brainbuzz.com™
Cramsession

Cramsession™ for Microsoft Windows 2000 Server

This study guide will help you to prepare for Microsoft exam 70-215, Installing, Configuring, and Administering Microsoft Windows 2000 Server. Exam topics include Installing Win2K Server, Resource Access, Hardware Devices & Drivers, Storage Use, Network Connections, and Security.

Check for the newest version of this Cramsession
http://cramsession.brainbuzz.com/checkversion.asp?V=2451991&FN=Microsoft/Win2kServer.pdf

Rate this Cramsession
http://cramsession.brainbuzz.com/cramreviews/reviewCram.asp?cert=Win2k+Server

Feedback Forum for this Cramsession/Exam
http://boards.brainbuzz.com/boards/vbt.asp?b=640

More Cramsession Resources:

Search for Related Jobs
http://jobs.brainbuzz.com/BrowseJobSearchRes.asp

CramChallenge - practice questions
http://www.cramsession.com/signup/default.asp#day

IT Resources & Tech Library
http://itresources.brainbuzz.com

Certification & IT Newsletters
http://www.cramsession.com/signup/

SkillDrill - skills assessment
http://skilldrill.brainbuzz.com

Discounts, Freebies & Product Info
http://www.cramsession.com/signup/prodinfo.asp

Contents:

Installing Windows 2000 Server: (KB#Q242955)

Requirements:

Component	Recommended Minimum	Suggested Configuration
CPU	Pentium 133	Pentium II or higher
Memory	128 MB*	256 MB or higher
Hard disk space	1 GB	2 GB or higher
Networking	NIC	NIC
Display	VGA	SVGA
CD-ROM	needed when not installing over the network	needed when not installing over the network
Keyboard and mouse	required	required
Sound card	not required	required for visually impaired users needing narrative voice to guide installation

*Some MS documentation says 64 MB is recommended for 5 users or less. Setup will abort if the machine has less than 64 MB. The MS site currently specs 128 MB as the minimum.

All hardware should appear on the Windows 2000 Hardware Compatibility List (HCL) (KB# Q142865)

Windows 2000 Server supports Symmetric Multi-processing with a maximum of four processors, and up to 4 GB of RAM. Advanced Server scales up to 8 processors and 8 GB of RAM. Windows 2000 DataCenter Server is only available in OEM configurations and supports up to 32 processors and 64 GB of RAM.

Servers install as Member Servers (standalone) by default. File, print and Web servers are usually installed as Member Servers to reduce the administrative overhead placed on the system by participating in Active Directory as a Domain Controller. Member Servers can access Active Directory information, but do not perform any AD related authentication or storage functions. To promote a machine to a Domain Controller, run **dcpromo**.

If Windows 2000 is being integrated into an existing Windows NT 4.0 domain structure, mixed mode must be used (installed by default). If Windows 2000 is being

installed into an infrastructure where all domain controllers will be running Windows 2000, then domain controllers should be switched to native mode to take advantage of Active Directory's full benefits. (KB# Q186153)

Attended installations

Setup has four stages

1. Setup Program (text mode)- preps hard drive for following stages of install and copies files needed for running Setup Wizard. Requires reboot.
2. Setup Wizard (graphical mode) - prompts for additional info such as product key, names, passwords, regional settings, etc.
3. Install Windows Networking - detects adapter cards, installs networking components (Client for MS Networks, File & Printer Sharing for MS Networks), and installs TCP/IP protocol by default (other protocols can be installed later). Choose to join a workgroup or domain at this point (must be connected to network and provide credentials to join a domain). After all choices are made components are configured, additional files are copied, and the system is rebooted.
4. Setup Completion - installs Start Menu items, register's components, saves configuration, removes temporary files and system rebooted one final time.

Installing from CD-ROM

- Setup disks are not required if your CD-ROM is bootable or you are upgrading a previous version of Windows.
- To make boot floppies, type **makeboot a:** in the \bootdisk directory of your W2K CD. Creates set of four 1.44 MB boot floppies. (KB# Q197063)
- If installing using a MS-DOS or Win95/98 boot floppy, run **winnt.exe** from the \i386 to begin Windows 2000 setup.
- Setup will not prompt the user to specify the name of an installation folder unless you are performing an unattended installation or using **winnt32** to perform a clean installation. (KB# Q222939)

Installing over a Network

- Create a distribution server which has a file share containing the contents of the /i386 directory from the Windows 2000 CD-ROM.
- 1 GB minimum plus 100 - 200 MB free hard drive space to hold temporary files during installation.
- Install a network client on the target computer or use a boot floppy that includes a network client (KB# Q142857). Run **winnt.exe** from the file share

on distribution server if installing a new operating system or **winnt32.exe** if upgrading a previous version of Windows.

- Clean installation is now possible with Windows 2000. NT 4 required a pre-existing FAT partition.

Command line switches for winnt.exe

Switch	Function
/a	Enables accessibility options
/e[:command]	Specifies a command that will be run at the end of Stage 4 of setup
/r[:folder]	Specifies optional folder to be installed. Folder is not removed with temporary files after installation
/rx[:folder	Specifies optional folder to be copied. Folder is deleted after installation
/s[:sourcepath]	Specifies source location of Windows 2000 files. Can either be a 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

Modifying Setup using winnt32.exe

Switch	Function
/checkupgradeonly	Checks system for compatibility with Windows 2000. Creates reports for upgrade installations.
/copydir:*folder_name*	Creates additional folder inside %systemroot% folder. Retained after setup.
/copysource:*folder_name*	Same as above except folder and its contents are deleted after installation completes
/cmd: *command_line*	Runs a command before the final phase of Setup
/cmdcons	This adds a Recovery Console option to the operating system selection screen
/debug[*level*] [:*file_name*]	Creates a debug log. 0=Sever errors only. 1=regular errors. 2=warnings. 3=all messages.
/m:*folder_name*	Forces Setup to look in specified folder for setup files first. If files are not present, Setup uses files from default location.
/makelocalsource	Forces Setup to copy all installation files to local hard drive so that they will be available during successive phases of setup if access to CD drive or network fails.

/nodownload	Used when upgrading from Win95/98. Forces copying of winnt32.exe and related files to local system to avoid installation problems associated with network congestion. (KB# Q244001)
/noreboot	Tells system not to reboot after first stage of installation.
/s:*source_path*	Specifies source path of installation files. Can be used to simultaneously copy files from multiple paths if desired (first path specified must be valid or setup will fail, though).
/syspart:*drive_letter*	Copies all Setup startup files to a hard disk and marks the drive as active. You can physically move the drive to another computer and have the computer move to Stage 2 of Setup automatically when it is started. Requires /tempdrive switch. (KB# Q234037 & Q241803)
/tempdrive:*drive_letter*	Setup uses the specified tempdrive to hold temporary setup files. Used when there are drive space concerns
/unattend: [number] [:*answer_file*]	Specifies answer file for unattended installations. [number] is the amount of time Windows waits at the boot menu before continuing.
/udf:id[,*udf_file*]	Establishes ID that Setup uses to specify how a UDF file modifies an answer file.

Unattended installations

- Unattended installations rely on an *answer file* to provide information to provide information during setup process that is usually provided through manual user input. (KB# Q183245)
- Answer files can be created manually using a text editor or by using the Setup Manager Wizard (SMW) (found in the Windows 2000 Resource Kit Deployment Tools).
- SMW allows for creation of a shared Distribution Folder and OEM Branding
- If you had a CD in drive D: and an unattended installation answer file named salesans.txt in C:\, you could start your install with this command: **D:\i386\winnt32 /s:d:\i386 /unattend:c:\salesans.txt** (KB# Q216258)
- To automatically promote a server to a Domain Controller during unattended setup, specify the following command to run after setup completes; **dcpromo /answer:<*answer_file*>**. The answer file is a text file containing only the [DCInstall] section. (KB# Q224390)
- There are five levels of user interaction during unattended installs:
    1. *Provide Defaults* - Administrator supplies default answers and user only has to accept defaults or make changes where necessary.
    2. *Fully Automated* - Mainly used for Win2000 Professional desktop installs. User just has to sit on their hands and watch.
    3. *Hide Pages* - Users can only interact with setup where Administrator did not provide default information. Display of all other dialogs is suppressed.

4. *Read Only* - Similar to above, but will display information to user without allowing interaction to pages where Administrator has provided default information.
5. *GUI Attended* - Only used for automating the second stage of setup. All other stages require manual input.

System preparation tool (SYSPREP.EXE): (KB# Q240126)

- Can be used to automate installations of Windows 2000 Server
- Removes the unique elements of a fully installed computer system so that it can be duplicated using imaging software such as Ghost or Drive Image Pro. Avoids the NT4 problem of duplicated SIDS , computer names etc. Installers can use sysprep to provide and answer file for "imaged" installations.
- Must be extracted from DEPLOY.CAB in the \support\tools folder on the Windows 2000 Professional CD-ROM.
- 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. This process can be automated by providing a script file. (KB# Q196667)
- Use 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.
- 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. (KB# Q238955)
- Available switches for sysprep.exe are: /quiet (runs without user interaction), /pnp (forces Setup to detect PnP devices), /reboot (restarts computer), and /nosidgen (will not regenerate SID on target computer).

Upgrading from a previous version: (KB# Q232039 & Q242859)

- Run **winnt32.exe** to upgrade from a previous version of Windows. (KB# Q199349)
- Windows 2000 Server will upgrade and preserve settings from the following operating systems: Windows NT 3.51 and 4.0 Server, Windows NT 4.0 Terminal Server, and Windows NT 4.0 Enterprise Edition.
- Upgrade paths do not exist for Windows NT 3.51 with Citrix or Microsoft BackOffice Small Business Server.
- Upgrade installations from a network file share are not supported in Windows 2000 (this *can* be done, but only by using SMS). You must either do a CD-based upgrade or perform a clean installation of Windows 2000 and re-install needed applications.

- Because of registry and program differences between Windows NT and 2000, upgrade packs (or migration DLLs) might be needed. Setup checks for these in the \i386\WinNTmig folder on the Windows 2000 CD-ROM or in a user specified location. (KB# Q231418)
- Run **winnt32 /checkupgradeonly** to check for compatible hardware and software. Generates a report indicating which system components are Windows 2000 compatible. Same as running the **chkupgrd.exe** utility from Microsoft's site.

Troubleshooting Failed Installations

Common errors

Problem	Possible fix
Cannot contact domain controller	*Verify that network cable is properly connected.* Verify that server(s) running DNS and a domain controller are both on-line. Make sure your network settings are correct (IP address, gateway, etc.). Verify that your credentials and domain name are entered correctly.
Error loading operating system	Caused when a drive is formatted with NTFS during setup but the disk geometry is reported incorrectly. Try a smaller partition (less than 4 GB) or a FAT32 partition instead.
Failure of dependency service to start	Make sure you installed the correct protocol and network adapter in the Network Settings dialog box in the Windows 2000 Setup Wizard. Also check to make sure your network settings are correct.
Insufficient disk space	Create a new partition using existing free space on the hard disk, delete or create partitions as needed or reformat an existing partition to free up space.
Media errors	Maybe the CD-ROM you are installing from is dirty or damaged. Try using a different CD or trying the affected CD in a different machine.
Nonsupported CD drive	Swap out the drive for a supported drive or try a network install instead. (KB# Q228852)

Log files created during Setup

Logfile name	Description
setupact.log	Action Log - records setup actions in a chronological order. Includes copied files and registry entries as well as entries made to the error log.
setuperr.log	Error Log - records all errors that occur during setup and includes severity of error. Log viewer shows error log at end of setup if errors occur.
comsetup.log	Used for Optional Component manager and COM+ components.
setupapi.log	Logs entries each time a line from an .INF file is implemented. Indicates failures in .INF file implementations.
netsetup.log	Records activity for joining a domain or workgroup.
mmdet.log	Records detection of multimedia devices, their port ranges, etc.

Install, Configure and Troubleshoot Access to Resources

Install and Configure Network Services

TCP/IP Server Utilities

- Telnet server - Windows 2000 includes a telnet server service (**net start tlntsvr**) which is limited to a command line text interface. Set security on your telnet server by running the admin tool, **tlntadmn**. (KB# Q225233)
- Web Server - Internet Information Services 5, Microsoft's full-blown Web server. Now supports Internet Printing and Web Distributed Authoring and Versioning (WebDAV). Can be managed using IIS snap-in.
- FTP Server - stripped version of Internet Information Server 5 (IIS5) FTP server. Also administered using the IIS snap-in.
- FrontPage 2000 Server Extensions - extends the functionality of the Web server by adding pre-compiled scripts and programs that allow Web site authors to implement advanced features in their pages without requiring much in the way of programming knowledge.
- SMTP Server - basic mail server included with IIS. Used for sending mail in conjunction with FrontPage 2000 Server Extensions and Active Directory replication. Does not support IMAP4, POP3, etc. If you need advanced mail handling, consider using Exchange Server.

TCP/IP Client Utilities

- Telnet client - Can be used to open a text based console on UNIX, Linux and Windows 2000 systems (run **telnet *servername***)
- FTP client - Command line based - simple and powerful (run **ftp *servername***)
- Internet Explorer 5 - Microsoft's powerful and thoroughly integrated Web browser (see IE5 Cramsession for details)
- Outlook Express 5 - SMTP, POP3, IMAP4, NNTP, HTTP, and LDAP complaint E-mail package.

Install and Configure Local and Network Printers

- Windows 2000 Server supports the following printer ports: Line Printer (LPT), COM, USB, IEEE 1394 (FireWire), and network attached devices.
- Print services can only be provided for Windows, UNIX, Apple, and Novell clients. (KB# Q124734)
- Windows 2000 automatically downloads the printer drivers for clients running Win2000, WinNT 4, WinNT 3.51 and Windows 95/98. (KB# Q142667)
- Internet Printing is a new feature in Windows 2000. You have the option of entering 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://*servername*/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. Priority ranges from 1, the lowest (default) to 99, the highest.
- Enabling "Availability" option allows Administrator to specify the hours the printer is available.
- Use Separator Pages to separate print jobs at a shared printer. A template for the separator page can be created and saved in the %systemroot%\system32 directory with a .SEP file extension. (KB# Q102712)
- You can select Restart in the printer's menu to reprint a document. This is useful when a document is printing and the printer jams. Resume can be selected to start printing where you left off.
- You can change the directory containing the print spooler in the advanced server properties for the printer. (KB# Q123747)
- 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. (KB# Q240683)
- Use the **fixprnsv.exe** command-line utility to resolve printer incompatibility issues. (KB# Q247196)

Services for UNIX 2.0:

Miscellaneous

- TCP/IP protocol is required for communicating with UNIX hosts
- Windows 2000 uses CIFS (Common Internet File System) which is an enhanced version of the SMB (Server Message Block) protocol
- UNIX uses NFS (Network File System)
- 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..

Client for NFS

- Installs a full Network File System (NFS) client that integrates with Windows Explorer. Available for both W2K Professional and Server.
- Places a second, more powerful Telnet client on your system in the %windir%\system32\%sfudir% directory. This new client has been optimized for Windows NT Telnet server and can use NTLM authentication instead of clear text. (KB# Q250879)
- 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.
- NFS shares can be accessed using standard NFS syntax (*servername:/pathname*) or standard UNC syntax (*servername**pathname*)
- If users' UNIX username/password differ from Windows username/password, click "Connect Using A Different User Name" option and provide new credentials.
- The following popular UNIX utilities are installed along with the Client for NFS (not a complete list):

Utility	Description
grep	Searches files for patterns and displays results containing that pattern
ps	Lists processes and their status
sed	Copies files named to a standard output; edits according to a script of commands
sh	Invokes the Korn shell
tar	Used to create tape archives or add/extract files from archives
vi	Invokes vi text editor

The **nfsadmin** (http://www.microsoft.com/technet/win2000/sfu.asp) command-line utility is used for configuration and administration of the Client for NFS. Its options are:

Option	Description
fileaccess	UNIX file permissions for reading, writing, and executing.
mapsvr	Computer name of the mapping server
mtype	Mount type, HARD or SOFT
perf	Method for determining performance parameters (MANUAL or DEFAULT)
preferTCP	Indicates whether to use TCP (YES or NO)
retry	Number of retries for a soft mount - default value is 5
rsize	Size of read buffer in KB
timeout	Timeout in seconds for an RPC call
wsize	Size of write buffer in KB

Server for NFS

- Allows NFS clients (think UNIX/Linux here) to access files on a Windows 2000 Professional or Server computer
- Integrates with Server for PCNFS or Server for NIS to provide user authentication
- Managed using the UNIX Admin Snap-in (**sfumgmt.msc**)

Gateway for NFS

- Allows non-NFS Windows clients to access NFS resources by connecting thru an NFS-enabled Windows Server to NFS resources.
- Acts as a gateway/translator between the NFS protocol used by UNIX/Linux and the CIFS protocol used by Windows 2000.

Server for PCNFS

- Can be installed on either W2K Professional or Server
- Provides authentication services for NFS clients (UNIX) needing to access NFS files. Works with the mapping server.

Server for NIS

- Must be installed on a Windows 2000 Server that is configured as a Domain Controller.
- Allows server to act as the NIS master for a particular UNIX domain.
- Can authenticate requests for NFS shares.

NWLink (IPX/SPX) and NetWare Interoperability:

- NWLink (MS's version of the IPX/SPX protocol) is the protocol used by NT to allow Netware systems to access its resources. (KB# Q203051)
- NWLink is all that you need to run in order to allow an NT system to run client/server applications from a NetWare server.
- To allow file and print sharing between NT and a NetWare server, CSNW (Client Services 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. (KB# Q235225)
- W2K Setup upgrades all Intel x86 based computers running version 4.7 or earlier of a Novell client to version 4.51.
- Gateway Services for NetWare can be implemented on your NT Server to provide a MS client system to access your NetWare server by using the NT Server as a gateway. (KB# Q121394)
- Frame types for the NWLink protocol must match the computer that the NT system is trying to connect with. Unmatching frame types will cause connectivity problems between the two systems.
- When NWLink is set to autodetect 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).

- Netware 3 servers uses Bindery Emulation (Preferred Server in CSNW). Netware 4.x and higher servers use NDS (Default Tree and Context.)
- 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.

File and Print Services for Macintosh: (KB# Q99765)

- Installed through Add/Remove Programs > Windows Components > Other Network File & Print Services > Details > File Services for Macintosh and/or Print Server for Macintosh.
- Installs the Appletalk protocol and Appletalk service.
- Mac readable shares can be created on an NTFS or CDFS file system. They cannot be created on FAT or FAT32 based volumes.
- To create Mac shares run **compmgmt.msc** and create a share as you normally would. Make the share available for a Macintosh client and assign it a Macintosh share name. Permissions are applied to Mac shares as they are to any Windows file share. Macs running System 7.5 or prior cannot see volumes larger than 2 GB.
- All printers on the NT Server should be visible and usable to connected Mac clients as translation is provided via a Postscript driver on the NT server. Mac clients will not need to install any special drivers.

Monitor, configure, troubleshoot, and control access to files, folders and shared folders

Choosing a File System

- NTFS provides optimum security and reliability through its ability to lock down individual files and folders on a user by user basis. Advanced features such as disk compression, disk quotas and encryption make it the file system recommended by MS. (KB# Q244600)
- FAT and FAT32 are only used for dual-booting between Windows 2000 and another operating system (like DOS 6.22, Win 3.1 or Win 95/98). (KB# Q184006)
- Existing NT 4.0 NTFS system partition will be upgraded to Windows 2000 NTFS automatically. If you wish to dual-boot between NT4.0 and 2000 you must first install Service Pack 4 on the NT4.0 machine. This will allow it to read the upgraded NTFS partition, but advanced features such as EFS and Disk Quotas will be disabled. (KB# Q197056 & Q184299)

- Use **convert.exe** to convert a FAT or FAT32 file system to NTFS. NTFS partitions cannot be converted to FAT or FAT32 - the partition must be deleted and recreated as FAT or FAT32 (KB# Q156560 & Q214579)
- You cannot convert a FAT partition to FAT32 using **convert.exe**. (KB# Q197627)

Distributed File System (DFS): (KB# Q241452)

If you are an NT4 administrator:

- DFS (administered via the dfsgui.msc snap-in) was an add on utility in NT4 with limited usefulness because it provided no fault-tolerance. In W2K it is fault-tolerant and more...
- There is no Directory Replication in Windows 2000 - this feature has been absorbed into DFS and is now called File Replication Service (FRS) which will replicate files between servers and is much easier to administer than the former. (KB# Q220140 & Q220938)
- NT4 stored logon scripts in the NETLOGON folder. In W2K they, and other items to be replicated, 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 - this has not changed.
- 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.

Standalone DFS:

- Created using Administrative Tools > Distributed File System and choosing "Create a standalone DFS root"
- Only single-level hierarchies are allowed when using standalone DFS.
- Standalone DFS is **not** fault-tolerant.

Domain-based DFS: (KB# Q232613)

- Created using Administrative Tools > Distributed File System and choosing "Create a domain DFS root"
- Directories from multiple different computers can be shown as one single file and folder hierarchy.
- The only limit on how many levels deep a domain-based DFS can go is the 260 character limit on a pathname in Windows.
- A domain Dfs root must be hosted on either a member server or a domain controller in the domain. Active Directory stores each DFS tree topology and

replicates it to every participating DFS root server. Changes to a DFS tree are automatically synchronized through AD.
- 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.

Local security on files and folders

NTFS Security and Permissions (KB#S Q183090, Q244600)

Miscellaneous

- NTFS in Windows 2000 (version 5) features enhancements not found in Windows NT 4.0 version 4). Reparse Points, Encrypting File System (EFS), Disk Quotas, Volume Mount Points, SID Searching, Bulk ACL Checking, and Sparse File Support. (KB# Q183090)
- Volume Mount Points allow new volumes to be added to the file system without needing to assign a drive letter to it. Instead of mounting a CD-ROM as drive E:, it can be mounted and accessed under an existing drive (e.g., C:\CD-ROM). As Volume Mount Points are based on Reparse Points, they are only available under NTFS5 using *Dynamic Volumes*.
- NTFS4 stored ACLs on each file. With bulk ACL checking, NTFS5 uses unique ACLs only once even if ten objects share it. NTFS can also perform a volume wide scan for files using the owner's SID (SID Searching). Both functions require installation of the Indexing Service.
- 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.
- NTFS partitions can be defragmented in Windows 2000 (as can FAT and FAT32 partitions). Use Start > Programs > Accessories > System Tools > Disk Defragmenter.
- Local security access can be set on a NTFS volume.
- Files moved from an NTFS partition to a FAT partition do not retain their attributes or security descriptors, but will retain their long filenames.
- Permissions are cumulative, except for Deny, which overrides anything.
- File permissions override the permissions of its parent folder.
- Anytime a new file is created, the file will inherit permissions from the target folder.
- The **cacls.exe** utility is used to modify NTFS volume permissions. (KB# Q237701)

File attributes when copying / moving within a partition or between partitions

Copying within a partition	Creates a new file resembling the old file. Inherits the target folders permissions.
Moving within a partition	Does not create a new file. Simply updates directory pointers. File keeps its original permissions.
Moving across partitions	Creates a new file resembling the old file, and deletes the old file. Inherits the target folders permissions.

Copying and Moving Encrypted Files

- An encrypted file moved to a compressed folder loses its encryption attribute and inherits the compression attribute of the target folder. (KB# Q223093)
- An encrypted file moved to an unencrypted folder remains encrypted.
- An encrypted file moved to a FAT or FAT32 loses its encryption attribute as that it is only available in the NTFS5 file system.
- An unencrypted file moved to an encrypted folder inherits the attributes of its target folder and becomes encrypted.
- An encrypted folder cannot be shared. If an encrypted file is copied over the network, it is transmitted in unencrypted form. Security for network/Internet file transfers are provided by separate technologies such as IPSec.

Network security on files and folders

Permission	Level of Access
Read	Can read and execute files and folders, but cannot modify or delete anything through the share.
Change	Can read, execute, change and delete files and folders through the share.
Full Control	Can perform any and all functions on all files and folders through the share.

- Folders are shared using Administrative Tools > Computer Management > System Tools > Shared folders or can be shared from within My Computer or Windows Explorer by right-clicking on them and clicking the Sharing tab.
- When sharing folders be aware that assigning share names longer than 8 characters will render them unusable to older DOS and Windows clients.
- Folders residing on FAT, FAT32 and NTFS volumes can all be shared.
- Share level permissions only apply to accesses made to the shared object via a network connection. They do not apply to a user logged on at the local console.
- When folders on FAT and FAT32 volumes are shared, only the share level permissions apply. When folders on NTFS volumes are shared, the effective permission of the user will be the most restrictive of the two (e.g., a user with a Share level permission of Change and an NTFS permission of Read will only be able to read the file. A user with a Share level permission of Read and an NTFS permission of Full Control would not be able to take ownership of the file).

Using offline files: (KB# Q214738)

Offline files, which is supported only on Windows 2000 based clients, replaces My Briefcase and works a lot like Offline Browsing in IE5.

Share a folder and set its caching to make it available offline - three types of caching:

- ***manual caching for documents*** - default setting. Users must specify which docs they want available when working offline
- ***automatic caching for documents*** - all files opened by a user are cached on his local hard disk for offline use - older versions on users machine automatically replaced by newer versions from the file share when they exist
- ***automatic caching for programs*** -same as above, but for programs

When synchronizing, if you have edited an offline file and another user has also edited the same file you will be prompted to keep and rename your copy, overwrite your copy with the network version, or to overwrite the network version and lose the other user's changes (a wise SysAdmin will give only a few key people write access to this folder or everyone's work will get messed up).

Using Synchronization Manager, you can specify which items are synchronized, using which network connection and when synchronization occurs (at logon, logoff, and when computer is idle).

Monitor, configure, troubleshoot, and control access to Web sites:

Virtual Servers: (KB# Q165180)

- Multiple Web sites can be hosted on the same machine by using Virtual Servers. There are three methods for setting up virtual servers:
    - Each virtual server must have its own IP address (most common method). Multiple IPs are bound to the server's NIC and each virtual server is assigned its own IP address
    - 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. (KB# Q190008)
    - Each virtual server can have the same IP address but a different port number (least commonly used)
- There can only be one home directory per virtual server.

Virtual Directories: (KB# Q172138)

- Virtual directories are referenced by alias names.
- An alias must be created for the directory. (e.g., d:\research becomes http://*servername*/research/)
- Do not put spaces in names of virtual directories, older browsers cannot handle them.
- Virtual directories can be mapped 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.
- Remember to specify the IP address of a virtual directory. If this is not done, the virtual directory will be seen by all virtual servers.
- A common scripts directory that is not assigned to the IP of a virtual server can handle scripts for all virtual servers.

Securing access to files and folders configured for Web Services

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

Authentication methods

- *Allow anonymous* - any visitor can access your site. Account used for anonymous access must be granted the right to log on locally.
- *Basic authentication* - username and password are sent in clear text. Not very secure.
- *Integrated Windows authentication* - was called "Windows NT Challenge/Response" in IIS4, but works the same way. Uses NTLM authentication in combination with local user database or Active Directory. Works with IE3 and up.
- *Digest authentication* - transmits a hash value over the Internet instead of a password. Passwords must be stored in clear text in Active Directory and client machines must be using IE5 or higher for digest authentication to work. (KB# Q222028)
- *SSL Client Certificate* - Certificate installed on the client system is used for authentication verification.

Configure and Troubleshoot Hardware Devices and Drivers

Miscellaneous

- Windows 2000 now fully supports Plug and Play. (KB# Q133159)
- Use the "System Information" snap-in to *view* configuration information about your computer (or create a custom console focused on another computer - powerful tool!!). This snap-in consists of these categories: System Summary, Hardware Resources, Components, Software Environment and IE5.
- "Hardware Resources" under System Information allows you to view Conflicts/Sharing, DMAs, IRQs, Forced Hardware, I/O, IRQs and Memory.
- Hardware is added and removed using the "Add/Remove Hardware" applet in the Control Panel (can also be accessed from Control Panel > System > Hardware > Hardware Wizard).
- All currently installed hardware is managed through the "Device Manager" snap-in.
- To troubleshoot a device using Device Manager, click the "Troubleshoot" button on the General tab.

Disk devices

- Managed through "Computer Management" under Control Panel > Administrative tools or by creating a custom console and adding the "Disk Management" snap-in. Choosing the "Computer Management" snap-in for

your custom console gives you the following tools: Disk Management, Disk Defragmenter, Logical Drives and Removable Storage. There is a separate snap-in for each of these tools except for Logical Drives.

- Using Disk Management, you can create, delete, and format partitions as FAT, FAT32 and NTFS. Can also be used to change volume labels, reassign drive letters, check drives for errors and backup drives.
- Defragment drives by using "Disk Defragmenter" under "Computer Management" or add the "Disk Defragmenter" snap-in to your own custom console. (KB# Q227463)
- Removable media are managed through the "Removable Media" snap-in.

Display devices

- Desktop display properties (software settings) are managed through the Display applet in Control Panel.
- Display adapters are installed, removed and have their drivers updated through "Display Adapters" under the Device Manager.
- Monitors are installed, removed, and have their drivers updated through "Monitors" under the Device Manager.

Input and output (I/O) devices

- Keyboards are installed under "Keyboards" in Device Manager.
- Mice, graphics tablets and other pointing devices are installed under "Mice and other pointing devices" in Device Manager.
- Troubleshoot I/O resource conflicts using the "System Information" snap-in. Look under Hardware Resources > I/O for a list of memory ranges in use.

Managing/configuring multiple CPUs

- Adding a processor to your system to improve performance is called scaling. Typically done for CPU intensive applications such as CAD and graphics rendering.
- Windows 2000 Server supports a maximum of four CPUs. If you need more consider using Windows 2000 Advanced Server (up to 8 CPUs) or Datacenter Server (maximum of 32 CPUs).
- Windows 2000 supports Symmetric Multiprocessing (SMP). Processor affinity is also supported. Asymetric Multiprocessing (ASMP) is not supported.
- Upgrading to multiple CPUs might increase the load on other system resources.

- Update your Windows driver to convert your system from a single to multiple CPUs. This is done through Device Manager > Computer > Update Driver. (KB# Q234558)

Install and manage network adapters

- Adapters are installed using the Add/Remove Hardware applet in Control Panel
- Change the binding order of protocols and the Provider order using Advanced Settings under the Advanced menu of the Network and Dial-up Connections window (accessed by right-clicking on My Network Places icon)
- Each network adapter has an icon in Network and Dial-up connection. Right click on the icon to set its properties, install protocols, change addresses, etc.

Updating drivers

- Drivers are updated using Device Manager. Highlight the device, right-click and choose Properties. A properties dialog appears. Choose the Drivers tab and then the Update Driver... button.
- Microsoft recommends using Microsoft digitally signed drivers whenever possible. (KB# Q244617)
- The Driver.cab cabinet file on the Windows 2000 CD contains all of the drivers the OS ships with. Whenever a driver is updated, W2K looks here first (e.g., c:\winnt\Driver Cache\i386\Driver.cab). The location of this file is stored in a registry key and can be changed: HKLM\Software\Windows\CurrentVersion\Setup\DriverCachePath (KB# Q230644)
- The Driver Verifier is used to troubleshoot and isolate driver problems. It must be enabled through changing a Registry setting. The Driver Verifier Manager, **verifier.exe**, provides a command-line interface for working with Driver Verifier. (KB# Q244617)

Driver signing: (KB# Q224404)

Configuring Driver Signing (KB# Q236029)

- 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
- ***Warn***- Display a message before installing an unsigned file
- ***Block***- Prevent installation of unsigned files
- The *Apply Setting As System Default* checkbox is only accessible to Administrators

Using System File Checker (sfc.exe) (KB# Q222471)

- ***/scannow*** - scans all protected system files immediately
- ***/scanonce*** - scans all protected system files at next startup
- ***/scanboot***- scans all protected system files at every restart
- ***/cancel***- cancels all pending scans
- ***/quiet*** - replaces incorrect files without prompting
- ***/enable*** - sets Windows File Protection back to defaults
- ***/purgecache*** - purges file cache and forces immediate rescan
- ***/cachesize=x***- sets file cache size

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 c:\winnt\Sigverif.txt

Windows Report Tool (KB# Q188104)

- Used to gather information from your computer to assist support providers in troubleshooting issues. Reports are composed in Windows 98 and Windows 2000 and then uploaded to a server provided by the support provider using HTTP protocol.
- Reports are stored in a compressed .CAB format and include a Microsoft System Information (.NFO) file.
- The report generated by Windows Report Tool (**winrep.exe**) includes a snapshot of complete system software and hardware settings. Useful for diagnosing software and hardware resource conflicts.

Manage, Monitor, and Optimize System Performance, Reliability and Availability

Monitor and optimize usage of system resources

Performance Console: (KB# Q146005)

- Important objects are *cache* (file system cache used to buffer physical device data), *memory* (physical and virtual/paged memory on system), *physicaldisk* (monitors hard disk as a whole), *logicaldisk* (logical drives, stripe sets and spanned volumes), and *processor* (monitors CPU load)

- *Processor - % Processor Time* counter measure's time CPU spends executing a non-idle thread. If it is continually at or above 80%, CPU upgrade is recommended
- *Processor - Processor Queue Length* - more than 2 threads in queue indicates CPU is a bottleneck for system performance
- *Processor - % CPU DPC Time* (deferred procedure call) measures software interrupts.
- *Processor - % CPU Interrupts/Sec* measures hardware interrupts. If processor time exceeds 90% and interrupts/time exceeds 15%, check for a poorly written driver (bad drivers can generate excessive interrupts) or upgrade CPU.
- *Logical disk - Disk Queue Length* - If averaging more than 2, drive access is a bottleneck. Upgrade disk, hard drive controller, or implement stripe set
- *Physical disk - Disk Queue Length* - same as above
- *Physical disk - % Disk Time*- If above 90%, move data/pagefile to another drive or upgrade drive
- *Memory - Pages/sec* - more than 20 pages per second is a lot of paging - add more RAM
- *Memory - Commited bytes* - should be less than amount of RAM in computer
- *diskperf* command for activating disk counters has been modified in Windows 2000. Physical disk counters are now enabled by default, but you will have to type **diskperf -yv** at a command prompt to enable logical disk counters for logical drives or storage volumes. (KB# Q253251)

Performance Alerts and Logs: (KB# Q244640)

- *Alert logs* are like trace logs, but they only log an event, send a message or run a program when a user-defined threshold has been exceeded
- *Counter logs* record data from local/remote systems on hardware usage and system service activity
- *Trace logs* are event driven and record monitored data such as disk I/O or page faults
- By default, log files are stored in the \Perflogs folder in the system's boot partition
- Save logs in CSV (comma separated value) or TSV (tab separated value) format for import into programs like Excel
- CSV and TSV must be written all at once, they do not support logs that stop and start. Use Binary (.BLG) for logging that is written intermittently
- Logging is used to create a baseline for future reference

Manage processes

- NT schedules threads to run by using application priorities. Application threads are assigned priorities, and run in order according to their priority level, from highest (31) to lowest (0).
- Starting applications in realtime mode can adversely effect other system processes and may even slow down total system performance. Running in realtime requires administrator or power user rights and is not generally recommended.
- You can change the priority of a running application by running Task Manager > Processes, right clicking the process and selecting "Set Priority."

Level	Priority
4	Low
8	Normal
13	High
24	Realtime

Optimize disk performance

- Mirrored volumes and spanned volumes slow down system performance.
- Striping a disk set causes greatest performance increase. Striping with parity is fast, but not so fast as without parity.
- Page files are fastest when spread across several disks, but not the boot or system disks. (KB# Q197379)
- Defragmenting your hard disks regularly will improve read performance.

Manage and optimize availability of System State data and user data

System State data: (KB# Q240363)

- Is 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 services and Sysvol directory are included. For machines running Cluster

Service, resource registry checkpoints and quorum resource recovery log are included.

- On a domain controller, moving system state data to a separate volume from the system volume can increase performance.
- Can be backed up from the command line by typing:
  ntbackup systemstate /m normal /f d:\sysstate.bkf /j "System State Data Backup"
  Where /m=backup type (can be copy or normal), /f=filename and /j=job name.
- 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. (KB# Q241594 & Q216243)

Establishing Fault-tolerance (KB# Q113932)

- Disk mirroring requires a second drive to make a duplicate copy of the first drive. When both drives are on separate controllers, it is referred to as disk duplexing. (RAID level one).
- Disk mirroring can be used on system and boot partitions but it degrades server performance somewhat. (KB# Q141702)
- When a basic disk that is part of a mirror set is disconnected or fails, the status of the mirror set becomes Failed Redundancy. You will need another basic disk of the same size to repair the mirror set - you cannot use a dynamic disk. When you repair the set, Disk Management creates a new mirror on a separate basic disk and resynchronizes the new mirror set.
- To break a mirror set, right-click on the mirror set you wish to break and choose Break Mirror.
- Disk striping with parity provides fault-tolerance as there is a parity stripe block for each row across a hard disk. The parity and data information are always arranged so that they are on separate hard disks. Works with a minimum of three drives and a maximum of thirty-two. (RAID level five)
- Disk striping with parity cannot be used on the boot and system partitions unless it is provided separately from Windows by a specialized hardware controller.
- The Disk Management tool will allow you to continue using any Stripe sets on basic disks that existed on your system from NT4 prior to an upgrade to W2K, but it will not allow you to create any new ones, unless they are on dynamic volumes.

Recover System State data and user data using:

Emergency Repair Disk

- Windows NT 4 users - the RDISK utility is gone, ERDs are now made exclusively with the backup utility. It has been changed from a repair disk to a boot disk which lets you run repair tools on the CD (KB# Q216337)
- To make an ERD, run **ntbackup**, choose Emergency Repair Disk and insert a blank formatted floppy into the A: drive. You will also have the option to copy registry files to the repair directory - it is a good idea to do so (%systemroot%\repair\regback). Also use backup to copy these registry files to a tape or Zip disk. (KB# Q231777)
- ERD contains the following files: autoexec.nt, config.nt and setup.log

Windows Backup

- Windows 2000 Backup is launched through Start > Accessories > System Tools > Backup or by running **ntbackup** from the Start menu (KB# Q241007)
- 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.

Backup type	Description
Normal	All selected files and folders are backed up. Archive attribute is cleared if it exists (fast for restoring)
Copy	All selected files and folders are backed up. Archive attribute is not cleared (fast for restoring)
Incremental	Only selected files and folders that have their archive attribute set are backed up and then archive markers are cleared
Differential	Only selected files and folders that have their archive attribute set are backed up but archive attributes are not cleared
Daily	All selected files and folders that have changed throughout the day are backed up. Archive attributes are ignored during the backup and are not cleared afterwards

Running NTBackup from the command line

Argument	Description
backup	Indicates to NTBACKUP that you're performing a backup operation. Must be included.
systemstate	Specifies that all System State data should be backed up. Can only be used for backing up drives on the local computer.
bks file name	Name of the selection info file where the backup will be stored. Multiple backups can be referenced from the same file.
/j "job name"	Name of the backup job.
/p "pool name"	Tells NTBACKUP which media pool to copy backup files to.
/g "guid name"	Specifies name of the tape that will be overwritten or appended with this backup job. Don't use with /p
/t "tape name"	Specifies name of the tape that will be overwritten or appended with this backup job. Don't use with /p
/n "new tape name"	Used to name a tape. Don't use with /p
/f "file name"	Specifies the path and file name of the file to which the backup will be copied. Cannot be used with any switch for removable media /pt, /t, or /n
/d "description"	Description of backup file
/a	Appends the backup set to any data on the media. When backing up to tape, must be used with /g or /t to specify the tape. Don't use with /p
/m backuptype	Specifies what type of backup to perform; normal, copy, incremental, differential or daily.
/v:yes or no	Specifies whether backup should be verified or not.
r:yes or no	Specifies whether the tape should be available only to it is owner/creator and Administrators.
l:f or s or n	Logging type: full, summary or none

rs:yes or no	Specifies whether or not to backup the removable storage database.
hc:on or off	Specifies whether or not to use hardware compression (only available on compatible tape drives).

Safe Mode:

Files used in the Windows 2000 boot process: (KB# Q114841)

File:	Location:
Ntldr	System partition root
Boot.ini	System partition root (KB# Q99743)
Bootsect.dos	System partition root
Ntdetect.com	System partition root
Ntbootdd.sys*	System partition root
Ntoskrnl.exe	%systemroot%\System32
Hal.dll	%systemroot%\System32
System	%systemroot%\System32\Config

* Optional - only if system partition is on SCSI disk with BIOS disabled

BOOT.INI switches: (KB# Q239780)

- **/basevideo** - boots using standard VGA driver
- /**fastdetect=[com*x*,*y*,*z*]** - disables serial mouse detection or all COM ports if port not specified. Included by default
- **/maxmem:*n*** - specifies amount of RAM used - use when a memory chip may be bad
- **/noguiboot** - boots Windows without displaying graphical startup screen
- **/sos** - displays device driver names as they load
- **/bootlog** - enable boot logging
- **/safeboot:minimal** - boot in safe mode
- **/safeboot:minimal(alternateshell)** - safe mode with command prompt
- **/safeboot:network** - safe mode with networking support (KB# Q236346)

Booting in Safe Mode: (KB# Q202485)

- 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. (KB# Q199175)
- ***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 botched driver installs and registry changes.
- ***Recovery Console*** - only appears if it was installed using **winnt32 /cmdcons** or specified in the unattended setup file.
- ***Directory Services Restore Mode*** - only in Server, not applicable to Win2000 Professional.
- ***Debugging Mode*** - again, only in Server
- ***Boot Normally*** - lets you boot, uh, normally. ;-)

Windows 2000 Control Sets (KB# Q142033)

- Found under HKEY_LOCAL_MACHINE\System\Select - has four entries
- ***Current***- CurrentControlSet. Any changes made to the registry modify information in CurrentControlSet
- ***Default*** - control set to be used next time Windows 2000 starts. Default and current contain the same control set number
- ***Failed*** - control set marked as failed when the computer was last started using the LastKnownGood control set
- ***LastKnownGood*** - after a successful logon, the Clone control set is copied here

Recovery Console

- Insert Windows 2000 CD into drive, change to i386 folder and run **winnt32 /cmdcons** (KB# Q216417)
- After it is installed, it can be selected from the "Please Select Operating System to Start" menu
- When starting Recovery Console, you must log on as Administrator. (KB# Q239803)
- Can also be run from Windows 2000 Setup, repair option.
- Allows you to boot to a "DOS Prompt" when your file system is formatted with NTFS.
- Looks like DOS, but is very limited. By default, you can copy from removable media to hard disk, but not vice versa - console can't be used to copy files to

other media (KB# Q240831). As well, by default, the wildcards in the copy command don't work (KB# Q235364). You can't read or list files on any partition except for system partition.

- There are four set variables: allowwildcards, allowallpaths, allowremovablemedia and nocopyprompt
- Can be used to disable services that prevent Windows from booting properly (KB# Q244905)

Command	Description
attrib	changes attributes of selected file or folder
cd or chdir	displays current directory or changes directories.
chkdsk	run CheckDisk
cls	clears screen
copy	copies from removable media to system folders on hard disk. No wildcards
del or delete	deletes service or folder
dir	lists contents of selected directory on system partition only
disable	disables service or driver
diskpart	replaces FDISK - creates/deletes partitions
enable	enables service or driver
extract	extracts components from .CAB files
fixboot	writes new partition boot sector on system partition
fixmbr	writes new MBR for partition boot sector
format	formats selected disk
listsvc	lists all services on W2K workstation
logon	lets you choose which W2K installation to logon to if you have more than one
map	displays current drive letter mappings
md or mkdir	creates a directory
more or type	displays contents of text file
rd or rmdir	removes a directory

ren or rename	renames a single file
systemroot	makes current directory system root of drive you're logged into

Startup and Recovery Settings

- Accessed through Control Panel > System applet > Advanced tab > Startup and Recovery
- Memory dumps are always saved with the filename memory.dmp (KB# Q192463)
- Small memory dump needs 64K of space. Found in %systemroot%\minidump
- In order to perform a recovery, the paging file must be on the system partition and the pagefile itself must be at least 1 MB larger than the amount of RAM installed for Write debugging information option to work
- Use dumpchk.exe to examine contents of memory.dmp (KB# Q156280)

Manage, Configure, and Troubleshoot Storage Use

Monitor, configure, and troubleshoot disks and volumes

Windows 2000 supports both *Basic* and *Dynamic* storage. In basic storage you divide a hard disk into partitions. Windows 2000 recognizes primary and extended partitions. A disk initialized for basic storage is called a *Basic disk.* 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. (KB# Q175761)

Dynamic storage (Windows 2000 only) allows you to create a single partition that includes the entire hard disk. A disk initialized for dynamic storage is called a *Dynamic disk.* Dynamic disks are divided into volumes which can include portions of one, or many, disks. These can be resized without needing to restart the operating system. (KB# Q225551)

There are three volume types

- *Simple volume* - contains space from a single disk
- *Spanned volume* - contains space from multiple disks (maximum of 32). First 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 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

Dynamic Volume Limitations

- Cannot be directly accessed by DOS, Win95/98 or any versions of Windows NT if you are dual-booting as they do not use the traditional disk organization scheme of partitions and logical volumes. MBR on dynamic disks contains a pointer to disk configuration data stored in the last 1 MB of space at the end of the disk. (KB# Q197738)
- Dynamic volumes which were upgraded from basic disk partitions cannot be extended, especially the system volume which holds hardware-specific files required to start Windows 2000 and the boot volume. Volumes created after the disk was upgraded to dynamic can be extended. (KB# Q222188)
- 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. (KB# Q216341)
- Not supported on portable computers or removable media. (KB# Q232463)
- A boot disk that has been converted from basic to dynamic cannot be converted back to basic. (KB# Q217226)

Translation of terms between Basic and Dynamic Disks

Basic Disks	Dynamic Disks
Active partition	Active volume
Extended partition	Volume and unallocated space
Logical drive	Simple volume
Mirror set	Mirrored volume (Server only)
Primary partition	Simple volume
Stripe set	Striped volume
Stripe set with parity	RAID-5 volume (Server only)
System and boot partitions	System and boot volumes
Volume set	Spanned volumes

To manage disks on a remote computer you must create a custom console focused on another computer. Choose Start > Run and type mmc. Press Enter. On console menu click Add/Remove Snap-in. Click Add. Click Disk Management then click Add. When Choose Computer dialog box appears choose the remote system.

Disk information is now stored on the physical disk itself, facilitating moving hard drives between systems. As managing disk numbering can become quite complex, the **dmtool.exe** utility has been provided. (KB# Q222470)

When using the Disk Management Snap-in Tool

- Whenever you add a new disk in a computer it is added as Basic Storage
- Every time you remove or add a new disk to your computer you must choose Rescan Disks
- Disks that have been removed from another computer will appear labeled as Foreign. Choose "Import Foreign Disk" and a wizard appears to provide instructions.
- For multiple disks removed from another computer, they will appear as a group. Right-click on any of the disks and choose "Add Disk".
- 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.

Configure data compression

- Files and folders on NTFS volumes can have their compression attributes set through My Computer or Windows Explorer.
- **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). Its switches are:

Switch	Function
none	displays the state of the current folder
/c	compresses specified folder or file
/u	uncompresses the specified folder or file
/s[:folder]	specifies that the action be applied to all sub-folders of the parent folder
/a	displays files with hidden/system attribute
/i	ignores errors
/f	forces specified file or folder to compress/decompress
/q	quiet - reports only essential information
/?	displays user help
filename	specifies a file or folder - can use multiple filenames and wildcards

Monitor and configure disk quotas

- Windows 2000 now supports disk-based quotas. Quotas can be set on NTFS volumes, but not on FAT or FAT32 volumes.
- Quotas cannot be set on individual folders within a NTFS volume, but must instead be set on the entire volume. A physical disk can be divided into multiple logical volumes with different quotas set for each. (KB# Q183322)
- By default, quotas are not enabled. Right-click the volume that you want to protect, click the Quota tab and select "Enable quota management"
- Users exceeding their quota will still be able to write to the volume unless "Deny disk space to users exceeding quota limit" is selected. (Do not enforce quotas on a system partition as W2K writes a fair amount of data to the disk

while booting and you may render your system unbootable - save this for data partitions only).

- Quotas can only be set on an individual basis, they cannot be assigned to groups. To select multiple users CTRL+click on the names you want to assign quotas to. You can choose to issue users a warning before they reach their disk usage limit. (Hopefully MS will fix this so quotas can be assigned to groups in the future).

Recover from disk failures

ARC paths in BOOT.INI: (KB# Q113977 & Q119467)

The Advanced Risc Computing (ARC) path is located in the BOOT.INI and is used by NTLDR to determine which disk contains the operating system. (KB# Q102873)

multi(x)	Specifies SCSI controller with the BIOS enabled, or non-SCSI controller. x=ordinal number of controller.
scsi(x)	Defines SCSI controller with the BIOS disabled. x=ordinal number of controller.
disk(x)	Defines SCSI disk which the OS resides on. When *multi* is used, x=0. When *scsi* is used, x= the SCSI ID number of the disk with the OS.
rdisk(x)	Defines disk which the OS resides on. Used when OS does not reside on a SCSI disk. x=0-1 if on primary controller. x=2-3 if on multi-channel EIDE controller.
partition(x)	Specifies partition number which the OS resides on. x=cardinal number of partition, and the lowest possible value is 1.

multi(0)disk(0)rdisk(0)partition(1). These are the lowest numbers that an ARC path can have.

Remote Storage: (KB# Q234776 & Q234692)

- Not installed by default. Added through Control Panel > Add/Remove Programs > Windows Components > Remote Storage.
- Remote storage moves eligible files from your local hard disk volumes to a remote storage location. When the space on your local, or managed, volume falls below the threshold you specify, remote storage automatically removes the content from the original file and sends it to the remote storage location. The file still appears on your local drive, but the file size is zero since the file actually resides in a remote location.

- When the file is needed again, remote storage recalls the file and caches it locally so it can be accessed.
- Response time is slower than if the file were stored on your local volume.
- You specify the files or the parameters for the files that should be stored remotely so that your most commonly used files remain on your local volume.

Removable Storage: (KB# Q250468)

- Removable storage allows you to store data on removable disks such as Zip disks and CD-ROMs.
- Removable storage can use jukeboxes or individual media drives, which can be grouped together in media pools.
- Removable storage works by configuring libraries to keep track of the location where data is stored (e.g., a Zip disk is removed and put in another location, the library remembers that disk and the data on it.)

Configure and Troubleshoot Windows 2000 Network Connections:

Internet Connection Sharing (ICS): (KB# Q237254)

- Enabled through Control Panel > Network and Dial-up Connections. Right-click the connection you want to share and choose Properties. On the Shared Access tab, select "Enabled shared access for this connection".
- If you want the connection to dial automatically whenever it is accessed, select the "Enable on-demand dialing" box.
- This feature should not be used in a network with other Windows 2000 Domain Controllers, DNS servers, DCHP servers, gateways or computers configured for static IP addresses.
- The machine with ICS enabled will have its LAN adapter's address set to 192.168.0.1. It becomes a DHCP server assigning addresses in the 192.168.0.x range to other machine's on the network that are configured as DHCP clients. It assigns them 192.168.0.1 as their gateway and uses Network Address Translation (NAT) to route information between the machines on the intranet and its valid connection to the Internet.
- This technology is intended for home use and use in small offices in peer-to-peer network environments. Corporate users should consider a more robust product such as MS Proxy Server 2.0.

Virtual Private Networks (VPNs)

- PPTP - Point to Point Tunneling Protocol. Creates an encrypted tunnel through an untrusted network. Supported by Windows 95, Windows 98 and Windows NT 4.0.
- L2TP - Layer Two Tunneling Protocol. Works like PPTP as it creates a tunnel, but it does not provide data encryption. Security is provided by using an encryption technology like IPSec. Only supported on Windows 2000 at this time.

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

Network Protocols

TCP/IP protocol

Miscellaneous

- Is an industry-standard suite of protocols
- It is routable and works over most network topologies
- It is the protocol that forms the foundation of the Internet
- Installed by default in Windows 2000
- Can be used to connect dissimilar systems
- Uses Microsoft Windows Sockets interface (Winsock)
- IP addresses can be entered manually or provided automatically by a DHCP server
- DNS is used to resolve computer hostnames to IP addresses
- WINS is used to resolve a NetBIOS name to an IP address
- Subnet mask - A value that is used to distinguish the network ID portion of the IP address from the host ID
- Default gateway - A TCP/IP address for the host (typically a router) which you would send packets for routing elsewhere on the network

Automatic Private IP Addressing

Windows 98 and Windows 2000 support this new feature. When "Obtain An IP Address Automatically" is enabled, but the client cannot obtain an IP address, Automatic Private IP addressing takes over:

- IP address is generated in the form of 169.254.x.y (where x.y is the computer's identifier) and a 16-bit subnet mask (255.255.0.0)
- The computer broadcasts this address to its local subnet
- If no other computer responds to the address, the first system assigns this address to itself
- 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.
- The 169.254.0.0 - 169.254.255.255 range has been set aside for this purpose by the Internet Assigned Numbers Authority

Troubleshooting (KB# Q102908)

- Ipconfig and Ipconfig /all - displays current TCP/IP configuration (KB# Q223413)
- Nbtstat - displays statistics for connections using NetBIOS over TCP/IP
- Netstat - displays statistics and connections for TCP/IP protocol
- Ping - tests connections and verifies configurations
- Tracert - check a route to a remote system
- Common TCP/IP problems are caused by incorrect subnet masks and gateways
- If an IP address works but a hostname won't check DNS settings

Authentication protocols

- EAP - Extensible Authentication Protocol. A set of APIs in Windows for developing new security protocols as needed to accommodate new technologies. MD5-CHAP and EAP-TLS are two examples of EAP
- 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
- RADIUS - Remote Authentication Dial-in User Service. Specification for vendor-independent remote user authentication. Windows 2000 Server can act as a RADIUS client or server.
- 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 NT4 and Win 95/98 (with DUN 1.3 upgrade) for VPN connections. MS-CHAP cannot be used with non-Microsoft clients
- SPAP - Shiva Password Authentication Protocol. Used by Shiva LAN Rover clients. Encrypts password, but not data
- CHAP - Challenge Handshake Authentication Protocol - encrypts user names and passwords, but not session data. Works with non-Microsoft clients
- PAP - Password Authentication Protocol. Sends username and password in clear text

Other protocols

- DLC is a special-purpose, non-routable protocol used by Windows 2000 to talk with IBM mainframes, AS400s and Hewlett Packard printers.
- Appletalk must be installed to allow Windows 2000 Professional to communicate with Apple printers. Do not confuse this with File and Print Services for Macintosh which allow Apple clients to use resources on a Microsoft network (only available on Server).
- NWLink is Microsoft's implementation of Novell's IPX/SPX protocol. It is adequate for small to medium sized networks and requires less administrative overhead than TCP/IP. It is routable.
- NetBEUI is used soley by Microsoft operating systems and is non-routable (it is broadcast-based)

Install and configure network services

Domain Name Service (DNS): (KB# Q217769)

- Resolves hostnames to IP addresses.
- Active Directory cannot run without it.
- A records are also called forward lookups or host records. An A record maps a domain name to an IP address.
- Start Of Authority (SOA) records names the primary DNS server for a domain, provides an e-mail address for the admin (note: "." used instead of "@" in e-mail address), and specifies how long its okay to cache its data. Keeps track of data changes through serial numbers. (KB# Q163971)
- NS records designate which servers are Name Servers in the domain.
- CNAME (Canonical Name) Records or Aliases used to provide an alias for the hostname of the server. For example, a Web server at brainbuzz.com may have the hostname "jaxx", but its CNAME alias allows it to respond to "www.brainbuzz.com". (KB# Q168322)
- MX (Mail Exchange) records allow an admin to designate which machines receive mail in a domain by order of preference (a lower number equals higher preference).

- PTR (Pointer) records are also called reverse records or reverse lookups. Allow an IP address to be resolved to a host name. Creates ".in-addr.arpa" entries. (KB# Q164213)
- SRV records allow DNS to identify server types. (KB# Q232025 & Q178169)
- A Standard Primary zone stores a master copy of the zone in a text file. Used to exchange DNS data with other servers that use text-based storage methods.
- A Standard Secondary zone creates a copy of an existing zone - used for load balancing and fault-tolerance.
- An Active Directory Integrated zone stores its data in Active Directory rather than on the local machine. Provides greater fault-tolerance and secure updates.
- Zones can be configured for Dynamic Updates. Resource records will then be updated by the DHCP clients and or server without administrator intervention. (KB# Q228803 & Q222463)
- There are two zone transfer types, full zone transfer (AXFR) and incremental zone transfer (IXFR):
    - *AXFR* - supported by most DNS implementations. When the refresh interval expires on a secondary server it queries its primary using an AXFR query. If serial numbers have changed since the last copy, a new copy of the entire zone database is transferred to the secondary. (KB# Q164017)
    - *IXFR* - Also uses serial numbers, but only transfers information that has changed rather than the entire database. The server will only transfer the full database if the sum of the changes is larger than the entire zone, the client serial number is lower than the serial number of the olds version of the zone on the server or the server responding to the IXFR request doesn't recognize that type of query.
- A caching DNS server simply resolves requests and caches data from resolved requests until its TTL expires. (KB# Q167234)
- Use **nslookup** to troubleshoot problems with DNS. (KB# Q200525)

Dynamic Host Configuration Protocol (DHCP): (KB# Q169289)

New features NT4 Admins should be aware of

- *Automatic Private IP Addressing* - When a DHCP server is unavailable, W2K can assign itself a temporary IP address in the 169.254.x.y range.
- *DHCP Relay Agent* - is only available as part of Windows 2000 Server family now - it is not part of Windows 2000 Professional.
- *DNS Integration* - DHCP can now register the addresses it assigns with the Windows 2000 DNS servers that support dynamic update (KB# Q191290)
- *Enhanced Monitoring* - The new DHCP MMC console snap-in provides a graphical display of statistical data.

- *Expanded Scope Support* - Superscope and multicast scopes are now supported. (KB# Q186341 & Q161571)
- *Option Class Support* - Used to separate different types of clients each having similar or special configuration needs. There are vendor-defined and user-defined option classes. (KB# Q240247)
- *Resource Record Re-registration* - DHCP clients automatically re-register in *DNS* upon renewal of their lease.
- *Rogue DHCP Server Detection* - Prevents unauthorized DHCP servers from creating address assignment conflicts.

Process for DHCP address assignment

1. Client broadcasts DHCPDISCOVER to all nearby DHCP servers.
2. Server(s) respond with DHCPOFFER message containing IP address and release time.
3. Client chooses offer it likes best and broadcasts back a DHCPREQUEST to confirm the IP address.
4. Server finalizes process by returning a DHCPACK to acknowledge the request.

Supporting DHCP

- DHCP server can provide default gateway, DNS, WINS, proxy and browser auto-config info (IE5 and higher) in addition to IP address and subnet mask.
- DHCP servers must be authorized to assign addresses. Whenever it first comes online, it sends out a DHCPINFORM message. Other servers will respond with a DHCPACK message providing the name of the directory domain they belong to. If the first DHCP server (as part of a workgroup) detects another DHCP server that is a member of a domain, the first server assumes it is unauthorized and cannot service requests for addresses.
- DHCP in W2K is configured to enable dynamic update of dynamic DNS servers by default. Here are the available options: (KB# Q228803)
    - *Update DNS only if client requests* (default option) - updates forward and reverse lookup zones based on type of request DHCP client makes during the lease process. W2K clients will propose that they update the A record while the DHCP server updates the PTR record (KB# Q251370)
    - *Always Update DNS* - updates forward and reverse lookup zones when a client acquires a lease, regardless of the type of lease request
    - *Discard forward lookups when lease expires* - removes A record entries when the lease expires (even if client is offline or unavailable)
    - *Enable updates for DNS clients that do not support dynamic update* - DHCP server registers A and PTR records on behalf of older Windows clients and non-Windows clients that do not support dynamic updates.

- To create a superscope, open DHCP Manager and right-click the name of the server you want to create a superscope for, and choose **New Superscope**. A wizard will appear - choose the scopes you want to create a superscope from.
- Multicast scopes are created as with above except you would choose **New Multicast Scope**. Multicast is used by conferencing and collaborative applications to send information to several computers at once by using a single directed message.
- W2K supports two types of option classes:
    - *Vendor-defined* - assigned to classes that are identified by vendor type (e.g., a specific brand of computer).
    - *User-defined* - assigned to clients that require a common configuration that is not based on vendor type (e.g., one group whose Internet access is being monitored could be directed to a proxy server while other groups are not)
- DHCP relies on broadcast traffic which cannot cross routers unless they have been specifically configured to pass BOOTP or as DHCP relay agents. W2K Server includes a DHCP Relay Agent (installs as a service) to help DHCP broadcasts through routers. (KB# Q120932)

Windows Internet Name Service (WINS): (KB# Q185786)

- WINS resolves NetBIOS names to IP addresses. They do not need to be authorized.
- Is used to reduce the number of B-node broadcasts on a network.
- It is only needed in mixed-mode networks for NT4 compatibility. Its functionality has been superceded by enhanced DNS functionality in W2K
- The Computer Browser service from previous versions of NT has been superceded by Active Directory. Computer Browser service is only maintained for backwards compatibility. (KB# Q188001)
- For WINS clients in a W2K network it is now possible to specify up to 12 WINS servers for increased fault-tolerance.
- WINS is managed using the WINS snap-in for MMC.
- WINS stores all entries in a database. The *Owner* of a record is the WINS server that originated it. When database verification is enabled (every 24 hours by default), entries should be verified against the owner server rather than randomly selected partners.
- Static entries can be made in the WINS database for computers that cannot register dynamically in WINS.
- Use **jetpack.exe** utility to compact WINS databases, found in the %systemroot%\system32\wins directory (KB# Q145881)
- The database is replicated between push/pull partners. A push partner lets its pull partner know that enough changes have occurred in the database that it should request updates to its database.

- Enabling WINS lookup in DNS allows the DNS server to query the WINS database when it is unable to resolve a hostname to an IP address. (KB# Q173161)
- Setting up a WINS proxy agent on a subnet allows B-node broadcasts to be relayed through routers and reach the WINS server. (KB# Q121004)

Configure, monitor, and troubleshoot Remote Access: (KB# Q160699)

Inbound connections

Multilink Support: (KB# Q235610)

- Multilinking allows you to combine two or more modems or ISDN adapters into one logical link with increased bandwidth. (KB# Q233171)
- BAP (Bandwidth Allocation Protocol) and BACP (Bandwidth Allocation Control Protocol) enhance multilinking by dynamically adding or dropping links on demand. Settings are configured through RAS policies. (KB# Q244071)
- Enabled from the PPP tab of a RAS server's Properties dialog box. (KB# Q233151)

Setting Callback Security

- Using callback allows you to have the bill charged to your phone number instead of the number of the user calling in. Also used to increase security
- For roving users like a sales force, choose "Allow Caller to Set The Callback Number" (less secure)

Remote Access Policies

- Remote Access policies are stored on the server, not in Active Directory.
- 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.
- **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. (KB# Q193897)
- 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.

- 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.
- 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 traveling sales force with laptops to avoid long-distance charges by having the RRAS server call them back.
- 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).
- Order of policy resolution is:
    1. User initiates connection with RRAS
    2. RRAS checks for policy that matches
    3. If policy matches, RRAS checks user account for dial-in permissions. If no policy match found, connection is denied.
    4. If permission is set to **allow access**, user is granted access and profile for the policy is applied. If permission set to **Control access through Remote Access Policy**, policies permission settings determine access.
    5. While user is connected, RRAS matches the connection to settings of user account and policy profile. As long as they match the connection stays alive (e.g., profile settings allow one hour maximum connection time. When user goes over an hour, the policy no longer matches and the user is disconnected).
- The three components of a remote access policy are its *conditions, permissions and profile:*
    - *Conditions* - a list of parameters such as the 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.
    - *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 in partnership with the user's dial-in permissions in Active Directory providing a wide range of flexibility when assigning remote access permissions.
    - *Profile* - settings such as authentication and encryption protocols which are applied to the connection. If connection settings do not match user's dial-in settings, the connection is denied.

Remote Access Profiles

- *Dial-in constraints* - idle time before disconnect, max session time, days and times allowed, phone numbers, and media types (VPN, ISDN, etc.)
- *IP* - used to configure TCP/IP packet filtering.
- *Multilink* - multilink and BAP are configured here. Configure to disconnect a line if bandwidth falls below a present threshold. Can be set to require BAP. (KB# Q233151 & Q233171)
- *Authentication* - define authentication protocols required for connections using this policy (e.g., SmartCards would need EAP-TLS).
- *Encryption* - used to specify the types of encryption that are allowed/required/prohibited.

Install, configure, monitor and troubleshoot Terminal Services (TS): (KB# Q243202)

Installing TS

- 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 Services include: *TS Client Creator,* creates floppies for installing TS Client, *TS Configuration*, used to manage TS protocol and server configuration, *TS Licensing*, manages Client Access Licenses, and *TS Manager*, used to manage and monitor sessions and processes on the server running TS.
- 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: (KB# Q243212 & Q238162)

- Remote Administration Mode allows Administrators to manage any number of Windows 2000 Servers from a single desktop. Admins have complete access to the remote system to perform tasks such as software installation, administrative functions, etc., as if they were logged on at the local console.

- 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.
- There are no licensing requirements for using the Remote Administration Mode.
- If another Admin 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 Admins are in session.
- Do not use for tasks that require reboots (e.g., you reboot a server in another city and it fails to come back up because a floppy is in the A: drive - oops)

Configuring TS for application sharing (Application Server Mode)

- 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.
- Best practice is to remove 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 (eg., .INI) are written to these directories.
- 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**). (KB# Q243555)
- Remember that all TS users log on locally in a virtual console on your server and have access to your local drives. **Use NTFS on all volumes** to prevent users from getting into places where they don't belong.
- Remote Control - is similar to Shadowing in Citrix MetaFrame. Allows an administrator to view and take control of a user's session as needed for help desk support. By design, this does not work from the console. (KB# Q232792)
- RDP-TCP Permissions..... (KB#s Q243554, Q225038 & Q224395)
- By default, users will be prompted for a password unless it is changed in the properties for RDP-TCP. (KB# Q247174)
- Sessions will disconnect when the connection is broken but will continue executing a user's processes by default. To prevent system resources being taken up by these processes set your sessions to *reset on broken* so that all processes are abruptly terminated when connections are broken.
- 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 (KB# Q243523). Alternately you can use round-robin DNS resolution to load balance your TS servers. (KB# Q168321)

- 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 user disconnects print queues and any print jobs are terminated. (KB#s Q238841, Q221509 & Q239088)
- Printers must be manually redirected for 16-bit Windows clients and Windows based terminals.

Configuring applications for use with TS

- Do not use the following types of applications with TS; multimedia applications, streaming applications, multimedia intensive games or applications that require special hardware to operate (like barcode scanners) unless the hardware can be connected to the terminal as a keyboard type device. TS does not recognize devices that connect to a parallel or serial port at this time.
- Some applications may require special installation or execution scripts to modify the app's performance in a multi-user environment.
- MS recommends that applications be installed using Add/Remove Programs in Control Panel. If you are installing the application directly, put TS into install mode by typing **change user /install** at a command prompt. Typing **change user /execute** turns off install mode. (KB# Q238840 & Q238357)

The TS Client is available for the following Windows operating systems

- 16-bit Windows for Workgroups with MS TCP/IP-32
- 32-bit Windows 95/98, Windows NT 3.51, Windows NT 4.0, or Windows 2000 Professional.
- Windows CE-based handheld and terminal devices
- Use the Citrix MetaFrame add-on product for Terminal Services for non-Windows clients.

Configuring TS Clients

- Windows 3.11 and Windows 95 clients should have at least 8 MB of RAM. Windows 98 clients should have at least 24 MB of RAM and Windows 2000 Pro needs 32 MB or more. 10 MB of hard drive space is needed if client bitmap caching is enabled.
- By default, all RDP client software is stored in the *%systemroot%***\system32\clients\tsclient** directory when TS is installed.

- Clients can be deployed via a file share for installation over the network or by using Terminal Services Client Creation from the Administrative Tools menu to create a client image that can be installed from a floppy disk.

TS Licensing (needed in addition to OS licenses, Windows 2000 Server/Microsoft BackOffice Client Access Licenses and application licenses): (KB#s Q244749, Q237811, Q232520, Q239107 & Q237801)

- *Built-in Licenses* - clients running Windows 2000 are automatically licensed as Windows 2000 clients.
- *Terminal Server Client Access Licenses* - purchased for known, non-Windows 2000 clients connecting to TS.
- *Terminal Services Internet Connector Licenses* - used to allow anonymous access to TS by clients across the Internet. Based on concurrent connections.

Temporary Licenses - issued when there are no valid licenses left to give. License server tracks issuance and expiration.

Implement, Monitor and Troubleshoot Security:

Encrypt data on a hard disk using Encrypting File System (EFS): (KB# Q223316 & Q230520)

About EFS

- Only works on Windows 2000 NTFS portions (NTFS v5).
- Encryption is transparent to the user.
- 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. (KB# Q241201 & Q230490)
- If the owner has lost his private key, an appointed recovery system agent can open the file using his/her key instead. (KB# Q242296)
- 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.
- EFS resides in the Windows OS kernel and uses the non-paged memory pool to store file encryption keys - this means no one will be able to extract them from your paging file.

- Encrypted files can be backed up using the Backup Utility, but will retain their encrypted state as access permissions are preserved. (KB# Q227825 & Q223178)
- Microsoft recommends creating an NTFS folder and encrypting it. In the Properties dialog box for the folder click the General tab then the Advanced button and select the "Encrypt Contents To Secure Data" check box. The folder isn't encrypted, but files placed in it will be automatically encrypted. Uncheck the box if you want to decrypt the file.
- Default encryption is 56-bit. North Americans can upgrade to 128-bit encryption.
- Compressed files can't be encrypted and vice versa. (KB# Q223093)
- You can't share an encrypted files
- Use the Cipher command to work with encrypted files from the command line. (KB# Q229530) & Q229546)
- The **efsinfo.exe** utility in the W2K Resource Kit allows an administrator to determine information about encrypted files (KB# Q243026)

Using the CIPHER command

Switch	Function
/a	performs the specified operation on files as well as folders
/d	decrypts specified folders and they are marked so files added to them will not be encrypted
/e	encrypts specified folders and they are marked so any files added later on are encrypted as well
/f	forces encryption operation on all specified files, even those already encrypted
/h	shows files with hidden/system attributes (not shown by default)
/i	specified operation continues even after errors have been reported
/k	creates a new file encryption key for user running Cipher command - cannot be used in conjunction with other options
/q	reports only essential information
/s	applies the specified operation to sub-folders as well
file_name	specifies a pattern, file, or folder

Implement, configure, manage and troubleshoot policies in a W2K environment:

Local & 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.

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

Group Policy snap-in (gpedit.msc) - Exclusive to Windows 2000 and supercedes the System Policy Editor. Uses Incremental Security Templates.

- Should only be applied to Windows 2000 systems that have been clean installed onto an NTFS partition. NTFS computers that have been upgraded from NT4 or earlier, only the Basic security templates can be applied.
- Settings can be stored locally or in AD. Are secure and cannot be changed by users - only Administrators.
- 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.

Incremental Security Templates for Windows 2000: (KB# Q234926)

Template:	Filename:	Description:
Compatibility	compatsv.inf compatdc.inf	Compatibility template, but also referred to in MS documentation as Basic template. Sets up permissions for local users group so that legacy programs are more likely to run. Not considered a secure environment.
Secure	securesv.inf securedc.inf	Increases security settings for Account Policy and Auditing. Removes all members from Power Users group. ACLs are not modified.
High Secure	hisecsv.inf hisecdc.inf	Secure template provided for Workstations running in W2K native mode only. Requires all network communications to be digitally signed and encrypted. Cannot communicate with downlevel Windows clients. Changes ACLs to give Power Users ability to create shares and change system time.

*sv.inf is for a member server, *.dc.inf is for a domain controller.

Local Groups

Local Group	Description
Administrators	Can perform all administrative tasks on the local system. The built-in Administrator account is made a member of this group by default.
Server Operators	Can manage the domain's servers (only found on domain controllers). Can create, manage, and delete printer and network shares, backup and restore, format fixed disks, lock and unlock servers and files and change the system time.
Account Operators	Can create and delete user accounts and groups. Cannot modify Administrator accounts, Domain Admins global group, local Administrator's group, Account Operators, Print Operators and Backup Operators.
Print Operators	Can create, manage, and delete printer shares.
Backup Operators	Can use Windows Backup to back up and restore data on the computer.
Guests	Used for gaining temporary access to resources for which the Administrator has assigned permissions. Members can't make permanent changes to their desktop environment. When a computer or member server running Client for MS Networks joins a domain, Windows 2000 adds Domain Guests to the local Guests group.
Replicator	Supports file replication in a domain
Power Users	Can create and modify local user accounts on the computer, share resources and can install drivers for legacy software. This group only exists on W2K Professional workstations and on non-domain controllers/member servers.

Users	Can perform tasks for which they have been assigned permissions. All new accounts created on a Windows 2000 machine are added to this group. When a computer or member server running Client for MS Networks joins a domain, Windows 2000 adds Domain users to the local Users group.

Local Group Policy

- There are two types of Group Policy objects: local Group Policy objects and non-local Group Policy Objects. Each Windows 2000 system can have only one local Group Policy object.
- Order of application is Local, Site, Domain and Organizational Unit. Local Policies have the least precedence whereas OU Policies have the highest.

Non-local Group Policy (stored in Active Directory)

- Can be linked to a site with AD Sites and Services and applies to all domains at the site
- When applied to a domain it affects all users and computers in the domain and (by inheritance) all users and computers in Organizational Units.

Config.pol, NTConfig.pol and Registry.pol

- Windows 2000 uses the **registry.pol** format. Two files are created, one for Computer Configuration (stored in the \Machine subdirectory) and one for User Configuration (stored in the \User subdirectory).
- Registry.pol files can be used with Windows 95/98, Windows NT 4.0 and Windows 2000 as it is a text file embedded with binary strings. NTConfig.pol is a binary file whereas Config.pol is a text file.
- .POL files can be viewed using the **regview.exe** tool from the W2K Resource Kit. Viewing them does not apply them to the registry.

Implement, configure, manage, and troubleshoot auditing

Auditing can be enabled by clicking Start > Programs > 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 (success/failure) for each object as desired then restart computer for new policies to take effect.

Implement, configure, manage, and troubleshoot local accounts: (KB# Q217050)

- 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.
- Domain user accounts reside in AD on domain controllers and can access all resources on a network that they have been accorded privileges for.
- Built in user accounts are Administrator (used for managing the local system) and Guest (for occasional users - disabled by default)
- Usernames cannot be longer than 20 characters and cannot contain the following illegal characters: " / \ [ ] : ; | = , + * ? < >
- User logon names are not case sensitive. You can use alphanumeric combinations to increase security, if desired.
- Passwords can be up to 128 characters but Microsoft recommends limiting them to about eight characters.
- The same characters that are considered illegal in usernames are also verboten for use in passwords
- User accounts are added and configured through the Computer Management snap-in.
- Users should be encouraged to store their data in their My Documents folder which is automatically created within their profile folder and is the default location that Microsoft applications use for storing data.
- Creating and duplicating accounts requires only two pieces of information: 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.
- 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.

Implement, configure, manage, and troubleshoot Account Policy

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

Password policy (default settings)

- Enforce password history = 0 days
- Maximum password age = 42 days
- Minimum password age = 0 days

- Minimum password length = 0 characters
- Passwords must meet complexity requirements = Disabled
- Store password using reversible encryption for all users in the domain = Disabled

Account lockout policy (default settings)

- Account lockout duration = not defined (suggested is 30 minutes)
- Account lockout threshold = 0 invalid login attempts/disabled (suggested is 5 attempts)
- Reset account lockout after = not defined

Miscellaneous

- Enforcing password complexity requires users to enter passwords at least 6 characters long that include upper and lowercase, numbers and punctuation. (KB# Q161990 & Q225230)
- Every failed login attempt increments the logon counter by one. When the counter reaches the threshold, the account is locked out for the specified duration. If the time between attempts exceeds the value specified for the counter reset policy, the counter is set back to zero.
- MS recommends storing passwords using reversible encryption (MD5-CHAP) to increase security when setting up a RRAS server for dial-in or VPN users.

Implement, configure, manage, and troubleshoot security using the Security Configuration Tool Set

- The Security Configuration and Analysis snap-in is used to troubleshoot security in Windows 2000.
- The security database (e.g., **mysecuresv.mdb**) is compared to an incremental template such as hisecsv.inf and the results displayed in the right hand pane. The log of the analysis will be placed in %systemroot%\security\logs\mysecure.log
- There is a text based version of this tool that can be run from the command line - **secedit.exe**.

Special thanks to Sean McCormick for contributing this Cramsession. To send feedback to Sean, please post a message labelled "Attention Cramsession Author" here:

W2K Server Forum