" option and click the Next button.
6. Setting Up Your Internet Connection dialog box appears.
   i) Select "I connect through a phone line and a modem" option for a Proxy Server and click the Next button.
   ii) Select "I connect through a local area network (LAN)" option for a Proxy Server client and click the Next button.
7. Choose Modem dialog box appears. Select the modem you want to use for this dial-up connection from the drop - down list box and click the Next button.
8. In the "Internet account connection information" screen, enter your area code and telephone number of your Internet Service Provider (ISP) in the text boxes provided. Select the country

you are located in from the “Country/Region name and code” drop-down list box and click the Next button.

9. In the “Internet account logon information” screen, enter the user name and password to log on to your ISP and click the Next button.
10. In the “Configuring your computer” screen, either accept the default name for this connection or type a new name and click the Next button.
11. Set Up Your Internet Mail Account dialog box appears. Select No, if you don’t want to set up an Internet mail account now and click the Next button.
12. Completing the Internet Connection Wizard dialog box appears. Click the Finish button.
13. Web Page Unavailable While Offline dialog box appears. Click Connect to connect to the Internet.
14. Windows 2000 attempts to connect to the Internet. If your connection is configured correctly, a Connection Complete dialog box is displayed. Click OK. (If error messages are displayed, you may need to reconfigure this connection).
15. To disconnect the connection, right click the connection in the Network and Dial-up Connections folder and select Disconnect from the pop-up menu. Or, right click the network connection icon in the taskbar (near the clock) and select Disconnect from the pop-up menu.

25.5. Creating a Dial-up Connection to the Internet on a Proxy Server Client

1. Click Start → Settings → Network and Dial-up Connections.
2. In the Network and Dial-up Connections folder, double click Make New Connection.
3. Network Connection Wizard starts. Click the Next button.
4. Network Connection Type dialog box appears. Select the “Dial-up to the Internet” option and click the Next button.
5. Internet Connection Wizard starts. Select “I want to set up my Internet connection manually, or I want to connect through a local area network (LAN)” option.
6. Setting Up Your Internet Connection dialog box appears.

   i) Select “I connect through a phone line and a modem” option for a Proxy Server and click the Next button.

   ii) Select “I connect through a local area network (LAN)” option for a Proxy Server Client and click the Next button.
7. Local area network Internet configuration dialog box appears. Check the, check box against “Automatic discovery of Proxy server [recommended]”.
8. Set Up Your Internet Mail Account dialog box appears. Select No, if you don’t want to set up an Internet mail account now and click the Next button.
9. Completing the Internet Connection Wizard dialog box appears. Click the Finish button.

10. Web Page Unavailable While Offline dialog box appears. Click Connect to connect to the Internet.
11. Windows 2000 attempts to connect to the Internet. If your connection is configured correctly, a Connection Complete dialog box is displayed. Click OK. (If error messages are displayed, you may need to reconfigure this connection).

25.6. **Configuring Internet Connection Sharing**

If you have a connection to the Internet on your Windows 2000 computer (dial-up or local area) and you want to enable other computers on your local area network to use that connection to access the Internet, then you can enable Internet Connection Sharing for the specific connection that will be shared.

Connection Sharing should not be used on networks that have existing Routers, DNS Servers or DHCP Servers because once Internet Connection Sharing is enabled on a computer, Windows 2000 automatically converts that computer into the Gateway, DNS Proxy Server and DHCP Server for that network segment and assigns this computer an IP address of 192.168.0.1.

25.7. **Enabling Internet Connection Sharing**

In order to enable Internet Connection Sharing on a Windows 2000 computer, the computer must have both a local area connection and a dial-up connection to the Internet. In addition, you must be a member of the Administrators group on the local computer to enable Internet Connection Sharing. You can enable Internet Connection Sharing by using the Network and Dial-up Connections folder as explained in the subsequent text.

1. In the Network and Dial-up Connections folder, right click the Internet connection you want to share. (This must be a Dial-up Connection to the Internet). Select Properties from the pop-up menu.
2. In the Connection's Properties dialog box, click the Sharing tab. Check the, check box against "Enable Internet Connection Sharing for this connection". Once this check box is checked, the "Enable on demand dialing" check box is also automatically checked if the connection being configured is a dial-up connection. Click the OK button.
3. A Network and Dial-up Connections confirmation dialog box appears. Click Yes to enable Internet Connection Sharing.
4. Close the Network and Dial-up Connections folder.
5. Configure all computers that will use this shared connection as DHCP clients.

25.8. **Configuring a Computer as a DHCP Client to Obtain an IP Address from a DHCP Server**

1. Click Start → Settings → Network and Dial-up Connections.
2. In the Network and Dial-up Connections folder, right click the connection for which you want to configure automatic IP addressing and select Properties from the pop-up menu.

3. If the connection you selected is not a local area connection, then in the connection's properties dialog box, click the Networking tab. Then, for all connection types, highlight Internet Protocol (TCP/IP) and click the Properties button.
4. In the Internet Protocol (TCP/IP) Properties dialog box, select the "Obtain an IP address automatically" option. If you also want a DNS server address to be automatically assigned, select the "Obtain DNS server address automatically" option.
5. In the Connection's Properties dialog box, click OK.
6. Close the Network and Dial-up Connections dialog box.

Practical

i) Installing modem.
ii) Configuring modem.
iii) Creating a Dial-up connection on a Proxy Server.
iv) Creating a Dial-up connection on a Proxy Server client.
v) Enabling Internet Connection Sharing.
vi) Configuring a computer as a DHCP client.

Exercise - 25

i) Modem can be installed using either _________ or ________. (Phone and Modem Options, Add/Remove Hardware)

ii) When Internet Connection Sharing is enabled on a computer, it will automatically be assigned with an IP address of _________. (192.168.0.1)

iii) When Internet Sharing is enabled on a computer, it is automatically converted into _____________. (Gateway, DNS Proxy Server and DHCP Server)

Q.2 Write short notes:

i) Installing and configuring modem

ii) Internet Connection Sharing

iii) Proxy Server

Q.3 Explain complete procedure of setting up a Cyber Cafe.