70-215SG

Installing, Configuring and Administering Microsoft Windows 2000 Server

Study Guide

DEMO Version

Important Note
Please Read Carefully

For demonstration purpose only, this free version Chinatag study guide contains **10** full length questions selected from our full version products which have more than **200** questions each.

This Study guide has been carefully written and compiled by Chinatag certification experts. It is designed to help you learn the concepts behind the questions rather than be a strict memorization tool. Repeated readings will increase your comprehension.

For promotion purposes, all PDF files are not encrypted. Feel free to distribute copies among your friends and let them know Chinatag website. Our IT certification products start at only **$7.99.**

Study Tips

This product will provide you questions and answers along with detailed explanations carefully compiled and written by our experts. Try to understand the concepts behind the questions instead of cramming the questions. Go through the entire document at least twice so that you make sure that you are not missing anything.

Latest Version

We are constantly reviewing our products. New material is added and old material is revised. Free updates are available for 180 days after the purchase. You should check the products page on the http://www.chinatag.com website for an update 3-4 days before the scheduled exam date.

Please tell us what you think of our products. We appreciate both positive and critical comments as your feedback helps us improve future versions. Feedback on specific questions should be send to feedback@chinatag.com.

Thanks for purchasing our products and look forward to supplying you with all your Certification training needs.

Good studying!

Technical and Support Team
Chinatag LLC.

TABLE OF CONTENTS

2. Managing Windows 2000

3. Configuring the Windows 2000 Network

5. Managing Users and Computers

LIST OF TABLES

Installing, Configuring, and Administering Microsoft Windows 2000 Server

Exam Code: 070-215

Certifications:

Microsoft Certified (MCP)	
Microsoft Certified Systems Administrator (MCSA)	**Core**
Microsoft Certified Systems Engineer (MCSE)	**Core**
Microsoft Certified Database Administrator (MCSA)	**Core**

Prerequisites:
Microsoft Windows 2000 Network and Operating System Essentials

About This Study Guide
This Study Guide is based on the current pool of exam questions for the 070-215 - Installing, Configuring, and Administering Microsoft Windows 2000 Server exam. As such it provides all the information required to pass the Microsoft 070-215 exam and is organized around the specific skills that are tested in that exam. Thus, the information contained in this Study Guide is specific to the 070-215 exam and does not represent a complete reference work on the subject of Installing, Configuring, and Administering Microsoft Windows 2000 Server. This StudyGuide also includes the information required to answer questions related to the installation of Windows 2000 Professional, DNS, Active Directory, and DCHP that may be asked during the exam. Topics covered in this Study Guide includes Installing Windows 2000 Server; Upgrading from Windows NT 4.0 Server; Deploying Service Packs; Installing, Configuring, and Troubleshooting Access to Resources; Monitoring, Configuring, Troubleshooting, and Controlling Access to Printers, Files, Folders, and Shared Folders; Configuring, Managing, and Troubleshooting Distributed file system (Dfs); Monitoring, Configure, Troubleshoot, and Controlling Access to Files and Folders via Web Services; Monitoring, Configuring, Troubleshooting, and Controlling Access to Web sites; Configuring and Troubleshooting Hardware Devices and Drivers; Monitoring, and Optimizing System Performance, Reliability, and Availability; Monitoring, Configuring, and Troubleshoot Disks and Volumes; Configuring and Troubleshooting Windows 2000 Network Connections; Installing, Configuring, and Troubleshooting a Virtual Private Network (VPN); Installing, Configuring, Monitor, and Troubleshoot Terminal Services; Implementing, Monitoring, and Troubleshooting Security; Encrypting Data by using Encrypting File System (EFS).

Intended Audience
This Study Guide is targeted specifically at people who wish to take the Microsoft MCSE exam 070-215 – Installing, Configuring, and Administering Microsoft Windows 2000 Server. This information in this Study Guide is specific to the exam. It is not a complete reference work. Although our Study Guides are aimed at new comers to the world of IT, the concepts dealt with in this Study Guide are complex and require an

understanding of material provided for the MCSA / MCSE exam: 070-210 – Installing, Configuring, and Administering Microsoft Windows 2000. Knowledge of CompTIA's A+ course would also be advantageous.

> **Note:** There is a fair amount of overlap between this StudyGuide and the 070-210 StudyGuide. We would not advise skimming over the information that seems familiar. Instead, read over it again to refresh your memory.

How To Use This Study Guide
To benefit from this Study Guide we recommend that you:

- Although there is a fair amount of overlap between this StudyGuide and the 070-210 StudyGuide, the relevant information from the 070-210 StudyGuide is included in this StudyGuide. This is thus the only StudyGuide you will require to pass the 070-215 exam.
- Study each chapter carefully until you fully understand the information. This will require regular and disciplined work. Where possible, attempt to implement the information in a lab setup.
- Perform all labs that are included in this Study Guide to gain practical experience, referring back to the text so that you understand the information better. Remember, it is easier to understand how tasks are performed by practicing those tasks rather than trying to memorize each step.
- Be sure that you have studied and understand the entire Study Guide before you take the exam.

> **Note:** Remember to pay special attention to these note boxes as they contain important additional information that is specific to the exam.

Good luck!

1. Installing and Deploying Windows 2000

You can install Windows 2000 Professional or Windows 2000 Sever directly from the CD-Rom or from a network share. The Windows 2000 installation process consists of four stages:

Stage 1: Hard Drive Preparation. In text mode Setup checks the hard drive for consistency and errors. It allows you to format and create the Windows 2000 partition if you need to and copies setup files to the hard drive. Setup then reboots the computer.

Stage 2: Setup Wizard. The graphical user interface Setup Wizard gathers information from you; such as regional settings, your name and organization, the Windows 2000 CD-key, and computer name. Creates the local Administrator user account and requests a password for it.

Stage 3: Installing Network Components. After the Setup Wizard has gathered the necessary information from you in Stage 2, it begins the network components installation. It detects your network adapter card; allows you to choose which network components, such as the network client, file and printer sharing and protocols, to install; allows you to join a workgroup or domain; and installs the components you have chosen.

Stage 4: Completing the installation. The Setup Wizard completes the installation by installing the start-menu items and applying and saving the configuration settings you chose in the previous stages. It then deletes the temporary setup files and reboots the computer.

1.1 System Requirements

Before installing Windows 2000, you must ensure that the computer meets the minimum system requirements for the various versions of Windows 2000 as indicated in the table below.

TABLE 1.1: *Windows 2000 Server System Requirements*

Hardware	Minimum requirement
Processor	Pentium 133 MHz
Memory	256 MB Ram
Hard disk space	2 GB with 1 GB free space (2 GB free space recommended)
Networking	Network adapter card
Display	Video display adapter card and VGA monitor
I/O devices	Keyboard and mouse or other pointing device

Note: Windows 2000 Server supports up to 4 processors and a maximum of 4 GB Ram while Windows 2000 Advanced Server supports up to 8 processors and a maximum of 8 GB Ram and Windows 2000 Data Centre supports up to 16 processors and a maximum of 8 GB Ram.

1.2 Installing Windows 2000 from the CD-Rom

When installing Windows 2000 from the CD-Rom you can either boot directly from the CD-Rom or, if your computer system does not support booting from the CD-Rom, you can create boot disks.

1.2.1 Booting from the CD-Rom.
To install Windows 2000 form the CD-Rom you must enter your system BIOS and set the CD-Rom drive as the ***First Bootable Device***. This is usually set in the ***BIOS Feature Setup***. While you are in the BIOS Setup you should also check that ***Boot Sector Virus Protection*** is disabled. The Boot Sector Virus protection prevents any attempt is made to write to the hard drive's boot sector or partition table. When BIOS detects an attempt to write to the boot sector it stops the computer and display an error message. The Windows 2000 Setup program must write to the boot sector, therefore the ***Boot Sector Virus Protection*** must be disabled.

Once you have configured the BIOS, place the Windows 2000 installation disk in the CD-Rom and reboot the computer. During the boot process you will be prompted to ***press any key to boot from CD-Rom***. Once you have pressed a key the installation of Windows 2000 will begin.

1.2.2. Using Setup Boot Disks
You can use Setup Boot Disks if you install Windows 2000 on an x86-based computer that does not have MS-DOS or a Windows operating system installed and does not support booting from the CD-Rom. You can also use these Setup Boot Disks to start Windows 2000 when it might not be able to start on its own because of a computer error, or to initiate an emergency repair. You must run *makeboot.exe* or *makebt32.exe* from the `\bootdisk` directory on the Windows 2000 Server installation CD to create the Setup Boot Disks. This must be done on a computer that has an operating system installed on it already and will require four density floppy disks. *Makeboot.exe* is a 16-bit DOS application that runs on 16-bit operating systems like MS-DOS, Windows 3.11 and Windows 9x while *makebt32.exe* is a 32-bit application that runs on Windows NT, Windows 2000 and Windows XP. To install Windows 2000 by using the Setup Boot disks, you must first boot the computer, enter the computer's system BIOS and set the `A:\` drive as the ***First Bootable Device***. This is usually set in the ***BIOS Feature Setup***. Then insert the Windows 2000 Setup Boot Disk 1 into the `A:\` drive, the Windows 2000 Server installation CD in the CD-Rom, and save and exit the BIOS setup. The Setup Boot Disks will then boot the computer, load the necessary drivers required to access the CD-Rom drive and will start the Windows 2000 Server setup automatically.

> **Note:** Boot disks operate in a **16-bit DOS mode** environment. You therefore cannot use *winnt32.exe* to install Windows 2000 Professional as *winnt32.exe* is **32-bit** application. You must use *winnt.exe*, which is the 16-bit equivalent of *winnt32.exe*, instead.

1.3 Installing Windows 2000 over the network.
To install Windows 2000 over the network you must copy the **i386** folder from the Windows 2000 installation CD to a shared folder on the network. You must also ensure that the computer has a can connect to the network share when it has booted. To be able to boot to the network share the computer must have a **PXE compliant** network adapter. If the computer cannot be booted over the network you will have to create a network boot disk for the computer. A boot disk can be created by using the *rbfg.exe* utility. If you must use a boot disk to boot the computer, you will have to run *winnt.exe* to install Windows 2000.

> **Note:** Boot disks operate in a **16-bit DOS mode** environment. You therefore cannot use *winnt32.exe* to install Windows 2000 Professional as *winnt32.exe* is **32-bit** application. You must use *winnt.exe*, which is the 16-bit equivalent of *winnt32.exe*, instead.

1.4 Performing an Unattended Installation.

Microsoft allows for the automated installation of Windows 2000 through unattended installations. There are three mechanisms through which an unattended installation can be performed. These are through:

- unattended answer files;
- disk imaging using the System Preparation Tool; and
- Remote Installation Services

1.4.1 Using an Unattended Answer file.

The first mechanism you can use to perform an unattended installation of Windows 2000 is to use an **answer file** (See FIG 1.1). An answer file is an automated script that supply's the Windows 2000 Setup program with all the information it would require during the installation.

You can use **Setup Manager** to create and modify an answer file or you can manually create the Answer file. Setup Manager is located in the *deploy.cab* file in the */support/tools* folder on the Windows 2000 installation CD and can be extracted to your computer by double-clicking on the *deploy.cab* file. This will display the files contained in the *deploy.cab* file. Right-click on the files and select **Extract** on the menu that pops up.

You can use Setup Manager to create an answer file for an unattended installation, a sysprep install, and for a Remote Installation Services. You can also choose the level of automation. This can be:

- **Provide Defaults:** The answer file provides defaults that the user can see and allows the user to accept or change these settings during the installation.
- **Fully Automated:** No input is required from the user and the user cannot alter any of the settings.
- **Hide Pages:** All pages that the answer file provides answers for are hidden from the user.
- **Read Only:** The user can view any of the answers on the pages that are not hidden but cannot change them.
- **GUI Attended:** The first stage of the installation is automated but the user must supply the information required by the Setup Wizard during the graphical user interface stage (stages 2 and 3) of the installation.

FIG1.1: *An example of an answer file.*

Note: When creating a **Fully Automated** answer file, you must include all the information the Setup Wizard requires during the Installation this includes Product key, which must be specified in the **ProductID** variable in the **UserData** portion of the answer file. (See FIG1) If the ProductID is missing the installation is stopped during the graphical user interface stage and the following error message is displayed:

```
Unattended Setup is unable to continue because a Setup
parameter specified by your system administrator or
computer manufacturer is missing or invalid.
```

If you want to start an unattended Windows 2000 installation from the Windows 2000 installation CD:

- the computer must support the El Torito Bootable CD-Rom mode format;
- the answer file must be named Winnt.sif and must be placed on a floppy disk that is inserted into the floppy drive as soon as the computer boots from the CD-Rom; and
- the answer file must contain a [Data] section with the required keys specified.

1.4.2 Using the System Preparation tool (disk imaging).

With disk imaging it is possible to install and configure Windows 2000 and all the applications and application update packs on a test computer and then create an exact image of the hard drive that can then be used to install Windows 2000 and the applications on other client computers. These computers that will become recipients of the disk image installation are also referred to as target computers.

During an installation that uses disk imaging, the source files on Windows 2000 installation CD are not used, except for the initial installation on the test computer. In other words, you would not be using *winnt.exe* or *winnt32.exe* to install the disk image on the target computers and thus will not run the Windows 2000 Setup program. Therefore, you will not be detecting the hardware devices and installing the appropriate drivers on the target computers. As a result, all the target computers must have the same hardware configuration as the test computer. You will also have to change the computer name of all the target computers as each computer on the network must have a unique name.

Microsoft has created a **System Preparation tool** (*Sysprep.exe*) which solves some of the problems associated with disk imaging. You would use the Sysprep, after installing and configuring Windows 2000, the applications and application update packages on a test computer, to prepare the computer of disk imaging. You would then run the disk imaging program after Sysprep has completed. Sysprep adds a mini-Setup Wizard to the disk image that will request the user-specific information such as productID, user name, network configuration, etc, on the first reboot of the target computer. This information can either be supplied by the user or by an answer file.

When using answer file with the sysprep tool, a Sysprep folder must be created on the *%systemdrive%* of the test computer or a ***Sysprep.inf*** file must be created and saved to a floppy disk that must be inserted at the beginning of the mini-Setup Wizard. The Sysprep folder that is created on the target computer when the disk image is copied is automatically deleted when the mini-Setup Wizard is completed.

Sysprep can also be used to force the target computer to perform a Plug and Play detection and to install the correct device drivers on the first reboot of the target computer; however, the target computer and the test

computer must have identical hard disk controllers and compatible **Hardware Abstraction Layers**. The –pnp switch is used to force the target computer to detect its hardware configuration on its first reboot. A full list of Sysprep switches are listed in Table 1.2.

TABLE 1.2: *System Preparation Tool Switches*

Switch	Description
-reboot	Restarts the test computer rather than allowing it to shut down after sysprep.exe is completed.
-quiet	Mini-Setup runs without user input. Requires an answer file.
-pnp	Forces a Plug and Play detection on the target computer.
-nosidgen	Does not regenerate the SIDs on the target computers.

1.4.3 Using Remote Installation Services (RIS)

Remote Installation is the process of connecting to **Remote Installation Services** (RIS) server from a target computer and then performing an automated installation of Windows 2000 on the target computer. This is the most effective method of deploying Windows 2000. Remote Installation allows administrators to use a centrally located computer to install Windows 2000 on a target computer, i.e. the computer on which the Windows 2000 operating system is to be installed, anywhere on a network. It however requires that your network already has a Windows 2000 server infrastructure in place and that the target computers support remote booting. A list of network services that the RIS server requires is listed in Tabe1.3.

TABLE 1.3: *Network services required by RIS*

Network Service	Reasons for RIS Requirement
DNS Service	Required for locating the Active Directory directory service and client computer accounts
DHCP Service	Required for supplying IP addresses to client computers
Active Directory directory services	Required for locating existing client computers and existing RIS servers

1.4.3.1 Setting up the RIS Server

To set up a RIS server, you must install RIS on a NTFS partition that is at least 2GB size and that does not contain the operating system, i.e. the boot partition, and is not the system partition, i.e. the startup partition, by running the RIS Setup Wizard. And you must specify a Remote Installation Folder that cannot be on a Distributed File System (Dfs) shared folder or on an Encrypting File System (EFS) volume.

The RIS creates and uses CD-based images and disk images. The process of creating the disk image is similar to the process required when using the sysprep tool; first install and configure Windows 2000 on a test computer, install and configure your applications, apply application update packs and then use the **Riprep utility** to create a **Riprep image**. Unlike the Sysprep tool, however, RIS creates its own disk images and does not require third party software. The Riprep utility automatically removes the test computer's SID from the image and creates an answer file based on the configuration of the operating system on the test computer.

1.4.3.2 Client requirements for Remote Installation

To deploy the image on the client computers, the client computers must be able to connect to the RIS server by booting from the network adapter card. To do this the client computer requires a **PXE-compliant network adapter**, which has a special chip that supports network booting. If the computer does not have a PXE-compliant network adapter card, you must use the *Rbfg.exe* file to make network a boot disk for the computer. The network boot disk can then be used to simulate the PXE boot process.

In addition, the user account that will be used to perform the installation must be assigned the right to 'Logon as a batch job' and must be assigned permissions to create computer accounts in the domain that they will be joining.

1.4.4 Deploying Software applications

1.4.4.1 Overview

In Windows 2000 you can use a **Group Policy Object** (GPO) in conjunction with **Windows Installer** to automate and manage software installations, updates and removal from a centralized location. Group Policy can be used to assign the software application to a group of users that are organized into a unit (an Organizational Unit) and allow you to manage the various phases of software deployment.

There are four phases of software deployment:

- **Preparation:** preparing the files that allows you to use Group Policy to deploy the application software. This involves copying the Windows Installer package files to a software distribution point. The Windows Installer application files can be obtained from the application's vendor or can be created through the use of third-party utilities.
- **Deployment:** the administrator creates a Group Policy Object (GPO) that installs the software on the target computers and links the GPO to the appropriate Organizational Unit. During this phase the software is installed.
- **Maintenance:** the software is upgraded with a new version or redeployed with a patch or a service pack.
- **Removal:** to remove software that is no longer required, you must remove the Windows installer package from the GPO that was used to deploy the software. The software is then automatically removed when a user log on or when the computer restarts.

1.4.4.2 Windows Installer

Windows Installer consists of Windows Installer **service**, which is a client-side service, and Windows Installer **package**. Windows Installer package uses the ***.msi*** file extension and contains all the information that Windows Installer services requires to install the software. The software developer provides the Windows Installer package with the application. If a Windows Installer package does not come with an application, you can create a Windows Installer package or repackage the application, using a third-party utility. Alternatively you could create an application file (.zap) that uses the application's existing setup program. A .zap file is not a native Windows Installer package.

Advantages of using Native Windows Installer packages:

- **Automatic File Repair** when a critical application file becomes corrupt. The application automatically returns to the installation source to retrieve a new copy of the file.
- **Clean Removal** without leaving orphaned files and without deleting shared files used by another application.

- **Transformable.** You can customize a Windows Installer package to meet the requirements set by your company by using authoring and repackaging tools. Transformed Windows Installer packages are identified by the *.mst* file extension.
- **Patches.** Patches and upgrades can be applied to the installed applications. These patches use the *.msp* file extension.

> **Note:** A *.zap* file is not a native Windows Installer package and does not offer the same benefits as Windows Installer packages. It therefore does not support **automatic repairing** and cannot be transformed.

1.5 Upgrading to Windows 2000

1.5.1 Upgrading to Windows 2000 Professional

You can upgrade all earlier Windows operating systems, with the exception of Windows 3.1, Windows for Workgroups 3.1 and Windows NT Workstation 3.5, directly to Windows 2000 Professional. **Windows 3.1** must first be upgraded to Windows 95 or Windows 98 and can then be upgraded to Windows 2000 Professional. **Windows for Workgroups 3.1** and **Windows NT Workstation 3.5** must first be upgrade to Windows NT Workstation 3.5.1 or Windows NT Workstation 4.0 and can then be upgraded to Windows 2000 Professional.

TABLE 1.4: *Windows 2000 Professional Upgrade Paths*

Operating System	Upgrade Path
Windows 3.1	First upgrade to Windows 95 or Windows 98 and then Windows 2000 Professional
Windows for Workgroups 3.1	First upgrade to Windows NT Workstation 3.5.1 or Windows NT Workstation 4.0 and then Windows 2000 Professional
Windows 95	Windows 2000 Professional
Windows 98	Windows 2000 Professional
Windows NT Workstation 3.5	First upgrade to Windows NT Workstation 3.5.1 or Windows NT Workstation 4.0 and then Windows 2000 Professional
Windows NT Workstation 3.5.1	Windows 2000 Professional
Windows NT Workstation 4.0	Windows 2000 Professional

You can use Windows 2000 to generate an **upgrade compatibility report** that can be used to check whether the devices and drivers on the existing operating system are compatible with Windows 2000. You can generate this compatibility report by running the ***winnt32 /checkupgradeonly*** command or the ***Chkupgrade.*exe** utility, which runs the Windows 2000 Readiness Analyzer but must be downloaded from Microsoft website. The */checkupgradeonly* switch of the for *winnt32* command runs the first part of the Windows 2000 Setup program and checks only for compatible hardware and software. For a full list of *winnt32* see Table 1.5 and for a full list of *winnt* switches see Table 1.6.

TABLE 1.5: *WINNT32 switches*

Switch	Description
/checkupgradeonly	Checks the computer for upgrade compatibility with Windows 2000
/copydir:*folder_name*	Creates a folder in the *systemroot* folder (which contains the Windows 2000 system files).
/copysource:*folder_name*	Creates a folder in the *systemroot* folder. Files created with /copysource are automatically deleted after the installation is completed.
/cmd: *command_line*	Specifies a command to be run before the final phase of Setup.
/cmdcons	Adds a Recovery Console option to the operating system selection screen.
/debug[*level*] [:*file_name*]	Creates a debug log at the specified level.
/m:*folder_name*	Specifies that Setup must copy replacement files from another location and to look for files in that location first.
/makelocalsource	Specifies that Setup must copy all installation files to the hard drive.
/noreboot	Prevents Setup from rebooting the computer following the file copy phase. This enables a command to be entered by the user prior to completing setup.
/s:*source_path*	Specifies the source location of Windows 2000 installation files.
/syspart:*drive_letter*	Copies Setup startup files to a hard disk and marks the drive as active. You can then install the drive on another computer. When you start that computer, Setup starts at the next phase. This requires use of the /tempdrive switch.
/tempdrive:*drive_letter*	Specifies a drive to contain temporary setup files and installs Windows 2000 on that drive.
/unattend [number][:*answer_file*]	Performs an unattended installation using an answer file that provides your custom specifications to the Setup program.
/udf:id[,*udf_file*]	Indicates an identifier (ID) that Setup uses to specify how a Uniqueness Database File (UDF) modifies an answer file.

Note: *winnt32.exe* is **32-bit** application. It cannot be used in a DOS-based environment such as DOS mode. Boot disks operate in a **16-bit DOS mode** environment. You therefore cannot use *winnt32.exe* to install Windows 2000 Professional from a boot disk. You must use *winnt.exe*, which is the 16-bit equivalent of *winnt32.exe*, instead.

TABLE 1.6: *WINNT switches*

Switch	Description
/a	Enables accessibility options
/e[:*command*]	Specifies a command to be executed at the end of Setup's GUI mode.
/r[:*folder*]	Specifies an optional folder to be installed on the hade drive. Setup retains the folder.
/rx[:*folder*]	Specifies an optional folder to be installed on the hade drive. Setup deletes the folder after installation
/s[:*sourcepath*]	Specifies the source location of Windows 2000 files.
/t[:*tempdrive*]	Specifies a drive to contain temporary setup files.
/u[:*answer file*]	Performs an unattended installation using an answer file that provides your custom specifications to the Setup program. This requires the /s switch.
/udf:*id*[,*UDF_file*]	Indicates an identifier (ID) that Setup uses to specify how a Uniqueness Database File (UDF) modifies an answer file.

1.5.2 Upgrading to Windows 2000 Server

1.5.2.1 Upgrading the Operating System

Windows 2000 Server allows you to upgrade directly from Windows NT 3.51 Server and Windows NT Server 4.0 to Windows 2000 Server. A computer running a version of Windows NT sever older than Windows NT 3.51 must first be upgraded to Windows NT Server 4.0 before it can be upgraded to Windows 2000 Server. You can upgrade the operating system by running *winnt32.exe* from the Windows 2000 Server installation CD or over the network from within the existing operating system. You however cannot upgrade the operating system from the setup boot disks or by booting from the CD-Rom.

TABLE 1.7: *Windows 2000 Server Upgrade Paths*

Operating System	Upgrade Path
Windows NT Server 3.1	First upgrade to Windows NT Server 3.51 or Windows NT Server 4.0 and then to Windows 2000 Server
Windows NT Server 3.5	First upgrade to Windows NT Server 3.51 or Windows NT Server 4.0 and then to Windows 2000 Server
Windows NT 3.51 Member Server	Windows 2000 Member Server and can then optionally be upgraded to a Windows 2000 Sever Domain Controller
Windows NT 4.0 Member Server	Windows 2000 Member Server and can then

	optionally be upgraded to a Windows 2000 Sever Domain Controller
Windows NT 3.51 PDC or BDC	Windows 2000 Sever Domain Controller
Windows NT 4.0 PDC or BDC	Windows 2000 Sever Domain Controller

1.5.2.2 Upgrading the Network Domain

A critical task in upgrading your network to Windows 2000 Server is upgrading the Windows NT Server domain. Domains are an important feature of both Windows NT Server and Windows 2000 Server. It is necessary to have one or more domains if you want to use domain-based user accounts and other domain security features in Windows 2000 Server.

In a Windows 2000 Domain, a server can have one of three roles. They can be:

- a **domain controller**, which contain copies of the user accounts and Active Directory services database for a given domain;
- a **member server**, which belong to a domain but does not contain a copy of Active Directory services database; or
- a **stand-alone server**, which do not belong to a domain but to a workgroup.

When upgrading the domain controllers in a Windows NT domain to Windows 2000, you must upgrade the Windows NT Primary Domain Controller (PDC) first.

The Windows 2000 server roles domain are named different as compared to Windows NT Server. In Windows NT Server, the possible server roles were PDC (limited to one per domain), Backup Domain Controller (BDC), member server, or stand-alone server. Windows 2000, however, has only one kind of domain controller, i.e. not a "primary" or "backup" domain controller, and also includes the roles of member server and stand-alone server. The following table illustrates how Windows 2000 Setup assigns server roles when you upgrade from Windows NT Server:

TABLE 1.8: *Upgrading Windows NT Server Roles*

Windows NT Server	Windows 2000 Server
Primary Domain Controller	Automatically upgraded to Domain Controller
Backup Domain Controller	Allows you to choose to upgrade to a Domain Controller or a Member Server
Member Server	Allows your to choose to upgrade to a Member Server or to a Stand-alone Server
Stand-alone Server	Allows you to choose to upgrade to a Member Server if a Windows 2000 domain exists, or to a Stand-alone Server

Note: Before upgrading the Windows NT Domain Controller you should first disable WINS and DHCP by using the Services option in Control Panel in Windows NT Server 4.0 so that the WINS database and the DHCP database can be converted during the upgrade process.

1.5.2.3 Upgrading the Primary Domain Controller

When upgrading the Windows NT domain, the first domain controller that must be upgraded must be the PDC. When you upgrade this server, you will be given the choice of creating a new domain or a child domain, and creating a new forest or a domain tree in an existing forest. During the upgrade, you will also have the opportunity to choose the location of three important files: the database containing user accounts and other Active Directory data, the log file, and the system volume file (*SYSVOL*). After the first Windows NT sever server is upgraded to a Windows 2000 domain controller, it will be fully backward compatible, i.e. in a mixed mode environment the upgraded Domain Controller appears as a Windows 2000 domain controller to the Windows 2000 servers and clients but emulates a Windows NT 4.0 PDC to other Windows NT servers and clients.

1.5.2.4 Upgrading the Backup Domain Controllers

After upgrading the PDC you can upgrade any BDC. You can either upgrade the BDCs to additional Windows 2000 Domain Controllers or to Windows 2000 Member Servers. It is however advisable to upgrade the BDCs soon after upgrading the former PDC. When you upgrade the BDCs, the upgraded PDC must be available and running on the network as this server is used as a template for the other domain controllers to copy as they are upgraded.

When you have upgraded all of the Windows NT servers to Windows 2000 Domain Controllers, you can change the domain from Mixed mode, in which Windows NT domain controllers can co-exist with Windows 2000 Domain Controllers in the domain, to Native mode, in which only Windows 2000 domain controllers can exist in the domain.

Note: You cannot convert a Native mode domain to a Mixed mode domain.

1.6 Deploying Service Packs

Windows 2000 Professional supports the integration of service-packs called **slipstreaming**, so service packs can be integrated with the Windows 2000 Professional installation files. This allows you to keep an image of the operating system. When Windows 2000 Professional is installed from this image, the appropriate files from the service pack are also installed. To apply a new service pack, run the *update.exe* file from the service pack with the */slip* switch. This will replace the existing Windows 2000 files with the appropriate files from the service pack.

You can also apply a service pack to computers that are already running Windows 2000 by running the *update.exe* file. This replaces the existing Windows 2000 files with the appropriate files from the service pack.

Mixed Mode

Mixed mode refers to a domain that contains both Windows 2000 and Windows NT Domain Controllers. In Mixed mode the PDC is upgraded to Windows 2000 Server and one or more Windows NT Server BDCs remains. The Windows 2000 Domain Controller that was upgraded from a Windows NT PDC uses the Active Directory store to save objects. It is still fully backward compatible because it exposes the data to down-level computers. The PDC appears as a Windows 2000 domain controller to other Windows 2000 computers, and as a Windows NT PDC to computers that are not yet upgraded. The Mixed mode domain still uses a single master replication with the upgraded PDC recognized as the domain master by the Windows NT Server BDCs and the domain is limited by the functionality of the Windows NT 4.0 domain controllers.

1.7 The Windows 2000 Professional Boot Process

1.7.1 Files Used in the Boot Process

A Windows 2000 Intel-based boot sequence requires a number of

files. A list of these files, their appropriate locations and the stages of the boot process associated with each file are listed in Table 1.9.

> **Note:** ***Systemroot*** represents the path to your Windows 2000 installation folder, which by default is ***C:\Winnt***

TABLE 1.9: *Files Used in the Windows 2000 Boot Process*

File	Location	Boot stage
Ntldr	System partition root (C:\ )	Preboot and boot
Boot.ini	System partition root	Boot
Bootsect.dos	System partition root	Boot (optional)
Ntdetect.com	System partition root	Boot
Ntbootdd.sys	System partition root	Boot (optional
Ntoskrnl.exe	*systemroot*\System32	Kernel load
Hal.dll	*systemroot*\System32	Kernel load
System	*systemroot*\System32\Config	Kernel initialization
Device drivers	*systemroot*\System32\Drivers	Kernel initialization

> **Note:** The string ***systemroot*** (typed as *%*systemroot*%*) represents the folder in the boot partition that contains the **Windows 2000 system files**.

1.7.1.1 Preboot Sequence

During startup, a Windows 2000-based computer initializes the boot portion of the hard disk and the preboot sequence begins. This sequence consists of four steps:

- The computer runs power-on self test (POST) process to determine the amount of physical memory; and
- The hardware components are present.
- If the computer has a Plug and Play (BIOS), enumeration and configuration of hardware devices occurs.
- The computer BIOS locates the boot device and loads and runs the master boot record (MBR).

> **Note:** Windows 2000 modifies the boot sector during installation so that Ntldr loads during system startup. Therefore you should disable the ***Boot Sector Virus Protection*** in your BIOS Setup.

1.7.1.2 Boot Sequence

After the computer loads **Ntldr** into memory, the boot sequence gathers information about hardware and drivers in preparation for the Windows 2000 load phases. The boot sequence uses the following files: **Ntldr**, *Boot.ini*, *Bootsect.dos* (optional), *Ntdetect.com*, and *Ntoskrnl.exe*.

The boot sequence also has four phases:

- **Initial Boot Loader** During the initial boot loader phase, **Ntldr** switches the microprocessor from real mode to 32-bit flat memory mode, which **Ntldr** requires. Then, **Ntldr** starts the appropriate the minifile

system drivers. The minifile system drivers are built into **Ntldr** so that **Ntldr** can find and load Windows 2000 from partitions formatted with either the FAT or NTFS file system.

- **Operating System Selection** During the boot sequence, **Ntldr** reads the *Boot.ini* file. If multiple operating systems are supported on the computer in the *Boot.ini* file, then the **Please Select The Operating System To Start** screen, which you can use to select the operating system that should be loaded within a specified time before the default operating system. If no *Boot.ini* file is present, **Ntldr** attempts to load Windows 2000 from the *Winnt* folder on the first partition of the first disk, typically *C:\Winnt*.
- **Hardware Detection** On Intel-based computers, *Ntdetect.com* and *Ntoskrnl.exe* perform hardware detection. *Ntdetect.com* executes if Windows 2000 should be loads. *Ntdetect.com* collects a list of installed hardware components and returns this list to **Ntldr** for later inclusion in the registry under the HKEY_LOCAL_MACHINE\HARDWARE key.
- **Configuration Selection** After **Ntldr** starts loading Windows 2000 and collects hardware information, the operating system loader process displays the **Hardware Profile/Configuration Recovery Menu** screen, which contains a list of the hardware profiles that have been created on the computer, if more that one hard profile exists on the computer. The first hardware profile is highlighted. You can press the Down arrow key to select another profile. You can also press L to invoke the **Last Known Good Configuration** option.

1.7.1.3 Kernel Load

After the configuration selection, ***Ntoskrnl.exe***, the Windows 2000 kernel loads and initializes. *Ntoskrnl.exe* also loads and initializes device drivers and loads services. If you press Enter when the **Hardware Profile/Configuration Recovery Menu** screen displays, or if **Ntldr** makes the selection automatically, the computer enters the kernel load phase. The screen clears and a series of white rectangles appears across the bottom of the screen. During the kernel load phase, **Ntldr**:

- Loads Ntoskrnl.exe but does not initialize it.
- Loads the hardware abstraction layer file (*Hal.dll*).
- Loads the HKEY_LOCAL_MACHINE\SYSTEM registry key.
- Selects the control set required to initialize the computer.
- Loads device drivers with a value of 0x0 for the Start entry. These are typically low-level hardware device drivers, such as those for a hard disk.

1.7.1.4 Kernel Initialization

When the kernel load phase is complete, the kernel initializes and takes control from **Ntldr**. The system displays a graphical screen with a status bar that indicates load status. During the kernel initialization stage four tasks are performed:

- The Hardware key is created.
- The Clone control set is created.
- Device drivers are loaded and initialized.
- Services are started.

1.7.1.5 Logon

The logon process begins at the end of the kernel initialization phase, when the Win32 subsystem automatically starts *Winlogon.exe*, which starts Local Security Authority (*Lsass.exe*) and displays the Logon dialog box. This allows you to log on while Windows 2000 initializes the network device drivers.

> **Note:** Windows 2000 startup is not considered **successful** until a user logs on at the computer. After a **logon**, the system automatically copies the Clone control set to the LastKnownGood control set making the current control set the ***Last Known Good Configuration***.

1.8 The Boot.ini File

The *Boot.ini* file is a hidden file that the Windows 2000 Setup program saves in the active partition when you install Windows 2000 Professional. **Ntldr** uses information in the *Boot.ini* file to display the **Please Select The Operating System To Start** menu, from which you select the operating system that should be loaded.

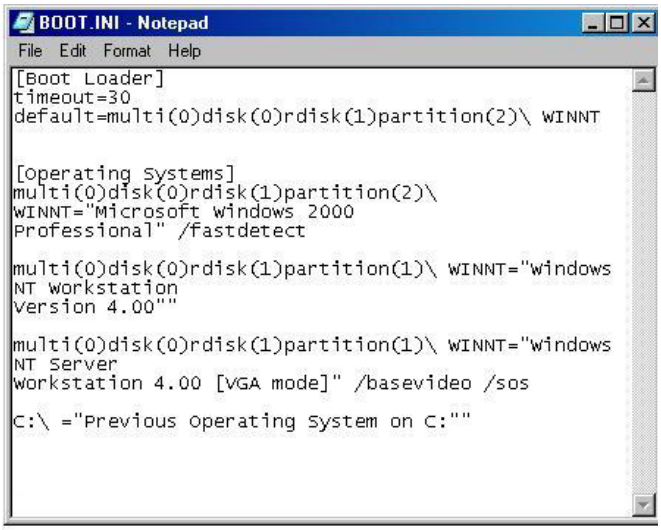

FIG1.2: *An typical Boot.ini file*. (NOTE the *ARC path*)

1.8.1 Components of the Boot.ini File

The *Boot.ini* file includes two sections, **[Boot Loader]** and [Operating Systems] (SEE FIGURE 1.2) The [Boot Loader] section of a *Boot.ini* file contains the specified time that the **Please Select The Operating System To Start** menu is displayed and the default operating system that should be loaded if no selection is made within the specified time. The **[Operating Systems]** section of the *Boot.ini* file contains a list of all the operating systems that are installed on the computer.

1.8.2 ARC Paths

During installation, Windows 2000 generates the *Boot.ini* file, which contains **Advanced RISC Computing** (ARC) paths pointing to the computer's boot partition.

TABLE 1.10: *ARC Path Naming Conventions*

Convention	Description
multi(*x*) | scsi(*x*)	The hardware **adapter or disk controller**. Use **scsi** only to indicate a SCSI controller on which SCSI BIOS is not enabled. All other hardware adapter or disk controllers use **multi**. **(x)** represents a number that indicates the load order of the hardware adapter. The hardware adapter first to load and initialize receives number 0.
Disk(*y*)	The **SCSI ID**. For multi, this value **(y)** is always 0
Rdisk(*z*)	A number **(*z*)** that identifies the disk and starts with (0).

Partition(*a*)	A number **(*a*)** that identifies the partition. Partition numbers start with (1)

1.8.3 Boot.ini Switches

You can add a variety of switches to the entries in the [Operating Systems] section of the *Boot.ini* file to provide additional functionality. Table 1.11 lists some of these switches.

TABLE 1.11: ***Boot.ini Switches***

Switch	Description
/basevideo	Boots the computer using the standard VGA video driver.
/fastdetect=[com*x* | com*x,y,z.*]	Disables serial mouse detection. Without a port specification, this switch disables peripheral detection on all COM ports. By default, this switch is included in every entry in the Boot.ini file.
/maxmem:*n*	Specifies the amount of RAM that the operating system should use.
/noguiboot	Boots the computer without displaying the graphical boot status screen.
/sos	Displays the device driver names as they are loading.

1.9 Advanced Boot Options

The Windows 2000 advanced boot options include Safe Mode, Enable Boot Logging, Enable VGA Mode, Last Known Good Configuration, Directory Services Restore Mode, and Debugging Mode.

- **Safe Mode** can be used if your computer does not start properly. Pressing **F8** during the operating system selection phase displays a screen with advanced options for booting Windows 2000. If you select Safe Mode, Windows 2000 loads only basic files and drivers that are required to support the operating system. If your computer does not start using safe mode, you can try Windows 2000 Automatic System Recovery. You can also choose **Safe Mode With Networking**, which is the same as Safe Mode except that it adds the drivers and services required to enable network access, and **Safe Mode With Command Prompt**, which is the same as Safe Mode except when the computer restarts, it displays a command prompt.
- **Enable Boot Logging** logs the loading and initialization of drivers and services in the ***ntbtlog.txt*** file, which is located in the *windir* folder and can be used for troubleshooting boot problems.
- **Enable VGA Mode** option starts Windows 2000 with a basic VGA driver.
- **Last Known Good Configuration** starts Windows 2000 using the registry information that Windows 2000 saved after the last successful startup of Windows 2000. Windows 2000 startup is not considered **successful** until a user logs on at the computer. After a **logon**, the system automatically copies the Clone control set to the LastKnownGood control set making the current control set the ***Last Known Good Configuration***

1.9.1 The Recovery Console

The Recovery Console is a **command-line** interface that can be used to perform a variety of troubleshooting and recovery tasks, including

- Starting and stopping services;
- Reading and writing data on a local drive; and
- Formatting hard disks.

1.9.1.1 Installing and Starting the Recovery Console

You can install the Recovery Console from the Windows 2000 Professional Installation CD by running the winnt32 command with the /cmdcons switch from the command prompt. After Recovery Console is installed, you can access it from the **Please Select Operating System To Start** menu. You can also use the Windows 2000 Professional Installation CD to start your computer and then select the Recovery Console option when you are prompted to choose repair options.

> **Note:** You can instruct the Windows 2000 Setup program to install the **Recovery Console** when you install Windows 2000 Professional by installing Windows 2000 Professional with the *winnt* command and adding the /e and /cmdcons switches. The /e switch specifies that the Windows 2000 Setup programme must run a command after the final stage of the installation of Windows 2000 is finished and the /cmdcons switch specifies that the command must install the recovery console onto the hard drive. The full command would be similar to this: **Winnt/e:z:\i386\winnt/cmdcons**

1.9.1.2 Using the Recovery Console

The Recovery Console provides you with a limited set of dos-based administrative commands that you can use to repair your Windows 2000 installation. A list of the Recovery Console commands is shown in Table 1.12.

TABLE 1.12: *Some Recovery Console commands*

Command	Description
Chdir (cd)	Displays the name of the current folder or changes the current folder
Chkdsk	Checks a hard drive and displays a status report
Copy	Copies a single file from a stiffy drive or CD-Rom drive to the hard drive
Delete (del)	Deletes one or more files
Dir	Displays a list of files and subfolders in a folder
Disable	Disables a system service or a device driver
Enable	Starts or enables a system service or a device driver
Exit	Exits the Recovery Console and restarts your computer
Fdisk	Manages partitions on your hard disks
Fixboot	Writes a new partition boot sector onto the system partition

Fixmbr	Repairs the master boot record of the partition boot sector
Format	Formats a disk
Help	Lists all of the Recovery Console commands
Listsvc	Lists the device drivers and services that are currently installed on the computer
Mkdir (md)	Creates a folder
Rmdir (rd)	Deletes a folder
Rename (ren)	Renames a single file
Systemroot	Sets the current folder to the systemroot folder of the system that you are currently logged on to
Type	Displays a text file

There are various ways of installing Windows 2000 Server, which can be installed clean, on a new computer or as an upgrade from Windows NT 4.0 Server.

2. Managing Windows 2000

Control Panel can be used to configure hardware settings, manage user-specific settings, and manage computer-specific settings.

2.1 Installing New Hardware

Installing a new device to a Windows 2000 computer typically involves physically connecting the device to the computer; loading the appropriate device drivers; and configuring the device properties and settings if required.

> **Note:** To be able to install a device you must be logged on as an **administrator** or as a member of the **Administrators group**.

When you install a **Plug and Play** device, Windows 2000 automatically configures the device so that it works properly with the other devices that are already installed on the computer. This includes assigning the appropriate system resources, such as Interrupt Request (**IRQ**) line number, Direct Memory Access (**DMA**) channels, Input/Output (**I/O**) port addresses and **Memory Address** ranges, to the device. Each device must be assigned a unique system resource or the device will not function properly. When you install a non-Plug and Play, or a legacy device, you must use the **Add/Remove Hardware Wizard**. If Windows 2000 does not detect the device you must configure the system resources for the device manually. You can assign system resources to the device in Device Manager.

> **Note:** Some old **legacy ISA** devices require the use of a specific IRQ number that Windows 2000 may have assigned to a Plug and Play device. In this event you should **reserve** the IRQ that is required by the device in your **system BIOS**. Windows 2000 then will assign another IRQ to the Plug and Play device that was using the IRQ that you have reserved.

> **Note:** When you install Windows 2000 on a new computer that does not have a standard **Hardware Abstraction Layer** (HAL) or a **RAID** device that is **not detected** by the Windows Setup program, you must install the drivers for these devices during the **text portion** of the Windows 2000 Setup program.

2.2 Using Driver Signing

Some device drivers and some applications overwrite existing operating files as part of their installation process. These files can cause system errors that are difficult to troubleshoot. Microsoft has greatly simplified the tracking and troubleshooting of altered files by digitally signing the original operating system files and allowing you to verify these signatures.

2.2.1 Configuring Driver Signing

You can configure how the computer responds to unsigned files on **HARDWARE** tab of **SYSTEM**. Here you can configure one of three responses:

- **Ignore** allows any files to be installed regardless of whether they are digital signature or not.

- **Warn** displays a warning message before allowing the installation of an unsigned file. This is the default option.
- **Block** prevents the installation of unsigned files.

> **Note:** When you change the default Driver Signing option, you must select the **Apply setting as system default** check box in the **Driver Signing Options** dialog box. This will make the new settings the default system setting. If you do not select the **Apply setting as system default** check box, the settings will revert to the old setting when the computer is next rebooted.

2.2.2 The File Signature Verification Utility

Windows 2000 also provides a File Signature Verification utility, ***sigverif***, that allows you to view the file's name, its location, its modification date, its type, and its version number.

2.3 Configuring Hard Disks

2.3.1 Disk Storage Types

Windows 2000 provides support for two types of disk storage: **basic storage**, which uses basic disks and is the standard storage type; and **dynamic storage**, which uses dynamic disks. Basic disks can be divided into up to four partitions that can either be **primary partitions** or **extended partitions**. You can have multiple primary partitions but only one extended partition. You can create multiple primary partitions to which enables you to **dual boot** between Windows 2000 and other operating systems such as Windows 98. One of the primary partitions must be set in **fdisk** as the **active partition** as the **boot files** required to start the operating systems must be located on the active partition.

> **Note:** If you plan to dual boot between Windows 2000 and **Windows 95**, **Windows 98** or **OSR2**, the primary partition must be formatted with the **FAT** or **FAT32** file system.

Basic disks can be converted to dynamic storage from which **dynamic volumes** can be created. Windows 2000 supports three types of dynamic volumes: **simple volumes**, which are created from disk space on a single physical disk and is not fault tolerant; **spanned volumes**, which can contain disk space from up to 32 physical disks and are also not fault tolerant; and **striped volumes**, which can combine the free space from up to 32 physical disks into one logical volume.

2.3.2 Configuring File Systems

Windows 2000 supports the **FAT**, **FAT32** and **NTFS** file systems. A computer can contain a combination of file systems but each file system must be located on a separate partition or volume.

> **Note:** DOS, Windows 95, Windows 98 and Windows Millennium Edition cannot access data on NTFS formatted disks.

The NTFS file system used by Windows 2000 is **version 5**. This is a new version of NTFS with new features that were not available in NTFS version 4 used by Windows NT 4.0. Windows NT 4.0 cannot

therefore fully support all the features of NTFS version 5. NTFS version 5 offers a number of benefits that include:

- File compression
- File and folder level security
- File encryption using Encrypting File System (EFS)
- Disk quotas
- NTFS permissions

> **Note:** You can **convert** a disk from the FAT and FAT32 file to NTFS at any time without data loss by using the ***convert*** command from a command prompt and using the ***fs:/ntfs*** switch. When you format the data on the disk is lost.

2.3.3 Encrypting File System (EFS)

EFS is a new feature that has been introduced with Windows 2000 and can be used to encrypt files and folders on NTFS volumes. When a user encrypts a file, only that user will be able to use the file. They can use the encrypted file without having to decrypt the file first. EFS can be implemented from Windows Explorer or from the command prompt using the **Cipher** command. The syntax for the cipher command is: **cipher [/e | /d] [/s:*folder_name*] [/a] [/i] [/f] [/q] [/h] [/k] [*file_name* [...]]**. A list of Cipher command switches is provided in Table 2.1.

- EFS is only supported on **NTFS version 5**
- **Compressed files** cannot be encrypted using EFS
- **System files** cannot be encrypted
- Encrypted files cannot be **shared**
- Encrypted flies or folders that are moved or copied to partitions or volumes that are not formatted with the NTFS file system will become decrypted
- Files and folders on network computers can be encrypted if you have the necessary access **permissions** to the network computer's NTFS volume and if file encryption is enabled on the network computer.

TABLE 2.1: ***Command-line Switches for the Cipher command***

Switch	Description
/e	Encrypts the specified folders and marks them so that files that are added later will be encrypted.
/d	Decrypts the specified folders. Files that are added to the folder will no longer be encrypted.
/s:*folder*	Performs the specified operation on folders in the given folder and all subfolders
/a	Performs the specified operation on files and folders.
/i	Continues performing the specified operation even after errors have occurred.

/f	Forces the encryption operation on all specified files, even those that are already encrypted.
/q	Reports only the most essential information.
/h	Displays files with the hidden or system attributes.
/k	Creates a new file encryption key.
File_name	Specifies a pattern, file, or folder.

2.3.4 Volume Mounting

The Disk Management tool can be used to mount local drives to an **empty folder** on an NTFS volume. This empty folder becomes the mount point. When a physical disk is mounted to a folder, it is assigned a **drive path** rather than a drive letter. The Administrator can identify and manage volume mount points by using the *mountvol.exe* command-line tool. To mount a drive:

- Open **MY COMPUTER**
- Open **CONTROL PANEL**
- Open **ADMINISTRATIVE TOOLS**
- Click on the **COMPUTER MANAGEMENT**
- Expand **STORAGE**
- Open **DISK MANAGEMENT**
- Right-click the partition or volume you want to mount
- Click **CHANGE DRIVE LETTER AND PATH**
- Click **ADD**
- Type the path to the *Empty Folder*

2.3.5 File Compression

Windows 2000 supports file and folder level compression. Compressed files can be read and written to by any Windows-based or MS-DOS-based application without first having to be uncompressed by another program. When you access a file via a Windows-based or MS-DOS-based application, NTFS automatically uncompresses the file. When you save or close the file again, NTFS compresses it again. Therefore NTFS allocates **disk space** based on the **uncompressed file size** and not on the compressed file size.

2.3.5.1 Copying and Moving Compressed Files and Folders

When copying a file within an NTFS volume, the file inherits the compression state of the target folder.

- When moving a file or folder within an NTFS volume, the file or folder retains its original compression state.
- When copying a file or folder to another NTFS volume, the file or folder inherits the compression state of the target folder.
- When moving a file or folder to another NTFS volume, the file or folder inherits the compression state of the target folder. Because Windows 2000 treats a move as a copy and then a delete, the files inherit the compression state of the target folder.

- When moving or copying a file or folder to a **FAT volume**, Windows 2000 automatically uncompresses the file or folder. This is because Windows 2000 only supports file and folder compression on NTFS volumes.
- When moving or copying a compressed file or folder to a **floppy disk**, Windows 2000 automatically uncompresses the file or folder, as floppy disks are formatted with the FAT file system. Floppy disks cannot support the NTFS file system.

2.4 Backing Up and Restoring Data

Performing regular back ups of the data on hard disks prevents **data loss** due to disk drive failures, power outages, virus infections, and other such incidents. If data loss occurs, and you have performed regular backup jobs, you can restore the lost data.

2.4.1 Windows Backup

Windows 2000 provides **Backup And Recovery Tools**. This includes the Backup Wizard, which you can use to easily back up and restore data. To launch Backup

- Click on the **START** button
- Point to **PROGRAMS**
- Point to **ACCESSORIES**
- Point to **SYSTEM TOOLS**
- Click **BACKUP**

Alternatively:

- Click on the **START** button
- Click **RUN**
- Type **ntbackup** in the text box
- Click **OK**

You can use Backup to back up data manually or you can schedule regular unattended backup jobs. You can back up data to a file or to a tape. Files can be stored on hard disks, removable disks, and recordable compact discs and optical drives.

To successfully back up and restore data on a Windows 2000 computer, you must have the appropriate permissions and user rights.

All users can back up their own files and folders, and files for which they have the Read, Read & Execute, Modify, or Full Control permission.

All users can restore files and folders for which they have the Write, Modify, or Full Control permission.

By default, members of the **Administrators and Backup Operators** groups have the **Backup Files and Directories**, and the **Restore Files and Directories** user rights and can therefore back up and restore all files regardless of the assigned permissions.

2.4.2 Backup Types

Backup Wizard provides five types of backup that define which data is backed up. Some backup types use backup **markers**, also known as archive bits, which mark a file as having changed. When a file changes, an attribute is set on the file that indicates that the file has changed since the last backup. When you back up the file, this **clears** or resets the attribute.

- **Normal** – backs up all selected files and folders and does not rely on markers to determine which files to back up. During a normal backup, any existing marks are cleared and each file is marked as having been backed up. Normal backups speed up the restore process because the as the files are the most current therefore you do not need to restore multiple backup jobs.
- **Copy** – backs up all selected files and folders without looking for or clearing markers.
- **Incremental** – only backs up selected files and folders that have a marker and then **clears** the markers. Thus, if you did two incremental backups in a row on a file and nothing changed in the file, the file would not be backed up the second time.
- **Differential** – only backs up selected files and folders that have a marker but does not clear markers. Thus if you did two differential backups in a row on a file and nothing changed in the file, the entire file would be backed up each time.
- **Daily** – backs up all selected files and folders that have changed during the day and does not look for or clear markers.

3. Configuring the Windows 2000 Network

Windows 2000 supports both Workgroup Networks and Domain-Based Networks. **Workgroup Networks** are also referred to as Peer-to-Peer networks and are the simplest type of network. They are ideal for networks of less than ten computers and supports file and print sharing. **Domain-Based Networks** are common to large companies and benefit from centralized administration. This results in the implementation of stronger security models with users requiring a user account to logon access network resources.

3.1 Creating Network Connections

In Windows 2000 you can create number of network connections. These include local area network (LAN) connections, remote connections, Virtual Private Network (VPN) connections and direct connections. All these connections are created in the **NETWORK AND DIAL-UP CONNECTIONS** folder.

A **Local Area Network** is also referred to as an intranet and has client support, such as Client for Microsoft Networks and Client Services for NetWare; services, such as Files and Printer Sharing; and user network protocols. A network **protocol** is a set of rules and conventions for computers use to communicate over a network. Windows 2000 supports:

- ***TCP/IP***, which is the default protocol and is installed automatically in Windows 2000;
- ***NetBEUI*****,** which is a nonroutable protocol suited for small networks of less than ten computers;
- ***AppleTalk***, which allows a Windows 2000-based computer to communicate on Apple Macintosh networks;
- ***NWLink (IPX/SPX)***, which allows a Windows 2000-based computer to communicate on Novell NetWare networks; and
- ***DLC***, which is a nonroutable protocol that allows a Windows 2000-based computer to communicate to an IBM host.

> **Note:** The AppleTalk protocol requires a Windows 2000 Server that is configured with Windows 2000 Services to function properly.

You can also specify the **protocol binding** order to optimize network performance by placing the protocol that is used the most at the top of the protocol bindings list. The computer will then attempt to use this protocol first when a user attempts to make a connection to a server.

- **Remote connections** allow for mobile users to dial into their corporate LAN and are also used to establish a connection to the Internet via an Internet Service Provider (ISP).
- **Virtual Private Networks** (VNP) use a tunneling protocol to secure a private network that is established across a public network. Windows 2000 supports two tunneling protocols that can be used to create a VNP connection:
- **Point-to-Point Tunneling Protocol (PPTP)**, which is a TCP/IP protocol that can encapsulate TCP/IP, IPX/SPX, or NetBEUI protocols. PPTP tunnels must be authenticated by using the same authentication mechanisms as PPP connections; and

- **L2TP**, which is a combination of PPTP and Layer 2 Forwarding. L2PT does not provide data encryption but relies on **Internet Protocol Security (IPSec)**, which is group of services and protocol that supports the secured transfer of information across an IP internetwork.

IP Address

An IP address is a logical 32-bit address that identifies a TCP/IP host. Each network adapter card in a computer running TCP/IP must have a unique IP address, which has two parts: a network ID that identifies all hosts on the same physical network, and a host ID that identifies a host on the network. An IP Address of 192.168.1.66 indicates that the network ID is 192.168.1, and that the host ID is 66.

3.2 Configuring automatic IP Addressing

In Windows 2000 client computer can obtain automatically obtain an IP address from a DHCP server or through Automatic Private IP Addressing.

3.2.1 DHCP Addressing

If the network has a server running the Dynamic Host Configuration Protocol (DHCP Service, it can automatically assign TCP/IP configuration information to the client computers if the client computers are configured as DHCP clients. You can then configure any client running Windows 2000, Windows 95, and Windows 98 to obtain TCP/IP configuration information automatically from the DHCP Service. This can simplify administration and ensure correct configuration information**.**

Subnet Mask

Subnet mask is used to subnets that divide a large network into multiple physical networks connected with routers. A subnet mask blocks out part of the IP address so that TCP/IP can distinguish the network ID from the host ID. When TCP/IP hosts try to communicate, the subnet mask determines whether the destination host is on a local or remote network. To communicate on a network, the computers must have the same subnet mask.

3.2.2 Automatic Private IP Addressing

Windows 2000 supports a new mechanism for automatic address assignment of IP addresses for simple LAN-based network configurations called **Automatic Private IP Addressing (APIPA).** This mechanism is an extension of dynamic IP addressing and enables the configuration of IP addresses without using static IP address assignment or installing the DHCP Service.

On a computer running Windows 2000 you must configure a network LAN adapter for TCP/IP and click **Obtain an IP Address Automatically in the Internet Protocol (TCP/IP)** Properties dialog box for the Automatic Private IP Addressing feature to function properly.

Default Gateway

The default gateway is a device on a local network that stores network IDs of other networks in the enterprise or Internet. To communicate with a host on another network you must configure an IP address for the default gateway. TCP/IP sends packets for remote networks to the default gateway, which forwards the packets to other gateways until the packet is delivered to a gateway connected to the specified destination.

APIPA can be used to set up IP configuration to allow network communication on a single subnet and is also used when the client computer cannot contact the DHCP server for IP address configuration. APIPA uses an addressing range from **169.254.0.1 through 169.254.255.254** and a subnet mask of **255.255.0.0.**

When you use DHCP to automatically configure TCP/IP information, the DHCP server supplies the necessary configuration information to the DHCP clients and ensures that the clients use the correct configuration information. Then, DCHP automatically updates client configuration information to reflect changes in network structure and the relocation of users to other physical networks, without manually reconfiguring client IP addresses.

Every time a DHCP client starts, it requests an IP address from a DHCP server. Once the DHCP server receives the request, it selects an IP address from a predefined range of addresses in its database and offers this address to the DHCP client. If the client accepts the offer, the DHCP server leases the IP address to the client for a specified period of time. The default duration of an IP address lease is eight days. The client then uses the IP address to access the network.

The IP addressing information sent by the DHCP server to the DHCP client includes:

- An IP address;
- A subnet mask; and
- Optional values, such as:
  - A default gateway address
  - The IP addresses of Domain Name System (DNS) servers
  - The IP addresses of Windows Internet Name Service (WINS) servers
  - Domain name

3.2.3 The DHCP Lease Process

The DHCP client waits one second for an offer. If it does not receive an offer, it rebroadcasts the request four times at 2, 4, 8, and 16 second intervals. If the client does not receive an offer after four requests, it uses an IP address in the reserved range from 169.254.0.1 through 169.254.255.254. This ensures that clients on a subnet without a DHCP server can communicate with each other. The DHCP client continues in an attempt to find a DHCP server every five minutes. When a DHCP server becomes available, clients receive valid IP addresses, allowing them to communicate with hosts both on and off their subnet.

DHCP uses a four-step process to lease IP addressing information to DCHP clients. This process is also referred to as **DORA**: **D**iscovery, **O**ffer, **R**equest, and **A**cknowledgment

- **IP Lease Discovery**
  When a client computer either starts or initializes TCP/IP for the first time, it initializes a limited version of TCP/IP and broadcasts a DHCP discovery (**DHCPDISCOVER**) message for IP addressing information. At this stage the client does not have an IP address. It therefore uses **0.0.0.0** as its IP address. The client also does not know the IP address of a DHCP server, and therefore uses **255.255.255.255** as the destination address. The DHCPDISCOVER message is broadcast to the entire subnet and contains the hardware address of the client's network adapter, which is known as the media access control (MAC) address; and the client's computer name so that DHCP servers can determine which client sent the DHCPDISCOVER message.
- **IP Lease Offer**
  The second stage in the DHCP lease process is the IP lease offer. All DHCP servers that have an IP address that is valid for the network segment to which the client is connected respond with a DHCP offer (**DHCPOFFER**) message. This message includes:
  - The client's hardware address
  - An offered IP address
  - A subnet mask
  - The length of the lease
  - The IP address of the offering DHCP server

Each responding DHCP server reserves the offered IP address so that it does not offer it to another DHCP client before the requesting client accepts the address.

- **IP Lease Request**
  The third stage is the IP Least Request. During this stage the DHCP client responds to the first offer that it receives by broadcasting a DHCP request (**DHCPREQUEST**) message to accept the offer. The DHCPREQUEST message includes the server identification of the server whose offer it accepted. All other DHCP servers then retract their offers and retain their IP addresses for other IP lease requests.
- **IP Lease Acknowledgement**
  The final stage is IP Lease Acknowledgement during which the DHCP server that issues the accepted offer broadcasts a DHCP acknowledgement (**DHCPACK**) message to acknowledge the successful lease. This message contains a valid lease for the IP address and other configuration information. When the DHCP client receives the acknowledgment, TCP/IP initializes by using the configuration information that the DHCP server provides. The client also binds the TCP/IP protocol to the network services and network adapter, permitting the client to communicate on the network.

3.2.3.1 Automatic Lease Renewal

At specific intervals, a DHCP client attempts to renew its lease to ensure that it has up-to-date configuration information. A DHCP client attempts to renew its lease **when 50 percent of the lease duration has expired**. The DHCP client sends a DHCPREQUEST message to the DHCP server from which it obtained the lease. If the DHCP server is available, it renews the lease and sends the client a DHCPACK message with the new lease duration and any updated configuration parameters. The client updates its configuration when it receives the acknowledgment. If the DHCP server is unavailable, the client continues to use its current configuration parameters and a DHCP client cannot renew its lease at the 50 percent interval, the client continues to use its current configuration parameters. It then broadcasts a DHCPDISCOVER message to update its address lease at regular intervals and accepts a lease that is issued by any DHCP server.

Client Reservations

You can configure a scope so that the DHCP server always provides the same IP address to a computer that requires a permanent IP address, such as a DNS server. This is called *client reservations*.

3.2.3.2 Manual Lease Renewal

You can use the IPConfig command with the /renew switch to manually renew an IP lease if you need to update DHCP configuration information immediately if you want DHCP clients to immediately obtain the address of a newly installed router from a DHCP server, renew the lease from the client to change this configuration. Windows 3.51, Windows NT 4.0, Windows 2000, and Windows XP clients can use the IPConfig command with the /release switch to release a lease while Windows 95 and Windows 98 clients must use the **winipcfg** command. These commands send a DHCPRELEASE message to the DHCP server to release a client lease. After you issue this command, the client can no longer communicate on the network by using TCP/IP.

Note: You must **authorize** a DHCP server before the server can issue leases to DHCP clients. This prevents unauthorized DHCP servers from offering incorrect IP configurations to clients. However, only DHCP servers running Windows 2000 Server check for authorization. Other DHCP servers can still operate even though they are not authorized. You must be a member of the Enterprise Administrators group to authorize a DHCP server as you need

network-wide administrative privileges to authorize a DHCP server.

3.3 Name Resolution

Windows 2000 supports the use of user-friendly domain names to represent the IP address of a host or a client. This however requires name resolution so that the computer can identify the IP address that the user-friendly name refers to. Windows 2000 supports two types of name resolution: **NetBIOS** name resolution and host name resolution.

DNS Zones

DNS uses *domain name space* is the naming. The DNS database is indexed by name; therefore, each domain must have a name. As you add domains to the hierarchy, the name of the parent domain is appended to its child domain. Consequently, a domain's name identifies its position in the hierarchy. Thus the domain name studyguides.testking.com identifies the studyguides domain as a child domain or subdomain of the testking.com domain and testking as a subdomain of the com domain. A discrete portion of the domain name space is represented as a zone. Zones provide a way to partition the domain name space into manageable sections.

3.3.1 NetBIOS Name Resolution

Although Microsoft has phased out NetBIOS name resolution, it remains in Windows 2000 for compatibility purposes. Two of the mechanisms implemented for NetBIOS name resolution are **Windows Internet Naming Service (WINS)**, which is a NetBIOS name server that stores NetBIOS names and their IP Addresses; and the **LMHOSTS file**, which is a static text file that contains a list of NetBIOS names and their corresponding IP addresses and is stored on the local computer.

3.3.2 Host Name Resolution

Windows 2000 uses **Domain Name Services** (DNS) to resolve host names. DNS name servers resolve **forward and reverse lookup queries**. A forward lookup query resolves a user-friendly domain name to an IP address. A reverse lookup query resolves an IP address to a user-friendly domain name. A name server can resolve a query only for a zone for which it has authority. If a name server cannot resolve the query, it passes the query to other name servers that can resolve the query. The name server caches the query results to reduce the DNS traffic on the network. This is the primary means for Windows 2000 and Windows XP client computers to locate and communicate with other computers on an IP network. However, clients using earlier versions of Windows, such as **Windows 98** or **Windows NT 4.0**, which use NetBIOS names for network communication, require Windows Internet Name Service (WINS) to register NetBIOS computer names and resolve them to IP addresses. This ensures that clients that use earlier versions of Windows can locate network resources and can communicate with other computers on network.

The recommended way to configure a DNS client is to make it a DHCP client and set the appropriate TCP/IP options.

To configure Windows 98 client computers to use DNS for name resolution

- On the Windows 98 Client computer, click on the **START** button
- Point to **SETTINGS**
- Click on **CONTROL PANEL**
- Double-click **NETWORK**
- Double-click the **TCP/IP PROTOCOL** that is bound to the network adapter
- Click on the **PROPERTIES**
- Click the **DNS CONFIGURATION** tab

- If a DNS server is available, click **ENABLE DNS**
- Click on **HOST**
- Type the client **computer name**
- Click on **DOMAIN**
- Type the **DNS domain name**
- In the DNS Server Search Order dialog box, use the **ADD** button to enter the IP addresses of the DNS servers that you want this client to use

To configure Windows NT 4.0 client computers to use DNS for name resolution

- On the Windows 98 Client computer, click on the **START** button
- Point to **SETTINGS**
- Click on **CONTROL PANEL**
- Double-click **NETWORK**
- Click **TCP/IP PROTOCOL**
- Click on **PROPERTIES**
- In the **DNS SERVER SEARCH ORDER** dialog box, on the DNS tab, use the **ADD** button to enter the IP addresses of the DNS servers that you want this client to use
- Click on **HOST**
- Type the client **computer name**
- Click on **DOMAIN**
- Type the **DNS domain name**

To configure Windows 2000 client computers to use DNS for name resolution

- On the **DESKTOP**, right-click **MY NETWORK PLACES**
- Click **PROPERTIES**
- Open the **PROPERTIES** dialog box for the connection
- Open the **INTERNET PROTOCOL (TCP/IP) PROPERTIES** dialog box
- Click **USE THE FOLLOWING DNS SERVER ADDRESSES**
- In the **PREFERRED DNS SERVER** dialog box, type the IP address of the primary server
- If you are configuring a second DNS server, in the **ALTERNATE DNS SERVER** dialog box, type the IP address of the additional DNS server.

To configure the primary DNS suffix:

- Right-click **MY COMPUTER**
- Click **PROPERTIES** to open the System Properties dialog box.
- On the **NETWORK IDENTIFICATION** tab, click **PROPERTIES**
- In the **COMPUTER NAME CHANGES** dialog box, click **MORE**
- In the **DNS SUFFIX AND NETBIOS COMPUTER NAME** dialog box, in the Primary DNS suffix of this computer dialog box, type the DNS domain name for the computer.

To configure Windows XP client computers to use DNS for name resolution

- Right-click **MY NETWORK PLACES**
- Click **PROPERTIES**
- Open the **PROPERTIES** dialog box for the connection
- Open the **INTERNET PROTOCOL (TCP/IP) PROPERTIES** dialog box.
- Click **USE THE FOLLOWING DNS SERVER ADDRESSES**
- In the **PREFERRED DNS SERVER** dialog box, type the IP address of the primary server
- If you are configuring a second DNS server, in the **ALTERNATE DNS SERVER** dialog box, type the IP address of the additional DNS server.

3.4 Testing IP Connections

3.4.1 Using the IPConfig Utility

The IPConfig utility is a command-line utility that can be used to display the **TCP/IP configuration** of your computer. This information can be used to verify that the client computer has received a valid IP configuration from DHCP. It can also display the IP configuration, and parameters for the network connection on your computer. This information can be used to verify that the client computer is configured with the correct WINS and/or DNS server IP addresses.

TABLE 3.1: *IPConfig Switches*

Switch	Function
/all	Displays the configuration all network interfaces.
/release <*adapter*>	Releases the IP address for a specified network adapter card.
/renew <*adapter*>	Renew the IP address for the specified network adapter card.
/flushdns	Clears all entries from the DNS Resolver Cache on the local computer.
/registerdns	Renews the local computer's DHCP lease and reregisters DNS names.
/displaydns	Displays the contents of the DNS Resolver Cache on the local computer.
/showclassid *adapter*	Displays all the DHCP class IDs allowed for the specified network adapter card.
/setclassid *adapter*	Modifies the DHCP class ID for the specified network adapter card
/?	Displays a list of all the IPConfig switches and their functions

Note: DNS clients **cache** the name resolution information it receives from DNS responses to its name resolution queries and uses this information to resolve future queries locally. When a query cannot be resolved locally, the client sends the query to the DNS server. However, when a server or remote host renews its IP address lease in DHCP, the local client computer will not

hold the correct information in cache and will thus resolving names incorrectly. In this event you can use the **/flushdns** switch of the IPConfig utility to clear the cache on the local client computer.

3.4.2 Using the ping Utility

The ping utility is another command-line utility that ca be used to test low-level communication over IP to another host on the network in the form of an echo request. If the ping utility fails, it returns an error message. You can receive various messages when you use the ping utility:

TABLE 3.2: *Ping Errors*

Error Message	Problem
Destination host unreachable	there is an IP routing problem between your computer and the remote host
Unknown host hostname	none of the client's name resolution mechanisms recognize the name that you typed - check that you typed the host name correctly
Request timed out	the name resolution mechanisms have recognized the name, but the remote host did not receive the request or did not respond to it - check connectivity to the remote host

3.4.3 Using the tracert Utility

The tracert utility is similar to the **ping** utility, except that it reports back from each router on the path from your client computer to the remote host. If you know the network topology in your organization, you can determine which router is unresponsive or slow.

3.4.4 Using the net and nbtstat Utilities

The net command can be used to view the computer's network settings. The **Net config** workstation command is a net command that is used for testing NetBIOS name resolution. The Net config workstation command reports the NetBIOS name and the domain name of the computer while the nbtstat command is used to check the state of current NetBIOS over TCP/IP connections, to **update the Lmhosts cache**, and to determine your registered name. This command can also be used to troubleshoot and preload the NetBIOS name cache.

TABLE 3.3: *nbstat Commands*

Command	Description
nbtstat -n	Lists the NetBIOS names registered by the client
nbtstat -c	Displays the NetBIOS name cache
nbtstat -R	Manually reloads the NetBIOS name cache by using entries in the Lmhosts file with a #PRE parameter
nbtstat /?	List all the nbstat commands

The DNS server contains information about a portion of the DNS namespace. A DNS client queries a DNS server for information about the DNS namespace; the server can query other DNS servers to resolve a query from the client. In other words, when a DNS server receives a DNS request, it attempts resolve the request by to locating the information in its own database first. If it cannot locate the information, it sends a request to the other DNS servers in the domain.

3.4.5 Lookup Types

The zone lookup type determines the tasks that a DNS server will perform. When you create a zone, you specify whether the zone will be used for resolving forward or reverse lookup queries by specifying the zone type.

- **Forward lookup**. A request to map **a name to an IP address**. This is the most common type of lookup, and is used to locate a server's IP address so that a connection can be made to it. This type of request requires name-to-address resolution.
- **Reverse lookup**. A request to map **an IP address to a name**. This lookup type is most commonly used when you know an IP address, but you want to know the domain name that is associated with the IP address. For example, if you monitor IP connections that are made to a server, you can use a reverse lookup to locate the domain name associated with the IP address of the connecting computer. This type of request requires address-to-name resolution.

3.5 DNS Zones

A zone is a contiguous portion of the domain namespace for which a DNS server has authority to resolve DNS queries. You can divide the DNS namespace into zones, which store name information about one or more DNS domains or portions of a DNS domain. For each DNS domain name included in a zone, the zone becomes the authoritative source for information about that domain. DNS servers can host various types of zones. To limit the number of DNS servers on your network, you can configure a single DNS server to support, or host, multiple zones. You can also configure multiple servers to host one or more zones to provide fault tolerance and distribute the name resolution and administrative workloads.
Zone file. The resource records that are stored in a zone file define a zone. The zone file stores information that is used to resolve host names to IP addresses and IP addresses to host names.

To create a zone, open the DNS console, right-click the name of the server to which you want to add the zone, and then click New Zone to start the New Zone wizard. The wizard prompts you to select a zone type and specify the domain name for the zone.

> **Note:** To create zones and administer a DNS server that is not running on a domain controller, you must be a member of the **Administrators group** on that computer. To configure a DNS server that is running on a domain controller, you must be a member of the DNSAdmins, Domain Admins, or Enterprise Admins group.

The following table describes the three types of zones that you can configure, and the zone files associated with them.

TABLE 3.4: *Zone Types*

Zone type	Description
Standard primary	Contains a read/write version of the zone file that is stored in a standard text file. Any changes to the zone are recorded in that file
Standard secondary	Contains a read-only version of the zone file that is stored in a standard text file. Any changes to the zone are recorded in the primary zone file and replicated to the secondary zone file. Create a standard secondary zone to create a copy of an existing zone and its zone file. This allows the name resolution workload to be distributed among multiple DNS servers
Active Directory integrated	Stores the zone information in Active Directory, rather than a text file. Updates to the zone occur automatically during Active Directory replication. Create an Active Directory integrated zone to simplify planning and configuration of a DNS namespace. You do not need to configure DNS servers to specify how and when updates occur, because Active Directory maintains zone information

3.5.1 Caching-only DNS servers

Caching-only DNS servers perform name resolution on behalf of clients and then **cache the results**. They are not configured to be authoritative for a zone, so they do not store standard primary or standard secondary zones instead the cache is populated with the most frequently requested names. These names and their associated IP addresses are available from the cache for answering subsequent client queries. Caching-only DNS servers help to reduce traffic across a WAN links as they do not maintains zone files, as do a primary DNS server, nor do they hold a copy of a zone file, as do a secondary DNS server. Therefore, they do not generate zone transfer traffic. You can configuring a Caching-Only DNS Server by installing the DNS Server service on a Windows 2000 computer, **without configuring any forward or reverse lookup zones**.

3.5.2 Zone Files

Zone files contain the information that a DNS server references to resolve host names to IP addresses and to resolve IP addresses to host names. This information is stored as resource records that populate the zone file. A zone file contains the name resolution data for a zone, including resource records that contain information for answering DNS queries. Resource records are database entries that contain various attributes of a computer, such as the host name or FQDN, the IP address, or the alias. DNS servers can contain the following types of resource records.

TABLE 3.5: *Resource Record Types*

Resource record type	Function
A (address)	Contains name-to-IP address mapping information, which is used to map a DNS domain name to a host IP address on the network. An A

	resource record is also referred to as a host record
NS (name server)	Designates the DNS domain names for the servers that are authoritative for a certain zone or that contain the zone file for that domain.
CNAME (canonical name)	Allows you to provide additional names to a server that already has a name in an A resource record. A CNAME resource record is also referred to as an alias record.
MX (mail exchanger)	Specifies the server to which e-mail applications can deliver mail.
SOA (start of authority)	Indicates the starting point or original point of authority for information stored in a zone. The SOA resource record is the first resource record created when you add a new zone. It also contains several parameters used by other computers that use DNS to determine how long they will use information for the zone and how often updates are required.
PTR (pointer)	Used in a reverse lookup zone created in the in-addr.arpa domain to designate a reverse mapping of a host IP address to a host DNS domain name
SRV (service)	Registered by services so that clients can locate a service by using DNS. SRV records are used to identify services in Active Directory.

3.5.3 Zone Transfers

Zone transfer is the process of replicating a zone file to another DNS server. Zone transfers occur when names and IP address mappings change in your domain. When this happens, the changes to the zone are copied from a master server to its secondary servers. In Windows 2000, zone information is updated by **incremental zone transfer** (IXFR), which replicates only changes to the zone file and not the entire zone file. DNS servers that do not support IXFR request the entire contents of a zone file when they initiate a zone transfer. Zone transfer occurs when:

- A **master serve**r sends a notification of a change in the zone to one or more secondary servers. When the secondary server receives the notification, it queries the master server for the changes.
- A **secondary server** queries a master server for changes to the zone file. This occurs when the DNS Server service on the secondary server starts, or when the refresh interval on the secondary server expires.

You can configure the frequency of a zone transfer by modifying the **Start of Authority** (SOA) resource record. The SOA resource record specifies the domains for which the zone is authoritative, and the parameters for how zone transfers occur. It also contains administrative information about the zone.

A secondary server queries its primary server for updates to a zone file and uses the serial number in the SOA resource record to determine whether changes have been made to the zone. If the serial number has changed, a zone transfer occurs to update the records on the secondary server. If a secondary server does not

receive updates from its master server, you can use the Nslookup utility to compare the serial numbers in each server's SOA resource record. To compare serial numbers by using the Nslookup utility:

- Click on the **START** button
- Click on **RUN**
- On the **RUN** dialog box, type **CMD**
- Click **OK**
- At the **COMMAND PROMPT** that appears, type **NSLOOKUP**
- Type the **name of the primary server**
- Type **set type=SOA**
- Type **domain name** in which the primary server resides
- **Record** the serial number that appears in the SOA resource record
- Type the name of the **secondary server**
- Type **set type=SOA**
- Type **domain name** in which the primary server resides
- **Record** the serial number that appears in the SOA resource record
- Type **EXIT**

You can force a zone transfer by increasing the serial number on the primary server. To do this open DNS on the server that hosts the primary zone file. You can locate DNS on the Administrative Tools menu. In DNS open the Properties dialog box for the zone, and then click the Start of Authority tab. Click Increment to increase the serial number, and then click OK.

3.5.4 Zone Transfer Security

You can also specify the servers that are authorized to receive zone transfers for the zone by selecting one of the options on the Zone Transfers tab of the Properties dialog box for the zone. These options are:

- **To any server**. Enables zone information to replicate to any server.
- **Only to servers listed on the Name Servers tab**. Enables zone information to replicate only to the servers that are listed on the Name Servers tab of the Properties dialog box for the zone. The Name Servers tab contains a list of servers that are in the same domain as the zone.
- **Only to the following servers**. Specifies whether you want to allow zone transfers only to the servers that you list under IP address on the Zone Transfers tab of the Properties dialog box for the zone.

3.5.5 Active Directory Integrated Zones

Active Directory integrated zone data is stored as an Active Directory object and is replicated as part of domain replication. This provides the following advantages:

- **No single point of failure**. With Active Directory integrated zones, changes made by using the dynamic update protocol can be made to any server that hosts the Active Directory integrated zone, rather than to a single server.
- **Fault tolerance**. All Active Directory integrated zones are primary zones. Therefore, each domain controller that hosts an Active Directory integrated zone maintains the zone information. Only domain controllers that reside in the Active Directory domain in which the zone data is stored can host the zone.

- **Single replication topology**. Zone transfers occur automatically as part of Active Directory replication, eliminating the need to configure replication for DNS and Active Directory separately.
- **Secure dynamic updates**. With Active Directory integrated zones, you can set permissions on zones and records in those zones. Also, updates that use the dynamic update protocol can come from only authorized computers. You can create Active Directory integrated zones only on servers that are configured as domain controllers and that have the DNS Server service installed on them.

3.6 Dynamic Updates

When a client receives a new IP address from a DHCP server, the name-to-IP address mapping information that is stored on a DNS server must be updated. By default, Windows 2000 and Windows XP clients and Windows 2000 DHCP servers can register with DNS and dynamically update DNS with their name-to-IP address mapping information with DNS servers that are configured to support dynamic updates.

> **Note:** Static DNS servers are not able to interact dynamically with DHCP when client configurations change. It is therefore recommended that you **upgrade** all DNS servers from Windows NT 4.0 to Windows 2000 to enable them to support dynamic updates.

However, computers running earlier versions of Windows, such as Windows NT and Windows 98 are not able to update DNS therefore you must **configure the DHCP server to update A and PTR resource** records for these clients.

When you configure dynamic updates you must configure the DNS server for dynamic updates; the DHCP server for dynamic updates; and the client computers for dynamic updates.

3.6.1 Secure Dynamic Updates

You can configure the DNS server to perform secure dynamic updates for **Active Directory integrated zones**. With secure dynamic updates, the authoritative DNS server accepts new registrations only from computers that have a computer account in Active Directory, and accepts updates only from the computer that originally registered the record. The DNS server refuses updates until the DHCP servers and clients encrypt the information. Secure dynamic updates allow you to specify which users and groups are authorized to modify zones and resource records and will prevent unauthorized users from modifying zones and resource records.

To configure secure dynamic updates on the DNS server:

- Click on the **START** button
- Point to **PROGRAMS**
- Point to **ADMINISTARTIVE TOOLS**
- Click on **DNS**
- Open the **PROPERTIES** dialog box for the Active Directory integrated zone on the DNS server that you want to configure.
- Click on the **GENERAL** tab
- In the **ALLOW DYNAMIC UPDATES** list, click **ONLY SECURE UPDATES**

- Click **OK**

Domain Controllers are also identified by the specific **services** that they provide. Windows 2000 uses DNS to locate domain controllers by resolving a domain or computer name to an IP address. DNS servers use the information in the **SRV resource record** and the **A resource record** to locate domain controllers. SRV resource records map a particular service to the domain controller that provides that service. The format of an SRV resource record contains this information and TCP/IP specific information. When a domain controller starts, the Net Logon service running on the domain controller uses the DNS dynamic update feature to register with the DNS database the SRV resource records for all Active Directory–related services that the domain controller provides. Therefore, a computer running Windows 2000 can query a DNS server when it must contact a domain controller.

3.6.2 SRV Resource Records and A Resource Records

When a domain controller starts, it registers SRV resource records and an A resource record that contains its DNS computer name and its IP address. A DNS server then uses this combined information to resolve DNS queries and return the IP address of a domain controller so that the client computer can locate the domain controller. In Windows 2000, domain controllers are also referred to as **Lightweight Directory Access Protocol** (LDAP) servers because they run the LDAP service that responds to requests to search for or modify objects in Active Directory.

3.6.3 Creating Resource Records

You can create resource records manually for clients that are unable to create them dynamically such as Windows NT 4.0 servers that have a static IP address. To create a new resource record, open DNS. Right-click the name of the zone to which you want to add the new resource record, and then click the type of resource record that you want to create, or click Other New Records for a complete list of resource records.

3.6.4 Using nslookup to resolve DNS problems

You can use nslookup to verify that the information contained in resource records is correct. Nslookup has two modes: interactive mode and noninteractive mode. You should use **interactive mode** when you require more than one piece of data and **noninteractive mode** when you require a single piece of data, or when you want to include an Nslookup command in a command or batch file. Type the Nslookup syntax at the **command** prompt, and the data is returned.

3.7 Security for Remote Connections

Windows 2000 uses authentication and authentication protocols to ensure network security. **Authentication** refers to the process in which the computer or network system checks a user's name and password against an authoritative database and only grants access if the user name and password match those in the database. **Authentication protocols** are used to transmit and receive user names and passwords. Windows 2000 supports a number of authentication protocols:

- **PAP** is the least secure authentication protocol and transmits passwords in plain text, i.e. unencrypted. This is used when two computers cannot negotiate a more secure form of authentication.
- **SPAP** is a proprietary authentication protocol used by Shiva clients to dial in to computers running Windows 2000 Server and by Windows 2000 clients to dial in to Shiva servers.

- **CHAP** resolves the problem of transmitting passwords in clear text by negotiating a secure form of encrypted authentication by using Message Digest 5 (MD5), which is a challenge-response hashing scheme.
- **MS-CHAP** uses the same type of authentication but uses MD4 as its hashing method.
- **MS-CHAP v2** is more advanced than CHAP and MS-CHAP and uses mutual authentication, stronger initial data encryption keys, and different encryption keys for sending and receiving data.
- **EAP** is an extension of PPP, which is the basis for PPTP, works with dial-in, PPTP and L2TP clients, and allows additional authentication methods with PPP. These include smart cards, public key authentication and certificates

3.8 Internet Connection Sharing (ICS)

ICS is a new feature that has been introduced with Windows 2000. It allows one computer to host an Internet connection for a network and provides IP address allocation, network address translation (NAT) and name resolution services for all ICS clients.

3.8.1 Configuring Internet Connection Sharing

The computer hosting ICS must have two connections; one to the internal network and one to the Internet. Once these connections have been created, you can enable ICS:

- Click on the **START** button
- Pont to **SETTINGS**
- Open **NETWORK AND DIAL-UP CONNECTIONS**
- Right-click on the desired remote connection and select **PROPERTIES**
- Select the **SHARING** tab on the **DIAL-UP CONNECTION PROPERTIES** dialog box that appears.
- Select the **ENABLE INTERNET SHARING FOR THIS CONNECTION** check box.

Note: You configure the Internet Connection for ICS, not the computer.

3.8.2 Configuring ICS Clients

The ICS client computers network properties must be configured as follows:

- LAN using Client for Microsoft Networks, TCP/IP, and file and printer sharing
- TCP/IP configured to obtain IP address and DNS server address automatically from a DHCP server.

- Start **Internet Explorer**
- Click on the **TOOLS** drop down menu
- Select **INTERNET OPTIONS**
- Click on the **CONNECTIONS** tab
- Select **NEVER DIAL A CONNECTION** in the **DIAL-UP SETTINGS**
- Click on **LAN SETTINGS**
- Select the **AUTOMATICALLY DETECT SETTINGS** check box

- Clear the **USE AUTOMATIC CONFIGURATIN SCRIPT** and the **USE A PROXY SERVER** check boxes
- Click on **OK** to close **LAN SETTINGS**
- Click on **OK** to the **INTERNET OPTIONS** dialog box

3.9 Connecting to a Novell NetWare Network

Windows 2000 computers can use **NWLink**, **Client Services for NetWare**, and **Gateway (and Client) services for NetWare** to connect to a Novell NetWare-based server using IPX/SPX.

3.9.1 Configuring NWLink

The NWLink protocol allows Windows 2000 computers to gain access to applications running on Novell NetWare-based servers. The configuration of NWLink involves three components: frame type, network number, and internal network number. When you install NWLink, Windows 2000 automatically detects a **frame type**, which defines the way that the network adapter card formats data and should match the frame type on the NetWare server; and a **network number**, which must be unique for each network segment and all computers on a segment using the same frame type must use the same network number to communicate with one another. Windows 2000 also provides a generic internal network number. However, you must manually specify an internal network number if you plan to run FPNW or IPX routing.