

# TABLE OF CONTENTS

## List of Tables

### Introduction

## 1. Installing and Deploying Windows 2000: A brief Overview

- 1.1 Performing an unattended installation.
  - 1.1.1 Using an unattended answer file.
  - 1.1.2 Using the System Preparation tool (disk imaging).
  - 1.1.3 Deploying Software applications
    - 1.1.3.1 Windows Installer
    - 1.1.3.2 Deploying Service Packs
- 1.2 The Windows 2000 Boot Process
  - 1.2.1 Files Used in the Boot Process
    - 1.2.1.1 Preboot SeZuence
    - 1.2.1.2 Boot SeZuence
    - 1.2.1.3 Kernel Load
    - 1.2.1.4 Kernel Initialization
    - 1.2.1.5 Logon
- 1.3 The Boot.ini File
  - 1.3.1 Components of the Boot.ini File
  - 1.3.2 ARC Paths
  - 1.3.3 Boot.ini Switches
- 1.4 Advanced Boot Options
- 1.5 The Recovery Console
  - 1.5.1 Installing and Starting the Recovery Console
  - 1.5.2 Using the Recovery Console

## 2. Managing Windows 2000

- 2.1 Installing New Hardware
- 2.2 Using Driver Signing
  - 2.2.1 Configuring Driver Signing
  - 2.2.2 The File Signature Verification Utility
- 2.3 Configuring Hard Disks
  - 2.3.1 Disk Storage Types
  - 2.3.2 Configuring File Systems
  - 2.3.3 Encrypting File System (EFS)
  - 2.3.4 Volume Mounting

- 2.3.5 File Compression
- 2.3.6 Copying and Moving Compressed Files and Folders

- 2.4 Backing Up and Restoring Data
  - 2.4.1 Windows Backup
  - 2.4.2 Backup Types

### **3. Configuring the Windows 2000 Network**

- 3.1 Creating Network Connections
- 3.2 Configuring automatic IP Addressing
  - 3.2.1 DHCP Addressing
  - 3.2.2 Automatic Private IP Addressing
  - 3.2.3 The DHCP Lease Process
    - 3.2.3.1 Automatic Lease Renewal
    - 3.2.3.2 Manual Lease Renewal
- 3.3 Name Resolution
  - 3.3.1 NetBIOS Name Resolution
  - 3.3.2 Host Name Resolution (DNS)
- 3.4 DNS Zones
  - 3.4.1 Caching-only DNS servers
  - 3.4.2 Zone Files
  - 3.4.3 Zone Transfers
    - 3.4.3.1 Zone Transfer Security
  - 3.4.4 Active Directory Integrated Zones
- 3.5 Dynamic DNS Updates
  - 3.5.1 Secure Dynamic Updates
  - 3.5.2 SRV Resource Records and A Resource Records
  - 3.5.3 Creating Resource Records
  - 3.5.4 Using nslookup to resolve DNS problems
  - 3.5.5 Lookup Types
- 3.6 Testing IP Connections
  - 3.6.1 Using the IPConfig Utility
  - 3.6.2 Using the ping Utility
  - 3.6.3 Using the tracert Utility
  - 3.6.4 Using the net and nbstat Utilities
- 3.7 Security for Remote Connections
- 3.8 Internet Connection Sharing (ICS)
  - 3.8.1 Configuring Internet Connection Sharing
  - 3.8.2 Configuring ICS Clients

- 3.9 Connecting to a Novell NetWare Network
  - 3.9.1 Configuring NWLink

## **4. The Windows 2000 Network Infrastructure**

- 4.1 Directory Service Functionality
  - 4.1.1 Simplified Administration
  - 4.1.2 Open Standards Support
- 4.2 Active Directory Support for Client Computers
- 4.3 Administering and Managing Active Directory
  - 4.3.1 Active Directory Objects
    - 4.3.1.1 Controlling Access to Active Directory Objects
  - 4.3.2 Moving Active Directory Objects
    - 4.3.2.1 The MOVETREE Command-line Utility
    - 4.3.2.2 LostAndFound Objects
- 4.4 Active Directory Replication
  - 4.4.1 Multimaster Replication
  - 4.4.2 Replication Latency
  - 4.4.3 Resolving Replication Conflicts
  - 4.4.4 Single Master Operations
  - 4.4.5 Using Sites to Optimize Active Directory Replication
    - 4.4.5.1 Creating A New Site
    - 4.4.5.2 Site Link Attributes
    - 4.4.5.3 Site Link Bridges
    - 4.4.5.4 Replication Within Sites
    - 4.4.5.5 Replication Between Sites
- 4.5 Managing Network Resources
  - 4.5.1 Delegating Administrative Control
  - 4.5.2 Publishing Resources
  - 4.5.3 Setting Up and Managing Published Printers
  - 4.5.4 Setting Up and Managing Published Shared Folders
- 4.6 Monitoring User Access to Shared Folders
  - 4.6.1 Monitoring User Sessions
  - 4.6.2 Sending Administrative Messages to Users

## **5 Routing and Remote Access Service (RRAS)**

- 5.1 Combining Routing and Remote Access
- 5.2 Installation and Configuration
  - 5.2.1 Routing and Remote Access Service Features
  - 5.2.2 Remote Access Client
  - 5.2.3 Remote Access Protocols

- 5.2.4 Remote Access Security
  - 5.2.4.1 Secure User Authentication
  - 5.2.4.2 Mutual Authentication
  - 5.2.4.3 Data Encryption
  - 5.2.4.4 Callback
  - 5.2.4.5 Caller ID
  - 5.2.4.6 Remote Access Account Lockout

- 5.3 Managing Authentication
  - 5.3.1 Windows Authentication
  - 5.3.2 RADIUS Authentication
  - 5.3.3 Virtual Private Networks (VNP)
  - 5.3.4 Tunnelling
  - 5.3.5 RRAS Tools

## **6 Administering User Accounts**

- 6.1 Types of User Accounts
  - 6.1.1 Local User Accounts
  - 6.1.2 Domain User Accounts
  - 6.1.3 Built-In User Accounts
- 6.2 Creating User Accounts
  - 6.2.1 Creating Local User Accounts
  - 6.2.2 Creating Domain User Accounts
  - 6.2.3 Copying Domain User Accounts
- 6.3 Configuring Account Policies
  - 6.3.1 Configuring Password Policy
  - 6.3.2 Configuring Account Lockout Policy
- 6.4 Managing Users and User Accounts
  - 6.4.1 Managing User Data
  - 6.4.2 Using User Profiles
    - 6.4.2.1 Mandatory User Profiles
    - 6.4.2.2 Roaming User Profiles
    - 6.4.2.3 Specifying Home Directories
- 6.5 Managing Users by Using Groups
  - 6.5.1 Group Scopes
    - 6.5.1.1 Local Groups
    - 6.5.1.2 Global Groups
    - 6.5.1.3 Domain Local Groups
    - 6.5.1.4 Universal Groups
    - 6.5.1.5 Special Identity Groups
- 6.6 Group Policy Objects
  - 6.6.1 Group Policy Settings for Computers and Users

### 6.6.2 Linking Group Policy Objects

### 6.7 Group Policy Inheritance

#### 6.7.1 Order of Application

#### 6.7.2 Controlling the Processing of Group Policy

#### 6.7.3 Refreshing Group Policy at Established Intervals

#### 6.7.4 Resolving Conflicts Between Group Policy Settings

#### 6.7.5 Modifying Group Policy Inheritance

### 6.8 Managing User Environments

#### 6.8.1 Administrative Templates

#### 6.8.2 Desktop Security Settings

#### 6.8.3 Group Policy Script Settings

##### 6.8.3.1 Folder Redirection

##### 6.8.3.2 Software Deployment

## 7. Controlling Access to Network Resources

### 7.1 Access Control List

### 7.2 NTFS Folder Permissions

### 7.3 NTFS File Permissions

### 7.4 Multiple NTFS Permissions

#### 7.4.1 Cumulative Permissions

#### 7.4.2 The Deny Permission

### 7.5 Setting NTFS Permissions

### 7.6 NTFS Permissions Inheritance

### 7.7 Assigning Special Access Permissions

#### 7.7.1 Changing Permissions

#### 7.7.2 Taking Ownership

### 7.8 Copying and Moving Files and Folders

## 8. Shared Files and Folders

### 8.1 Shared Folder Permissions

### 8.2 Shared Application Folders

### 8.3 Data Folders

### 8.4 Administrative Shared Folders

### 8.5 Offline Files

- 8.5.1 Enabling Offline Files
- 8.5.2 Offline File Synchronization

## 8.6 Combining Shared Folder Permissions and NTFS Permissions

## 9. Monitoring Network Resources

- 9.1 Monitoring Access to Shared Folders
  - 9.1.1 Monitoring Shared Folders
  - 9.1.2 Modifying Shared Folder Properties
  - 9.1.3 Monitoring Open Files
  - 9.1.4 Disconnecting Users from Open Files
  - 9.1.5 Monitoring Network Users
  - 9.1.6 Monitoring User Sessions
  - 9.1.7 Disconnecting Users
- 9.2 Auditing
  - 9.2.1 Using an Audit Policy
  - 9.2.2 Using Event Viewer to View Security Logs
  - 9.2.3 Setting Up Auditing
    - 9.2.3.1 Setting an Audit Policy
    - 9.2.3.2 Auditing Access to Files and Folders
    - 9.2.3.3 Auditing Access to Printers
- 9.3 Using Event Viewer
  - 9.3.1 Viewing Security Logs
  - 9.3.2 Locating Events
  - 9.3.3 Managing Audit Logs

## 10. Monitoring System Performance

- 10.1 Adding Counters
- 10.2 Monitoring Active Directory Performance

## 11 Practice Labs

- 11.1 Installing Active Directory
- 11.2 Installing and Configuring DNS
  - 11.2.1 Installing DNS
  - 11.2.2 Configuring DNS Zones
- 11.3 Setting up the Internet Connection and Configuring ICS
  - 11.3.1 Setting up the Internet Connection
  - 11.3.2 Configuring the Internet connection for ICS
- 11.4 Creating new user accounts in Active Directory

- 11.5 Organizing users into User Groups
  - 11.5.1 Creating a User Group
  - 11.5.2 Placing Users in User Groups
- 11.6 Creating Organizational Units
- 11.7 Organizing User Groups in Organizational Units
- 11.8 Working with Printers
  - 11.8.1 Installing Additional Printers
  - 11.8.2 Specifying Printer Priorities
- 11.9 Configuring Disk Quotas
- 11.10 Encrypting Files and Folders
- 11.11 Compressing Files and Folders

## LIST OF TABLES

TABLE 1.1	System Preparation Tool Switches
TABLE 1.2	Windows 2000 Boot Files
TABLE 1.3	ARC Path Naming Conventions
TABLE 1.4	Boot.ini Switches
TABLE 1.5	Some Recovery Console commands
TABLE 2.1	Command-line Switches for the Cipher command
TABLE 3.1	Zone Types
TABLE 3.2	Resource Record Types
TABLE 3.3	IPConfig Switches
TABLE 3.4	Ping Errors
TABLE 3.5	nbstat Commands
TABLE 4.1	Common Active Directory Objects
TABLE 4.2	Find Dialog Box Options
TABLE 4.3	Standard Active Directory Object Permissions
TABLE 4.4	MOVETREE Command-Line Switches
TABLE 4.5	Delegation Of Control Wizard Options
TABLE 5.1	Netsh command-line options
TABLE 5.2	Netsh global commands
TABLE 6.1	Password Policy Options
TABLE 6.2	Account Lockout Policy Options
TABLE 6.3	The Administrative Templates
TABLE 6.4	The Desktop Security Settings
TABLE 6.5	Group Policy Settings to Control the Network Environment
TABLE 6.6	Group Policy Settings to Control Access to the Administrative Tools
TABLE 7.1	Permission Inheritance Options
TABLE 8.1	Shared Folder Permissions
TABLE 9.1	Options for Filtering and Finding Events
TABLE 10.1	Some Performance Console Objects
TABLE 10.2	Some Useful Performance Console Counters



# Implementing and Administering a Microsoft Windows 2000 Directory Services Infrastructure

**Exam Code: 070-217**

## Certifications:

**Microsoft Certified (MCP)**

**Microsoft Certified Systems Engineer (MCSE)**

**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 070-217 - Implementing and Administering a Microsoft Windows 2000 Directory Services Infrastructure exam. As such it provides all the information required to pass the Microsoft 070-217 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 070-217 exam and does not represent a complete reference work on the subject of Implementing and Administering a Microsoft Windows 2000 Directory Services Infrastructure. This StudyGuide also includes the information required to answer Questions related to the installation of Windows 2000 Server, Windows 98 and Windows NT, DNS, DHCP and NAT that may be asked during the exam. Topics covered in this Study Guide includes Installing, Deploying and Managing Windows 2000; Configuring the Windows 2000 Network Infrastructure; DNS Name Resolution and DNS Replication; Installing, Administering and Managing Active Directory; Monitoring Active Directory Performance; Administering User Accounts; Using Group Policy to Manage User Accounts; Controlling Access to Network Resources; and Monitoring System Performance.

## Intended Audience

This Study Guide is targeted specifically at people who wish to take the Microsoft MCSE exam 070-217 ... Implementing and Administering a Microsoft Windows 2000 Directory Services Infrastructure. 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 exams: 070-210 ... Installing, Configuring, and Administering Microsoft Windows 2000 and 070-215 .. 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 the 070-217 StudyGuide and the 070-215 and 070-216 StudyGuides. 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 070-215 and 070-216 StudyGuides, The relevant information from the 070-215 and 070-216 StudyGuides are included in this StudyGuide. This is thus the only StudyGuide you will reZuire to pass the e am.
- Study each chapter carefully until you fully understand the information. This will reZuire 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 e perience, referring back to the te t 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 e am.

**Note:** Remember to pay special attention to these note bo es as they contain important additional information that is specific to the e am.

Good luck!

## 1. Installing and Deploying Windows 2000: A brief Overview

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. These are, however, not related to managing a Windows 2000 Network Infrastructure. What follows in this section is related to the e am.

### 1.1 Performing an unattended installation.

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

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

#### 1.1.1 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**. An answer file is an automated script that supply.s.the Windows 2000 Setup program with all the information it would reZuire during the installation.

You can use **Setup Manager** to create and modify an 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 e tracted 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 **E tract** on the menu that pops up.

You can use Setup Manager to create an answer file for various types of unattended installations and you can also choose the answer file.s.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 reZuired 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 reZuired by the Setup Wizard during the graphical user interface stage (stages 2 and 3) of the installation.

#### 1.1.2 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 e ct 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, e cept for the initial installation on the test computer. In other words, you would not be using *winnt.e e* or *winnt32.e e* 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 uniZue name.

The **System Preparation tool** (*Sysprep.e e*) 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 reZuest 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 1.1.

TABLE 1.1: *System Preparation Tool Switches*

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

### 1.1.3 Deploying Software applications

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.

#### Group Policy ad GPO

Group Policy and GPO is discussed in detail in Section 8.4 of this Study Guide

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.

### 1.1.3.1 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 require 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.

### 1.1.3.2 Deploying Service Packs

Windows 2000 supports the integration of service-packs called **slipstreaming**, so service packs can be integrated with the Windows 2000 installation files. This allows you to keep an image of the operating system. When Windows 2000 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.

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

## 1.2 The Windows 2000 Boot Process

### 1.2.1 Files Used in the Boot Process

A Windows 2000 Intel-based boot seZuence reZuires 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 1.2

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

TABLE 1.2 *Windows 2000 Boot Files*

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.e e	<i>systemroot</i> \System32	Kernel load
Hal.dll	<i>systemroot</i> \System32	Kernel load
System	<i>systemroot</i> \System32\Config	Kernel initialization
<i>Device drivers</i>	<i>systemroot</i> \System32\Drivers	Kernel initialization

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

#### 1.2.1.1 Preboot SeZuence

During startup, a Windows 2000-based computer initializes the boot portion of the hard disk and the preboot seZuence begins. This seZuence 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.

#### 1.2.1.2 Boot SeZuence

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

The boot seZuence 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 loaded. *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 than one hardware 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.

### 1.2.1.3 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 0 0 for the Start entry. These are typically low-level hardware device drivers, such as those for a hard disk.

### 1.2.1.4 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.

### 1.2.1.5 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**.

## 1.3 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. *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.

### 1.3.1 Components of the Boot.ini File

The *Boot.ini* file includes two sections, **[Boot Loader]** and **[Operating Systems]** (SEE FIGURE 1.1) 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.

```
[boot loader]
timeout=10
default=multi(0)disk(0)rdisk(1)partition(1)
\WINDOWS

[operating systems]
multi(0)disk(0)rdisk(0)partition(1)
\WINDOWS="Microsoft Windows 2000 Server I"
/fastdetect
multi(0)disk(0)rdisk(1)partition(1)
\WINDOWS="Microsoft Windows 2000 Server II"
/fastdetect

[boot loader]
\WINDOWS="Microsoft Windows
Recovery Console" /cmdcons
```

FIGURE 1.1: A typical *Boot.ini* file.

### 1.3.2 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. For a list of ARC Paths see Table 1.3.

TABLE 1.3: ARC Path Naming Conventions

Convention	Description
multi( )   scsi( )	The hardware <b>adapter or disk controller</b> . Use <b>scsi</b> only to indicate a SCSI controller on which SCSI BIOS is not enabled. All other hardware adapter or disk controllers use <b>multi</b> . ( ) 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 <b>SCSI ID</b> . 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)

**Note:** The lowest ARC Path, i.e., the ARC Path that points to the first partition on the first hard drive, is **multi(0) disk(0) partition (1)** and not multi(0) disk(0) partition (0)

### 1.3.3 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 1.4 lists some of these switches.

### 1.4 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.

TABLE 1.4: *Boot.ini* Switches

Switch	Description
/basevideo	Boots the computer using the standard VGA video driver.
/fastdetect=[com   com ,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 <i>Boot.ini</i> file.
/ma mem: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.

- **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 reZuired 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 e cept that it adds the drivers and services reZuired to enable network access, and **Safe Mode With Command Prompt**, which is the same as Safe Mode e cept when the computer restarts, it displays a command prompt.
- **Enable Boot Logging** logs the loading and initialization of drivers and services in the *ntbtlog.t t* 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***

**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***.

## 1.5 The Recovery Console

The Recovery Console is a **command-line** interface that can be used to perform a variety of troubleshooting and recovery tasks. These include:

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

### 1.5.1 Installing and Starting the Recovery Console

You can install the Recovery Console from the Windows 2000 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 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 by installing Windows 2000 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**

### 1.5.2 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 1.5.

TABLE 1.5: *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
E it	Enters 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

## 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 **test 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