Windows 2000

Win 2000 Installation

Configuration Options

Files and Shares

Tools

Use

Services

User Management

Appendices

The CTDP Windows 2000 Guide Version 0.6.1 Oct 28, 2001

This guide may have inaccuracies, use at your own risk.

Introduction

This guide is best used after reading the CTDP Windows NT guides or with the CTDP Windows NT guides in order to fully understand the operation and use of this operating system. Also, to understand Active Directory, the reader should have some knowledge of object oriented concepts. It should be helpful to read the Object Guide and the UML Guide on this website. RFCs are posted at www.ietf.org.

There are four Windows 2000 operating systems:

- Windows 2000 Professional - Supports up to two processors and up to 4GB of RAM. Used as a workstation or client computer and it is the replacement for Windows NT Workstation.
- Windows 2000 Server - Supports up to four processors and up to 4GB of RAM. It is used for web, application, print and file servers.
- Windows 2000 Advanced Server - Supports up to eight processors and up to 8GB of RAM. It is used in an enterprise network and very useful as an SQL server.
- Windows 2000 Datacenter Server - Supports up to 32 processors and up to 64GB of RAM. It is used in an enterprise network to support extremely large databases and real time processing.

System	Microprocessor	RAM	HD Requirements
Windows 2000	Pentium 133	64Mb	650 MB free (2 G recommended)
Windows 2000 Server	Pentium 133	128Mb (256Mb Recommended)	1 GB free (2 G recommended)
Windows 2000 Advanced Server	Pentium 133	256Mb	1 Gb free (2 G recommended)
Windows 2000 Datacenter Server	Pentium 133	256Mb	1 GB free (2 G recommended)

VGA video or better is required for all systems alnog with a CDROM, and keyboard. Also a mouse, floppy disk drive and network card should be on the system, but are not required.

100MB additional disk space may be required if using a FAT file system and over the network installations also require additional hard disk room.

New Features of Windows 2000 over NT

- Plug and play support.
- Keberos 5 security protocol.
- New file systems:
  - FAT32 support - A file allocation table operating system that supports larger disk partition size than older FAT filesystems.
  - EFS - Encrypting File System support.
- Internet Explorer version 5 with XML support and Outlook Express version 5.
- Additional control panel power options.
- Can support up to 10 displays simultaneously.

User interface

The Windows 2000 user interface is similar to Windows 98. Some selections using various icons and selections include:

- Recycle Bin - Used to store deleted files and folders. When emptied, files or folders are gone for good.
- My Network Places Icon
  - Add Network Place selection - Used to connect to a shared network folder or the world wide web.
  - Computers Near Me selection - Used to connect to computers in your domain or workgroup.
  - Entire Network selection
    - Used to view all domains, workgroups, and computers on the organizational network.
    - Used to search for a specific computer.
    - Used to search for specific files or folders.
- Windows Explorer - To run, select "Start", "Programs", "Accessories", and "Windows Explorer".

Platform Support

Windows 2000 will only run on the Intel Pentium platforms. Windows NT additionally supported the Compaq Alpha (previously Dec Alpha) platform, the MIPS R4000, and the Power PC. The Alpha platform was not supported after Windows NT service pack (SP) 6, and the other platforms lost support after Windows NT service pack 1.

Windows 2000 does not allow direct hardware access. All hardware access must be through the hardware abstraction layer (HAL).

Other Support

- **Windows NT 4.0 domains**
- User and group accounts using Windows 2000 Active Directory or a local database.
- **IPSEC** - Internet security protocol.
- **Smart cards**.

Windows 2000 Professional

Windows 2000 Professional is used primarily for desktop use. It only supports up to 10 concurrent network connections.

Hardware Support

- Up to 4 Gigabytes of RAM
- Up to 2 microprocessors

Application Support

Windows 2000 Professional and Windows 2000 Servers support the following application types:

- **DOS applications** without terminate and stay resident functions or virtual device drivers.
- **16 Bit Windows** applications
- **32 Bit Windows** applications
- **POSIX 1.x** applications
- **OS/2 1.x** applications

Windows 2000 Server

Windows 2000 Server is used primarily for web, application, print and file servers.

Hardware Support

- Up to 4 Gigabytes of RAM.
- Up to 4 microprocessors.

Features not provided by Windows 2000 Professional

Windows 2000 server can be a domain controller with the ability to have a read/write copy of Active Directory data.

- Disk Quotas - Disk space use is tracked for each user.
- DFS - Distributed file system support. Shares that are stored on various remote computers can appear as one share
- Supported Servers:
    - Internet Information Server
    - SQL Server
    - Exchange Server
    - Systems Management Server
    - RADIUS - Remote Authentication Dial-In User Service
    - SNA Server

Supported Protocols

- Network Protocols
    - IP
    - IPX
    - AppleTalk
- Routing Protocols
    - RIP version 2 (Routing Information Protocol)
    - OSPF - Open shortest path first.
- ATM - Asynchronous Transfer Mode.

Windows 2000 Advanced Server

Windows 2000 Advanced Server is used in an enterprise network and very useful as an SQL server.

Hardware Support

- Up to 8 Gigabytes of RAM.
- Up to 8 microprocessors.

Additional Support beyond Windows 2000 Server

- Clustering - Makes several computers appear as one to applications and clients. It supports clustering for up to two nodes. Between 2 and 32 servers may be clustered. The "Cluster Service" must be installed to implement clustering. Features are:
  - Network Load balancing (NLB).
  - Automatic takeover if a computer running an application fails.

Windows 2000 Datacenter Server

Used for real time transaction processing and database services. Provides the capabilities of Windows 2000 Advanced Server plus more scalability. It supports clustering for up to four nodes.

Hardware Support

- Up to 64 Gigabytes of RAM.
- Up to 32 microprocessors.

Windows 2000 Application Support

Applications that run out the normal Windows 2000 environment are supported with virtual machines. The following virtual machines are used:

- DOS VDM (Virtual Dos Machine) - Three threads - One used for applications and the other two are used to run the VDM. The files **autoexec.nt** and **config.nt** are used to setup the DOS environment rather than the autoexec.bat and config.sys files used traditionally with the original DOS operating system. These files are stored in the **System Root\System32** directory.
- Win16 is used to support applications that ran on Windows 3.x and WFW. This is also called **WOW** which refers to the fact that Windows 16 bit applications run on the Windows 32 bit environment. Windows 16 bit applications are supported so long as they do not make direct calls to the hardware. All applications run on a single Win16VDM by default. There is no pre-emptive multitasking. These applications can be run on separate Win16 virtual machines if required.
- POSIX - The system must run on an NTFS filesystem to support POSIX applications. This is because POSIX requires user file permission support and security that is not provided by FAT filesystems. Each POSIX application runs in its own separate memory.
- OS/2 - Text OS/2 version 1.x is supported. There is no support for 2.x, 3.x, and presentation manager.

Of course applications written for the native Windows 32 bit environment. are supported.

Windows 2000 System Operation

Windows 2000 Operating Modes

Windows 2000 and Windows NT both provide two modes of operation from a security level which are:

- **User mode** - This mode does not have full system access or privileges, but is dependent on APIs to acquire system access. Runs with privileges to access its own memory area. User applications and environmental subsystems execute in this mode.
- **Kernel Mode** - Executive which runs in protected memory mode with full privileges of system access. Any process running in this mode is not restricted to any specific memory space.

Executive Services

The Executive Services provides kernel mode services for the following:

- All applications
- Win32 Subsystem
- Win16 Subsystem
- POSIX Subsystem
- OS/2 Subsystem
- DOS VDM Subsystem

The Executive Services is an interface between the user and kernel modes. It consists of the Monitors or managers listed below it in the table below.

Executive Services							
I/O Manager	Window Manager			Object Manager			IPC Manager
Cache Manager		Security Reference Monitor	Virtual Memory Manager	Process Manager	Plug and Play Manager	Power Manager	Local Procedure Call (LPC) Facility
File System Drivers	Graphics Device Drivers						Remote Procedure Call (RPC) Facility

Device Drivers
Hardware

Micro Kernel
HAL

Services in Windows 2000 that were in Windows NT

- **I/O Manager** manages all input and output for the operating system, including cache manager, file system drivers, hardware device drivers, and network device drivers.
- **Win32K window manager and GDI** - Functions from Win32k.sys for graphics support and communication with graphic devices. This includes the Graphics Device Interface (GDI) which enables graphics devices to communicate with NT or 2000.
- **Security Reference Monitor** is responsible for enforcing the access-validation and audit-generation policy as defined by the Security subsystem. This Monitor, also called the **Security Subsystem** supports Active Directory and the logon process in Windows 2000.
- **Virtual Memory Manager** maps virtual addresses in the user's address space to physical pages in the computer's memory.
- **Object Manager** monitors the creation and use of objects. It also manages the global name space where access to all local objects is controlled. This now includes some functions from the process manager in Windows NT.
- **Hardware Device drivers** - An interface between specific hardware devices and NT which interfaces to HAL

Services deleted or modified in Windows 2000 that were in Windows NT

- **Process Manager** creates and deletes processes and also tracks process objects and thread objects.
- **Local Procedure Call Facility** using a client/server relationship, provides a communications mechanism between the applications and the Environmental subsystem.

Services added or modified in Windows 2000 that were not in Windows NT

- **Plug and Play Manager**
- **Power Manager**
- **IPC Manager** - This includes the Local Procedure Call (LPC) facility that was included with Windows NT, and also adds a Remote Procedure Call (RPC) facility
- **Microkernel** - Schedules threads, handles interrupts, and talks to the HAL. It enhances the Windows NT Process Manager and handles some of its functions.

Memory Model

The Windows 2000 memory model is **demand paged**. That means that virtual memory may be stored on the hard drive, and memory is swapped between RAM and the hard drive as demand requires it. A 32 bit linear flat address space is used. **Each application gets 4 Gb of virtual memory with one half reserved for kernel system data and the other half for application data.**

Windows 2000 Volumes and Disks

Hard Drive Partitions

A hard drive may be split into partitions. NT uses two main partitions but I believe these two may be installed on one partition. There can be up to 4 primary partitions and only one extended partition which may include several logical drives. A logical drive is assigned its own drive letter and uses part of or all the space in an extended partition. Only one partition may be extended and an extended partition may not be marked as active which means operating systems cannot be booted from it. Only one partition on a disk may be active at a time. On IBM compatible computers, only a primary partition may be a system partition which is where the NT boot loader must reside.

Windows 2000 Logical Partitions

Windows 2000 logical partitions include:

- **System** - Stores system files for booting such as NTLDR, BOOT.INI, and NTDETECT. COM.
- **Boot** - WINNT_Root partition where system files are.

These partitions may be on the same or on separate physical hard drive partitions.

The filesystem containing the boot files is referred to as the system partition and the partition that contains the WINNT40 directory is the boot partition.

Windows Disk Types

Windows uses the below two terms to refer to disks in a computer.

- **Basic Disks** - A standard disk with standard partitions (primary and extended).
- **Dynamic Disks** - Disks that have dynamic mounting capability to add additional local or remote partitions or directories to a disk drive. These are called dynamic volumes. This is new with the Windows 2000 operating system and is not supported by any other operating systems. Any volume that is on more than one hard drive must be created with dynamic disks. A disk can only be converted from dynamic to basic by first deleting all the volumes in the dynamic disk.

Windows NT Volume Sets

A Windows NT volume may span several partitions and includes:

- The disk directory area also called the root directory.
- Allocation tables to track used disk space.

Characteristics and limitations:

- A volume may contain 1 to 32 disk areas and can be formatted as FAT or NTFS.
- These combined areas cannot be split or one part of a volume can't be deleted without destroying the entire volume.
- They may contain disk areas from various drive types such as IDE or SCSI.
- NT system and boot partitions cannot be part of a volume set. Windows 95 and DOS don't recognize volume sets.

Volume sets (which are on basic disks) created with Windows NT are supported by Windows 2000 but may not be created with Windows 2000.

Windows 2000 supports the following types of volumes which can only be created on dynamic disks:

- **Simple Volumes** - Formatted partition on a hard drive. Has no fault tolerance.
- **Spanned Volumes** - Formatted partition or disk space on more than one partition or hard drive that appears as one volume. In Windows NT, this is called a volume set. Has no fault tolerance. The system or boot partitions cannot be included in a spanned volume. FAT, FAT32 and NTFS file systems may be included. Space from two to thirty two dynamic disks can be included. If one disk on the spanned volume fails, all data is lost, and no part of a spanned volume may be removed without destroying the entire volume.
- **Striped Volumes** - Also called disk stripingor a striped set in Windows NT, it is when two areas of disk space which are identical in size have half the information written on one area and the other half written on the second area. This effectively doubles the disk access speed, but provides no fault tolerance. In Windows NT, this is called a stripe set which is created on a basic disk.
- **Mirrored Volumes** - Also known as RAID 1 or a mirror set on Windows NT, this is a fault tolerance method where data is stored on two volumes (that appear as one) rather than a single volume. This costs access time, but is fault tolerant.
- **RAID-5 Volumes** - Require three or more areas of formatted drive space. Generating parity information can cost processor time.

Mirrored volumes and RAID-5 volumes are not supported by Windows 2000 Professional. Other than sector fixing, there is no fault tolerance provided with Windows 2000 Professional.

For a certification test, fault tolerance is not provided with Windows 2000 Professional.

Stripe Sets

A stripe set is established using free space from between 2 and 32 physical hard drives. The free space on each drive must be the same capacity. Data is written is 64k blocks simultaneously on each drive in the stripe set which increases disk drive read and write access speed. Windows 2000 Professional supports stripe sets, but not stripe sets with parity. **Windows 2000 Professional does not support disk drive fault tolerance**, only supporting stripe sets without parity and sector sparing.

NT system and boot partitions cannot be part of a stripe set.

Other Windows 2000 fault tolerant options include:

- RAID 5 or stripe sets with a parity drive.
- Disk mirroring
- Sector hot fixing

Other Windows 2000 file and filesystem characteristics that enhance file storage:

- Confirmation that hard drive write requests were done.
- Disk cache is used to store data going to or from the disk to speed up access time. This is referred to as lazy writing.
- Hard links are used to tie file physical location to multiple file names.

Windows 2000 Filesystems

Windows 2000 systems can support the following file systems:

- FAT, FAT32
- NTFS - New Technology File System
- CDFS - Compact Disk File System
- UDF - Universal Disk Format for DVDs.
- EFS - Encrypting File System runs as a service and is used to encrypt and decrypt files on an NTFS file system for security purposes. The EFS is not a file system like NTFS since it does not create partitions and control the placement of file data, it only is used to control the encryption of data. See the Section called "Security" in this document for more information on NFS.

FAT Filesystem Characteristics

Used with DOS, it can only support partitions up to 4 G. No spaces are allowed in the file name.

FAT32 or VFAT Filesystem Characteristics

VFAT - Virtual File Allocation Table introduced by Windows 95 which allows long file names. VFAT is not natively supported by Windows 2000.

- FAT32 filesystems support partitions up to 32GB.
- Filenames up to 255 characters long.
- Filenames begin with a letter and exclude " / \ [ ] : ; | = , ^ * ?
- The last part is the extension but spaces can be used
- It supports file attributes used by DOS such as read-only, archive, system, and hidden.
- Won't support running POSIX applications.

FAT partitions provide no local security, only share level security across a network.

NTFS Filesystem Characteristics

Windows 2000 NTFS file systems are newer than Windows NT NTFS file systems. In order for Windows NT and Windows 2000 to use the Windows 2000 file system together, the Windows NT system must have service pack 4 or later installed.

- Filenames up to 255 characters long
- Filenames preserve case but are not case sensitive.
- Filenames exclude " / \ < > : | * ?
- Supports built in file compression as a file attribute. Compression is applied to files in a folder if that folder has its compression attribute set. Also optionally sub folders and their contents may be compressed. **Compression is not supported if the cluster size is above 4K in size**. Moved files retain their compression attribute, but if they are copied they will assume the compression attribute of the target folder.
- Provides automatic transaction tracking of disk activity for correcting corrupt or failed operations.
- Supports auditing.
- Provides sector sparing.
- There is a recycle bin for each user.
- Windows 16 bit and DOS environments can't use this filesystem.
- A master file table is used to save individual file, boot sector, disk structure, and file recovery information.
- Automatically makes 11 character DOS file names. When the first 8 characters of long filenames match, the first four DOS file names use the first for characters of the long name, the ~ and 1, then2, etc. After the fourth duplicate name, the first two characters are used, then the next four characters are hashed, then the ~ character then a number. The first two duplicate file names may be: DOCU~1.DOC and DOCU~2.DOC. The long extension is used as part of the extension for the 8.3 filename alias.Directory entries used by long filenames include 1 for the 8.3 alias and 1 for each 13 characters in the long filename.
- Provides file logging ability and file recovery.
- Supports POSIX.
- Maximum file or partition size of 16 exabytes.
- Supports file sharing with MacIntosh clients.
- The disk is in 8M bands with a 2K file allocation map between each band. The 2K map is a map for the associated 8M band. This structure is called the BTREE and is used to reduce fragmentation.
- Supports file encryption with the Encrypting File System (EFS) on Windows 2000.
- Allows volumes on remote computers or local computers to be mounted as though they are part of the same partition they are mounted on. This feature is available on Windows 2000.
- Disk quotas (tracking of disk space) on a user by user basis are tracked.
- Removable media formatted in NTFS can be changed and accessed without rebooting the system in Windows 2000 (not NT).

If installing DOS with NT, install DOS first so DOS will not corrupt the NT boot sector and stop the NT boot manager from running. Floppies are formatted as FAT, not NTFS.

CDFS

The file system that supports compact disks (CDs) is the Compact Disk File System (CDFS).

UDF

The file system that supports DVDs is the Universal Disk Format (UDF).

Filesystems and Windows Systems

Operating System	NTFS	FAT32	FAT	CDFS	UDF	HPFS
Windows 2000	Yes	Yes	Yes	Yes	Yes	No
Windows NT 4.0	Yes	No	Yes	Yes	Yes	No
Windows NT 3.51	Yes	No	Yes	Yes	No	Yes
Windows 98	No	Yes	Yes	Yes	Yes	No
Windows 95	No	Yes	Yes	Yes	Yes	No
Windows 3,x & WFW	No	No	Yes	Yes	No	No
OS/2	No	No	Yes	Yes	No	Yes
MS-DOS	No	No	Yes	Yes	No	No

The FAT file system does not support file compression on Windows 2000 systems. The file compression utilities with Windows 95 and Windows 98 are not supported by Windows 2000.

FAT file systems may be converted to NTFS file systems using the command line convert utility. Once converted, they may not be changed back to FAT.

Windows 2000 contains an NTFS file defragmentation utility which Windows NT does not contain.

Support for Security

Each object has an **Access Control List (ACL)** which defines users and group permissions for the object. Each entry **(ACE - Access Control Entry)** in an ACL defines the permissions a specific user or group has for the object. Access token attributes are added to the object's ACL. The user's **security identifier (SID)** is compared to the contents of the ACL to determine if the user has the correct privileges to access the object.

The NTFS file system supports Access Control Lists for objects.

Volumes

A volume and a partition are the same thing. It is a formatted part of a disk that appears as one drive. Volume types supported by Windows 2000 include:

- **Simple volumes** - Formatted partition on a hard drive. Has no fault tolerance.
- **Spanned volumes** - Space on multiple disk drives that appears as one drive.
- **Striped volumes** - Identical sized areas of two or more hard drives that appear as one although part of the data is stored on each drive in a way so data is written to both at the same time. This is used to increase drive speed.
- **Mirrored volumes** - Also known as RAID 1 or a mirror set on Windows NT, this is a fault tolerance method where data is stored on two volumes (that appear as one) rather than a single volume. This costs access time, but is fault tolerant.
- **RAID-5 Volumes** - Require three or more areas of formatted drive space. Generating parity information can cost processor time.

A normal hard disk can contain up to four partitions total. It can contain one extended partition which can be further broken up into additional logical drives. It can contain four primary partitions or three primary partitions and one extended partition.

Disk Tools

The Computer Management Console Tools, Storage section describes these tools in greater detail.

- Disk Defragmenter - Used to analyze volumes and defragment the disk.
- Disk Management - Used to create, format, and manage volumes.
- Logical Drives
- Removable Storage

Windows 2000 Configuration Files

Required files

On Intel based machines:

- NTLDR - The boot loader
- BOOT.INI - Contains the boot menu with selections the user can boot from.
- BOOTSECT.DOS - A boot sector file for DOS for booting DOS or Windows 3.1 or 95.
- NTDETECT.COM - Detects the hardware for the NTLDR program.
- NTOSKRNL.EXE - The NT kernel.
- NTBOOTDD.SYS - Used for booting SCSI devices when no SCSI BIOS is available.

On RISC based machines:

- OSLOADER.EXE - The RISC boot loader
- NTOSKRNL.EXE - The kernel
- NTBOOTDD.SYS - Used for booting SCSI devices when no SCSI BIOS is available.

BOOT.INI

BOOT.INI is stored in the root directory of the computers primary boot partition and contains the menu of operating systems that may be booted. Has two sections:

1. [Boot Loader]
    - Timeout - The number of seconds the bootloader waits for the user to select an operating system other than the default.
    - Default - The path of the default operating system that is booted if the user makes no selection
2. [Operating Systems] - Lists the operating systems that may be booted and their paths using the Advanced RISC Computer (ARC) naming convention which is:
    - scsi(n) or multi(n) - The option scsi(n) is used for SCSI adapters that do not include BIOS support or have it enabled on their adapter. The multi(n) term is used for all other types of hard drives. The value of n indicates the number of the hardware adapter to use.
    - disk(n) - The value of n is 0 if the multi option is used, above, but for SCSI, the value indicates the SCSI bus number.
    - rdisk(n) - The SCSI LUN number. If scsi is used above, this value will be 0, "rdisk (0)". Otherwise this value is 0 for primary or 1for secondary.
    - partition(n) - The partition with the system files. This starts with 1 for the first

partition. It does not use 0 to indicate the first partition.
- \path - The directory with the operating system files with the default being \Winnt.

Options are:
- /FASTDETECT=[COMx | COMy] - This was the /NOSERIALMICE option in Windows NT. Useful if hooking up a UPS to the serial port, so Windows 2000 will not probe the port. Without com ports specified, makes the detection of a mouse on serial ports be skipped which is the default setting for Windows 2000.
- ?/BASEVIDEO - Standard VGA mode is used to load which is needed if the video card drivers are incorrect.
- ?/CRASHDEBUG - Enables automatic recovery and restart. Can be set from the control panel. Sends debut output to COM1, not a file.
- /SOS - Displays names of device drivers as they are loaded.
- ?/NODEBUG - Debugging information is not monitored.
- /MAXMEM:n - Limits the amount of RAM to be used by NT or 2000.
- ?/SCSIORDINAL:n - Selects the SCSI controller to be used to boot when there are more than one controller.
- /NOGUIBOOT - A Windows 2000 switch causes booting without display of the boot status screen.

To modify this file, you must change its properties so it is not system and read only. Then it may be edited and the properties must be restored when complete.

An example BOOT.INI file:

```
[boot loader]
timeout=5
default=multi(0)disk(0)rdisk(0)partition(1)\WINNT40
[operating systems]
multi(0)disk(0)rdisk(0)partition(1)\WINNT40="Windows NT Workstation Version 4.00"
multi(0)disk(0)rdisk(0)partition(1)\WINNT40="Windows NT Workstation Version 4.00
[VGA mode]" /basevideo /sos
C:\="Windows 95"
```

Boot Option configuration

The system applet in the control panel may be used to select the default operating system to boot and modify the boot.ini timeout value. The Startup/Shutdown tab supports this function. However it will not allow renaming of the bootable systems. Boot options are not configurable from the registry since it is not loaded at the time the boot selection is made. Most boot option changes are done by editing the boot.ini file directly.

Windows 2000 Security

Authentication is performed by the system to be sure the user is really who they claim to be. Authentication may be done at and for a local computer or at a global level for a domain using domain controllers across the network. Windows 2000 supports the following types of authentication:

- **Kerberos V5** (RFC 1510) - An internet standard authentication protocol which is the default protocol for Windows 2000 computers within a domain. This is not used for computers in different forests.
- **Windows NT LAN Manager (NTLM)** - Used to authenticate users from Windows 95, 98, and NT systems. Windows 2000 Active Directory must be operating in mixed mode to use this authentication method.
- **Secure Sockets Layer/Transport Layer Security (SSL/TLS)** - Requires certificate servers and is used to authenticate users that are logging onto secure web sites.
- **Smart card**

Authentication uses X.509 standard and kerberos.

Additional security features include IPSec for Virtual Private Networking (VPN) encryption, and Encrypting File System (EFS) to encrypt file contents.

Kerberos

Kerberos was developed at Masachussets Institute of Technology (MIT). Kerberos uses a Kerberos Domain Controller (KDC). The kerberos ticket is proof that the client has permission to access the resource.

NTLanman Authentication

NT 4.0 uses NTLanman (NTLN) authentication where a domain controller authenticates clients and passes a token. The server with the resource contacts the domain master to find out if the client has access permission.

Encrypting File System (EFS)

A public and private key system is used to control the encryption and decryption of files on the EFS which runs as a service. The encryption process breaks the files into blocks and encrypts each block with a different one of multiple symmetric keys. The keys are stored inside the file

header in a **Data Decryption Field (DDF)** and a **Data Recovery Field (DRF)**. This file header is encrypted and can only be decrypted with a recovery agent or using the user private key. The key used to encrypt the file is encrypted using the user account X.500 certificate and stored in the file. Different keys are used to encrypt different files so someone cannot get a key from one file and use it to decrypt another file. The encryption keys are never written to memory paging files.

Files or directories may be encrypted, but the contents of directories are encrypted together. Files cannot be encrypted across the network by EFS. Files that are moved are still encrypted, but the files must be moved to other NTFS volumes. Files that are move to an encrypted folder are encrypted when they are moved. If applications that are setup to store temporary files, store those files in an encrypted directory, the temporary files are encrypted.

To do EFS recovery the user must be designated an EFS recovery agent in Group policy and have an EFS Recover Agent certificate. When recovery agents are used to recover files, the keys are not recovered and cannot be copied. To decrypt files, the recovery agent unlocks the Data Recovery Field (DRF) using the public key. Recovery keys can only be used to decrypt files that were encrypted after the recovery key was created.

The **cypher.exe** command line program can be used to perform encryption and decryption. Command line options:

- /d - Decrypt files or folders.
- /e - Encrypt files or folders.
- /f - Force encryption or decryption regardless of the file or folder current state. Encrypt all files.
- /I - Ignore errors.
- /q - Only report essential information.
- /s - Encrypt all subdirectories and files in a directory.

A filename parameter is required on the command line to specify the name of a file or directory.

SSL

Secure Sockets Layer (SSL) is used to encrypt data going across the network.

Windows 2000 Network Support

Windows 2000 systems support the following network protocols and capabilities.

TCP/IP Protocols

- ARP
- RARP
- Proxy ARP - Allows subnetting on networks with old versions of TCP/IP that did not support subnetting

Network Address Translation

Network Address Translation (NAT) is used to allow multiple computers behind a single computer to use the single computer for access to another network or internet. The computer performing NAT will masquarade as though it is each individual computer (IP masquarading) using NAT. This hides the IP addresses on the computers behind the NAT computer.

The Network Address Translation properties dialog box may be entered by double clicking "IP Routing" then double click "Network Address Translation (NAT)" on the tree, right click a connection and select "Properties". Network Address Translation properties dialog box tabs are:

- General - Event logging options.
- Translation - Set time period for removing TCP and UDP mappings.
- Address Assingment - Configure IP addresses for DHCP.
- Name Resolution - IP to DNS resolution.

Windows 2000 Access Management

Windows NT access is controlled using the following methods:

- **Domains** - A domain is used to manage a large group of computers. It is used to control resource access for users. The term domain as used with Windows systems is not the same as an internet domain.
- **Workgroups** - A workgroup is used to manage groups of less than ten computers.
- **Local access**

Windows 2000 adds Active Directory to this list. When Active directory is used, one server maintains the Active Directory database, and other servers that are domain controllers keep a read/write copy of the database. Active Directory allows:

- User logon and authentication.
- Users can find resources using Active Directory.
- Administrators to manage user accounts, groups, and network resources.

Other Systems

Windows 95, 98, and NT computers cannot use Active Directory group policy.

Windows 2000 Processes

Process Priority Setting

Process priority may be set to a value from 1 to 31. Priorities are categorized as follows:

- 0-7 - Low user
- 7-15 - High user
- 15-23 - Real Time
- 23-31 - Administration only

Base thread priority is 8. Threads inherit the base priority of their parent process. The NT operating system can vary priorities higher or lower by a value of two in order to remain responsive. Processes may be launched with different priority settings from the command line using the following syntax:

start /priority /path/name.exe

The "/path/name.exe" is the path to and name of the program to be run. Where /priority may be:

- /low - Priority 4
- /belownormal - Priority 6
- /normal - Priority 8
- /high - Priority 13
- /realtime - Priority 24

Other options:

- /min - The application starts in a minimized start window.
- /max - The application starts in a maximized start window.
- /separate - The application starts in a separate memory area.
- /shared - The application starts in a shared memory area.

Setting Priority of foreground tasks

To modify foreground task priority use the **system applet in the control panel**. Selecting the performance tab will allow three foreground task settings to be set. If set to none on the left, foreground tasks are not boosted in priority, On the middle setting foreground tasks get a

priority increase of 1. On the right on the maximum setting, foreground tasks get a priority increase of two.

Task Manager

Can be used to start and stop applications, change process priority, and monitor performance statistics. It can be used to change the priority of a process, by right clicking on the process and selecting "Set Priority". Can enter the task manager one of the following ways:

- Press CTRL ALT DEL and select Task Manager
- Press CTRL SHIFT ESC
- Right click the taskbar and select Task Manager
- Select "Start, "Run", and type "taskmgr".

Tabs include:

- Applications
- Processes - Shows PID, CPU, CPU time, and memory usage.
- Performance - Shows:
    - CPU usage and history
    - Memory usage and history
    - Total handles, threads, and processes
    - Physical memory
    - Commit Charge - Memory allocated to the system or programs.
    - Kernel memory

Active Directory Structure

To understand Active Directory, the reader should have some knowledge of object oriented concepts. It should be helpful to read the Object Guide and the UML Guide on this website.

Features:

- Network resources are easy to find.
- Uses group policies for easier administration
- Scalability
- Flexibility with the ability to add new classes, attributes, and objects.
- Fully integrated security
- Extensibility
- Works on any network.

Parts and Structure

The domain is the core unit in the Active Directory structure. Active Directory includes:

- A **database** of information about network users and resources.
- A **service** managing the database.

Active directory is organized hierarchially and contains information about:

- **User Accounts**
- **Computers**
- **Shared folders**
- **Printers**

Active directory depends on and requires Domain Name Service (DNS) to be implemented on the network.

Functions

- Users can logon and are authenticated.
- Users can locate network resources.
- Administrators manage user and group access to network objects (resources).
- Users can have some administrative rights to some parts of the Active Directory database.

Object Oriented

Active Directory is object oriented. This means that items in active directory is treated as objects. Objects contain both behavior (executable code) and attributes (data or characteristics). Objects are constructed using classes, similar to the way a cookie cutter is used to construct cookies. Classes are templates for objects. Active Directory object classes include:

- **Domain**
- **Organizational Unit** - Contain either objects and/or other organizational units and are also called container objects. **The OU simplifies administration by allowing the organization of objects and other OUs (Its primary purpose).**
- **Group**
- **User**
- **Computer**
- **Contact**
- **Shared folder**
- **Printer**

A **domain tree** is a hierarchial group of one or more domains with one root domain.

Structure of Active Directory Database

All databases have a **schema** which is a formal definition (set of rules) which govern the database structure and types of objects and attributes which can be contained in the database. The schema contains a list of all classes and attributes in the forest.

The schema keeps track of:

- Classes
- Class attributes
- Class relationships such as subclasses (Child classes that inherit attributes from the super class) and super classes (Parent classes).
- Object relationships such as what objects are contained by other objects or what objects contain other objects.

The Active Directory database is stored in the **SystemRoot\NTDS** directory. The file "ntds.dit" contains the directory and schema data, and the file "schema.ini" contains the information to control Active Directory security and create the default directory. Changes to the database are stored temporarily in log files in this directory until changes are finalized to the database with replication to other controllers complete.

A **forest** is the set of all domains in an organization's network. It consists of one or more trees, combined with two way transitive trusts. It represents a non-contiguous or disjointed namespace in Active Directory.

A **tree** represents a contiguous name space in Active Directory and consiste of a hierarch of domains.

A **Global Catalog** is a searchable master index with data about all objects in a forest. The schema is stored in the global catalog. Only information required to find an object is stored in the global catalog. When the first domain controller in the forest is established, a default catalog is created automatically on that controller. More than one server can house the global catalog.

An **Organizational Unit (OU)** is an Active Directory container object that contains other organizational units or objects.

Changing the Active Directory Database Structure (Schema)

There are several ways to change the schema of Active Directory:

- Application vendors can provide the capability to change the schema.
- MMC - The Microsoft Management Console snap-in is a tool provided by Microsoft to allow the schema to be changed. The Windows 2000 Administration Tools (ADMINPAK) must be installed. The snap-in is called Active Directory Schema. The group that can use this tool is called "Schema Admins". This is a new group for Windows 2000 just for administering the Active Directory database schema.

Domain Controllers

When Active Directory is installed on a Windows 2000 server computer, that computer becomes a domain controller. Domain controllers are used to authenticate users and control access to objects in the Windows domain. A windows domain is a partial or full organizational structure which may or may not coincide with DNS domains on the internet. Active Directory allows these Windows domains to be structured into a tree relationship using trusts which are described later.

Domain controllers each contain a **"replica"** which is a copy of the domain directory.

Active Directory Objects

Object Types

There are two types of Active Directory groups, each with a different purpose. These are:

- **Security principal groups** - These objects can be assigned permissions and consist of:
  - users
  - groups
  - computers
- **Distribution groups** - Used to group users for applications such as mail.

Object Characteristics

Every object has a:

- **Globally Unique Identifier (GUID)** - Uniquely identifies each object. Its size is **128 bits**.
- **Security Identifier (SID)** - A SID is created by the Windows 2000 security subsystem and assigned to security principal objects.

Active Directory Objects

Active directory may contain all objects listed here and all objects listed that are contained by organizational units (OU).

- **Domain** - The core unit in the Active Directory structure.
- **Organizational Unit** (automatically published) - Other organizational units may be contained inside organizational units.

Leaf objects are objects such as users and computers which cannot contain other objects.

Organizational Units

Organizational Units are called container objects since they help to organize the directory and can contain other objects including other OUs. The basic unit of administration is now organizational units rather than domains. Organizational units allow the creation of **subdomains** which are also called logical domains. Microsoft recommends that there should never be more than 10 levels or organizational unit nesting. Since deeper OU nesting slows directory access, normally there should be no more than three or four levels of nesting.

Organizational units may contain:?

- **Organizational Unit** (automatically published) - Used to create a heirarchy of AD objects into logical business units. Other organizational units may be contained inside organizational units.
- **User** (automatically published) - Individual person
- **Group** (automatically published) - Groups of user accounts. Groups make user management easier.
- **Computer** (Those in the domain are automatically published) - Specific workstations.
- **Contact** (automatically published) - Administrative contact for specific active directory objects.
- **Connection** - A defined one direction replication path between two domain controllers making the domain controllers potential replication partners. These objects are maintained on each server in "Active Directory Sites and Services".
- **Shared folder** - Used to share files and they map to server shares.
- **Printer** (Most are automatically published) - Windows NT shared printers are not published automatically.
- **Site** - A grouping of machines based on a subnet of TCP/IP addresses. An administrator determines what a site is. Sites may contain multiple subnets. There can be several domains in a site. For example, an organization may have branches around the city they are located in. Each location may be a site.
- **Site container**
- **Site link** - Defines the connection between sites. Can indicate the cost of sending data across a network in terms of available bandwidth. It is a list of two or more connected sites. Whether the link will use RPC or SMTP for passing data must be determined before creating the link since it cannot be changed
- **Site link bridge** - Allows one site in a string of sites to replicate through one or two sites to a second or third site. These are only used for fine control of how replication will occur across WAN links.
- **Site settings**
- **Subnet** - A part of a network based on addresses which is usually connected using routers. Subnets must be created in each site object before it is really active. A network address and subnet mask is used to define the subnet.
- **Subnet container**
- **Trusted domain**

Pre-installed Container Objects

Pre-installed container objects provide backward compatibility with Windows NT. They look and act like organizational units and include:

- **Builtin** - Build in local groups.

- **Computers** - Computer accounts created using Windows NT. It is a list of workstations
- **Computer** - Used to manage particular workstations.
- **Domain Controllers** - A list of domain controllers.
- **Foreign Security Principles** - Shows trust relationships with other domains.
- **Users** - Windows NT users.

Object Access

Controlling objects in Active Directory controls access only to objects in Active Directory. Objects outside Active Directory may have their own access control. Permissions on corresponding objects in Active Directory do not affect permissions on external objects. Therefore, the user must have both Active Directory and object access.

When setting object permissions, they can be set so the change applies to all children of the object or only to the object itself. You can also set **child** objects to inherit permissions from their **parent** object. Access to specific object properties can be controlled. Object permissions for users and groups include:

- **Full Control** - Allows full access to the object and its sub objects, with the ability to take ownership of objects and change permissions of objects and sub objects
- **Read** - Allows object contents and properties to be displayed.
- **Write** - Allows object contents and properties to be changed except for modifying permissions, configuring auditing, or taking ownership.
- **Create All Child Objects** - Allows creation of any child objects.
- **Delete All Child Objects** - Allows deletion of any child objects.

Object access is controlled using the Active Directory Users and Computers tool by clicking on "View", "Advanced Features", Click + next to the domain, right click the object, select "Properties", click the "Security" tab, and continue.

Permission Combinations

When user and group permissions that the user is in differ for specific objects the least restrictive permissions normally apply. The only exception to this if the user or group is specifically denied one or more specific permissions to the object. When some permissions are denied, the user will have the most restricrictive denials of permissions apply. If the full control permission is denied to a user or group, that user or group will have no permissions. Explicit permissions set at the child object level override permission denial at the parent level even if the child is set to inherit permissions from the parent.

Object Ownership

Ownership can be taken if a user has the take ownership right to the object or if the user is part of the Domain Admins group. Object access is controlled using the Active Directory Users and Computers tool by clisking on "View", "Advanced Features", Click + next to the domain, right click the object, select "Properties", click the "Security" tab, click "Advanced", and continue.

Active Directory Object Administration Delegation

Management of objects listed in Active Directory can be delegated to other administrators. **Administrative authority cannot be delegated for objects smaller than the Organizational Unit (OU).** There are two ways to delegate object control:

- Find the object in the Active Directory Users and Computers tool, right click on the object, and select "Delegate Control". The Delegation of Control Wizard will start.
- Perform the same action as is done when configuring permissions by using the "View" menu in the Active Directory Users and Computers tool, and click on "Advanced Features".

Object Identifiers

Object identifiers are strings in a dot notation similar to IP addresses. There are authorities that issue object identifiers. Each of these authorities can give an object identifier on a sublevel to other authorities. The **International Standards Organization (ISO)** is the root authority. The ISO has a number of 1. When it assigns a number to another organization, that number is used to identify that organization. If it assigned CTDP the number 469034, and CTDP issued 1 to Mark Allen, and Mark Allen assigned 10 to an application, the number of the application would be "1.469034.1.10".

Object Attribute Syntax

Attribute syntax defines the type of data the attribute contains. The following are attribute syntaxes defined by the oMSyntax numbers 2.2.2.0 through 2.5.5.17

- Undefined - illegal
- Object (DN-DN)
- String (Object ID)
- Case sensitive string
- String not sensitive to case
- Printable string
- Numeric string
- Binary object
- Boolean

- Integer
- Octet string
- Time string
- Unicode string
- Presentation address
- DN string object
- NT-sec-desc - Windows NT security descriptor
- Large integer
- Security ID - Windows NT security ID

Active Directory Object Naming

Active Directory Naming is based on Lightweight Directory Application Protocol (LDAP) (RFC 1777) and Domain Name System (DNS).

Distinguished Name

A **Distinguished Name (DN)** is used to uniquely name an Active Directory Object. All objects can be referenced using a Distinguished Name. A DN has three components:

- **DC** - Domain Component
- **O** - Organization
- **OU** - Organizational Unit
- **CN** - Common Name

The Distinguished name takes the form:

/DC=organization/OU=Dept/CN=Win2kserver1

Where "Organization" is the name of the organization, and "Dept" is the department name.

A **Relative Distinguished Name (RDN)** is assigned by an administrator to an object. A Distinguished Name (DN) is a RDN with the location of the object in Active Directory.

UPN

A **User Principal Name (UPN)** (defined by RFC 822) is an RDN with a FQDN which is used for email and user logon.

The UPN takes the form:

Win2kserver1@Dept.Organization.org/document_name

Where "Organization" is the name of the organization, and "Dept" is the department name.

Important LDAP RootDSE Object Attributes

Active Directory uses the **Lightweight Directory Access Protocol (LDAP)** naming method to name objects. The **RootDSE** search tree can be used to identify the forest root, domain, and

various parts of the Active Directory schema. Important attributes of RootDSE:

- **schemaNamingContext** - Can be used to send a query to locate the schema.
- **subSchemaSubEntry** - Has the location of the subschema. The **subschema** contains classes and attributes in the Active Directory database.

Active Directory Schema

All databases have a **schema** which is a formal definition (set of rules) which govern the database structure and types of objects and attributes which can be contained in the database. The schema contains a list of all classes and attributes in the forest.

The schema keeps track of:

- Classes
- Class attributes
- Class relationships such as subclasses (Child classes that inherit attributes from the super class) and super classes (Parent classes).
- Object relationships such as what objects are contained by other objects or what objects contain other objects.

There is a **class Schema** object for each class in the Active Directory database. For each object attribute in the database, there is an **attributeSchema** object.

Partitions

Active Directory objects are stored in the **Directory Information Tree (DIT)** which is broken into the following partitions:

- **Schema partition** - Defines rules for object creation and modification for all objects in the forest. Replicated to all domain controllers in the forest. Replicated to all domain controllers in the forest, it is known as an **enterprise partition**.
- **Configuration partition** - Information about the forest directory structure is defined including trees, domains, domain trust relationships, and sites (TCP/IP subnet group). Replicated to all domain controllers in the forest, it is known as an **enterprise partition**.
- **Domain partition** - Has complete information about all domain objects (Objects that are part of the domain including OUs, groups, users and others). Replicated only to domain controllers in the same domain.
    - Partial domain directory partition - Has a list of all objects in the directory with a partial list of attributes for each object.

The DIT holds a subset of Active Directory information and stores enough information to start and run the Active Directory service.

Schema Container

The schema container is a special container at the top of the schema partitionand is an object created from the **directory Management Domain (dMD)**. It can be viewed using the MMC "Active Directory Schema" console or the **Active Directory Services Interface (ADSI)** edit utility from the installation CDROM. The distinguished name schema container address is:

/CN=schema/CN=configuration/DC=forest root <domain_name>

Classes and attributes are stored in **classSchema** objects and **attributeSchema** objects respectively.

attributeSchema Mandatory Attributes

These attributes provide information about attributes of another Active Directory object.

- **attributeID** - Identifies the attribute with a unique value.
- **attributeSyntax** - Identifies the object which defines the attribute type.
- **cn** - A unicode string name of the attribute.
- **isSingleValued** - A boolean variable which when true indicates there is only one value for the attribute. If false, the attribute can have several values.
- **LDAPDisplayName** - LDAP unicode name string used to identify the attribute.
- **NTSecurityDescriptor** - The object security descriptor.
- **ObjectClass** - Is always attributeSchema.
- **OMSyntax** - Identifies the object syntax specified by the open object model.
- **SchemaIDGUID** - Unique global ID value of the attribute.

classSchema Mandatory Attributes

These attributes provide information about another Active Directory object.

- **cn** - A unicode string name of the object.
- **DefaultObjectCategory** - A distinguished name of where the object belongs.
- **GovernsID** - A unique number identifying the class.
- **LDAPDisplayName** - LDAP unicode name string used to identify the object.
- **NTSecurityDescriptor** - The object security descriptor.
- **ObjectClass** - Is always classSchema.
- **ObjectClassCategory** - An integer describing the object class type. The class type is one of the following with values in "()" indicating the integer value used to signify them:
  - Abstract class (2) - A class that can't be an object, but is used to pass attributes down to subclasses.
  - Auxillary class (3) - Used to provide structural or abstract classes with attributes
  - Structural class (1) - These classes can have objects created from them and are

the class type that is contained as objects in the directory.
    - Type 88 class (0) - These classes don't have a type and they are class types created before 1993 before class types were established in the X.500 standard.
- **SchemaIDGUID** - Unique global ID value of the class.
- **SubClassOf** - Identifier of the class parent class.

System Attributes

These system attributes can only be changed by the **Directory System Agent (DSA)** which manages the Active directory database.

- **systemAuxillaryClass** - Identifies the auxiliary protected classes that compose the class.
- **systemMayContain** - Optional system protected class attributes.
- **systemMustContain** - Required system protected class attributes.
- **systemPossSuperiors** - Parent system protected classes.

SAM Read Only Attributes

The SAM is the **Security Access Manager**.

- badPasswordCount
- badPasswordTime
- creationTime
- domainReplica
- isCriticalSystemObject
- lastLogoff
- lastLogon
- LockoutTime
- modifiedCount
- ntPwdHistory
- PrimaryGroupName
- revision
- SAMAccountName
- SAMAccountType

Schema Modifications

The schema should only be modified when absolutely necessary. Control mechanisms include:

- The schema operations master domain controller is the only controller that the schema

can be changed from.
- The **Schema console** must have schema modification set to enabled.
- Each schema object has permissions set through the Windows 2000 security model.

Ways to modify the schema include:

- Using an **application programming interface (API)**.
- **Lightweight Directory Interface Format (LDIF)** scripts.
- LDIFDE bulk schema modification tool.
- CSVDE bulk schema update tool.

Document the following when changing the schema:

- Object issuing authority
- Object ID
- Class heirarchy
- NT security descriptor
- LDAP display name
- Common name
- Class attributes

When the schema is changed, the following checks are done by Active Directory:

- Consistency - Makes sure identifiers are unique and mandatory attributes exist. Also existance of superclasses in the schema is checked.
- Safety - Check to be sure Active Directory functionality is not disrupted. Checks the following object types:
    - Category 1
    - Category 2

Active Directory Sites

A **site** is a grouping of machines based on a subnet of TCP/IP addresses. An administrator determines what a site is. Sites may contain multiple subnets. There can be several domains in a site.

Active Directory replication to various sites is performed using Active Directory Sites and Services. (Make section explaining how to use this). Sites and subnets are not related to the structure of the domain.

The following may be created:

- **Sites** - One or more IP subnets. Generally this refers to a physical site such as a portion of the organization in particular city or part of a city which is linked by leased lines or other media to other parts of the organization.
- **Subnets** - Subnets must be created in each site object before it is really active. A network address and subnet mask is used to define the subnet.
- **Site links** - It is a list of two or more connected sites. Whether the link will use RPC or SMTP for passing data must be determined before creating the link since it cannot be changed. Selection IP means selection RPC over IP. Site link information includes:
    - Replication schedule - Specify the times the sites can replicate and how often they attempt replication.
    - Link cost - High for a low bandwidth link. A high cost link gets lower priority. A lower priority link is normally used if there are more than one link to the same location.
    - Member sites - Lists sites that are connected using the site link.
    - Transport Mechanism - RPC or SMTP (Mail) is specified.
        - SMTP (Mail) - It cannon be used for replication inside the same site and is a form of **asynchronous replication**.
        - RPC - Requires more bandwidth than SMTP.

  Bridgehead server - A domain controller that is used to send replication information to one or more other sites across a site link.
- **Site link bridges** - Allows one site in a string of sites to replicate through one or two sites to a second or third site. These are only used for fine control of how replication will occur across WAN links. This is actually done automatically by AD, without fine control. To use this feature, automatic bridging of site links must be turned off. You must have three sites to create a site link bridge since it takes three sites and two site links to make a string of sites.
- **Global catalog servers** - The global catalog is a searchable master index with data about all objects in a forest. The global catalog server maintains this catalog. It:
    - Helps Active Directory resources be located by users.

- During logon, it provides group membership information.

There is one in each domain by default, and the first domain controller in the domain is originally the global catalog server. It is worthwhile to have a global catalog server on each side of a WAN connection if the domain is spread out across a WAN.

If several domain controllers are placed on the network, and later the network is broken into sites, appropriate servers must be manually moved to the appropriate site that they are on. If the domain controller is created after the site is created, the server is placed automatically in the correct site (based on IP address).

Windows 2000 Domains

Domain Structure and Relationships

Terms:

- **Domain tree** - A hierarchial group of one or more domains with one root domain. **Only one domain is required to make a tree.**
- **Parent domain** - One domain above another in a domain tree.
- **Child domain** - One domain below another in a domain tree. The child inherits the domain name of its parent in a DNS hierarchial naming convention. Example: "child.parent.root.com".
- **Forest root domain** The first domain created in a forest.
- **Tree root** - The first domain created in a tree.

Trusts and Trust Relationships

Trust relationship is a description of the user access between two domains consisting of a one way and a two way trust. Terms:

- **One way trust** - When one domain allows access to users on another domain, but the other domain does not allow access to users on the first domain.
- **Two way trust** - When two domains allow access to users on the other domain.
- **Trusting domain** - The domain that allows access to users on another domain.
- **Trusted domain** - The domain that is trusted, whose users have access to the trusting domain.
- **Transitive trust** - A trust which can extend beyond two domains to other trusted domains in the tree.
- **Intransitive trust** - A one way trust that does not extend beyond two domains.
- **Explicit trust** - A trust that an administrator creates. It is not transitive and is one way only.
- **Cross-link trust** - An explicit trust between domains in different trees or in the same tree when a descendent/ancestor (child/parent) relationship does not exist between the two domains.

Windows 2000 only supports the following types of trusts:

- Two way transitive trusts
- One way non-transitive trusts.

This means the two way non transitive trust supported by Windows NT is no longer supported. The way to deal with this is to create two one way trusts in Windows 2000.

Controllers

The program "**dcpromo.exe**" is used to make a Windows 2000 domain member server a domain controller or demote it from domain controller status back to a member server. It can be used to add a domain controller for an existing domain or create a domain controller for a new domain.

Terms:

- **Forest root controller** - The first domain controller created when Active Directory is first installed on any computer if there are no previously installed controllers available on the network.

Active Directory Trusts

Windows NT 4.0 does not support transitive trusts. All windows 2000 Active Directory trusts are transitive by default with trusts existing between parents and children. Transitive trusts do not exist between children even if they are of the same parent. Transitive trusts extend up and down through parents to children to grandchildren and so on. Administrators may create **explicit trusts** between any two domains.

It is good policy for the administrator to set up a root domain with the administrator account. This will allow all child domains to be controlled from that domain.

Domain Controller Data Replication

Replicated data between domain controllers contains:

- **Schema**
- **Configuration data** - Forest, tree, and domain information.
- **Domain data** - Information about all domain objects sent to domain controllers in the domain.

Domain Controllers

Windows NT uses a Primary Domain Controller (PDC) and Backup Domain Controllers (PDC) to control the operations of its domains. The BDC or BDCs back up the operations of the PDC in the event that it fails. Data is constantly replicated between these controllers. Windows 2000

has changed this method of controlling the domain.

Windows 2000 may be operated in one of two modes:

- **Native mode** - In this mode Active Directory interfaces only with Windows 2000 domain controllers and directory service client software. Windows 2000 is more efficient in native mode. In this case, the PDC emulator will get password changes faster.
- **Mixed mode** - Used to support domains where there are still Windows NT domain controllers. Mixed mode occurs when Active Directory interfaces with NT 4.0 BDCs or ones without Windows 2000 Directory Service client software. In mixed mode, computers without Windows 2000 client software must contact the PDC emulator to change user account information

A domain cannot be changed from native mode to mixed mode. An NT domain controller cannot be added to a Windows 2000 network runing in native mode.

Upgrading from Win NT to Win 2000 Domains

1. Upgrade the PDC in the master domain that will be the root domain. Upgrade the PDC to Windows 2000.
2. Use mixed mode for active directory.
3. Upgrade BDCs and servers to Windows 2000.
4. Update client computers in the domain to Windows 2000 or install Directory Service Client on them.
5. Follow the same procedure for each succeeding domain down through the domain tree.
6. Once all updates are complete, the multiple domains may be merged into one or reconfigured using Windows 2000 tools.

When the NT Domain controller is upgraded to Windows 2000, the following changes are made:

- The PDC computer account is placed in the domain controller's AD container object.
- Computer acccounts are placed in the Computers AD container object.
- User acccounts, global groups, local groups, and created groups are placed in the Users AD container object.
- Default groups are put in the Builtin AD container object.

Adding a Computer to a Domain

Requirements:

1. Know the DNS domain name such as "server.department.company.com".
2. Have a computer account or administration privileges to create a computer account.
3. The DNS server and domain controller must be working.

Adding a Child Domain

Before adding a child domain, create a DNS subdomain first.

Active Directory Functions

Flexible Single Master Operations (FSMO)

Windows 2000 Domains work using a **multiple master design** with restricted master operations on a master domain controller. This was done to distribute the load on domain controllers but there are some operations that can only be done on a single or "master" controller.

There are a set of **Flexible Single Master Operations (FSMO)** which can only be done on a single controller. An administrator determines which operations must be done on the master controller. These operations are all set up on the master controller by default and can be transferred later. FSMO operations types include:

- **Schema Master** - Makes changes to the database schema. Applications may remotely connect to the schema master.
- **Domain Naming Master** - Adds or removes domains to or from the forest.
- **PDC Emulator** - When Active Directory is in mixed mode, the computer Active Directory is on acts as a Windows NT PDC. The first server that becomes a Windows 2000 domain controller takes the role of PDC emulator by default. Functions pewrformed by the PDC emulator:
    - User account changes and password changes.
    - SAM directory replication requests.
    - Domain master browser requests.
    - Authentication requests.

  The NTLM protocol is used by the PDC emulator to contact non-Windows 2000 clients and servers for exchange of authentication information. When contacting Windows 2000 servers , the Windows 2000 protocol is used.
- **Relative ID Master (RID Master)** - All objects have a Security Identifier (SID) and a domain SID. The RID assigns relative IDs to each domain controller.
- **Infrastructure Master** - Updates group membership information when users from other domains are moved or renamed. If you transfer this function, it should not be transferred to the domain controller that is the global catalog server. If this is done, the Infrastructure Master will not function.

An **Operation Master** performs one or more of the flexible single master operations listed above.

Windows 2000 client Authentication

When operating in mixed mode, the PDC emulator will allow non Windows 2000 clients to use NTLM authentication protocol rather than Kerberos. If a Windows 2000 client cannot find a Windows 2000 domain controller for logon purposes, it will attempt to contact a Windows NT PDC using the NTLM protocol. If the Windows 2000 client successfully logs on using an NT server, group policy objects cannot be loaded.

Global Catalog Server

The **Global Catalog Server (GCS)** maintains an Active Directory global catalog with information about all objects the forest along with universal groups and group members. It has a copy of all objects in its domain and some objects in other domains. It has a copy of domain local and global groups, but not members of those groups. It provides universal group membership information and allows users to find resources. It is used to search for objects in the forest.

Normally the first domain controller is a global catalog server. The "Active Directory Sites and Services tool: in "Administrative Tools" is used to move the global catalog server or create another one.

A global catalog server must be available or the user cannot logon to the domain unless the user is in the group "Domain Admins".

A Universal group may contain users and groups from any domain in a forest.

Adding more global catalog servers will make searching the forest faster, but more network bandwidth will be required for replication between global catalog servers.

AGDLP rule

AD File Storage

- Database file - Stored in SystemRoot\NTDS\ntds.dit, it holds all AD objects and attributes. Contains these tables:
  - Object table - Has a row for each object in AD.
  - Link table - Stores inter object relationship information.
  - Schema table - Has a list of all objects and their attributes.
- Log file - The following files are stored in the System Rootdirectory in the NTDS folder.
  - Checkpoint log files - Holds pointers to transaction logs that have been committed to the AD database. The file name is edb.chk.
  - Transaction log files - Stores transactions that are either commited or are about to be committed to the AD database. The file name is edb.log. If more than one log file is used the log file name is edbhhhhhh.log where "hhhhhh" is a hexadecimal

based number.

- Patch files - Manages data while backups are done. These files have the file extension ".pat".
- Reserve log files - Reserves hard drive space for transaction log files. The files names are res1.log and res2.log.

Garbage collection

Active Directory performs garbage collection. Deleted AD objects are are tagged with a tombstone rather than being immediately removed. The toumbstone lifetime attribute (default of 60 days) defines how long the tombstoned object will remain in the database until it is deleted.

Active Directory Replication

As mentioned in an earlier section, the Active Directory database is replicated between domain controllers. The data replicated between controllers called "data" are also called **"naming context"**. Only the changes are replicated, once a domain controller has been established. Active Directory uses a **multimaster model** which means changes can be made on any controller and the changes are sent to all other controllers. The replication path in Active Directory forms a ring which adds reliability to the replication.

How Replication is Tracked

- **USN** - Each object has an Update Sequence Number (USN), and if the object is modified, the USN is incremented. This number is different on each domain controller.
- **Stamps** - Each object has a stamp with the version number, timestamp, and the GUID of the domain controller where the change was made

Domain controllers each contain a **"replica"** which is a copy of the domain directory. The **"directory update type"** indicates how the data is replicated. The two types are:

- **Origination update** - A change made by an administrator at the local domain controller.
- **Replicated update** - A change made to the replica because of a replication from a replication partner.

Replication Sequence

Terms:

- **Latency** - The required time for all updates to be completed throughout all comain controllers on the network domain or forest.
- **Convergence** - The state at which all domain controllers have the same replica contents of the Active directory database.
- **Loose consistency** - The state at which all changes to the database are not yet replicated throughout all controllers in the database (not converged).

1. A change is made to the Active Directory database on a domain controller. The attribute of the object and the new USN is written to the database. The entire object is NOT replicated. This is called an **atomic operation** becuase both changes are done, or neither change is done. This is an origination update. There are four types:
    - Add - An object is added to the database.

    - Delete - An object is deleted from the database.
    - Modify - An object in the database has its attributes modified.
    - Modify DN - An object is renamed or moved to another domain.
2. The controller the change was made on (after five minutes of stablilty), notifies its replication partners that a change was made. It sends a change notification to these partners, but only notifies one partner every 30 seconds so it is not overwhelmed with update requests. Each controller, in turn, when it is updated, sends a change notice to its respective replication partners.
3. The replication partners each send an update request with a USN to the domain controller that the change was made on. The USN identifies the current state of the domain controller making the change. Each change has a unique USN. This way the domain controller that has the change knows the state of the domain controller requesting the changes and only the changes are required to be sent. The time on each controller, therefore, does not need to be synchronized exactly although timestamps are used to break ties regarding changes.
4. Changes are made through replication partners until all partners are replicated. At some point, replication partners will attempt to replicate partners that are already updated. This is where propagation dampening is used.

If no changes have been performed in six hours, replication procedures are performed to be sure no information has been missed.

Information sent during an update includes:

- Updated object
- The GUID and USN of the domain server with the originating update.
- A local USN of the update on the updated object.

Replication Path

The replication path that domain controller Active Directory replicated data travels through an enterprise is called the **replication topology**. **Connection objects** are used to define the replication paths between domain controllers. Active Directory, by default, sets up a two way ring replication path. The data can travel in both directions around the ring which provides redundancy and reliability. Two types of replication occur in the path:

- **Direct replication** - When replication is done from a primary source of data.
- **Transitive replication** - When replication is done from a secondhand or replicated source of data.

The Knowledge Consistency Checker (KCC) (running on all domain controllers) generates the replication topology by specifying what domain controllers will replicate to which other

domain controllers in the site. The KCC maintains a list of connections, called a **replication topology**, to other domain controllers in the site. The KCC ensures that changes to any object are replicated to all site domain controllers and updates go through no more than three connections. Also an administrator can configure connection objects.

The KCC uses information provided by the administrator about sites and subnets to automatically build the Active Directory replication topology.

Propagation Dampening

Terms:

- **Propagation dampening** is used to prevent unnecessary replication by preventing updates from being sent to servers that are already updated. Each domain controller keeps a list of other known domain controllers and the last USN received from each controller. Two **up-to-date vector** numbers support this:
  - Replica GUID
  - Update Sequence Number (USN) - Mentioned earlier it is incremented anytime an origination or replicated update is received. The USN stored is from the originating server. It is stored as **metadata** with:
    - An attribute indicating "added" or "changed" for the object being updated.
    - The GUID (above).
    - A local USN for the object attribute changed.
    - The changed data.

    The **up-to-date vector** numbers are incremented when replication occurs with the originating server. Each domain controller has its own different USN (They may not start at the same number). The highest USN from each domain controller that is stored in other domain controllers is called the **high watermark** for that domain controller.
- **Propagation delay** describes the amount of time required for a change to be replicated to domain controllers throughout the domain.
- **Ring Topology** - The Active Directory replication process uses a **ring topology** where the replication partners form a ring. This adds reliability to the process and also helps decrease propagation delay.

The information sent in an update request includes the high water mark entry for the originating server for the last change received. If the highwater mark received from the server that sent the update request is the same as the highwatermark for the originating server on the server receiving the request, the receiving server will not send the replicated information.

The **usnChanged** parameter is the highest USN number for any object.

Replication Partitions

Types of Active Directory data storage categories which are called partitions:

- **Schema partition** - Defines rules for object creation and modification for all objects in the forest. Replicated to all domain controllers in the forest. Replicated to all domain controllers in the forest, it is known as an **enterprise partition**.
- **Configuration partition** - Information about the forest directory structure is defined including trees, domains, domain trust relationships, and sites (TCP/IP subnet group). Replicated to all domain controllers in the forest, it is known as an **enterprise partition**.
- **Domain partition** - Has complete information about all domain objects (Objects that are part of the domain including OUs, groups, users and others). Replicated only to domain controllers in the same domain.
    - Partial domain directory partition - Has a list of all objects in the directory with a partial list of attributes for each object.

These partitions are all replicated between domain controllers by Active directory. Different partitions may be replicated between different replication partners.

Replication Conflict

Replication conflict occurs when changes are made to the same object and attribute before the changes can be replicated throughout all domain controller's copies of the database. Additional data (metadata) stored for each object attribute includes (not related to USN):

- **Time stamp** of the last change.
- **Attribute version number** - For each object's attributes, this value is the same on all domain controllers.

When an Active Directory database update is received on a domain controller, one of the following happens:

- If the update attribute version number is higher than the current version number on the controller, the new value of the attribute is stored and the version number is updated.
- If the update attribute version number and stored attribute version number are the same, timestamps are used to resolve the conflict.
- If the both version numbers and both timestamps are the same, the update from the controller with the highest GUID is used.

File Replication Service

In Windows 2000, the SYSVOL share is used to to authenticate users. The SYSVOL share includes group policy information which is replicated to all local domain controllers. **File replication service (FRS)** is used to replicate the SYSVOL share. The "Active Directory Users and Computers" tool is used to change the file replication service schedule.

Intrasite Replication

Replication that happens between controllers inside one site. All of the subnets inside the site should be connected by high speed network wires. Replication between two sites may need to be sent over a slower WAN link or leased line. Intrasite replication data is sent uncompressed.

Site replication is done using **Remote Procedure Call (RPC)**. If a change is made, replication occurs within five minutes, and replication is done every six hours if no changes were made. Domain controllers that receive updates replicate that information to other domain controllers on their route list. All changes are therefore completed within a site within 15 minutes since there can only be three hops.

The topology used here is the ring topology talked about earlier and this replication is automatically set up by Active Directory, but may be modified by an administrator.

DNS Replication

The DNS IP address and computer name is stored in Active Directory for Active Directory integrated DNS zones and replicated to all local domain controllers. DNS information is not replicated to domain controllers outside the domain.

Intersite Replication

Intrasite replication is replication between sites and must be set up by an administrator.

Replication Management

The administrative tool, "Active Directory Sites and Services", is used to manage Active Directory replication. Replication data is compressed before being sent to minimze bandwidth use. There are two protocols used to replicate AD:

- Normally **Remote Procedure Call (RPC)** is used to replicate data and is always used for intrasite replication since it is required to support the FRS. RPC depends on **IP** (internet protocol) for transport.
- **Simple Mail Transfer Protocol (SMTP)** may be used for replication between sites.

SMTP can't replicate the domain partition, however. Therefore the remote site would need to be in another domain to be able to effectively use SMTP for carrying replication data.

Bridgehead server - A domain controller that is used to send replication information to one or more other sites.

Flexible Single Master Operations (FSMO) (discussed in an earlier section) can be transferred manually to various domain controllers. Roles and tools used to transfer are:

- **Schema Master** - Use "Active Directory Domains and Trusts". Makes changes to the database schema. Applications may remotely connect to the schema master.
- **Domain Naming Master** - Use the MMC "Active Directory Schema Snap-in". Adds or removes domains to or from the forest.
- **Primary Domain Controller (PDC) Emulator** - Use the "Active Directory Users and Computers" administrative tool. When Active Directory is in mixed mode, the computer Active Directory is on acts as a Windows NT PDC. Mixed mode occurs when Active Directory interfaces with NT 4.0 BDCs or ones without Windows 2000 Directory Service client software. In mixed mode, computers without Windows 2000 client software must contact the PDC emulator to change user account information.
- **Relative ID Master (RID Master)** - Use the "Active Directory Users and Computers" administrative tool. All objects have a Security Identifier (SID) and a domain SID. The RID assigns relative IDs to each domain controller.
- **Infrastructure Master** - Use the "Active Directory Users and Computers" administrative tool. Updates group membership information when users from other domains are moved or renamed.

Any master role can be transferred by using the command line program, ntdsutil.exe. When a server performing a master role fails and goes offline, you can perform "seizing master operations" to have another server perform that role. Only the ntdsutil.exe program can perform this function. Commands include:

- connections - A connections prompt appears:
  - connect to server "FQDN of server to connect to"
  - quit
- sieze "name of role to transfer". Role names are:
  - PDC
  - RID master
  - schema master
  - domain naming master
  - infastructure master

  Example: "sieze RID master"

Replication Associated Performance Monitor Counters

- **DRA Inbound Bytes Not Compressed** - Replicated uncompressed bytes that are probably from a Directory Services Agent (another controller sending data) in the same site.
- **DRA Inbound Bytes Compressed (Before Compression)** - Replicated bytes received (as though in uncompressed form).
- **DRA Inbound Bytes Not Compressed (After Compression)** - Replicated bytes received (as in compressed form).
- **DRA Inbound Bytes Total** The sum of the DRA Inbound Bytes Not Compressed plus the DRA Inbound Bytes Not Compressed (After Compression).
- **DRA Outbound Bytes Not Compressed** - Replicated uncompressed bytes that are being sent to another domain controller in the same site.

Schema Cache

A schema cache which is a copy of the schema in memory can be used to speed up schema queries but should be used sparingly due to the high memory requirements. If the schemaUpdateNow attribute is added to the RootDSE a schema cache update is done immediately. Normally the schema cache is stored in memory when the system boots and updated every five minutes.

Windows 2000 DNS

In Windows 2000, DNS is required to use Active Directory.

Domain Name Service is used to change internet domain and computer computer names into IP addresses and vice versa. DNS works at the application layer and uses TCP and UDP for transport. TCP is only used if returned data is truncated. See the DNS section in the Networking Guide for information about DNS. DNS was originally based on HOSTS files that were maintained by a centralized Network Information Center. Today of is based on a hierarchy of servers with a distributed hierarchial database throughout the network or internet.

DNS Levels

DNS is a hierarchial naming structure with the following levels:

- Root designated by a dot (.).
- First level - This indicates country or type of organization such as "org", "com", and "net".
- Second level - Indicates the organization name and can be purchased for a yearly fee.

Notice that the highest level of the domain is listed last. An example of a domain name that you may be familiar with is:

comptechdoc.org.

DNS Operation

DNS Servers

On the client side, a DNS resolver is used to send queries to DNS servers. The resolver is normally part of a library routine or it is built into the application. DNS uses zone files to keep name and IP address database information for the internet domain or hierarchial set of domains. Zones are a storage of information in a file for a DNS domain or DNS subdomains (DNS domains are not the same as Windows domains). DNS does not yet support dynamic configuration but has been modified for Windows systems to do so. Different aliases may be created by the administrator for the same host. Three types of name servers as defined by how it relates to the zone information:

- **Primary** - Locally stored files exist on the name server data base. The master zone file

copy is stored here.
- **Secondary** - Gets data called a zone transfer from another server that is the zone authority.
- **Caching Only** - Caches name server information and does not contain its own files.

A primary and secondary name server should be used on a network. **When a zone is defined, some server must be configured to be a master name server for the zone**. There can be different master name servers for different zones. The master server provides copies of the zone information to the secondary DNS server. Name servers can be configured to get information from other name servers when the information is not found in the local database. These types are forwarders and slaves. Name servers as categorized by function:

- **Master** - The zone authority that contains the master zone files.
- **Forwarders** - A name server that passes name resolution requests to other name servers. This configuration is done on a per server basis.
- **Slaves** - Slave name servers are configured to use forwarders.

Windows introduces additional terminalogy:

- **Standard primary** - The same as a primary DNS server listed above. This is a master server by function.
- **Active Directory Integrated** (primary) - DNS entries are stored with Active Directory data rather than a normal zone file. More than one of these Active Directory primary servers may exist due to Active directory replication. This term is used to refer to both the Active Directory Integrated zones and files that support the zone.
- **Standard secondary** - The same as a secondary DNS server listed above. This is a slave server by function.
- **Root server** - The server that has the DNS data for the root zone. The root zone is the organization internal network root zone or internet root zone. It is used when a private network is not directly on the internet (no connection or via proxy server).

If the DNS server is connected to the internet, the DNS Server Wizard will not allow the DNS server to be configured as a root server.

Queries

Query types are:

- **Inverse** - Getting the name from the IP address. These are used by servers as a security check.
- **Iterative** - Server gives its best answer. This type of inquiry is sent from one server to another.

- **Recursive** - Cannot refer the query to another name server.

Zone Transfers

The DNS zone file serial number is used to trach DNS changes. The notify function is used to initiate zone transfers. Zone transfer types are:

- **Full** - AXFR Query - Secondary server refresh interval expires and it sends an AXFR qurey.
- **Incremental** - IXFR query - Only new or updated entries are copied.

DNS Zones

Possible zones include:

- **Forward lookup zone** - Name to IP address map.
- **Reverse lookup zone** - IP address to name map.
- **Standard primary zone (primary zone)** - A master copy of a forward or reverse lookup zone.
- **Active Directory integrated zone** - A copy of a standard primary or Active Directory integrated zone. The IP address and computer name is stored in Active Directory and replicated to all local domain controllers. DNS information is not replicated to domain controllers outside the domain.
- **Standard secondary zone (secondary zone)**

Microsoft DNS

Microsoft DNS is compatible with BIND, but it is not the same. Microsoft supports RFCs 1033, 1034, 1035, 1101, 1123, 1183, 1536, 2052, and 2136. RFC 1996 addresses DNS notify issues. RFC 2065 defines DNS security extensions. Windows 2000 Server or more advanced server is required to run DNS. It will not run on Windows 2000 Professional.

Windows 2000 DHCP clients register forward lookup entries (A record) by default. The DHCP server registers forward (A) and reverse (PTR) DNS records.

Windows 2000 computers can register their IP address and names with the network DNS server that supports dynamic updates (Not all DNS servers support dynamic updates, but Windows 2000 DNS servers do). Other operating systems other than Windows 2000 can not register their IP address and names with DNS dynamically. A Windows DHCP server can be configured to register assigned IP address and host names with the DNS server which can support dynamic updates. Heres the procedure on the DHCP server:

1. Run the administrative tool, "DHCP" and highlight the DHCP server.
2. Select "Action" and "Properties".
3. Click the DNS tab.
4. Select the checkbox, "Enable updates for DNS clients that do not support dynamic update". Select the "Always update DNS" checkbox to have the DHCP server update DNS, even for Windows 2000 systems.

Installing DNS

1. Configure the computer to use a static IP address for each local area connection. In the Control Panel use the "Network and Dial-Up Connections" applet, right click on "Local Area Connections", select "Properties", "Internet Protocol (TCP/IP)", and set the IP address.
2. Configure the computer to use a primary DNS suffix. Right click "My Computer", select "Properties", click the "Properties" tab, click "more" in the "Identification Changes" box and type the FQDN in the NETBIOS Computer Name and DNS Suffix boxes.
3. Install the DNS Server Service by putting the Windows 2000 appropriate Server install CD in the CD-ROM drive, then open the "Add/Remove Programs" applet in the control panel. In the Windows Components Wizard, highlight "Networking Services", click "Details", check "DNS", and continue.

Configuring DNS

Configure DNS from the "DNS" selection of Administrative tools. Do the following:

1. Configure the DNS server to be its own client so it can resolve other computer names and IP addresses. In the Control Panel use the "Network and Dial-Up Connections" applet, right click on "Local Area Connections", select "Properties", "Internet Protocol (TCP/IP)". Enter the IP address of the DNS server. for the preferred DNS server. Click "Advanced and "DNS" tab in the "Advanced TCP/IP Settings" box. Type the FQDN of the DNS server.
2. Configure a root server (if required) if internet access is not available or the connection is through a proxy server. This is done from the "DNS" selection of "Administrative Tools". Highlight the computer, then select "Action", and "Configure the Server".
3. To configure properties perform the same action as in the item above, but select "Properties" after the "Action" selection. Here the Interfaces (network cards) that will provide the DNS service can be set or limited. Also IP addresses that are allowed service can be set. Advanced Options include:
    - DNS process recursion can be enabled or disabled. - This means the processes of trying to satisfy a query is repeated until a solution is found. This is enabled by default causing DNS servers to contact other servers to resolve queries.

- BIND secondaries - Zones are transferred to secondary servers from master servers. Enabled by default
- Fail on load if bad zone data - A zone with bad data is not used. This is not enabled by default.
- Enable round robin - Used to balance loads when multiple servers have the same name and configuration with different IP addresses. A different IP address can be provided to clients when the host name is requested.
- Enable netmask ordering - This is for hosts with multiple network cards and is resolved with the address that is on the same subnet of the client. This option is selected by default and if it is not selected, round robin policy is used.
- Secure cache against pollution - Normally all DNS server information due to queries is cached for further use. This option only allows the final answer to be cached.
- Name Checking - The options are Strict RFC (ANSI), Non-RFC (ANSI), and Multibyte (UTF8). Multibyte is the default.
- Load zone data on startup - Determines where data is loaded when the DNS service starts. It can be from Active Directory and registry, from file, or from the registry.
- Enable automatic scavenging of stale records - Old resource records on zones may be deleted if older than a set amount of time.

The root hints tab is used to associate internet or the organizations root servers names and IP addresses. Root hints is not configurable on a root server.

4. To configure other properties select "Start", "Administrative Tools", "DNS", click the plus by the DNS server name, then click + next to the Forward or Reverse Lookup Zones. Highlight the **zone** to configure and select "Action" and "Properties". Tabs include:
   - General - Set zone file name and allow or not allow dynamic updates. Set whether stale resource records are scavenged, no-refresh interval time, and refresh interval time. This allows old records in the zone to be deleted. The refresh interval is the amount of time to wait before scavenging the record.
   - Start of Authority (SOA)
   - Name Servers
   - WINS - Configure DNS to use WINS.
   - Zone Transfers - Sets the servers the Active Directory DNS Zone transfers are sent to.

Configuring Zones

This is done from the "DNS" selection of "Administrative Tools". Click the + next to the DNS server name, Highlight the "Forward Lookup Zones (or "Reverse Lookup Zones") folder, then select "Action", and "New Zone".

The **Start of Authority (SOA)** record defines the authoritative server for the DNS zone. SOA properties are:

- **Serial number** - If less than master's SN, the slave will get a new copy of this file from the master.
- **Primary server**
- **Responsible person**
- **Refresh interval** - The time in seconds between when the slave compares this file's SN with the master.
- **Retry Interval** - The time the server should wait before asking again if the master fails to respond to a file update (SOA request).
- **Expires after** - Time in seconds the slave server can respond even though it cannot get an updated zone file. Needs to be longer than the refresh interval.
- **Minimum TTL** - The time to live (TTL) in seconds that a resolver will use data that was received from a nameserver before it will ask for the same data again.

Monitoring DNS

Select "Start", "Programs", "Administrative Tools", "DNS". Highlight the DNS server name, select "Action", "Properties" and click the Monitoring tab. Tabs include:

- Interfaces
- Forwarders
- Advanced
- Root Hints
- Logging - Used to set logging options to be sent to the file SystemRoot\system32\dns \dns.log. Options representing DNS events are Query, Notify, Update, Questions, Answers, Send, Receive, UDP, TCP, Full packets, and Write through.
- Monitoring - Select and perform tests such as a simple query to this DNS server or a recursive query to another DNS server.

The event log will also show and DNS problems. The "Event Viewer" is an administrative tool.

Zone Properties Dialog Box

Tabs:

- General - Sections:
  - Status - The status is indicated and a "Pause" button allows DNS to be paused.
  - Zone type - Has a "Change" button that allows setting the zone type to one of standard primary, standard secondary, and Active Directory integrated.
  - Allow dynamic updates - Updates can be allowed from DHCP servers.
- Start of Authority (SOA) - Correspond to the SOA properties listed above.

    - Serial number
    - Primary server
    - Responsible person
    - Refresh interval
    - Retry interval
    - Expires after
    - Minimum (default) TTL
    - TTL for this record - Defines the TTL for the SOA record.
- Name Servers
- WINS - Controls whether WINS is used to resolve names in this zone.
- Zone Transfers - Determines how requests for zone transfers from other servers are handled. These are the choices:
    - No zone transfers.
    - Allow zone transfers only to specified servers listed in this tab.
    - Allow zone transfers to servers listed in the name servers tab only.
    - Allow zone transfers to any server.
- Security

Configuring DNS

Characters allowed in DNS names are:

A-Z a-z 0-9 -

The characters / . _ are illegal. Configuration keywords:

- **Interfaces** - Specifies interfaces to use on a multihomed host.
- **Forwarders** - Specifies other name servers to use as a forwarder.
- **Boot Method** - Display whether the boot method is through the use of the registry or data files.

DNS files are stored in:

\WINNTROOT\System32\DNS

Hosts File

The Hosts file at **\SystemRoot\system32\drivers\etc** can act as a replacement for DNS which is a file containing IP addresses and DNS names for hosts. Files in this directory include:

- **Hosts**

- **Protocol**
- **Lmhosts** - NetBIOS name to IP address.

DNS Tools

- NSLOOKUP - It is run from the command prompt. Syntax:

  nslookup [-options] [searchname] [-server]

  To see options, "Help" can be typed at the NSLOOKUP command prompt .

The DNS Database

Below is a partial explanation of some records in the database. An example /var/named/db. mycompany.com.hosts file is listed below.

```
mycompany.com.          IN      SOA     mymachine.mycompany.
com.    root.mymachine.mycompany.com. (
                1999112701          ; Serial number as date
and two digit number YYMMDDXX
                10800               ; Refresh in seconds
28800=8H
                3600                ; Retry in seconds 7200=2H
                604800              ; Expire 3600000=1 week
                86400 )             ; Minimum TTL
86400=24Hours
mycompany.com.                  IN      NS      mymachine.
mycompany.com.
mycompany.com.                  IN      MX
10              mailmachine.mycompany.com.
mymachine.mycompany.com.        IN      A       10.1.0.100
mailmachine.mycompany.com.      IN      A       10.1.0.4
george.mycompany.com.           IN      A       10.1.3.16
```

Below are listed some of the entries with explanations:

- Serial number - If less than master's SN, the slave will get a new copy of this file from the master.
- Refresh time - Time between checks to see if the master has a new database.
- Retry Time - The time a secondary waits to try a new zone transfer
- Expiration time
- TTL - Time to live is the amount of time a DNS server may cache the entry that was

received from another DNS server.

Database file storage on MIcrosoft Windows 2000 is as follows:

- Database file - zone.dns
- Cache file - Cache.dns - Used to resolve names outside the domains. Contains the addresses of root name servers.
- Reverse lookup file and Arps-127.rev
- Boot file (options) - Defines BIND startup options such as the directory DNS files are contained in. Bootfile commands:
    - Cache - The cache file location. The file must exist.
    - Primary - Syntax is "primary (domain) (filename)" - The domain indicates the domain that this authoritative server is in charge of. The filename indicates theresource record file for the zone.
    - Secondary - Syntax is "secondary (domain) (hostlist) - The domain indicates the domain the server is authoritative for. The hostlist is a list of master servers where zone information is downloaded from.

DNS Record types:

- **A** - Address record allowing a computer name to be translated into an IP address. Each computer must have this record for its IP address to be located. These names are not assigned for clients that have dynamically assigned IP addresses, but are a must for locating servers with static IP addresses.
- **AAAA** Host resource record for IPv6 protocol.
- **AFDSB** - Andrew File System Database resource record
- **ATMA** - Asynchronous Transfer Mode resource record.
- **CNAME** - Canonical name allowing additional names or aliases to be used to locate a computer.
- **HINFO** - Host information record with CPU type and operating system.
- **ISDN** - Integrated Services Digital Network resource record.
- **MB** - Mailbox resource record.
- **MG** - Mail group resource record.
- **MINFO** - Mailbox mail list information resource record.
- **MR** - Mailbox renamed resource record.
- **MX** - Mail Exchange server record. There may be several.
- **NS** - Name server record. There may be several.
- **PTR** - Pointer resource record.
- **RP** - Responsible person.
- **RT** - Route through resource record for specifying routes for certain DNS names.
- **SOA** - Start of Authority record defines the authoritative server and parameters for the DNS zone. These include timeout values, name of responsible person,

- **SRV** - Service locator resource record to map a service to servers providing the service. Windows 2000 clients will use this record to find a domain controller.
- **TXT** - Test resource record for informative text.
- **WKS** - Well known service resource record.
- **X25** - To map a host name to an X.25 address.

Country codes include:

- de - Germany
- nz - New Zealand

Active Directory Security

The following components are used to implement Active Directory security:

- **Security Descriptors** - Every object has a security descriptor which:
  - Defines the permissions that can be assigned to the object or object type.
  - Contains the object owner security identifier (SID) which identifies the owner (security principle) of the object.
  - Contains any group security identifiers (SID) which is used for compatability with systems not created by Microsoft.

  Access Control Lists that are contained in security descriptors:
  - Discretionary Access Control List (DACL) - Contains security principle SIDS that have permission for an object.
  - Security Access Control List (SACL) - Defines auditable events for specific objects.
- **Security Identifiers (SIDs)** - These are always unique numbers within a forest which are used to identify security principle objects. There are two SID types:
  - Owner SID
  - Group SID

  There are two parts of a SID which are:
  - Domain - Identifies the domain the object was created in.
  - Relative Identifier (RID) - Specifies the domain account object the object was created in.
- **Security Principles** - Objects that can have permissions assigned to them and each contain security identifiers. The following objects are security principles:
  - User
  - Computer
  - Group

Permission Inheritance

Objects inherit the permissions of the organizational unit that they were created in. Permissions can be applied to container objects such that they apply to:

- Only the object.
- The object and all its children.
- Only the children objects.
- Only specific child object types such as folders.

If inheritance is blocked from the container object, either previously inherited permissions are

copied to the objects in the parent, orpreviously inherited permissions are removed from child objects meaning permissions must be manually set.

If an object is moved to another container object, the permissions directly assigned to that object remain. Any inherited permissions are lost and the object inherits permissions from its new container object unless inheritance is blocked.

SYSVOL Share

In Windows 2000, the SYSVOL share is used to to authenticate users. The SYSVOL share includes group policy information which is replicated to all local domain controllers.

Access Control Lists

Every Active Directory object has an access control list (ACL). ACEs (Access control entries) are entries in an access control list (ACL). Each ACE contain security IDs for users and groups (security principles) along with the associated permissions for that user or group ID.

Active Directory Installation

Active Directory must be installed on Windows 2000 servers that are to be Windows 2000 domain controllers. It can be installed on Windows 2000:

- Server
- Advanced Server
- Datacenter Server.

When Active Directory is installed on a computer, that computer is promoted by Active Directory to a domain controller. If the computer is the first domain controller, it creates an Active Directory database. If it is not the first, it gets a read and write copy of the AD database.

Requirements

- The computer must be Windows 2000 Server, Advanced Server or Datacenter Server.
- At least one volume on the computer must be formatted with NTFS.
- DNS must be active on the network prior to AD installation or be installed during AD installation. DNS must support SRV records and be dynamic.
- The computer must have IP protocol installed and have a static IP address.
- The Kerberos v5 authentication protocol must be installed.
- Time and zone information must be correct. **Simple Network Time Protocol (SNTP)** (RFC 1769) synchronizes time on network computers (nodes)

Installation Process

You can install Active Directory by selecting "Start", "Run", and typing "Dcpromo.exe" in the text box or follow the following selections:

1. Click "Administrative Tools".
2. Select "Configure Your Server".
3. Select "Active Directory Installation Wizard".

Directory Service Client

On non Windows 2000 systems, the Directory Service Client can be installed which will allow those systems to:

- Search the Active Directory.

- Change passwords on domain controllers.
- Use D6 shares that are fault tolerant.

Internet Explorer 4.01 or later must be installed on any system that the Directory Service Client is to be installed on in order for the install wizard to run. To install Directory Service Client:

1. Place the Windows 2000 CD in the CDROM drive.
2. Indicate that you do not want to upgrade Windows and close the dialog box.
3. Open a DOS prompt and change drives to the drive letter of the CDROM drive,
4. Type "cd \clients\win9x" and type "dsclient".
5. Follow the wizard prompts to complete the installation.

DNS

DNS is required to use Active Directory since clients use DNS to locate Active Directory controllers. Servers and client computers register their names and IP addresses with the DNS server. The DNS server must support **Service Resource Records (SRVs)** according to RFC 2052 and **dynamic update protocol** according to RFC 2136. DNS can be installed with the Active Directory server or on a separate DNS server.

Active Directory Installation Effects

- The server becomes a domain controller.
- A new Windows 2000 domain is created.
- A new domain tree and forest is created.

In each child domain, Active Directory must be installed on the first domain controller.

Verification of Active Directory

Select "Start", "Programs", "Administrative Tools", "Active Directory Users and Computers" and click the + next to the domain. Highlight the domain controllers folder, and the computer Active Directory was installed on should appear in the right pane.

Active Directory Configuration

Active Directory Users and Computers

Active Directory Users and Computers is a Microsoft Management Console snap-in. It is started by selecting "Start", "Programs", "Administrative Tools", and "Active Directory Users and Computers". Only members of the Domain Admins or Enterprise Admins group can use this tool. This tool is used to create, configure, locate, move, and delete objects including:

- **User** (automatically published)
- **Group** (automatically published)
- **Computer** (Those in the domain are automatically published)
- **Contact** (automatically published)
- **Domain**
- **Organizational Unit** (automatically published)
- **Shared folder**
- **Printer** (Most are automatically published) - Windows NT shared printers are not published automatically.

It is also used to publish resources, control security and access to objects, and set up administrative control of objects to users. Published resources allow users to find and use them without knowing what server they reside on. Most browse lists do not cross subnet boundaries, but published resources are seen across subnets. These published resources may be browsed from "My Network Places". The "Computer Management" administrative tool or "Active Directory Users and Computers" is used to publish resources in Active Directory.

Active Directory Administration

Active Directory is normally administered from domain controllers but can be administered from a Windows 2000 Professional workstation by using the ADMINPAK tool. It is on the Windows 2000 CDROM in the directory /i386/Adminpak.msi.

Action Items that can be selected from the domain:

- New
  - Shared Folder
  - Printer
- Find

View Menu items:

- Advanced Features - Used to set object permissions.

When using Active Directory Users and Computers, once the domain is highlighted, the following options are available by selecting the menu item, "Action", and "New".

- Organizational Unit

To configure an object, click the + next to the domain name, and highlight the object. The following selections are available by selecting "Action":

- Properties

Searching With Windows Explorer

Windows Explorer can be used to search for Active Directory objects. This is done by selecting "View", Explorer Bar", and "Search".

Publishing Resources

Publishing is the act of making an object publically browseable and accessible using Active directory. Most objects are automatically listed in Active Directory when they are created, but some objects must be published to be made available. Things that are not automatically published:

- Windows NT shared printers
- Computers outside the domain.

Moving AD Objects

From Active Directory Users and Computers click the + next to the domain name, and highlight the object. Right click on the object in the right pane to be moved, and select Move. Expand any container objects required, and highlight the container to move the object to, then click "OK".

To move an object to another directory, use the command line program called MoveTree.exe. This program is part of the "Windows 2000 Support Tools "on the Windows 2000 Server or above CD in \Support\Tools.

Changes

When a user is moved from one OU to another the following is true:

- The user inherits permissions from the new OU.
- The user loses permissions from the original OU.
- The users and groups that could manage the user still can manage the user.

The MoveTree.exe tool is used to move an OU from one domain to another.

The "Delegation of Control Wizard" or "Active Directory Users and Computers" can be used to delegate OU administrative control to a specific user.

Active Directory Performance

The System Monitor object NTDS is useful for monitoring domain controller performance. The below counters in the Performance Monitor tool show replication traffic information.

- **DRA Inbound Bytes Total/sec**
- **DRA Outbound Bytes Total/sec**
- **DRA Inbound Bytes Not Compressed** - Replicated uncompressed bytes that are probably from a Directory Services Agent (another controller sending data) in the same site.
- **DRA Inbound Bytes Compressed (Before Compression)** - Replicated bytes received (as though in uncompressed form).
- **DRA Inbound Bytes Not Compressed (After Compression)** - Replicated bytes received (as in compressed form).
- **DRA Inbound Bytes Total** The sum of the DRA Inbound Bytes Not Compressed plus the DRA Inbound Bytes Not Compressed (After Compression).
- **DRA Outbound Bytes Not Compressed** - Replicated uncompressed bytes that are being sent to another domain controller in the same site.

Active Directory Replication Monitor

The Active Directory Replication Monitor is used to monitor Active Directory database replication between domain controllers.

The Active Directory Replication Monitor is one of the Windows 2000 support tools. Install it from the Windows 2000 Server installation CD. When the menu comes up, select browse, and double click each of "SUPPORT", "TOOLS" and "SETUP". Enter appropriate information when prompted to complete the Windows 2000 Support Tools installation.

The Active Directory Replication Monitor is run by selecting "Start", "Run", and typing "replmon" on the command line. You can add monitored servers to its monitor list. Replication can be forced by right clicking on a partition, then selecting "Synchronize this Directory Partition with All Servers".

Some of the following functions can be done with Active Directory Replication Monitor.:

- Manually make two domain controllers replicate Active Directory database information between each other.
- View replication partner information.
- View unreplicated objects, list object metadata, and find out why a replication attempt

may have failed.
- Log and monitor the domain or forest replication state and statistics.
- Change replication time intervals.
- Setup the system response to exceeding replication thresholds. The system response may be to log the event or send an e-mail.

Network Monitor

This tool can be used to observe replication data and help with diagnosis of any replication problems. TCP port 25 is monitored to observe replication using mail transfers. When RPC is used for replication, which is the normal method, the following entry in the registry may be modified to a particular port number to cause RPC traffic to use the same port:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\NTDS\Parameters\TCP/IP Port

Active Directory Queries

LDAP queries are used by Active Directory to find objects and the query is passed from domain controller to domain controller until the object is found. Active directory objects must be in the current tree for an LDAP query to find the object.

Adding more global catalog servers will make searching the forest faster, but more network bandwidth will be required for replication between global catalog servers.

Windows 2000 Installation

See the introduction for information about minimum system requirements. All hardware on the system should be in the Microsoft Hardware Compatibility List (HCL) as listed at http://www.microsoft.com/hcl. The HCL file is also on the installation CDROM at \Support\hcl.txt.

Windows 2000 supports plug and play devices so the Windows NT Hardware Qualifier (NTHQ) program is not included with Windows 2000.

Install Methods

Ways to install Windows 2000:

- From CDROM - Boot the computer from the CDROM or from the Windows 2000 Setup Boot Disks. The **makeboot.exe** program on the CDROM "Bootdisk" folder can be used to create setup disks from the installation CDROM.
- Winnt.exe - Used from a CDROM that is not on the HCL or do the installation over the network.
- Winnt32.exe

Stages of the Install

1. Text mode - "You specify whether Setup should install Win2K Server or upgrade another Windows platform, accept the licensing agreement, and select an installation partition. "
2. GUI phase - "You must enter the product key, along with a user and organization name. You specify regional settings and a password in this stage."
3. Networking - "Networking settings and components are detected, installed, and configured along with workgroup and domain membership information. "
4. Final Setup - "Start menu programs are installed, components are registered, and temporary setup files are removed."

Winnt

Winnt is used to install NT on computers running 16 bit operating systems such as DOS, Windows3.x, or even Windows 95. Winnt.exe is used to start an installation of Windows 2000 over ae network. Winnt32 is used to install NT when running an NT system such as NT workstation. The Winnt syntax is :

"Winnt or Winnt32 [/s:sourcepath] [/r:directory] [/rx:directory] [/t:drive_letter] [/a] [/e:

command] [/u:answer_file] [/udf:id, [UDF_file]] "

The following is a list of Winnt command line installation options:

- /? - to see options
- /a - Turn on accessibility options.
- /E:command - Will execute the command specified after the install.
- /I:inf_file - The name of the setup information file without path information. If this option is not used dosnet.inf is the default.
- /R - An optional directory to be created is specified.
- /RX - An optional directory to be copied is specified.
- /S:sourcepath - Windows 2000 or NT set files' location.
- /T:drive_letter - Setup will put temporary setup files on the drive specified.
- /U:answer_file - Specifies an unattended install and an answer file location which is required for unattended installation. Use the /s option to specify the location of source files.
- /UDF:id [,UDF_file] - Specifies the UDF file used to identify the computer. The data from the UDF file is applied to some sections in the answer file. The install program will ask for a disk containing a unique UDF file if the UDF is not specified on the command line.

"Winnt32 [/s:sourcepath] [/I:inf_file] [/t:drive_letter] [/unattend[num]:answer_file] [/udf:id, [UDF_file]] [/copydir:directory] [/copysource:directory] [/cmd:command] [/debug [level]:filename] [/syspart:drive] [/checkupgradeonly] [/cmdcons] [/m:directory] [/makelocalsource] [/noreboot]"

The following is a list of Winnt32 command line installation options:

- /? - to see options
- /checkupgradeonly - The computer is checked for compatability with Windows 2000 and an upgrade report is prepared.
- /copydir:directory - An additional directory is copied into the system root directory on the hard disk.
- /copysource:directory - An additional directory to be copied to the hard disk in the system root directory during installation. It is removed when the installation is done.
- /cmd:command - A command to be executed after the system setup is complete.
- /cmdcons - The recovery console is installed and included in the start menu.
- /debug[level]:filename - Debug log is created with detail level from 1 to 4 specified.
- /makelocalsource - Source files are copied to the hard drive.
- /noreboot - The computer is not rebooted after files are copied.
- /S:sourcepath - Windows 2000 or NT installation files location.
- /syspart:drive - Source files are copied to the hard drive and the drive is marked as active.

- /tempdrive:drive_letter - Setup will put temporary setup files on the drive specified.
- /unattend - Specifies an unattended install and settings are taken from an existing operating system.
- /unattend[num]:answer_file - Specifies an unattended install and an answer file location which is required for unattended installation. Use the /s option to specify the location of source files. Num specifies the number of seconds to wait before rebooting after files are copied.
- /UDF:id [,UDF_file] - Specifies the UDF file used to identify the computer. The data from the UDF file is applied to some sections in the answer file. The install program will ask for a disk containing a unique UDF file if the UDF is not specified on the command line.

Other commands which I'm not sure are still supported.

- /RX:directory - Defines the location option of an executable directory.
- /X - Setup will not create boot floppies.
- /B - The boot files are loaded on the system's hard disk, rather than using floppy disks. This option with Winnt cannot be used to install NT on a multi-processor machine since the required installation files are different.
- /O - Setup will only create boot floppies.
- /OX - Setup will setup floppies for installation from CD-ROM or a network location.
- /F - Copy files from boot floppies without verification (Only winnt).
- /C - Don't check for free space on installation and boot floppies (Only winnt).

Installation Media

Windows 2000 must be installed on a partitioned basic disk. The disk may be made dynamic after installation.

Upgrades

Upgrades to Windows 2000 Professional may be made from the following systems:

- Windows 95
- Windows 98
- Windows NT 3.51
- Windows NT 4.0

Upgrades directly to windows 2000 from Windows 3.x and Windows for Workgroups are not possible without first indirectly upgrading to windows 95.

Upgrades to Windows 2000 Server may be made from the following systems:

- Windows NT Server 3.51
- Windows NT 4.0 Server, Terminal Server Edition, and Enterprise Edition

Windows NT version 3.1 to 3.50 can be upgraded to windows 2000 by first upgrading to Windows NT Server 3.51 or 4.0.

An upgrade check may be run prior to performing an upgrade to check computer hardware for system compatability. The report is automatically saved on Windows 95 and Windows 98 systems, but must be manually saved (if desired) on windows NT systems. The upgrade check is done as follows:

1. Place the Windows 2000 CD in the CDROM drive.
2. Indicate that you do not want to upgrade Windows and close the dialog box.
3. Open a DOS prompt and change drives to the drive letter of the CDROM drive,
4. Type "cd \i386" and type "win32 /checkupgradeonly".
5. Read the report in c:\Windows\Upgrade.txt.

If you do an upgrade from Windows 95 or Windows 98, it may be necessary to apply upgrade packs (also called update packs) to some applications.

If applications exist on the computer that are not compatible with Windows 2000, contact the application manufacturer to get an upgrade pack for windows 2000. When performing the upgrade the Windows 2000 setup program will ask for upgrade packs for applications.

If upgrading Windows NT domains to Windows 2000, first upgrade the primary domain controller on the domain that will be the root domain in Active Directory.

Installation Folder

Windows 2000 is installed by default in the /Winnt directory.

Custom Setting Selections

Types of components that can be selected when choosing custom settings for network settings:

- Clients
- Protocols
- services

Installation Errors

Installation errors are logged based on the error type. These error loge files are stored in the \Windir directory.

- Comsetup.log - "Records COM+ information "
- Mmdet.log - "Stores multimedia device detection information "
- Netsetup.log - "Records workgroup and domain membership information "
- Setupact.log - "Logs setup activity chronologically "
- Setupapi.log - "Logs .INF file entries "
- Setuperr.log - "Records setup errors"

Windows 2000 Installation Options

Installation Information

Installation information to be provided to the setup wizard for all systems (professional, server, etc.):

- Whether third party RAID or SCSI drivers will be installed.
- The drive to install the system on.
- The file system to use. The choices are:
    - FAT - Supports DOS and OS/2 through Windows 2000 but has limited partition size (4MB) and no local security, only sharing permission on the network.
    - FAT32 - Supported by Windows 95, 98, NT, and Windows 2000. Allows large partition sizes up to 32 GB. It has no local security, only sharing permission on the network.
    - NTFS - USed by Windows NT and Windows 2000 and provides many additional features including security, sector sparing, and partition sizes up to 2 Terabytes. This is the best choice unless you need to run another operating system that must access data on this partition.

  A FAT file system can be converted to NTFS, but an NTFS file system cannot be converted to a FAT file system without destroying all data on the partition. This should be considered when selecting file systems.

- The installation directory the system will be installed on. The default is C:\Winnt. If another operating system is in this directoryr, it will be overwritten. Windows 2000 contains a boot manager and will allow booting between the current installation and any previous installation of Windows so long as the current installation is installed in its own directory.
- Regional settings which indicate choice of language.
- The product key from the installation CDROM.
- Computer name
- Administrator password.
- Network settings - Typical or Custom. Custom allows the choice of networking components. Components installed by default with the typical settings are:
    - Client for Microsoft Networks
    - File and Print Sharing for Microsoft Networks
    - TCP/IP Protocol
- Place the computer in a workgroup or a domain. For a domain, an authorized user name and password must be provided.

Additional information for Windows 2000 Server and Windows 2000 Advanced Server.

- **Per server or per seat licensing.**
  - With **per server** licensing a maximum specific number of concurrent users can connect to one server. Therefore the licence is done for each server for some number of connections on each server.
  - **Per seat** licensing allows clients to connect to any number of servers with one license. Microsoft allows only one conversion from per server licensing to per seat licensing. It cannot be converted from per seat licensing to per server licensing. There are conversions for:
    - Windows 2000 Server
    - Windows 2000 Exchange Server
    - Windows 2000 SQL Server
    - Windows 2000 SNA Server
- **Components**
  - Accessories and Utilities. Subcomponents:
    - Accessibility Wizard. Subcomponents:
      - Calculator
      - Character map
      - Desktop Wallpaper
      - Document Templates
      - Mouse Pointers
      - Object Packager
      - Paint
      - Screen Savers
      - WordPad
    - Communications. Subcomponents:
      - Chat
      - HyperTerminal
      - Phone Dialer
    - Games. Subcomponents:
      - Freecell
      - Minesweeper
      - Pinball
      - Solitaire
    - Multimedia. Subcomponents:
      - CD Player
      - Media Player
      - Sample Sounds
      - Sound Recorder
      - Utopia Sound Scheme
      - Volume Control
  - Certificate Services. Subcomponents:

        - Certificate Services CA
        - Certificate Services Web Enrollment Support
    - Cluster Service
    - Indexing Service
    - Internet Information Service (IIS) Subcomponents:
        - Common Files
        - Documentation
        - FTP Server
        - FrontPage 2000 Server Extensions
        - Internet Information Services Sanp-In
        - HTML Internet Services Manager
        - NNTP Service. Subcomponents:
            - NNTP Service
            - NNTP Service Documentation
        - SMTP Service. Subcomponents:
            - SMTP Service
            - SMTP Service Documentation
        - Visual InterDev RAD Remote Deployment Support
        - World Wide Web Server
    - Management and Monitoring Tools. Subcomponents:
        - Connection Manager Components
        - Network Monitor Tools
        - Simple Network Management Protocol
    - Message Queuing Services
    - Networking Services. Subcomponents:
        - COM Internet Services Proxy
        - Directory Service Migration Tool
        - Domain Name System (DNS)
        - Dynamic Host Configuration Protocol (DHCP)
        - Internet Authentication Service
        - QoS Admission Control Service
        - Simple TCP/IP Services
        - Site Servew ILS Services
        - Windows Internet Name Service (WINS)
    - Other Network File and Print Services. Subcomponents:
        - File Services for Macintosh
        - Print Services for Macintosh
        - Print Services for Unix
    - Remote Installation Services
    - Remote Storage
    - Script Debugger
    - Terminal Services. Subcomponents:
        - Client Creator Files

        - Enable Termnal Services
    - Terminal Services Licensing

Typical Installation Components Installed

- Client for Microsoft Networks
- File and Printer sharing for Microsoft Networks
- TCP/IP

Windows 2000 Unattended Installation

The Winnt.exe and Winnt32.exe programs provide the unattended installation ability, allowing the rapid creation of large numbers of similar workstations using existing installation media. Two types of files are required:

- Answer files - Files requires to answer the system queries during an unattended installation normally sent to the monitor during an attended installation.
- Uniqueness Database Files (UDF) - Used to insert the User name, organization, and computer name in the [UserData]section of the unattend.txt file.

The Computer Profile setup utility or the **Setup Manager utility (SETUPMGR.EXE on the Windows NT install CD at \SUPPORT\TOOLS\Deploy.cab) may be used to set up unattended installation answer file**. On Windows 2000, this program is called the Setup Manager wizard and can be installed from the resource kit on the CDROM by running \Support \Reskit\Setup.exe.Options:

- Create a new answer file.
- Create an answer file that duplicates this computer's configuration.
- Modify an existing answer file.

Answer file types are:

- Unattend.txt for Windows 2000 Professional.
- Unattend.txt for Windows 2000 Server.
- Remboot.sif for remote installation services.
- Sysprep.inf for the system preparation tool.

Products that can be installed with answer files include:

- Windows 2000 Unattended Installation
- Sysprep Install - System preparation utility located on the CDROM in the \SUPPORT \TOOLS\Deploy.cab file. Works on non-domain controller windows 2000 computers. This utility allows a Windows 2000 hard drive to be copied to other computers.
- Remote Installation Services

User interaction levels can be set at:

- Provide defaults - The answer file provides default answers.
- Fully automated - No user interaction.

- Hide pages - There is some interaction by the user with pages hidden that have answers provided by the answer file.
- Read only - The setup screens are displayed, but the user cannot make selections.
- GUI attended - The text part of the installation is automated and the user responds to the graphical part of the installation.

A distribution folder is created to do an installation over the network. An unattend.txt answer file and a unattend.bat file, for starting the installation, is created by the Setup Manager.

Booting from the network involves:

1. Have a network card in the computer the installation is to be done on.
2. Format the hard drive.
3. Boot a computer with DOS client for Microsoft Networks on it (Comes With Windows NT Server).
4. Map the shared distribution folder to a network drive, and from that drive run "unattend" or "unattend computer"

One UDF file is required for installing to various types of computers. **There must be a different answer file for each type or configuration of computer**.

Answer Files

There is a sample answer file on the install CD-ROM called UNATTEND.TXT. These files contain categories of information defined by the [and] symbols. Some categories are:

- DetectedMassStorage - Mass storage devices that Setup should recognize, whether they are available at installation time or not.
- Display - Display settings.
- DisplayDrivers - Display drivers.
- GuiUnattended - Defines the setup program behavior during graphical mode setup.
- KeyboardDrivers - Specifies keyboard drivers.
- LicenseFilePrintData - Used for servers only.
- MassStorageDrivers - Specifies SCSI drivers.
- Modem - Determines if a modem is to be installed.
- Network - Network settings, with adapters and protocols.
- OEM_Ads - The bitmap information to be displayed when the graphical user mode is starting.
- OEMBootFiles- The files required for system boot must be listed here.
- PointingDeviceDrivers - Specifies any pointing devices.
- Unattended - This section defines setup program behavior during text mode setup.
- UserData - User or computer information.

A sample unattend.txt answer file:

```
[Unattended]
OemPreinstall = no
ConfirmHardware = no
NtUpgrade = no
Win31Upgrade = no
TargetPath = WINNT
OverwriteOemFilesOnUpgrade = no
[UserData]
FullName = "Your User Name"
OrgName = "Your Organization Name"
ComputerName = COMPUTER_NAME
[GuiUnattended]
TimeZone = "(GMT-08:00) Pacific Time (US & Canada); Tijuana"
[Display]
ConfigureAtLogon = 0
BitsPerPel = 16
XResolution = 640
YResolution = 480
VRefresh = 70
AutoConfirm = 1
[Network]
Attend = yes
DetectAdapters = ""
InstallProtocols = ProtocolsSection
JoinDomain = Domain_To_Join
[ProtocolsSection]
TC = TCParameters
[TCParameters]
DHCP = yes
```

UDF Files

The UDF file below assigns user name, organization name, and computer names for three computers.

```
; The UID on the left is a unique string for this file which cannot contain a
; space, asterisk, comma, or equals character.
; The right hand side value must match the name of a section in the unattend.txt file.
UID1=UserData
UID2=UserData
```

```
UID3=UserData
; The sections below specify sections to be merged into the unattend.txt answer file
sections.
; They may be specified for unique computer IDs with the format "[UIDn:
SectionName]".
; They may be set for all computers is the format "[SectionName]" is specified.
; Any matching values on the left side of the "=" sign (key) are replaced by the value
on the
; right. If a key does not match, the key and value are added to the unattend.text
values.
; Format: "key=value".
[UID1:UserData]
FullName = "Mark Allen"
OrgName = "CTDP"
ComputerName=NTWS1
[UID2:UserData]
FullName = "Chris Smith"
OrgName = "Acme Corp"
ComputerName=NTWS2
[UID3:UserData]
FullName = "John Brown"
OrgName = "Acme Corp"
ComputerName=NTWS3
```

OEM Directory

The OEM directory is used to install files that are not a standard part ot the NT product. Additional drivers and files may be installed using this directory.

Winnt and Winnt32.exe use

An example command line that uses the answer files and UDF files is:

```
winnt /s:e:\ /u:unatt.txt /UDF:id1,udffile.txt
```

The Sysdiff Utility

Used to customize Windows 2000 or NT installation to one or more computers over the network. It records the differences between a installation files that have been added to an installation and a normal installation that has not had additions added. Functions:

- Snap - Takes a snapshot of the state of files, directories, and the registry.

- Diff - Records differences between a current system and a previous snapshot.
- Apply - Apply data in a differences file to an installation.
- Inf - Create an inf file from a diff file. The .inf file allows differences to be automatically applied to installations of NT from the server based share.
- Dump - Allows review of the contents of a diff file.

If sysdiff is used to create an inf file and the difference files are put in the directory tree, %OEM $, you can use the command sysdiff.exe /apply in a file named cmdline.txt located in OEM. If this is done, the OemPreinstall line in the unattend file must be set to "Yes". Windows NT 3.5.1 used the Windiff utility which is still available in NT 4.0, but Sysdiff is used for unattended installation while Windiff may be used to compare files.

Beginning an Install

To install from the hard drive:

1. Copy i386 information from the i386 directory to a created i386 directory on the hard drive.
2. Run Winnt.exe or win32.exe
3. Nomally you will create three setup disks unless you skip this option.
4. The installation will create a temporary WIN_NT~LS or ~BS directory. If this file is gone at the end of the installation, the installation was completed.
5. When done you will reboot the system and the system will run 32 bit code.

Syntax:

sysdiff /snap [/log:logfile] snapshotfile
sysdiff /diff [/log:logfile] snapshotfile differencefile
sysdiff /inf [/u] snapshotfile oemroot
sysdiff /dump differencefile dumpfile

The "oemroot" location, above, is the directory with additional files and directories with custom installation. An emergency repair disk can be created at installation time or it can be made later using the RDISK.EXE utility.

To install over the network:

- The i386 directory must be in a shared network folder

Using Sysprep

Sysprep is used to prepare a Windows 2000 system hard disk for duplication. Sysprep can't be used on domain controllers. Duplication requirements that both the master and duplicated computers must have in common:

- Identical type hard drive controllers.
- Identical size hard drives.
- The same HAL must be used.
- Peripheral cards such as modems and video cards do not need to be identical, but drivers must be available for all computers.

Sysprep will remove any user specific information on the prepared hard drive. It strips the Security Identifiers (SIDs) from the disk before capturing the disk image. Once duplicated, the system that gets a copy of the disk generates its own SIDs for its objects.

1. Create a Windows 2000 installation that you want copied (the master).
2. Install any applications that are to be in the new system(s).
3. Copy the administrator profile folder contents to the Default user profile folder and be sure the group, "everyone" can use the profile.
4. Create a c:\sysprep directory and possibly a sysprep.inf file. Copy setupc1.exe and sysprep.exe from the directory where Setup Manager is installed into the c:\sysprep folder.
5. Use the Sysprep utility on the master computer hard drive, to prepare for duplication. Typing "sysprep /?" lists options, and "sysprep -pnp" causes the mini-setup program to run hardware detection on the duplicated computers.
6. Use a **vendor tool** to duplicate the hard drive to target computers. Drive Image Pro from Power Quest will work.
7. Boot the duplicated computers and enter user information when the mini-setup wizard runs.

The mini-setup wizard can be automated using a **c:\sysprep\sysprep.inf** file. Timezone, domain name or workgroup, network settings, display settings and additional settings may be preset.

Sysprep switches include:

- -quiet - No user interaction.
- -pnp - Detect PNP devices on systems the information is being sent to.
- -reboot - The new system will restart rather than shutdown.
- -nosidgen - NO security identifier (SID) is created on the new system.

Windows 2000 Software Distribution

Software Packages

Software may be packaged for Windows systems in Windows installer files which have an extension of ".msi". The Windows Installer utilities can be used to package applications into Windows installer packages if they are not already in these packages. Other packages include:

- **Transform files** - Files have a ".mst" extension and are used to customize applications. Complements the ".msi" Windows installer files.
- **Patch files** - Files have a ".msp" extension and are used to apply software fixes (patches) to applications. Complements the ".msi" Windows installer files.
- **ZAP files** - Applications that don't use the ".msi" file format for the Windows Installer Service can be set up for distribution by creating a text file with a ".zap" file extension. This method is not as flexible as the ".msi" package files.

Software Installation Utilities

Installation services and utilities include:

- **Windows Installer Service** - On Windows 95, 98, Me, NT, and 2000 systems. The service installs package files with the ".msi" extension. This sservice is used by the client computer.
- **Windows 2000 IntelliMirror utility** can be used to manage software from anywhere on the organization's network.
- **Microsoft Management Console software installation snap-in** can be used to assign applications to computers, organizational units, or users by using group policies.
- **Add/Remove Programs Control Panel applet** - Applications can be placed on an Active Directory distribution location (published) where users can get applications. The Add/Remove Programs Control Panel applet can then be used by the user to install the software.
- **WinInstall** - Written by Veritas software, it is included on the Windows 2000 Server CD. It is used to edit, view, and create application installation package files.

Ways to Distribute Software

- **Assignment** - This method is not by the user choice and can be assigned to the following:
  - Computer - The software is installed when the computer boots.
  - User - A shortcut for the software is placed on the user's desktop when the user

logs into the domain. The software is installed when the user clicks on the shortcut to run the application.

- **Publication** - The software can be installed by using the Add/Remove Programs Control Panel applet. The software will be available on the list of available programs in the "Add New Programs" dialog box.

Software Distribution Methods

- **Push Model** - Microsoft's System Management Service (SMS) uses this model. SMS works for Windows 95, 98, ME, NT, and 2000 client systems. Software is deployed to selected users and computers based on the administrators' choices. This model helps control software licensing, use of network bandwidth, and can determine whether clients have sufficeint system hardware to support the application.
- **Pull Model** - When users need the software, they pull it from its stored location. Windows 2000 distribution features are compliant with group policies. The administrators must be sure licensing is done properly when this method is used. This model can overuse valuable network bandwidth, and can't determine if clients have sufficient hardware to run the software.
- **Windows 2000 Remote Installation Service (RIS)** - Windows 2000 Professional can be installed on computers that can boot to the network using a BIOS program running from their network card. This is called Pre-boot Execution Environment (PXE). A Windows 2000 Professional image with desired applications can be created using the RIPREP utility.

Group Policy Software Settings

In the Microsoft Management Console (MMC) Group Policy snap-in, one of the settings, in both computer and user configuration, is software settings. This is used to set the policy for deploying applications. The Software Settings dialog box has the following tabs:

- **General** - Allows setting the following:
  - Set the Default Package Location for applications.
  - New Packages Options:
    - Display the Deply Software dialog box.
    - Publish - The softeare is automatically published.
    - Assign - Assign the software (without the user's choice) to a computer or user.
    - Advanced published or assigned
  - Installation User Interface Options:
    - Basic
    - Maximum
  - Uninstall the application when they fall out of the scope of management (policies

management) checkbox.
- **File Extensions** - Allows files to be set to be associated with the application.
- **Categories** - Allows the application to be listed in a category that is displayed when users use the Control Panel Add/Remove Programs applet to select "Add New Programs".

Client Option Configuration

In the Microsoft Management Console (MMC) Group Policy snap-in, under the "User Configuration" and "Windows Settings" nodes is a selection "Remote Installation Services". Clicking on this allows a "Choice Options" icon to appear in the right pane. Under each selection group are the options:

- Allow - Allows the setting it is associated with to be set by administrators and other users.
- Don't Care - Allow or deny options are determined by higher level Active Directory objects.
- Deny - The setting may not be chosen by administrators or users.

One of these choices are selected in each selection group. The choice options section groups are:

- Automatic Setup - The administrator specifies installation options and the client cannot make selections.
- Custom Setup - The client or administrator can choose specific options.
- Restart Setup- The client or administrator can restart RIS setup if the connection was lost during a previous session.
- Tools - Allows access to different Client Administration Wizard tools.

Microsoft Office

Microsoft Office properties dialog box tabs:

- **General** - Friendly Name, Version and package name.
- **Deployment** - Options:
  - Deployment type is published or assigned.
  - Deployment Options:
    - Auto-install the application by file extension activation - The program is installed when a user tries to open a file associated with the application.
    - Uninstall the application when it falls out of the scope of management (policies management).
    - Do not display this poackage in the Add/Remove Programs control panel.

    - Installation User Interface Options:
        - Basic
        - Maximum
- **Upgrades** - Upgrade options.
- **Categories** - Two columns:
    - Software categories from the group policies software installation properties node.
    - Shows the selected categories for the software package.
- **Modifications** - The transform files (with .mst extension) are configured here.
- **Security** - Shows the DACL for the users and groups that may use the package.

Windows 2000 Remote Installation Service (RIS)

Revised 10-30-2002

RIS can be used to deploy Windows 2000 operating systems to client systems from the server. It can install the operating system with applications. It provides the following additional capabilities:

- Other technical personnel that are not administrators may install Windows 2000 Professional.
- It provides an extra way to fix failed networked computers.
- Specific hardware images do not need to be provided since Windows 2000 supports plug and play devices.

A Windows 2000 computer can have remote installation files for Windows 2000 Professional computers then send those files out to the appropriate computers and provide a unique security identifier for the new computer. The "Add/Remove Programs" applet in the control panel is used to install RIS. It is installed as a "Component" and is called "Remote Installation Services".

Requirements

Requirements/steps for using RIS:

- The RIS server must have at least two volumes. The second volume contains the RIS installation information which is separate from the Windows 2000 Server installation volume.
- The RIS volume must be NTFS.
- The network must use DNS, DHCP, and Active Directory to use this service.
- The RIS server **must be authorized in Active Directory** using the DHCP administrative tool. It is easier if the RIS server is the DHCP server and is already authorized.
- The RIS server must have the same service pack of the Windows 2000 professional image that you intend to create. If it does not, there will be a failure in creating the image. This means that if the server is running SP2 and you want to create a Windows 2000 professional image with SP3, it will fail to create the image. (Note: there is information on Microsoft's site indicating that you can update the image to SP3, but I could not get that to work.)

RIS Server Setup

1. On the server install the Remote Installation Service by opening the Control Panel, select "Add/Remove Programs", click on the "Add/Remove Windows Components" button on the lower left, then select the Remote Installation Service box. After the install, reboot the server.
2. The RIS server must be setup using the command line utility called "risetup". Open a command line window by selecting "Start", "Programs", "Accesssories", and "Command Prompt", then type "risetup". This can also be accessed from the Control Panel by opening the "Add/Remove Programs" applet and selecting "Add/Remove Windows Components". A box allowing Remote Installation Services configuration will appear. The configuration wizard will allow selection of the Remote installation folder (must not be on the system partition, must be NTFS partition, and must be shared which will be automatically created and shared). It will also request the path to the Windows 2000 Professional installation files which may be your Windows 2000 Professional installation CD.

Authorizing the RIS Server for DHCP Services

If the RIS server is not performing DCHP assignments, it must be authorized to do so. This can be done from an authorized DCHP server using the DCHP tool in Administrative Tools.

1. Select the main DHCP box, then select the menu item "Action", and select "Manage Authorice Servers".
2. Click the "Add" button and enter the computer name or IP address of the RIS server.

Client Creation

The list below is how I recommend the client be created for best results.

1. Install the client operating system on a 2.1 gig NTFS partition. This should be the minimum size required for your OS unless you have additional or special software.
2. Install all appropriate drivers (video, audio, etc.) for your main type of computer hardware depending on the make and model of your computers that you plan to do most client installations on.
3. Install SP2 if yous CD did not have it, then install SP3.
4. Install the latest version of Internet Explorer (current as of this writing is IE6.1).
5. Install or remove any additional components of Windows that you may want or not want your client computers to have.
6. Install security updates from the Microsoft windows update website at Microsoft's Windows Update.
7. Setup automatic updates on your system according to your IT department update policy. A choice of automatic updates at a specific time, downloading the updates and notifing

the user when they are ready to be installed, or Notification before downloading updates is given. I recommend installing the updates at a secific time according to your IT department security policy. This is because most users won't understand or care about updates and unless you have a lot of staff or some third party software to do this job for you, your network will not be secure.

8. Install any additional programs which are used widely throughout your organization such as Office 2000, and antivirus software. Install the latest updates to these programs.
9. Set your system settings the way you would like them as a standard through your organization such as file view settings by selecting "Tools" and "folder Options" from "My computer". For security reasons, I recommend that file extensions for known file types are not hidden (It is the Windows default to hide them). This setting can hide a file of the type "myvirus.txt.exe" making it appear harmless as "myvirus.txt".
10. Shrink your partition to a minimum size on the client computer before making the image. Use Partition Magic if you have it available, otherwise you should have created a 2.1 G partition as outlined in the first step.

CD Image Creation

To create a CD, you can use the sysprep utility with third party software to create the CD image, or use the RIPrep utility. With RIPrep, the target computer hardware does not need to match the master computer hardware.

Using Sysprep

1. Log on to the previously created client computer as a domain administrator.
2. Copy the Setup Manager and sysprep utility to a client accessible computer drive. On the Windows 2000 Server or Professional installation CD, unzip the contents of the \SUPPORT\TOOLS\DEPLOY.CAB file and copy them to your computer into a directory that you create such as "c:\deploy".
3. Use the Setup Manager (setupmgr.exe) to create a sysprep install answer file. Create a sysprep folder during this process.
4. Copy the sysprep.exe file to the sysprep folder.
5. From the sysprep folder, run the sysprep.exe utility. When starting sysprep, run it from the command line, typing "sysprep - pnp" which will allow it to detect any plug and play devices on the computer the image will be deployed to. If all hardware is the same, the pnp option is not necessary.
6. After sysprep runs, the computer shuts down.
7. Use third party software to duplicate the hard drive of the system you ran the sysprep utility on. Than can be Norton Ghost.
8. Reboot the computer from which the master hard drive image was made. Login as a domain administrator. The Mini-Setup utility will run and remove the sysprep folder.

Using RIPrep

1. Log on to the previously created client computer as a domain administrator.
2. Select the "Start" button, and select "Run", then type "\\RIS_server\Remote_inst_dir \Admin\i386\riprep.exe".
3. In the Remote Installation preparation wizard select the RIS server the image will be placed on, and create a name for the folder the image will be stored in. Enter description information and click next.
4. If any services must be stopped, then open the services tool in Administrative Tools and stop those services, then click next in the Remote Installation preparation wizard. Click Next.
5. RIPrep will shut down the client computer the copy is made from when it is done. When the client computer, which the CD image was made from, is started again, a Mini-Setup Wizard must be run to return the computer to an operational condition.

If the security settings for the remote installation server will only allow a response to known clients, the RIS client must be prestaged using Active Directory Users and Computers. Right click the OU in the domain you want to create the computer in. Select "New", and "Computer". Enter a name for the new computer, and click "Next". In the next dialog box, select the "This is a managed computer" check box and enter the computer's Globally Unique Identifier (GUID). The GUID should be available in the computer system BIOS or on the case. A computer that does not have a GUID cannot be prestaged and can only be remotely installed if the remote installation server will respond to unknown clients. After the computer is created, right click the new computer object, and select "Porperties". Select the "Security" tab, and add users, or groups that are to be allowed to perform a network installation on this computer.

Creating Answer files from a client install

The answer files are created using the Setup Manager. On the Windows 2000 Server or Professional installation CD, unzip the contents of the \SUPPORT\TOOLS\DEPLOY.CAB file and copy them to your computer into a directory that you create such as "c:\deploy".

1. Double click on setupmgr.exe.
2. Select "Create an answer file that duplicates this computer's configuration". The other two choices are "Create a new answer file", and "Modify an existing answer file".
3. On the next screen the installation product is selected. Choices are:
    - Windows 2000 Unattended Installation
    - Sysprep Install
    - Remote Installation Services

   Select "Windows 2000 Unattended Installation". Click "Next".
4. Select the platform the answer file will install to. Choices are Windows 2000 Professional, and Windows 2000 Server. Select Windows 2000 Professional to be able

to perform client installations.

5. Select the user interaction level. Choices are:
    - Provide Defaults - The user can review the answers supplied in the answer file when the installation is done.
    - Fully automated - All the answers are automatically provided by the answer and the user does not see them.
    - Hide pages - Only setup screens that are not answered are supplied to the user.
    - Read only - Setup screens are shown to the user, but they can not make any changes.
    - GUI attended - Text answers are automated, but GUI screens are not.

   Select "Fully Automated", and click "Next".
6. Accept the license agreement and click "Next".
7. Supply the Name and organization and then click "Next".
8. Enter the names of destination computers that Windows 2000 will be installed on, then click "Next".
9. Supply the administrator password to be used for local administrator rights and click "Next". You could click the checkbox that says "When the computer starts, automatically logon as administrator", but I would not usually do this unless an administrator will be there at the conclusion of the install.
10. Select the screen size, refresh frequency, and colors the client computer is to use, and click "Next".
11. Select either Typical or Custom network settings, and click "Next".
12. Select the domain or workgroup the computer will be a member of. Check the "Create a computer account in the domain checkbox, and add an administrator name and password that has the authority to create the account, then click "Next".
13. Select Time zone, and click "Next".
14. The Wizard allows you to edit the settings at this point. These include Telephony settings, regional settings, additional language support, browser and shell settings, the system folder for the Operating system which is normally c:\WINNT, printers to be installed, And commands to run once.
15. Normally you will probably want to create a distribution folder for device drivers or other customizations.
16. Additional mass storage drivers. Click "Next" here.
17. This screen allows you to specify a different HAL other than the default hardware abstraction layer (HAL). Normally, click "Next" here.
18. Additional commands to run.
19. OEM Branding - You can choose a Gif logo file and a background bitmap to be displayed during Windows Setup.
20. This screen allows you to locations to copy additional files or folders to.
21. This screen allows you to choose the location to place the answer file which is c:\win2000dist\unattend.txt by default..
22. Specify the location of the Windows setup files, and click "Next".
23. At this point the setup files are copied. You can copy them from the Windows 2000

Professional installation CD or choose another location.

Associating RIS Answer file to the Image

This is required for unattended network installation.

RIS answer files are in \\RIS_server\REMINST\Setup\language\Images\image_name\i386 \templates and have .sif extensions. These files are called "setup information files".

Answer files are associated (or created) with the CD image from Active Directory Users and Computers by right clicking on the RIS server and selecting "properties". Select the "Remote install" tab and click on the "Advanced Settings" button. In the next dialog box, select the "Images" tab and click on the "Add" button. At this point you can either "Associate a new answer file to an existing image", or "Add a new installation image".

Creating a RIS client boot disk

1. On the server, open the \RIS_server\REMINST\admin\i386\ folder. Double click the program "rbfg.exe" to run it.
2. Put a blank floppy in the A drive of the Server, and click "Create Disk".

Additional Preparation

- Assign appropriate users the authority to "Create Computer Objects" in Active Directory using the administrative tool "Active Directory Users and Computers".
- Configure RIS options using the administrative tool "Active Directory Users and Computers", right click the RIS server and select properties. Server properties tabs:
    - General
    - Operating System
    - Member Of
    - Location
    - Managed By
    - Object
    - Security
    - Remote Install - Options:
        - **Respond to client computers requesting service.** - This or the next option is chosen. This is of one of the main configuration choices with RIS.
        - **Do not respond to unknown clients** - For setting up installation for prestaged computers only.
        - Verify Server - Used to correct problems on the RIS server.
        - Show Clients - Lists clients that have used RIS for an install.
        - Advanced Settings - Displays a dialog box with these tabs:

        - New Clients - Set how computer names are generated, whether from user names and where the client account will be.
        - Images - Shows the Windows 2000 professional images available to be used for an install
        - Tools
        - Object - Shows the fully qualified domain name of the Remote installation service.
        - Security - Can set up for use exclusively by computers that are prestaged for RIS.
- Configure the client with one of:
    - Boot the client using a network card on the client with a **preboot execution environment (PXE)** .99c or later ROM.
    - Create a RIS client boot disk using the program in **RIS_install_volume:\RemoteInstall\Admin\i386\rbfg.exe**. This program is called the Windows 2000 Remote Boot Disk Generator.

The user account that is doing the install must be able to logon as a batch job user. The user must be able to create computer accounts in Active Directory in the domain to be joined, or the computer account must have been previously created by an administrator.

If the "UNDI initialize failed" error occurs, it means that no network card was detected by the setup program at installation while attempting RIS.

RIS Additional Services

Additional services installed on servers when RIS is installed on servers:

- BINL - Boot Information Negociation Layer is used to be sure the installation using RIS is being done on the correct computer.
- SIS - Single Instance Store is used to reduce storage space for installation images on the server by using links to files that are the same in various images.
- TFTPD - Trivial File Transfer Protocol Daemon is used to send files to the client when they are requested. There is no logon with TFTP services.

RIS Security and Prestaging RIS Clients

An Active Directory computer object is created and the users of the new computer are assigned appropriate Active Directory permissions. Group Policy can also be used for security to restrict RIS installation options and choices. The "Active Directory Users and Computers" tool is used to set this policy.

To set up prestaging so specific clients wil get the correct RIS images do the following:

1. Get the GUID from the computer which is in the computer system BIOS or on a label on the computer case. This is a 32 character number.
2. Create a client account on the server and provide the computer GUID during client account creation.

RIS Images

Supported images:

- CD image - A CD image is made and an RIS answer file is associated with the image.
- Remote Installation Preparation (RIPrep) wizard images - A copy of a master computer hard drive, which is prepared for installation. Mass storage controllers and disk sizes don't need to be the same on both the master and duplicate computer. The RIPREP utility is in \\RIS_server\Reminst\Admin\i386\riprep.exe. Some services cannot be run while this utility is run. The wizard will notify you of any unallowed services that are running.
- Windows 2000 Professional images

The RIPrep tool is used to make RIS images containing both an operating system and applications.

Windows 2000 Accessibility Options

- Accessibility Wizard - Used to configure the computer for a person with special requirements.
- Magnifier Utility - An additional window is used to magnify part of the screen.
- Narrator Uility - Text that is on the screen is read to the user.
- On-Screen Keyboard - A mouse can be used to control a keyboard which is displayed on the screen.
- Utility Manager - Used to control when the accessibility utilities listed above are run.

Windows 2000 File Attributes

- Archive - The directory or file has been changed since it was last backed up.
- Compress - The directory or file is compressed on an NTFS volume. The directory or file cannot be compressed and encrypted.
- Encrypt - The directory or file is encrypted on an NTFS volume. The directory or file cannot be encrypted and compressed. Encryption is provided by the Encrypting File System (EFS) which comes with and is installed automatically on Windows 2000 systems. The user who encrypted the file or a local or domain administrator can decrypt encrypted files. The administrator account is called a recovery agent because it has a global key which can decrypt any files. Group policy can be used to make other accounts recovery agents.
- Hidden - The directory or file is invisible to a normal directory search and cannot be copied or deleted.
- Index - The directory or file is indexed by the Windows Indexing Service on an NTFS volume. Once files are indexed, Windows Explorer can find files that contain specific phrases or words.
- Read-only - The directory or file cannot be modified by writing to it or deleting it.
- System - The directory or file is needed by the operating system. Files with this attribute set are read-only and hidden, even if those attributes are not set.

Encrypting File System

If a user encrypts files, then leaves, the administrator is an EFS recovery agent and can decrypt the file. An EFS recovery agent has a certificate allowing them ot unencrypt files. The user that is a recovery agent can have their certificate removed and stored on a floppy until needed. This prevents accidental viewing of secure files by unauthorized persons, even the administrator.

- A recovery agent certificate can be requested using the MMC Certificate snap-in command line utility by typing "mmc" on the command line and selecting "Certificates" after selecting "Console", "Add/Remove snap-in", and "Add". A user may be made a recovery agent using this snap-in.
- The administrative tool, "Active Directory Users and Computers" is used to designate recovery agents.
- The control panel "Internet Options" applet is used to remove EFS recovery agent certificates.

Windows 2000 Shares

Shares are directories that are shared over the network. All subdirectories and files in the shared folder are shared with users who have the correct permissions. Users that can share directories are:

- On Windows 2000 domain controllers:
  - Local Administrators
  - Local server operators
  - Global Domain Admins group since they are automatically a member of the Administrators local group on all computers in the domain.
- On Windows 2000 computers that are not domain controllers:
  - Local Administrators
  - Local power users
  - Global Domain Admins group since they are automatically a member of the Administrators local group on all computers in the domain.

Computer Management can be used to share directories on local and remote computers. Windows Explorer can be used to share folders on local computers. Share name length supported by operating systems:

- MS-DOS - 8 characters plus 3 leter extension.
- Windows 95 and Windows 98 - 12 characters
- Windows NT and Windows 2000 - 80 characters

Directory Property dialog box tabs:

- General
- Web Sharing
- Sharing - Share name, user limit, permissions, and caching (manual or automatic caching for documents and automatic caching for programs for offline access).
- Security

Share permissions:

- Read - Users can see contents of files and directories.
- Change - Users can create, change and delete files and directories.
- Full Control - Allows Change benefits and ability to change permissions and take ownership of directories and files.

These permissions are set as allowed or denied to users or groups. If permission is denied for a particular permission to a particular user or group, then that user or group is denied that permission, even if another group they are in has permission for that permission.

Share Modofications:

- Changing share names - Remove the share, then re-create the share.
- Assign multiple names to a share - Create a new share for the same directory as a previous share, and set up share permissions.

UNC or FQDN may be used to access shared resources.

Universal Naming convention (UNC)

A UNC includes:

- Server name
- Shared resource name

Syntax:

\\Server\Share

Fully Qualified Domain Names (FQDN)

A FQDN includes:

- Server name
- Domain name
- Root domain name

Syntax:

Server.domain.root_domain

Example:

Myserver.myorganization.org

An example share access using FQDN:

\\Myserver.myorganization.org\Myshare

Administrative shares

Administrators may view administrative shares from the Control panel server applet by selecting the "Shares" button. The Server Manager may be used on NT server. Adding a $ to the end of a share will make them hidden and you must know the share name thereafter to use the share. The registry may be modified to prevent the creation of hidden shares in "/HKEY_LOCAL_MACHINE/CurrentControlSet/Services/lanmanserver". Set or create the double word value "AutoShareServer" or "AutoShareWks" on Windows 2000 server or professional respectively. Set the value to 0.

- **Admin$** - This is where the system files were installed, usually C:\WINNT40. Users that can use these shares remotely are administrators, backup operators, and server operators.
- **drive$** - Every partition's root directory followed by a $. Users that can use these shares remotely are administrators, backup operators, and server operators.
- **IPC$** - Named pipes to be used to communicate between systems and programs. It is used to access resources on other computers.
- **NETLOGON/SYSVOL** - The Netlogon share is used on Windows NT domain controllers to authenticate users. In Windows 2000, the SYSVOL share carries out these functions. The SYSVOL share includes group policy information which is replicated to all local domain controllers.
- **Print$** - Provides shared printer support.
- **REPL$** - Used on an NT server for directory replication.

Accessing a shared folder

The following ways may be used to access shared folders.

- Network Neighborhood
- The find command
- Drive mapping with Windows Explorer
- Drive mapping with My Computer

Distributed File System (DFS)

The Distributed File System (DFS) allows files and directories in various places to be combined into one directory tree. Only Windows 2000 Servers can contain DFS root directories and they can have only one.

DFS Characteristics

- The permissions of shared folders that are part of the DFS are still the same.
- Shares with important information can be replicated to several servers providing fault tolerance.
- The DFS root must be created first.

DFS Components

- DFS root - A shared directory that can contain other shared directories, files, DFS links, and other DFS roots. One root is allowed per server. Types of DFS roots:
  - Stand alone DFS root - Not published in Active Directory, cannot be replicated, and can be on any Windows 2000 Server. This provides no fault tolerance with the DFS topology stored on one computer. A DFS can be accessed using the following syntax:

    \\Server\DFSname

  - Domain DFS root - It is published in Active Directory, can be replicated, and can be on any Windows 2000 Server. Files and directories must be manually replicated to other servers or Windows 2000 must be configured to replicate files and directories. Configure the domain DFS root, then the replicas when configuring automatic replication. Links are automatically replicated. There may be up to 31 replicas. Domain DFS root directories can be accessed using the following syntax:

    \\domain\DFSname

- DFS link - A pointer to another shared directory. There can be up to 1000 DFS links for a DFS root.

DFS administration is done on the Administrative Tool, "Distributed File System". This tool is on all Windows 2000 Server computers, and Windows 2000 Professional computers that have the ADMINPAK installed.

Client Computers

- Windows 2000 Server
- Windows 2000 Professional
- Windows NT 4.0 or later Server and Workstation
- Windows 95 and Windows 98 with DFS client software. (No access to DFS links on NetWare servers).

Replication

The **File Replication Service (FRS)** can used to replicate DFS shares automatically.

Windows 2000 Control Panel

Windows 2000 Professional Control Panel

Holds mini application (applet) programs for changing the system environment. Most changes are saved in the system registry. Applets include:

- **Accessibility** - Five tabs are keyboard, sound (Can have visible sound indications), display, mouse(Can move the mouse with the keyboard), and general (alternatives to keyboard and mouse).
- **Add/Remove Hardware** - Can add and remove hardware device drivers for display devices, CDROM and DVD drives, I/O devices (Keyboard, mouse, USB devices and more), **Mobile computer hardware**, **modems**, **multimedia**, and network cards. A **device driver** is a software3 program that allows the system to interact with hardware. If the driver is signed, it has a digital signature from its creator verifying its authenticity.
- **Add/Remove Programs** - Allows programs to be installed or removed from the system including optional Windows 2000 components. Vendor programs must be written to use this applet.
- **Administrative Tools** - Only the members of the Administrators group can use these tools.
- **Console** - Allows settings for MS-DOS console. Uses four tabs which are options (for cursor size, command history, and display options), font, layout, and colors tabs.
- **Date/Time**
- **Display** - Tabs are Background, Screen Saver, Appearance, Web, Effects, and Settings (Sets the video mode). The Screen saver allows power settings to be adjusted along with selection of the screen saver. Appearance tab adjusts the Windows color schemes. The Web tab allows a specific web page to be displayed all the time on the desktop. The effects tab allows desktop icons to be changed. The Settings tab allows screen size and colors to be changed.
- **Fax** - Is used to configure Fax information and access theFax Service Management Console which allows a Fax to be setup to receive or send faxes. It is also accessed using "Start", "Programs", "Accessories", "Communications", and "Fax".
- **Folder Options** - Allows the way files and folders are displayed to be modified. It includes the tabs "General", "View", "File Types", and "Offline Files". The View tab allows settings to specify whether the whole path is displayed, and whether hidden files are shown. The File Types tab specifies the application to be used to open files with extensions of specific types. The Offline Files tab allows setting of whether offline files are displayed and worked on. Once changed these files may be placed back into the online source. The default setting is on for Windows Professional and off for Windows Servers.

- **Fonts** - Allows viewing of current fonts and installation of new fonts. It is a shortcut to the fonts folder.
- **Game Controllers**- Allows configuration of joysticks and gamepads.
- **Internet Options** - These are options for Internet Explorer. They can be accessed from the Tools menu of IE. Tabs include General (Control of temporary files, history, and home page), Security (Allows trusted site settings, cookie settings, JavaScript settings and more), Content (Allows certificates, and storage of private information), Connections, Programs (Specification of programs for e-mail, HTML editing, newsgroups, and more), and Advanced tabs(JavaScript debugging options, HTML versions and more).
- **Keyboard** - Includes Speed, Input Locales (assign hotkeys), and Hardware (physical type of keyboard) tabs.
- **Mouse** and mouse pointer settings including mouse speed - Tabs include, Buttons (to set right or leeft handed mouse), Motion (speed), Pointers (Selection of mouse icons for normal, waiting, and other states), and Hardware (Sets up the mouse type such as PS2 Intellimouse and options available in the Device Manager).
- **Network and Dial-up Connection** - Can change computer name, and set to workgroup or domain. bindings are set here with the first one on the list to be the first one tried when services are attempted to be used. Also used to install NIC drivers. Tabs are:
    - Identification - computer name and domain or workgroup name
    - Services - Can add, or remove services and check their properties.
    - protocols - Can add or remove protocols or check their setup (properties).
    - Adapters - Add or remove NIC adapter drivers.
    - bindings - Where the binding priority may be set for various services.
- **Phone and Modem Options** - Modem properties and dialing rules are configured here.
- **Power Options** - Settings for how long hard drives and the monitor stays on are configured here. Tabs are "Power Schema", "Advanced", "Hibernate", "APM", and "**UPS**". The Power Schema tab controls how long of a period of inactivity to wait before turning off the monitor and hard drives. The Advanced Power Management (APM) tab controls older power management for laptops. The UPS tab is used to configure commands to execute when a UPS event occurs.
- **Printers** - Allows addition and deletion of printers. Right clicking and selection properties for a specific printer, opens a properties window with General (Driver Selection, Separator page, print processor [RAW, text], print test page), ports, Scheduling (priority, When printing starts relative to spooling, Hours of availability), Sharing, Security, and About tabs.
- **Regional Options** - Set up regional and language settings for NT. Select General, Numbers, Currency, Time, Date, or Input Locales tabs. The Regional Options tab is used to add additional language support.
- **Scanners and Cameras** - Digital cameras and scanners may be installed and configured here.
- **Scheduled Tasks** - Also called the "Task Scheduler", it is used to schedule programs or scripts to run at specific times. An "Add Scheduled Task" icon is in this folder.

- **Sounds and Multimedia** - Used to setup sound schemes and sounds to play for specific events. Tabs are "Sounds", "Audio", and "Hardware". The Sounds tab is used to associate events and sounds. The Audio tab allows the device to use for playing and recording sound to be set. The Hardware tab is used to configure and view multimedia devices.
- **System**
  - General - Describes the name and version of the system, who it is registered to and the hardware it is running on.
  - Network Identification - Allows the changing of the computer name, workgroup, or domain.
  - Hardware - Allows selection of hardware profiles and what to do if the system cannot determine which profile to use. Includes Hardware Wizard, Device Manager, and Hardware Profiles sections. The Hardware Profiles section allows additional hardware profiles to be created. The Device Manager section includes a Device Manager and a Driver Signing button. The Device signing allows configuration of what to do when system files are not digitally signed. Options are Ignore, Warn, or Block. **Sigverif command line utility is used to find unsigned files on the computer. Sfc.exe command line utility is used to replace any unsigned files with the original Microsoft version from the SystemRoot \System32\Dllcache directory.** The device manager includes the ability to configure:
    - Computer - Used to configure for multiple processors.
    - Disk drives
    - Display adapters
    - DVD/CD-ROM drives
    - Floppy disk controllers
    - Floppy disk drives
    - IDE ATA/ATAPI controllers
    - Imaging devices
    - Infared devices
    - Keyboards
    - Mice and other pointing devices
    - Modems
    - Monitors
    - Network adapters
    - PCMCIA adapters - (Card Services)
    - Ports (COM & LPT)
    - Sound, video and game controllers
    - System devices
    - Universal Serial Bus controllers
  - User Profiles - Allows user profiles to be added and changed which will affect desktop settings. **Roaming profiles may be set using this tab**.
  - Advanced - Used to set:

        - Environment variables - Used to set environment variables. If the path is modified to include applications run on Win95, these applications can be run when using a dual boot system or migrating from Windows 95.
        - Performance options- Allows performance to be optimized for applications or background services (all programs with equal priority). Also allows configuration of **page files**.
        - Startup and shutdown options - Allows **default selection of system to boot** and amount of delay before timeout. Allows selection of what to do when a stop error occurs. More than one choice may be selected.
            - Write an event to the system log
            - Send an administrative alert
            - Automatically reboot
            - Write debugging information (selection of none, small, kernel dump, and complete memory dump) to a specified file (default is Memory. dmp).
- **Users and Passwords (Only on 2000 Professional)** - Manage user access and passwords on this computer.
- **Wireless Link** - Configuration of infared devices. Tabs include "File Transfer", "Image Transfer", and "Hardware".
- **ports** - Allows configuration of serial and parallel ports.
- **SCSI Adapters** - SCSI adapters may be added or removed here. They are not configured here but may be configured at boot time using the manufacturer bIOS.
- **Server** - Tells who is connected, see shared resources, directory replication.
    - Users - Shows users logged onto the domain and where they are logged on from. (NT Server ONLY)
    - Shares - Shows resource name and path along with connected users.
    - In Use - Shows resources being used and the associated permissions.
    - Replication - Allows setup of directory replication.
    - Alerts - Controls where administrative alerts are sent
- **Services** - Can start or stop services or set them to automatically start when the system is booted. Description entries include:
    - Service - The name of the service.
    - Status - Whether the service is running.
    - Startup - Manual or automatic.

  buttons include:
    - Start
    - Stop
    - pause
    - Continue - Restart a service that is paused.
    - Startup - Set the service to be started by selecting one ot the radio buttons automatic, manual or disabled. Can also select one of two radio buttons called "System Account" or "This Account".
    - HW profiles - Allows selection of the hardware profile the service is being

configured for.

There is also a "Startup parameters" text box used to configure special startup parameters for the service.

- **Sounds**- Alignment of sound (.wav) files to system events.
- **Tape Devices** - This is where tape device drivers are added to allow the system to perform backups. They can be added using the detect button or using the drivers tab.
- **Telephony** - Used to configure part of RAS. The TApI (telephony application programming interface) and unimodem service provider are automaticllly installed. Unimodem works for modems on com ports and TApI is used for telephony applications.
- **UpS** - Configure the UpS. UpS command configuration is configured here so the systems may receive information from the UpS unit. Commands can be programmed here to execute when a UpS event occurs.

Windows 2000 Server Control Panel

This section only describes control panel applets and features not described for Windows 2000 Professional.

- **Licensing** - Allows setting of per server or per seat licensing.
- **Licensing** - Allows software package licenses to be added.
- **Mail** - Microsoft Mail client control.
- **Microsoft Mail postoffice** - Setup and control of the messaging server Microsoft mail post office.
- **ODbC** - ODbC database information routing control. Need database software or IIS ti be installed for this applet to be visible.
- **MacFile** - Allows setup of AppleShare services for Macintosh clients. Services for Macintosh must be installed for this applet to appear.
- **GSNW** - Gateway services for NetWare. Services for Netware must be installed for this applet to appear.
- **Monitoring Agent** - Network monitor tools and agent must be installed for this to appear.
- **RAS** - One of modem, ISDN, or X.25 must be installed to use this applet. The modems applet is used to install modems, ISDN, or X.25.
- **Server** - Tells who is connected, see shared resources, directory replication. This applet is included with NTWS but can be used to control users and shares on the domain so it is noteworthy here.
    - Users - Shows users logged onto the domain and where they are logged on from.
    - Shares - Shows resource name and path along with connected users.
    - In Use - Shows resources being used and the associated permissions.
    - Replication - Allows setup of directory replication.
    - Alerts - Controls where administrative alerts are sent

Active Directory Tools

These tools are available in "Administrative Tools" after Active Directory is installed.

- **Active Directory Users and Computers** - Active Directory Users and Computers is a Microsoft Management Console snap-in. It is started by selecting "Start", "Programs", "Administrative Tools", and "Active Directory Users and Computers". Only members of the Domain Admins or Enterprise Admins group can use this tool. This tool is used to create, configure, locate, move, and delete objects including:
    - User (automatically published) - Domain user accounts may be copied.
    - Group (automatically published)
    - Computer (Those in the domain are automatically published)
    - Contact (automatically published)
    - Domain
    - Organizational Unit (automatically published)
    - Shared folder
    - Printer (Most are automatically published) - Windows NT shared printers are not published automatically.

  Tabs from the OU Properties dialog box:
    - Group policy - Group policy object selections:
        - Windows Settings
            - Security Settings
                - Public key policies
                    - Automatic certificate request menu items:
                        - Action
                            - New
                                - Automatic Certificate Request
- **Active Directory Domains and Trusts**
- **Active Directory Sites and Services**
- **DCPROMO** Domain controller management tool which is run from the command line.
- **LDIFDE** bulk schema modification tool.
- **CSVDE** bulk schema update tool. Parameters:
    - -? - Help
    - -i - Mode for command. Choices are import, export, or modify.
    - -f - File name
    - -v - Verbose mode
    - -p - Specify the port for the socket. The LDAP default is 389.
- **Active Directory Connector (ADC)** It simplifies administration among multiple directory services. The ADC can aid Windows 2000 implementations where Exchange Server is deployed. It can replicate Active Directory information, and Exchange Server 5.5 information as well. It comes with Windows 2000 and Exchange 2000. It:

- Uses LDAP to perfrom replication.
- Only replicates changes.
- Hosts all active Active Directory replication components.
- Supports multiple connections on one server.
- Maps objects for replication.

Requirements:

- Windows 2000 Server
- Available TCP Port
- Microsoft Exchange Server 5.5 or 2000.
- LDAP version 3

Connection agreements configure directory synchronization between Exchange and Active Directory and one or more are supported with ADC. Items used to configure a connection agreement:

- Server name
- Targer containers
- Objects to be synchronized
- Synchronization schedule

ADC Installation:

1. ADC requires a service user account and password.
2. Put the Windows 2000 Server installation CDROM in the computer.
3. Enter the directory \Valueadd\MSFT\Mgmt\ADC.
4. Double click on setup.exe.
5. Select the "Microsoft Active Directory Connector Service component" to install ADC and the"Microsoft Active Directory Connector Management component" to install the ability to manage the service. The Management component can be installed on Windows 2000 Professional computers to allow ADC management from them.
6. Choose a directory to install the components to.
7. Enter the account name and password for the service to use.
8. Continue and finish the installation.

ADC Configuration:

1. Run the Administrative tool, "Active Directory Connector (ADC) Management".
2. Right click the server to configure and select "properties" to see the properties dialog box. This is used to configure connection agreements between Active Directory and the Exchange 5.5 directory service. The following tabs exist in the box:
    - General - Select replication direction as "Two way", "From Exchange to Windows", or "From Windows to Exchange". Set the connection name, and the server to run the connection agreement. For slow network connections, the agreement can use Exchange Server's **Site Replication Service (SRS)**.
    - Connections - Configure the bridgehead servers to handle the connection. The servers receiving updates only require write permission. Select the

Windows server name, the Windows authentication protocol, the Exchange server, The Exchange server port, and the Exchange server authentication protocol.

- Schedule - Set synchronization schedule. The registrey setting at **"HKEY_LOCAL_MACHINES\System\CurrentControlSet\Services \MSADC\Parameters"** can be used to reduce the default polling schedule. The parameters that are configurable are:
  - Name - The delay in seconds to wait between checking for updates. The default value is every 5 seconds.
  - Type - DWORD
  - Data - Seconds to wait between cycles.
- From Exchange - Specify the objects to replicate and the Exchange receipient containers.
- From Windows - Specify objects to be synchronized and the containers that will receive objects. The option "Replicate secured Active Directory objects to the Exchange Directory" can be checked and the objects can be filtered using Discretionary Access Control Lists (DACLs).
- Deletion - Use this tab to configure object deletion behavior. When objects are deleted, the deletions are stored in SystemRoot\System32\MSADC \Connection_Agreement_Name\NT5.LDF for Active Directory and SystemRoot\System32\MSADC\Connection_Agreement_Name\Ex55.CSV for Exchange.
- Advanced - Configure "Paged results" configures the quantity of entries to be synchronized for each request. The settings are "Windows Server entries per page" and "Exchange Server entries per page". Checkbox options include "This is a primary Connection Agreement for the connected Exchange organization", and "This is a primary Connection Agreement for the connected Windows Domain". Choices for "When replicating a Mailbox whose Primary Windows Account does not exist in the domain" are:
  - Create a Windows Contact
  - Create a Disabled Windows User Account
  - Create a New Windows User Account

ADC Event logging levels:

- None - Only log critical events
- Minimum - Log LDAP session errors, success or failure of added or removed user accounts.
- Medium - Log directory object events and proxy errors.
- Maximum

The Administrative tool "Active Directory Connector Management" is used to set up event logging. ADC Event Logging categories:

- Replication
- Account Management - Events while writing to or deleting an objects.
- Attribute Mapping - Events while attributes are mapped between AD and

Exchange.

- Service Controller - Events when the ADC service is stopped or started.
- LDAP Operations - Events when LDAP accesses the directory.

Management Console Tools

Computer Management

The computer management console has the following categories of tools:

- System Tools
- Storage
- Services and Applications

System Tools

- **Event Viewer** - Used to view logs about events associated with file and directory replication, DNS, security, and more.
- **System Information** - Replaces Windows NT Diagnostic Administrative Tool. Listed folders include:
  - System Summary - Lists operating system version, installed services packs, processor, and memory.
  - Hardware Resources - Interrupt, DMA, and I/O address usage are listed.
  - Components - Information about peripheral devices such as modems, ports, USB, and display is listed.
  - Software Environment - Lists installed software including services and drivers.
  - Internet Explorer - Internet Explorer configuration information.
  - Applications - Information about installed application programs.
- **Performance Logs and Alerts** - Includes:
  - Alerts - Alerts can be sent when system performance falls below minimum settings.
  - Counters - Objects that can be monitored.
  - Trace Logs
- **Shared Folders Tool** - Entered from Administrative Tools, "Computer Management" or by right clicking on "My Computer" and selecting "Manage". Categories:
  - Shares - Used to create shares and list all system shares.
  - Sessions - Any open session from the local computer or a remote computer is listed.
  - Open Files - Files being used by users or other computers are listed.
- **Device Manager** - Used to view all system resources.
- **Local Users and Groups** - Used to make user and group accounts on the local computer.

Storage

- **Disk Management** - This is a snap-in for the Microsoft Management Console (MMC) and is the replacement for the Windows NT Disk Administrator. Only a member of the Administrators group can use this tool. It can manage local or remote disk volumes. It is used to:
  - Make and format partitions.
  - Create, format, or delete simple, spanned, mirrored, striped, or RAID-5 volumes.
  - Modify a disk from basic to dynamic type or vice versa, create. A disk can only be converted from dynamic to basic by first deleting all the volumes in the dynamic disk.
  - Display information about the disk including the disk type (basic or dynamic), disk number, disk size and disk status. Disk status can be:
    - Online
    - Foreign - Remote disk
    - No Media - For removable disks.
    - Offline - For dynamic disks that cannot be reached due to various possible reasons. The disk may be remote.
    - Online (errors) - There are errors on the disk.
    - Unreadable - Errors preventing access have occurred.
    - Unrecognized - Unknown type of disk.

    It will also provide volume information including size, name, and status. Volume status can be:
    - Healthy
    - Healthy (boot) - Active primary partition on the first drive.
    - Healthy (system) - if same as boot volume, it is called "Healthy (boot)".
    - Failed
    - Failed Redundancy - A fault tolerant volume is not on line.
    - Failed Redundancy (At Risk) - A fault tolerant volume that has lost fault tolerence has errors detedted on it.
    - Healthy (At Risk) - Errors have been detected on the volume.
    - Initializing - Dynamic volume being initialized.
    - Regenerating
    - Resynching - Mirrored volumes are being resynchronized
  - Recover from drive failures.

  To install Disk Management:

  1. From an MMC console, click "Add/Remove Snap-in".
  2. Click "Add", select "Disk Management".
  3. Select the computer to install on, and finish.

  To start Disk Management, do one of:

- Right click the "My Computer" icon on the desktop and select "Manage" and click "Disk Management" in the left pane.
- Select "Start", "Programs", "Administrative Tools", and "Computer Management". In the left pane of the computer management box in the MMC, select "Disk Management".
- Run the program "Diskmgmt.msc" from the command line.
- Double click Diskmgmt.msc in the SystemRoot\Winnt\System32 directory.

Volume and disk properties dialog box tabs:

- General - Label, volume type, capacity and use are displayed. Options include "Compress drive to save disk space" and "Allow Indexing Service to index this data for fast file searching".
- Tools - Contains defragmentation, backup and error checking tools.
- Hardware - Device properties are listed with the type and name of the disk drives.
- Sharing - Volume sharing options are set including permissions, user limits and share name.
- Security (NTFS volumes) - Can set user, group and computer permissions along with auditing configuration.
- Quota (NTFS volumes) - Can enable disk quotas and set disk quota administration values. Quota management must be enabled. Warning levels may be set and hard limits may also be set. Disk space may be denied to users who exceed their quota limit. The events may be logged when the user exeeds their warning and/or quota limit.
- Web Sharing - Can share the volume on a web site.

Disk properties:

- Disk - Number
- Type - Basic, Dynamic, or Removable
- Status - Online, offline, foreign, or unknown.
- Capacity
- Unallocated Space
- Device Type - IDE, EIDC, SCSI, etc.
- Hardware Vendor
- Adapter Name
- Volumes Contained On This Disk

- **Disk Defragmenter** - This is a snap-in for the Microsoft Management Console (MMC) and is used to analyze and defragment volumes.

  To start Disk Defragmenter, do one of:

  - Right click the "My Computer" icon on the desktop and select "Manage" and click "Disk Defragmenter" in the left pane
  - Select "Start", "Programs", "Administrative Tools", and "Computer Management". In the left pane of the computer management box in the MMC, select "Disk Defragmenter".

- **Logical Drives** - This is a snap-in for the Microsoft Management Console (MMC) and is used to change logical drive labels, configure security settings, and view properties.

  To start Logical Drives, do one of:

  - Right click the "My Computer" icon on the desktop and select "Manage" and click "Logical Drives" in the left pane
  - Select "Start", "Programs", "Administrative Tools", and "Computer Management". In the left pane of the computer management box in the MMC, select "Logical Drives".
- **Removable Storage** - Information about removable storage media such as tapes and CD-ROMS is provided.

Services and Applications

Is only available on Windows 2000 Servers. It lists information about installed services such as DNS.

- **WMI Control** - Windows Management Instrumentation control allows monitoring and controlling system resources.
- **Services** - Lists all computer services
- **Indexing Service** - Creates an index of files on the computer allowing search functions to work better.

- **Windows Scripting Host (WSH)** assists administrators in creating many users and groups quickly
- **Fax Service Management**
- **Security Configuration and Analysis**

Windows 2000 MMC Tools

The Microsoft Management Console (MMC) provides a common environment for snap-ins. Snap ins can be added when required to control and manage different parts of the computer or network. (The below items may be part of the Computer Management tool.

Microsoft Management Console Tools

- **Disk Management** - This is a snap-in for the Microsoft Management Console (MMC) and is the replacement for the Windows NT Disk Administrator. Only a member of the Administrators group can use this tool. It can manage local or remote disk volumes. It is used to:
  - Make and format partitions.
  - Create, format, or delete simple, spanned, mirrored, striped, or RAID-5 volumes.
  - Modify a disk from basic to dynamic type or vice versa, create. A disk can only be converted from dynamic to basic by first deleting all the volumes in the dynamic disk.
  - Display information about the disk including the disk type (basic or dynamic), disk number, disk size and disk status. Disk status can be:
    - Online
    - Foreign - Remote disk
    - No Media - For removable disks.
    - Offline - For dynamic disks that cannot be reached due to various possible reasons. The disk may be remote.
    - Online (errors) - There are errors on the disk.
    - Unreadable - Errors preventing access have occurred.
    - Unrecognized - Unknown type of disk.

    It will also provide volume information including size, name, and status. Volume status can be:
    - Healthy
    - Healthy (boot) - Active primary partition on the first drive.
    - Healthy (system) - if same as boot volume, it is called "Healthy (boot)".
    - Failed
    - Failed Redundancy - A fault tolerant volume is not on line.
    - Failed Redundancy (At Risk) - A fault tolerant volume that has lost fault tolerence has errors detedted on it.
    - Healthy (At Risk) - Errors have been detected on the volume.
    - Initializing - Dynamic volume being initialized.
    - Regenerating
    - Resynching - Mirrored volumes are being resynchronized
  - Recover from drive failures.

To start Disk Management, do one of:

- Right click the "My Computer" icon on the desktop and select "Manage" and click "Disk Management" in the left pane.
- Select "Start", "Programs", "Administrative Tools", and "Computer Management". In the left pane of the computer management box in the MMC, select "Disk Management".

- **Disk Defragmenter** - This is a snap-in for the Microsoft Management Console (MMC) and is used to analyze and defragment volumes.

  To start Disk Defragmenter, do one of:

  - Right click the "My Computer" icon on the desktop and select "Manage" and click "Disk Defragmenter" in the left pane
  - Select "Start", "Programs", "Administrative Tools", and "Computer Management". In the left pane of the computer management box in the MMC, select "Disk Defragmenter".
- **Logical Drives** - This is a snap-in for the Microsoft Management Console (MMC) and is used to change logical drive labels, configure security settings, and view properties.

  To start Logical Drives, do one of:

  - Right click the "My Computer" icon on the desktop and select "Manage" and click "Logical Drives" in the left pane
  - Select "Start", "Programs", "Administrative Tools", and "Computer Management". In the left pane of the computer management box in the MMC, select "Logical Drives".
- **Device Management**
- **Fax Service Management**
- **Indexing Service**
- **Performance Logs and Alerts**
- **Security Configuration and Analysis**
- **System Information**

Windows 2000 Network Tools

- **Nslookup**
- **IPConfig** - Options:
  - /ALL
  - /RELEASE - Release address
  - /RENEW - Renew Address
  - /REGISTERDNS - Refresh all DHCP leases.
  - FLUSHDNS - Purge DNS resolver cache.
- **Ping**
- **Netmon**

Windows 2000 Network Monitor

It is installed from the Network applet in control panel using the "Add/Remove Programs" applet. It is listed in "windows Components", Management and Monitoring Tools", and "Network Monitor". This is not a fully functional network monitor. The tool that ships with SMS, a separate purchase, is fully functional. Network Monitor can:

- Capture frames coming from or going to the server
- Capture broadcast or multicasts.

This tool does not set the network card in promiscuous mode. It can be invoked from administrative tools after the install. Also there is a control panel applet installed for this tool. This tool can also detect other copies of Network Monitor running on other domain computers and what users are running it. Display sections include:

- Bar graphs - Network activity real time information. Graphs include network utilization, broadcasts per second, bytes per second, and frames per second.
- Session statistics - Sessions between this computer and others.
- Station Statistics - Includes frames sent and received, bytes sent and received, multicasts sent, directed frames sent, broadcasts sent, and network address.
- Summary (Total) statistics - Summation of captured statistics, network statistics, MAC statistics, MAC errors, and per second statistics.

Captured data is saved in the default directory \WINNT_ROOT\system32\netmon \captures. A filter on the Monitor can be established to collect the frames you want. Filtering may be done based on:

- Protocol
- Address
- Protocol Properties

To see other users using Network Monitor, select "Identify Network Monitor Users" while in the Network Monitor program.

Network Monitor is installed from the control panel network applet services tab. It is "Network Monitor Tools, Agent". Once installed, there is a "Network Monitor" applet in the control panel where the password for the Network Monitor program may be set or changed. A program called "Network Monitor" is added to administrative tools.

Network Monitoring Agent Installation?

When installed the following is added:

- Control Panel : Monitoring Agent
- Administrative Tools: Network Monitor.

Monitoring agent has the following characteristics:

- Dual level password.
- Detection of other NT or SMS monitors.

Network Monitor Menu selections

- File
- Capture
  - Start
  - Stop
  - Stop and View
  - Pause
  - Continue
  - Display Captured Data - Displays captured frames stored in the network buffer.
  - find All Names
  - Clear Statistics
  - Addresses
  - Buffer Settings
  - Filter - Set up filtring for capturing packets. This allows packets with specific characteristics to be captured.
  - Networks
  - Trigger
  - Dedicated Capture Mode
  - Save Configuration
- Tools
  - Identify Network Monitor Users - Will show other computer's names that are running network monitor along with the user name, MAC address, network monitor state (running, capturing, or transmitting), and network monitor version.
- Options
- window

Monitoring Agent?

The monitoring agent selected from the control panel. This agent allows specification of both a display and a capture password. This way some users may be allowed to capture data and

others may display it.

System Performance Monitoring

The System Monitor Windows 2000 tool replaces the Windows NT Performance Monitor tool (although I think it is the same tool, renamed for marketing reasons, and to make certification testing more confusing). System Monitor uses:

- **Objects** - A part of the computer system or operating system such as the processor, logical disk, memory, thread and other objects.
- **Instances** - When there are more than one occurance of an object such as threads.
- **Counters** - Used to measure some characteristic of an object. Specific counters are available for specific objects to measure their performance or use.

System Monitor can be used as was Performance Monitor to do some of the following:

- Create a baseline after system installation to compare system performance over time.
- Monitor system resource use.
- Find any performance problems.
- Determine bottlenecks to performance.
- Monitor changes in performance over time.

To start System Monitor select "Performance" in administrative tools. This tool runs on Windows 2000 Professional and Windows 2000 servers. Alternatively Performance Monitor may be started on the command line by typing "perfmon"

Ways to View Statistics

- **Alerts** - The administrator can be notified when a counter exceeds or falls below a preset value. Saved as *.pma file. The computer for the alert along with object, counter, and threshold value must be specified. A specified program may be run if an alert is triggered.
- **Chart** - The default view. Graphs and histograms (vertical bar charts) are used. To switch to histograms, use the menu item "Options", "Chart" selection. The Gallery section has Graph and Histogram radio button selections. Graphs display data every second and display 100 seconds worth of data. Chart file saved as *.pmc. A particular counter may be highlighted by clicking on the counter and pressing the backspace key. Chart Options include:
    - Legend checkbox?
    - Value Bar checkbox?
    - Vertical Grid checkbx?
    - Horizontal Grid checkbox?

    - Vertical Lables checkbox?
    - Vertical maximum textbox (Default is 100).?
    - Gallary section - Graph and Histogram checkboxes?
    - Update Time section - Periodic Updates and Manual Updates checkboxes with Interval (seconds) textbox.?

  Statistical values displayed include:
    - Last - The most recent measurement of the counter on the chart.
    - Average - The average measurement of the counter on the chart.
    - Minimum - The lowest measurement of the counter on the chart.
    - Maximum - Highest measurement of the counter on the chart.
    - Duration - The amount of time on the chart.
- **Log** - Used to create data in log files for future analysis. Data can be acquited from several systems in one log file. Log files can be used to create charts, reports, or alerts by sending them back through performance monitor. Saved as *.pml. This information may be exported to a spreadsheet or database.
- Report - Used to show a large number of objects and counters at one time. It is a list of counters and their average values. Saved as *.pmr.

Objects and Counters

- Cache - Level 2 cache. Data Map Hits %
- Logical Disk* - % Free Space
- Memory* - Counters:
    - Pages/Sec - How much RAM and virtual memory on the hard drive are being swapped. If above 5 or 6 on average, more RAM is needed.
- Network interface* - Counters:
    - Bytes Total/sec
- Objects - Process and thread counts
- Paging file - Virtual memory. Counters:
    - % Usage - The amount of the paging file being used. Create a larger paging file or add RAM if the number is near 100%.
- Physical disk - Counters:
    - Disk Queue Length - The number of disk reads and writes in queue to be done. - If above 4 or 5 on average, a faster hard drive is needed.
    - Average disk Sec/Transfer
    - % disk time - The percent of time the disk is busy doing reads or writes. A high number near 100% indicates a disk or drive controller bottleneck.
- Process - Currently running programs. Counters:
    - % Processor Time - The percent of time the processor is used by this process object including all its threads.
- Processor* - Counters:
    - % Processor Time - A number close to 100% indicates the processor is a bottleneck.

- Redirector
- Server - Counters:
    - Bytes Total/Sec - The total number of bytes sent through or received through all network cards on a computer by the server service.
- System - NT Performance. File Read or Write Operations/Sec
- Thread - Thread performance. Counters:
    - % Processor Time - The percent of time the processor is used by this thread object.

Windows 2000 Guide Contents Page

Windows 2000 Tools

Graphical Tools

- **Windows 2000 Help Troubleshooter**
- **Users and Passwords** - This is a tool accessible from the Control Panel on Windows 2000 systems and is used for managing domain and local user accounts. Tabs include:
  - General - Used to add and remove users and set passwords.
  - Group Membership. Selections:
    - Standard user - A power user on the local computer that can install programs but not read other user's files.
    - Restricted user - A user that cannot install programs or change system settings.
    - Other - To make the user a member of any other group on the local computer such as Administrators.
- **Active Directory Users and Computers** - Active Directory Users and Computers is a Microsoft Management Console snap-in. It is started by selecting "Start", "Programs", "Administrative Tools", and "Active Directory Users and Computers". Only members of the Domain Admins or Enterprise Admins group can use this tool. This tool is used to create, configure, locate, move, and delete objects including:
  - User (automatically published) - Domain user accounts may be copied.
  - Group (automatically published)
  - Computer (Those in the domain are automatically published)
  - Contact (automatically published)
  - Domain
  - Organizational Unit (automatically published)
  - Shared folder
  - Printer (Most are automatically published) - Windows NT shared printers are not published automatically.

  Tabs from the OU Properties dialon box:
  - Group policy - Group policy object selections:
    - Windows Settings
      - Security Settings
        - Public key policies
          - Automatic certificate request menu items:
            - Action
              - New
                - Automatic Certificate Request
- **System Policy Editor** - To start the System Policy Editor, click "Start", "Run", and type

"poledit" in the text box. System policy settings for all users on the domain set using the System Policy Editor are merged with local profiles. User logon restrictions are set in the user manager for domains. A policy may be set to automatically log users off during restricted logon hours.

- **Distributed File System** - Used to manage distributed file systems. Options:
  - Action
    - New DFS Root
    - Display an Existing DFS Root
- **Windows Task Manager** - Can be used to start and stop applications, change process priority, and monitor performance statistics. Can enter the task manager one of the following ways:
  - Press CTRL ALT DEL and select Task Manager
  - Press CTRL SHIFT ESC
  - Right click the taskbar and select Task Manager
  - Select "Start, "Run", and type "taskmgr".

  Tabs:
  - Applications
  - Processes - Shows PID, CPU, CPU time, and memory usage.
  - Performance - Shows:
    - CPU usage and history
    - Memory usage and history
    - Total handles, threads, and processes
    - Physical memory
    - Commit Charge - Memory allocated to the system or programs.
    - Kernel memory
- **Setup Manager utility** (SETUPMGR.EXE on the Windows NT install CD at \SUPPORT \TOOLS\deploy.cab) may be used to set up unattended installation answer file. On Windows 2000, this program is called the Setup Manager wizard and can be installed from the resource kit on the CDROM by running \Support\Reskit\Setup.exe.Options:
  - Create a new answer file.
  - Create an answer file that duplicates this computer's configuration.
  - Modify an existing answer file.
  - **Sysprep Install** - System preparation utility located on the CDROM in the \SUPPORT\TOOLS\Deploy.cab file. Works on non-domain controller windows 2000 computers. This utility allows a Windows 2000 hard drive to be copied to other computers.
  - **Security Configuration and Analysis** - An MMC snap-in which is used to analyze security on your system. To do a security analysis:
    - Create a security database store the results of the security analysis.
    - Open and change a security template .
    - Import a security template which is used to compare secure settings against. There are several security templates in the \Windir\Security \Templates directory. There are several of which some are for domain

controllers and others for member servers.
        - Perform the analysis. Policies that do not match the template will have an "x" next to them.
    - **Registry editor** - Regedit32 or Regedit.
- **Imaging** - In the Accessories folder this tool is the only tool that can transfer images from digital cameras.

Command Line Tools

- **cipher** - Used to encrypt files on NTFS volumes. Syntax:

  cipher /[parameter] [filename]

  Parameters:
    - /d - Decrypt files or folders.
    - /e - Encrypt files or folders.
    - /f - Force encryption or decryption regardless of the file or folder current state.
    - /I - Ignore errors.
    - /q - Quiet mode, displaying only important information.
    - /s:dir - Encrypt or decrypt subfolders and files also.
- **dcpromo.exe** - Used to demote a Windows 2000 Active Directory domain controller to a domain member server.
- **ipsecmon.exe** - The IPSec monitoring tool can be used to provide a summary of the local computer IPSec connections. This tool can be started by clicking on "Start", "Run" and entering "ipsecmon.exe" and pressing the ENTER key.
- **Secedit** - It is used to perform computer security configuration and analysis. For help type "secedit /?" on the command line.
- **Sigverif** - Used to find unsigned files on the computer.
- **Sfc.exe** - Used to replace any unsigned files with the original Microsoft version from the SystemRoot\System32\Dllcache directory.
- **CONVERT.EXE** - Resides on WINNT40\SYSTEM32\CONVERT.EXE. Will convert FAT partitions to NTFS partitions with the command "convert D: /FS:NTFS". The syntax is:

  convert volume /FS:NTFS [/V]

  The /V switch allows the program to run in verbose mode. Convert must have exclusive drive access to perform the conversion.

- **NET** - Used to perform network operations. Subcommands:
    - USER - To create users. For help type: "net help user | more".
    - USE - This is a method to map a network shared folder to a drive number. Syntax:

NET USE DRIVE: \\computername\sharename

- view - Used to browse the network Options are "/domain" to see network domains and workgroups, "/domain/domainname" to see computers on a domain or workgroup. "\\server" to see available shares on a server.

- **Windows 2000 Support Tools**
  - MoveTree.exe - Used to move an object to another domain in Active Directory

Troubleshooting Tools

- Troubleshooters - Series of questions.
- Add/Remove Hardware
- Device Manager - Displays device resource settings.
- System Information - To open this tool, right click on "My Computer", and select "Manage". Expand the "System Information" section to reveal:
  - System Summary - Shows the operating system name and version being used and other hardware information.
  - Hardware Resources. Options:
    - Conflicts/Sharing - Shows any resource conflicts.
    - DMA - Shows DMA addresses in use.
    - Forced Hardware - Shows any manually configured devices.
    - I/O - Shows ports.
    - IRQs - Shows interrupts in use.
    - Memory - Shows the memory in use and what devices are using the memory.
  - Components
  - Software Environment
  - Internet Explorer 5

Windows 2000 Guide Contents Page

Managing Windows 2000 Services

The services on the computer can be managed through the Computer Management utility or the MMC. To manage a cervice open the Services window in one of the utilities and double click on the service to manage. The service properties dialog box will open.

Service Properties Dialog Box

Tabs:

- General
  - Name of the service
  - Path to the program that provides the service
  - How the service is started such as manual.
  - Status
  - Buttons alowing the service to be started, stopped, paused, or resumed.
- Log On - Configure the account used to run the service. A hardware profile the service is to be associated with can be selected. The service can be enabled or disabled in each hardware profile.
- Recovery - Set action to take if the service fails or fails to start on the first, second or additional failures.
  - No action
  - Restart the service
  - Run a file
  - Reboot the system
- Dependencies - shows services that must run before the selected service can run. These are services the selected service depends on to run.

Windows 2000 Connections

The Windows 2000 computer creates one local area connection for each network adaptor card installed.

Connection Types

- Local area connections - Properties:
  - Clients or services used by the connection.
  - The protocols bound to each client or service **(bindings)**.
  - **Provider order** specifies the order the bound protocols are used by the client or service when making a connection.
- Dial-up connections
- Direct cable connections between two computers
- Virtual private networking (VPN) connections
- Connections coming into a computer over a port such as over a modem or infared port.

A high speed connection is considered to be 512Kbps of bandwidth with 128Kbps available.

Modems

Modem Installation tools:

- Control Panel, "Add/Remove Hardware" applet.
- Control Panel, "Phone and Modem Options" applet. Tabs:
  - Dialing Rules -
  - Modems - Shows modems and ports they use. Allows addition or removal of modems along with setting properties. Three properties tabs:
    - General - Properties allows modem speaker volume and maximum port speed to be set.
    - Diagnostics - Can set to record log files.
    - Advanced - Can set custom initialization strings.
  - Advanced

Network and Dial-up Connections

Network and dial-up connections are created and configured from the "Network and Dial-up Connections" folder which is accessible from the "Start", "Settings" menu. It us used to create:

- Internet connections - Internet connection sharing is done so other users on the network can share a connection to the internet. Internet connection sharing causes the computer to become a DHCP server, DNS proxy server and change the IP address of the computer to 192.168.0.1.
- Connections to remote access servers
- Direct connections to other computers
- Set up a computer to allow incoming connections
- Create VPN connections

Dial-up Connection Properties

Dial-up connections can be set by clicking on the connection in the "Dial-up Connections" folder. It is used to install network clients and services. Tabs include:

- General - Select the modem or device to use for the connection. Set the phone number and dialing rules. The configure button dialog box includes setting modem maximum speed, protocol, hardware flow control to be set, modem error control to be enabled, modem comptession to be enabled, an initialization script to be run, and the modem speaker to be enabled.
- Options - Can set to display progress of connection, prompt for name and password, include Windows logon domain, prompt for phone number. Cal also set redialing options including the number of redial attempts, time between attempts, and idle time before hanging up. Can configure X.25 settings for connections to X.25 networks. The Windows logon domain option is for the case when there are several Windows 2000 domains on the network being connected to.
- Security
- Networking
- Sharing - Allows the sharing of internet connections by several computers at one time through the computer being configured. On demand dialing can also be enabled.

Windows 2000 Supported Network Protocols

Protocols installed on Windows 2000 systems are normally available to all connections. Protocols are installed and configured from the "Network and Dial-up Connections" folder.

- TCP/IP
- NetBEUI
- NWLink IPX/SPX - Frame types are Ethernet_II, Ethernet SNAP, Ethernet 802.3 (older), and Ethernet 802.2 (newer). May need to configure to use both 802.2.and 802.3.
- AppleTalk - Only available for incoming and local area connections.
- DLC - For connections with older Hewlett Packard printers. This is only available for local area connections.

- Network Monitor Driver

Several transport protocols listed above may be bound to any number of clients or services. This is called binding. Also the order in which a specific transport protocol is used when making a new connection may be set. This means that the connection may be attempted with one protocol, then if that fails, the next protocol is tried. The order is set for connections on a local area connection on the computer. The settings of the bindings is setting the order in which clients are tried when making the connections. Some of these clients include "Client for Microsoft Networks" and "Client Service for NetWare". These are set in the "Network and Dial-up Connections" folder by selecting "Advanced", and "Advanced Settings".

Available Clients and Services

Client/Service	Description	Windows 2000 Professional	Windows Server/ Advanced
Client for Microsoft Networks		Yes	Yes
Client Service for Netware		Yes	**No**
Gateway and Client Services for Netware		No	Yes
File and Print Sharing for Microsoft Networks		Yes	Yes
FTP Server		Yes	Yes
File Services for Macintosh		No	Yes
FrontPage 2000 Server Extensions	Allows web pages to be published on web servers using FrontPage	Yes	Yes
Indexing Service	Indexes documents on hard drives into a database to speed search capabilities.	Yes	Yes
Internet Information Service (IIS)		Yes	Yes
Message Queuing Service	Allows distributed applications to communicate to each other on the network.	Yes	Yes
Print Services for UNIX		Yes	Yes

QOS Packet Scheduler	Allows network packet scheduled deliveries. Required for computers using applications managed by QOS Admission Control Service.	Yes	Yes
RIP Listener	Listens to RIP routing messages.	Yes	No
SAP Agent	Allows advertising and maintenance of services using TCP/IP, IPX/SPC, or NetBEUI protocols.	Yes	Yes
Script Debugger		Yes	Yes
SNMP		Yes	Yes
Simple TCP/IP Services	Five TCP/IP Services (Character Generator, quote of day, etc...)	Yes	Yes
SMTP Services		Yes	Yes
Visual InterDev RAD Remote Deployment Support	Applications can be remotely deployed on the Web server.	Yes	Yes
World Wide Web Server		Yes	Yes
Certificate Services		No	Yes
Connection Manager Components	Allows custom dial-up profiles to be created allowing remote users to connect to the network.	No	Yes
Internet Authentication Service (IAS)	Authenticates users on the network who are dialing in or using VPN.	No	Yes
Cluster Service		No	Yes
COM Internet Services Proxy	Lets distributed HTTP applications communicate using IIS over the network.	No	Yes
DHCP		No	Yes

Network Load Balancing		No	Yes
Network Monitor Tools	Allows network monitoring and analysis by capturing and analyzing network packets.	No	Yes
NNTP Service		No	Yes
Print Services for Macintosh		No	Yes
QOS Admission Control Service	Quality of Service allows network bandwidth allocation management.	No	Yes
Remote Installation Services (RIS)	Allows Windows 2000 to be installed remotely.	No	Yes
Remote Storage		No	Yes
Site Server ILS Services	Allows IP multicast conferences to be published on the network	No	Yes
Terminal Services		No	Yes
Windows Internet Name Service (WINS)		No	Yes
Windows Media Services	Multimedia content can be streamed to users.	No	Yes

Configuring Services

The Computer Management MMC is used to configure network services. This is done by right clicking "My Computer", selecting "Manage", click the + next to "Services and Applications", and highlight "Services". This starts the Services tool. At this point services can be managed by right clicking on them. They can be stopped, started, paused, resumed, and restarted. Services can be set to have one of the following start up status':

- Automatic - The service starts when the system boots.
- Manual - An application can start the service.
- Disabled - The service can not be started by an application.

A service can be configured to use a particular account when logging onto the system. Service dependencies can be checked.

When a service fails, there are several options that can be set for recovery:

- Take no action
- Restart the service
- Run a file
- Reboot the computer

Windows 2000 TCP/IP

The menu selection "Start", "Settings", "Network and Dial-up Connections" is used to configure TCP/IP. Two ways for a computer to get its IP address:

- Using DCHP from a DHCP server.
- Manual configuration.

NetBIOS Name Resolution - See the Network Certification Reference and the WINS Section in the Windows NT Server Reference

- WINS
- lmhosts - In \SystemRoot\system32\drivers\etc in Windows 2000 and NT. In Windows NT it is stored in C:\Windows. The #DON keyword indicated the machine is a domain controller. A sample line:

  10.1.0.144 dcmyorg #DOM:mydomain

  A computer that is not a domain controller will not have the information after the #DOM. Notice that the name of the domain is included.

WINS Installation:

1. Open the Control Panel.
2. Run the "ADD/Remove Programs" applet.
3. Click "Add/Remove Windows Components"
4. Highlight "Networking Services" and click "Details".
5. Select the "Windows Internet Name Service (WINS)" checkbox.
6. Click OK and continue.

To make a Windows 2000 computer be a WINS Proxy, edit the registry at HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Services/NetBT. Add the parameter "EnableProxy with a value type of REG_SZ with a value of 1.

WINS replication is configured using the WINS administrative tool. Select the WINS server to configure, then click "Action", "New Replication Partner". Select "Action" and "Properties" to configure when replication will occur. Types of partners:

- Push - Notifies its partner when its database changes.

- Pull - Requests database changes from the WINS server.
- Push/Pull

If one server is push, the other must be pull, and vice versa. The WINS administrative tool is used to monitor the WINS server. Can view the last replication data and time, NetBIOS queries received, and the actual database contents. The System Monitor may also be used to monitor the WINS server.

Use the "Network and Dial-up Connections" tool selected from "Start", and "Settings" to configure client computers to use WINS servers for NetBIOS name resolution.

DHCP Relay Agent

Used to forward DHCP requests through routers to the DHCP server. Usually the router is configured as the DHCP relay agent, but any computer on the segment to be serviced may be configured as the agent. The "Routing and Remote Access" administrative tool is used to install and configure the DHCP relay agent.

Ports

Windows 2000 server computers are configured as a router or RAS server five each of L2TP and PPTP ports are configured. A demand-dial interface is required for demand dial routing and requires a modem or VPN connection. The "Routing and Remote Access" tool must be used to create demand-dial interfaces and it is also used to configure ports. If the server is configured as a VPN server, 128 PPTP ports and 128 L2TP ports are configured. Up to 30,000 of each type of port can be supported.

Windows 2000 DHCP

Dynamic host configuration protocol is used to automatically assign TCP/IP addresses to clients along with the correct subnet mask, default gateway, and DNS server. Two ways for a computer to get its IP address:

- Using DHCP from a DHCP server.
- Manual configuration.

DHCP Scopes

- Scope - A range of IP addresses that the DHCP server can assign to clients that are on one subnet.
- Superscope - A range of IP addresses that span several subnets. The DHCP server can assign these addresses to clients that are on several subnets.
- Multicast scope - A range of class D addresses from 224.0.0.0 to 239.255.255.255 that can be assigned to computers when they ask for them. A multicast group is assigned to one IP address. Multicasting can be used to send messages to a group of computers at the same time with only one copy of the message. The Multicast Address Dynamic Client Allocation Protocol (MADCAP) is used to request a multicast address from a DHCP server.

One way to create a superscope is to set up a range of addresses that span more than one subnet. Another way is to create several scopes and merge them using the "New Superscope" wizard by selecting "Action" and "New Superscope"

There are global and scope options. **Global** options apply to all client computers. **Scope** options apply to specific subnets or range of IP addresses. DHCP RFCs are 1533, 1534, 1541, and 1542.

Beyond the address assignments DCHP can assign other **options** which can be applied globally or to various scopes. Some options and address configuration includes:

- IP address
- Netmask
- Default Gateway address
- Primary and secondary DNS server addresse(s)
- NetBIOS Name server (NBNS) address(es).
- Lease period in hours
- IP address of DHCP server.

- WINS server address
- WINS node type
- Vendor equipment options
- Class of user options - The client will provide a class ID.

Windows 2000 Client Option Levels

When options are in conflict, more specific options override less specific options.

- **Client level** - Includes one client.
- **Class level** - Includes clients in one class.
- **Scope level** - Includes one scope.
- **Server level** - Includes all DHCP server scopes and clients of the server.

Windows 2000 Multicast Scope

The DHCP console allows multicast scopes to be set up similar to normal scopes. This scope assignes a secondary IP address to a client for receiving multicasts in a multicast group. The address range for this scope is 224.0.0.0 through 239.255.255.255. Multicast Address Dynamic client Access Protocol (MADCAP) is used to assign dynamic multicast addresses to clients in multicast groups. DHCP can assign MADCAP options but MADCAP servers cannot assign DHCP options.

DHCP Lease Process

DHCP leases are used to reduce DHCP network traffic by giving clients specific addresses for set periods of time. The DHCP process stages can be remembered using the ROSA acronym:

1. **Request** - A broadcast is sent by the client with the client MAC address. This is a **DHCP discover** message with source IP address of 0.0.0.0 and destination address of 255.255.255.255. The client tries to get its last address. If it is not available, the DHCP server will send a NACK signal. The client state is **initialization** during the request stage.
2. **Offer** - A **DHCP offer** message is sent from the DHCP server with some or all the optional information as listed above. Information sent includes the IP address of the DHCP server that sent the accepted offer. All offered IP addresses are marked unavailable by the DHCP server when the DHCP server offers them until they are rejected. The client is in the **selecting** state during this offer stage.
3. **Selection (or acceptance)** - The first offer received by the client is accepted. The client broadcasts its selected choice using a **DHCP request** message which includes the IP address of the DNS server that sent the accepted offer. The client is in the **requesting**

state during this selection stage.

4. **Acknowledgement** - The server acknowledges with a **DHCP acknowledge** indicating the client can use the address or it will send a **DHCP Nak** instructing the client that the address became unavailable. Other DHCP servers retract their offers and mark the offered address as available and the accepted address as unavailable. Any offered IP addresses not selected are freed to be used again. The client state is the **binding** state during this acknowledgement stage.

When the client sends the lease request, it then waits one second for an offer. If a response is not received, the request is repeated at 9, 13, and 16 second intervals with additional 0 to 1000 milliseconds of randomness. The attempt is repeated every 5 minutes thereafter. The client uses port 67 and the server uses port 68.

Client systems that are Windows 98 or later attempt to tell if another client is already using the address received from the DHCP server by pinging the address. The DHCP server can be configured to pretest addresses by pinging them, but this will increase overhead and slow server response time.

DHCP Lease Renewal

After 50% of the lease time has passed, the client will attempt to renew the lease with the original DHCP server that it obtained the lease from using a DHCPREQUEST message. Any time the client boots and the lease is 50% or more passed, the client will attempt to renew the lease. At 87.5% (7/8ths) of the lease completion, the client will attempt to contact any DHCP server for a new lease. If the lease expires, the client will send a request as in the initial boot when the client had no IP address. If this fails, the client TCP/IP stack will cease functioning.

Additional messages include a **DHCP decline** message which is sent by the client if it decides the information from the server is not appropriate. A **DHCP release** message is used by the client to indicate to the server that the IP address is now released and available for use by other clients. The client is in the **renewing** state when the lease is half expired.

DHCP Scope and Subnets

One DHCP scope is required for each subnet.

DHCP Relay Agents

May be placed in two places:

- Routers

- Subnets that don't have a DHCP server to forward DHCP requests.

Client Reservation

Client Reservation is used to be sure a computer gets the same IP address all the time. Therefore since DHCP IP address assignments use MAC addresses to control assignments, the following are required for client reservation:

- MAC (hardware) address
- IP address

Exclusion Range

Exclusion range is used to reserve a bank of IP addresses so computers with static IP addresses, such as servers may use the assigned addresses in this range. These addresses are not assigned by the DHCP server.

DHCP and WINS

To use WINS the DHCP server must specify:

- WINS server IP address.
- NetBIOS resolution mode (B, P, N, or H - node).

DHCP backup interval

Configured in the registry at:

\hkey\local_machine\system\currentcontrolset\services\dhcp\server\parameters

DHCP files are stored in **"SystemRoot\System32\Dhcp"**.

DHCP Server Installation and Configuration

Installation:

1. TCP/IP services must be installed on the computer first.
2. Select "Start", "Settings", and "Control Panel", then double click the "Add/Remove Programs" applet.
3. Click "Add/Remove Windows Components", highlight "Networking Services", and click

"Details".
4. Select the "Dynamic Host Configuration Protocol" checkbox and click OK.
5. Continue and complete the installation.
6. If Active Directory is used on the domain, any Windows 2000 DHCP servers must be authorized in Active Directory. Servers from other operating systems do not need to be authorized. How to authorize:
    1. Run the administrative tool, "DHCP" and highlight the DHCP server.
    2. Select "Action" and "Authorize".
    3. Wait, and after several minutes select "Action" and "Refresh".

DHCP Administrative Tool

Menu selections:

- Action
    - Authorize - Used to get a DHCP server authorized in Active Directory.
    - New Multicast Scope - Usec to create multicast scopes.
    - New Reservation - Used to configure DHCP address reservation for address that are assigned by the DHCP server to specific network cards. You'll need the card MAC address to use this function.
    - New Scope - Used to add a scope (range of addresses for assignment) to the DNS server.
    - New Superscope - Start the New Superscope wizard.
    - Properties
    - Refresh

Other Options can be set using "Server Options" or "Scope Options" in the DHCP Administrative Tool. Server option settings apply to all scopes on the DHCP server unless they conflict with scope options. Scope options override server options settings since they are on a sublevel to the entire server. The Scope Options dialog box tabs include:

- General
- Advanced

The DHCP server should be configured to know the address of the WINS/NBNS server for clients that will use WINS. Also the NODE type for WINS should be set. This specifies method used to resolve IP addresses from computer names. These are:

- b-node - Broadcast node.
- p-node - Point-to-point node queries an NBNS name server to resolve addresses.
- m-node - First uses broadcasts, then falls back to querying an NBNS name server.
- h-node - The system first attempts to query an NBNS name server, then falls back to

broadcasts if the name server fails. As a last resort, it will look for the lmhosts file locally.

The DHCP server tool can be used to view information about the DHCP server including:

- The allocated scopes and IP addresses and the amount being used.
- Specific address lease information including when the lease for that address expires.
- The names of hosts which have specific IP addresses assigned to them.

The "System Monitor" administrative tool can also be used to monitor the performance of the DHCP server.

Starting DHCP

DHCP is available for NT 3.5 and later Servers. Only one scope (range of IP addresses) can be configured for one DHCP server.

1. Install DHCP. DHCP service is installed from the control panel network applet services tab. Select add, and "Microsoft DHCP Server". Restart the computer
2. Configure DHCP - **The DHCP Manager is used to configure DHCP which can be run from any networked NT computer**. The DHCP manager is accessed using Administrative Tools. The following items are set for each scope (local subnet):
    - Start Address
    - End Address
    - Subnet Mask
    - Exclusion Range start and end addresses.
    - Lease duration in days, hours, minutes or unlimited.
    - Name - The scope name
    - Comment

    Global options include (These options may be set within each scope as necessary):
    - Domain name
    - DNS server
    - WINS server (WINS/NBNS)
    - WINS/NBT node type
    - Router (Default gateway)
3. DHCP can be started by entering "NET START DHCPSERVER" on the command line on Windows 2000 server systems.

Option levels:

- Global - Options for all scopes and clients served by the DHCP server. Overridden if specified otherwise in scope or client options.
- Scope - Options for specific subnets or ranges of addresses.

- Client - Options for specific clients.

The specific client options have greater priority than scope options and scope options have priority over global options. Options may be set to allow various global options to be set as defaults for undeclared options in the scope or client options (Each subnet may have its own WINS server). Global and scope options may be reached from the DHCP options menu. Some of these options are:

- 002 Time Offset
- 003 Router - For setting default gateway
- 004 Time Server
- 005 Name Servers
- 006 DNS Servers
- 007 Log Servers
- 044 WINS/NBNS Servers - Used if the client is not manually configured for the WINS server.
- 046 WINS/NBT Type - NetBIOS name configuration designation of B,P, M, or H node.
- 047 NetBIOS Scope ID - Set so NBT hosts communicate only with other similarly configured hosts.
- cookie Servers
- LPR Servers
- Impress Servers

There can be several DCHP servers on a network. More than one may be configured to back up the other in case of failure.

Because of how leases are assigned and accepted, operation with multiple DHCP servers is not a problem as long as the DCHP servers are configured correctly. The DCHP servers must be configured so the scope of available IP addresses are not the same on any redundant DHCP server. DHCP servers do not communicate with each other.

DHCP Database Options

- Backup - Includes scopes and all options. The database is automatically backed up to:

  \WINNTROOT\System32\Dhcp\Backup\Jet

  The backup interval is stored in the registry at:

  HKey_Local_Machine\System\CurrentControlSet\Services\DhcpServer\Parameters\BackupInterval

A duplicate registry key is in the \WINNTROOT\System32\Dhcp\Backup\dhcpcfg file

- Restore - The backup is loaded if the DHCP database is determined to be corrupt by the system at initialization. A backup can be forced by copying the backup directory contents into the DHCP directory.
- Compact - The database is normally compacted, but for NT3.51 or earlier, the JETPACK.EXE utility can be used to compact the database to improve performance. If the size is 30MB, it should be compacted. This utility is run from the \WINNTROOT\System32\Dhcp directory. The DHCP service should be stopped before running this utility.

Database files:

- DCHP.MDB - The main database
- DHCP.TMP - Temporary DHCP storage.
- JET*.LOG - Transaction logs used to recover data.
- SYSTEM.MDB - USed to track the structure of the DHCP database.

DHCP terms

- Default gateway - The gateway that clients on the subnet can or must use to access other subnets or networks.
- Domain name - The DNS name (Internet name) of your internet domain.
- Lease - The time the client may use the assigned DHCP address. Normally this is a period of time in which if the client does not use the address, it is made available to the address pool for another client to use.
- Scope - A range of IP addresses in a subnet.
- Global options - IP configuration settings that apply to the entire network (all scopes the DCHP server manages).
- Scope options - IP configuration settings for a particular subnet including the IP address of the router (default gateway) and the available IP range to be used by the DHCP server for this particular subnet.

DHCP Client Configuration

If changing from static IP mapping to DHCP mapping, a reboot is not required. If changing from DHCP mapping to static IP mapping a reboot is required for the IP address to be effective.

Tools

IPConfig options:

- /all - Shows much configuration information from local hostname, IP address, subnet mask to DHCP server and WINS server address and lease dates. It will display an IP address of 0.0.0.0 and DHVP address of 255.255.255.255 if the DHCP attempt was unsuccessful.
- /renew
- /release

IPConfig is used with Windows NT and 2000 systems. Winipcfg is used with windows 9x systems.

Windows 2000 DHCP Installation and Configuration Issues

The first Windows 2000 DCHP server must be a domain controller. DHCP services must be on a member server or domain controller. Rogue (additional non domain controller) DHCP servers must be authorized in Active Directory. The DHCP Inform message is used to detect rogue DHCP servers.

When upgrading a DHCP server from Windows NT to Windows 2000, it is converted to the Windows 2000 format. This stops the DHCP service until done and may use much disk room. The DHCP database cannot be converted back to the NT format.

When DHCP is installed, the DHCP MMC snap-in is installed. This can be accessed from administrative tools. and is called "DHCP command".

Windows 2000 clustering services allow redundant DHCP servers to provide DHCP fault tolerance with one acting as primary and the other acting as a backup.

Windows 2000 DHCP can update DNS A and PRT records dynamically. This can be done is Windows 2000 from the DHCP Manager in administrative tools, by right clicking on the DHCP server or scope and selecting "Properties". There are three tabs:

- General
- DNS - Can check a checkbot to "Automatically update DHCP client information in DNS". One of "Update DNS only if DHCP client requests" or "Always update DNS". Other checkbox options are "Discard forward (name to address) lookups when lease expires", and "Enable updates for DNS clients that do not support dynamic update".
- Advanced

Helpful DHCP System Monitor Counters

- Declines per second - Indocates a conflict of Ip addresses if this is high.

- Packets received per second - Indicates how busy the server is with the network.
- Requests per second - If this number is high, the lease time may be too short.

APIPA

Windows 98 and later systems support Automatic Private IP Addressing (APIPA) for small networks addressed with the network address 169.254.0.0. If more than 25 clients, DHCP should be used. If a APIPA server detects a DHCP server, it will discontinue services.

BOOTP

BOOTP or the bootstrap protocol can be used to boot diskless clients. An image file is sent from the boot server. The image file contains the image of the operating system the client will run. DHCP servers can be configured to support BOOTP or the BOOTP server may be a separate server. CommonBOOTP options include:

- Subnet mask (1)
- Router (3)
- Name Server (5)
- Computer Name (12)
- Domain name (15)
- WINS server (44)
- NetBIOS node type (46)
- Additional options (55)
- SMTP server (69)
- POP server (70)
- Boot image server, type and path

Windows 2000 Printing

Windows uses one driver to support printing for all applications. Operating systems of the past required each application to support printing independently which required a print driver for each application or print functionality built into each application.

Printer Terms

- **Printer** - In Windows, it refers to the printer driver software which interacts with the print device to be sure the print job is formatted for that print device. Provides the interface to view and modify print jobs. This is also known as the print queue.
- **Print device** - The device that physically prints on paper.
- **Print job** - The print job is the request to print.
- **EMF** - Ehanced metafile format is a journal file print job. It is smaller than a RAW print file and can be produced faster.

When a shared print device made available as a remote printer, the printer is actually shared, not the print device. Therefore, one print device may have several printers associated with it. This allows various priorities and characteristics to be set up for different users on the same print device.

Windows NT Print Model

Components:

- **GDI** - Graphics Device Interface provides a single system for presenting graphic information to the user through the monitor and it translates print requests into driver requests that match the printing characteristics of the print device called device driver interface (DDI) calls. The printer is considered to be a graphic device with higher resolution and less color than the monitor. One of the following outputs is produced when the print request is made:
  - Raw print job - Instructions the printer can use to produce the printed document.
  - Journal file print job - A list of DDI calls that can produce a raw print job. Produced when the printing device is local.
- **Print driver** - Translates DDI calls into commands for the specific print device and consists of:
  - Printer Graphics driver - Does the DDI which applications use to print device language conversion. NT includes PLOTTER.DLL, PSCRIPT.DLL, and RASDD. DLL for HPGL/2, PostScript, and raster printers respectively.
  - Printer interface driver - Provides the interface used to configure the printer and

manage print jobs. NT includes PLOTUI.DLL, PSCRIPTUI.DLL, and RASDDUI. DLL for HPGL/2, PostScript, and raster printers respectively.
    - Minidriver or Characterization Data file - Contains information about printer device for the printer graphics driver. It includes internal cartridge information, Available paper trays and amount of print device memory.
- **Print router** - Directs the print job to the correct print spooler providing the print service. The router can download the print driver from the remote computer.
- **Print spooler or provider** - Accepts print jobs from the router for a local or remote printer, uses the print processor to make required modifications to the print job, and sends print jobs one at a time to the print monitor. Separator pages are added here. It assigns priority to the jobs. Print job files are spooled to the WINNT40\SYSTEM32\ SPOol\PRINTERS directory by default. It is a service and can be controlled by the services applet in the control panel.
- **Print processor** - Processes DDI calls into printer instructions. It modifies the print job before it is sent to the print monitor and may append form feeds. The default processor is WINPRINT.DLL. Also a Macintosh print processor is provided. The print processor recognizes simple text, postscript, raw printer data, and enhanced metafile (EMF) data which can be used with any print device. The two types of processed RAW jobs are "Raw FF auto" and "Raw FF Appended" The "Raw FF auto" job always appends a form feed, even if one is already present, and the "Raw FF appended" type only appends a form feed if one is not already present..
- **Print monitor** - Transmits the print job to the print device and reports the condition of the print device. Print monitors include:
    - LOCALMON.DLL can store the print job in a file and communicates to the print device over serial or parallel ports, named pipes or remote shares.
    - HPMON.DLL for print jobs on an HP printer on the network.
    - LPRMON.DLL for UNIX line printer daemon print servers.
    - LEXMON.DLL for Lexmark Mark Vision print devices which use DLC, TCP/IP, or IPX for their transport protocol to communicate.
    - PJLMON.DLL for bi-directional print devices using the Printer Job Language (PJL) standard. The HP LaserJet 5Si uses this standard.
- **Network printing device**

Two additional utilities called LPR.EXE and LPQ.EXE are provided on Windows NT for managing print jobs destined for Unix hosted printers. LPR is used to print files and LPQ is used to manage the print queue.

NT remote print drivers

Clients that are attempting to print on remote computers do not need a local print driver installed. When the print request is made to the print server computer, the client will check to see if a print driver exists. If not or its print driver is older than the print driver on the server, the

print server sends a copy of its print driver to the client computer which keeps it until the session ends.

Print Process

When print requests are made to a print device that is available through a print server the following happens:

1. If the requesting computer does not have a print driver for the print device or it's print driver is older than the print driver on the print server, it will receive a copy of the print driver from the print server.
2. Tthe Graphics Device Interface (GDI) of the client computer receives the print request and sends the print request to the print device driver.
3. The print request driver will produce a EMF file or RAW print file and send it to the GDI.
4. The GDI sends the print job to the print spooler component on the local computer.
5. The local print spooler component connects to the print spooler on the print server (or locally spools the file if the printer is on the local computer) and sends the print file.
6. The spooler stores the file in temporary storage and sends a request to the print processor.
7. If the file is in EMF format it is converted to a RAW print file by the print processor for the specific print device the print job is being sent to. The RAW file is a file converted from DDI commands to commands specific for the print device the job is being sent to. A separator page is attached if it was requested.
8. The print job is sent to a specific print monitor for the given print device. It will complete the process of sending the job to the print device and monitor the progress of the job.
9. The print device will print the print job.

Adding Printers

The "Add Printer Wizard" in the "Printers" folder is used to add printers. Users who do this must be an Administrator or Power User. Windows 2000 will detect USB plug and play printers, but a parallel printer must be added manually. To add **TCP/IP printers**, use the "Add Printer Wizard" to add the printer, select "Create a new port" and select "Standard TCP/IP Port". You'll enter the printer name or its IP address.

To add **UNIX printers**, the "Add/Remove Programs" applet in the Control Panel can be used to install "Print Services for Unix". Use the "Add Printer Wizard" to add the printer, select "Create a new port" and select "LPR Port". You'll enter the printer name or its IP address and the name of the print queue for the print device.

Old HP print devices may use the DCL protocol rather than TCP/IP. If you connect to one of these printers, use the "Control Panel", "Network and Dial-up Connections" applet to add the

DLC protocol, then use the "Add Printer Wizard" to add the printer. You must "Create a new port" and select "Hewlett-Packard Network Port" and enter the MAC address of the printer card that the printer uses. Choose "Job Based" connection if more than one computer is using this printer. Choose "Continuous" connection if this is the only computer to use the printer.

To add an **AppleTalk printer**, use the "Control Panel", "Network and Dial-up Connections" applet to add the AppleTalk protocol. Use the "Add Printer Wizard" to add the printer, select "Create a new port" and select "AppleTalk Printing Devices". Select the divice from the list. If you capture the print device, this will be the only computer that can use the print device.

Internet Printing Protocol (IPP) is used to communicate with internet printers. Id does not need installed since it is a part of Internet Explorer and IIS. Internet Explorer is used to connect to these printers and you must know the URL of the printer since you cannot browse for it.

To share a printer, right click on the printer, select "Properties", click the "Sharing" tab, click the "Shared as:" radio button and enter the name you want to call the printer. To list it in Active Directory, click the "List in the Directory" checkbox.

Managing Printers

The Add Printer Wizard is used to create or add new printers (print drivers). The Add Printer Wizard may be started by selecting, "Start", "Settings", and "Printers" or by selecting "Printers" in "My Computer". Printer drivers that support other operating systems such as Windows 95 may be installed on the computer that is hosting the printer. This way if a client computer with that operating system tries to use the print device and does not have a print driver, it can still print since the print driver will be available from the print server.

Printer Properties window tabs:

- **General** - A printer comment (textbox) can be added, printer location may be described (textbox), the print driver selection may be made (dropdown box/NewDriver button), placement of separator pages (button) is selected, the print processor is selected (button), and a test page (button)may be printed. Available separator pages are in the WINNT40\SYSTEM32 directory and are:
    - SYSPRINT.SEP - This page is compatible with PostScript print devices and will print a page at the start of each document.
    - PCL.SEP - Sets PCL mode for HP print devices and prints a page at the start of each document.
    - PSCRIPT.SEP - Makes HP print devices switch to PostScript mode. A page is not printed before the print document.

  Separator pages are text files and may be created with any editor. Some separator page control characters are:

  - \D - Date
  - \H - Followed by a specific control sequence for the print device will perform a specific control on the printer.
  - \N - User name that sent the print job.
  - \T - Time
- **Sharing** - Allows other stations to use the printer. The print server can be configured here to download print drivers to other computers that access your printer. Windows NT 4.0 printer permissions:
  - No Access - The group or user with no access will not be able to use the printer.
  - Print Permission - Users may send print jobs to the printer and manage their print jobs by using the delete, pause, resume, and restart functions on their own print jobs.
  - Manage Documents - Allows the user or group with this permission to manage jobs sent by other users or groups.
  - Manage Printers - The user or group with this permission may change printer permissions, delete or add printers, enable and disable sharing, and change other print settings.
- **Ports** - Multiple print devices that are in the same print pool may be added (Print pooling is enabled here). **A print job may be redirected to a file**. Also a printer may be redirected to another print device so long as the other device is of the same type.
- **Advanced** - Controls print priority (1-99), when printing starts relative to spooling or whether to spool at all, hours of availability for the print device. **Spooling Options** include the default selection of "Spool Print Documents so program finishes printing faster", causes the job spool to the hard drive allowing the application to return faster. The two sub options to "Spool Print Documents" are "Start Printing Immediately" and "Start Printing After Last Page Is Spooled". Another option is "Print Directly to the Printer" that does not allow spooling of the print job. Checkboxes include whether the spooler should hold mismatched jobs, whether to print spooled jobs first, whether to "Keep documents after they have printed" and "Enable advanced printing features". Scheduling priority can be set from 1 to 99 with 99 being the highest priority. To make scheduling priority effective, more than one printer driver with different priorities may be associated with one print device. This tab also controls hours of operation for the printer. A new print driver may be added here. Buttons at the bottom include "Printing Defaults", "Print Processor", and "Separator Page".
- **Security** - Permissions are set here. There is a box that contains a list of users or groups that can have permissions. Users and groups may be added or deleted. Permissions each have an allow or deny check box for each user or groupas follows:
  - Print
  - Manage Printers
  - Manage Documents
- **Device Settings** - Sets up device specific settings such as printer fonts, default tray, available printer memory, and font substitution table.

Print Pools

Multiple print devices may support one printer (driver) with a print pool. Print jobs are sent to the next available print device. All print devices must be of the same type, however, since the printer (driver) must be able to interface to all print devices in the print pool. Windows for workgroups (WFW) cannot spool to an NT printer pool, but Windows 95 through NT4.0 can.

Managing Print Jobs

Print jobs are managed by double clicking on the desired printer in the printers folder. Menus include:

- **Document** - Print jobs may be paused (pause), resumed (resume), restarted(restart), or canceled (cancel).
- **Printer** - Selections are Paues, Resume, Restart, Cancel, and "Properties". Capabilities include:
  - The printer may be paused (Pause Printing)
  - Sharing and permissions may be changed
  - The default printer may be changed
  - Defaults for all print jobs may be set
  - Printer properties may be set
  - Spooler documents may be deleted
- **View**
  - Document List
  - Properties
  - All Printers
- **Help**

Printer registry entries

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Print\Printers - To change the location of the spool folder for all printers, change the value of DefaultSpoolDirectory to reflect the new spool location. This affects all printers installed on the computer. You can also change the spool location of each of the printers installed on the computer individually by modifying the SpoolDirectory value of their key entry.

Two troubleshooting tips

- Remember that the computer spooling the print job must have sufficient space to queue the print job.
- To test, you can print to a file. If you copy the file to the printer port and it prints, either

the print spooler is not working or the data is not being transmitted to the printer.

Managing Print Servers

In the "Printers" folder, select "File", and "Server Properties". Four tabs are:

- Forms - Can set the size of the print page and use it as a form.
- Ports - Used to Add, Delete, or Configure ports.
- Drivers - Used to Add, Remove, Update or configure print driver properties.
- Advanced - Used to set the location of the spool folder and set the followint options:
    - Log spooler error events
    - Log spooler warning events
    - Log spooler information events
    - Beep on errors of remote documents
    - Notify when remote documents are printed
    - Notify computer, not user, when remote documents are printed

Internet Printer

The Windows 2000 Server system that shares a printer as an Internet printer must have the following installed:

- TCP/IP
- Internet Information Services (IIS)

Internet Printing Protocol (IPP) is used to support printing from Internet Explorer(IE) across the internet. This provides the ability for clients using IE to print to Universal Resource Locations (URLs), view printer information, and download printer drivers.

Internet Explorer or the Printers folder can be used to manage these printers. Internet Explorer or the Add Printer Wizard can be used to connect to Internet printers.

Windows 2000 Routing

The **"Routing and Remote Access"** administrative tool is used to enable routing on a Windows 2000 server that is multihomed (has more than one network card). Windows 2000 professional cannot be a router. The "Routing and Remote Access" administrative tool or the "route" command line utility can be used to configure a static router and add a routing table. A routing table is required for static routing. Dynamic routing does not require a routing table since the table is built by software. Dynamic routing does require additional protocols to be installed on the computer. When using the "Routing and Remote Access" tool, the following information is entered:

- Interface - Specify the network card that the route applies to which is where the packets will come from.
- Destination - Specify the network address that the packets are going to such as 192.168.1.0.
- Network Mask - The subnet mask of the destination network.
- Gateway - The IP address of the network card on the network that is configured to forward the packets such as 192.168.1.1.
- Metric - The number of routers that packets must pass through to reach the intended network. If there are more than 1, the Gateway address will not match the network address of the destination network.

Dynamic Routing

Windows 2000 Server supports Network Address Translation (NAT) and DHCP relay agent. Three Windows 2000 supported Dynamic routing protocols are:

- Routing Information Protocol (RIP) version 2 for IP
- Open Shortest Path First (OSPF)
- Internet Group Management Protocol (IGMP) version 2 with router or proxy support.

The "Routing and Remote Access" tool is used to install, configure, and monitor these protocols and routing functions. After any of these dynamic routing protocals are installed, they must be configured to use one or more routing interfaces.

OSPF Terms

- Area border router - A router that interfaces to subnets in more than one OSPF area.
- Autonomous system - Routing areas that are administered by a single organization.
- Autonomous system boundary router - A router that connects an autonomous system to

another autonomous system or the internet.
- Backbone area - The main OSPF or root routing area that is connected to all other areas with an ID of 0.0.0.0 (ID number does not reflect any IP address).
- Internal router - Router that does internal routing.
- Internal routing - Routing done in one routing area.
- Routing area - A group of IP subnets connected by links with an ID similar to an IP address that is used to identify the area. In Active Directory, a routing area would likely be configured for each site. Passwords are used for each routing area.

Routing Configuration Issues

- RIP - Tabs:
  - On the **security** tab of the RIP properties dialog box there as a selection of one of:
    - Accept announcements from all routers
    - Accept announcements from listed routers only - A list must be created.
    - Ignore announcements from all listed routers - A list must be created.
  - **General** - Maximum delay setting controlling how long the router waits to update other routers. Includes logging controls.
- OSPF - Property box tabs:
  - Areas - In the OSPF properties dialog box (Areas tab?) select one of the following network types:
    - Broadcast - For normal local area networks.
    - Point-to-point - For demand dial interfaces.
    - Non-broadcast multiple access (NBMA) - For frame relay or X.25 networks.
  - General - Includes logging controls along with "Router Identification field" and "Enable Autonomous System Boundary Router" checkbox.
  - Virtual Interfaces - If an OSPF area is not connected directly to the backbone area, a virtual interface must be created to allow for it to go through one or more intermediate networks. The virtual interface tells OSPF which router has an interface that connects to the backbone area. The entered password must be the one required by the router with the interface connecting to the backbone area that packets are being sent to.
  - External Routing - Allow or reject external route table sources.
- Internet Group Management Protocol (IGMP) version 2 Router and Proxy is used to manage routing of multicast network traffic.
  - Routers must be configured with IGMP to use multicasting on a network. The interface may be configured as an IGMP router or an IGMP proxy. An IGMP router will update its table with group information and forward multicast traffic.

The "Routing and Remote Access" tool server properties dialog box contains these tabs:

- General - Can enable the computer as a router for LAN routing only or for LAN and demand dialing. Also the computer may be enables as a Remote Access Server (RAS).
- Security - Can select Windows Authentication or RADIUS authentication for remote access and dial on demand connections. A provider to log all sessions with the router can be selected. Chioces are none, Windows accounting, or RADIUS accounting.
- IP - Can "Enable IP routing", and "Allow IP-based remote access and demand-dial connections". The computer may also be configured to use a DHCP server to assign IP addresses to client computers or to use a static IP address pool.
- PPP - Options:
    - Multilink connections
    - Dynamic bandwidth control using BAP or BACP
    - Link control protocol (LCP) extensions
    - Software compression
- Event Logging - Can enable or disable PPP logging. Other options:
    - Log errors only
    - Log errors and warnings
    - Log the maximum amount of information
    - Disable event logging

NAT

Network Address Translation (NAT) is the same thing as IP Masquerading. It is used to allow one computer to masquarade on one interface for all other computers that are on another of its interfaces. It it not a firewall but adds security by allowing multiple computers to access the internet or an external network through it. External computers cannot directly contact computers on the network inside the NAT computer. The only registered interface is the interface on the NAT computer on the outside. If it is on the internet, it must have a registered IP address. NAT must be set up to use an interface that is set for routing.

The "Routing and Remote Access" administrative tool is used to install and configure NAT. Components:

- Addressing - A server component that assigns IP address, netmask, gateway, and DNS server address to clients.
- Translation - Maintains NAT table for connections.
- Name Resolution - Acts as DNS server for internal machines on the network.

NAT Properties dialog box tabs:

- General - Configure event logging to one of log errors only, log errors and warnings, log the maximum amount of information, and disable logging.
- Translation - Configure the number of minutes it takes for NAT to remove TCP and UDP

port mappings.
- Address Assignment - Can set "Automatically assign IP addresses by using DHCP" and specify ranges and excluded addresses.
- Name Resolution - Can configure NAT to act as a DNS proxy. If you have a separate DNS server, this option will not be necessary.

NAT Interface Properties dialog box tabs:

- General - Select private interface connected to network or select public interface connected to internet. If it is connected to the internet, there is an option to allow TCP and UDP headers to be translated to send and receive data through the interface.
- Address Pool - A public IP address may be assigned to an internal server (although on a different internal address) such as a FTP or web server. Requests to that public address will be sent internally to that server.
- Special Ports - Allows requests to specific ports to another internal address.

TCP/IP Packet Filtering

Controls the type of packets (based on port destination) that a routing interface will receive or forward. It is configured using the "Network and Dial-up Connections" folder by right clicking on the local connection and selecting "Properties". You can set specific TCP and UDP ports along with specific IP protocols. Each protocol has a protocol number listed in the protocol or protocols file. Some examples are TCP, UDP, ICMP, IGMP, and more.

Windows 2000 IPSec

IPSec stands for Internet Protocol Security and it is used to encrypt TCP/IP data so the information cannot be captured and understood by outsiders. It is used both on internal networks and between two private networks over the internet to support virtual private networking (VPN). Terms:

- Transport mode - The data portions of the packet are encrypted.
- Tunnel mode - The data and address portions of the message are both encrypted and that packet is used in the data portion of a new packet of a new IP packet with a new address. It is used between two routers for VPN.

Security Methods

IPSec can use various security encryption algorithms and key lengths. These are the characteristics of IPSec connections (security methods):

- A specified encryption algorithm.
- A negotiated key length.
- A negotiated key lifetime.

Supported Authentication Methods

- A shared secret such as a key or phrase.
- Kerberos
- Certificates - The certificate can only be created using a private key and the certificate is verified using the public key. This way the certificate can be used for authentication.

Enabling

Enabling IPSec is enabled on individual computers by using the "Network and Dial-up Connections folder". The "Domain Security Policy" administrative tool is used to enable IPSec on all computers or domain controllers in a domain. "Active Directory Users and Computers" can be used to set up a group policy object which can enable IPSec on Windows 2000 computers in an organizational unit. IPSec can be managed by using the Microsoft Management Console (MMC) IP Cecurity Policy Snap-in.

When using group policy to set IPSec, the following options are available:

- Client (Respond Only) - Only Uses IPSec to respond to requests for use of IPSec but outgoing requests are done with normal communications.
- Server (Request Security) - Always uses IPSec for outgoing communications. Computers without IPSec enabled can still communicate with computers set in this mode.
- Secure Server (Require Security) - Uses IPSec for all communications. Computers without IPSec enabled can not communicate with computers set in this mode.

One IPSec policy may be set for one computer which includes one or more rules which are applied from the most restrictive to the least restrictive. IPSec Rules:

- IP Filter - Defines the type of traffic the rule applies to.
- IP Filter Action - Determines how the type of traffic is handled such as requiring encryption, requesting encryption for outgoing traffic, or allowing traffic that is not encrypted.
- Authentication Method - Three methods are Windows 2000 default, Keberos 5, or use an encryption key.
- Tunnel Setting - Determines whether IPSec will work in transport ("This rule does not specify a tunnel") or tunnel mode ("The tunnel endpoint is specified by this IP address").
- Connection Type - Determines if the rule applies to the local area network, all network connections or to remote access.

IPSec policy is set using "Active Directory Users and Computers".

The Security Monitor tool is used to monitor IPSec. Although it is a graphical tool, it is started from the command line by typing "Ipsecmon" followed by the name of the computer to be monitored.

IPSec Monitoring Tool

The IPSec monitoring tool can be used to provide a summary of the local computer IPSec connections. This tool can be started by clicking on "Start", "Run" and entering "ipsecmon.exe" and pressing the ENTER key.

Windows Internet Connection Sharing (ICS)

It is used to connect small office environments to the internet. It will work on Windows 2000 Server, Advanced Server, or Professional.

Enabling ICS

From "Network and Dial-up Connections", right click on the adapter icon which connects to the internet and select "Properties". Click on the "Sharing" tab and be sure the "Enable Internet Connection Sharing for this Connection" checkbox is selected.

Enable On-demand dialing if this is a dial in connection and yuo want automatic dialing to happen.

Tabs available when the sharing button at the bottom of the sharing tab is clicked:

- Applications - Outbound port maping is controlled.
- Services - Inbound port maping is controlled.

Windows 2000 Guide Contents Page

Windows 2000 Fault Tolerance

Windows 2000 Professional supports stripe sets but not mirroring or any other fault tolerance exclusive of sector sparing. The below mechanisms are fault tolerance mechanisms except for Disk Striping (RAID0):

- Disk mirroring (RAID1) - One disk is a mirror copy of the other. This is geared for reliablilty, not speed. The boot and system partition may be mirrored. Mirrored volumes must be of the same size. Mirroring is done by clicking on the volume to be mirrored while holding the CTRL key down, then clicking on some free space of equal or greater size while the CTRL key is held down. Then click "Fault Tolerance", "mirror", and "establish mirror". To break a mirror, click on the mirror, and break.
- Disk Striping (RAID0) - Data is split into sections with part of the data being written to each disk in parallel. Can use 2 to 32 disks. This provides speed but not reliability unless disk striping with parity is used. Each partition in a stripe set must be the same size. The boot or system partition may not be part of a stripe set. Data is stored in 64K blocks. Must drives be of the same type to be part of a stripe set? (I don't think so.)
- Disk striping with parity (RAID2/3/4/5) - The same as disk striping except an additional disk that stores parity information is used. Can use 3 to 32 disks. The parity information may be used to recreate the contents of a failed drive. At least three disks are required to create a stripe set with parity. To make a stripe set from Disk Administrator, click on three areas of free space on three drives. From the fault tolerance menu choose "create stripe set with parity". Select the "Partition" menu, "commit changes". Reboot, then format the stripe set by highlighting the stripe set and selecting "tools", and "format".
- Disk duplexing - Each disk gets its own controller so one controller failure can't bring both disks down. Without redundant controllers, this is the same as disk mirroring.
- Replication - One server is a complete copy of another in case one server fails. One is used as a primary server and the other is a backup server.

Redundant Array of Inexpensive disks (RAID)

RAID is a fault tolerant method of storing data, meaning that a failure can occur and the system will still function. When RAID is hardware supported, the RAID hardware will perform parity calculations, thus freeing the system. The various RAID categories are:

- 0 - Disk striping - Data is written across multiple drives in parallel. Different parts of the data is written at the same time to more than one drive. If there are two drives, half the data is written to one drive, while the rest of the data is written to the other drive. All

partitions on striped drives must be the same size. No fault tolerance is provided with RAID-0.

- 1 - Disk mirroring - All the data is written to two drives so each drive has a complete of all stored data. If one drive fails, the other can be used to get a copy of the data. To be more fault tolerant, more than one controller card may be used to control the mirrored hard drives. This is called disk duplexing and will allow the system to keep functioning if one controller card fails.
- 2 - Disk striping with error correction codes (ECC).
- 3 - Disk striping with ECC parity information stored on a separate drive.
- 4 - Disk striping with blocks with parity information stored on a separate drive.
- 5 - Disk striping with blocks with parity information stored using multiple drives. Uses five disks with one fifth of each one to store parity information.

Windows 2000 Server supports RAID 0, 1, and 5.

Computer Mnanagement Administrative Tool

The administrative tool called "Computer Management" is used to create and manage RAID volumes. To perform disk management, enter the "Computer Management" tool, click on the + next to "Storage", and select the "Disk Management" folder. At this point, volumes or partitions can be created, disk mirroring or duplexing may be set up or broken. RAID drives can only be created on Windows 2000 volumes which are dynamic volumes rather than partitions. See the section callled "Disks and Volumes" in this guide.

Volume Sets

Volume sets are used to extend volumes across multiple hard drives. Neither the system nor boot partition may be part of a volume set. A volume set may use different type drives (IDE, SCSI) and can be any combination of FAT, NTFS or filesystem that NT can use.

Extending Partitions

The boot partition cannot be extended in size.

Repairing a mirrored drive

1. Replace the failed hard drive.
2. Break mirror set using the "Computer Management" administrative tool.
3. Create a new mirror set.

Tape Drive Addition

Tape drives are added using the "Tape Devices" applet in the Control Panel. You can allow the tape to be detected automatically or use the drivers tab to select and add a driver.

Windows 2000 Guide Contents Page

Windows 2000 Backups

Backup Permissions

Users with the "Backup files and directories" or "Restore files and directories" permission can backup or restore files. On Windows 2000 computers Administrators and Server Operators can backup and restore data.NT server, users who are members of the Server Operators group can back up files. On NT workstation, other users who can backup any files include:

- Administrators.
- Users who are in the local Backup Operators group.

Microsoft Backup Strategy

When choosing backup strategy consider what data requires backup, whether it is stored in a central location or if it resides on several computers, and how often the data should be backed up. The registry and the SAM on the domain controller should be backed up daily.

Data Types

- System data - Important operating system files, databases, and directories. It may include:
  - The registry
  - System startup files
  - Component services data class registration database
  - Active Directory (Windows 2000 Servers only)
  - Certificate server database (Windows 2000 Servers only)
  - SYSVOL filder (Windows 2000 Servers only)
- User data - Applications installed by the user along with other data created by the users.

Backup Functions

- Backup
- Restore
- Create an emergency repair disk (ERD).

Types of Backups

- **Normal** - Saves files and folders and shows they were backed up by clearing the

archive bit.
- **Copy** - Saves files and folders without clearing the archive bit.
- **Incremental** - Saves files and folders that have been modified since the last backup. The archive bit is cleared.
- **Differential** - Saves files and folders that have been modified since the last backup. The archive bit is not cleared.
- **Daily** - Saves files and folders that have been changed that day. The archive bit is not cleared.

To perform a backup, select "Start", "Programs", "Accessories", "System Tools", and "Backup". The Windows 2000 "Backup Utility" will start. It has these tabs:

- **Welcome** - Includes:
  - Backup Wizard - Options
    - Backup everything.
    - Backup selected files, drives, or network data.
    - Only back up system state data.
  - Restore Wizard - Used to restore data including system state data on computers that are not domain controllers. Restoring system state data is only done as a last resort to recover a failed system.
  - Emergency Repair Disk - Used to create an emergency repair disk.
- **Backup** - Shows computer drives that can be backed up and allows selection for manual backup.
- **Restore** - Used to restore part or all of a backup.
- **Schedule Jobs** - Used to schedule backups.

Options Dialog Box

This dialog box may be entered by selecting "Tools" and "Options" from the menu from the Windows 2000 "Backup Utility". It has these tabs:

- **General** - Checkboxes:
  - Compute selection information before backup and restore operations - Allows progression bar to be shown
  - Use the catalogs on the media to speed up building restore catalogs on disk - The existing hard drive file catalog is used tor the backup tape.
  - Verify data after the backup completes
  - Backup the contents of mounted drives
  - Show alert messages when I start Backup and Removable Storage is not running
  - Show alert messages when I start Backup and there is compatible import media available
  - Show alert messages when new media is inserted into Removable Storage

    - Always move new import media into the backup media pool.
- **Restore** - When restoring a file that is already on my computer - Radio button options:
    - Do not replace the file on my computer (recommended)
    - Replace the file on disk only if the file is older
    - Always replace the file on my computer
- **Backup Type** - Select the backup option to be one of:
    - Normal
    - Copy
    - Incremental
    - Differential
    - Daily
- **Backup Log** - Amount of backup logging detail:
    - Summary Only
    - Copy full detail - Logs the names of files and directories backed up.
    - Don't log
- **Exclude Files** - Select files to be excluded from the backup.

Restoring a Domain controller system

Domain controllers contain Active Directory data. Two restores:

- **Nonauthoritative Active Directory restore** - Active directory entries on other domain controllers overwrite older entries restored from backup.
- **Authoritative Active Directory restore** - Whan done, if any entries are marked as authoritative, those entries will replace other corresponding entries on other domain controllers.

How to restore a domain controller system:

1. Reboot the domain controller.
2. Press F8 while booting.
3. Open Advanced Options Menu, select "Directory Services Restore Mode".
4. Select the correct Windows 2000 Server operating system if more than one system is on the computer.
5. During safe mode, press CTRL-ALT-DEL.
6. Log on as Administrator.
7. Select "Start", "Programs", "Accessories", "System Tools", and "Backup".
8. Use the "Restore Wizard".
9. After the restore, if an authoritative restore was done use the **"ntdsutil"** command line utility. Type "authoritative restore". Syntax for restoration of partial database format:

restore subtree OU=OUname, DC=domainname, DC=rootdomain

Type "restore database" to make the entire database authoritative.

10. Reboot the Domain Controller.

Microsoft Backup Terms

- **Backup Set** - The group of files and directories that are stored on a tape during one backup session. Multiple backup sets may be stored on a tape.
- **Family Set** - Tapes that the backup set is stored on.
- **Catalog** - The list of directories and files stored on the backup set. **It is stored on the last tape in the set**.
- **Backup Log** - The log file for the backup which records the backup details including the date and files backed up.

Tape Options

- **Append** - Puts the new backup set after the previous set on the tape.
- **Replace** - Old backup sets are overwritten by the new backup.
- **Verify after backup** - Verifies whether the files were accurately saved on the tape.
- **Backup Registry** - Allows the system registry to be backed up.
- **Restrict Access** - Only allows administrators, backup operators, or the tape owner to use the tape for file recovery.
- **Hardware Compression** - Allows the backed up data to be compressed on the tape.

The registry cannot be restored remotely on a computer, but files may.

Restore Options

- **Restore Registry** - The system registry is restored from the tape to the local computer.
- **Restore Permissions** - The file and file permissions (Access control list entries) are restored to their state when the file was backed up. The file will have the default permissions of the directory it is restored to unless this option is chosen.
- **Verify After Restore** - It is confirmed that the files were correctly restored.

The registry cannot be restored remotely on a computer, but files may.

Scheduling the Backup

The AT command may be used to schedule backups from the command line interface. The most common way to schedule a back is to use the Windows 2000 "Backup Utility"by selecting "Backup" in the "Administrative Tools" section of the start menu. Select the "Backup" tab and

click the "Schedule" button to set a schedule. A user name and password will be required to run the backup.

Common Backup Strategies

- Daily normal backup
- Weekly normal backup with daily differential backups.
- Weekly normal backup with daily incremental backups.

Removable Storage Tool

Used to manage removable media. Enter by right clicking "My Computer" and selecting "Manage".

Active Directory Storage and Restoration

Extensible Storage Engine

The Extensible Storage Engine is used by Active Directory to provide a transaction based database with fault tolerance. This means that partial transactions will not be stored but only complete transactions are logged. Log files are used to provide fault tolerance by writing the transaction to the log file before commiting it to the Active Directory database. There are three steps to saving a transaction:

1. The transaction is written to a log file.
2. The transaction is written to a Active Directory database page in memory.
3. The transaction is committed to disk storage.

Directory Store Files that are Backed up

- Database file - Stored in SystemRoot\NTDS\ntds.dit, it holds all AD objects and attributes. Contains these tables:
    - Object table - Has a row for each object in AD.
    - Link table - Stores inter object relationship information.
    - Schema table - Has a list of all objects and their attributes.
- Log file - The following files are stored in the System Rootdirectory in the NTDS folder.
    - Checkpoint log files - Holds pointers to transaction logs that have been committed to the AD database. The file name is edb.chk.
    - Transaction log files - Stores transactions that are either commited or are about to be committed to the AD database. The file name is edb.log. If more than one log file is used the log file name is edbhhhhhh.log where "hhhhhh" is a hexadecimal

based number.
- Patch files - Manages data while backups are done. These files have the file extension ".pat".
- Reserve log files - Reserves hard drive space for transaction log files. The files names are res1.log and res2.log.

AD Restoration

The AD restores are done by starting the computer in Directory Service Restore mode described in the "System Failure" section of this guide.

- Non-Authoritative Restore - Changes are accepted from other domain controllers after the backup is done.
- Authoritative Restore - Changes are NOT accepted from other domain controllers after the backup is done.
- recovery without Restore - Transaction logs are used to recover uncommited AD changes after a system crash. This is done by the system automatically without using a restore from a tape backup.

Windows 2000 Failure Recovery

Tools used to recover from a system failure:

- Safe Mode/Startup Options
- Emergency Repair disk
- Recovery Console

Safe Mode/Startup Options

Safe mode is used to start the system with minimul programs and drivers in case some of them may be adversely affecting the system. When the system is booting, press F8 to get the option (advanced options menu) to enter safe mode. There are also other startup options which can be used in the case of video problems or if more information about a boot problem is required. These otions are:

- Safe Mode
- Safe mode with Networking
- Safe mode with command prompt - The desktop is not run, but a command prompt is used to run the system.
- Enable Boot Logging - Logs the results of each attempt to load a driver. This is saved in a file on C:\WINNT\Ntbtlog.txt.
- Enable VGA Mode
- Last Known Good Configuration
- Directory Services Restore Mode
- Debugging Mode - A serial connection between two machines can be made and information from the server having the problem is sent to the second computer for analysis.

Last Known Good Configuration

When the system is booting, press F8 to get the advanced options menu and select "Last Known Good". The last configuration that was used to successfully boot is used to perform the boot.

Emergency Repair disk

Can be used to restore corrupted or missing system files on a system that will not boot. Only the Backup program can be used to create an emergency repair disk after system installation.

Recovery Console

Used to:

- Repair the master boot record (MBR) of a disk
- Manually copy files to the hard drive
- Stop or start a service.

The recovery console provides command line access to the system, but permissions are enforced. There are two ways to start it:

- **Prior to having trouble, install the recovery console on the computer** and place it on the boot menu so it may be selected from the boot loader (Requires Administrator logon). Recovery console installation on boot menu:
  1. Insert the installation CD in the CDROM drive and exit the menu that appears.
  2. Open a command prompt window and change the default drive to the CDROM drive.
  3. Type "cd \i386", and "winnt32 /cmdcons" to run the program and install the recovery console.

  Use of the recovery console:
  - To list available commands, type "help"
  - To get help with specific commands, type "help command".
  - The recovery console uses the same commands as MS-DOS.
- Boot from the Windows 2000 installation CD and run the recovery console by selecting it on the menu that appears.

Windows 2000 Services

GSNW

Add "Gateway and Client Services for NetWare", installing from the CDROM. The GSNW and CSNW are installed as one piece since both are required to support the gateway. On the NetWare server, create a group calleds NTGATEWAY. Create a user in the NTGATEWAY group on the NetWare Server or NDS tree that has rights to the resources to be shared.

SNMP

This service sends SNMP trap messages (Messages when siginificant network events or errors occur) to computers configured to receive traps. They can be recorded in event logs. The tabs in the SNMP properties box:

- General
- Log On
- Recovery
- Dependencies
- Agent
- Traps
    - Community name - The computer must have the correct community name to send traps to another computer.
    - Trap destinations - List of computers where trap messages are sent.
- Security

Dial-up connections

Connection to a Remote Access Server Tabs:

- General
- Options
- Security - Options:
    - Typical
        - Validate my identity as follows: with options of "Allow unsecured password", Require secured password", or "Use smart card".
        - Automatically use my Windows logon name and password (and domain if any)
        - Require data encryption (disconnect if none)
    - Advanced (custom settings) - Manually select authentication methods and data

encryption or not.
    - Show terminal window - Display a terminal window when the connection is started.
    - Run script - A script that automates the connection process is run.
- Networking
- Sharing

All connections except dial-in connections can be renamed.

Windows 2000 Remote Access

Remote Access Service (RAS) is considered to be a Wide Area Network (WAN) connection. Clients that use remote access use either:

- Dial-up to private connections or the internet.
- Virtual private networking (VPN) to the internet or across some other network.
- Cable connections to other computers using infared, serial or parallel ports.
- RAS can laso be configured to handle incoming connections by phone, the internet, or a cable.

RAS servers can be used as gateways to link LANs together.

Required Client Components

Required components to use RAS on a client:

- Networking
- Transport Prococol (NetBEUI, NWLink, TCP/IP) - The best protocol depends on line conditions. TCP/IP is best when line conditions are poor, but it is slower. If line conditions are good, and speed is desired, use NetBEUI.
- Workstation service for NTWS or Client for Microsoft Networks fro Windows 95

Required Server Components

- Modems or ISDN interface or X.25 PAD. Modems are configured using the control panel modems applet. ATM and ISDN is installed using the control panel network applet.
- Networking
- Must run the "Routing and Remote Access" service. This service is only available on servers but is installed by default.

Connection Protocols Supported

- **Point to Point Protocol (PPP)** - Point to Point Protocol is a form of serial line data encapsulation that is an improvement over SLIP which provides serial bi-directional communication. Packets are delivered in the order they were sent. It is much like SLIP but can support AppleTalk, IPX, TCP/IP, and NetBEUI along with TCP/IP which is supported by SLIP. It can negociate connection parameters such as speed, transport protocol, and selection of PAP or CHAP user authentication method.

- **Serial Line Interface Protocol (SLIP)** - Serial Line Internet Protocol. This protocol places data packets into data frames in preparation for transport across network hardware media. This protocol is used for sending data across serial lines. There is no error correction, addressing, compression, or packet identification. There is no authentication or negotiation capabilities with SLIP. SLIP will only support transport of IP packets.
- **CSLIP** - Compressed SLIP is essentially data compression of the SLIP protocol. It uses Van Jacobson compression to drastically reduce packet overhead by reducing the TCP/IP headers and not the data. It requires CSLIP support on both the client and server ends. This may also be used with PPP and called CPPP.
- **Point to Point Multilink Protocol** - Combines bandwidth from several physical connections into one logical connection.
- **Microsoft RAS** - Also known as AsyBEUI.

Other Protocols

- **Callback Control Protocol (CBCP)** - Allows the server to negociate with the client to call the client back to establish the connection.

VPN Protocols

- **Point to Point Tunneling Protocol (PPTP)** - Point-to-Point Tunneling Protocol (RFC 2637) works at the link layer. No encryption or key management included in specifications. A VPN tunneling Protocol used to send secure communications from point to point. It is used to access a network through the network using the speed of a modem. It uses PPP encryption or Microsoft Point to Point Encryption (MPPE) over TCP as a transport protocol. This means that PPP packets are encrpted, then placed in TCP packets and sent over the internet. On the other side, the information is unwrapped and decrypted and sent on as PPP. Therefore the same protocols supported by PPP are supported with PPTP (AppleTalk, IPX, TCP/IP, and NetBEUI). **PPTP Installation is done with the Routing and Remote Access Administration Tool**.
- **Layer Two Tunneling Protocol (L2TP)** - Layer2 Tunneling Protocol. (RFC 2661) combines features of L2F and PPTP and works at the link layer. No encryption or key management is included in specifications. A VPN tunneling Protocol. It uses IPSec for encryption. It puts data in PPP packets, then adds more headers to route the packet. L2TP supports header compression and tunnel authentication support, and PPTP does not.**L2TP Installation is done with the Routing and Remote Access Administration Tool**. It is a new protocol with Windows 2000.
- **IPSec** - Internet protocol security, developed by IETF, implemented at layer 3. it is a collection of security measures that address data privacy, integrity, authentication, and key management, in addition to tunneling. Does not cover key management. A VPN tunneling Protocol. It is a new protocol with Windows 2000.

- IPSec installation - It is installed in Windows 2000 from the Microsoft Management Console (MMC) by adding the "IP Security Policy Management" snap-in and choosing the computer the new snap-in will manage.
- IPSec Configuration - Once installed, IPSec is configured from the TCP/IP properties dialog box in "Network and Dial-up Connections" for the connection you want to configure.
    1. In the TCP/IP properties box, click "Advanced".
    2. Click on "Options"
    3. Select "IP Security", and click "Properties".

  The allowed settings are "Do not use IPSEC" or "Use the IP security policy". The choices are:
    - Client (Respond Only)
    - Secure Server (Require security)
    - Server (Request Security)

Authentication Protocols Supported

- **PAP** - Password Authentification Protocol is a two way handshake protocol designed for use with PPP. Authentication Protocol Password Authentication Protocol is a plain text password used on older SLIP systems. It is not secure.
- **CHAP** - Challenge Handshake Authentication Protocol is a three way handshake protocol which is considered more secure than PAP. Authentication Protocol.
- **MS-CHAP (MD5)** - Uses a Microsoft version of RSA message digest 5 challenge and reply protocol. It only works on Microsoft systems and enables data encryption. Selecting this authentification method causes all data to be encrypted.
- **RADIUS** - Remote Authentication Dial-In User Service used to authenticate users dialing in remotely to servers in a organization's network. It can be used to track users' time on networks. User information is sent to a RADIUS server for validation when the user logs on to a network. It is a new protocol with Windows 2000. The RAS server must be configured as a RADIUS client on the **Remote Access Service properties dialog box security tab**. The RAS server may be configured to use any of several RADIUS servers for user authentication. The "Configure" button is used to add or remove RADIUS server information. The working sequence between the RAS server and the RADIUS server is as follows:
    1. A server running Remote Access Service (RAS) receives a connection request from a user on a remote computer.
    2. The remote computer is requesting RADIUS authentication.
    3. The RAS server forwards the request to a RADIUS server for authentication. (The RAS server becomes a RADIUS client).
    4. The **Internet Authentication Service (IAS)** on the RADIUS server responds to the request from the RAS server. (IAS can be installed and configured in the Control Panel network services dialog box.
    5. The RAS server takes appropriate action in verifying the user based on the

RADIUS server response.

- **EAP** - Extensible Authentication Protocol is used between a dial-in client and server to determine what authentication protocol will be used. Used to support smart card and other high tech forms of authentication through its support of **Transport Layer Security (TLS)** which is used by these devices. It is a new protocol with Windows 2000.

Open the RAS server Remote Access Service properties dialog box and select the "Security" tab to enable these protocols (exclusive of RADIUS which is actually a service).

Bandwidth Allocation Protocols

- **BACP** - Bandwidth Allocation Control Protocol. It is used with PPP.
- **BAP** - Bandwidth Allocation Protocol is a bandwidth control protocol for PPP connections. It is a new protocol with Windows 2000. It works with BACP.

Open the RAS server Remote Access Service properties dialog box and select the "PPP" tab to enable these bandwidth allocation protocols.

Transport Protocols Supported

Supports:

- **NetBEUI** - Microsoft developed a suite of protocols around NetBIOS using NetBEUI for transport. The primary advantage of this protocol is that it is easy to configure and Microsoft claims that it runs faster.
- **NWLink (IPX/SPX)** - IPX/SPX is a routable protocol and can be used for small and large networks. It was created by Novell primarily for Novell NetWare networks, but is popular enough that it is used on products that are not from Novell.
- **TCP/IP** - The TCP/IP suite of protocols is the set of protocols used to communicate across the internet. It is also widely used on many organizational networks due to its flexiblity and wide array of functionality provided.
- **AppleTalk** - Apple Computers have had their own set of protocols for many years. More and more operating systems today now can communicate with Apple systems using Apple networking protocols.

The client may support one or more of these protocols but the RAS server can act as a router for dial in clients supporting various transport protocols even if the client does not.

Supported Connection Types

The RAS service supports both hardware ports and virtual private networking (VPN) ports.

VPN is a method of providing an encrypted virtual private network over a public network. It encapsulates IP packets as data inside other IP packets (tunneling) to send them across the public network.

- Analog Telephone (PSTN). Uses PPP or SLIP for support over PSTN lines. NT RAS hosts only answer when PPP is used, but the other protocols are supported for dial out. SliP only supports TCP/IP and does not support logon encryption or dynamic Ip assignments.
- Digital Telephone (ISDN)
- X.25 - Packet switching protocol used on dial-up or leased lines.
- ATM
- Point to point tunneling protocol (PPTP) and L2TP for VPN connections across the Internet.
- RS-232 NulL modem cable.

Clients that the RAS server can host

- TCP/IP clients using PPP - These clients cannot use domain resources.
- LAN Manager
- DOS RAS
- Windows for Workgroups
- Windows 95/98
- Windows NT 3.1 and above
- Windows 2000

RAS Server Properties Box

Tabs:

- General - Used to set up as a router (for LAN only or LAN and demand dialing) or as a remote access server.
- Security - Used to set authentication provider (Windows or RADIUS-Remote Authentication Dial-in User Service) and accounting methods (none, Windows, or RADIUS). If RADIUS is used, RAS must be configured to use one or several RADIUS servers. Authentication methods are set here. These are the choices:
    - Extensible authentication protocol (EAP) - Allows the client and server to negociate a common method. It allows Transport Layer Security (TLS) which supports smart cards and thumbprint readers.
    - Microsoft encrypted authentication version 2 (MS-CHAP v2)
    - Microsoft encrypted authentication (MS-CHAP)
    - Encrypted authentication (CHAP) - Uses Message Digest 5 (MD5) encryption. It is for non Microsoft clients or clients not supporting MS-CHAP.

- Shiva Password Authentication Protocol (SPAP) - For Shiva LANRover clients.
- Unencrypted Password (PAP)
- Allow remote systems to connect without authentication

CHAP stands for Challenge Handshake Authentication Protocol. It causes the Server to send a challange to the client that contains a session and challenge key. The client sends the encrypted remote user name, password, session key and challenge key. The server verifies the information and sends a response back to the client indicating that it is authenticated. The client receives the response and begins the connection. MS-CHAP version two encrypts all authentication information. MS-CHAP does not encrypt the user name. CHAP requires user passwords to be stored in an encrypted form that can be reversed.

- IP - Options:
  - Enable IP routing
  - Allow IP based remote access and demand-dial connections
  - IPaddress assignment using either DHCP or a static address pool.
  - Specify the adapter to be used to obtain DHCP, DNS, and WINS addresses for dial-up clients.
- IPX - Options:
  - Allow IPX based remote access and demand-dial connections
  - Enable network access for remote clients and demand-dial connections
  - IPX network number assignment as automatic or in a listed range.
  - Use the same network number for all IPX clients
  - Allow remote clients to request an IPX node number
- NetBEUI - Options are allow NetBEUI based remote access clients to access either this computer only or the entire network.
- AppleTalk
- PPP - Options:
  - Multilink connections
    - Dynamic bandwidth control using BAP or BACP - As bandwidth requirements change, the server and client can negociate for the addition or deletion of physical connections.
  - Link control protocol (LCP) extensions
  - Software compression - More efficient than modem compression, but compression on the modem should be disabled, if this is enabled.
- EventLogging - Options:
  - Log errors only
  - Log errors and warnings
  - Log the maximum amount of information
  - Disable event logging
  - Enable Point-to-Point Protocol (PPP) logging

Remote Access Policies

These policies are stored on the remote access server, not in Active Directory. Three components which must be met by the client in order:

1. Conditions - Conditions to be met by the client such as:
    - Called station number
    - Calling station number
    - Client friendly name
    - Client IP address
    - Client vendor - RADIUS proxy Manufacturer .
    - Day and time restrictions
    - Framed protocol - PPP, AppleTalk, etc.
    - NAS Identifier - Network Access Server (NAS) is a proprietary hardware access server. The identifier is a string identifer of the station starting the service request.
    - NAS IP address
    - NAS Port Type
    - Service Type - Logon, callback.
    - Tunnel Type - Type of tunneling protocol that must be used.
    - Windows Groups - Security group the user must belong to.
2. Permissions (Dial-in) - Access to the RAS is allowed or denied. These permissions are checked if the above conditions are met. Can be set using remote access policies or with the user's account properties.
3. Profile - Tabs: Includes multilink options, authentication methods, IP address assignment methods and more.
    - Dial-in Constraints
        - Disconnect if idle for:
        - Restrict maximum session to: number of minutes
        - Restrict access to the following days and times:
        - Restrict dial-in to this number only:
        - Restrict Dial-in media: Includes Ethernet, ISDL, SDSL, and others.
    - IP
        - IP address assignment policy:
            - Server must supply an IP address
            - Client may request an IP address
            - Server settings define policy
        - Define IP filters to apply during the connection. They are defined from client and to client.
    - Multilink - Maximum ports may be limited
        - Default to server settings
        - Disable multilink (restrict client to single port)
        - Allow multilink
        - Can set bandwidth to allow for one or more lines to be dropped if bandwidth requirements fall below a certain percent of capacity for a period of time. Uses the BAP protocol.

- Authentication - Selections:
  - Extensible Authentication Protocol and selection of EAP type such as smart card.
  - Microsoft encrypted authentication version 2 (MS-CHAP v2)
  - Microsoft encrypted authentication (MS-CHAP)
  - Encrypted authentication (CHAP)
  - Unencrypted Password (PAP, SPAP)
  - Allow remote PPP clients to connect without negociating any authentication method.
- Encryption - Selections:
  - No Encryption
  - Basic - IPSec 56 bit DES is used for L2TP VPN connections and MPPE (Microsoft Point to Point Encryption) 40 bit is used for other connections.
  - Strong - IPSec 56 bit DES is used for L2TP VPN connections and MPPE (Microsoft Point to Point Encryption) 56 bit is used for other connections.
  - Strongest - IPSec Triple DES is used for L2TP VPN connections and MPPE (Microsoft Point to Point Encryption) 128 bit is used for other connections.
- Advanced - Selections:
  - Filter ID
  - Framed compression
  - Service type

If there are no Remote Access Policies, the connection is denied. The connection is allowed if it matches the conditions of one policy, but may be later denied if permissions or the profile are not met. The order of the policies may be set using the "Routing and Remote Access" tool. The last component sets profiles rather than being met, however, if the dial-in client is not compatable with the profile, the connection is terminated.

The "Routing and Remote Access" tool can be used to monitor the status of the RAS server and monitor connections.

User Account Policy Settings affecting RAS

The Dial-in tab affects RAS:

Dial-in tab - Options:

- Choose one of Allow access, Deny access, or Control access through Remote Access Policy.
- Verify Caller ID may be checked.
- Callback options are one of No callback, Set by caller (Routing and Remote Access

Service Only), and Always callback to a specified number.
- Assign a Static IP Address
- Apply Static Routes with a button that allows for definition of static routes.

Modem Configuration

Use the Administrative Tool, Routing and Remote Access. Right click on "Ports" and select "Properties". Select the device, then select "Configure".

Inbound Connection Configuration

After installation of the Routing and Remote Access Server, do the following:

- Start the Administrative Tool, "Routing and Remote Access".
- Right click the server, select "Configure and Enable Routing and Remote Access".
- When the Routing and Remote Access Setup wizard starts, click "Next", then select "Remote Access Server".
- Configure the protocols to be used and the authentication options.
- Select the network connection, method of IP address assignment, and whether a RADIUS server will be used.

VPN Port Creation

- Start the Administrative Tool, "Routing and Remote Access".
- Right click "Ports" and select "Properties".
- Choose PPTP or L2TP for the WAN port.
- Click on the "Configure" button and select "Remote Access (inbound)" and click "OK".

Network Connection Wizard

The following connection configurations are created by using the "Network Connection Wizard". This wizard is started by clicking on "Start", "Settings", "Network and Dial-up Connections" and selecting "Make New Connection". These types cf connections may be configured using the wizard:

- Dial-up to a private network - Outbound connection to a private network.
- Dial-up to the nternet - Outbound connection to an internet server.
- Connect to a private network through the internet - Used to setup the ability to connect a system using VPN through the internet.
- Accept incomming connections
- Connect directly to another computer - This is a direct cable connection to another

computer

Multilink

In some cases, multiple lines may be used as though they are one connection to gain higher transfer speeds. The client and server must be NT computers to use multilink. The calling and receiving host must have the same number and type of multilink connections. This is supported in any combination of connections by NT. This is based on RFC 1717. Multilink is configured on the client and server using the Phonebook entry basic tab.

RAS Monitor

Used to monitor RAS performance. It is found on the Taskbar next to the time system tray. You can select it then have it display as a window.

RAS Logging

The following registry entry controls RAS logging by turning it on or off:

\HKey_Local_machine\system\CurrentControlSet\Services\Rasman\PPP\Logging

The log is stored in the file:

\WINNTROOT\system32\Ras\PPP.log

Installing and Configuring RAS

RAS must have at least one of TCP/IP, NWLink, or NetBEUI installed as a transport protocol. A different transport protocol may be selected to support each modem or RAS device.

1. Set up one or more of the following service types.
    - Use the modem applet in the control panel to install modems and configure them to use specific COM ports.
    - If using ISDN, it may connect straight into a serial port, or use a NT-1 network termination device. This can be on a separate card or may be on your network card. If the NT-1 is used, the RAS server treats the ISDN connection like a network card. The control panel network applet adapters tab is used to install this as though installing a network card. The ISDN adapter must be configured to use the appropriate ISDN protocol. The main ones are:
        - N11
        - AT&T 5ESS

        - Northern Telcom DMS-100

      Set ISDN SPIDs (Service profile IDs) to two for maximum speed and use two telephone numbers. The SPID is a prefix and suffix along with the normal 10 digit phone number. Set the connection to be multipoint to use each channel.
    - To install X.25, the RAS setup dialog box is usedX.25 PAD button
2. The "Routing and Remote Access" administrative tool is used to configure RAS. The "Network and Dial-up Connections" folder is used to add additional protocols. If more protocols are required, add them first. The "Routing and Remote Access" administrative tool can be installed from the /i386/Adminpak.msi package file on the Windows 2000 server(s) CDROMs.
3. Configure the RAS network protocols - The RAS server will use the PPP data link protocol rather than a protocol like ethernet. It may use PPP or SliP to dial out.
    1. Different modems or RAS devices may be configured to use different network/ transport protocols. For example one may use TCP/IP, while another uses NetBEUI. To set the protocol, use the control panel's Network applet, services tab. Any combination of TCP/IP, NWLink, or NetBEUI may be used.
    2. Set up each transport protocol and select whether clients can access the entire network or not.
4. **Configuration is done using the control panel network applet services tab.** Select "Remote Access Service" and properties. Highlight the port to use and click on the network button. A Network Configuration dialog box will appear with the following options:
    - Dial Out Protocols with selections of NetBEUI, TCP/IP, and IPX. The configure buttons next to the checkboxes allows each protocol to be configured including the ability to use the protocol for dialing out.
    - Server Settings with:
        - Allow remote clients running:
            - NetBEUI
            - TCP/IP - Options for IP addresses include:
                - Use DHCP to assign remote TCP/IP client addresses - If DHCP is used, DCHP must be run on the RAS server, or the DHCP relay agent must be run on the RAS server.
                - Use static address pool - Used when DHCP is not available on the network and IP address are still desired
                - **Allow remote clients to request a predetermined IP address** - Used when DHCP is not available on the network and RAS clients have a unique IP address assigned. IP address cannot be assigned based on user account.
            - IPX
        - Encyption Settings with:
            - Allow any authentication including clear text.
            - Require encrypted authentication.
            - Require Microsoft encrypted authentication with an additional

checkbox, "Require data encryption".
    - Enable Multilink checkbox

RAS clients are configured using the control panel Dial-up Networking applet. The phone book entry is used and it has the following tabs:

- Basic
- Server - Select the RAS server type, transport protocols to use and "Enable software compression" and "Enable PPP LCP extensions".
- Script - Used for dial up servers that are not RAS servers
- Security - Specifies type of authentication, clear text, encrypted, and Microsoft encrypted. Must match the server side unless the server allows any authentication.
- X.25

To use ISDN with RAS, the following must be done:

1. An ISDN BRI circuit must be installed by the provider.
2. An ISDN adapter must be installed on the RAS server.

Server Configuration Selections

- Allow access to RAS server only or act as a gateway to the rest of the network.

When the RAS service is running, the COM ports and modems being used by the RAS service are not available for outgoing connections such as FAX or terminal software. To use these functions, stop the RAS service, then start it again when done.

Remote Access Administrative Utility

Used to configure RAS permissions for users. The following features exist on the Remote Access Permissions dialog box:

- Grant dialin permission to user checkbox
- Call back radio button section with options:
    - No Call Back
    - Set By Caller
    - Preset To followed by a text box.

Permissions cannot be set for groups.

Authorizing RAS Users

RAS users can be authorized in two places:

- User Manager for Domains dial-up button.
- Remote Access administrative tool.

RAS Security

Security settings are entered by using the **phonebook entry security tab**. This is the same on the client and server side.

- Encrypted passwords - Protocols used:
  - PAP - Password authentication protocol
  - CHAP - Challenge handshake authentication protocol uses encrypted authorization.
  - MS-CHAP - This uses MD-5 (Message Digest 5) security protocol over PPP. If the option to "Require data encryption" is set when using MS-CHAP, all data between the client and ther server will be encrypted. **Only Microsoft clients can use this protocol**.
- Callback (server only) - Calls the client back to establish the connection. Options are "No Callback", "Set by caller" or "Preset to...".
- Permissions (server only) - Can set up users who can use RAS as a client.
- PPTP (server only) - Point to Point Tunneling Protocol used for virtual private networking (VPN) as a means of sending secure information. To use this, when enabled on the server, the client will connect to the internet, then connect to the RAS server using the PPTP client service. The control panel, network applet protocols tab is used to add PPTP.

When having trouble getting authentication to work, the option "Allow any authentication including clear text" can be useful while debugging. Be careful of allowing access to sensitive information that will not be encrypted over the serial line.

PPP Security

- Encryption of logon requests.
- Supports multiple transport protocols.

Windows 2000 WINS

The purpose of WINS is to allow a NetBIOS name to be converted to an IP address. Therefore computers using WINS must be using NBT (NetBIOS over TCP/IP). WINS was originally put in place to compensate for a shortcoming of NetBEUI which is the fact that it is not routable. Therefore on large Networks IP is used to transport NetBIOS and rather than using broadcasts, information is sent to the WINS server.

WINS converts Windows computer names to IP addresses but does not do name lookups based on IP addresses. The use of Windows Explorer or NET commands invokes the NetBIOS interface. NetBIOS names, if repeated on another domain that is on the network, may cause a problem since there is no way to distinguish NetBIOS names between two domains. Each computer, when booted, sends a name registration broadcast. If there is no response, the computer will use the name it registered. A NetBIOS broadcast releases the computer name when the computer is shutdown gracefully.

WINS reduces this broadcast traffic when using NBT. The registration and release is sent to the WINS server rather than being broadcast. The clients have the IP address of the WINS server and they are configured to use WINS before using NetBIOS broadcasts. A backup WINS server may be available on the network for fault tolerance.

Five NBT Name Resolution Methods

- **B-node** - broadcast - Uses UDP broadcast datagrams. Default node type.
- **P-node** - Peer to peer - Uses a NetBIOS name server such as WINS. If a WINS server is not available, broadcasts are not used as a backup. The WINS IP address must be specified at each client?
- **M-node** - Mixed - Tries B-node, then P-node resolution.
- **H-node** - Hybrid - Tries P-node, then B-node resolution. After this attempt for Windows 2000, LMHOSTS and HOSTS files are used, then the DNS server is used.
- **Microsoft enhanced B-node** - Checks address cache which is loaded brom the lmhosts file when the system boots. After checking address cache, a broadcast is sent, then the lmhost file is checked if broadcasting did not resolve the query.

NetBIOS Names

On the WINS server, there is a NetBIOS name for each service a NetBIOS computer offers. This uses the 16th hidden character of the NetBIOS names. Up to 25 records of groups, domain browsers, and multihomed computers may be registered. The characters and their meanings are:

- 00 - Workstation service (Domain name) or (Workgroup name) or (Computer name)
- 03 - Messenger service (Computer name) or (User name)
- 06 - RAS server service (Computer name)
- 1B - Primary domain controller (Domain name)
- 1C - Domain controller or PDC or BDC (Domain name)
- 1D - Master browser (Domain name)
- 1E - Only is on servers, indicates the computer would become a browser if requested.. (Domain name) or (Workgroup name)
- 1F - NetDDE service (Computer name)
- 20 - Server service (Computer name)
- 21 - RAS client (Computer name)
- BE - Network Monitoring Agent service (Computer name)
- BF - Network monitor utility service (Computer name)

WINS Operation

When a NetBIOS broadcast is to go out, a computer sends over TCP/IP to a WINS server to resolve NetBIOS names. WINS dynamically builds its database. When a client uses WINS it announces to the WINS server over TCP/IP rather than broadcasting to all computers. WINS Message Modes:

- **Client Name Registration** - When a client service is started, the appropriate NetBIOS name for that service, for all NetBIOS processes (Using the hidden 16th byte) is sent to the WINS server. If the registration fails, the client retries every ten minutes. If the primary WINS server fails to respond, the request is sent to the secondary WINS server after three tries. If no WINS server responds, B-node broadcasts are used by the client. When contacted, the WINS server returns a time to live (TTL) field containing the length of time the client may use that name. If a duplicate name is received, the server sends a **wait for acknowledgement (WACK)** to the registering client. Then a **challenge** is sent by the server to the registered client. If the current owner responds correctly, the new client request is rejected.
- **Client Lease Renewal** - When the name lease is at 50%, the client sends a name **renewal** request to the WINS server with its name and IP address. When the lease is 7/8 up, the client will try again then attempt a lease with the secondary WINS server. After 4 attempts with the secondary WINS server, it attempts lease renewal with the primary WINS server again.
- **Client Name Release** - The client sends a name **release** message with its name and IP address. The server responds with a positive release message. If no confirmation is received by the client a NetBIOS broadcast release is sent up to three times.
- **Server Name Query and Name Resolution response** - With WINS server on the network, resolution is done using H-node on UDP port 137 (NetBIOS Name Service). Name query order:

1. Local cache
2. WINS server (primary then secondary, two times).
3. Broadcast
4. Lmhosts file
5. Hosts file
6. DNS

WINS Database

When a client is turned off, it releases its name, but there is a WINS extinction interval that allows the record to remain for some period of time in case the client is turned on again (as in the case of a reboot). The extinction interval reservs the record for some period so other clients cannot use it until the interval expires. **WINS files are in SystemRoot\System32\Wins**. A file names **WINS.MDB** is used to store a WINS database which can be backed up and repaired. The WINS service will back up the database every three hours (by default) to the configured backup path. Version numbers can be used to backup minor changes. The only way to replace a new copy with an older copy is to delete the old database copy first. The easy way to restore a database is to force replication from a WINS partner with a good copy of the database.

The database contains the following records:

- **Renewal interval** - Equivalent to the DHCP lease interval, it is the amount of time for the client to re-register the NetBIOS name before it is released.
- **Extinction interval** - The time a releast record exists before being tombstoned.
- **Extinction timeout** - The time a tombstoned record exists before being erased.
- **Verification interval** - The time an active record exists before being verified with the name owner.

WINS Proxy Agent

A WINS proxy agent can be configured to act as a relay for non-WINS clients. The WINS proxy agent can intercept client broadcast requests, forward them to a WINS server and return the response. It may also reply with the response without contacting the WINS server if the required information is in its cache. One WINS proxy is used on each subnet that has non-WINS clients. This means that machines that are not using WINS (Even Windows machines such as those without TCP/IP) can use a proxy agent to let them find resources on other subnets. There should be a maximum of two proxy agents per subnet. The agent must be a Windows based client, not a server. When NetBIOSs names are registered, both the proxy agent and the WINS server checks the name. The proxy agent is configured at the following registry location:

Hkey_Local_Machine\System\CurrentControlSet\Services\NetBT\Parameters

Set the EnableProxy parameter to REG_DWORD value of 1 and restart the computer.

WINS Replication

When two WINS servers are configured to communicate with each other replication occurs any time the data base on one of them changes. Servers are configured as a push or pull partner. A server can be both a push and pull partner. Push partners send update notices when a database change is made. A pull partner asks push partners for database entries more recent than their current listings. Only changes are replicated. Pull servers are used across slow links since pull requests can be set for specific times.

- A pull server will pull updates when it is started, then at chosen times thereafter.
- A push partner will send updates when a change threshold is reached. A thershold and update interval may be set.

WINS Properties Box

The WINS properties box can be opened by right clicking on a server in the WINS snap-in and selecting "Properties". Tabs:

- General - Can set how often databases and logs are updated with new information. Set where database files are backed up
- Intervals - The following intervals can be set (described above):
  - Renew interval
  - Extinction interval
  - Extinction timeout
  - Verification interval
- Database Verfication - Controls whether the WINS database integrity is verified and how often this is done.
- Advanced - Controls logging of events. Also can set the number of requests the server can handle at one time. The location of the database is set.

Replication Properties Box

Tabs:

- General
- Push Replication
- Pull Replication

- Advanced

Windows 2000 Internet Information Server

IIS Components

- File transfer Protocol (FTP) Server
- World Wide Web (WWW) Server
- Simple Mail Transfer Protocol (SMTP) Service
- Network News Transport Protocol (NNTP) Service
- FrontPage 2000 Server Extensions
- Internet Services Manager (HTML)
- Internet Information Services Snap-in
- Visual InterDev RAd Remote Deployment Support
- Indexing Service
- Certificate Services

Windows 2000 Professional can only support 10 network connections and Windows 2000 Servers support an unlimited number of connections. Windows 2000 Professional includes the **Personal Web Manager** package (a web site administration tool) not included on Windows 2000 servers. The HTML Internet Services Manager and the NNTP Service are not available on Windows 2000 Professional.

Most IIS components are installed when Windows 2000 is installed. The "Add/Remove Programs" applet in the control panel may be used to add any additional IIS components. Select "Add/Remove Windows Components", click on "Internet Information Services (IIS)', then click details.

Created at Installation of IIS

- Default Web Site located in c:\Inetpub\wwwroot

Security Enhancements

Security of the WWW server can be increased by:

- Obtaining a certificate for the web server
- Enable IP address or domain name access restrictions.
- Disable anonymous access and specify a secure authentication method.
- Configure the web server to send encrypted communication.
- Place all content on an NTFS file system.
- Set up home directory security settings.

- Use firewalls to protect the server.

Web Site Management

The "Internet Services Manager" is used to manage web sites on the computer. This can be done locally or remotely.

The Web Site Properties dialog box can be displayed by starting the "Internet Services Manager", click on the + next to the server to be configured, then right click the web site to configure, and select "Properties". The Web Site Properties dialog box tabs are:

- **Web Site** - Web site properties window with an IIS 3.0 Admin tab allowing selection of the web site to be administered if a user connects with the IIS 3 administration tool. Only one web site may be managed with the IIS 3 administration tool. This tab is used to configure **Web site ID, Connections, and Logins**. The following may be set:
  - Description - Identifies the site in the Microsoft Management Console.
  - IP Address
  - Advanced button brings up a window:
    - Multiple Identities - A text list box set of entries including IP address, port and host header the site responds to. Default port is 80 and SSL port is 443.
    - Multiple SSL Identities - The site and port number secure connections are made over (default 443).
  - TCP Port - Default is 80.
  - SSL Port - Port for SSL communications. Default is 443.
  - Connections limited or unlimited - Default limited connections is 1000.
  - Connection Timeout - Default is 900 seconds.
  - Enable Logging checkbox and specify "Active log format". Format types:
    - Microsoft IIS Log Format
    - NCSA Common Log Fromat
    - ODBC Logging - For database, very resource intensive.
    - W3C Extended Log File Format - The most flexible
  - Log "Properties" button and window:
    - General Properties - Set log file creation frequency and location where log files are stored.
      - The New Log Time Option - Causes new file creation, set to daily, weekly, monthly, unlimited, or when the log file gets to a specific size. The default is daily.
      - Directory path the log file is stored in.
      - Extended Logging Options list items that can be in the logging file:
        - Date
        - Time - default

        - Client IP Address - default
        - User Name
        - Service Name
        - Server IP
        - Server Port
        - Method - default
        - URL Stem - default
        - URL Query
        - HTTP Status - default
        - Win32 status
        - Bytes Sent
        - Bytes Received
        - Time Taken
        - Protocol Version
        - User Agent
        - Cookie
        - Referrer
    - ODBC Properties - Set the data source name (DSN), log data table. The user name and password used to store data in the database is set.
    - Extended Properties - Use checkboxes to select fields to be put in the log file. Time, client IP address, method, URI stem, and HTTP status are saved by default.
- **Operators** - Configure what users may manage the web site. In the Web Site tab, operators cannot set IP Address, Port, SSL Port, or use the Advanced button. In the performance tab, operators can't use the Bandwidth throttling. In the home directory, operators cannot set Directory Source, read setting, write setting, and application settings.
- **Performance**
    - Performance Tuning - Sliding bar used to adjust server resources to he held in reserve to service requests quickly. This can be set depending on the number of hist per day that are expected. Fewer than 10,000, fewer than 100,000, or more than 100,000.
    - Enable Bandwidth Throttling - Limits the bandwidth use of one web site. It is enabled (default) or disabled.
    - Maximum Network Use - The value in Kbps of maximum bandwidth the website may use.
    - HTTP Keep-alive Enabled - Requires more resources, but keeps the connection to the web browser open for quicker response. Turning off keep-alives or setting a short timeout can improve the performance of an IIS server that is low on memory and bandwidth.
- **ISAPI Filters** - Add ISAPI filters to modify IIS performance for the web site. They are Internet Server Application Prrogramming interfaces and have global and site filters. Global filters are not be displayed, although they are applied. The web server must be

restarted after adding or modifying global filters but, site filters are effective immediately. Global filters are run prior to Site filters.

- **Home Directory** - Enter username and password who has access to a remote directory where that username and password is used for the access. Select where home files are:
  - Content comes from "A directory located on this computer" radio button.
  - Content comes from "A share located on another computer" radio button.
  - Content comes from "A redirection to a URL". This option is used to redirect to another web site, when that web site has been moved.
  - "Local Path" or "Network Directory".
  - Access Permissions checkboxes of **Read**, **Write** (The browser may update files with the PUT command is Write access is allowed), and **Script source access**".
  - **Content Control** checkboxes of "**Log visits**" (Access is logged), "**Directory browsing**" allowed (A directory listing is sent to the browser), and "**Index this resource**" (A searchable index is generated)).
  - **Application Settings**
    - Name
    - Starting point
    - Execute Permissions:
      - None
      - Scripts only - Files with appropriate extensions are run as scripts without execute permission set.
      - Scripts and Executables - Files with proper extensions are run as scripts or ISAPI DLLs or CGI executables.
    - Application Protection
- **Documents** - Specifies the default document to be returned by the browser if no document on the web page is specified. A footer for all HTML pages on the web site may also be specified. Options:
  - Enable default document - The page to show if a specific page is not requested. Several documents may be listed with the document at the top of the list being the default document.
  - Enable document footer - Can be used to add footer information to each page.
- **Directory Security** - Three buttons:
  - Anonymous Access and Authentication Control - Any account using the anonymous logon or basic authentication must have the log on locally privilege configured in User Manager for Domains.
    - Allow Anonymous Access checkbox - Allows any web browser to access without a username or password. Used rather than basic or Windows NT Challenge/Response authentication if this is on also.
    - Account Used for Anonymous Access button - Specification of the anonymous access account.
    - Basic Authentication checkbox - Allows uses with web browsers that don't support Windows Authentication to give a username and password for restricted web page access. The account name and password are not

encrypted. Used if anonymous access is disabled or file permission does not permit anonymous access requiring a domain user account. This requires a domain user account.
        - Default Domain for Basic Authentication "Edit" button - The domain the user using basic authentication is assumed to belong in.
        - Digest authentication for Windows domain servers. - User accounts must store passwords with reversible encryption.
        - Integrated Windows Authentication - Required for requiring SSL communications to the web. Required to connect to the administration web site for this site (To perform remote administration). This requires a domain user account. Used under these conditions:
            - Anonymous access is disabled or denied due to file permissions requiring an NT user account.
        - Secure Communications - The "Server Certificate" button starts the IIS server certificate wizard.
    - IP Address and Domain Name Restrictions - Set all computers to either be granted access (radio button) or denied access (radio button) except those listed in the textbox. The textbox lists the IP and station address or internet names.
    - Assign a certificate to the web site
- **HTTP Headers**
    - Enable Content Expiration checkbox
    - Content should (radio buttons) - Sets when the content will expire in the web browser cache by sending expiration headers with the web page.
        - Expire Immediately.
        - Expire after Days(textbox) and minutes (textbox). Default is 30 minutes.
        - Expire on Date (boxes).
    - Custom HTTP Headers
    - Content Rating (Edit Ratings button) - Voluntary classification of subject matter.
        - Rating Service - Tab containing buttons to display a public web site with rating classification information.
        - Ratings - Set ratings from 0 to 4 for violence, sex, language, and nudity. An e-mail address of the rating person and rating expiration date is set.
    - **MIME Map** (File Types button) - Associate file types on the web page with MIME types. Multipurpose Internet Mail Extensions (MIME) types are sent to the web browser.
- **Custom Errors** - What to do if an error is encountered in serving the requested web page. Can specify an HTML file to be sent when an error occurs and use one of the following to specify where the file is:
    - File path
    - URL
- **Server Extensions** - Can be used after the web server is configured to use FrontPage server extensions.

Publication Methods

- Copy web pages into the default web site's home folder in c:\Inetpub\wwwroot.
- **Virtual Directories** - Causes directories on other servers to appear as though they are on your server. The Web Services Manager or Windows Explorer can be used to create virtual directories
- **Virtual Servers** - A single server is made to appear as though it is more than one server. They only work on Windows 2000 Servers, not on Windows 2000 Professional. Requirements:
    1. One of:
        - **An IP address is required for the primary server and each virtual server**. **IP addresses must be on one NIC**. Multiple IP addresses can be assigned to one NIC using the "Network Dial-up Connections" folder.
        - **A different TCP port number to be used**.
        - A different FQDN to be used to access the new site in the **Host Header for this site:** text box.
    2. **A home directory must be assigned to each IP address using the directories tab**.
-

Web Services Manager Menu Selections

Selections when the web site is selected:

- New
    - Virtual directory
    - Web Site - Used to create additional virtual web servers.

Personal Web Manager

Accessed from Administrative Tools, Personal Web Manager is for novices.

Indexing Service

This service indexes web site content by creating two databases of words, one based on web server HTML files and the other based on other document types. The database take about 40% of the amount of room the original data takes. The Indexing Service works on all Windows 2000 operating systems and must be configured to start automatically if desired.

Search Tools:

- Windows Explorer search tool.
- Start menu search tool.
- The "Computer Management" Index Service search tool. Computer Management is started by right clicking on "My computer" and selecting "Manage".

Certificate Services

Used to manage and issue security certificates which are used for providing secure web connections between the web client and the web server. The "Add/Remove Programs" applet in the control panel may be used to add Certificate Services.

Terms:

- Certificate Authority (CA) - An organization that is trusted to issue certificates.
  - Enterprise root CA - The first and most trusted CA on the network requires the use of Active Directory.
  - Enterprise subordinate CA - Subordinate to the enterprise root CA requires the use of Active Directory.
  - Stand-alone root CA - A root for the certificate hierarchy and does not require Active Directory.
  - Stand-alone subordinate CA - Subordinate to the stand-alone root CA and does not require Active Directory.
- Public Key Infastructure (PKI) - Implemented when certificates are used.
- Public Key
- Private Key

After Certificate Authorities are created, certificates can be set up fro use th selecting the administrative tool, "Certification Authority". Selections:

- Action
  - New
    - Certificate to Issue - Display certificates the CA cannot issue yet. This is where the CA can be authorized to issue these various certificates.

How users get Certificates

- Windows 2000 users can use the MMC Certificate snap-in command line utility by typing "mmc" on the command line.
- Access http://CA_server_name/certsrv with a web browser.
- Administrators can set group policy so computers request certificates automatically when they are required using the administrative tool "Active Directory Users and Computers".

Windows 2000 Terminal Services

Terminal services may be provided by Windows 2000 server computers. Terminal services can allow remote computers to run desktops and applications on a server as though it is running locally. This is similar to the functionality provided by X on UNIX and Linux platforms. Keystrokes and mouse action information is sent from the client to the server over the network and visual display information is sent back to the client from the server. Terminal services offer the following advantages:

- Since the computing is done on the server side, the terminal computer can be an older PC that is not powerful and it does not even require a hard drive.
- Administration of applications is easier since they are run on the server only.
- Users on the client computers cannot accidently misconfigure their computers, since there is virtually nothing to configure.

Modes

- Remote administration - The terminal server may be remotely managed, but applications cannot be run remotely.
- Application server - The terminal server may be remotely managed, and applications can be run remotely.

Licensing

No license is required for remote administration mode, but licensing is required for application server mode. The application server mode will run for 90 days without a license. Licensing is done on a per seat basis which means there must be a license for each computer that will access the terminal server. To set up licensing:

1. Use the "Add/Remove Programs" control panel applet to install "Terminal Services Licensing". It contacts the Microsoft Clearinghouse database to verify licensing.
2. Select either "Your entire enterprise" or "Your domain or workgroup" for the license option.

Required licenses:

- Windows 2000 Server license
- Windows 2000 Server client access license for each computer to connect.
- Windows 2000 Professional license or Windows 2000 Terminal Services Client Access License (TSCAL) for each client.

Additional licenses that may be purchased:

- Windows 2000 terminal Services Internet Connector License - For up to 200 users to connect over the internet.
- Work at Home Terminal Services Client Access License - For each user using the Terminal Services to work from home.

Terminal Services licensing uses the Microsoft Clearinghouse database to verify licensing.

Installation

The control panel "Add/Remove Programs" applet is used to install terminal services. Select "Add/Remove Windows Components", and select "terminal Services". Set up terminal services in **remote administration mode** or **application server mode** during installation. **Another option is to make permissions compatible with Windows 2000 users or make permissions compatible with Terminal Server 4.0 users**. The former setting is more secure, but most legacy applications won't run with that setting. If running in application server mode, the recommended server hardware includes:

- 600Mhz or faster microprocessor
- 512MB or more RAM
- Large hard drive

Components that are installed when Terminal Services is installed:

- Client Creator Files - Has a wizard for creating installation disks for clients.
- Enable Terminal Services - Used to turn terminal services on and off on the server.
- Licensing

Win16 on Win32 (WOW) is used to translate 16 bit applications to a 32 bit operating environment by terminal services. Running 16 bit windows or MS-DOS applications is not recommended since it will cost additional processing power and memory due to the overhead of rinning the Win16 or DOS virtual machines.

Additional Administrative Tools from Terminal Services Installation

- Terminal Services Client Creator - Used to create terminal services client boot disks.
- Terminal Services Configuration - Allows management of terminal services setup.
- Terminal Services Licensing - Management of client access licences (CALs).
- Terminal Services Manager - Allows session and process monitoring.

Installing Applications

Applications to be used with terminal services must be installed after terminal services is installed. The applications must be installed in a multiuser format and on an NTFS partition. Terminal Services must be in **"Install Mode"** when an application is being installed. Once applications are installed, to run applications from terminals, Terminal Services must be in **"Execute Mode"**. The control panel "Add/Remove Programs" applet is used to install the applications. Procedure:

1. Install all applications.
    1. Start the control panel "Add/Remove Programs" applet.
    2. Select "All Users Begin With Common Application Settings".
    3. Follow the installation prompts.
2. **Run scripts in the SystemRoot\Application Compatibility Scripts\Install directory on the Windows 2000 Terminal server computer**. There are scripts for several common applications, and these scripts optimize the applications to run with the terminal server. They add multiuser support, modify CPU intensive features, and modify the registry as required.
3. Log off, then log on.
4. Configure applications to use lower intensity video settings for maximum performance.
5. For better performance turn off application features that run in the background.
6. Remove the capability for applications to start other applications since this costs memory and performance.

The **Change User** command prompt command can also be used to install applications, but should be used to set up or confirm multiuser access capability for the application.

The most secure terminal services permissions mode is "permissions compatible with Windows 2000 users".

Client Configuration

The Terminal Services Client uses Remote Desktop Protocol (RDP) to connect to the server. Supported client systems:

- Windows 2000
- Windows 95, 98, Me
- Windows NT 3.51 or 4.0
- Windows for Workgroups 3.11

The Terminal Services Client creator was installed with the Terminal Services. This can be

used to create a floppy disk for Win32 or Win16 systems to get the Terminal Services Client to the client machines. Another method is to share the terminal services directory in SystemRoot \system32\clients\tsclient\net\Win32 or Win16 and access the software across the network. The Windows for Workgroups system must use the Win16 folder.

Terminal Services Command line utilities

Commands:

Command	Meaning
change logon	Used to **disable**, **enable**, or **check** the status of logons
change port	Modify DOS com ports or **query** for the status of ports.
change user	Change .ini file mapping for the current user. Applicable change user parameters are **install**, **execute**, and **query**.
cprofile	Remove user's profile file associations
dbgtrace	Enable or disable debug tracing
flattemp	Enable or disable temporary flat directories
logoff	End a client session
msg	Send a message to a client
query process	Display process information
query session	Display terminal services session information
query termserver	Display terminal server list
query user	Display logged on user list with information. Like "who" in UNIX.
register	Register a program
reset session	Reset or delete a terminal session.
shadow	Monitor or remotely control a Terminal Service session
tscon	Start a Terminal Services session
tsdiscon	End a Terminal Services session
tskill	Terminate a Terminal Server process
tsprof	Change a user profile path or copy user information
tsshutdn	Shut down a terminal server.

Terminal Services Manager

The Terminal Services Manager is a graphical based administrative tool used to manage terminal services. It is used on the terminal server or on a client during a session. It will perform the same functions as the command set listed above. The most important functions

include using remote control and monitoring and managing terminal services usage. The remote control ability will allow the administrator to take over a user's session. The user's remote control tab of the user's properties dialog box in "Active Directory Users and Computers" determines if the administrator can remotely control a user's session. Additionally it allows:

- Finding a terminal services server remotely.
- Making, managing, controlling, and ending sessions.
- Connecting to another session.
- Posting messages to sessions.

Terminal Services Configuration Tool

This is the Administrative Tool called "Terminal Services Configuration". To open the RDP-Tcp properties sheet, click on connections, right click on "RDP-Tcp", and select "Properties". The properties RDP-Tcp properties dialog box tabs are:

- General - Can set the encryption level of the terminal session.
- Logon Settings
- Sessions - Can override user settings that are set in Active Directory Users and Computers. The maximum length of a session and idle session may be set here. Sessions may be manually disconnected. Also reconnection parameters may be set so it is only possible to reconnect from the original connecting client.
- Environment
- Remote Control
- Client Settings - Can disable or enable print mapping, clipboard mapping, and LPT port mapping.
- Network Adapter - The the number of possible connections.
- Permissions - Set the permissions for users' access to connections.

Terminal Services can be used to remotely administer the server computer, but Microsoft recommends setting the following parameters:

- Disconnected or idle sessions end after five minutes.
- Override user settings so the session must end when the session limit is reached.
- Disable wallpaper to save memory.
- Set the encryption level to high.
- Set the maximum number of connections to 1.
- Change the registry value HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Terminal Server to 0.
- Disable print mapping, clipboard mapping, and LPT port mapping.

User Settings for Terminal Services

These are settings in Active Directory Users and Computers that affect user Terminal Services sessions.

1. Open "Active Directory User's and Computers"
2. Right clock on the user to be configured for terminal services and select "Properties".
3. The User's Properties Dialog box will open.

User's Properties Dialog box Tabs:

- General
- Address
- Account
- Profile
- Telephones
- Organization
- MemberOf
- Dial-in
- Environment
- Sessions - The maximum length of a session and idle session may be set here. Sessions may be manually disconnected. Also reconnection parameters may be set so it is only possible to reconnect from the original connecting client.
- Remote control - Can allow a users session to be remotely controlled. It can be configured to require the user's permission and allow the session to be view or allow interaction in the session.
- Terminal Services Profile - The user terminal services profile and terminal services home directory are set here.

The client can end a session by using the hot key combination that they selected.

Windows 2000 Web Services

Web services are used to act as a server for clients to provide web pages and web content upon request from clients. There are several tools in Windows 2000 systems which can perform these services:

- Peer Web Services - Used on Windows 2000 Professional computers.
- Internet Information Server - Used on Windows 2000 Server computers.

Peer Web Services

Peer web services is used on Windows 2000 Professional computers. It is installed from the Add/Remove Programs applet in the control panel. The following are added to administrative tools upon installation:

- Personal Web Manager
- Internet Services Manager

Windows 2000 Authentication

Authentication is performed by the system to be sure the user is really who they claim to be. Authentication may be done at and for a local computer or at a global level for a domain using domain controllers across the network. Windows 2000 supports the following types of authentication:

- **Kerberos V5** (RFC 1510) - An internet standard authentication protocol which is the default protocol for Windows 2000 computers within a domain. This is not used for computers in different forests.
- **Windows NT LAN Manager (NTLM)** - Used to authenticate users from Windows 95, 98, and NT systems. Windows 2000 Active Directory must be operating in mixed mode to use this authentication method.
- **Secure Sockets Layer/Transport Layer Security (SSL/TLS)** - Requires certificate servers and is used to authenticate users that are logging onto secure web sites.
- **Smart card** - Contains a chip with information about the user along with the user's private key. A personal identification number (PIN) is normally required to be authenticated using a smart card. Requires Extensible Authentication Protocol (EAP) to be enabled for the server to allow smart card authentication. Also some certificate authority must provide keys.

Authentication uses X.509 standard and kerberos.

Process of Logging On

1. CTRL+ALT+DEL is pressed, name and password entered, and local or domain logon is indicated.
2. If the logon is local, the name and password are checked against the local database. If the logon is a domain logon, the name and password are encrypted into a key, and timestamp information is encrypted. This information is sent to the Windows 2000 domain controller with an authentication request.
3. The domain controller decrypts the information and checks for a valid timestamp. If the timestamp is valid, two Kerberos tickets are made and encrypted with the password. The tickets are sent back to the client computer. The tickets are:
    - User session key - Used to log on.
    - User ticket - Used to get other Kerberos tickets for accessing other domain resources.
4. The client decrypts the tickets and uses the session key to log on.

Authentication when Accessing an Object

1. The user tries to access the network object.
2. The user ticket, user name, name of the object to access, and timestamp, are sent with a Kerberos ticket granting service request to the domain controller.
3. The domain controller decrypts the information, checks the timestamp, makes an encrypted session key (with user account and group information) and returns the key to the local client.
4. The client sends a request for the resource with the session key to the the server that has the resource.
5. The receiving server decrypts the session key, and checks the information against its ACL for the object being requested.

Shares used for logon

NETLOGON/SYSVOL - The Netlogon share is used on Windows NT domain controllers to authenticate users. In Windows 2000, the SYSVOL share carries out these functions. The SYSVOL share includes group policy information which is replicated to all local domain controllers.

Windows 2000 Accounts

Built In Accounts

The below accounts are created when any Windows 2000 system is installed. These accounts are also created on domain controllers automatically when Active Directory is installed.

- Administrator - Cannot be deleted or disabled and should be renamed.
- Guest - Disabled by default. A password is not required. This account can't be deleted but can be renamed, and should be disabled.

Account Types

- Local - For local computer access.
- Domain - For access to network resources in the domain.

Administrators and power users can create and modify accounts in the domain. Administrators on local computers can create and modify accounts locally. **Windows Scripting Host (WSH)** assists administrators in creating many users and groups quickly.

User Properties

- Username - A unique name up to 20 characters excluding:

  " / \ [ ] : ; | , + * ? < >\

  The username may be changed after it is created. Choose a naming convention for large organizations.
- Full name
- Description
- Password - Case sensitive and up to 14 characters.
- Confirm password
- User must change password at next logon - Checkbox
- User cannot change password - Checkbox
- Password never expires - Checkbox
- Account Disabled - Checkbox
- Account locked out - Checkbox

User accounts can be renamed. To change user characteristics, from User Manager for

Domains click on the user, then select the menu item "user", and change.

Account Creation and Modification

- Local account: - Use the "Local Users and Groups" tool.
    1. Right click "My Computer", select "Manage".
    2. Click the + next to "Local Users and Groups" in the "Computer Management" box.
    3. Enter user information into the "New User" dialog box.

    To modify the user properties, right click on the user and select "Properties". User Property tabs include:
    - General - Set up when user must change password (User must change password at next login, User cannot change password, or password never expires) and disable the account here. Indication of account lockout is here.
    - Member Of - Set up local groups the user is a member of.
    - Profile - Set up the environment variables, set a network path to the user profile folder and user home folder. The profile includes desktop settings.
    - Dial-in (Only on Server computers) - Set remote access permission, callback policy, and IP address and routing information.
- Remote account: - Use the "Active Directory Users and Computers" tool.
    1. From the Active Directory Users and Computers tool click + next to the domain name.
    2. Highlight the "Users" folder and select "Action", "New", and "User".
    3. Enter user information into the "New User" dialog box.

    To modify the user properties, right click on the user and select "Properties". User Property tabs include:
    - General - Set up when user must change password (User must change password at next login, User cannot change password, or password never expires) and disable the account here. Indication of account lockout is here.
    - Address - Set mail address or physical address information.
    - Account - Set hours that the user can logon during and restrict computers the user can use. Can set::
        - User must change password at next login
        - User cannot change password
        - Password never expires
        - Store password using reversible encryption.
        - Account is disabled
        - Smart card is required for interactive logon
        - Account is trusted for delegation - The user can delegate authority for their privileges or rights to other users.
        - Account is sensitive and cannot be delegated.
        - Use DES encryption types for this account.
        - Do not require Kerberos preauthentication - For systems supporting Kerberos but not preauthorization.

        - Indication of account lockout is here.
        - Can set when account expires.
    - Profile - Set up the environment variables, set a network path to the user profile folder and user home folder. A logon script file can be set. **Domain user logon scripts are in the NETLOGON share on the domain controller in the SystemRoot\SYSVOL\sysvol\domainname\SCRIPTS folder**. The profile includes desktop settings. Default profile file location is **C:\Documents and Settings\username** on the computer that the user logged on to.
    - Telephones - Can specify the user's home, pager, mobile, and fax phone numbers.
    - Organization - The user title, department, manager, and company can be listed.
    - Member Of - Used to assign users to groups and remove users from groups.
    - Dial-In - Dial-in provileges can be granted or denied and callback options are set here.
    - Environment - (With terminal services)
    - Sessions - (With terminal services)
    - Remote Control - (With terminal services)
    - Terminal Services Profile - (With terminal services)
    - Published Certificates - Can add or remove user internet certificates.
    - Object - View information about the user account object such as when the account was modified last.
    - Security - Can set users and groups that can modify this domain user account properties.

The "NET USER" command line tool may be used to create users when used with a batch file

Windows 2000 Permissions

The permissions on Windows 2000 systems are all selectable with two boxes which are:

- Allow - Grant the permission.
- Deny - **Any denied permission for a group or user will override any allow permission, even if the user is in a group that is granted that permission.**

If neither box is checked, the permission is not granted for the user or group, but if the user is in another group that has the permission, it will not be denied. Normally, if a user is a member of several groups that have different levels of permissions to an object, the least restrictive permissions apply unless the user, or one of their groups have the no access box checked for that permission.

Standard File and Folder Permissions

- **Read(R)** - View attributes, contents, and permissions. Can synchronize.
- **Write(W)** - Can change attributes, and file contents. Can create files or folders. Can synchronize.
- **Read(R) and Execute(E)** - Can change sub folders, perform read operations, and execute a file.
- **List Folder Contents** - Can perfrom read and execute permissions on folders. Can view folder contents, attributes, permissions. Can synchronize and change to subfolders.
- **Modify** - Perform Read, Execute, and Write permissions along with ability to delete.
- **Full Control** - Can perform Modify functions (above), take ownership, and modify permissions.

Permissions assigned to directories are inherited (default) by all files and subdirectories that are contained in the directory. The inheritance option, selected by default, may be deselected. Each file or directory has an Access Control List (ACL). To set permissions for additional users or groups, they are added to the ACL of the file or directory. Windows Explorer or the Cacls command line utility can be used to set permissions.

Special File and Folder Permissions

On the file or folder properties dialog, click the "Security" tab and the "Advanced" button to assign special file or folder permissions.

- **Traverse Folder/Execute File** - .
- **List Folder/Read Data** - .

- **Read Attributes** - The user can read the attributes (archive, compress, hidden, etc.) of the file, but not read the contents of the file.
- **Read Extended Attributes** - .
- **Create Files/Write Data** - .
- **Create Folders/Append Data** - .
- **Write Attributes** - .
- **Write Extended Attributes** - .
- **Delete Subfolders and Files** - .
- **Delete** - The user can delete the file.
- **Read Permissions** - The user can read the file.
- **Change Permissions** - Lets the user change permissions for the file, but not view or change the contents of the file.
- **Take Ownership** - The user can take ownership of the file, but can't give it back.

These permissions can be applied to directories, files, and subdirectories with one of the following selections:

- **This folder, subfolders and files**
- **This folder only**
- **This folder and subfolders**
- **This folder and files**
- **Subfolders and files only**
- **Subfolders only**
- **Files only**

File or Folder Creation, Moving, Copying and Permissions

- Created Files or folders - Inherit permissions of the folder they are created in.
- Moved or copied files or folders in the same NTFS volume - Keep their own original permissions.
- Moved or copied files or folders in a different NTFS volume - Inherit the NTFS permissions of the destination folder.
- Movement to any FAT volume - All permissions are lost.

Moving Files

When permissions are changed on a folder, by default, permissions are replaced on files in the folder, but not on subdirectories. This may be changed using the provided checkboxes such as "Replace Permissions on Subdirectories". When files are moved on NTFS partitions, if they are moved from one partition to another, it is as though they were copied. If files are moved to another folder, they retain their normal attributes including compression attribute reguardless

of the attributes of the parent folder they are being moved to. When files are copied to another folder, they will adopt the attribute s of the folder they are being copied to.

NTFS File and Share Permissions

When these permissions are different, the most restrictive permissions are applied. The share and NTFS file permissions must overlap in order for the user to have the permission. That means to read a file, the user must have both read share and read NTFS permission.

When a user has full control permission for a folder, the permissions will apply to the files in the folder even though permission for an individual file in the folder may be set to NO ACCESS for that user.**When a file or folder is moved, it retains its current permissions, but when it is copied, it inherits the permission of the parent folder or partition it is being copied to.**

Ownership

If the owner's user is a member of the administrators group, the owner is the administrators group. Administrators do not have access to all resources, but they may take ownership of any resource. Once ownership is taken, it cannot be given back. Also taking ownership of a resources changes all existing permissions for that resource.

Delegated Permissions

Permissions that can be delegated include:

- Create, delete, and manage user groups.
- Create, delete, and manage user accounts.
- Manage group policy links - Gourp policies assigned by organizational unit may be modified.
- Modify group membership.
- Read all user information.
- Read user account passwords.

Setting Permissions

1. Right click on the file or folder.
2. Select properties
3. Select the security tab on the properties sheet.
4. Click on the permissions button.
5. If the file you selected is a subdirectory there are the following check box choices:
    - Replace permissions on subdirectories - Permission changes are applied to all

sub folders.
    - Replace permissions on existing files - Permissions are applied to all files in the folder. If both are selected, permissions are applied to all sub folders and files in all files in the folder and its sub folders.
6. Click on OK to exit the permissions box and OK to exit the properties box.

Disk Quotas

Disk quotas are used to track the use of disk space for each user. They are normally disabled and are only supported on NTFS file systems. Quotas are tracked per partition and per user using ownership information to account for resource use. Compressed file sizes are measured according to the uncompressed file size.

Disk quotas may be viewed and administered by using the "Disk Management" tool to select the properties dialog box of the disk or volume. The "Quota" tab contains quota information and management functions. Quota management must be enabled. Warning levels may be set and hard limits may also be set. Disk space may be denied to users who exceed their quota limit. The events may be logged when the user exeeds their warning and/or quota limit.

Windows Explorer can be used to setup and monitor disk quotas. Windows Explorer local disk properties tabs:

- General
- Tools
- Hardware
- Sharing
- Security
- Quota - Used to enable quota management, deny disk space if the quota is exceeded, limit the disk space and set where the disk quota warning is given. You can also log when the user exceeds their warning level or quota level. The "Quota Entries" selection box is used to view quota utilization for the volume. To modify the quota levels for any given user, double click the user's entry.
- Web Sharing

Windows 2000 Groups

Groups cannot be renamed. Four types of group accounts:

- **Local group** - Has local computer permissions and rights only.
- **Global group** - The groups permissions and rights exist in the group's domain and domains that have a trust relationship with the group's domain. Global groups may be given rights and permissions of local groups. Only NT Server can create global groups.
- **Domain Local group** - Created on Active Directory controllers and are used manage access to resources in the domain.
- **Universal group** - Users from multiple domains that perform similar tasks or share resourses across the domains. Any group or user in any domain can be a member of the universal group. The universal group is however, not available in Active Directory mixed mode.

Local groups can include global groups. They will not include other local groups. Local groups are created in the User Manager. Created groups may be deleted with the User Manager, but built in system groups may not be deleted. When a domain is joined the domain administrators group is added to the local administrators group and the domain users group is added to the local users group on the computer that joins the domain.

Local Groups created on non domain controllers at installation time

- **Administrators** - Used to administer the system. It is a good idea to make a backup administrator user.
- **Power Users** - Have some administrative privileges such as ability to share directories and printers. Can manage Power Users, Guests and User groups.
- **Users** - Have privileges for daily tasks. All users on the computer are normally in this group. Can manage local groups they create.
- **Guests** - Have minimal privileges. Can be renamed. but can't be deleted.
- **Backup Operators** - Have privileges for performing system backup.
- **Replicators** - A service account that NT uses to perform the replication function. Allows the server to replicate files to the NT workstation machine.

Non-Domain Controller Special Groups

These are special groups that are not on the group menu. These groups also exist on domain controllers.

- **System *** - Used to manage accounts that provide system services such as the

webserver.

- **Everyone *** - All on the local machine, in the domain and trusted domains.
- **Interactive *** - A user at the local machine.
- **Network *** - Anyone who accesses information on this computer over the network (remotely). It can be used to restrict users from getting to specific resources over the network.
- **Creator/Owner *** - The owner of the resource.
- **Creator Group** - For Apple users or POSIX application users.
- **Anonymous Logon** - Any user that used anonymous logon.
- **Authenticated Users** - Any Windows 2000 locally or globally authenticated user.
- **Batch** - A program that logged on using the logon as batch job user right.
- **Dialup** - A user logged on using a phone line, VPN, or cable connection.
- **Service** - A service logged on with a user account.
- **Terminal Server Unit** - A user logged on using a terminal.

Local Groups on domain controllers

Created during Active Directory installation.

- **Administrators *** - Those who administer the domain and the server. It initially contains the DOMAIN ADMINS global group.
- **Account Operators *** - This group has privileges to to create and manage local and global users and groups in the domain. This group can also shut down the domain controller. This group is only on domain controllers.
- **Backup Operators *** - Those who can save file to tape backup media. This group is on all NT servers.
- **Print Operators *** - This local group can control the sharing of printers, along with shutting down the domain controller.
- **Server Operators *** - Basically this group can do anything on the NT server. They can format the hard drive, restore or backup files or directories, create and control shared directories, control the sharing of printers, lock/unlock the server, shut down the domain controller locally or remotely, and modify the system time.
- **Replicators *** - Used to perform directory replication. This group is on all NT servers.
- **Users *** - Those who use the server.
- **Guests *** - Includes the Guest account and Domain Guests group.
- **Pre-Windows 2000 Compatible Access** - Allows Windows NT 4.0 users to get domain access. The everyone needs to be a member of this group when there are NT computers in the domain.

Global and Universal Groups

- **Domain Admins *** - It is automatically a member of the administrators local group on all

machines that are a member of the domain. This way global administrators may remotely administer any machine in the domain. It initially contains the Administrator user account.
- **Domain Users *** - Contains all created domain user accounts. On the domain controller, this group is a member of the users local group. It initially contains all users in the domain except for guests.
- **Domain Guests *** - Contains the domain Guest account.
- **Enterprise Admins** - It is automatically a member of the administrators local group on all machines that are a member of all domains in the forest.
- **Schema Admins** - This group has rights to modify the schema of the Active Directory database. This group only exists on the highest level domain in the forest.
- **Domain Controllers**
- **Domain Computers** - Computers that are members of the domain.
- **Cert Publishers** - Users that can publish security certificates.
- **Group Policy Admins** - Users who can modify group policy settings for objects in the domain.

Group Creation

- Local group - Open the "Computer Management" dialog box by clicking on "My Computer", and "Manage". Click + next to "Local Users and Groups", highlight "Groups", select "Action", and "New Groups".
- Global group - The Administrative Tool, "Active Directory Users and Computers" is used to create and manage these groups.

Group Accounts

Pass through authentication is the process of a local user logon being passed to the domain allowing the user to be logged onto the domain at the same time. The local user name and password must be the same as the domain user name and password. domain user and group accounts are created and stored on the PDC (Primary Domain Controller) SAM (Security Accounts Manager) database. Two types of groups in a domain are:

- **Local groups** - These groups are used to manage local resources. They can exist on workstations, member servers, and domain controllers (PDC and BDC).
- **Global groups** - These groups can be used on any computer that is a part of the domain. Domain controllers are the only way to create and modify global groups.

Three domain global groups built in to the NT domain:

- **Domain Admins** - It is automatically a member of the administrators local group on all machines that are a member of the domain. This way global administrators may

remotely administer any machine in the domain.
- **Domain Users** - Contains all created domain user accounts. On the domain controller, this group is a member of the users local group.
- **Domain Guests** - Contains the domain Guest account.

Three local groups on the domain controller:

- **Account Operators** - This group has privileges to to create and manage local and global users and groups in the domain. This group can also shut down the domain controller.
- **Print Operators** - This local group can control the sharing of printers, along with shutting down the domain controller.
- **Server Operators** - Basically this group can do anything on the NT server. They can format the hard drive, restore or backup files or directories, create and control shared directories, control the sharing of printers, lock/unlock the server, shut down the domain controller locally or remotely, and modify the system time.

Active Directory Groups

There are two types of Active Directory groups, each with a different purpose. These are:

- Security principal groups. These groups can be assigned permissions. Their scope can be:
  - **Domain local**
  - **Global**
  - **Universal**
- Distribution groups- Used to group users for applications such as mail.

Windows 2000 User Rights and Auditing

User rights are different from access permissions which allow access to resources such as read, write or execute access. User rights allow system control which includes the ability to format a hard drive or shut the system down.

Local Users created at installation time

1. **Administrators** - Used to administer the system. It is a good idea to make a backup administrator user.
2. **Guests** - Have minimal privileges. It can be renamed. but can't be deleted. On NT workstation, disable the guest account or give it a password, since it is enabled upon installation.
3. **Initial User** - Member of administrators group.

Two levels of security

- **Logon**
- **User Rights**

Adding Accounts

The Use the "Local Users and Groups" tool is used to create user and group accounts locally and the "Active Directory Users and Computers" tool is used to create users remotely. They are also used to with managd functional user rights, security auditing, and account policies. Functional user rights determine what programs the user can run or what system capabilities they have. Passwords are case sensitive, but user names are not. Both can contain spaces.

Two methods of adding user accounts:

- Creation
- Make a copy of an existing account.

User names may be up to 20 characters long using upper and lowercase letters although it is not case sensitive. Does not use " / \ [ ] : ; | = , + * ? <, > characters in a user name. When an account is copied from a template the following fields are left blank:

- **Username**
- **Full Name**

- **Password and confirm password**
- **User cannot change password**
- **Account disabled**

User accounts should not be made local on various workstations when using domain user accounts. If a user account is deleted, when it is recreated, even though it may have the same name, it will have a different user ID number and resource access for that account must be set up again.

Logon

Password setting options the administrator can set for the user are:

- User must change password at the next login
- The user cannot change the password.
- The password never expires

Passwords are case sensitive and can be up to 14 characters. User names are not case sensitive and can be up to 20 characters. The user's home directory can be specified when the user is created or set later. The home directory is where data from an application is saved by default and where the command prompt will be when a command line session is begun.

User Rights

User rights are divided into:

- Logon rights
- User privileges

Logon Rights

Right	Description	Groups with the Rights
Access this computer from the network *	The user can connect to the computer remotely.	Administrators, Power Users, Everyone
Deny access to this computer from the network	The user cannot connect to the computer remotely.	?
Deny logon as a batch job		?
Deny logon as a service		?

Logon as a batch job		?
Logon as a service *	This right is used by background applications. The rights are required for the service to function	?
Log on locally *		All built-in groups, including Everyone, except Replicator

User Privileges

Privilege	Description	Groups
Act as part of the operating system		?
Add workstations to domain		?
Back up files directories *	The user can back up files or directories to storage media.	Administrators, Backup Operators
Bypass traverse checking *	Lets the user or group move through directory trees even if the group does not have permission to access the directories. Normally this right is given to Power Users.	Everyone
Change the system time *	Can change the current time.	Administrators, Power Users
Create a page file	The system memory pagefile size and location can be changed.	Administrators
Create a token object		?
Create permanent shared objects		?
Debug programs	Can debug threads	Administrators
Enable computer and user accounts to be trusted for delegation		?
Force shutdown from a remote system *	A system can be shutdown across the network.	Administrators, Power Users
Generate security audits		?
Increase quotas		?

Increase scheduling priority	Increase a processes execution priority.	Administrators, Power Users
Load and unload device drivers *	Device drivers may be added or removed from the system.	Administrators
Lock pages in memory	?	
Manage auditing and security log *	View auditing log files and control what the system audits.	Administrators
Modify firmware environment values	BIOS firmware may be changed.	Administrators
Profile single process	View a specific system performance counter.	Administrators, Power Users
Profile system performance	Check the system performance with Performance Monitor.	Administrators
Remove computer from docking station		?
Replace a process level token		?
Restore files and directories *	The user can restore files or directories from storage media.	Administrators, Backup Operators
Shut down the system *	Shut the system off.	Administrators, Backup Operators
Synchronize directory service data		?
Take Ownership of files or objects *	Make any objects owned by the user that is taking ownership. Ownership cannot be assigned to other users.	Administrators

Setting User Rights

- Organizational Units - In Administrative Tools, select "Active Directory Users and Computers".
- Domain - In Administrative Tools, select "Domain Security Policy". The ADMINPAK must be installed on the computer.
- Domain controllers - In Administrative Tools, select "Domain Controler Security Policy". The ADMINPAK must be installed on the computer.

- Local computers - From the Control Panel, "Administrative Tools" applet, double click "Local Security Policy".

Domain controllers do not have a power users group. On the Domain Controllers, Server Operators are similar to the Administrator group on the Workstation with all rights.

Auditing

The following user events may be audited:

- **File and Object Access** - Logs user access to directories, files, or printers.
- **Logon/Logoff** - Local and remote logon and logoff connections may be audited.
- **Process Tracking** - Logs events about the running of programs.
- **Restart, Shutdown, System** - Logs when the system is shutdown or started.
- **Security Policy Changes** - Logs changes to User Rights and Account Policies.
- **Use of User Rights** - Logs when a user exercised a user right.
- **User and Group Management** - Logs user and group management events.

Windows 2000 Auditing

Auditing is done from two programs depending on if the computer is local or a domain computer;

- Local computer - "Local Security Policy" administrative tool.
- Domain computers - "Domain Controllers Security Policy" administrative tool on domain controllers or other computers with the ADMINPAK installed. The "Domain Controllers Security Policy" administrative tool must be used to first enable auditing then the appropriate Active Directory administrative tool as listed below can be used.

Audit policy is configured at the following levels:

- Local
- Organizational Unit - Use the "Active Directory Users and Computers" administrative tool.
- Domain - Use the "Active Directory Sites and Services" administrative tool.

Audit policy is applied in the same order as group policy as listed by priority in the System Policy Editor's, Group Priority dialog box. The policy applied last overrides policies applied first if there is a conflict.

Auditing is divided into two main areas which are auditing of access to:

- Objects
- Systems - The "domain Controller Security Policy" tool is the best choice for enabling system access on a Windows 2000 Server computer.

Audit Policy

These policies are set using the administrative tool "Domain Security Policy". The following event successes or failures may be logged:

- Account logon events - User logs onto the domain.
- Account management - Account created, modified, renamed, or deleted.
- Directory service access - An active directory object was accessed. The active directory object must have auditing on.
- Logon events - A user logs on or off a Windows 2000 computer.
- Object access - An object was accessed. The object must have auditing on.
- Policy change - A user right, security policy, or other policy was changed

- Privilege use - A user right other than access to a computer or log on locally was used.
- Process tracking - A process was started.
- System events - System was shutdown, restarted, or security event happened.

The "Active Directory Users and Computers" administrative tool is used to configure auditing for active directory objects.

Active Directory Object Auditing

To enable object auditing on a computer System access auditing must be enabled. The administrative tool "Domain Security Policy" can be used to enable system access auditing. The "Domain Controller Security Policy" tool to enable system auditing on a domain controller. The administrative tool, "Active Directory Users and Computers" is used to modify active directory object auditing configuration. Failure and success of the following object events may be audited by user or group:

- Full Control
- List Contents
- Read All Properties
- Write All Properties
- Delete
- Delete Subtree
- Read Permissions
- Modify Permissions
- Modify Owner
- All Validated Writes
- All Extended Rights
- Create All Child Objects
- Delete All Child Objects

Auditing entries inherited from parent objects cannot be removed.

File Auditing

Windows Explorer is used to enable auditing on files and folders. The file or folder to be audited must be on an NTFS file system. Failure and success of the following file events may be audited by user or group:

- Traverse Folder / Execute File
- List Folder / Read Data
- Read Attributes
- Read Extended Attributes

- Create Files / Write Data
- Write Attributes
- Write Extended Attributes
- Delets Subfolders and Files
- Delete
- Read Permissions
- Change Permissions
- Take Ownership

Auditing settings are inherited from parent folders into sub folders or files contained in the parent folder(s).

Printer Auditing

Auditing on printers may be controlled from the "Printers" folder. Failure and success of the following file events may be audited by user or group:

- Print
- Manage Printers
- Manage Documents
- Read Permissions
- Change Permissions
- Take Ownership

Viewing the Audit Log

Use the administrative tool, "Event Viewer" to view the logs. Highlight "Security Log" in the left pane. Events may be filtered by selecting "View", and "Filter", then clicking the "Filter" tab. Events may be filtered by:

- Source
- Category
- Event ID
- User
- Computer
- Types including and of the checkboxes, Information, Warning, Error, Succes audit, and Failure audit.

Event viewer Menus:

- Action
    - Save Log File As

    - Clear all Events
    - Properties
- View
    - Filter - Filter to only see certain events.

To save a security log for analysis in a spreadsheet, save it as a comma delimited (.csv) file.

Security Templates

A file with security settings that can be applied to several computers. It is a text ".INF" file. They are managed with the MMC "Security Templates" snap-in. Once installed, it is the administrative tool called "Security Console" which is used to add and manage security templates. Security templates can:

- Be applied to several computers
- Be compared to a computer's current security configuration

Common templates:

- basicdc.inf - Default domain controller.
- basicsv.inf - Default server.
- basicwk.inf - Default workstation.
- compatws.inf - Compatable server or workstation.
- securede.inf - Secure domain controller.
- securews.inf - Secure server or workstation.
- hisecdc.inf - High security domain controller.
- hisecws.inf - High security workstation.

The following methods can be used to implement a security template:

- Import the template into a Group Policy Object (GPO) in Active Directory using the administrative tool, "Active Directory Users and Computers". Menus:
    - Action
        - Policies
- Import the template locally to a computer using the administrative tool, "Local Security Policy" or "Security Configuration and Analysis". Menus:
    - Action
        - Import Policy - Import a policy locally into the computer.

Security Configuration and Analysis

The "Security Configuration and Analysis" tool is used to analyze a computer security configuration. To get ready to use this tool, do the following:

- The MMC "Security Templates" snap-in must be previously installed Once installed, it is the administrative tool called "Security Console".
- The MMC "Security Configuration and Analysis" snap-in must be installed to the "Security Console" by starting it from "Administrative Tools", selecting "Console" and "Add/Remove snap-in".
- A database in the snap-in must be created by selecting "Administrative Tools", "Security Console", select "Action", and "Open database".
- To perform the analysis against a template, open a database, then select "Action", and "Analyze Computer Now".
- To apply settings from a template, open a database that has the settings you want to apply to the computer, then select "Action", and "Configure Computer Now".

Secedit Command Line Tool

It is used to perform computer security configuration and analysis. For help type "secedit /?" on the command line

Windows 2000 User Profiles

The user's profile allows the user's environment to be configured. The User Manager administration tool allows user profiles to be modified when "user properties", then "profile" are selected. The user profile contains:

- Desktop settings - screen colors, wallpaper, screen saver
- Persistent network and printer connections
- Mouse settings and cursor settings
- Recently edited documents.
- Start-up programs, shortcuts, and personal groups
- Settings for Windows applications - Notepad, Paint, Windows Explorer, Calculator, Clock, and more.
- Start menu settings - Programs that can be selected from the start menu.

The user profile settings are saved on disk. They are loaded when the user logs on. There are two profile types:

- **Local profile** - Stored in the C:\Documents and Settings\username folder. The profiles file is NTUSER.DAT in the directory called by the user's name. A mandatory profile which discards any changes the user makes to their profile at logoff time, can be implemented by modifying the name of the user profile file from NTUSER.DAT to NTUSER.MAN. The ntuser.ini file is used to set up the user roaming profile components that are not copied to the server. The ntuser.dat.LOG file is used for NTUSER.DAT file recovery in the case of an error. Additional folders in the C:\Documents and Settings \username folder are:
  - Application Data - Refers to data used by application programs that the user may modify when they change a setting in the application.
  - Cookies
  - Desktop - Refers to desktop and briefcase shortcuts.
  - Favorites - Application favorites such as web site favorites on IE and favorite programs.
  - FrontPageTempdir - Only on Windows 2000 Servers for files made by Microsoft FrontPage
  - Local Settings - Settings used by common applications such as IE.
  - My Documents
  - NetHood - Network servers or shared network folder shortcuts.
  - PrintHood - Network printers.
  - Recent - Shortcuts to documents recently used.
  - SendTo - Shortcuts to places where files are copied.
  - Start Menu - The user's start menu and shortcuts.

    - Templates - Application templates.
- **Roaming** - Stored on an NT server and downloaded to the computer that the user logs onto. This way the same user's profile can be available on any machine.

Profile Creation

- For local users - If no user profile exists when the user logs on, the contents of the Default User profile folder are copied to the C:\Documents and Settings\username folder.
- For domain users - The NETLOGON share on the domain controller is checked for a default user profile. If one does not exist, it copies the contents of the local Default User profile folder to the local computer NETLOGON\username directory.

The default user settings are used to create a new user's profile when the new user logs on the first time. The administrator may modify the contents of the Default User profile directory to change the settings for first time users of the system. The **Control Panel, System applet is used to copy user profiles**. The "User Profiles" tab is used. The System applet is also used to delete user profiles. Shortcuts may be added to the Default User profile directory using Windows Explorer.

All Users Profile

Administrators may install applications and place shortcuts in the All Users Profile directory. All users will have access to these shortcuts and applications. These applications appear on users' desktops. The All Users Profile is not available on a domain wide basis.

Roaming Profiles

Roaming and local profiles may be mandatory which will not allow the user to modify them. Roaming profiles are profiles that have been placed on a central server. When the user logs onto the domain, the roaming profile is copied to the local computer the user logged on from. If the user makes changes to the profile, they are saved to the local computer and the central server. When the user logs on from another computer the most recent of the local or server stored profile is used. If a user's profile is a mandatory profile and that profile is not available when the user attempts to log on, the logon attempt will fail.

To create a roaming user profile:

1. Create a shared directory on a domain controller computer or server.
2. Assign a profile path to the shared directory on domain user accounts. This is done on a domain controller from the "Active Directory Users and Computers" tool.

1. Click + next to the domain the user is in.
2. Highlight the Users folder.
3. Right click the user's account and select properties.
4. Set the path in the Profile path text window.

On a local computer the user profile path is set using the Computer Mnangement Dialog box which is activated by right clicking on "My Computer" and selecting "Manage"

If a user is deleted, the user profile should first be deleted by using the "User Profile" tab of the User Manager.

On Windows NT servers, the System Policy Editor is used to control user profile settings. The authenticating domain controller gets system policies from the file WINNT40\SYSTEM32\REPL \IMPORT\SCRIPTS\NTCONFIG.POL. Therefore to have policies replicated to all domain controllers, place the NTCONFIG.POL file in the directory WINNT40\SYSTEM32\REPL \EXPORT\SCRIPTS.

Roaming profiles can be configured between workstations by setting up a user profile in a shared directory that is accessible to all workstations the user will log on from. Then on each workstation, the user will log in from, the UNC path to the profile file must be set. This is done from the User Manager, "select "User Properties" for the user, then "Profile", then enter in the UNC path in the "User Profile Path" text box.

Windows 2000 Policies

Types of Policies

- **Account policy** - Determines how passwords are validated and how unsuccessful login attempts are handled. Account policies can be set for Organizational Units, domain, domain controllers, and local computers. Three types of account policies:
  - Password policy - Determines how often the user must change passwords and various password requirements.
  - Account lockout policy - Determines when accounts are locked when failed logon attempts occur.
  - Kerberos policy - Windows 2000 domain controller computers are key distribution centers (KDC) for the Kerberos security protocol which us used for authentication.
- **User Rights policy** - Determines what users and groups can perform specific actions on the system.
- **Audit policy** - Determines the amount and type of security logging that Windows NT performs.
- **System policy** - Helps Administrators manage users that are using Windows 95, 98, or NTcomputers. It can be used to provide a uniform environment for large numbers of users.
  - User System Policy
    - Individual User Policy
    - Default User Policy - Applies to users without individual user policies. There are initally no restrictions to this policy. The policy overwrites the Windows registry HKEY_CURRENT_USER section.
  - Group system Policy
  - Computer system Policy
    - Individual Computer system Policy
    - Default Computer system Policy
- **Group policy** - This policy, which is new with Windows 2000, applies to all members of the group they are set for, unless the member has an individual policy. Groups are listed by priority in the System Policy Editor's, Group Priority dialog box. When a user is in multiple groups, the highest priority group's policy applies. Applies to only Windows 2000 computers and/or their users, or both. Consists of:
  - Group Policy Object in Active Directory.
  - Files and folders that are created when the group policy object is created.

System Policies

System Policy Priorities

Policy settings may be applied to any computer or user on the domain from the System Policy Editor.

- **Individual User** - HKEY_CURRENT_USER registry portion is modified. Settings for one user are changed.
- **Group** - Policies applied to groups. One group may have a higher profile priority than another, for the case when a user belongs to multiple groups. This is set using the "Options" menu with "Group Priority". If the user does not have an individual policy, this is applied.
- **Default user** - HKEY_CURRENT_USER registry portion is modified. Settings for any domain user that logs on from any computer are changed. If the user does not have an individual policy, this is applied
- **Individual Computer** - (Non Windows 2000 computers) HKEY_LOCAL_MACHINE registry portion is modified. Policies apply to a specific computer.
- **Default computer** - HKEY_LOCAL_MACHINE registry portion is modified. Settings are changed for all domain computers are changed. If the computer does not have an individual computer policy, this is applied

Policy settings are determined by precidence as listed above. For example, user settings override all other group, and default user policies. Group policies override Default user policies. System (computer) policies override user and group policies. Specific computer policy overrides default system policy. **Group policy priority may be specified from the System Policy Editor when a user is a member of multiple groups**.

System Policy Editor

System policy settings for all users on the domain set using the System Policy Editor are merged with local profiles. User logon restrictions are set in the user manager for domains. A policy may be set to automatically log users off during restricted logon hours. To start the System Policy Editor, click "Start", "Run", and type "poledit" in the text box.

The System Policy Editor is available on Windows 2000 Server type systems. Installation of the ADMINPAK will make it available on Windows 2000 Professional computers.

The following policy files are used for the following systems:

- NTCONFIG.POL - For NT
- CONFIG.POL - Windows 95/98

They must be created on the operating system on which they are intended for use. They are not used on Windows 2000.

Account Policies

Account policy and lockout Options

The three main groupings are "Password restrictions", "Account lockout", and "Kerberos". The first four items below are under "Password restrictions"

- Password policy
  - Enforce password history - Determines the number of passwords that must be used before an old password can be reused.
  - Maximum password age - If 0, passwords never need to be changed.
  - Minimum password age - If 0, passwords can be changed whenever the users want to. This can prevent users recycling back to their original password.
  - Minimum password length - Values are 0 to 14 characters. Of 0, passwords are not required.
  - Passwords must meet complexity requirements - Uppercase, lowercase, numeric, and special characters may be required.
  - Store password using reversible encryption for all users - One way encryption is more secure, and reversible encryption is used for users on Apple computers.
- Account lockout policy
  - Account Lockout Threshold - Number of consecutive unsuccessful logon attempts before the account is locked. If 0, the account is not locked due to bas logon attempts.
  - Account Lockout Duration - Determines how long accounts remain locked. This is "Not Defined" or from 0 to 99,999 minutes. If "Not Defined" user accounts are never locked out. If 0, the account is locked out until the administrator re-enables the account.
  - Reset Acount Lockout After - Specifies how long between bad logon attempts before the account lockout threshold counter is reset. Possible values are "Not Defined" or 1 to 99,999. If "Not Defined" user accounts are never locked out.
- Kerberos policy
  - Enforce user logon restrictions
  - Maximum lifetime for service ticket
  - Maximum lifetime for user ticket
  - Maximum lifetime for user ticket renewal
  - Maximum tolerance for computer clock synchronization

Account policy changes become effective when the user logs off and back on again.

Setting Account Policies

- Organizational Units - In Administrative Tools, select "Active Directory Users and Computers".
- Domain - In Administrative Tools, select "Domain Security Policy". The ADMINPAK must be installed on the computer.
- Domain controllers - In Administrative Tools, select "Domain Controler Security Policy". The ADMINPAK must be installed on the computer.
- Local computers - From the Control Panel, "Administrative Tools" applet, double click "Local Security Policy".

User Rights Policies

- Shutdown the computer from a remote location - Administrators, Power users.
- Access to the computer via the network - Administrators, Power users, everyone
- Use the computer locally - All users
- Backup or restore directories and files - Administrators, backup operators
- Change time - Administrators, Power users.
- Delete or add device drivers - Administrators
- Change the security logging policy - Administrators
- Shut the system down - All users except guests
- Take file ownership - All operators

Audit Policies

The Event Viewer allows viewing of events specified by the audit policy

Auditing must be enabled in the Audit Policy window by checking the "Audit these Events" box from the User Manager. The event viewer allows the following types of event information to be viewed.

- **System** - Logs system errors, driver errors, binding errors, or service failures.
- **Security** - Bad logon attempts.
- **Application**

Each message has an event ID number. A maximum size of logs and writing over of event logs can be set depending on available disk space.

Windows 2000 Group Policies

Group policies are used by administrators to configure and control user environment settings. Group Policy Objects (GPOs) are used to configure group policies which are applied to sites, domains, and organizational units (OUs). Group policy may be blocked or set so it cannot be overridden. The default is for subobjects to inherit the policy of their parents. There is a maximum of 1000 applicable group policies.

Group policies are linked to domains, organizational units, or sites in Active Directory. A policy **must be linked to a container object** in Active Directory to be effective. They are stored in any domain for storage but can be linked to other domains to make them effective there also. The policy must be linked to the container (site, domain, or OU) that it is stored in to be effective in that container. One policy object can be linked to sveral containers. Several policy objects can be linked to one container.

Group Policy Settings

Group policy settings only work for Windows 2000 computers. Settings that do the following may be applied with group policy:

- Manage user environments - Wallpaper and other settings.
- Manage scripts - Logon/logoff and startup/shutdown scripts.
- Manage security - Event log settings, account policies, and more.
- Manage software deployment - Applications may be automatically installed when the client computer starts.
- Redirect folders - Folders on a local computer may be redirected to a network share.

Group Policy Types

Group policy types and their order of application are:

- Local Policy
- Site Linked Policies
- Domain Linked Policies
- Organizational Unit Policies

Group policy may be set using Active Directory globally or or using Local Group Policy on local computers. The files are stored:

- Locally - SystemRoot\System32\GroupPolicy\

- Globally - SystemRoot\SYSVOL\sysvol\domainname\Policies\ on domain controllers. The global group policy is made of a Group Policy Object (GPO) which is an Active Directory object and the files in this directory.

The GPT.INI file contains information about the policy. Group policy templates are in the system volume\public directory.

Group Policy Priorities

Group policy is inherited by children objects of parents. If a parent object has group policy, then the children have the same policy. Group policies are applied down from the higher level objects to the lower level objects. The policies are cumulative unless they conflict, in which case the lower level policy applies to the object.

1. Local or Roaming Individual user profile is applied. Local policies cannot be blocked.
2. Local Group Policy is applied. Conflicts with individual policy are overridden by local group policy.
3. Group Policy is applied. Conflicts with individual policy or local group policy are overridden by group policy. The group policies are processed in the following order based on the object they are linked to:
    1. Sites
    2. Domains
    3. Organizational Units

Policies normal behavior can be modified with the following settings:

- No Override - Normally the local policies or lower level policies will take presidence. If this setting is made on a higher level policy, the lower level policy cannot modify it and the policy associated with this setting will take precidence.
- Block Policy - Group Policy Objects (GPOs) are entirely blocked or applied. The No Override option takes priority over the Block Policy option.

Policy application steps:

1. When the computer is turned on, all group policies that are applicable to the computer are applied.
2. Any group policy startup scripts are run.
3. At user logon, after the user profile is set, all group policies for that user are applied.
4. Any group logon scripts are run, then any individual logon scripts are run.
5. At user logoff, group logoff scripts are run.
6. At system shutdown, any group policy shutdown scripts associated with the computer are run.

Group policy is updated by active directory to domain controllers every 5 minutes and to all Windows 2000 computers that are not domain controllers every 90 minutes. These updates are requested by the computer and the intervals may be modified by administrators.

Setting Group Policy

The creator of a policy and administrators have Full Control permission for policies. To set Group Policy, the user must have permission to Log on Locally on a domain controller

Group policies can be set from any domain controller, but the one that is the best to use is the PDC Emulator domain controller.

All group policy object containers have a default policy. Group policies can be managed using the Group Policy Editor. There are two default policy nodes:

- Computer configuration - Settings are applied to the computer and the user on the computer does not affect the settings.
- User configuration

Both nodes contain three sections for various settings which are:

- **Administrative templates** - Additional confuguration for computer and user settings.
- **Software settings** - Applications can be assigned to computers or users. The application can be run by the user or on the computer on which they are assigned. Either a stub for the application or the application is installed.
- **Windows settings** - The behavior of the operating system may be customized here.

The Microsoft Management Console (MMC) Group Policy snap-in is used to set local group policy. To start it, select "Start", "Run", and type "gpedit.msc". It also allows configuration of local Security Policies that may be set using the "Local Security Policy" Administrative Tool. The Group Policy snap-in on a remote computer may be used to set local Group Policies also. The following Local Group Policy settings are possible:

- Computer Configuration - Applies to specific computers
    - Software Settings - Applications can be assigned to computers or users. The application can be run by the user or on the computer on which they are assigned. Either a stub for the application or the application is installed.
    - Windows Settings - Used to manage startup and shutdown scripts.
        - Scripts (Startup/Shutdown)
        - Security Settings
            - Account Policies - Password and account lockout policy.

        - Account lockout policy - Set the reset interval between logon attempts. Set the failed logon counter reset interval. Set the duration of the lockout.
        - Password policy - Number of passwords remembered that can't be repeated. Maximum pasword age (42 default). Minimum password length.
        - Kerberos policy - Set lifetime of service tickets.
      - Local Policies - Audit, User rights, security options.
        - Audit policy - These may include Logon and logoff, File and object access, Use of user rights, User and group management, Security policy changes, System shutdown and restart, and Process Tracking.
        - User rights - Determines actions that a user can perform such as shutting the system down, change time, use the computer locally, and others.
        - Security options - Must be enabled by an administrator. Restricted groups are used to help automate group management. A user can be added to a restricted group temporarily and that user will be removed during the next security audit.
      - Event Log - Application, Security, and System log settings.
      - Restricted Groups - Can be sure certain group memberships are not modified locally.
      - System Services - Set services to automatic, manual, or disabled.
      - Registry - Registry settings to be affected by this group policy. Permissions for registry keys may set up here.
      - File system - Security settings for files and directories on several computers can be set along with file system extension associations with applications.
      - Public Key Policies - Encrypted Data Recovery Agents, Automatic Certificate Request Settings, Trusted Root Certificate Authorities, and Enterprise Trust.
    - IP Security Policies on Active Directory - Rules for secure servers, servers, and clients. These rules control whether information sent between clients and the server is encyrpted or secure. These are the default policies:
      - Client policy - Most communication is not secure (encrypted) but the client may request and get a secure channel.
      - Secured server policy - Only secure communication is attempted.
      - Server policy - The server attempts to use a secure channel, but if the client does not respond through the secure channel, an unsecure channel will be used.
  - Administrative Templates - Can be used to manage a user's environment. More templates may be added for applications by creating a unicode file (usually

provided by the application creator) with the ".adm" extension. The .adm file causes the HKEY_LOCAL_MACHINE registry key to be changed.
        - Windows Components - Can configure the user's ability to use specific Windows programs or certain functions in those programs. Those programs include Internet Explorer, Task Scheduler, Windows Installer, and NetMeeting.
        - System - Settings for:
            - Disk quotas - Levels of warnings and hard limits may be set.
            - DNS clients - The DNS suffix may be set.
            - Group policy
            - Logon - Scripts at startup or shutdown may be configured to run.
            - Windows file protection - System files may be scanned.
        - Network - Can configure access to offline files and limit the user's ability to configure connection sharing.
        - Printers - Policies may allow local printers to be published in Active directory.
- User Configuration - Applies to specific users.
    - Software Settings - Applications can be assigned to computers or users. The application can be run by the user or on the computer on which they are assigned. Either a stub for the application or the application is installed.
    - Windows Settings - Used to manage logon, and logoff scripts. It is best to manage these scripts here rather than by configuring user account properties.
        - Internet Explorer maintenance. - Settings:
            - Browser user interface settings
            - Connection settings
            - URLs section
            - Security zones
            - Programs settings
        - Scripts - Used for user configuration are used during logon and/or logoff.
        - Security Settings - Public key policies.
        - Remote Installation Service
        - Folder Redirection - Determines where users can get specific types of files. It is based on user groups or specific folders.
    - Administrative Templates - Can be used to manage group policy options. More templates may be added for applications by creating a unicode file (usually provided by the application creator) with the ".adm" extension. The .adm file causes the HKEY_CURRENT_USER registry key to be changed.
    - Windows Components - Can configure the user's ability to use specific Windows programs or certain functions in those programs. Those programs include:
        - Internet Explorer
        - Task Scheduler
        - Windows Installer
        - NetMeeting

        - Windows Explorer - Menu items may be disabled or removed.
        - Microsoft Management Console.
    - System - The configuration may be set so the user cannot change their password or logoff. The group policy refresh interval is configured here.
        - Logon/logoff settings - Logon and logoff scripts may be hidden so the user is unaware that they are run. Part of the Task Manager or its entirety may be disabled.
        - Group policy settings
    - Network - Can configure access to offline files and limit the user's ability to configure connection sharing.
    - Start Menu and Taskbar - Can remove some options.
    - Desktop - Desktop icons may be hidden.
    - Control Panel - Configure the user's ability to use the control panel and specific features. Specific applets or the entire control panel may be hidden.

Creating Group Policy Objects

There are several tools used to create and manage group policy objects. The most appropriate tool to use depends on the level the group policy object is at. The tools are as follows:

- Active Directory Sites and Services Administrative tool - Used to create and manage **Group Policy Objects (GPOs)** that are associated with a site.
- Active Directory Users and Computers Administrative tool - Used to create Group Policy Objects (GPOs) that are associated with an OU or domain.
- MMC Group Policy snap-in - This tool, also called the "Group Policy Console" can be used to manage GPOs at any level.

Setting Group Policy

The Microsoft Management Console (MMC) Group Policy snap-in can be used to create and manage Group Policy objects if the user has the correct permissions. Enterprise Admins, Domain Admins groups and domain Administrators have correct permissions.

Group Policy inheritance is configured on the Active Directory container the GPO is in and on the object itself.

- There is a "Block Policy Inheritance" checkbox in the Group Policy Tab on the object container's properties dialog box.
- There is a "No Override: prevents..." checkbox in the Group Policy Tab on the object's properties dialog box.

In the case of a conflict between the two above settings, the "No Override: prevents..."

checkbox option prevails. If this option is set on a parent container, the child cannot override the inheritance.

GPO Security

GPO security is used to specify the users and groups that can modify the GPO settings and to specify those to whom they apply as follows:

- The Group Policy settings apply to users and groups that have the Active Directory read and apply group policy permissions to the GPO. Authenticated Users have these settings apply by default.
- Users or groups that have the Active Directory read and write permissions to the GPO can modify the GPO settings.

The Object's or container's properties dialog box (Select "Action", "Properties") group policy tab, GPO's security tab is where the security settings are modified. This is done in the Administrative Tool "Active Directory Sites and Services" or "Active Directory Users and Computers". This allows policies to be set, or "filtered" so they only affect specific users or groups. When these permissions for the group policy objects are modified, the Discretionary Access Control List (DACL) for the policy object is modified. The DACL must permit the groups that the policy is for to have both "Read" and "Apply Group Policy" permission.

Linking GPOs

A GPO may be linked to another container. When this is done a new GPO, pointing to the original GPO, is created. The GPO settings of the original GPO apply to all objects it is linked to. At this point the new GPO may be modified and the new settings will apply only to the new GPO. If settings in the original GPO are modified, the settings in the linked GPOs will also be changed.

Group Policy Application Order

Groups are listed by priority in the System Policy Editor dialog box, Group Priority tab. When a user is in multiple groups, the highest priority group's policy applies. The groups may be moved up and down the list which sets their relative priorities..

Using Group Policy for Software Deployment

Methods:

- Assign the application to a computer - The application shortcut appears in the user start

menu, and the application is installed the first time the user runs it..]

- Assign the application to a user - The application is installed the next time the computer is booted.
- Publish the application to the user - The application is installed the first time the user opens a document that is associated with the application. Once installed, the start menu lists the application.

Installation steps:

1. Prepare application for deployment if it is not in a Windows installer file (ending with .msi). Do one of:
    - Convert the file to a Windows installer file.
        1. Use WinINSTALL LE to repackage the application as a Windows installer file. This program is on the Windows 2000 Server CD in \VALUEADD \3RDPARTY\WINSTLE.
    - Create application installation instructions in a text file ending with ".zap". These applications can only be published. Two sections of .zap file:
        - {Application] - Give "FriendlyName = " and "SetupCommand =" on two separate lines followed by the appropriate information.
        - [Ext] - List extensions to be associated with the application on separate lines followed by "=".

Group policies can also be used to:

- Deploy service packs
- Create application categories
- Maintain or upgrade software
- Remove previously deployed applications.

Policy Refresh Intervals

The default refresh interval for policies is 90 minutes. The default refresh interval for domain controllers is 5 minutes. Group policy object's group policy refresh intervals may be changed in the group policy object. The appropriate refresh interval depends on link speed. A slow network should have longer refresh intervals. A slow link is defined as one slower than 500Kbps.

Misc

- Advanced Power Management is supported by windows 2000 Professional but is not support by Windows 2000 Server.
- To change the workgroup of a Windows 2000 Professional computer use the System tool.
- To configure a hardware profile, use the System tool.
- Use windows explorer to configure synchronization settings for offline files
- The System tool is used to manage paging files
- To search for a specific shared folder in AD, use Active Directory Users and computers. Windows explorer cannot search for a specific shared folder.
- To connect two computers using infared ports, configure one to accept incoming connections and the other computer to connect directly to the first.
- The "Services" tool is used to configure a service to log on using a specific user account.
- Is EFS covered? To do EFS recovery the user must be designated an EFS recovery agent in Group policy and have an EFS Recover Agent certificate.
- Windows 2000 deployment tools are located on the installation CD at \SUPPORT \TOOLS. The tools are in "deploy.cab".
- Where is Task Manager Covered? In Processes
- Unicode - A method of coding characters that supports foreign language character sets.

Windows 2000 Terms

- ACE - Access Control Entry - Part of an ACL which specifies a users access to specific objects.
- ACL - Access Control List is a database of permissions for an object or file which determines who can access an object and how much access is allowed.
- AD - Active Directory
- API - Application programming interface
- APM - Advanced Power Management for mobile computers.
- ATM - Asynchronout Transfer Mode.
- BDC - Backup Domain Controller provides failure backup for a PDC and keeps the replicated SAM database.
- BINL - Boot Information Negociation Layer is used to be sure the installation using RIS is being done on the correct computer.
- CD - Compact disk.
- CDFS - Compact Disk File System supports compact disks (CDs).
- Child domain - Domain below another in a domain tree. Example: "child.parent.root.com".
- DACL - Discretionary Access Control List - Contains security principle SIDS that have permission for an object.
- DDNS- Dynamic Domain Name Service allows for Dynamic updates to DNS information.
- DFS - Distributed file system allows administrators to make shares on several different servers appear to be on one share on one server..
- DN - Distinguished Name is a RDN with the location of the object in Active Directory.
- DNS - Domain Name Ssystem is a service and database used to convert between human readable names and IP addresses of computers.
- Domain - A domain is used to manage a large group of computers. It is used to control resource access for users. The term domain as used with Windows systems is not the same as an internet domain as used with DNS.
- Domain tree - A hierarchial group of one or more domains with one root domain
- DOS - Disk Operating System is the original system used when IBM variety personal computers were introduced around 1980.
- DVD - Digital Video Disks.
- Explicit trust - A trust that an administrator creates.
- EFS - Encrypting File System supports file encryption.
- FAT32 filesystem - A file allocation table operating system that supports larger disk partition size than older FAT filesystems. It uses 32 bits to point to clusters rather than 16 or 24 bits.
- Forest - The set of all domains in an organization's network.
- FQDN - Fully Qualified Domain Name used on the internet such as "myserver.myorganization.org". The maximum length is 63 characters.

- FRS - File replication service (FRS) is used to replicate the SYSVOL share.
- FSMO - Flexible Single Master Operations are operations that are done on a domain which can only be done on a single controller.
- GCS - Global catalog server.
- Global Catalog - A searchable master index with data about all objects in a forest. When the first domain controller in the forest is established, a default catalog is created automatically on that controller.
- GPO - Group policy object.
- GUID - Globally Unique Identifier which is a 128 bit number.
- HAL - Hardware abstraction layer.
- HCL - Hardware Compatibility List is a list of hardware that is compatible with Windows NT and Windows 2000.
- HPFS - High Performance File System used with older Windows NT and OS/2 operating systems.
- IE - Internet Explorer is the web browser from Microsoft.
- IIS - Internet Information Server.
- Intransitive trust - A one way trust that does not extend beyond two domains.
- IPP - Internet Printing Protocol (IPP) is used to support printing from Internet Explorer across the internet.
- IPSEC - Internet security protocol.
- IrDA - Infared Data Association sets standards for infared/wireless devices.
- KDC - Kerberos Domain Controller used for Kerveros authentication.
- LDAP - Lightweight Directory Application Protocol.
- Mixed mode - When Active Directory interfaces with NT 4.0 BDCs or ones without Windows 2000 Directory Service client software. In mixed mode, computers without Windows 2000 client software must contact the PDC emulator to change user account information.
- MMC - Microsoft Management Console
- Native mode - Active Directory interfaces only with Windows 2000 domain controllers and directory service client software. In this case, the PDC emulator will get password changes faster.
- NLB - Network Load balancing
- NTLN - NT Lanman authentication
- One way trust - When one domain allows access to users on another domain, but the other domain does not allow access to users on the first domain.
- OU - Organizational unit - An Active Directory container object that contains other organizational units or objects.
- OS/2
- OSPF - Open shortest path first is a dynamic routing protocol that takes less bandwidth than RIP.
- Parent domain - Domain above another in a domain tree.
- PDA - Personal digital assistant.
- PDC - Primary Domain Controller required for a Windows NT domain to operate. The

PDC (primary domain controller) is used to store and administer the master SAM database.

- PKI - Public Key Infrastructure applications are applications that use security keys to authenticate users. These applications may be used for purposes of getting e-mail, generating user signatures, and logging onto networks.
- POSIX
- PXE - Preboot eXecution Environment.
- RADIUS - Remote Authentication Dial-In User Service
- RDN - Relative Distinguished Name is assigned by an administrator to an object.
- RIP - Routing Information Protocol is a dynamic routing protocol.
- RIPrep - Remote Installation Preparation Wizard
- RIS - Remote Installation Services
- RPC - Remote Procedure Call is normally used to replicate data between domain controllers.
- SACL - Security Access Control List - Defines auditable events for specific objects.
- SAM - Security Accounts Manager.
- Schema - A formal definition (set of rules) which govern a database structure and types of objects and attributes which can be contained in the database.
- Security principal objects - Users, groups and computers.
- SID - Security Identifier. It is created by the Windows 2000 security subsystem and is assigned to users, groups, and computers.
- SIS - Single Instance Store is used to reduce storage space for installation images on the server by using links to files that are the same in various images.
- Site - Groupings of machines based on a subnet of TCP/IP addresses. An administrator determines what a site is. Sites may contain multiple subnets. There can be several domains in a site.
- SMS - Systems Management Server.
- SQL - Structured Query Language.
- TFTP - Trivial File Transfer Protocol is used to send files to the client when they are requested. There is no logon with TFTP services.
- Transitive trust - A trust which can extend beyond two domains to other trusted domains in the tree.
- Trusted domain - The domain that is trusted, whose users have access to the trusting domain.
- Trusting domain - The domain that allows access to users on another domain.
- Trust relationship - A description of the user access between two domains consisting of a one way and a two way trust.
- TSR - Terminate and stay resident function allows a program to stay in memory until activated by some event.
- Two way trust - When two domains allow access to users on the other domain.
- UDF - Universal Disk Format supports DVDs.
- Unicode - A method of coding characters that supports foreign language character sets.
- Universal group - May contain users and groups from any domain in a forest.

- UPN - User Principal Name is an RDN with a FQDN which is used for email and user logon.
- URL - Universal Resoruce Locator is a standard convention that is used to locate resources on the internet or networks. Its format is "protocol://www.domain.root/directory/file".
- VDD - Virtual device drivers.
- VDM - Virtual DOS Machine.
- WBEM - Web Based Enterprise Management from the Desktop Management Task Force is a standard for collecting data for desktop management.
- WFW - Windows for Workgroups was an enhancement to the Windows 3.1 version with networking support. It ran 16 bit applications.
- WIN16 - Windows versions that ran 16 bit applications such as Windows 3.1 and WFW.
- WMI - Windows Management Instrumentation helps administrators know about vendor hardware and applications. It is based on WBEM.
- Workgroup - A workgroup is used to manage groups of less than ten computers.
- WOW - Windows on Windows which refers to the Windows 16 bit applications running on the Windows 32 bit environment.

The CTDP Windows 2000 Guide Credits

This document was produced for the Computer Technology Documentation Project and the latest version is available at http://www.comptechdoc.org/os/windows/win2k/.

Document:

The CTDP Windows 2000 Guide Version 0.6.1

Author:

Mark Allen

Those who contributed by submitting comments:

- **Stephen Wilson**