Study guide by ExamNotes.net
Exam 70-215: Installing, Configuring, and Administering Microsoft Windows 2000 Server

Installing Windows 2000 Server
Requirements

Component	Minimum Requirement	Recommended Configuration
CD-ROM	*Needed when not installing over the network*	*Needed when not installing over the network*
CPU	*Pentium 133*	*Pentium II or higher*
Display	*VGA*	*SVGA*
Hard disk space	*1 GB*	*2 GB or higher*
Keyboard and Mouse	*Required*	*Required*
Memory	*128 MB*	*256 MB or higher*
Networking	*NIC*	*NIC*

• If you choose to reformat the partition as NTFS, only Windows 2000 and Windows NT has access to that partition.
• Use FAT if your boot partition is smaller than 2 GB and you want to gain access to that partition when running MS-DOS, Windows 3.x, Windows 95, Windows 98, or OS/2 on this computer.
• You should choose the NTFS option if you are running Windows 2000 and you want to take advantage of these features in NTFS:

Attribute	Description
File-level and directory-level local security	*NTFS allows you to control access to files and directories regardless of whether access is local or over the network.*
Disk compression	*NTFS compresses files to store more data on the partition.*
Disk quotas	*NTFS allows you to control disk usage on a per-user basis.*
Encryption	*NTFS allows you to encrypt file data on the physical hard disk.*

• All hardware should appear on the Windows 2000 Hardware Compatibility List (HCL).
• If Windows 2000 is being integrated into an existing Windows NT 4.0 domain

structure, mixed mode must be used. If Windows 2000 is being installed into an infrastructure where all domain controllers will be running Windows 2000, the domain controllers should use native mode. Once all domain controllers in a domain are upgraded, the domain can be moved from Mixed mode to Native mode. In Native mode all clients make use of Windows 2000 transitive trust. A user can connect to any resource in the enterprise. Native mode allows group nesting.

- Servers are installed as Member Servers by default. To promote a machine to a Domain Controller, run dcpromo.
- Windows 2000 Server supports Symmetric Multi-processing with a maximum of four processors, and up to 4 GB of RAM. Advanced Server supports up to 8 processors and 8 GB of RAM. Windows 2000 DataCenter Server is available in OEM configurations and supports up to 32 processors and 64 GB of RAM.

Attended Installation

Four stages of Setup: Setup Program, Setup Wizard, Installing Networking, Complete Setup.

1. Setup Program: Loads Setup program into memory. Starts text-based Setup program. Creates Win2000 partition. Formats partition. Copies setup files to hard disk. Reboots computer.
2. Setup Wizard: Graphical user interface for installation information (e.g. product key, names, passwords).
3. Install Windows Networking: Detection of adapter cards, installation of default networking components; Client for MS Networks, File and Printer Sharing for MS Networks and TCP/IP protocol. Join a workgroup or domain. Installation of components.
4. Complete Setup: Copy files. Configure the computer. Save the configuration. Removal of temporary files.

Installing from CD-ROM

- Does not require floppies.
- If installing using a MS-DOS or Win95/98 boot floppy, run WINNT.EXE from the i/386 to begin Windows 2000 setup.
- To make boot floppies, type MAKEBOOT A: in the \bootdisk directory of the installation CD.

Installing over a Network

- 685 MB minimum plus 100+ MB free hard drive space for temporary files created during installation.
- Boot the network client. Connect to the distribution server. Run WINNT.EXE. Boot from the Setup boot disks. Install Windows 2000. Run WINNT32.EXE if upgrading a previous version of Windows.
- Create a Distribution Server with a file share containing the contents of the /i386 directory from the Windows 2000 CD-ROM.

WINNT.EXE Command Line Switches

Switch	Function
/a	*Enables accessibility options.*
/e:command	*Specifies the command to be executed at the end of GUI setup.*
/i:inffile	*Specifies the file name (no path) of the setup information file. Default is DOSNET.INF.*
/r[:folder]	*Specifies optional folder to be installed.*
/rx[:folder]	*Specifies optional folder to be copied.*
/s[:sourcepath]	*Specifies source location of Windows 2000 files. Full path or network share.*
/t[:tempdrive]	*Specifies drive to hold temporary setup files.*
/u[:answer file]	*Specifies unattended setup using answer file (requires /s).*
/udf:id[,UDF_file]	*Establishes ID that Setup uses to specify how a UDF file modifies an answer file.*

Troubleshooting Installations

Problem	Fix
Failure of Dependency service to start	*Verify that you installed the correct protocol and network adapter. Verify that the network adapter has the proper configuration settings, such as transceiver type, and that the local computer name is unique on the network.*
Failure of Windows 2000 Server to install or start	*Verify that Windows 2000 is detecting all of the hardware and that all of the hardware is on the HCL.*
Inability to connect to the domain controller	*Verify that the domain name is correct. Verify that the server running the DNS service and the domain controller are both running and online. Verify that the network adapter card and protocol settings are set correctly.*
Insufficient disk space	*Use the Setup program to create a partition by using existing free space on the hard disk. Delete and create partitions as needed to create a partition that is large enough for installation. Reformat an existing partition to create more space.*
Media errors	*If you are installing from a CD-ROM, use a different CD-ROM drive. If you still receive media errors, try another CD.*
Unsupported CD-ROM drive	*Replace the CD-ROM drive with one that is supported, or try installing over the network. After you have completed the installation, you can add the driver for the CD-ROM drive.*

Unattended Installations

- Answer files are created using the Setup Manager Wizard or a text editor.
- SMW allows for creation of a shared Distribution Folder and OEM Branding.
- Unattended installations use an answer file to provide information during the setup process.

Creating the Answer File

The answer file is a customized script that allows you to run an unattended installation of Windows 2000 Server. The file answers the questions that Setup normally prompts you for during installation. Use the Setup Manager to create the answer file, or create it manually. To create the answer file manually, you can use a text editor such as Notepad. An answer file consists of section headers, parameters, and values for those parameters. Although most of the section headers are predefined, you can also define additional section headers.

User Interaction Levels for Unattended Installs

Interaction	Description
Fully Automated	*Mainly used for Win2000 Professional desktop installs.*
GUI Attended	*Only used for automating the second stage of setup. All other stages require manual input.*
Provide Defaults	*Administrator supplies default answers. User can accept defaults or make changes when needed.*
Hide Pages	*Users only interact where Administrator did not provide default information.*
Read Only	*Displays information to user without allowing interaction to pages where Administrator has provided default information.*

System Preparation Tool (SYSPREP.EXE)

- Use SYSPREP when the master computer and the target computers have identical or nearly identical hardware, including the HAL and mass storage devices.
- Adds a mini-setup wizard to the image file which is run the first time the computer it is applied to is started. Guides user through re-entering user specific data. Can be automated by providing a script file.
- Available switches for SYSPREP.EXE are: /quiet (no user interaction), /pnp (forces detection of PnP devices), /reboot (restarts computer), and /nosidgen (does not regenerate SID on target computer).
- Must be extracted from DEPLOY.CAB in the \support\tools folder on the Windows 2000 Professional CD-ROM.
- Removes unique elements of a fully installed computer system so it can be duplicated using imaging software.
- Specifying a CMDLINES.TXT file in your SYSPREP.INF file allows an administrator to run commands or programs during the mini-Setup portion of SYSPREP. The Cmdlines.txt file contains the commands that are executed during the GUI mode phase of

the installation process. Setup executes these commands when installing optional components, such as applications that need to be installed immediately after Windows 2000 Server is installed. If you plan to use CMDLINES.TXT, you need to place the file in the \$OEM$ subfolder of the distribution folder. If you are using SYSPREP, place CMDLINES.TXT in the \$OEM$\$1\Sysprep subfolder.

- To use the SYSPREP tool, install Windows 2000 Server on a reference computer. Install any other applications on the reference computer that you want installed on the target computers. Then run SYSPREP followed by a third-party disk imaging utility. SYSPREP prepares the hard disk on the master computer so that the disk imaging utility can transfer an image of the hard disk to the other computers.
- Uses Setup Manager Wizard (SMW) to create a SYSPREP.INF file. SMW creates a SYSPREP folder in the root of the drive image and places SYSPREP.INF in this folder. The mini-setup wizard checks for this file when it runs.

Upgrading from a Windows NT Domain

Upgrading a Windows NT domain involves several stages:

1. Planning for a Windows NT domain upgrade.
2. Preparing for a Windows NT domain upgrade.
3. Upgrading the PDC.
4. Upgrading the BDCs.
5. Upgrading member servers.

Upgrading from Microsoft Windows NT 4.0

- Run WINNT32 /CHECKUPGRADEONLY to check for compatible hardware and software. This generates a report indicating which system components are Windows 2000 compatible.
- Run WINNT32.EXE to upgrade from a previous version of Windows.
- Upgrade installations from a network file share are not supported in Windows 2000. Do a CD-based upgrade or perform a clean installation of Windows 2000 and re-install needed applications.
- Upgrade paths are not available for Windows NT 3.51 with Citrix or Microsoft BackOffice Small Business Server.
- Upgrading Windows NT Server retains most system settings, preferences, and application installations. If you prefer a dual-boot configuration, choose the Install Windows 2000 Server option. Press Enter or click Next to continue. Only Windows NT Server can be upgraded to Windows 2000 Server. If you are installing Windows 2000 Server on a Windows NT Server computer, you are prompted to select Upgrade to Windows 2000 Server or Install Windows 2000 Server. If your computer is currently running Windows 95, Windows 98, or Windows NT, connect to the system files over the network and run WINNT32.EXE, located in the I386 directory.
- Windows 2000 Server will upgrade and preserve settings from Windows NT 3.51 and 4.0 Server, Windows NT 4.0 Terminal Server, and Windows NT 4.0 Enterprise Edition.

Troubleshooting Remote Installations

Problem	Solution
Insufficient disk space	*Create a new partition or reformat an existing partition to free up space.*
Error loading operating system	*Disk geometry is reported incorrectly on a NTFS partition. Use a partition less than 4 GB or use a FAT32 partition.*
Dependency service will not start	*Verify correct protocol and network adapter in the Network Settings.*
Cannot contact domain controller	*Ensure network cable is connected. Verify that servers running DNS and a domain controller are both on-line. Make sure all network settings are correct.*

Install, Configure and Troubleshoot Access to Resources

Install and Configure Network Services

TCP/IP Server Utilities

Utility	Feature
Web Server	*Internet Information Services 5. Supports Internet Printing and Web Distributed Authoring and Versioning (WebDAV).*
Telnet Server	*Windows 2000 includes a Telnet Server Service, which is limited to a command line text interface.*
SMTP Server	*Used for sending mail in conjunction with FrontPage 2000 Server Extensions and Active Directory replication. Does not support IMAP4, POP3, etc.*
FTP Server	*File Transfer Protocol. Administered using the IIS snap-in.*
FrontPage 2000 Server Extensions	*Adds pre-compiled scripts and programs that allow Web site authors to implement advanced features without much programming knowledge.*

TCP/IP Client Utilities

Utility	Feature
Telnet Client	*Can be used to open a text-based console on UNIX, Linux and Windows 2000 systems.*
FTP Client	*Command line based.*
Outlook Express 5	*SMTP, POP3, IMAP4, NNTP, HTTP, and LDAP complaint E-mail package.*
Internet Explorer 5	*Microsoft's powerful and thoroughly integrated Web browser.*

Install and Configure Local and Network Printers

- Enabling Availability option allows Administrator to specify the hours the printer is available.
- Internet Printing allows you to enter the URL where your printer is located. The print server must be a Windows 2000 Server running Internet Information Server. All shared printers can be viewed at: http://*servernam*e/printers.
- Print Pooling allows two or more identical printers to be installed as one logical printer.
- Print Priority is set by creating multiple logical printers for one physical printer and assigning different priorities to each.
- Print services can only be provided for Windows, UNIX, Apple, and Novell clients.
- The FIXPRNSV.EXE command-line utility to resolves printer incompatibility issues. Services for UNIX 2.0.
- To remedy a stalled spooler, you will need to stop and restart the spooler services in the Services applet in Administrative Tools in the Control Panel.
- Windows 2000 automatically downloads the printer drivers for clients running Win2000, WinNT 4, WinNT 3.51 and Windows 95/98.
- Windows 2000 Server supports Line Printer (LPT), COM, USB, IEEE 1394, and network attached devices.
- You can change the directory containing the print spooler in the advanced server properties for the printer.

Folders and Shared Folders

Distributed File System (Dfs)

- Dfs is a single, logical, hierarchical file system. It organizes shared folders on different computers in a network to provide a logical tree structure for file system resources.
- Computers running Windows 98, Windows NT 4 and Windows 2000 have a Dfs client built-in. Computers running Windows 95 will need to download and install a Dfs client to have access to Dfs resources.
- Logon scripts are stored in the SYSVOL folder. Both NT4 and W2K create a hidden share called REPL$ on the export server when it sends out a replication pulse to the import server.

Standalone Dfs

- Created by using Administrative Tools, Distributed File System, Create a standalone Dfs root.
- Only single-level hierarchies are allowed when using standalone Dfs.
- Stand-alone Dfs information is stored in the local registry.
- Stand-alone Dfs roots have no replication or backup. You can create a replica from a stand-alone Dfs root; however, file replication services are not available.

Domain-based Dfs

- A domain Dfs root must be hosted on either a member server or a domain controller in the domain. Changes to a Dfs tree are automatically synchronized through AD.
- Created using Administrative Tools, Distributed File System, Create a domain Dfs root.
- Directories from multiple different computers can be shown as one single file and folder hierarchy.
- Fault-tolerance is implemented by assigning replicas to a Dfs link. If one replica goes offline, AD directs the Dfs client making the request to mirrored information that exists in a different replica.
- In a domain Dfs root, multiple servers hand out referrals for the Dfs namespace. Fault tolerant Dfs roots use Active Directory services to store Dfs tree topology and remove the root as a single point of failure.

Local Security on Files and Folders

- Anytime a new file is created, the file will inherit permissions from the target folder.
- Features Reparse Points, Encrypting File System (EFS), Disk Quotas, Volume Mount Points, SID Searching, Bulk ACL Checking, and Sparse File Support.
- NTFS 5 uses unique ACLs only once regardless of the number of objects that share it. NTFS can perform a volume wide scan for files using the owner's SID (SID Searching). Both functions require installation of the Indexing Service.
- NTFS partitions can be defragmented in Windows 2000 (as can FAT and FAT32 partitions).
- Permissions are cumulative, except for Deny, which overrides anything.
- Sparse File Support prevents files containing large consecutive areas of zero bits from being allocated corresponding physical space on the drive and improves system performance.
- Volume Mount Points allow new volumes to be added to the file system without needing to assign a drive letter to it. As Volume Mount Points are based on Reparse Points, they are only available under NTFS 5 using Dynamic Volumes.

NTFS File and Folder Permissions

File attributes within a partition or between partitions:

Command	File Attribute
Copying within a partition	Inherits the target folders permissions.
Moving across partitions	Inherits the target folders permissions.
Moving within a partition	File keeps its original permissions.

- Files moved from an NTFS partition to a FAT partition do not retain their attributes, but retain their long filenames.
- The CACLS.EXE utility is used to modify NTFS volume permissions.

Access to Web Sites

Virtual Servers
Multiple Web sites can be hosted on the same machine by using Virtual Servers. There can only be one home directory per virtual server. There are three methods for setting up virtual servers:
1. Each virtual server can have its own IP address. Multiple IPs are bound to the server's NIC and each virtual server is assigned its own IP address.
2. Each virtual server can have the same IP address, but uses a different name under host headers. Host headers rely on newer browsers knowing which site they want to access. Workarounds will have to be implemented for older browsers.
3. Each virtual server can have the same IP address but a different port number.

Virtual Directories
- An alias must be created for the directory.
- Specify the IP address of a virtual directory. If this is not done, the virtual directory will be seen by all virtual servers.
- To map to shares on another server, use the UNC path for the remote server and share and provide a Username and Password to connect with. If the share is on a server in another domain, the credentials must match up in both domains.
- Use a common scripts directory that is not assigned to the IP of a virtual server can handle scripts for all virtual servers.
- Virtual directories are referenced by alias names.

Controlling Access to Web Services
- Requires IIS to be running on the machine where folders are to be shared.
- Use My Computer or Windows Explorer to share folders using Web Sharing tab.Access permissions are; Read, Write, Script Source Access, and Directory Browsing. Application permissions are; None, Scripts, and Execute (includes scripts).

Hardware Devices and Drivers
- Add and remove hardware by using the "Add/Remove Hardware" applet in the Control Panel.
- The Device Manager snap-in manages all currently installed hardware.
- Use Hardware Resources to view Conflicts/Sharing, DMAs, IRQs, Forced Hardware, I/O and Memory.
- Use the System Information snap-in to view configuration information about your computer.

Disk Devices
- Removable media are managed through the Removable Media snap-in.
- To Manage disk devices, use Control Panel, Administrative Tools, Computer Management or by creating a custom console and adding the Disk Management snap-in. The Computer Management snap-in for your custom console enables Disk

Management, Disk Defragmenter, Logical Drives and Removable Storage. There is a separate snap-in for each of these tools except for Logical Drives.
- Use Disk Management to create, delete, and format partitions as FAT, FAT32 and NTFS. Used to change volume labels, reassign drive letters, check drives for errors and backup drives.

Display Devices
- Desktop display properties are managed through the Display applet in Control Panel.
- Monitors are installed, removed, and drivers are updated through Monitors under the Device Manager.
- Use Display Adapters under the Device Manager to install, remove and update drivers.

Driver Signing
- Open System applet in Control Panel and click Hardware tab. Then in the Device Manager box, click Driver Signing to display options:
- *Ignore* - Install all files, regardless of file signature.
- *War*n- Display a message before installing an unsigned file.
- *Bloc*k- Prevent installation of unsigned files.
- The Apply Setting As System Default checkbox is accessible only to Administrators

Windows Signature Verification (SIGVERIF.EXE)
- Running SIGVERIF launches File Signature Verification.
- Checks system files by default, but non-system files can also be checked.
- Saves search results to SIGVERIF.TXT.

System Performance, Reliability and Availability

Usage of System Resources

Performance Console

Windows 2000 provides the System Monitor snap-in and the Performance Logs and Alerts snap-in for monitoring resource usage. The System Monitor snap-in allows you to track resource use and network throughput. The Performance Logs And Alerts snap-in allows you to collect performance data from local or remote computers.

System Monitor Snap-In

Allows you to measure the performance of your own computer or other computers on a network. It performs the following tasks:
- Collect and view real-time performance data on a local computer or from remote computers.
- Create HTML pages from performance views.
- Create reusable monitoring configurations that can be installed on other computers that use MMC.
- Incorporate System Monitor functionality into Microsoft Word or other applications in the Microsoft Office suite by means of Automation.
- Present data in a printable graph, histogram, or report view.
- View data collected either currently or previously in a counter log.

Objects include:

Object	Feature
Cache	*File system cache used to buffer physical device data.*
Logicaldisk	*Logical drives, stripe sets and spanned volumes.*
Memory	*Physical and virtual/paged memory on system.*
Physicaldisk	*Monitors hard disk as a whole.*
Processor	*Monitors CPU load.*

Performance Logs and Alerts Snap-In
Allows you to collect performance data automatically from local or remote computers. Data can be viewed by using System Monitor, or exported to a spreadsheet program or database for analysis and report generation. Performance Logs and Alerts snap-in performs the following:
- Collect data in a comma-delimited or tab-separated format for easy import to spreadsheet programs. A binary log-file format is also provided for circular logging or for logging instances such as threads or processes that might begin after the log starts collecting data.
- Define start and stop times, file names, file sizes, and other parameters for automatic log generation.
- Manage multiple logging sessions from a single console window.
- Set an alert on a counter, thereby stipulating that a message be sent, a program be run, or a log be started when the selected counter's value exceeds or falls below a specified setting.
- View counter data during collection and after collection has stopped.

Optimize Disk Performance
- Defragmenting your hard disks regularly will improve read performance.
- Mirrored volumes and spanned volumes slow down system performance.
- Page files are fastest when spread across several disks, but not the boot or system disks.
- Striping a disk set causes greatest performance increase.

System State Data and User Data

System State data
Comprised of the registry, COM+ class registration database and system startup files. Can also include Certificate Services database if Certificate Services is installed. If machine is a domain controller, Active Directory directory services and SYSVOL directory are included. For machines running Cluster Service, resource registry checkpoints and quorum resource recovery log are included.
- Can be backed up from the command line by typing:

ntbackup systemstate /m normal /f d:\sysstate.bkf /j “System State Data Backup”

• On a domain controller, an Authoritative Restore may need to be performed to force restored system state data to replicate to other domain controllers throughout Active Directory.
• On a domain controller, moving system state data to a separate volume from the system volume can increase performance.
Where /m=backup type (can be copy or normal), /f=filename and /j=job name.

Recovering System State Data
Emergency Repair Disk
Use the Backup utility to create an emergency repair disk. To create an ERD, from the Start menu, select Programs, Accessories, System Tools, Backup. Click Emergency Repair Disk. Insert a blank formatted floppy into the A: drive. Select the Also Backup the Registry to the Repair Directory (%systemroot%\repair\regback) check box. ERD contains AUTOEXEC.NT, CONFIG.NT and SETUP.LOG.

Windows Backup
Launched through Control Panel, System applet, Backup or by running ntbackup from the Start menu. Users can back up their own files and files they have read, execute, modify, or full control permission for. Users can restore files they have write, modify or full control permission for. Administrators and Backup Operators can backup and restore all files regardless of permissions. To restore System State data, start Backup, click the Restore tab and check the box next to System State to restore it along with any other data you have selected. If you do not specify a location for it, it will overwrite your current System State data.

Safe Mode
• Enter safe mode by pressing F8 during operating system selection phase.
• Safe mode loads basic files/drivers, VGA monitor, keyboard, mouse, mass storage and default system services. Networking is not started in safe mode.

Mode	Feature
Boot Normally	*Normal boot.*
Debugging Mode	*Only in Server.*
Directory Services Restore Mode	*Only in Server, not applicable to Win2000 Professional.*
Enable Boot Logging	*Logs loading of drivers and services to ntbtlog.txt in the windir folder.*
Enable VGA Mode	*Boots Windows with VGA driver*
Last Known Good Configuration	*Uses registry info from previous boot. Used to recover from unsuccessful driver installs and registry changes.*
Recovery Console	*Only appears if it was installed using winnt32 /cmdcons or specified in the unattended setup file.*

Running the Recovery Console

To install the Recovery Console, run WINNT32 /CMDCONS from the Windows 2000 CD i386 folder.

- Allows you to boot to a DOS prompt when your file system is formatted with NTFS.
- Can be used to disable services that prevent Windows from booting properly.
- When starting Recovery Console, you must log on as Administrator.

Storage Use

Disks and Volumes

Windows 2000 supports Basic and Dynamic storage. For Windows 2000, basic storage is the default, so all disks are basic disks until you convert them to dynamic storage. Basic storage is the division of a hard disk into partitions. A partition is a portion of the disk that functions as a physically separate unit of storage. Windows 2000 recognizes primary and extended partitions. It can contain primary partitions, extended partitions and logical drives. Basic volumes cannot be created on dynamic disks. Basic volumes should be used when dual-booting between Windows 2000 and DOS, Windows 3.x, Windows 95/98 and all version of Windows NT.

Only Windows 2000 supports dynamic storage. Dynamic storage allows you to create a single partition that includes the entire hard disk. Dynamic disks are divided into volumes, which can consist of a portion, or portions of one or many disks. You do not need to restart the operating system after resizing.

Volume Types

You can upgrade basic disks to dynamic storage and then create Windows 2000 volumes. Fault tolerance is the ability of a computer or operating system to respond to a catastrophic event without loss of data. In Windows 2000, RAID-1 and RAID-5 volumes are fault tolerant.

Volume Type	Characteristics
Mirrored volume	*A mirrored volume consists of two identical copies of a simple volume, each on a separate hard disk. Mirrored volumes provide fault tolerance in the event of hard disk failure.*
RAID-5 volume	*A RAID-5 volume is a fault-tolerant striped volume. Windows 2000 adds a parity-information stripe to each disk partition in the volume. Windows 2000 uses the parity-information stripe toreconstruct data when a physical disk fails. A minimum of threehard disks is required in a RAID-5 volume.*
Simple volume	*Contains space from a single disk*
Spanned volume	*Contains space from multiple disks (maximum of 32). Fills one volume before going to the next. If a volume in a spanned set fails, all data in the spanned volume set is lost. Performance is degraded as disks in spanned volume set are read sequentially.*
Striped set	*Contains free space from multiple disks (maximum of 32) in one logical drive. Increases performance by reading/writing data from all disks at the same rate. If a disk in a stripe set fails, all data is lost.*

Dynamic Volume Limitations

- A boot disk that has been converted from basic to dynamic cannot be converted back to basic.
- Cannot be directly accessed by DOS, Win95/98 or any versions of Windows NT if you are dual-booting.
- Dynamic volumes which were upgraded from basic disk partitions cannot be extended. Volumes created after the disk was upgraded to dynamic can be extended.
- Not supported on portable computers or removable media.
- When installing Windows 2000, if a dynamic volume is created from unallocated space on a dynamic disk, Windows 2000 cannot be installed on that volume.

Dynamic Volume States

State	Description
Failed	*Volume cannot be automatically restarted and needs to be repaired.*
Healthy	*Is accessible and has no known problems.*
Healthy (at risk)	*Accessible, but I/O errors have been detected on the disk. Underlying disk is displayed as Online (Errors).*
Initializing	*Volume is being initialized and will be displayed as healthy when process is complete.*

Disk Management Snap-in Tool

- Disks can be upgraded from Basic to Dynamic storage at any time but must contain at least 1 MB of unallocated space for the upgrade to work.
- Disks that have been removed from another computer will appear labeled as Foreign. Choose "Import Foreign Disk" and a wizard appears to provide instructions.
- Each time you remove or add a new disk to your computer you must choose Rescan Disks.
- For multiple disks removed from another computer, they will appear as a group. Right-click on any of the disks and choose "Add Disk".
- Whenever you add a new disk in a computer it is added as Basic Storage.

Configuring Data Compression

- Compact is the command-line version of the real-time compression functionality used in Windows Explorer. It can be used to display or alter the compression attributes of files or folders on NTFS volumes (does NOT work on FAT or FAT32 volumes).
- Files and folders on NTFS volumes can have their compression attributes set through My Computer or Windows Explorer.

Disk Quotas

By default, only member of the Administrators group can view and change quota settings. Users can be allowed to view quota settings. Volume usage can be monitored on a per-user basis. Disk usage is based on file and folder ownership. Quotas do not use compression. Free space for applications is based on a quota limit. Quotas can be applied only to volumes formatted with NTFS that use Windows 2000. A quota warning should

be set to log an event indicating that the user is nearing his limit. An event should be logged when a user exceeds a specified disk space threshold.

Windows 2000 Network Connections

Using Shared Resources
The Administrators and Power Users groups can create shared folders on a Windows 2000 Professional workstation. Windows 2000 creates administrative shared folders for administrative reasons. These shares are appended with dollar sign ($) which hides the share from users browsing the computer. The system folder (Admin$), the location of the printer drivers (Print$) and the root of each volume (C$, D$, etc.) are all hidden shared folders.

Shared folder permissions apply only when the folder is accessed via the network. By default, the Everyone group is assigned Full Control for all new shared folders. Share level permissions can be applied to FAT, FAT32 and NTFS file systems.

Sharing Tab

Option	Description
Caching	*The settings to configure if and how files within the shared folder are cached locally when accessed by others.*
Do Not Share This Folder	*If you do not want to share this folder. All other options are grayed out.*
Permissions	*The shared folder permissions that apply only when the folder is accessed over the network. By default, the Everyone group is assigned Full Control for all new shared folders.*
Remove Share	*The option that allows you to remove a share. This option appears only after the folder has been shared more than once.*
Share Name	The name that users from remote locations use to make a *connection to the shared folder. You must enter a share name.*
Share This Folder	*If you want to share this folder. All other options are active.*
User Limit	*The number of users who can concurrently connect to the shared folder. The Maximum Allowed option allows Windows 2000 Server to support an unlimited number of connections. The number of Client Access Licenses (CALs) purchased limits the connections.*

Virtual Private Networks (VPNs)
A virtual private network (VPN) is an extension of the private network that encompasses encapsulated, encrypted, and authenticated links across shared or public networks. A VPN mimics the properties of a dedicated private network, allowing data to be transferred between two computers across an internetwork, such as the Internet. Point-to-point connections can be simulated through the use of tunneling, and LAN connectivity can be simulated through the use of virtual LANs (VLANs).

• L2TP - Layer Two Tunneling Protocol. Creates a tunnel, but it does not provide data encryption. Security is provided by using an encryption technology like IPSec.
• PPTP - Point to Point Tunneling Protocol. Creates an encrypted tunnel through an untrusted network.

Feature	PPTP	L2TP
Built-in encryption	*Yes*	*No*
Header compression	*No*	*Yes*
Transmits over IP-based internetwork	*Yes*	*Yes*
Transmits over UDP, Frame Relay, X.25 or ATM	*No*	*Yes*
Tunnel authentication	*No*	*Yes*

Network Protocols and Services

Protocols
A protocol is a set of rules and conventions for sending information over a network. Windows 2000 relies on TCP/IP for logon, file and print services, replication of information between domain controllers, and other common functions. Primary network protocols that Windows 2000 supports include:

• AppleTalk.
• Asynchronous Transfer Mode (ATM)
• Data Link Control (DLC)
• Infrared Data Association (IrDA)
• Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX)
• NetBIOS Enhanced User Interface (NetBEUI)

TCP/IP protocol
• Can be used to connect dissimilar systems.
• Installed by default in Windows 2000.
• IP addresses can be entered manually or provided automatically by a DHCP server.
• It is routable and works over most network topologies.
• TCP/IP protocol is required for communicating with UNIX hosts.
• Uses Microsoft Windows Sockets interface.

Configuring DHCP to Allow Dynamic Updates
You must configure the DHCP server to perform dynamic updates. To do so, on the DNS tab of the Properties dialog box for a DHCP server, select Automatically Update DHCP Client Information In DNS. You must also specify; Update DNS Only If DHCP Client Requests, or Always Update DNS. Additional options include Discard Forward Lookups When Lease Expires, and Enable Updates For DNS Client That Do Not Support Dynamic Update.

Automatic Private IP Addressing
When "Obtain an IP Address Automatically" is enabled, but the client cannot obtain an IP address, Automatic Private IP addressing takes over.

- If no other computer responds to the address, the first system assigns this address to itself.
- IP address is generated in the form of 169.254.x.y (x.y is the computer's identifier) and a 16-bit subnet mask (255.255.0.0).
- The 169.254.0.0 - 169.254.255.255 range has been set aside for this purpose by the Internet Assigned Numbers Authority.
- The computer broadcasts this address to its local subnet.
- When using the Auto Private IP, it can only communicate with other computers on the same subnet that also use the 169.254.x.y range with a 16-bit mask.

Services for UNIX 2.0
- FTP support has been added to Windows Explorer and to Internet Explorer 5.0 allowing users to browse FTP directories as if they were a local resource.
- Install SNMP for Network Management (HP, OpenView, Tivoli and SMS).
- Print Services for UNIX allows connectivity to UNIX controlled Printers (LPR).
- Simple TCP/IP Services provides Echo, Quote of Day, Discard, Daytime and Character Generator.
- UNIX uses NFS (Network File System).
- Windows 2000 uses CIFS (Common Internet File System) which is an enhanced version of the SMB (Server Message Block) protocol.

Client for NFS
- Installs a full Network File System (NFS) client that integrates with Windows Explorer.
- NFS shares can be accessed using standard NFS syntax (servername:/pathname) or standard UNC syntax (\\servername\pathname)
- Places a second Telnet client on your system that uses NTLM authentication instead of clear text.
- Users can browse and map drives to NFS volumes and access NFS resources through My Network Places. Microsoft recommends this over installing Samba (SMB file services for Windows clients) on your UNIX server.

Troubleshooting
- Common TCP/IP problems are caused by incorrect subnet masks and gateways.
- Check DNS settings if an IP address works but a hostname won't.
- The Ping command tests connections and verifies configurations.
- The Tracert command checks a route to a remote system.
- Use IPConfig and IPConfig /all to display current TCP/IP configuration.
- Use NetStat to display statistics and connections for TCP/IP protocol.
- Use NBTStat to display statistics for connections using NetBIOS over TCP/IP.

NWLink (IPX/SPX) and NetWare Interoperability

- Gateway Services for NetWare can be implemented on your NT Server to provide an MS client system to access your NetWare server by using the NT Server as a gateway. Frame types for the NWLink protocol must match the computer that the NT system is trying to connect with. Mismatching frame types will cause connectivity problems between the two systems.
- NetWare 3 servers uses Bindery Emulation (Preferred Server in CSNW). NetWare 4.x and higher servers use NDS (Default Tree and Context.)
- NWLink is used by NT to allow NetWare systems to access its resources.
- There are two ways to change a password on a NetWare server - SETPASS.EXE and the Change Password option (from the CTRL-ALT-DEL dialog box). The Change Password option is only available to NetWare 4.x and higher servers using NDS.
- To allow file and print sharing between NT and a NetWare server, CSNW (Client Service for NetWare) must be installed on the NT system. In a NetWare 5 environment, the Microsoft client does not support connection to a NetWare Server over TCP/IP. You will have to use IPX/SPX or install the Novell NetWare client.
- When NWLink is set to auto-detect the frame type, it will only detect one type and will go in this order: 802.2, 802.3, ETHERNET II and 802.5 (Token Ring).

Other protocols

- AppleTalk must be installed to allow Windows 2000 Professional to communicate with Apple printers. File and Print Services for Macintosh allows Apple Clients to use resources on a Microsoft Network.
- DLC is a special-purpose, non-routable protocol used by Windows 2000 to talk with IBM mainframes, AS400s and Hewlett Packard printers.
- NetBEUI is used solely by Microsoft operating systems and is non-routable.

Remote Access Services (RAS)

Authentication protocols

- CHAP - Challenge Handshake Authentication Protocol - encrypts user names and passwords, but not session data. Works with non-Microsoft clients.
- EAP - Extensible Authentication Protocol. Allows for an arbitrary authentication mechanism to validate a dial-in connection. Uses generic token cards, MD5-CHAP and TLS.
- EAP-TLS - Transport Level Security. Primarily used for digital certificates and smart cards.
- MD5-CHAP - Message Digest 5 Challenge Handshake Authentication Protocol. Encrypts usernames and passwords with an MD5 algorithm.
- MS-CHAP (V1 and 2) - Microsoft Challenge Handshake Authentication Protocol. Encrypts entire session, not just username and password. V2 is supported in Windows 2000 and NT 4.0 and Win 95/98 (with DUN 1.3 upgrade) for VPN connections. MS-CHAP cannot be used with non-Microsoft clients.

- PAP - Password Authentication Protocol. Sends username and password in clear text.
- RADIUS - Remote Authentication Dial-in User Service. Provides authentication and accounting services for distributed dial-up networking.
- SPAP - Shiva Password Authentication Protocol. Used by Shiva LAN Rover clients. Encrypts password, but not data.

Dial-up Networking

- Add new connections by using the Make New Connection wizard.
- Dial-up networking entries can be created for modem connections, LAN connections, direct cable connections and Infrared connections.
- PPP is generally preferred because it supports multiple protocols, encryption, and dynamic assignment of IP addresses. SLIP is an older protocol that only supports TCP/IP and is used for dialing into legacy UNIX systems.

Remote Access Policies

- A static IP can be assigned to a user when their connection is made.
- Applying static routes allows an admin to define a series of static IP routes that are added to the routing table of the RRAS server (used for demand-dial routing between RRAS servers).
- Callback options let you specify, no callback, set by caller, and always callback to. The last option provides the greatest level of security. Letting the user specify the callback number provides little in the way of security but allows users such as a travelling sales force with laptops to avoid long-distance charges by having the RRAS server call them back.
- Caller ID verification requires specialized answering equipment and a driver that passes Caller ID info to RRAS. If Caller ID is configured for a user but you do not have the proper equipment/drivers installed, the user is denied access.
- Control access through Remote Access Policy is not available on domain controllers in mixed-mode. While connections are initially accepted, they must still meet policy requirements or be disconnected.
- Default remote access policy denies all connection attempts unless user account is set to Allow. In Native mode, every account is set to Control access through Remote Access Policy. If this is changed to Grant remote access permission all connections are accepted.
- On a stand-alone server, policies are configured through Local Users and Groups, Dial-in, Properties. On an AD-based server, they are configured through Active Directory Users and Computers, Dial-in, Properties.
- Remote Access policies are stored on the server, not in Active Directory.
- The three components of a remote access policy are its conditions, permissions and profile:

Component	Feature
Conditions	*List of parameters (time of day, user groups, IP addresses or Caller Ids) that are matched to the parameters of the client connecting to the server. The first policy that matches the parameters of the inbound connection is processed for access permissions and configuration.*
Profile	*Settings (authentication and encryption protocols) which are applied to the connection. If connection settings do not match the user's dial-in settings, the connection is denied.*
Permissions	*Connections are allowed based on a combination of the dial-in properties of a user's account and remote access policies. The permission setting on the remote access policy works with the user's dial-in permissions in Active Directory providing a wide range of flexibility when assigning remote access permissions.*

Remote Access Profiles
Encryption used to specify the types of encryption that are allowed /required /prohibited.

Feature	Description
Dial-in constraints	*Idle time before disconnect, maximum session time, days and times allowed, phone numbers, and media types.*
IP	*Used to configure TCP/IP packet filtering.*
Multilink	*Configure to disconnect a line if bandwidth falls below the preset threshold. Can be set to require BAP.*
Authentication	*Define authentication protocols required for connections using this policy.*

Terminal Services

Terminal Services running on a Windows 2000 Server enables all client application execution, data processing, and data storage to occur on the server. It provides remote access to a server desktop through terminal emulation software. The terminal emulation software can run on a number of client hardware devices, such as a personal computer, Windows CE-based Handheld PC (H/PC), or terminal.

Installing Terminal Services
TS Services include:

Feature	Description
TS Manager	*Used to manage and monitor sessions and processes on the server running TS.*
TS Licensing	*Manages Client Access Licenses.*
TS Configuration	*Used to manage TS protocol and server configuration.*
TS Client	*Creator Creates floppies for installing TS Client.*

- Added through Control Panel, Add/Remove Programs, Windows Components.
- TS can be enabled during an unattended installation by setting TSEnable=On in the [Components] section of the answer file. If the ApplicationServer key is not added then TS is installed in Remote Administration mode.
- TS uses RDP or RDP-TCP (Remote Desktop Protocol over TCP/IP). This is a presentation protocol and it sends input from the terminal to the server and returns video from the server back to the terminal. It has been optimized for low-speed (modem) connections and is suitable for deployment in a RAS dial-up environment.

Remote Server Administration Using TS
- Do not use for tasks that require reboots.
- If another Administrator is in session on the same server you are working on, you may overwrite each other's work. Use the QUSER command to see if other Administrators are in session.
- Remote Administration Mode allows a maximum of 2 concurrent connections to be made per server by an Administrator. Memory and CPU utilization settings remain unaffected and application compatibility settings are completely disabled.
- Remote Administration Mode allows Administrators have complete access to the remote system to perform tasks such as software installation, and administrative functions, etc.
- There are no licensing requirements for using the Remote Administration Mode.

Configuring TS for Application Sharing
- A Temp folder is created for each user by default. Use the FLATTEMP.EXE tool or the Terminal Services Configuration Tool to change the location of the temporary folders or disable them and force all users to share one Temp folder (flattemp /disable).
- Automatic Printer redirection is supported for all 32-bit Windows clients. TS will detect printers attached locally to the client and create corresponding print queues in the user's session. When a user disconnects print queues and any print jobs are terminated. Printers must be manually redirected for 16-bit Windows clients and Windows based terminals.
- By default, users will be prompted for a password unless it is changed in the properties for RDP-TCP.
- Remove the default Home Directories created by Windows 2000 for each user and create TS specific network Home Directories on a file server. All application specific files (e.g., .INI) are written to these directories.

- Sessions will disconnect when the connection is broken but will continue executing a user's processes by default. To prevent system resources from being taken up by these processes, set your sessions to reset on broken connections.
- TS cannot be clustered, but it can be load-balanced using Network Load Balancing. This causes a group of servers to appear as a single virtual IP address. Alternately you can use round-robin DNS resolution to load balance your TS servers.
- Users can be assigned a specific Terminal Services profile. If one is not available TS will then try to load a user's Roaming Profile. If the two previous are not available TS will load the standard Windows 2000 Profile.

Configuring Applications for Use with TS
- Some applications may require special installation or execution scripts to modify the application's performance in a multi-user environment.
- TS does not recognize devices that connect to parallel or serial ports (multimedia applications, streaming applications, etc.).
- Use Add/Remove Programs in Control Panel to install applications. If you are installing an application directly, put TS into install mode by typing change user /install at a command prompt. Typing change user /execute turns off install mode.

Security

Security Configuration
The Security Configuration and Analysis snap-in can be used to directly configure local system security. You can import security templates created with the Security Templates snap-in, and apply these templates to the group policy object (GPO) for the local computer.
Security Templates Snap-In
A security template is a physical representation of a security configuration; it is a file where a group of security settings may be stored. Windows 2000 includes a set of security templates, each based on the role of a computer. The templates range from security settings for low security domain clients to highly secure domain controllers. They can be used as provided, modified, or serve as a basis for creating custom security templates.

Security Configuration Tool Set
- The Security Configuration and Analysis snap-in is used to troubleshoot security in Windows 2000.
- The security database is compared to an incremental template such as HISECSV.INF and the results displayed. The log of the analysis will be placed in %systemroot%\security\logs\mysecure.log
- The text-based version is run from the command line using SECEDIT.EXE.

Encrypting File System (EFS)

- Compressed files can't be encrypted and vice versa.
- Cut and paste to move files into an encrypted folder - if you drag and drop files, the files are not automatically encrypted in the new folder.
- Default encryption is 56-bit. North Americans can upgrade to 128-bit encryption.
- Designated Recovery Agents can recover encrypted data for the domain using AD and Certificate Server.
- EFS resides in the Windows OS kernel and uses the non-paged memory pool to store file encryption keys.
- Encrypted files are decrypted if you copy or move them to a FAT volume.
- Encrypted files can be backed up using the Backup Utility, but will retain their encrypted state as access permissions are preserved.
- Encryption is transparent to the user.
- If the owner has lost his private key, an appointed recovery system agent can open the file using his/her key instead.
- Only works on Windows 2000 NTFS partitions (NTFS v5).
- The EFSINFORMATION.EXE utility in the Win2000 Resource Kit allows an administrator to determine information about encrypted files.
- There can be more than one recovery agent, but at least one public recovery key must be present on the system when the file is encrypted.
- Use the Cipher command to work with encrypted files from the command line.
- Uses public-key encryption. Keys that are used to encrypt the file are encrypted by using a public key from the user's certificate. The list of encrypted file-encryption keys is kept with the encrypted file and is unique to it. When decrypting the file encryption keys, the file owner provides a private key which only he has.
- You can't share encrypted files.

Policies in a W2K Environment

Local and System Policy

System Policies are a collection of user environment settings that are enforced by the operating system and cannot be modified by the user. User profiles refer to the environment settings that users can change.

System Policy Editor (POLEDIT.EXE) - Windows NT 4, Windows 95 and Windows 98 all use the System Policy Editor (POLEDIT.EXE) to specify user and computer configuration that is stored in the registry.

- Are considered "undesirably persistent" as they are not removed when the policy ends.
- Not secure. Settings can be changed by a user with the Registry Editor (regedit.exe). Settings are imported/exported using .ADM templates.
- Windows 2000 comes with SYSTEM.ADM (system settings), INETRES.ADM (Internet Explorer settings) and CONF.ADM (NetMeeting settings).

Group Policy snap-in (GPEDIT.MSC)

Exclusive to Windows 2000 and supercedes the System Policy Editor. Uses Incremental Security Templates.

- More flexible than System Policies as they can be filtered using Active Directory.

• Settings are imported/exported using .INF files. The Group Policy snap-in can be focused on a local or remote system.
• Settings can be stored locally or in AD. Are secure and can be changed only by Administrators.
• Should only be applied to Windows 2000 systems that have been clean installed onto an NTFS partition. NTFS computers that have been upgraded from NT 4.0 or earlier, only the Basic security templates can be applied.

Auditing

Auditing in Microsoft Windows 2000 is the process of tracking both user activities and Windows 2000 events. You can specify that Windows 2000 writes a record of an event to the security log. The security log maintains a record of valid and invalid logon attempts and events related to creating, opening, or deleting files or other objects. Auditing can be enabled by clicking Start, Program, Administrative Tools, Local Security Policy. In the Local Security Settings window, double-click Local Policies and then click Audit Policy. Highlight the event you want to audit and on the Action menu, click Security. Set the properties for each object as desired then restart computer for new policies to take effect.

Auditable Events

Event	**Description**
System	*A user restarted or shut down the computer, or an event occurred that affects Windows 2000 security or the security log.*
Process tracking	*A program performed an action.*
Privilege use	*A user exercised a right, such as changing the system time.*
Object access	*A user gained access to a file, folder, or printer. Configure specific files, folders, or printers for auditing. Directory service access is auditing a user's access to specific Active Directory objects. Object access is auditing a user's access to files, folders, and printers.*
Logon events	*A user logged on or logged off, or a user made or canceled a network connection to the computer.*
Policy change	*A change was made to the user security options, user rights, or audit policies.*
Account logon events	*A domain controller received a request to validate a user account.*
Account management	*An administrator created, changed, or deleted a user account or group. A user account was renamed, disabled, or enabled, or a password was set or changed.*
Directory service access	*A user gained access to an Active Directory object. Configure specific Active Directory objects for auditing to log this type of event.*

Local accounts

- Built in user accounts are Administrator and Guest.
- Creating and duplicating accounts requires username and password. Disabling an account is typically used when someone else will take the user's place or when the user might return.
- Delete an account only when absolutely necessary for space or organization purposes.
- Domain user accounts reside in AD on domain controllers and can access all resources on a network that they have been accorded privileges for.
- Resides only on the computer where the account was created in its local security database. If computer is part of a peer-to-peer workgroup, accounts for that user will have to be created on each additional machine that they wish to log onto locally. Local accounts cannot access Windows 2000 domain resources and should not be created on computers that are part of a domain.
- User accounts are added and configured through the Computer Management snap-in.
- User logon names are not case sensitive. You can use alphanumeric combinations to increase security, if desired.
- When copying a user account, the new user will stay in the same groups that the old user was a member of. The user will keep all group rights that were granted.through groups, but lose all individual rights that were granted specifically for that user.

Account Policy

Accessed through Administrative Tools, Local Security Policy, Account Policies. There are two choices, Password Policy and Account Lockout Policy.