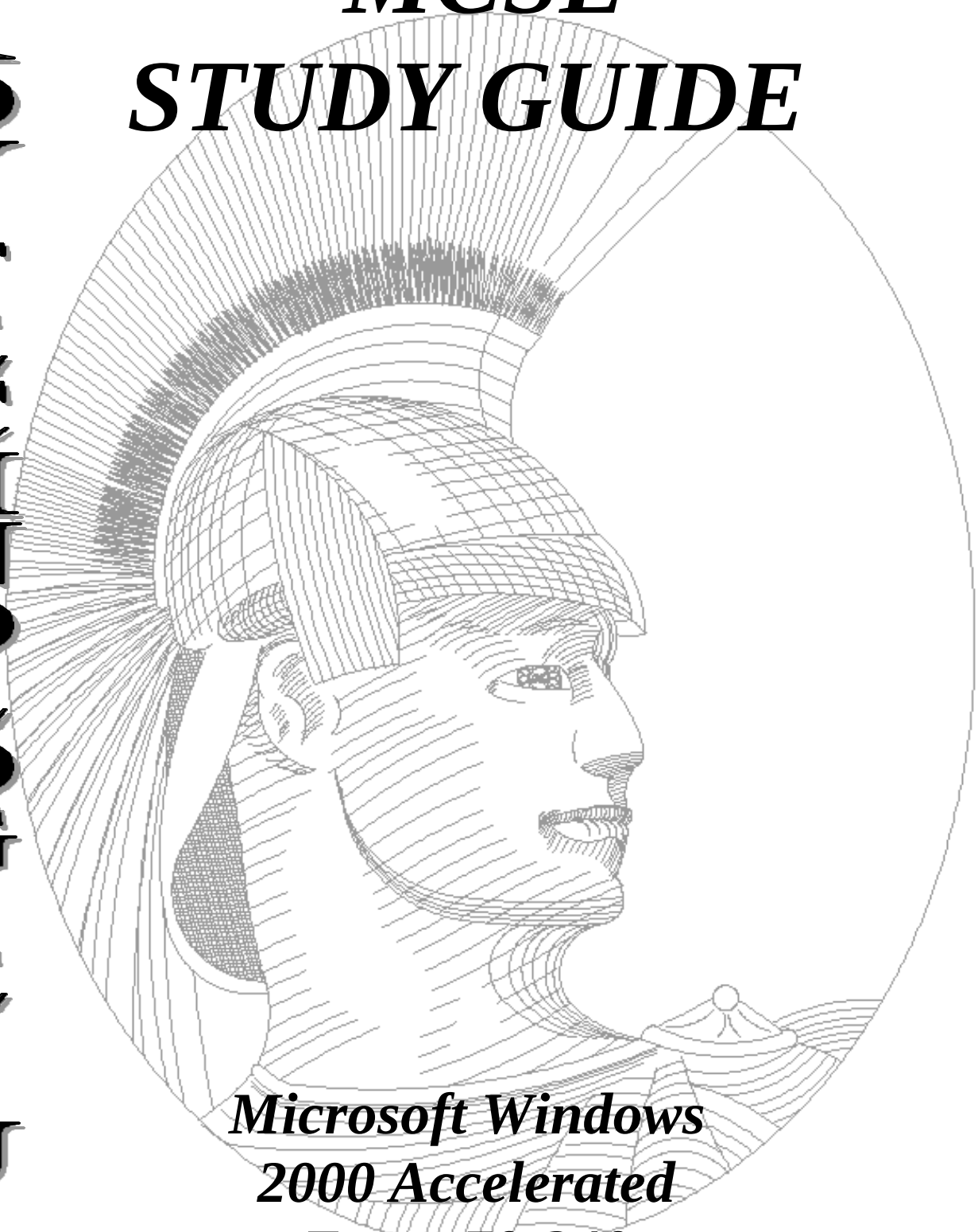
TROY TECHNOLOGIES USA

MCSE STUDY GUIDE



Microsoft Windows 2000 Accelerated Exam 70-240

Edition 1

Congratulations!!

You have purchased a ***Troy Technologies USA*** Study Guide.

This study guide is a selection of questions and answers similar to the ones you will find on the official Microsoft Windows 2000 Accelerated MCSE exam. Study and memorize the following concepts, questions and answers for approximately 40 to 50 hours and you will be prepared to take the exams. We guarantee it!

Remember, average study time is 40 to 50 hours and then you are ready!!!

GOOD LUCK!

Guarantee

If you use this study guide correctly and still fail the 70-240 exam, send your official score notice and mailing address to:

Troy Technologies USA
8200 Pat Booker Rd. #368
San Antonio, TX 78233

We will gladly refund the cost of this study guide. However, you will not need this guarantee if you follow the above instructions.

Until December 31, 2001, individuals who have passed the three Windows NT 4.0 exams have the option of fulfilling part of the core exam requirement by passing Exam 70-240: Microsoft Windows 2000 Accelerated Exam for MCPs Certified on Microsoft Windows NT 4.0 instead of four of the core exams in the Windows 2000 track.

Exam 70-240 is a four-hour exam. This exam may include adaptive testing technology and simulation items. Microsoft does not identify the format in which exams are presented. Exam 70-240 includes more items than a traditional exam but less than the combined total for those four core exams. Fewer items are required because exam 70-240 makes use of critically important items, takes advantage of the overlap in objectives for the four core exams, and is designed with the knowledge that candidates who have passed the three Windows NT 4.0 exams (70-067, 70-068, and 70-073) have demonstrated some of the skills tested by the core Windows 2000 exams. The test consists of four distinct sections which are clearly defined as Windows 2000 Professional, Windows 2000 Server, Network Infrastructure, and Directory Services Infrastructure. Each section is timed, and students are allowed to review questions and answers for that section, only while they are in the section. Once a student ends a section of the exam, they cannot review items for that section. There are approximately 20-30 questions in each section, with 97 total questions given.

The Windows 2000 "accelerated" exam measures all of the skills measured by the following exams:

- Exam 70-210: Installing, Configuring and Administering Microsoft Windows 2000 Professional tests the skills required to install, configure and administer Windows 2000 Professional as a desktop operating system in a generic network operating environment.
- Exam 70-215: Installing, Configuring and Administering Microsoft Windows 2000 Server tests the skills required to install and configure Windows 2000 Server to participate as a member server of a domain in an Active Directory environment.
- Exam 70-216: Implementing and Administering a Microsoft Windows 2000 Network Infrastructure tests the skills required to install, configure, manage, monitor, and troubleshoot DNS in a Windows 2000 network infrastructure, DHCP in a Windows 2000 network infrastructure, remote access in a Windows 2000 network infrastructure, network protocols (such as TCP/IP), IP routing, connection sharing, and security.
- Exam 70-217: Implementing and Administering a Microsoft Windows 2000 Directory Services Infrastructure tests the skills required to install, configure, and troubleshoot Active Directory, DNS for Active Directory, change and configuration management including RIS and Group Policy, and Active Directory Security solutions.

To request a free voucher to take the accelerated exam, visit http://www.microsoft.com/trainingandservices/default.asp. Only candidates who have passed all three Windows NT 4.0 exams are eligible to request one free voucher to take exam 70-240.

Your score report will only indicate whether you passed or failed.

IMPORTANT

This exam is basically made up of questions from the 4 individual Windows 2000 core exams. You will notice that this folder contains four separate pamphlets. One for each core subject (70-210, 70-215, 70-216 and 70-217). Although it is true that you could probably use these individual sections to prepare for and pass the individual core exams, we do not guarantee this study guide for that purpose. The only thing we guarantee is that you will pass the 70-240 exam by using this study guide.

Any time we update one of our individual study guides, we will at the same time update this document. You may want to contact us a couple of days before you actually sit for the Accelerated Exam to ensure you have the most current edition. Be sure to provide us the edition number from the front of this study guide when you make your inquiry. Send all queries to me at garry@troytec.com.

Further Suggested Reading for Microsoft Certified System Engineer

- Exam Cram, MCSE Windows 2000 Network: Exam 70-216 (Exam Cram) by Hank Carbeck, et al. Paperback (September 28, 2000)
- MCSE Windows 2000 Accelerated Study Guide (Exam 70-240) (Book/CD-ROM package) by Tom Shinder (Editor), et al. Hardcover (October 6, 2000)
- MCSE 2000 JumpStart: Computer and Network Basics by Lisa Donald, et al. Paperback (April 2000)
- MCSE: Windows 2000 Network Infrastructure Administration Exam Notes by John William Jenkins, et al. Paperback (September 19, 2000)
- Public Key Infrastructure Essentials: A Wiley Tech Brief - Tom Austin, et al; Paperback
- Planning for PKI: Best Practices Guide for Deploying Public Key Infrastructure - Russ Housley, Tim Polk; Hardcover
- Digital Certificates: Applied Internet Security - Jalal Feghhi, et al; Paperback
- Ipsec: The New Security Standard for the Internet, Intranets, and Virtual Private Networks - Naganand Doraswamy, Dan Harkins; Hardcover
- A Technical Guide to Ipsec Virtual Private Networks - Jim S. Tiller, James S. Tiller; Hardcover
- Big Book of IPsec RFCs: Internet Security Architecture - Pete Loshin (Compiler); Paperback
- MCSE Windows 2000 Core 4 for Dummies: Exam 70-210, Exam 70-215, Exam 70-216, Exam 70-217

Table of Contents

Installing, Configuring and Administering Microsoft Windows 2000 Professional Concepts

Installing Windows 2000 Professional

Requirements:

(http://www.microsoft.com/windows2000/upgrade/upgradereqs/default.asp)

Windows 2000 Professional

133 MHz or higher Pentium-compatible CPU.
64 MB RAM minimum. 4 GB RAM maximum
2 GB hard disk with a minimum of 650 MB of free space. (Additional free hard disk space is required if you are installing over a network.)
Network Adapter Card
Video display adapter and monitor with VGA or higher resolution
Support for up to 2 processors.

Windows 2000 Server

133 MHz or higher Pentium-compatible CPU.
128 MB RAM minimum (4GB Maximum) 256 min recommended.
2 GB hard disk with a minimum of 1 GB of free space. (Additional free hard disk space is required if you are installing over a network.)
Network Adapter Card
Video display adapter and monitor with VGA or higher resolution
Support for up to 4 processors.

Windows 2000 Advanced Server

133 MHz or higher Pentium-compatible CPU.
128 MB RAM minimum (8GB Maximum) 256 min recommended.
2 GB hard disk with a minimum of 1 GB of free space. (Additional free hard disk space is required if you are installing over a network.)
Network Adapter Card
Video display adapter and monitor with VGA or higher resolution
Support for up to 8 processors.

Pre-Installation Activities:

Prior to installing Win2000, the following tasks must be performed:

- Ensure all hardware requirements are met.
- Determine if hardware is on the Hardware Compatibility List (HCL).
- Determine how you want to partition the hard disk where Win2000 will be installed.
- Choose a file system for the installation partition.

- Choose a licensing mode for a server that will be running Win2000.
- Identify whether the computer will join a domain or a workgroup.
- Run the Win2000 Upgrade Compatibility Verification tool.

Attended Installation:

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

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

Installing from CD-ROM:

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

Installing over a Network:

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

WINNT.EXE command line switches

Switch	Function
/a	Enables accessibility options.
/e:*command*	Specifies the command to b executed at the end of GUI setup.
/i:*inffile*	Specifies the file name (no path) of the setup information file. Default is DOSNET.INF.
/r[:folder]	Specifies optional folder to be installed.

/rx[:folder]	Specifies optional folder to be copied.
/s[:sourcepath]	Specifies source location of Windows 2000 files. Full path or network share.
/t[:tempdrive]	Specifies drive to hold temporary setup files.
/u[:answer file]	Specifies unattended setup using answer file (requires /s).
/udf:*id*[,UDF_*file*]	Establishes ID that Setup uses to specify how a UDF file modifies an answer file.

Unattended installations:

- Unattended installations use an answer file to provide information during the setup process.
- Answer files are created using the Setup Manager Wizard or a text editor.

Domains, Trusts and AD

Active Directory

Active Directory is a hierarchical database of all objects in the entire enterprise. It includes users, groups, domain controllers, printers, computers, contacts, shared folders, and organizational units. AD uses TCP/IP as its network protocol. All Win2000 computers can use AD by default. Non-Win2000 computers can still log onto the domain, but cannot use AD features. They must use a Directory Services add-on client (DSCLIENT.EXE).

Domains

Domains are now a hierarchical model with a parent domain and child domains under it. A single domain tree consists of a parent domain and all of its child domains. Multiple trees in the same AD are called a forest. Domains are named in accordance with the Internet's Domain Name System standard. If the parent (root) domain is called "troytec.com", a child may be called "support.troytec.com".

Global Catalog

To facilitate finding objects in the AD, the Global Catalog is used. It is an index of all objects published in the AD. A Global Catalog can only exist on a domain controller.

Forest

A Forest defines the outside perimeter of the Windows 2000 Active Directory. It is also called an enterprise. Within the forest are trees, and within the trees are domains.

Organizational Units

OUs are sub-domains that contain AD objects. They are groups by similar function or geographical locations. They exist to delegate administrative authority and to group policy application.

Deploying Windows 2000 Using Remote Installation Services (RIS):

Allows administrators to install Win2000 Professional on client computers from a central location. RIS server can be a domain controller or a member server.

RIS Server requirements:

- DNS Server Service
- DHCP Server Service
- Active Directory
- Minimum of 2 GB of disk space. Two hard disk partitions for the Operating System and for the images. Image partition must be formatted with NTFS. RIS cannot be installed on the system, boot partition, or on an EFS volume or DFS shared folder.

Setting up RIS Server:

- Install Remote Installation Services by using Windows Control Panel, Add/Remove Programs, Windows Components.
- Start the RIS Setup Wizard by running RISETUP. Specify the Remote Installation Folder Location. To build the initial CD-based image, specify the location of the Win2000 Professional source files. Inside the RIS folder, indicate where the CD image will be stored. Provide a friendly text name for the CD-based image.
- Setup Wizard will then create the folder structure, copy source files to the server, create the CD-based Win2000 Professional image and the default answer file, **RISTANDARD.SIF**, and start the RIS services on the server.
- To authorize the server, open Administrative Tools, DHCP. Right-click DHCP, choose Manage Authorized Servers. Click Authorize and enter the name or IP of the RIS server.
- Configure your RIS Server to respond to client requests.
- Assign users/groups that will be performing RIS Installations permissions to Create Computer Objects in Active Directory.
- Client Computer Naming Format is defined through Active Directory Users and Computers. Right-click RIS Server and click Properties, Remote Install, Advanced Settings, New Clients. Either choose a pre-defined format or create a custom one.
- Associate an answer file (.SIF) with your image.

RIS Client requirements:

- Must have a network adapter, or a 3 1/2" floppy drive and PCI network adapter supported by the RIS Startup Disk utility's list of supported adapters.
- Client machine must meet minimum hardware requirements for Windows 2000 Professional and must use the same Hardware Abstraction Layer (HAL).

Troubleshooting Remote Installations:

Symptom	Solution
Client cannot connect to RIS Server using the Startup disk	Verify correct network adapter driver in RBFG.EXE.

Computer displays a BootP message but does not display the DHCP message	Verify if it can obtain an IP address. Ensure the DHCP server is online, is authorized, has a valid IP address scope. Ensure DHCP packets are being routed.
Computer displays the DHCP message but does not display the Boot Information Negotiations Layer (BINL) message	Verify the RIS server is online and authorized. Verify DHCP packets are being routed.
Installation options you expected are not available	Verify another Group Policy Object did not take precedence over your GPO.
System is unable to connect to RIS server, but BINL message is displayed	Restart the NetPC Boot Service Manager (BINLSVC) on the RIS Server.

Miscellaneous:

- The answer file (.SIF) supports the new [RemoteInstall] section. By setting the repartition parameter to yes, the install will delete all partitions on the client computer and reformat the drive with one NTFS partition.
- The Remote Boot Floppy Generator utility (RBFG.EXE) only works on Windows 2000 systems. To create boot floppies, click Start, Run. Enter *RISServerName*\REMINST\ADMIN\I386\RBFG.EXE.
- RIPrep images cannot be created on a server unless it already has an existing CD-based image.

Upgrading from Previous Versions:

- Run WINNT32.EXE for upgrading from a previous version of Windows.
- Windows 2000 will upgrades support: Windows 95 and 98, Windows NT Workstation 3.51 and 4.0, and Windows NT 3.1 or 3.5 (must be upgraded to NT 3.51 or 4.0 first, then Professional).
- Run WINNT32 /CHECKUPGRADEONLY to check for compatible hardware and software. A report will be generated indicating which system components are Windows 2000 compatible.
- All operating system files associated with Windows 95/98 will be deleted after an upgrade.

Troubleshooting Failed Installations:

Common errors:

Problem	Possible fix
Cannot contact domain controller	Ensure network cable is connected. Verify that servers running DNS and a domain controller are both on-line.

	Make sure all network settings are correct.
Dependency service will not start	Verify correct protocol and network adapter in the Network Settings.
Error loading operating system	Disk geometry is reported incorrectly on a NTFS partition. Use a partition less than 4 GB or use a FAT32 partition.
Insufficient disk space	Create a new partition or reformat an existing partition to free up space.

Implementing and Conducting Administration of Resources:

Choosing a file system:

- NTFS provides optimum security and reliability by securing individual files and folders on a user by user basis. Features include disk compression, disk quotas and encryption.
- FAT and FAT32 are used for dual booting between Windows 2000 and other operating systems. If the partition size is less than 2 GB, setup will format the partition as FAT. If greater than 2 GB, it will be formatted as FAT32.
- Existing NT 4.0 NTFS system partition will be upgraded to Windows 2000 NTFS automatically. If you are dual booting between NT 4.0 and 2000, you must install Service Pack 4 on the NT 4.0 machine first.

Disk Quotas

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

NTFS File and Folder Permissions:

File attributes within a partition or between partitions:

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

- The CACLS.EXE utility is used to modify NTFS volume permissions.
- File permissions override the permissions of its parent folder.
- Files moved from an NTFS partition to a FAT partition do not retain their attributes, but retain their long filenames.
- Permissions are cumulative, except for No Access, which overrides everything.

Local and Network Print Devices:

- Windows 2000 Professional supports: Line Printer (LPT), COM, USB, IEEE 1394, and network attached devices.
- Print services can only be provided for Windows and UNIX clients on Windows 2000 Professional.
- Windows 2000 Professional automatically downloads the printer drivers for clients running Win2000, WinNT 4, WinNT 3.51 and Windows 95/98.
- Windows 2000 Server is required to support Apple and Novell clients.
- Print Pooling allows two or more identical printers to be installed as one logical printer.
- Internet Printing allows you to enter the URL where the printer is located. The print server must be a Windows 2000 Server running Internet Information Server or a Windows 2000 Professional system running Personal Web Server. Shared printers can be viewed at: http://servername/printers.
- Print Priority is set by creating multiple logical printers for one physical printer and assigning different priorities to each. Priority ranges from 1, the lowest (default) to 99, the highest.
- To fix a stalled spooler, stop and restart the spooler services in the Services applet in Administrative Tools in the Control Panel.
- Availability option allows Administrator to specify the hours the printer is available.

Managing File Systems:

Windows 2000 supports Basic and Dynamic storage. Basic storage divides a hard disk into partitions. It can contain primary partitions, extended partitions and logical drives. Basic volumes cannot be created on dynamic disks. Basic volumes should be used when dual-booting between Windows 2000 and DOS, Windows 3.x, Windows 95/98 and all version of Windows NT.

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

Volume Types:

Volume Type	Characteristics
Simple volume	Contains space from a single disk
Spanned volume	Contains space from multiple disks (maximum of 32). Fills one volume before going to the next. If a volume in a spanned set fails, all data in the spanned volume set is lost. Performance is degraded as disks in spanned volume set are read sequentially.
Striped set	Contains free space from multiple disks (maximum of 32) in one logical drive. Increases performance by reading/writing data from all disks at

	the same rate. If a disk in a stripe set fails, all data is lost.

Dynamic Volume Limitations:

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

Disk Management on a Remote Computer:

You must create a custom console focused on another computer. Choose Start, Run and type MMC. Choose Add/Remove Snap-in. Click Add. Click Disk Management then click Add. When Choose Computer dialog box appears choose the remote system.

Windows 2000 supports disk-based quotas. Quotas can be set on NTFS volumes, but not on FAT or FAT32 volumes. Quotas cannot be set on individual folders within a NTFS partition.

Using the Disk Management Snap-in Tool:

- The default is Basic storage when adding a new disk.
- You must choose Rescan Disks when you remove or add a new disk.
- Use Import Foreign Disk for disks that have been removed from another computer.
- Upgrading from Basic to Dynamic storage requires at least 1 MB of unallocated space.

Implementing, Managing, and Troubleshooting Hardware Devices and Drivers:

Display devices:

- Monitors are installed, removed, and drivers are updated through Monitors under the Device Manager. Windows 2000 Professional supports multiple monitors running concurrently.
- Use Display Adapters under the Device Manager to install, remove and update drivers.
- Desktop display properties are managed through the Display applet in Control Panel.

Disk devices:

- Use Disk Management to create, delete, and format partitions as FAT, FAT32 and NTFS. Used to change volume labels, reassign drive letters, check drives for errors and backup drives.

- To Manage disk devices, use Control Panel, Administrative Tools, Computer Management or by creating a custom console and adding the Disk Management snap-in. The Computer Management snap-in for your custom console enables Disk Management, Disk Defragmenter, Logical Drives and Removable Storage. There is a separate snap-in for each of these tools except for Logical Drives.

Mobile computer hardware:

- PCMCIA (PC Card) adapters, USB ports, IEEE 1394 (FireWire), and Infrared devices are supported through Device Manager.
- SmartCards and Encrypting File System decrease the likelihood of confidential data being compromised if the computer is stolen or lost.
- Support is provided for Advanced Power Management (APM) and Advanced Configuration and Power Interface (ACPI).
- Hibernation (complete power down while maintaining state of open programs and connected hardware) and Suspend (sleep with some power) modes are supported for extending battery life.
- Use hardware profiles for mobile computers. Accessed through Control Panel, System applet, Hardware tab, Hardware Profiles. Multiple profiles can be created and designated as a docked or undocked portable computer.

Managing/configuring multiple CPUs:

- Windows 2000 Professional supports a maximum of two CPUs.
- Windows 2000 supports Symmetric Multiprocessing (SMP). Processor affinity is also supported. Asymmetric Multiprocessing (ASMP) is not supported.
- Upgrading to multiple CPUs might increase the load on other system resources.
- Update your Windows driver to convert your system from a single to multiple CPUs. This is done through Device Manager, Computer, Update Driver.

Updating drivers:

- Driver Verifier is used to troubleshoot and isolate driver problems. It must be enabled through changing a Registry setting. The Driver Verifier Manager, VERIFIER.EXE, provides a command-line interface for working with Driver Verifier.

Installing and Managing Network Adapters:

- Adapters are installed using the Add/Remove Hardware applet in Control Panel.
- Change the binding order of protocols and the Provider order using Advanced Settings under the Advanced menu of the Network and Dial-up Connections window. Access by right-clicking on My Network Places icon.

Startup and Recovery Settings:

- Use DUMPCHK.EXE to examine contents of MEMORY.DMP.
- Accessed through Control Panel, System applet, Advanced tab, Startup and Recovery.

- Memory dumps are always saved with the filename MEMORY.DMP.
- A paging file must be on the system partition and the pagefile itself at least 1 MB larger than the amount of RAM installed for Write debugging information option to work.

Running the Recovery Console:

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

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

Emergency Repair Disk:

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

Monitoring and Optimizing System Performance and Reliability:

Windows Signature Verification:

- Run SIGVERIF to launch File Signature Verification.
- Saves search results to **SIGVERIF.TXT.**

Using offline files:

By default, offline files are stored in the %systemroot%\CSC directory. Share a folder and set its caching to make it available offline.

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

Encrypted files (EFS) provides 56-bit (standard) encryption for data in NTFS files. It is public key based, and runs as an integrated system service. If a user has a private key to an encrypted NTFS file, the user can edit the file as a normal document. Encrypted files cannot be shared. EFS files are NOT encrypted in the offline cache. You must be a member of the Administrators group to view the offline cache (on an NTFS volume). File and folder permissions still apply in the offline cache, even when it is located on a FAT or FAT32 volume.

Hardware profiles:

- Created to store different sets of configuration settings, usually used with portables.
- Profiles are created through Control Panel, System applet, Hardware tab, Hardware Profiles

Data recovery:

- Windows 2000 Backup is launched through Control Panel, System applet, Backup or by running NTBackup from the Start menu.
- Users can back up their own files and files they have read, execute, modify, or have full control permission for.
- Users can restore files they have write, modify or full control permission for.
- Administrators and Backup Operators can backup and restore all files regardless of permissions.

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

Configuring and Troubleshooting the Desktop Environment:

User profiles:

- When a user logs onto a client computer running Win2000 Pro, the user will receive their individualized desktop settings and all of their network connections regardless of how many users share the same computer.
- A user can change their user profile by changing their desktop settings. When they log off, Windows 2000 incorporates the changes into their user profile.
- Setting a profile as mandatory forces Windows to discard any changes made during the session so the next time the user logs on, the session remains unchanged from their last login.
- User profiles are stored in the %systemroot%\Documents and Settings\%username% folder in a new install of Win2000. When upgraded from NT 4.0, they are stored in %systemroot%\Profiles\%username%.
- Roaming profiles are used in Windows 2000 domains for users who move from one computer to another but require a consistent desktop environment.

Multiple languages and locations:

- Changed through the Regional Options applet in Control Panel. To add more locales, use Region Options, Input Locale, Add.

- To see the available languages and the current default, from the Regional Options applet, General tab, check the "Your System is Configured to Read and Write Documents in Multiple Languages" ListBox.

Managing and Troubleshooting Software Using Group Policies

Deploying software Using Group Policies:

- The software life cycle consists of four phases, Preparation, Deployment, Maintenance, and Removal.
- Windows Installer packages are recognized by their .MSI file extension.
- Integrates software installation into Windows 2000 so that it is centrally controlled, distributed, and managed from a central-point.

Maintaining Software Using Group Policies:

- A software package is installed on a Windows 2000 Server in a shared directory. A Group Policy Object (GPO) is created. Behavior filters are set in the GPO to determine who gets the software. The package is then added to the GPO under User Configuration, Software Settings, Software Installation. Then, select the publishing method.
- Set up Application Categories in Group Policy, computer or user configuration, Software Settings, Software Installation (right-click), Properties, Categories, Add. Creating logical categories helps users locate the software they need under Add/Remove Programs on their client computer.
- When upgrading deployed software, AD can either uninstall the old application first or upgrade over the top of it.
- Selecting the "Uninstall this application when it falls out of the scope of management" option forces removal of software when a GPO no longer applies.

Configuring Deployment Options:

- You can assign or publish software packages.
- Software that is assigned to a user has a shortcut appear on a user's Start, Programs menu, but is not installed until the first time they use it. Software assigned to a computer is installed the next time the user logs on regardless of whether or not they run it.
- When software is assigned to a user, the new program is advertised when a user logs on, but is not installed until the user starts the application from an icon or double-click a file-type associated with the icon. Software assigned to a computer is not advertised - the software is installed automatically. When software is assigned to a computer it can only be removed by a local administrator. Users can repair software assigned to computers, but not remove it.
- Published applications are not advertised. They are only installed through Add/Remove Programs in the Control Panel or through invocation. Published applications lack resiliency (do not self-repair or re-install if deleted by the user). Finally, applications can only be published to users, not computers.

- With invocation, when a user double-clicks on an unknown file type, the client computer queries Active Directory to see what is associated with the file extension. If an application is registered, AD checks to see if it has been published to the user. If it has, it checks for the auto-install permission. If all conditions are met, the application is installed.
- Non-MSI programs are published as .ZAP files. They cannot take advantage of MSI features such as elevated installation privileges, rolling back an unsuccessful installation, installing on first use of software or feature, etc. .ZAP files can only be published, not assigned.
- When software requires a CD key during installation, it can be pushed down with the installer package by typing misexec /a <***path to .msi file***> PIDKEY="[***CD-Key***]"
- Modifications are created using tools provided by the software manufacturer and produce .MST files which tell the Windows Installer what is being modified during the installation. .MST files must be assigned to .MSI packages at the time of deployment.
- Patches are deployed as .MSP files.

Configuring and Troubleshooting Desktop Settings:

Desktop settings can be configured using the Display applet in Control Panel or by right clicking on a blank area of the desktop and selecting Properties.

Users can change the appearance of the desktop, desktop wallpaper, screen saver settings and more.

Fax support:

- If a fax device (modem) is installed, the Fax applet appears in Control Panel.
- Use the Fax applet to setup rules for how the device receives faxes, number or retries when sending, where to store retrieved and sent faxes, user security permissions, etc.
- The Fax printer in your printer folder cannot be shared.
- If the Advanced Options tab is not available in the Fax applet log off then log back on as Administrator.

Accessibility services:

- Accessibility Wizard is used for deploying accessibility features to users who require them. Define the settings you want to deploy and, on the Save Settings to File page, save them to a file that has the .ACW extension. Place the file on a network share and modify each user's login script so that it imports the settings. The command to import the file is this: %SystemRoot%\System32\Accwiz.exe filename.
- Utility Manager enables users to check an Accessibility program's status, and start or stop an Accessibility program. Administrators can designate to have the program start when Windows 2000 starts. Built-in programs include Magnifier, Narrator, and On-Screen Keyboard.

- By default, automatic reset for accessibility options is disabled. When enabled, accessibility options will be turned off if they have not been used for a pre-defined period of time.
- SoundSentry displays visual warnings when your computer makes a sound.
- FilterKeys tells the keyboard to ignore brief or repeated keystrokes.
- StickyKeys allows you to press multiple key combinations (CTRL-ALT-DEL) one key at a time.
- ShowSounds forces programs to display captions for the speech and sounds they make.
- MouseKeys lets you control the mouse pointer with the numeric keypad.
- Magnifier magnifies a portion of the desktop.
- Narrator reads menu options aloud using speech synthesis.

Implementing, Managing, and Troubleshooting Network Protocols and Services:

TCP/IP protocol:

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

Configuring DHCP to Allow Dynamic Updates:

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

Automatic Private IP Addressing:

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

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

- The 169.254.0.0 - 169.254.255.255 range has been set aside for this purpose by the Internet Assigned Numbers Authority.

Services for UNIX 2.0:

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

Client for NFS:

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

Troubleshooting:

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

NWLink (IPX/SPX) and NetWare Interoperability:

- NWLink is used by NT to allow NetWare systems to access its resources.
- To allow file and print sharing between NT and a NetWare server, CSNW (Client Services for NetWare) must be installed on the NT system. In a NetWare 5 environment, the Microsoft client does not support connection to a NetWare Server over TCP/IP. You will have to use IPX/SPX or install the Novell NetWare client.
- Gateway Services for NetWare can be implemented on your NT Server to provide an MS client system to access your NetWare server by using the NT Server as a gateway. Frame types for the NWLink protocol must match the computer that the NT system is trying to

connect with. Mismatching frame types will cause connectivity problems between the two systems.
- When NWLink is set to auto-detect the frame type, it will only detect one type and will go in this order: 802.2, 802.3, ETHERNET II and 802.5 (Token Ring).
- NetWare 3 servers uses Bindery Emulation (Preferred Server in CSNW). NetWare 4.x and higher servers use NDS (Default Tree and Context.)
- There are two ways to change a password on a NetWare server - SETPASS.EXE and the Change Password option (from the CTRL-ALT-DEL dialog box). The Change Password option is only available to NetWare 4.x and higher servers using NDS.

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

Remote Access Services (RAS):

Authentication protocols:
- RADIUS - Remote Authentication Dial-in User Service. Provides authentication and accounting services for distributed dial-up networking.
- EAP - Extensible Authentication Protocol. Allows for an arbitrary authentication mechanism to validate a dial-in connection. Uses generic token cards, MD5-CHAP and TLS.
- EAP-TLS - Transport Level Security. Primarily used for digital certificates and smart cards.
- MD5-CHAP - Message Digest 5 Challenge Handshake Authentication Protocol. Encrypts usernames and passwords with an MD5 algorithm.
- MS-CHAP (V1 and 2) - Microsoft Challenge Handshake Authentication Protocol. Encrypts entire session, not just username and password. V2 is supported in Windows 2000 and NT 4.0 and Win 95/98 (with DUN 1.3 upgrade) for VPN connections. MS-CHAP cannot be used with non-Microsoft clients.
- CHAP - Challenge Handshake Authentication Protocol - encrypts user names and passwords, but not session data. Works with non-Microsoft clients.
- SPAP - Shiva Password Authentication Protocol. Used by Shiva LAN Rover clients. Encrypts password, but not data.
- PAP - Password Authentication Protocol. Sends username and password in clear text.

Dial-up networking:
- Add new connections by using the Make New Connection wizard.

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

Virtual Private Networks (VPNs):

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

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

Multilink Support:

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

Using Shared Resources on a Microsoft Network:

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

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

Windows 2000 Professional is limited to 10 concurrent connections for file and print services.

Implementing, Monitoring, and Troubleshooting Security:

Active Directory:

Active Directory (AD) services provide a single point of network management, allowing you to add, remove, and relocate resources. It offers centralized management, scalability and open standards support.

Active Directory Structure:

Name	**Characteristic:**
Object	A distinct named set of attributes that represent a network resource such as a computer or a user account.
Classes	The logical groupings of objects such as user accounts, computers, domains or organizational units.
Organizational Unit (OU)	Used to organize objects inside a domain into logical administrative groups such as computers, printers, files shares, and applications.
Domain	Joining a domain requires a domain name, a computer account, and an available domain controller and a DNS server. All network objects exist within a domain with each domain storing information only about the objects it contains. ACLs contain the permissions associated with objects that control which users or types of users can access them.
Tree	A grouping or hierarchical arrangement of one or more Windows 2000 domains that share a contiguous names space (e.g. support.troytec.com, mcse.troytec.com, and mcsd.troytec.com).
Forest	A grouping or hierarchical arrangement of one or more domain trees that form a disjointed namespace. Domains in a forest operate independently of each other, but the forest enables communication across the domains.
Sites	Combination of one or more IP subnets connected by high-speed links. Not part of the AD namespace, and contains only computer objects and connection objects used to configure replication between sites.

Site Replication:

- Active Directory information is replicated between Domain Controllers (DCs) and ensures that changes to a domain controller are reflected in all DCs within a domain. A DC is a computer running Windows 2000 server which contains a replica of the domain directory (member servers do not).

- DCs store a copy of all AD information for their domain, manage changes to it and copy those changes to other DCs in the same domain. DCs in a domain automatically copy all objects in the domain to each other. When you change information in AD, you are making the change on one of the DCs.
- DCs immediately replicate important changes to AD like a user account being disabled.
- AD uses multimaster replication. No single DC is the master domain controller. All DCs within a domain are peers.
- Having more than one DC in a domain provides fault-tolerance. If a DC goes down, another is able to continue authenticating logins and providing required services using its copy of AD.

Local user accounts:

- Resides only on the computer where the account was created in its local security database. If computer is part of a peer-to-peer workgroup, accounts for that user will have to be created on each additional machine that they wish to log onto locally. Local accounts cannot access Windows 2000 domain resources and should not be created on computers that are part of a domain.
- Domain user accounts reside in AD on domain controllers and can access all resources on a network that they have been granted privileges to.
- Built in user accounts are Administrator (used for managing the local system) and Guest (for occasional users - disabled by default).
- Usernames cannot be longer than 20 characters and cannot contain illegal characters.
- User logon names are not case sensitive. Alphanumeric combinations are allowed.
- Passwords can be up to 128 characters.
- User accounts are added and configured through the Computer Management snap-in.
- Creating and duplicating accounts requires username and password. Disabling an account is typically used when someone else will take the user's place or when the user might return.
- When copying a user account, the new user will stay in the same groups that the old user was a member of. The user will keep all group rights that were granted through groups, but lose all individual rights that were granted specifically for that user.

Group Policy:

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

System Policy Editor (POLEDIT.EXE)

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

- Are not removed when the policy ends.

- Not secure because settings can be changed by a user with the Registry Editor (REGEDIT.EXE). Settings are imported/exported using .ADM templates.
- Windows 2000 comes with SYSTEM.ADM (system settings), INETRES.ADM (Internet Explorer settings).

Group Policy snap-in (GPEDIT.MSC)

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

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

Security Configuration:

Security Configuration and Analysis snap-in is a stand-alone MMC snap-in that can configure or analyze Win2000 security based on contents of a security template created using Security Templates snap-in. The text-based tool can be run from the command line using SECEDIT.EXE.

By default, Windows 2000 Professional doesn't require users to press CTRL-ALT-DEL to logon. To increase security, disable this feature to force users to log on. To disable access to the workstation, but allow programs to continue running, use the Lock Workstation option (from the CTRL-ALT-DEL dialog box). To disable access to the workstation, and not allow programs to continue running, use the Logoff option (from the CTRL-ALT-DEL dialog box). To lock the workstation after a period of idle time, use a screensaver password.

Auditing can be enabled by clicking Start, Programs, Administrative Tools, Local Security Policy. In the Local Security Settings window, double-click Local Policies and then click Audit Policy. Highlight the event you want to audit and on the Action menu, click Security. Set the properties for each object as desired then restart computer for new policies to take effect.

To further enhance security, clear the Virtual Memory Pagefile when the system shuts down. By default it is not cleared, but this can be changed under Local Security Policy Settings and will prevent unauthorized person from extracting information from your system's pagefile. You can also prevent the last user name from being displayed at logon (Win2000 Pro does this by default). Use the Group Policy snap-in, Local Computer Policy, to change this. When using Event Viewer, only local administrators can see the security log, but anyone (by default) can view other logs.

Encrypting File System (EFS):

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

IPSec:

IPSec encrypts Transmission Control Protocol/Internet Protocol (TCP/IP) traffic within an Intranet, and provides the highest levels of security for VPN traffic across the Internet. IPSec is implemented using Active Directory or on a Windows 2000 machine through its Local Security settings. It is not available for Windows 95/98 or Windows NT. IPSec is a protocol, not a service. It consists of two separate protocols, Authentication Headers (AH) and Encapsulated Security Payload (ESP). AH provides authentication, integrity and anti-replay but does not encrypt data and is used when a secure connection is needed but the data itself is not sensitive. ESP provides the same features plus data encryption and is used to protect sensitive or proprietary information but is associated with greater system overhead for encrypting and decrypting data.

Supported IPSec authentication methods are Kerberos v5 Public Key Certificate Authorities, Microsoft Certificate Server, and Pre-shared Key.

Before two computers can communicate they must negotiate a Security Association (SA). The SA defines the details of how the computers will use IPSec, with which keys, key lifetimes, and which encryption and authentication protocols will be used. When participating in a Windows 2000 domain, IPSec policies are stored in Active Directory. Without AD, they are stored in these registry keys.

Installing, Configuring and Administering Windows 2000 Professional Exam Questions

1. **What is the compression attribute of an uncompressed file after it is moved within an NTFS partition to a compressed folder on a Win2000 Professional computer?**

   A: The file remains uncompressed.

2. **What should you do on your Win2000 Professional computer to find the location of a shared folder?**

   A: Use System Tools in Computer Management to display the file paths of your shared folders.

3. **You are rewriting an accounting application so that it will run on computers loaded with both Win2000 Professional and Windows 98 computers. Computers must be configured for optimal disk performance. Users must be able to access all of the files on their computers while using either operating system. What should you do?**

   A: Create and format a FAT32 partition.

4. **Your Win2000 Professional computer contains a single hard disk configured as a single partition. You want to move a folder named Accounting under a folder named Corp on your computer. You want the files in the Accounting folder to remain compressed after moving the folder. You want the files in the Corp folder to remain uncompressed. You must ensure that the files are recoverable in case of any disk problems. Using the least amount of administrative effort, what should you do?**

   A: Back up the Accounting folder, move the Accounting folder to the Corp folder.

5. **A shared printer named Printer1 will print, although it has numerous jobs in the print queue. You want to print to an identical print device, which has been shared as Printer2 on Computer2. Without having to reconfigure the default printer, how can you allow users who currently connect to Printer1 to automatically use Printer2?**

   A: Configure Printer1 to add a port and set the port to \\Computer2\\Printer2.

6. **You upgrade six MPS-compliant computers from Windows NT Workstation 4.0 to Win2000 Professional. Each computer has two 550 MHz processors. The computers are used for high-end graphics applications. After the upgrade, users report that the processing time for the graphics applications is much slower. What should you do?**

   A: Use Device Manager to install the MPS-compliant drivers for the second processor.

7. **You install Win2000 Professional on ten computers that have video capture cards installed. A user reports the video capture card is not functioning correctly. Using Device Manager, you view the hardware settings. There is an exclamation mark before the Multimedia Audio Controller. What should you do?**

   A: Use Device Manager to update the drivers for the device.

8. **What user mode MMC console type allows the creation of a new MMC window?**

   A: Full Access.

9. **Which feature of Windows 2000 allows an Administrator to enforce desktop settings for users?**

   A: Group Policy.

10. **To logon locally, a computer must be a member of what?**

    A: The computer must be a member of a Workgroup.
    The computer must be a member of a domain.

11. **You are installing Windows 2000 over the network. Before you install to a client computer, what must you do?**

    A: Establish the path to the shared installation files on the Distribution Server. Create a 500 MB FAT partition on the target computer. Create a client disk with the network client so that you can connect to the distribution server.

12. **After installing an ISA-based SCSI adapter in your docking station, the SCSI adapter is not detected during the startup process. You start the Add/Remove Hardware wizard, but the SCSI adapter is not listed. What should you do to allow Win2000 Professional to detect the SCSI adapter?**

    A: Restart the Add/Remove Hardware wizard.
    Manually add the SCSI adapter drivers.

13. **What file systems are supported by Windows 2000?**

    A: NTFS, FAT, FAT32.

14. **Computers on the ACCOUNTING subnet, which runs Win2000 Professional, are dynamically assigned IP addressing and configuration information from a DHCP**

server on the subnet. Computers on the DEVELOPMENT subnet run Windows 98. They are statically assigned IP addressing and configuration information. Users on the ACCOUNTING subnet report that they cannot communicate with users on the DEVELOPMENT subnet. A user who works on Computer3 reports that he cannot communicate with computers on either subnet. You view the network is configuration (an exhibit will be shown), and it shows computers in subnet ACCOUNTING get IP and gateway addresses by DHCP, but the gateway configuration of DHCP Server is wrong. Computer3 only has NWLink protocol. What should you do? (Choose two)

A: Change the default gateway option IP address on the DHCP server.
Enable TCP/IP protocol with the default settings on Computer3.

15. What is the resulting action when you click on the lock computer button on the Windows Security Dialog Box?

A: Computer is locked.
Applications continue to run.

16. You configure the network adapter card for each Win2000 Professional computer to use TCP/IP and assign static IP addressing information. You configure two computers with 10/100 MBPS UTP-only network adapter cards. On all other computers, you use 10 MBPS BNC/UTP combination network adapter cards. All computers are connected to a 10/100 switch that has category 5 UTP cabling. After the installation you find that only the computers with the 10/100 MBPS UTP-only cards can communicate with each other. What should you do so that all computers on the network can communicate with each other?

A: Change the combination network adapter cards to use the UTP transceiver setting.

17. Your want your computer to use both Win2000 Professional and Windows 98. It has three 6 GB hard disks; Disk 0, Disk 1 and Disk 2. Each hard disk needs to have a 6 GB partition. Windows 98 will be installed on Disk 0, and Win2000 Professional on Disk 1. Project files are to be stored on Disk 2. File level security should be implemented on Disk 1. Project files must be accessed when using either operating system. What should you do? (Select and Place)

A: Disk 0 FAT32
Disk 1 NTFS
Disk 2 FAT32

18. Users are complaining that they can communicate with some of the machines on their network segment, but are having trouble communicating with other machines.

Furthermore, they are unable to access any network resources on other segments. How should you troubleshoot this problem?

A: Use the IPConfig utility to determine what IP addresses have been assigned and check to see if a functioning DHCP server is available for the segment.

19. You have three encrypted files. You want to make a backup copy of the three files and maintain their security settings. You have the option of backing up to either to the network or a floppy disk. What should you do?

A: Copy the files to a network share on an NTFS volume.

20. You have 75 identically configured Win2000 Professional computers that will be shared by users in the OU. With the least amount of administrative effort, what should you do so that users are able to maintain their individual desktop settings regardless of which computer they use?

A: Configure each computer to join the domain.
Create a domain user account that uses roaming user profiles.

21. Randy is a member of the local Administrators group. Users report that Randy has been viewing and changing their files. What should you do to limit Randy to installing programs, perform backups and manage printers, but not to view or change other users files?

A: Remove Randy from the local Administrators group.
Add him to both the Power Users group and the Backup Operators group.

22. Your network's dialup server is configured to support certificate authentication. You want to use smart card authentication on your Win2000 Professional Portable computer. Your computer has a PC Card smart card reader and the appropriate drivers installed, and a smart card. What else should you do to enable smart card authentication on your computer?

A: Configure a dial-up connection to use EAP.
Select the smart card device for authentication.

23. Files are being deleted from your shared hard drive. You want to track all users who access your files in the future. What should you do? (Choose two)

A: Enable the local Group Policy for auditing object access events that are successful.
Use Win2000 Explorer to enable auditing for your files.

24. You have an employee named Drew leaving your company. A new employee named Adam will replace him. Drew has a local user account on a Win2000 Professional computer, with rights and permissions to multiple files and folders on the computer. You want Adam to have the same rights and permissions. What should you do?

A: Rename Drew's user account to Adam, and change the account password.

25. You install a new AGP video adapter in your Win2000 Professional computer. You install the manufacturer's device drivers, and reboot. During the startup process, the monitor goes blank. What should you do?

A: Start the computer by using the Emergency Repair Disk.
Restore the original adapter driver settings.

26. You are having problems with your video driver. What should you do?

A: Reboot the computer, and press F8 to get to the Advanced Options menu. Select Enable VGA Mode.

27. You purchase an USB-based ISDN terminal adapter for your Win2000 Professional portable computer. You install the device, but Plug and Play fails to detect the new device. You test the device on a Win2000 Professional desktop computer, and everything is OK. From Device Manager on the portable computer, you see that all devices are working properly (an exhibit will be shown). What should you do?

A: Contact the hardware manufacturer to obtain an upgrade for the Plug and Play BIOS.

28. Your Win2000 Professional computer has a single Pentium II 400 MHz processor, 64 MB of RAM and an IDE hard disk. When you are working on multiple graphics design applications simultaneously, you notice that your computer responds very slowly. You use System Monitor to view your computer's performance. It shows the percent processor time as high (an exhibit will be shown). What should you do to improve the performance?

A: Add a second Pentium II 400 MHz processor.

29. You use Windows Backup to daily back up the files on drive D of your Win2000 Professional computer. On Thursday morning drive D fails. You replace it with a new hard disk. You want to restore your files on drive D to the new hard disk. You view your backup log and see the backup method is incremental (an exhibit will be shown). In what order do you restore your data?

A: Friday, Saturday, Sunday, Monday, Tuesday, Wednesday. Files will be current as of Wednesday night.

30. Which of the following are user mode MMC console types?

A: Delegated, Multiple Window
Full Access
Delegated, Single Window

31. You use a Win2000 Professional computer to run a weekly report. When the report is running on the computer, another task stops responding and eventually times out. When you run only the other task, the task completes successfully. You use Task Manager to view your system resources. They show the weekly report CPU time is high (an exhibit will be shown). You want to resolve the problem by using Task Manager. What should you do?

A: Decrease the base priority of the weekly report task.

32. You are required to deploy 35 new Windows 2000 desktop computers on your network as quickly as possible. Most of the computers possess the same hardware configurations, but a few have different BIOS chips and video cards. Which installation method should you use?

A: Remote Installation Services.

33. You have Win2000 Professional installed on your C drive. Both your C and D drives have more than 500 MB of free disk space. You frequently run many memory intensive graphics applications simultaneously. You notice that access to drive C is much slower when you are using the graphics applications. You want to maximize disk performance. What should you do?

A: Move the paging file from drive C to drive D.
Set the initial size of virtual memory and the maximum size of virtual memory to 256 MB.

34. You configure your Win2000 Professional portable computer to redirect your My Documents folder to your home folder. You want to ensure that you can access all files in your My Documents folder when you are not connected to the network. What should you do? (Choose two)

A: Use Windows Explorer to enable Offline Files.
Use Windows Explorer to configure the properties of your home folder to be available offline.

35. After installing an USB camera to your Win2000 Professional computer, you notice that your USB keyboard does not respond. You suspect that the camera drivers are not

certified for Win2000 Professional. You want to configure your computer to enable your USB keyboard and to prevent uncertified drivers from being installed in the future. What should you do? (Choose two)

A: Configure Win2000 Professional to enable driver signing.
Start the computer in safe mode. Replace the camera drivers with Win2000 Professional certified drivers by using Device Manager.

36. You open the DHCP console, and notice the DHCP server icon is marked with a red arrow. Why?

A: The DHCP Service is not authorized to operate in the domain.

37. You want to configure your Win2000 Professional portable computer to use offline files. The files include a large project file and some smaller personal files. Your portable computer uses a dial-up connection to the server at scheduled times during the day to automatically download your e-mail messages. You do not want to synchronize the project file during this time. What should you do?

A: Configure Synchronization Settings to synchronize the project file only when using the LAN connection.
Set synchronization for the personal files for both the LAN connection and your dial-up connection.

38. You want to upgrade several computers from Windows NT Workstation 4.0 to Win2000 Professional. Using Setup Manager you create an UNATTEND.TXT file and copy the file to a floppy disk. You then start the installation on a test computer by using the Win2000 Professional CD-ROM. You insert the floppy disk after the computer starts. Although you had set the user interaction level to full unattended mode, you are prompted for all the required parameters. You want to ensure that the unattended installation does not prompt you for input. What should you do? (Choose two)

A: Rename UNATTEND.TXT on the floppy disk to WINNT.SIF.
Add a [Data] section to the unattend.txt and set the unattended install parameter to YES.

39. How do you stop the sharing of a folder?

A: Do Not Share This Folder option.

40. You want to install Win2000 Professional on several new computers. You first install Win2000 Professional on one of the new computers. You log on to the computer by using the local Administrator account. You install some standard applications. You then create a RIS image of the computer you configured. You want to configure the RIS

image so that the standard applications will be accessible to the user when the user first logs on to the network. What should you do?

A: Copy the Local Administrator account profile to the default user profile.

41. You want to install Win2000 Professional on 20 new PXE compliant computers, which do not have operating systems installed. You create a RIS image and load the image onto the RIS server and then start the new computers. You find that the new computers cannot connect to the RIS server. You verify that existing client computers on the network can connect to network servers. What should you do? (Select and Place)

A: DHCP Server is required for RIS.

42. You install Win2000 Professional on your portable computer. You have an external CD-ROM drive is connected to the parallel port, but Win2000 Professional cannot see the CD-ROM drive. Computer Management unsuccessfully scans for the CD-ROM. You want to enable Win2000 Professional to detect the CD-ROM drive. What should you do?

A: Configure the parallel port to enable legacy Plug and Play detection.

43. You want to install Win2000 Professional on 30 PXE compliant computers and 30 non-PXE compliant computers. All computers are included on the current Hardware Compatibility List. You create a RIS image and load the image onto the RIS server. You then start the all computers. PXE compliant computers can connect to the RIS server. Non-PXE compliant computers cannot connect to the RIS server. What should you do?

A: Run Rbfg.exe to create a non-PXE compliant startup disk.

44. You are upgrading a computer from Win98 to Win2000 Professional. You install by using the Win2000 Professional CD-ROM. After the text mode installation portion is complete, you restart the computer. The BIOS virus checker indicates that your computer is infected with a Master Boot Record virus. What should you do before you continue the installation?

A: Disable the BIOS virus checker and restart the computer.

45. A Win2000 Professional computer that is shared by several users. You add two new user accounts named User7 and User8 to the computer. When User7 log on, she receives the error message: "Windows cannot copy file C:\Documents and Settings\default user\ to location C:\Documents and Settings\User7". User8 gets a similar message. What should you do? (Choose two)

A: Add the Everyone group to the DACL for the C:\Documents and Settings\default user folder.
Log on by using the local Administrator account and create new folders for User7 and User8 in the c:\Documents and Settings folder.

46. What type of event is audited to log changes made to user security options?

A: Policy Change.

47. Office 2000 was assigned to all the computers on the network by using a Group Policy object (GPO). You deploy the Office 2000 service release to all of the Win2000 Professional computers on the network. One computer fails. What should you do?

A: Restart Windows Installer on the computer that failed to install the service release.

48. Users in your company use English, French and Spanish create document and to communicate with vendors internationally. Users run the Russian localized edition of Win2000 Professional on their desktop and portable computers. Natasha wants to create a word processing document in both English and Spanish by using Notepad in Win2000 Professional. What should you do?

A: Have Natasha use the Regional Options in Control Panel to add input locales and keyboard layouts/IME for both English and Spanish.

49. You are deploying two new applications to users in your company. All users in your organization use MS Word. All users in the Finance department use MS Access. Some users outside of the Finance department need occasional access to Access. If you have a single domain and each department has their own organizational unit, how should you deploy these applications?

A: MS Word would be assigned in a GPO at the domain level. MS Access would be assign in a GPO at the Finance department's organizational unit and would also be published in a GPO at the domain level.

50. You have text in both English and Spanish. The word processing program you are using is a Windows 16 bit character based application. You complete the English portion of your document. You then install Spanish as a language group by using Regional Options in Control Panel. However, you cannot use Spanish to complete the Spanish portion of your document. What should you do?

A: Save and close the word processing program. Select Spanish by using the locale indicator on the taskbar and restart the word processing program.

51. Which of the following is true of RADIUS support in Windows 2000?

A: A Windows 2000 server can be a RADIUS server, a RADIUS client or both simultaneously.

52. You configure a local group to have a mandatory user profile. The mandatory profile has a logo with 16-bit color and 1024 x 768 resolution. Users have both standard VGA video adapters and SVGA video adapters. Several users report that when they log on to certain Win2000 Professional computers the custom bitmap is distorted. What should you do?

A: Change the custom bitmap to 640 x 480 resolution and reconfigure the mandatory user profile.

53. What must be present on the network when installing a computer to the domain?

A: At least one domain controller and one DNS server.

54. You are using Windows Installer to deploy an application. A Group Policy Object (GPO) is created for the Accounting OU. During the deployment, some users in the Accounting OU report that the installation aborts, while others report that the software shows general protection fault errors. What should you do?

A: Repackage and redeploy the application's .MSI file to the Accounting OU.

55. Your routed TCP/IP network consists of 10 Win2000 Server computers and 75 Win2000 Professional computers. TCP/IP is the only network protocol. You want newly installed computers to use NetBIOS names to connect to all shared resources on the network. You configure a TCP/IP address and a shared mask on each new computer. Which two additional TCP/IP properties should you configure on each new computer? (Choose two)

A: A gateway address.
A WINS server address.

56. By default, which permissions will be changed when you modify the permissions on an NTFS folder?

A: The permissions on the folder, files and sub-folders.

57. You recently added a new hard drive to your principal file storage server so users can store customer documents and contact information. You must format the drive before it

can be used to store files. Which commands will provide access to Disk Management, by default?

A: Select Start|Run, type "DISKMGMT.MSC", then click OK.
Double-click DISKMGMT.MSC in the Sysroot\Winnt\System32 directory.

58. Your network uses DHCP to assign IP addresses in the range 194.134.154.10 - 194.134.154.198. Your computer has been configured to use DHCP but has an IP address of 169.254.134.194. What is the most likely reason for this?

A: The DHCP server is unavailable. Your computer has randomly assigned itself an address from the 169.254.0.0 network.

59. What feature is used to restore Win2000 when Last Known Good does not work?

A: Automatic System Recovery (ASR).

60. You install Win2000 Professional at home. You create a new dial-up connection to connect to your company's RAS. The connection uses both of your external modems and Multilink to bind the modems together. You start the dial-up connection and connect to the RAS. You notice that only one of the modems is connected to the RAS. What should you do?

A: Configure the company's remote access server to accept Multilink connections.

61. Which Windows 2000 technology allows Windows Installer packages to be automatically installed, upgraded or removed using group policy?

A: Windows 2000 Software Installation and Maintenance.

62. You use your Win2000 Professional computer to transfer 20 large files. Each file is 100 MB in size. You want to copy the files from a UNIX server in your branch office to a computer running SQL Server at the main office. When you copy the files by using Windows Explorer, the connection times out and the file copy is aborted. You want to monitor the performance of TCP/IP of your computer. What should you do?

A: Install SNMP. Use the Performance Console to view all the counters of the TCP object.

63. Your Win2000 Professional Client2 has an IP address of 10.10.167.4, a default gateway of 10.10.167.1, and a subnet mask of 255.255.252.0. You want to connect to a shared folder on ServerB. ServerB's IP is 10.10.13.10. But you receive the following error message: "The network location could not be reached". You run IPConfig to review the configuration on Client2. Which configuration setting should you change?

A: Click the incorrectly configured network setting in the IP configuration display. Client2 and ServerB belong to different subnets. Click the subnet mask of Client2.

64. Win2000 Professional Client2 has an address of 10.10.167.4 and a default gateway of 10.10.167.1. You want to connect to a shared folder on ServerB. But you receive the following error message: "The network location could not be reached". You want to allow Client2 to connect to ServerB. What should you do?

A: Configure Client2 to use a WINS server address of 10.10.13.24.

65. You upgrade five computers from NT Workstation 4.0 to Win2000 Professional. The computers are used by members of the Accounting OU. All five computers are configured to have the default security settings. Helen reports that she can't run the accounting applications on her Win2000 Professional computer. Prior to the upgrade, Helen could run it. Helen is a member of the Local Users group. You want the accounting applications to run on Helen's computer. What should you do?

A: Use SECEDIT.EXE to apply the COMPATWS.INF security template to Helen's Security Policy to loosen the permissions for the Local Users group on Helen's computer.

66. You have 200 client computers on your network that run Win2000 Professional. How many auditing policies should be set to audit one type of event?

A: One for each computer.

67. You have 50 MB of free disk space on drive C and 500 MB of free disk space on drive D. Print jobs are failing because the available space on drive C is inadequate. You want print jobs to be able to use the space on drive D. What should you do?

A: From the Print Server Properties dialog box, change the location of the spool folder to any existing file path on drive D.

68. What should you do before installing Win2000 Professional on an NT Workstation 4.0 computer when you want to run both systems?

A: Install Service Pack 4 or later for Windows NT Workstation 4.0.

69. You have a share on your local computer. You believe someone has been intentionally damaging your files. What do you do to determine who is doing this?

A: Turn on Auditing For Objects in the Local Security Policy and select Use Windows Explorer to turn on auditing for specific files.

70. Saul needs access to files that are in the Accounting folder on his computer. A local group named Accounting is granted Full Control permission to the Accounting folder and the files within it. Saul is a member of the Accounting local group but he cannot access the files that he needs. What should you do?

A: Remove Saul from any other groups that have been explicitly denied access to the Accounting folder.

71. You have a Win2000 computer used by several students. You use an account that does not have administrative rights for security reasons, for most activities. You want to schedule a task to run a command file named ADDUSERS.CMD that automatically adds six more student user accounts. What should you do?

A: Schedule the task to run under an Administrative account.

72. You accidentally delete an OU containing 300 user objects. How should you recover the deleted OU?

A: Restart the domain controller in Directory Services Restore Mode. Use the Backup utility to restore the system state data. Use NTDSUTIL.EXE utility to mark the deleted OU as authoritative. Restart the domain controller and replicate the changes to the remaining domain controllers.

73. From the Recovery Console, what command allows you to disable a service?

A: Disable.

74. You schedule a task to run an MMC snap-in to perform configuration tasks on other computers. It is not completing correctly. You manually start MMC, add the snap in. You can successfully run the task, and all tasks are working correctly. You want to enable your task to complete successfully. What should you do?

A: Use Scheduled Tasks to configure the task to run under the security context of your account.

75. You have a shortcut for a folder named Accounting on a network share. When attempting to configure the shortcut to be available offline, you don't see the option. What should you do?

A: Use Windows Explorer to configure the folder to be available for offline access.

76. What are the default networking components included by default in the typical installation of Win2000?

A: Client for Microsoft Networks.
File and Printer Sharing for Microsoft Networks.
TCP/IP.

77. What do you need to do to Windows Backup to ensure that your registry, boot files, and COM objects are also backed up?

A: Configure Windows Backup to back up the System State data.

78. You install a 16-bit ISA sound card and manufacturer's device driver on your Win2000 Professional computer. You restart the computer, but the computer won't start correctly. You start the computer in safe mode. What should you do next?

A: Disable the sound card device driver by using Computer Management.

79. What should you do to prevent users from enabling offline access for the network share that contains a confidential report, but still allow them online access to the report?

A: Use Windows Explorer to disable caching for the records on the network share.

80. You have configured accessibility options for a user. Everything seems to be working correctly. The user leaves his computer and when he returns, none of the accessibility options work anymore. What should you do?

A: On the General tab of Accessibility Options, disable "Turn off Accessibility features after idle for X minutes".

81. A user installs a shared laser printer on his Win2000 Professional computer. The laser printer is connected to a computer named Server1. But when the user logs on to an NT Workstation 4.0 computer, the printer is not included in the list of available printers. You want to allow the user to send print jobs to the shared laser printer from any computer on the network. What should you do?

A: Configure a roaming user profile for the user's user account.

82. You have associated GPOs with your site, domain and OUs. In what order are GPOs processed?

A: Site, Domain, OU.

83. You have a Multilanguage version of Win2000 Professional. When you log on to the network by using you username_eng user account, you are not allowed to add any languages to your computer other than English. What should you do?

A: Reconfigure the Group Policy object (GPO) for the username_eng user account to allow you to change languages on your computer.

84. You upgrade your Win98 computers to Win2000 Professional. You want to remove the Logoff option from the Start menu on the new computers. Which two methods can you use to accomplish your goal? (Choose two)

A: On the Advanced tab of the Taskbar/Start Menu dialog box, clear the Displaylogoff option.
Use a Local Computer Policy that will not include the Logoff option on the Start menu.

85. What parameter is used with SYSPREP to run it without generating a security identifier?

A: NOSIDGEN

86. What is true of a Windows 2000 Domain Controller?

A: A Domain Controller can be demoted to be a member server and vice-versa.
All Domain Controllers in Windows 2000 are of equal status with no primary.
Changes to the Active Directory can be made on any Domain Controller.

87. Using a user's account on his computer, you configure the StickyKeys, FilterKeys, and ToggleKeys accessibility options and then log off of his computer. The user then boots the computer, but the accessibility options are turned off. What should you do?

A: Use Utility Manager to configure the accessibility options to start automatically when Win2000 Professional loads.

88. By using disk-duplicating software you install Win2000 Professional on 20 PXE-compliant computers in the Graphics OU. The reference computer is configured to have Win2000 Professional default desktop settings. Users in the Graphics OU have home folders specified in their user account settings. The home folders are located on the \\Server1\Users network share. You want to change the default path of the user's My Documents folders to their home folders whenever users log on to the network. What should you do?

A: Create a Group Policy object (GPO) for the Graphics OU to redirect the My Documents folder, and define the UNC path \\Server1\Users\%Username%.

89. Where is the Group Policy Template (GPT) for a GPO stored?

A: In the SYSVOL share.

90. Where do you view all shares in use on your computer?

A: Computer Management\System Tools\Shared Folders\Shares.

91. You have a Windows 2000 Professional portable computer that is shared by users in one of your departments. You want to configure a roaming user profile so that users can logon from any location including by using a dial-up connection. You log on to the computer by using the local Administrator account. You create user accounts for the users. When you attempt to configure each individual user account profile to be a roaming profile, you fail. You receive the Change Profile Type dialog box. What should you do?

A: Connect the portable computer to the network, and configure the user accounts for a roaming user profile.

92. What file name extension identifies a Windows Installer file?

A: .MSI

93. You deploy an application to users in the Graphics Organizational Unit. You want to create a custom installation for three users, who are members of the Graphics OU. You want these three users to be able to access additional text, filters, and other graphics options for the software. What should you do?

A: Create the Advanced Software OU within the Graphics OU, and add the users. Create a .MST file, including changes and apply the modifications to the Advanced Software OU.

94. You want to deploy a Win2000 Professional service pack to 10 computers in the Development Organizational Unit. You create a Windows Installer package file for the service pack. You use the package file to successfully install the service pack to other computers in the domain. You assign the package file to the Development OU. After the installation, you notice that the service pack was not installed on any of the 10 computers. You want to ensure that the service pack is successfully installed on the computers in the Development OU. What should you do?

A: Add the user accounts from the Development OU to the DACL. Grant the user accounts Read permission to the service pack deployment directory.

95. You are upgrading two computers from NT Workstation 4.0 to Win2000 Professional. You successfully upgrade the first computer. During the upgrade of the second computer, a power failure interrupts the upgrade. The second computer can no longer run NT Workstation 4.0. It also does not support booting from the Win2000 Professional CD-ROM. Using the first computer, how should you recover the failed upgrade?

A: On the first computer, run Makebt32.exe from the Bootdisk folder on the Win2000 Professional CD-ROM. Restart the upgrade with the new disks on the second computer.

96. Which group scope has its memberships listed in the Global catalog?

A: Universal group.

97. Sam wants to be able to work at home on files that were created in the office on the company network. Prior to logging off the network, Sam enables Offline Files. But, when he attempts to access the files, they are not available. What should you instruct Sam to do?

A: At the office, make all files available offline. Sam will be able to access his files the next time he logs off the network.

98. Which services or protocols must be installed to automatically turn off the power of the display and hard disk after a period of inactivity?

A: APM and ACPI.

99. How can you restore short file names to long file names during the Windows 2000 setup?

A: Build $$RENAME.TXT file and put it in the folder that contains the files that need to be converted.

100. After a user leaves the company, you move all of the files from his home folder (NTFS, EFS enabled) to his manager's folder. When the manager attempts to open any of the files, access is denied. What should you do to allow the manager to access the files?

A: Log on to the network as a Recovery Agent. Decrypt the files for the manager.

101. Users on the network save their work files in home folders (NTFS, EFS enabled) on a network server. The partition also has disk quotas defined. A user reports that she cannot save or update any files to her home folder, due to insufficient disk space. Other users are not experiencing this problem with their home folders. What should you do?

A: Increase the server disk quota entry for the user.

102. Your network only uses TCP/IP. You install Win2000 Professional on a computer named Client2. Client2 has the following configuration:

IP address: 10.10.20.234
Default Gateway: 10.10.13.1
WINS Server: 10.10.13.10.

You cannot connect to shared resources on ServerB and ServerC by using UNC names. You check the configuration settings, and see that the gateway of the subnet which Client2 belongs to is 10.10.20.1 (an exhibit will be shown). What should you do?

A: Configure Client2 to use a default gateway of 10.10.20.1.

103. You configure the Internet connection to enable Internet Connection Sharing. After you configure the connection, you cannot see or connect to any shared resources on your local network. What should you do?

A: Configure the dial up connection to disable shared access.

104. You install Win2000 Professional on a computer named Client2. You connect to shared resources on ServerE daily. Suddenly you are no longer able to connect to ServerE. Other users can connect to ServerE. You ping ServerE. You verify that all of the servers are connected to the network and are running correctly. What is the most likely cause of the problem?

A: The router configuration. It shows Client2's IP is 10.10.167.4, and Client2's Router IP is 10.10.164.3.

105. Your company has two domains; troytec.com and rileysales.com. ServerA is in the troytec.com domain. It runs IIS, Microsoft Proxy Server 2.0, and it is an Intranet site. You want Win2000 Professional computers in the rileysales.com domain to access the Intranet site by connecting to the URL http://ServerA rather than its fully qualified domain name. What should you do?

A: Add troytec.com to the Domain Suffix Search Order on the computers.

106. What kinds of services does Win2000 Professional support for the highest level of security for VPN traffic across the Internet?

A: Kerberos and IPSec

107. You install a DOS application on your Win2000 Professional computer. The application uses the Win2000 Professional default settings Autoexec.nt and Config.nt. Your video adapters are set to 16-bit, 1024 x 768 and default refresh rates. On the first desktop, you create a shortcut for the DOS application, using the default PIF settings. Both monitors are unable to display the application. Both monitors function correctly when you run Windows based applications. What should you do?

A: Change the color setting for both video adapters to 256 colors. Reconfigure the shortcut properties to run the DOS based application in full screen mode.

108. What software specification allows several protocols to be bound to a single network adapter?

A: NDIS

109. How should you configure your laptop to save the contents of memory to the hard disk and then to shut down when the sleep button is chosen?

A: Configure the power settings to use the Hibernation option.

110. You have 3 sites; Houston, Paris and Rome. Houston is connected to Paris via a 256K WAN link. Houston is also connected to Rome via a 256K WAN link. Paris is connected to Rome via a 56K WAN link. You wish to create site links so that you can optimize Active Directory synchronization traffic. How many site links should you create?

A: 3

111. You have 3 sites; Houston, Paris and Rome. Houston is connected to Paris via a 256K WAN link. Houston is also connected to Rome via a 256K WAN link. You wish to create site links so that you can optimize Active Directory synchronization traffic. How many site links should you create?

A: 2

112. You have a 2 MB Windows Bit Map. You have compression enabled on your C:\ drive. The file has been compressed to 1 MB. You try to copy the file to a floppy disk but you get the message "Insufficient disk space". How can you copy the file to the disk?

A: You must use a third party compression tool to compress the file.

113. You then attempt to install 32-bit application printer software that came with a new laser printer. During the installation, you receive the error message "failed to load

WINPRINT.DLL. Specified module could not be found" (an exhibit will be shown). What should you do before you share the printer with other users?

A: Obtain and install the WDM-compliant device drivers and printing software for the printer.

114. What two types of DFS are supported by Windows 2000?

A: Fault-Tolerant DFS and Stand-Alone DFS

115. What type of event is audited to log changes made to the system time on a computer?

A: Privilege Use.

116. Your Win2000 Professional computer has a built in 33.6 kbps modem. You install a 56K ISA based modem. When the installation is complete, you notice that the 56K modem is not functioning. Device Manager shows that the 33.6K modem and the 56K modem are conflicting with each other. You want to configure Win2000 Professional to use only the 56K modem. What should you do?

A: Using Device Manager, disable 33.6K modem.
No action required on 56K modem.

117. You want to install Win2000 Professional on 100 MPS compliant computers. Each computer has two 550 MHz processors, and are configured identically. One of the computers will be used as a reference computer for deploying Win2000 Professional to the others. You install Win2000 Professional on the reference computer. You view Device Manager and notice that the drivers for the second processor are not installed. You want to add support for the second processor on the remaining 99 computers. What should you do?

A: Use Device Manager to add the appropriate HAL to the reference computer to support the second processor, and then create a disk image.

118. What is the minimum processor specification for Windows 2000 Professional or Windows 2000 Server on an Intel-based computer?

A: P133

119. In a default installation to an Intel-based computer, which folder is used as the destination of Windows 2000 Professional?

A: WINNT

120. What needs to be included in the [UNATTENDED] section of the UNATTEND.TXT file to convert a FAT or FAT32 partition to NTFS during an unattended install?

A: FileSystem=ConvertNTFS

121. You wish to create a Windows 2000 Professional startup floppy disk set. What command would you run to create the disk set?

A: Makeboot A:

122. You want to use the Remote Installation Service (RIS) to install Win2000 Professional on a client computer. What services must be available?

A: DNS Server.
DHCP Server.
Active Directory.

123. How can you apply OU GPO settings to only some of the user objects in the OU?

A: Create a security group containing only the users that will use the GPO settings. Give this only this security group both READ and APPLY GROUP POLICY permissions on the GPO.
Move the user objects that do not require the GPO settings to a sub OU within the parent OU. Use the block inheritance setting on the child OU to stop the parent GPO settings being applied.
Create a security group which contains all the users that will not use the GPO settings. DENY this security group APPLY GROUP POLICY permission on the GPO.

124. You are working from home using a dial-up connection. You can access resources on the first subnet, where the dial-up server is located, but you cannot access other resources on the network. What dial-up parameters should you change?

A: The default gateway on remote network.

125. What are the two types of user groups in Windows 2000?

A: Security and Distribution.

126. You have associated a GPO with both a parent OU and one of its child OUs. What statements are true of how the GPO settings will be applied?

A: If the GPO settings are compatible with each other then BOTH GPOs will be applied.
If the GPO settings are not compatible then the child OU GPO settings take precedence.

127. You have created three GPOs for your site, domain and OU. Each of the three GPOs has been configured with "No Over-Ride". Which GPO settings are guaranteed to be applied to the OU?

A: Site.

128. Where in the Group Policy settings would you configure computer Startup and Shutdown scripts?

A: Computer Configuration.

129. What is true of L2TP?

A: L2TP supports header compression.
L2TP supports tunnel authentication.

130. What is true of PPTP?

A: PPTP require an IP-based network.
PPTP provides data encryption.

131. What is the maximum number of WINS server addresses that can be listed on a WINS client?

A: 12

132. You are planning to install Win2000 Professional on your Win98 computer. You want to select the best file system and features. You must to be able to use both operating systems to access all disks. Which file system do you use?

A: FAT32

133. A user wants to use a dial-up connection to your network. He will be using a Smart Card for authentication. Which authentication protocol must he use?

A: EAP

134. True or False: A domain and a workgroup can share the same name.

A: True

135. What parameter in the [GUIUnattended] section of the UNATTEND.TXT file allows you to skip presetting the regional Settings?

A: OEMSkipRegional

136. What must be done before a computer running Windows 2000 can join a domain?

A: A computer account must be created or added to the domain database.

137. What name is given to the site link created by default on Windows 2000?

A: DEFAULTIPSITELINK

138. Which information is available in the Windows 2000 Security Dialog Box?

A: Name of user account in use.
Name of domain user logged onto.

139. What entry is required in the [Data] section of the .SIF file during a Win2000 CD-ROM boot pre-installation?

A: [Data] Unattendedinstall=yes Msdosinitiated =0 Autopartition =1

140. What protocol allows users to print to a URL over an Intranet or the Internet?

A: IPP

141. Which user interface provides additional feedback and sort options to view installed or available application by size, frequency of use and time of last use?

A: Add/Remove Programs Wizard.

142. What switch is used with WINNT.EXE to specify the file name for the setup information file?

A: WINNT.EXE /I

143. What is required to join a workgroup?

A: A new or an existing workgroup name.

144. What statements are true of assigning an application using Group policy?

A: Assigned applications can be installed by document invocation.

Assigned applications are resilient and can automatically repair themselves.
Assigned applications are advertised on the user's desktop.

145. You realize as you attempt to install Windows 2000 Professional that your computer does not support booting from the CD-ROM. What should you do?

A: Start the computer by using the Setup boot disks. Insert the Windows 2000 Professional CD-ROM when prompted, and then continue Setup.

146. Two of your users have connected to their home folders on the same file and print server. When the users query the amount of free disk space on the server they receive different answers. Why is this?

A: The users have different amounts of unused disk quota on the server.

147. Which feature of Windows 2000 allows you to secure your network traffic so that it cannot be easily read by anybody capturing the packets?

A: IPSec

148. You have just installed a DHCP server on your Windows 2000 network. No leases are being obtained from the DHCP server. You have checked the scope settings and they all appear correct. The scope has been activated. Why are no clients obtaining leases from this DHCP server?

A: The DHCP server has not been authorized.

149. Why can't users log on locally to a domain controller?

A: PDCs do not maintain local security databases.

150. What statements are true of moving objects in Active Directory?

A: Any permission assigned directly to that object will be moved with the object.
Multiple objects can be moved simultaneously.
Any currently inherited permission on the object will be lost and replaced with inherited permissions from the new container.

151. How many domain controllers and DNS servers must be online to allow you to join a domain?

A: One DC and one DNS.

152. Your company has a forest consisting of two Domain trees. Each Domain tree contains a root Domain and two sub-Domains. You have just created a Domain Local group and would like to assign permissions to this Domain Local group to resources within your company. To which resources can permissions be given to this Domain Local group?

A: Only resources in the same Domain as the Domain Local group.

153. Your company has a forest consisting of 2 Domain trees. Each Domain tree contains a root Domain and two sub-Domains. You have just created a Global group and would like to assign permissions to this Global group to resources within your company. To which resources can permissions be given to this Global group?

A: Any resource in the forest.

154. How can you reduce the time it takes for a client to process a GPO, that only modifies user settings, to determine what settings need be applied?

A: Disable the computer configuration settings for the GPO.

155. Where in the Group Policy settings would you configure user logon and logoff scripts?

A: User configuration.

156. Which folder redirection option would you choose to enable folders to be redirected to different alternate locations?

A: Advanced

157. Using a Group policy, you want to automatically remove software on a user's computer. What two removal options are available?

A: Forced, Optional

158. What are the differences between assigning an application to a user and assigning an application to a computer?

A: Applications assigned to the user will be available whenever the user logs on Applications assigned to the computer are available to all users of that computer.
Applications assigned to a user require the user to either invoke a program before it installs. Applications assigned to a computer are automatically installed the next time the computer restarts.

159. What tool is used to create a distribution tool and create a single UNATTEND.TXT file to pre-install 500 Win2000 computers?

A: Setup Manager.

160. You have recently published a software upgrade to your users using a Group policy. You have noticed, however, that when a user invokes an associated document, the older version is installed. How can you install the newer version using document invocation?

A: Change the upgrade to be mandatory.
Alter the software order listed in the GPO so that the newer version is higher than the older version.

161. By default, what is available on Windows 2000 Professional?

A: Customized Start Menu and Automated Recovery System (ARS).

162. What is true of a Global catalog in Windows 2000?

A: A Global catalog contains only the commonly queried objects and attributes for a forest.

163. You install a new video card into your Win2000 computer. After the installation, the system will not start. What should you do?

A: Use Recovery Console

164. You want to create a shared Internet connection on your network. Users should not have any permission other than HTTP and FTP access. How should you configure the port settings?

A: Configure HTTP port settings to 80.
Configure FTP port settings to 21.

165. You have installed and configured fax service on your Win2000 Professional computers. A user states that she is able to receive faxes, but to send them. What should you do?

A: Use the Fax Service Management tool to enable the device to receive faxes.

166. You update some Windows 98 machines to Win2000 Professional. After rebooting, you get a virus warning from your BIOS. The MBR is damaged. What should you do?

A: Boot from the Win2000 Professional installation CD-ROM and repair the Master Boot Record.

167. What section do you need to add to your answer file to load third party SCSI drivers?

A: AC

168. Windows Installer Service should be run in what security context?

A: In the security context of the system, not the context of the current user to avoid lack of rights or permissions.

169. By default, what happens to the files that were redirected when a folder redirection policy is removed?

A: The redirected files remain in the redirected location.

170. A single network logon is made possible in Windows 2000 due to support for which protocol?

A: Kerberos.

171. You have a laptop that is configured for a SCSI adapter when docked. You want to maximize the battery performance of your laptop computer. You do not want the SCSI adapter available when you are not docked. What should you do?

A: Start the system without the docking station. Disable the SCSI adapter device for the current profile.

172. You are creating a dial-up connection on your Windows 2000 portable computer to connect to your customer's dial-up server. Although you are not sure which type of server your customer is using for dial-up connections, you still want to ensure that your dial-up connection authentication is secure and that your logon information is not sent in plain text. You view the Advanced Security Settings dialog box. What options should you select to obtain your goals?

A: Challenge Handshake Authentication Protocol (CHAP)
Microsoft CHAP (MS-CHAP)
Microsoft CHAP Version 2 (MS-CHAP v2)

173. How do you stop the printer from notifying you when a print job has printed?

A: In the server properties of the Printers system folder, clear the Notify when remote document has been printed option.

174. When you perform a new installation of Windows 2000. As Setup must request a DHCP (server assigned) IP address during GUI-mode Setup before you can choose between using a static IP address and using DHCP to obtain an IP address automatically, this may cause a Dynamic Domain Name System server to retain an incorrect DNS-host-name-to-IP-address mapping. How can you prevent this from occurring?

A: Create a Setup answer file (WINNT.SIF) that contains the static IP address you intend to use.

175. How do you make a web page available for offline viewing in Windows 2000?

A: On the Favorites menu in Internet Explorer, click Add to Favorites. Select the Make Available Offline check box. To schedule updates for the page, content download, click Customize.

176. You want a certain group of your Windows 2000 Professional computers to be able to communicate with other Windows 2000 computers on your network. However, you do not want the computers to communicate with computers that are not running Windows 2000. How should you configure a security policy on each computer to ensure that the computers can only communicate with other Windows 2000 computers?

A: Use Security Configuration and Analysis to import the hisecws.inf security template file to modify the security settings.

177. You are upgrading several Windows 95 computers to Windows 2000 Professional. Most have the same hardware, but there are many different peripheral devices throughout the company. How can you verify that all of the hardware in use is compatible with Windows 2000 Professional?

A: Use Setup Manager to create a Setup.inf file. Add the entry ReportOnly=Yes to the [Win9xUpgrade] section of the answer file. Run Winnt32.exe /Unattend:Setup.inf.

178. You install Windows 2000 Professional on a new APM-compliant laptop computer. But whenever you attempt to shut down the computer, the power remains on, even when you use the power button. What should you do?

A: Restart the computer, use the Power Options in Control panel to enable APM, then reboot.

179. You configure a user's Windows 2000 Professional computer to use the on-screen keyboard and StickyKeys options. You save the accessibility option settings to a shared folder on the local hard disk of the user's computer. You want to configure the same options for another user. You log onto the second user's computer using his local user account. You access the shared folder over the network, and select the .acw file from the shared folder. You receive an error message stating that there was a problem loading the specified file. What should you do?

A: Change the permissions of the .acw file on the shared folder to allow read access for the second user's account.

180. You are configuring a roaming user profile for a Drew Morgan. You create a user account named DrewM on a Windows 2000 Server. You define a network profile directory path named \\Server1\Profiles\%Username%. When Drew logs onto the computer, he receives the error message, "Cannot locate your roaming profile". What should you do?

A: Change the %Username% variable to DrewM.

181. You replace the uniprocessor computer in your design department with new MPS-compliant computers. Each computer has two 550-MHz processors. You install design software that includes Win32, Win16, and DOS-based applications. When users use a Win16-based application, they do not notice an improvement in performance compared to using the uniprocessor computers. What should you do?

A: Replace the Win16-based applications with available Win32-based applications.

182. Your computers have both Windows NT Workstation 4.0, and Windows 2000 Professional. You configure the hard disk on each computer to have a two 4-GB partitions. Windows NT Workstation is installed on drive C, and Windows 2000 Professional is installed on drive D. You configure a disk quota on drive D to prevent users from saving data on the disk. How can you prevent users from saving files to drive D in either operating system?

A: Use Windows NT Workstation to configure NTFS permissions on drive D to deny users Write permission.

183. A user in your Accounting OU reports that their mouse is not working. You log onto the domain from that user's computer by using the domain Administrator's account. You discover the user is using an old mouse driver. You install an updated mouse driver, and restart the computer. The mouse is still not working correctly. You view Device Manager, and notice the previous mouse driver is still installed. What should you do?

A: Set the Accounting OU policy for security to warn and allow the installation to override the local security.

184. You schedule a task to run after 15 minutes. After an hour, you check the Event Viewer system log. It contains the error message: "The Task Scheduler service failed to start". You want to run the scheduled task again. What should you do before restarting the Task Scheduler?

A: Set the Task Scheduler service to log on as a Local System account.

185. A user downloads a video card driver from the Internet. You are unsure of the source of the driver. You want to ensure the user does not lose production time because of an incompatible driver. What should you do?

A: Install the driver. If the computer fails after installing the driver, restart the computer with the Last Known Good configuration to recover the original driver.

186. A user reports that their Windows 2000 Professional computer is running very slowly. What methods can you use to improve performance? (Choose all that apply)

A: Perform a disk analysis, and use disk defragmenter.
Use Disk Clean to delete temporary files and unnecessary program files.

187. You install a SCSI adapter and a SCSI tape drive on your Windows 2000 Professional computer. Windows 2000 Professional detects and installs drivers for the new SCSI devices. After you restart the computer later that day, the computer stops. What should you do to enable your Windows 2000 Professional computer to start successfully?

A: Start the computer using the Recovery Console.
Disable the SCSI adapter device driver by using the disable command.

188. You attempt to install a printer driver on a Windows 2000 computer, but receive an error message: "Error 11 – Cannot install printer driver". How should you configure the computer to check for driver integrity and to allow you to install the driver?

A: Use the Print troubleshooter.
Configure the computer to prevent the installation of unsigned drivers.

189. You are preparing to deploy many new Windows 2000 Professional computers on your network. You want to be able to recover from disk failures and corrupt system files on the new computers. What should you do to configure the computers to

automatically update their system configuration and emergency repair files on a scheduled basis?

A: Use Windows Backup to schedule a backup of System State data.

190. Your Windows 2000 Professional computer has a shared printer that several departments use. The Accounting department prints extremely large ledgers causing others to wait. How can you improve printing efficiency so that other users do not have to wait for their print jobs?

A: Configure the priority of the printer to 50. Add a new printer, and set the priority to 95. For the new printer, deny Print permissions for users in the Accounting department.

191. The computers in your design department have built-in USB controllers. You install a USB tablet-pointing device on each computer. A tablet icon appears in Control Panel to configure the device, but it doesn't work. What should you do?

A: Enable the USB ports in the BIOS, and re-install the USB tablet device drivers.

192. Your computer has a built-in 10-MB Ethernet adapter. You then install a 100-MB Ethernet PC Card adapter. You notice that the 100-MB adapter is not functioning. What should you do so that the Windows 2000 Professional computer uses only the 100-MB Ethernet PC Card adapter?

A: Use Device Manager to disable the device for the 10-MB adapter.

193. Your network has five Windows 2000 Servers, and 50 Windows 2000 Professional computers. The Professional computers were installed by using a RIS image on one of the Windows 2000 Servers. You need to upgrade several applications on the Windows 2000 Professional computers. The applications do not have built-in support for scripted installations. You want to accomplish the following goals:

- **The upgraded applications will be installed using the unattended installation method.**
- **Existing user environments will be maintained.**
- **The network name will be changed to match its serial number.**
- **The RIS image and the upgraded applications are enabled as they are added to the network.**

You take the following actions:

- **Install the RIS image on a Windows 2000 Professional computer named Pro1.**
- **Install the upgraded applications on Pro1.**
- **Change the network name of Pro1 to %DMI-SERIAL_NUM%.**
- **Run RIPrep.exe on Pro1.**

- **Start all of the Windows 2000 Professional computers and load the RIS image.**

Which results do these actions produce? (Choose all that apply)

A: An unattended installation of the upgraded applications is performed.

194. You want to configure all of your Windows 2000 Professional computers to allow access to the Internet. You do not plan on installing a permanent Internet connection. You do have a single dial-up account at a local ISP, and a 56-Kbps modem. What should you do to configure access for the Windows 2000 computers? (Choose all that apply)

A: Configure the dial-up connection to enable on-demand dialing.
Configure the dial-up connection to enable Internet Connection Sharing.
Attach the modem to one of the Windows 2000 Professional computers, and create a dial-up connection to the ISP.

195. You create a new dial-up connection to connect to your company's remote access server. You can connect to servers on the same segment as the remote access server, but cannot access shared resources on remote segments. What should you do?

A: Configure the TCP/IP properties for the dial-up connection to use the default gateway.

196. You create a new dial-up connection to connect to the Internet. You configure the Internet connection to enable Internet Connection Sharing. However, you cannot see or connect to any shared resource on your network. What should you do?

A: Use the ipconfig command to release and renew your network TCP/IP address.

197. You are install Windows 2000 Professional on several MPS-compliant computers. The computers are configured identically with two 550-MHz processors. You intend on using one of the Windows 2000 Professional computes as a reference computer for the other computers. After you install Windows 2000 Professional on the reference computer, you notice that the drivers for the second processor are not installed. How can you add support for the second processor on the other computers?

A: Use the System Preparation Tool with the –pnp parameter to set up the reference disk.

198. You are adding new PXE-compliant computers to your network which contains Windows NT Workstation 4.0 computes. The hardware on the new computers is identical. You are using a RIS image to deploy Windows 2000 Professional to the new computers. You successfully deploy Windows 2000 Professional on the first ten computers, but cannot install it on the remaining computers. What should you do?

A: Configure the DHCP scope to add additional IP addresses.

199. You want to create a standard installation image to install Windows 2000 Professional. The computers have different hardware and component configurations. You install Windows 2000 Professional and other standard software on one of the computers. You log on to the computer by using the local Administrator account. After configuring the applications, and customizing the desktop settings, you run Setup Manager and create the Sysprep.inf file. You copy Sysprep.exe and Setupcl.exe to the \Sysprep folder. You run both Sysprep.exe and your third party disk imaging software. You then copy the image to several test computers and restart them. Some of the computers do not start. Some of the desktop settings are different that the original computer. What should you do? (Choose two)

A: Copy the Administrator profile to the Default User profile. Grant permissions to the Everyone group to use the profile.
Include the –pnp parameter for the Sysprep.exe when you rerun that utility.

200. You are upgrading Windows NT Workstation computers to Windows 2000 Professional. You create an Unattend.txt file and copy the file to a floppy disk. You start the installation on a test computer by using the Windows 2000 Professional CD-ROM. You insert the floppy disk after the computer starts. You had set the user interaction level to full unattended mode, but you are still prompted for parameters. What should you do?

A: Rename Unattend.txt on the floppy to Winnt.sif.

201. Users have attached USB devices and have installed device drivers that were not supported by Windows 2000 Professional. You want to configure the computers to install device drivers only for devices that are included on the current HCL. Which option should you enable in the Driver signing Options dialog box?

A: Block – Prevent installation of unsigned files.

202. You install an updated driver for the Zip drive in your Windows 2000 Professional computer. The computer stops responding. You restart in safe mode. The computer stops responding again. What should you do? (Choose three)

A: Use the disable command to disable the Zip device driver.
Select Recovery Console from the Repair menu.
Start the computer by using the Windows 2000 CD-ROM.

203. You are configuring your Windows 2000 Professional portable computer to use a dial-up connection to connect to a Routing and Remote Access server. Your computer has a smart card, and has the appropriate drivers installed. You use MMC to request a new certificate. What options should you enable in the Advanced Security Settings dialog box? (Choose all that apply)

A: Use Extensible Authentication Protocol.

Installing, Configuring, and Administering Microsoft Windows 2000 Server Concepts

Installing Windows 2000 Server

Requirements

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

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

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

- All hardware should appear on the Windows 2000 Hardware Compatibility List (HCL).
- If Windows 2000 is being integrated into an existing Windows NT 4.0 domain structure, mixed mode must be used. If Windows 2000 is being installed into an

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

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

Attended Installation

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

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

Installing from CD-ROM

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

Installing over a Network

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

WINNT.EXE Command Line Switches

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

Troubleshooting Installations

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

Unattended Installations

- Answer files are created using the Setup Manager Wizard or a text editor.
- SMW allows for creation of a shared Distribution Folder and OEM Branding.

- Unattended installations use an answer file to provide information during the setup process.

Creating the Answer File

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

User Interaction Levels for Unattended Installs

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

System Preparation Tool (SYSPREP.EXE)

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

distribution folder. If you are using SYSPREP, place CMDLINES.TXT in the \$OEM$\$1\Sysprep subfolder.

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

Upgrading from a Windows NT Domain

Upgrading a Windows NT domain involves several stages:

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

Upgrading from Microsoft Windows NT 4.0

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

Troubleshooting Remote Installations

Symptom	Solution

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

Install, Configure and Troubleshoot Access to Resources

Install and Configure Network Services

TCP/IP Server Utilities

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

TCP/IP Client Utilities

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

Install and Configure Local and Network Printers

- Enabling Availability option allows Administrator to specify the hours the printer is available.

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

Folders and Shared Folders

Distributed File System (Dfs)

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

Standalone Dfs

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

Domain-based Dfs

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

Local Security on Files and Folders

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

NTFS File and Folder Permissions

File attributes within a partition or between partitions:

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

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

Access to Web Sites

Virtual Servers

Multiple Web sites can be hosted on the same machine by using Virtual Servers. There can only be one home directory per virtual server. There are three methods for setting up virtual servers:

1. Each virtual server can have its own IP address. Multiple IPs are bound to the server's NIC and each virtual server is assigned its own IP address.
2. Each virtual server can have the same IP address, but uses a different name under host headers. Host headers rely on newer browsers knowing which site they want to access. Workarounds will have to be implemented for older browsers.
3. Each virtual server can have the same IP address but a different port number.

Virtual Directories

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

Controlling Access to Web Services

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

Hardware Devices and Drivers

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

Disk Devices

- Removable media are managed through the Removable Media snap-in.
- To Manage disk devices, use Control Panel, Administrative Tools, Computer Management or by creating a custom console and adding the Disk Management snap-in. The Computer Management snap-in for your custom console enables Disk Management, Disk Defragmenter, Logical Drives and Removable Storage. There is a separate snap-in for each of these tools except for Logical Drives.
- Use Disk Management to create, delete, and format partitions as FAT, FAT32 and NTFS. Used to change volume labels, reassign drive letters, check drives for errors and backup drives.

Display Devices

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

Driver Signing

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

Windows Signature Verification (SIGVERIF.EXE)

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

System Performance, Reliability and Availability

Usage of System Resources

Performance Console

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

System Monitor Snap-In

Allows you to measure the performance of your own computer or other computers on a network. It performs the following tasks:

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

Objects include:

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

Performance Logs and Alerts Snap-In

Allows you to collect performance data automatically from local or remote computers. Data can be viewed by using System Monitor, or exported to a spreadsheet program or database for analysis and report generation. Performance Logs and Alerts snap-in performs the following:

- Collect data in a comma-delimited or tab-separated format for easy import to spreadsheet programs. A binary log-file format is also provided for circular logging or for logging instances such as threads or processes that might begin after the log starts collecting data.
- Define start and stop times, file names, file sizes, and other parameters for automatic log generation.
- Manage multiple logging sessions from a single console window.
- Set an alert on a counter, thereby stipulating that a message be sent, a program be run, or a log be started when the selected counter's value exceeds or falls below a specified setting.
- View counter data during collection and after collection has stopped.

Optimize Disk Performance

- Defragmenting your hard disks regularly will improve read performance.
- Mirrored volumes and spanned volumes slow down system performance.

- Page files are fastest when spread across several disks, but not the boot or system disks.
- Striping a disk set causes greatest performance increase.

System State Data and User Data

System State data

Comprised of the registry, COM+ class registration database and system startup files. Can also include Certificate Services database if Certificate Services is installed. If machine is a domain controller, Active Directory directory services and SYSVOL directory are included. For machines running Cluster Service, resource registry checkpoints and quorum resource recovery log are included.

- Can be backed up from the command line by typing:
  ntbackup systemstate /m normal /f d:\sysstate.bkf /j "System State Data Backup"
- On a domain controller, an Authoritative Restore may need to be performed to force restored system state data to replicate to other domain controllers throughout Active Directory.
- On a domain controller, moving system state data to a separate volume from the system volume can increase performance.
  Where /m=backup type (can be copy or normal), /f=filename and /j=job name.

Recovering System State Data

Emergency Repair Disk

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

Windows Backup

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

Safe Mode

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

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

Running the Recovery Console

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

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

Storage Use

Disks and Volumes

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

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

Volume Types

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

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

Dynamic Volume Limitations

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

Dynamic Volume States

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

Disk Management Snap-in Tool

- Disks can be upgraded from Basic to Dynamic storage at any time but must contain at least 1 MB of unallocated space for the upgrade to work.

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

Configuring Data Compression

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

Disk Quotas

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

Windows 2000 Network Connections

Using Shared Resources

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

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

Sharing Tab

Option	Description
Caching	The settings to configure if and how files within the shared folder are cached locally when accessed by others.
Do Not Share This Folder	If you do not want to share this folder. All other options are grayed out.

Permissions	The shared folder permissions that apply only when the folder is accessed over the network. By default, the Everyone group is assigned Full Control for all new shared folders.
Remove Share	The option that allows you to remove a share. This option appears only after the folder has been shared more than once.
Share Name	The name that users from remote locations use to make a connection to the shared folder. You must enter a share name.
Share This Folder	If you want to share this folder. All other options are active.
User Limit	The number of users who can concurrently connect to the shared folder. The Maximum Allowed option allows Windows 2000 Server to support an unlimited number of connections. The number of Client Access Licenses (CALs) purchased limits the connections.

Virtual Private Networks (VPNs)

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

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

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

Network Protocols and Services

Protocols

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

- AppleTalk

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

TCP/IP protocol

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

Configuring DHCP to Allow Dynamic Updates

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

Automatic Private IP Addressing

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

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

Services for UNIX 2.0

- FTP support has been added to Windows Explorer and to Internet Explorer 5.0 allowing users to browse FTP directories as if they were a local resource.
- Install SNMP for Network Management (HP, OpenView, Tivoli and SMS).
- Print Services for UNIX allows connectivity to UNIX controlled Printers (LPR).
- Simple TCP/IP Services provides Echo, Quote of Day, Discard, Daytime and Character Generator.

- UNIX uses NFS (Network File System).
- Windows 2000 uses CIFS (Common Internet File System) which is an enhanced version of the SMB (Server Message Block) protocol.

Client for NFS

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

Troubleshooting

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

NWLink (IPX/SPX) and NetWare Interoperability

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

Other protocols

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

Remote Access Services (RAS)

Authentication protocols

- CHAP - Challenge Handshake Authentication Protocol - encrypts user names and passwords, but not session data. Works with non-Microsoft clients.
- EAP - Extensible Authentication Protocol. Allows for an arbitrary authentication mechanism to validate a dial-in connection. Uses generic token cards, MD5-CHAP and TLS.
- EAP-TLS - Transport Level Security. Primarily used for digital certificates and smart cards.
- MD5-CHAP - Message Digest 5 Challenge Handshake Authentication Protocol. Encrypts usernames and passwords with an MD5 algorithm.
- MS-CHAP (V1 and 2) - Microsoft Challenge Handshake Authentication Protocol. Encrypts entire session, not just username and password. V2 is supported in Windows 2000 and NT 4.0 and Win 95/98 (with DUN 1.3 upgrade) for VPN connections. MS-CHAP cannot be used with non-Microsoft clients.
- PAP - Password Authentication Protocol. Sends username and password in clear text.
- RADIUS - Remote Authentication Dial-in User Service. Provides authentication and accounting services for distributed dial-up networking.
- SPAP - Shiva Password Authentication Protocol. Used by Shiva LAN Rover clients. Encrypts password, but not data.

Dial-up Networking

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

Remote Access Policies

- A static IP can be assigned to a user when their connection is made.

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

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

Remote Access Profiles

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

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

Terminal Services

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

Installing Terminal Services

TS Services include:

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

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

Remote Server Administration Using TS

- Do not use for tasks that require reboots.
- If another Administrator is in session on the same server you are working on, you may overwrite each other's work. Use the QUSER command to see if other Administrators are in session.

- Remote Administration Mode allows a maximum of 2 concurrent connections to be made per server by an Administrator. Memory and CPU utilization settings remain unaffected and application compatibility settings are completely disabled.
- Remote Administration Mode allows Administrators have complete access to the remote system to perform tasks such as software installation, and administrative functions, etc.
- There are no licensing requirements for using the Remote Administration Mode.

Configuring TS for Application Sharing

- A Temp folder is created for each user by default. Use the FLATTEMP.EXE tool or the Terminal Services Configuration Tool to change the location of the temporary folders or disable them and force all users to share one Temp folder (flattemp /disable).
- Automatic Printer redirection is supported for all 32-bit Windows clients. TS will detect printers attached locally to the client and create corresponding print queues in the user's session. When a user disconnects print queues and any print jobs are terminated. Printers must be manually redirected for 16-bit Windows clients and Windows based terminals.
- By default, users will be prompted for a password unless it is changed in the properties for RDP-TCP.
- Remove the default Home Directories created by Windows 2000 for each user and create TS specific network Home Directories on a file server. All application specific files (e.g., .INI) are written to these directories.
- Sessions will disconnect when the connection is broken but will continue executing a user's processes by default. To prevent system resources from being taken up by these processes, set your sessions to reset on broken connections.
- TS cannot be clustered, but it can be load-balanced using Network Load Balancing. This causes a group of servers to appear as a single virtual IP address. Alternately you can use round-robin DNS resolution to load balance your TS servers.
- Users can be assigned a specific Terminal Services profile. If one is not available TS will then try to load a user's Roaming Profile. If the two previous are not available TS will load the standard Windows 2000 Profile.

Configuring Applications for Use with TS

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

Security

Security Configuration

The Security Configuration and Analysis snap-in can be used to directly configure local system security. You can import security templates created with the Security Templates snap-in, and apply these templates to the group policy object (GPO) for the local computer.

Security Templates Snap-In

A security template is a physical representation of a security configuration; it is a file where a group of security settings may be stored. Windows 2000 includes a set of security templates, each based on the role of a computer. The templates range from security settings for low security domain clients to highly secure domain controllers. They can be used as provided, modified, or serve as a basis for creating custom security templates.

Security Configuration Tool Set

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

Encrypting File System (EFS)

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

- Use the Cipher command to work with encrypted files from the command line.
- Uses public-key encryption. Keys that are used to encrypt the file are encrypted by using a public key from the user's certificate. The list of encrypted file-encryption keys is kept with the encrypted file and is unique to it. When decrypting the file encryption keys, the file owner provides a private key which only he has.
- You can't share encrypted files.

Policies in a W2K Environment

Local and System Policy

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

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

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

Group Policy snap-in (GPEDIT.MSC)

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

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

Auditing

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

Auditable Events

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

Local accounts

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

through groups, but lose all individual rights that were granted specifically for that user.

Account Policy

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

Installing, Configuring and Administering Windows 2000 Server Practice Questions

1. **After installing Terminal Services on a Windows 2000 domain controller, and Terminal Services Client on user's client computers, user report they are not allowed to logon interactively. You are able to log on to the Terminal server as an administrator. What should you do to allow users to log on to the Terminal server?**

   A: Grant the users the right to log on locally.

2. **Your manager uses computers in many different locations. Many of the files he works with are confidential. What should you do to allow the manager to maximize security yet still allow him to access the confidential folder from any location?**

   A: Configure the managers account to have a roaming user profile, and instruct him to use folder properties to set the encryption attribute for his folder.

3. **A temporary employee has left your company. This employee used encryption to secure files in a shared folder. The files must now be made available to a new employee. What should you do? (Choose two)**

   A: Log on as an administrator and remove the encryption attribute from the files. Configure the new employee's account to be an Encrypted Data Recovery Agent.

4. **You configure the Local Security Options for the Default Domain Policy object in your domain. You also enable a local security option to display a logon message when a user logs onto the domain. You want a different logon message for the New York OU without changing the other Local Security Options. What should you do?**

   A: Create a new GPO in the New York OU with the appropriate logon message. Enable policy inheritance for the new GPO.

5. **What should you do to add a custom registry entry into a Group Policy Object with the least amount of administrative effort?**

   A: Configure an ADM template and add the template to the GPO.

6. **An employee has created a file where he lists himself as the only person in the access control list. The file contains sensitive information and must be removed. Using the minimum amount of authority necessary, without modifying any of the permissions for the other files in the folder, how would you delete this file?**

   A: Take ownership of the file. Grant yourself Modify permission for the file. Delete the file.

7. You have the following share and NTFS permissions for a Distributed file system root Public. You add a shared folder named Files as a Dfs node under the root.

Folder	Share Permissions		NTFS permissions	
Public	Everyone:	Read	Everyone:	Read
Files	Users:	Read	Sales:	Full Control
	Domain Admins:	Full Control	Domain Admins:	Full Control

A user name Sharon is a member of the Sales group. When saving a file to the Public\Files folder, she receives an access denied message. What should you do to allow Sharon to be able to change and delete files in the folder without giving her more permission that necessary?

A: Set the share permissions for the Files folder to grant Sharon Change permission.

8. Sales users in your network have permission to access the Internet through a Windows 2000 Server running Microsoft Proxy Server. Sales users must enter their proxy server user names and passwords to connect to the proxy server, to the Internet, and to the Intranet server. Users who do not access the Internet do not have accounts on the proxy server. What should you do to allow all users to be able to connect to the Intranet server without entering a separate user name and password?

A: Configure each client computer to bypass the proxy server for local addresses.

9. You configure a server named print01.marketing.troytec.local as a print server at your New York site. You create and share printers on the server for use by your employees in the marketing.troytec.local domain. From Tokyo, you want to review the configured properties of all of the shared printers on the print01.marketing.troytec.local server. What should you do?

A: Use your Web browser to connect to http://print01.marketing.troytec.local/printers.

10. Your TCP/IP network consists of Windows 2000 Servers computers, Windows 2000 Professional computers and UNIX servers, and uses IP addresses from the private range 10.0.0.0. Print jobs are sent to a shared printer on a Windows 2000 Server named PTRSRV. A print device is attached to one of the UNIX servers. This server uses LPR printing protocol and its IP address is 10.1.1.99. The name of the printer queue is UPRINT. What should you do to allow users to be able to connect to this printer from their computers?

A: Create a local printer on PTRSRV.
Create a new TCP/IP port for an LPR port for an LPR server at address 10.1.1.99 with a queue named UPRINT.
Share this printer and connect to it from the users' computers.

11. You have shared a printer named HPPTR on a Windows 2000 Server computer named ptrsrv.troytec.local. You grant Print permission only to the Domain Local group named TroytecSales. You then add a new child domain named bristol.troyresearch.local. A member of the global group named BrisolSales in the bristol.troyresearch.local domain reports that she is unable to send a print job to HPPTR. What should you do to allow all member of the BrisolSales group to be able to print to HPPTR?

A: Add the BrisolSales group to the TroytecSales group.

12. Your network consists of a Windows 2000 Server which runs Internet Information Services (IIS). Web developers need to update Web sites and virtual directories from remote locations simultaneously. What should you do to ensure that each developer can use Microsoft FrontPage to update the sites and manage content?

A: Configure the server extensions for each Web site by selecting Configure Server Extensions from the All Tasks menu in IIS.
Configure the server extensions to allow each developer update access for each Web site.

13. You install Client Service for NetWare on your Windows 2000 Professional computers and gateway Service for NetWare on your Windows 2000 server computers. You have NetWare 4.0 servers in your network. After adding a new Windows 2000 Server computer, you install Gateway Service for NetWare on it, but it is unable to connect to any of your NetWare servers. What should you do?

A: Configure the NWLink IPX/SPX/NetBIOS Compatible Transport Protocol to use the correct Ethernet frame type.

14. You have two employees. One is a member of the Administration group, and the other is a member of the Intern group. Both groups are in the same domain. On the Intranet server, the Administration group is placed in the Security group, and the Intern group is placed in the non-security group. The Security group is granted Full Control permission for the Finance virtual directory. The member of the non-security group needs to update new financial information that is located on the Financial virtual directory. What should you What should you do?

A: Make the non-security group employee a member of the Security group.

15. You are upgrading a Windows NT Server 4.0 computer to Windows 2000 Server. It is a member server in a Windows 2000 domain named sales.troytec.local. The domain runs in native mode. What should you do to change the role of the upgraded server from a member server to a domain controller? (Choose two.)

A: Upgrade the server to Windows 2000 Server.

Run the Active Directory Installation Wizard to make the server a domain controller in the sales.troytec.local domain.

16. Your routed Windows 2000 network includes 25 Windows 2000 Server computers. You want to install a new Windows 2000 Server computer as the first computer on a new routed segment. You configure the existing DHCP server with a scope that is valid for the new segment, and specify that the server should obtain its IP address from an existing DHCP server. But, after you complete the installation, you can only see the new server in My Network Places. You run ipconfig, and find that your IP address is 169.254.1.200, with a 16-bit subnet mask and no default gateway address. What should you do? (Choose two)

A: Configure all of the routers to route BOOTP broadcast frames.
Add a DHCP Relay Agent computer to the new routed segment.

17. Your network consists of a single Windows NT 4.0 domain. You want to install Windows 2000 Server on a new computer. What should you do to make the computer act as a domain controller in the existing domain?

A: On the new computer, install Windows NT Server 4.0 and designate the computer as a BDC in the existing domain.
Promote the computer to the PDC of the domain.
Upgrade the computer to Windows 2000 Server.

18. What should you do to configure the deployment of a Windows 2000 service pack so that users automatically receive the service pack when they log on to the domain?

A: Create a Microsoft Windows Installer package for the service pack.
Configure the package in a Group Policy.

19. You are installing Windows 2000 on new computers in your network. These servers will provide file and print services. You want to use a centralized copy of the Windows 2000 installation files, which are stored on an existing Windows 2000 Server. What three actions should you take? (Choose three)

A: Create an MS-DOS network boot disk.
Create an Unattend.txt file.
Create a UDF file that identifies the names of the new computers.
Begin the installation process by running the Winnt /s /u /udf.

20. Your network consists of numerous domains within a single LAN, with one remote domain. The remote location is running an outdated service pack. Retaining the domain administrator's access to the Group Policy configuration, what should you do to update the remote location while reducing network traffic and easing administration of Group Policies?

A: Configure a Group Policy for the remote domain.
Configure a service pack software package for the Group Policy.

21. Your 32-bit application stops responding several days after installation. Task Manager shows the CPU usage to be 100 percent. You end the application. The CPU usage is still at 100 percent. What should you do?

A: Use Task Manager to end any related child processes.

22. Your application writes a large number of temporary files to a single directory on your Windows 2000 Server. You add three new 100-GB SCSI disks to hold the temporary files. You want the application to use all 300 GB of space with a single drive letter, using the fasted performance when writing to the disks. What should you do?

A: Convert all three disks to dynamic disks.
Create a striped volume.

23. Your boot volume is installed on volume C on your Windows 2000 Server, and volume C is mirrored on dynamic Disk 1. Later, you find that the status of volume C is Failed Redundancy, and the status of Disk 1 is Missing. The status of volume C does not return to Healthy after you attempt to reactivate Disk1. What should you do?

A: Remove the mirror on Disk1, replace the disk, and add back the mirror to the new Disk 1.

24. After upgrading a Windows NT Server 4.0 computer to Windows 2000 Server, Disk 1 fails. The computer has two hard disks, and the system and boot partitions are located on two primary partitions on Disk 0. Both partitions are mirrored on Disk 1. You replace the failed disk with another from a Windows 2000 computer, but find the Repair Volume option is unavailable when you try to repair the fault-tolerant volumes. How should you repair the mirror set? (Choose two)

A: Delete all volumes on Disk 1.
Change Disk 1 back to a basic disk.
Repair the fault-tolerant volumes on Disk 0.
Break the mirror set.
Convert Disk 0 to a dynamic disk.
Create a mirror on Disk 1.

25. You have installed the boot volume D on your Windows 2000 Server computer on dynamic Disk 0, and mirror volume D on dynamic Disk 1. Later, you find the status of volume D is Failed Redundancy. The status of Disk 1 is Online (Errors). What should you do? (Choose two)

A: Break the mirror, delete the volume on Disk 1, and re-create the mirror. Reactivate the mirror on Disk 1.

26. Your Windows 2000 Server computer has a single hard disk with two partitions. One of your applications creates a large log file in the Systemroot\Temp folder. The disk does not contain enough free space to accommodate the log file. What should you do?

A: Add a second hard disk.
Delete the contents of the Systemroot\Temp folder.
Create and format a partition.
Mount the partition as the Systemroot\Temp folder.

27. You convert the stripe set with parity to a dynamic RAID-5 volume on your Windows 2000 Server computer that contains a stripe set with parity on a four-disk array. User then report that disk access on the server is slow. The status of the third disk in the array shows Missing. What should you do first to recover the failed RAID-5 volume?

A: Ensure that the third disk is attached to the server and has power.
Use Disk Management to reactivate the disk.

28. You share a folder on your Windows 2000 Server that contains multiple subfolders. Some of these subfolders are compressed, and some are not. How do you move files from one uncompressed folder to a compressed folder, and ensure the files are compressed when you move them, without compressing the remaining files in the original uncompressed folder?

A: Copy the files from the uncompressed folder to the compressed folder, then delete the original files.

29. You have configured your Windows 2000 Server, which utilizes a large NTFS volume, to have disk quotas for the NTFS volume. All users have a default limit of 100 MB, and the option to deny space to users who exceed their limit has been enabled. A user complains that they are receiving the error message "The disk is full or too many files are open". What should the user do?

A: Remove files until the total uncompressed file size is less than 100 MB.

30. You are the administrator of your company's network. You use a non-administrator account to log onto the server to perform routine upgrades. Prior to updating all the critical system files and patches on the server, what should you do?

A: Log on as an Administrator and run Windows Update.

31. Each of your branch offices uses Internet Connection Sharing to connect to the Internet. Randy is configuring a Windows 2000 Server as a file server. When he uses Windows Update for the first time, he selects Product Update, and receives an access denied error. What should you do to allow Randy to configure the server?

A: Give Randy's user account administrator privileges on the Windows 2000 Server computer.

32. What three things can you do to help diagnose why users cannot connect to a second modem configured with Routing and Remote Access on your Windows 2000 Server? (Choose three)

A: Use the Diagnostics tab on the Phone and Modem Options.
Use Device Manager to identify any port resource conflicts.
Use the Routing and Remote Access snap-in to find out whether the ports are operational.

33. An incorrect driver was installed during the installation of a modem on your Windows 2000 Server computer. The computer will be used as a Routing and Remote Access server for a branch office. You attempt to remove the modem by the Phone and Modem Option, but the computer stops responding. What is the quickest way to install the correct driver after restarting the computer?

A: Use the Add/Remove Hardware Wizard to uninstall the modem.
Restart the server.

34. You are replacing an integrated 10-MB Ethernet adapter with a new 100-MB Ethernet adapter. After installing the new adapter you receive an error message stating the new adapter is missing or is not working. What should you do?

A: Use Device Manager to disable the integrated 10-MB Ethernet adapter.

35. You have a Windows 2000 Server which uses a non-Plug and Play ISA modem that uses IRQ 5. You add a PCI modem and restart the computer. You realize that both modems are trying to use IRQ 5. What should you do?

A: Edit the CMOS settings on the computer to reserve IRQ 5 for the non-Plug and Play.

36. Your network is not directly connected to the Internet, and uses the private IP address range of 192.168.0.0. You install Routing and Remote access. You can successfully dial into the server, but cannot access any resources. The ipconfig command shows the dial-up connection has been given the IP address of 169.254.75.182, and when you ping the server, you receive a "Request timed out" message. What should you do?

A: Ensure that the remote access server is able to connect to a DHCP server that has a scope for its subnet.

37. You want to make an application available on all of the client computers in your network using Terminal Services on a Windows 2000 Server computer. The server will not run as a domain controller. You install Terminal Services. The Support department needs to be able to remote control users' sessions to support and troubleshoot the application. What should you do to enable the Support department to control users' sessions?

A: Grant the Support department Full Control permission to the Remote Desktop Protocol on the Terminal server.

38. Your network consists of ten subnets that contain 10 domain controllers, 10 member servers, and numerous client computers. All servers run Windows 2000 Server, and all clients run Windows 2000 Professional. Two domain controllers are DNS servers. You use only TCP/IP. You want client computers to be able to register and resolve addresses if a server fails. How should you configure the DNS servers so that all computers can resolve the address of all other computers by using DNS?

A: Configure at least two servers with Active Directory integrated primary zones for the domain.

39. You have a multiple-process database named Application on your Windows 2000 Server. Users report that the application has stopped responding to queries. The server is running, so you decide to restart the application. What should you do before restarting the application?

A: End the Application.exe process tree.

40. Your Windows 2000 Server computer uses a SCSI adapter that is not included in the HCL. You install an updated driver for the adapter. After restarting the computer, you receive "Inaccessible_Boot_Device". What should you do? (Choose two)

A: Start the computer by using the Windows 2000 Server CD-ROM.
Perform an emergency repair.
Reinstall the old driver for the SCSI adapter.
Start the computer by using the Recovery Console.
Copy the old driver for the SCSI adapter to the system volume and to C:\ntbootdd.sys
Restart the computer.

41. How can you revert Active Directory to a version that was backed up on each of three domain controllers on a previous day?

A: Shut down and restart a single domain control in Directory Services Restore Mode.
Use Windows Backup to restore the System State Data.

Run the Ntdsutil utility.
Restart the computer.

42. After adding a new partition to your disk, you receive a "Windows 2000 could not start because the following file is missing or corrupt: <Windows 2000 root>\system32\ntoskrnl.exe. Please re-install a copy of the above file". What should you do?

A: Start the computer by using the Recovery Console.
Modify the Partition parameter in the operating system path in C:\Boot.ini.

43. Your Windows 2000 Server computer is a file server. It runs many 16-bit applications. One of these stops responding, causing all other 16-bit applications to stop responding. What should you do to isolate the application for monitoring and troubleshooting? (Choose all that apply)

A: Create a batch file that starts the application by running the start /separate command.
Use this batch file to start the application.
Create a shortcut to the application, and select the Run in a separate memory space.
Use this shortcut to start the application.

44. What columns would you choose to find out whether the response times of a new application would improve by the addition of one or more processors on your Windows 2000 Server? (Choose two)

A: USER Objects and I/O Reads.

45. After using Regedt32 to edit the registry of your Windows 2000 Server to insert a new value, and remove an unused key, your computer stops responding before the logon screen appears after you reboot. What should you do to return the computer to its previous configuration?

A: Restart the computer using Last Known Good.

46. You have a 12 GB primary partition formatted as FAT32 on your Windows 2000 Server computer. The number of users and average size of files remains constant over a period of time. Users then begin to report that the server does not retrieve files as fast as when the server was first installed. What should you do?

A: Defragment the disk.

47. You install a new tape device on your Windows 2000 Server. After restarting the computer, you receive the error: "IRQL_NOT_LESS_OR_EQUAL". What should you do to bring the server back online as quickly as possible?

A: Restart the computer by using the Recovery Console.

Disable the driver.
Restart the computer.
Remove the driver.

48. Users report that when you run Microsoft Excel every afternoon, the response time on the server lags. What should you do?

A: Use Task Manager to set the priority of the Excel.exe process to Low.

49. Running System Monitor locally, and ensuring it has the least impact on other processes, how do you measure the physical disk performance counters on your Windows 2000 Server computer? (Choose two)

A: From the command prompt, run the Start/low perfmon command.
Use Task Manager to set the priority of the MMC.EXE process to Low.

50. Your Windows 2000 Server runs both 32-bit and 16-bit applications. Each 16-bit application is configured to run in a separate memory space. You want to create a performance baseline chart for all applications on the server. You add all of the 32-bit applications. What should you do to add the 16-bit applications?

A: Add the ntvdm and the ntvdm#2 instances of the %Processor Time counter for the Process object.

51. You work with files that are confidential. These files are kept in your Private folder located in your home folder. You use numerous computers to access these folders. What should you do to maximize security of the Private folder, and still allow access from remote computers?

A: Configure your account to use a roaming user profile. Use the properties of the Private folder to set the encryption attribute.

52. Your Windows 2000 Active Directory network consists of Windows 2000 Professional computers and Windows NT Workstation computers. Users of the Windows 2000 Professional computers cannot change their desktops or the display settings on their computers. Users of the Windows NT Workstation computers can change all display settings. What should you do to restrict all users of Windows NT Workstation computers from changing their desktop settings?

A: Configure a Windows NT policy file and place it in the proper folder on the PDC emulator.

53. Your Windows 2000 network consists of Windows 2000 Servers that were upgraded from Windows NT, Windows 2000 Professional computers and Windows NT Workstation computers. After you implement GPOs for each OU, you find that the GPOs only apply to users of the Windows 2000 Professional computers. You want to

restrict users of the Windows NT Workstation computers from accessing registry-editing tools. What should you do?

A: Create a Windows NT system policy file on a Windows 2000 domain controller.
Configure the policy so that it restricts default users from accessing registry editing tools.

54. You have created a GPO for the Finance OU in your network. You want to prevent users in the Finance OU from accessing My Network Places and running System in Control Panel. But, you want the Managers Domain Local group to be able to access My Network Places, yet not run System in Control Panel. What should you do?

A: Create a second GPO in the OU.
Add the Manager's group to the ACL of the GPO.
Allow the Manager's group to apply the Group Policy.
Disable the permission of the Authenticated Users group to read and apply the Group Policy.
Configure the new GPO to allow access to My Network Places.
Give the new GPO a higher priority than the original GPO.

55. How do you configure a Group Policy so that future changes to the Group Policy will be applied within 15 minutes to any computers that are logged onto the network?

A: Enable and configure the Group Policy refresh interval for computers.

56. You share a folder on your Windows 2000 Server that contains multiple subfolders. Some of these subfolders are compressed, and some are not. The Marketing folder is compressed. You want to delete it, but want to keep all the files in the folder. You want to copy all the files to the Admin folder before deleting the Marketing folder. You want the files to remain compressed, but do not want to compress any files in the Admin folder. What should you do?

A: Move all the files from the Marketing folder to the Admin folder.

57. Your Windows 2000 Server computer has a spanned volume that consists of areas on three disks. The disks support hot swapping. One of the disks fails. You replace the disk with a new, non-partitioned disk. How should you recover the spanned volume and its data as quickly as possible?

A: Rescan the disks.
Remove the spanned volume and create a new spanned volume that includes the new disk.
Format the spanned volume.
Use Windows Backup to restore the data.

58. Your Windows 2000 Server has a RAID-5 controller. The RAID array is configured as two partitions. Drive C is a 2 GB partition that hold the operating system and paging file. Drive D is a 30 GB partition that holds the home folders. Engineering employees use a data capture application that generates files that can be larger than 100 MB. You want to implement disk quotas. Normal users can be allowed to store a maximum of 75 MB. Quotas should not limit engineers. What should you do? (Choose two)

A: Enable quota management on drive D.
Select the Deny disk space to users exceeding quota limit check box.
Set the default quota limit to 75 MB.
Create a new quota entries for the Engineers' user accounts.
Select the Do not limit disk usage for this entry.

59. Your Windows 2000 Server contains two hard disks. Each disk is partitioned as a single primary partition. The first disk is formatted as FAT32, the second as NTFS. You compress shared folders on second disk. When users move compressed files from a shared folder on the second disk to a shared folder on the first disk, the files lose their compression. What two actions should you take to ensure that all files moved from folders on the second disk to shared folders on the first disk remain compressed?

A: Convert the first disk to NTFS.
Compress the shared folders on the first disk.

60. You have two Windows 2000 Servers, Srv1 and Srv2. Srv1 has a spanned volume over three physical disks. These disks support hot swapping. The drive letter that the spanned volume uses on Srv1 is not currently in use on Srv2. You want to move the three disks to Srv2, using the same drive letter as Srv1. You back up the spanned volume. What should you do next?

A: Move the disks from Srv1 to Srv2.
On Srv1, rescan the disks.
On Srv2, rescan the disks.

61. You are installing Windows 2000 Server on a new computer that is connected to a network that contains Windows 98 computers, and Windows 2000 Server computers. You want to install Windows 2000 Server from source files located on a server on the network. What should you do?

A: Start the new computer by using a Windows 98 network boot disk.
Connect to the network server.
Run WINNT.EXE.

62. Your Windows 2000 Server has two NTFS partitions. Windows 2000 Server is installed on drive D. After a power failure, you receive the error message: "NTLDR is missing. Press any key to restart". What should you do?

A: Start the computer by using the Windows 2000 Server CD-ROM and choose to repair the installation.
Select the Recovery Console and copy the NTLDR file on the CD-ROM to the root of the system partition.

63. What should you do to install a customized HAL designed for a computer on which you are installing Windows 2000 Server?

A: During the hardware confirmation portion of Windows 2000 Setup, install the customized HAL.

64. Your network consists of two domains: troytec.local and tech.troytec.local. It has Windows 2000 Professional computers and Windows 2000 Server computers. You enable auditing in the domain policy object for troytec.local to audit the success and failure of object access. After installing a printer on a domain controller, you configure auditing on this printer to monitor printing successes and failures. When you review the security log later, no events have been written to the log, even though you know the printer has been used. What should you do to log all successes and failures of printing for the printer?

A: Configure auditing of successes and failures of object access in the Default Domain Controllers Policy object in the Domain Controllers OU of the tech.troytec.local domain.

65. Your network uses the TCP/IP protocol for its Windows 2000 Professional and Windows NT computers. You have one server that acts as both a WINS server, and a DNS server. All the client computers are configured to use this server for DNS and WINS. Users of Windows NT Workstation cannot connect to a file server, but Windows 2000 Professional users can. This server has a static address of 192.168.1.11. What should you do to allow the Windows NT Workstation computer to connect to the file server?

A: Select the Enable NetBIOS over TCP/IP. Add the WINS address used by the Windows NT Workstation computers.

66. Both of your domains are Active Directory domains that run in native mode. How can you see a list that shows which users are allowed to use remote access to your network?

A: Create a group named RAS_USERS.
Add users who are permitted to dial in to the network.

Create a remote access policy that allows only this group to use the remote access server.
Display the members of the group.

67. Your network is a routed and uses TCP/IP as its only protocol. You have a single domain with Windows 2000 Professional and Windows NT Workstation computers. You install Gateway Service for NetWare on a Windows 2000 Server computer. You install a second network adapter on the gateway server. You want to configure the first adapter for communications to and from your Windows-based client computers exclusively. Which checkboxes in the Local Area Connection Properties dialog box should you select? (Choose all that apply)

A: Client for Microsoft Networks
File and Printer Sharing for Microsoft Networks
Internet Protocol (TCP/IP)

68. You have Routing and Remote Access on a server that has one modem. The server is configured to use demand-dial routing to connect to the main office. The manager wants users to be able to dial in to the server only between 6:00 p.m. and 8:00 a.m., but wants users to be able to log on at any time when connected directly to the LAN. What should you do to limit only dial-in access to this timeframe?

A: Set the remote access policy to deny connections between 8:00 a.m. and 6:00 p.m.

69. Your company has developed a 32-bit application that collects information from various processes. You want to make the application available on all of the client computer by using Terminal Services. The company wants users to shut down their computers at the end of their shifts, and to leave the application running on the Terminal Server. What should you do?

A: Set the RDP on the server to override user settings, and set the End disconnected sessions setting to Never.

70. Frequently, a newly installed modem stops communicating with your ISP. The only way to reactivate the modem is to restart the computer. You want to install a new driver for the modem. What should you do?

A: In Device Manager, on the property sheet for the modem, click the Update Driver command button.

71. You have a Windows 2000 Server which uses a non-Plug and Play EISA modem that uses IRQ 11. You add a second PCI network adapter and restart the computer. You realize that both adapters are trying to use IRQ 11. What should you do?

A: Edit the CMOS settings on the computer to reserve IRQ 11 for the non-Plug and Play devices.

72. Your Windows 2000 Server has an integrated network interface adapter. You are replacing it with a new network interface adapter which will be installed in an available PCI slot. When your restart the computer, you receive an error message stating that the new network interface adapter is missing or not working. What should you do?

A: Disable the integrated network interface adapter.

73. A disk with the ARC path multi(1)disk(0)rdisk(1)partition(1) is not responding. Which disk should you replace?

A: Click Controller 1, Disk number 2.

74. You add a new SCSI disk controller that has six new disks attached to your Windows 2000 Server that has two disks attached to an EIDE disk controller. The new controller is not included in the HCL. When you restart your computer, Windows does not detect the new controller. What should you do? (Choose two)

A: Use the Add/Remove Wizard to add a new SCSI and RAID controller.
Use the manufacturer's setup program to install the SCSI driver.

75. You are logged on to a Windows 2000 Server computer as a member of the Backup Operators group. You try to configure the software for a tape backup device, but the configuration fails. You must update the driver. What should you do?

A: Instruct a domain administrator to run the runas command using the domain administrator's user name and password. Click the Update Driver button on the Driver tab for the tape backup device.

76. You are installing Windows 2000 Server on ten new computers. These computers will provide file and print services to branch offices. You want to install, configure and test Windows 2000 Server on the branch offices' computers before shipping them to the branch offices. The users of the branch offices should enter the computer names and serial numbers when they receive the computers. What should you do?

A: Install Windows 2000 Server on the computers. Use Setup Manager to create a SYSPREP.INF file for SYSPREP.EXE.
Place the SYSPREP.INF file on the computers and run the sysprep –nosidgen command.

77. You are upgrading a Windows NT Server 4.0 computer to Windows 2000 Server. The system partition uses FAT. After starting the Setup program from the Windows 2000 Server CD-ROM you receive an error message: "You chose to install Windows 2000 on a partition that contains another operating system. Installing Windows 2000

on this partition might cause the operating system to function improperly". What should you do?

A: Restart the computer. Run WINNT32.EXE from the Windows NT Server environment.

78. Your network consists of two trees, with four domains in each tree. You plan to deploy a service pack to support.IS.troytec.com domain and the support.IS.devon.com domain, but to no other domains. You will use a Group Policy to configure the service pack package. You want to minimize complexity, administration, and network traffic. You create a Windows Installer package for the service pack. What should you do to configure the Group Policy?

A: Configure the Windows Installer package in a Group Policy for the support.IS.troytec.com and support.IS.devon.com domains.

79. Your computer has three 100 GB hard disks without any partitions defined. You want as much space on Disk 0 as possible for the partition on which Windows 2000 Server is to be installed. You want as much disk space as possible across all three disks to be accessible by using a single driver letter. What should you do?

A: Install Windows 2000 Server on a 100 GB NTFS partition Disk 0.
After Setup is complete, create a 100 GB partition on Disk 1 and Disk 2.
Mount the partition on Disk 1 and Disk 2 as subdirectories on the Disk 0 partition.

80. You configure a new Windows 2000 Server as an Intranet server. You configure a sales Web site, and a Finance virtual directory in the Departments Web site. Users report that they can only see .htm, and .asp files. For security, you need to disable the users' ability to view the files of all Web sites in the form of a list. What should you do?

A: Clear the Directory Browsing checkbox for the server properties. Apply the settings to the child web sites.

81. You configure a HP JetDirect device with an IP address of 10.4.20.200/16. You want to create and share a printer at a domain controller with an IP address of 10.5.20.50/16 that is connected to the TCP/IP port of the print device. When you enter the IP address of the device, you receive an error message. What should you do?

A: Change the IP address of the print device to 10.5.20.200.

82. Permissions for a shared folder on your NTFS partition are as follows:

Type of permission	Account	Permission
Share	Users	Change
NTFS	Users	Full Control

Users are connected to this folder. You have an immediate need to prevent ten of the files in this folder from being modified. What two actions have the smallest possible effect on users who are using other files on the server? (Choose two)

A: Modify the NTFS permission for the ten files.
Disconnect the users from the Data folder.

83. Your network consists of Windows 2000 Servers. Each has separate system partitions and separate boot partitions formatted as NTFS. After you shut down one of the servers and restart, you receive the error message: "NTLDR is missing. Press any key to restart". You do not want to lose any settings you made since the original installation. What should you do to install a new NTLDR file on the server?

A: Start the computer by using the Windows 2000 Server CD-ROM and choose to repair the installation.
Select the Recovery Console and copy the NTLDR file on the CD-ROM to the root of the system partition.

84. You are planning to install a Windows 2000 Server computer that has a disk controller that is not included in the HCL. You start the computer using the Windows 2000 Server CD-ROM. At the end of the text mode on the restart of the computer, you receive "Inaccessible_Boot_Device". What should you do? (Choose two)

A: Restart Windows 2000 Setup by using the Windows 2000 Server CD-ROM.
Install a driver for the SCSI controller from a floppy disk.

85. What should you do to configure the deployment of an application update so that users automatically install the update when they log on to the domain?

A: Create a Microsoft Windows Installer package for the application update.
Apply the package to a Group Policy.

86. Each of your company's offices has a network of 5 – 20 computers. Employees have a limited knowledge of Windows 2000. You plan to install 50 identical computer with Windows 2000 Server in these offices. You create a Setup Information File that specifies the company's standard configuration. Using the least possible amount of time, how should you automate the installation process?

A: Create a floppy disk that contains only the SIF.
Instruct an employee at each office to start the installation by using the Windows 2000 Server CD-ROM, with the floppy disk inserted.

87. Your network consists of Windows NT Server computers, Windows NT Workstation computers and UNIX computers, in a single Windows NT domain. You are upgrading a Windows NT Server to Windows 2000 Server. It is currently a BDC. The existing DNS server is a UNIX computer that supports SRV (service) records and accepts dynamic updates. Another Windows NT Server serves as a WINS server. You plan on configuring the upgraded server as a domain controller in a new Active Directory forest, with the Windows NT domain accounts upgraded to Active Directory. Other domain controllers will be upgraded after this initial server upgrade. What should you do?

A: Promote the server to the PDC of the domain.
Run Windows 2000 Setup on the server.

88. You are installing Windows 2000 Server on a multiprocessor computer. What should you do to install a customized HAL designed for a computer on which you are installing Windows 2000 Server?

A: During the text mode portion of Windows 2000 Setup, install the customized HAL.

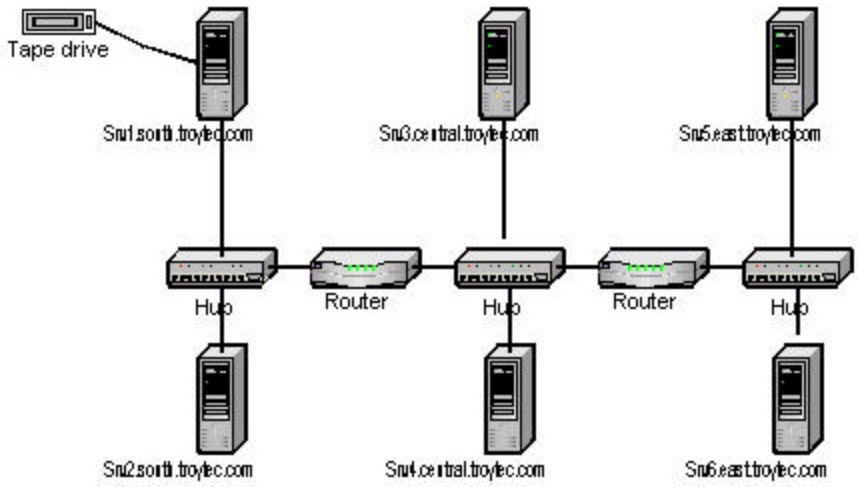
89. Your network consists of Windows 2000 Server computers, and Windows 98 computers. You are installing Windows 2000 Server on a new computer that has one 20 GB hard disk with no partitions defined. The Windows 2000 Server CD-ROM is unavailable, so you are installing Windows 2000 Server from files on a server on the network. You want the entire hard disk of the new computer to be used for the system partition. What should you do?

A: Start the new computer by using a Windows 98 network boot disk
Create and format a single FAT32 partition.
Connect to the network server.
Run WINNT.EXE.

90. Your Windows 2000 Server has five hard disks. Four 100 GB disks are configured as a single striped volume. You want to reconfigure these so that the volume is fault-tolerant, and has as much space as possible. Using only the existing hardware, what should you do?

A: Backup the data on the striped volume, then delete the striped volume.
Create a RAID-5 volume from the four disks.
Restore the data to the new RAID-5 volume.

91. You back up all of the System State data of your network, which has three main segments and six domain controllers to a single tape.



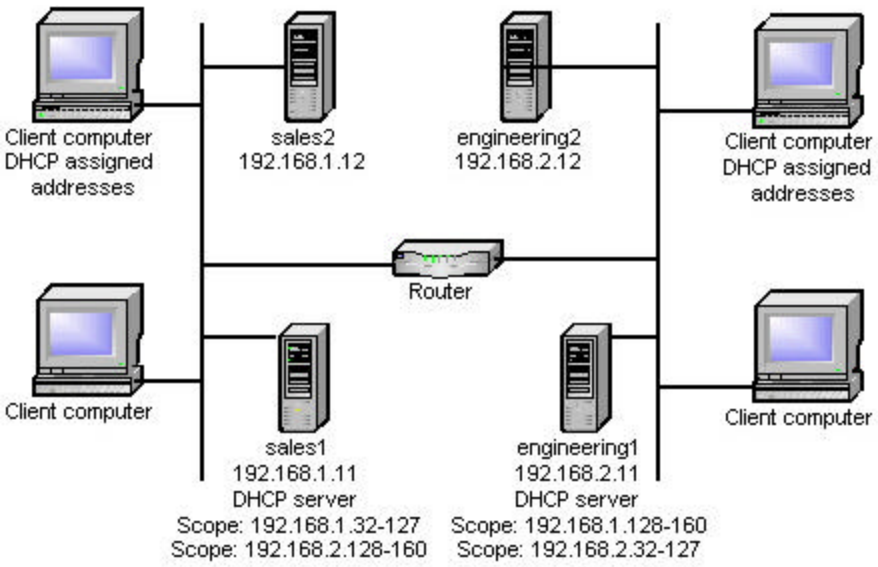
The tape is attached to the Srv1.south.troytec.com computer. To which server can you restore the System State data from Srv1.south.troytec.com? (Choose all that apply)

A: Srv1.south.troytec.com.

92. You configure a remote access server on your TCP/IP network. When users connect to the server, they receive the error message: "IPX/SPX compatible CUSTOMIZED PACKAGE OF INTERNET EXPLORER reported error 733: The PPP control network protocol for the network protocol is not available". If the users allow the connection to continue, they are able to connect to services that use TCP/IP. How should you prevent this message from being displayed?

A: Configure the client computers to use only TCP/IP for the connection to the remote access server.

93. All Windows 2000 Servers in your network use TCP/IP. The sales department uses one subnet, and the engineering department uses another subnet.



The router that joins the two subnets is not RFC 1542 compliant and does not support DHCP/BOOTP relay. What should you do to allow the DHCP servers on sales domain and the engineering domain to support client computers on each other's subnet?

A: On a second Windows 2000 Server computer in each subnet, install and configure the DHCP Relay Agent service.

94. Your company consists of a main office and several branch offices. Each branch office has a private network with a 56-Kbps connection to the Internet. To provide each office with access to the Internet, you will use Network Address Translation. After configuration, you discover that connections cannot be made to sites by using the FQDN, but connections can be made by their IP address. What should you do?

A: Configure the computers on each of the branch office networks with the address of a DNS server on the Internet.

95. You have created a shared printer for your managers so they do not have to wait for their documents to print when the printer queue is large. You set up permissions for the following groups; Administrators, Creator Owner, Everyone, Managers, Print Operators and Server Operators. You select the check box to allow Printer permission for the Managers group. You want only the Administrators, Print Operators, Server Operators, and Managers groups to be able to print to the printer. What should you do?

A: Remove the Everyone group.
Clear all check boxes for the Everyone group.

96. Your Windows 2000 Server network runs in mixed mode. You create and share a new HP LaserJet printer. Your Windows 2000 Professional clients can print to the

new printer successfully, but your Windows NT Workstation clients cannot. You receive the following error message on your NT Workstation clients: "The server on which the printer resides does not have a suitable HP LaserJet printer driver installed. Click on OK if you wish to install the driver on your local machine". What should you do to have the printer driver automatically installed on the Windows NT Workstation computers?

A: Change the sharing options on the printer to install additional drivers for Windows NT or Windows 2000.

97. You suspect someone is trying to log onto your domain by guessing user account names and passwords. What should you do to find out which computers are being used for this?

A: Edit the Default Domain Policy object to audit account logon failures.

98. Your Windows 2000 domain trusts each of your two Windows NT domains, and the Windows NT domains trust the Windows 2000 domain. A Windows 2000 domain controller is configured to use the highly secure domain controller security template. Windows NT users report they cannot access resources on this domain controller. What should you do?

A: Apply a less restrictive custom security template to the domain controller.

99. You are the administrator of the troytec.local domain. You configure the Local Security Options and other options for the Default Domain Policy object. You delegate administration of the New York and Connecticut OUs. What should you do to prevent those administrators from creating any other Group Policy objects with settings that conflict with those you configured?

A: From the Group Policy options for the troytec.local domain, set the option not to override.

100. Your Active Directory single domain consists of Windows NT workstation clients, and Windows 2000 Professional computers. You create a Windows NT default user policy on the Windows 2000 Server computer that is configured as a PDC emulator. It denies access to Network Neighborhood. You install Terminal Services on one of the servers, and Terminal Services Client on the NT Workstation client computers. Users of the Terminal server can still browse the network when they open My Network Places. What should you do to prevent all default users from browsing the network?

A: Create a Windows 2000 Group Policy that denies user access to My Network Places.

101. You have a Windows 2000 Server which serves as a print server. You install a second Plug and Play network adapter to improve network performance. The first

network adapter uses IRQ 11. The second network adapter uses IRQ 5. The server is now unable to print to the print device connected to the non-Plug and Play LPT2 port adapter. What should you do?

A: Edit the CMOS settings on the computer to reserve IRQ 5 for the non-Plug and Play devices.

102. Your Windows 2000 Server is configured with Routing and Remote Access. What can you do to help diagnose why dial-in users cannot connect to the server via a new modem?

A: Use the Routing and Remote Access snap-in to find out whether the ports for both modems are operational.

103. How do you configure the remote Windows 2000 server computers so that whenever a new Microsoft driver becomes available, branch offices are notified automatically when the administrator logs onto the server?

A: Install Windows Critical Update Notification.

104. After you install a new video adapter, one of the users at a remote location reports that Routing and Remote Access does not accept calls. After you resolve the Routing and Remote Access problem, you need to configure the server to prevent users from installing any unsigned device drivers. What two actions should you take in the Driver Signing Options dialog box?

A: Set File Signature Verification to Block.
Select the Apply settings as system default check box.

105. To provide redundancy for all data stored on your RAID-5 disk, you install a second RAID-5 disk array. When you right-click the free space on the new array in Disk Management, you see no option to create a new volume or mirrored volume. What should you do before you create a mirrored volume on the new array?

A: Convert both arrays to dynamic disks.

106. Your network uses the Encrypting File System (EFS) to encrypt data. You are installing a new server that has a 6 GB NTFS partition. You want to move numerous EFS folders to a new server. These folders must maintain their encryption. What should you do?

A: Backup the folder using the Backup utility in Windows 2000.

107. You are implementing a 140-node network. It should be divided into 10 subnets. Each subnet must be able to accommodate up to 14 nodes. How should you configure the IP addressing structure if your company's IP address is 194.194.194.0?

A: 194.194.194.0/28.

108. You have a Pentium III 400 MHz Windows 2000 Server computer with a built-in sound card. You must install another sound card that is on the HCL and enable it on the server. How should you configure the computer to use the new sound card and install the drivers for the sound card? (Choose three)

A: Install the new sound card.
In Device Manager, disable the integrated sound card.
Allow Windows 2000 to automatically detect the new sound card during the next boot of the computer after the sound card is installed.

109. Your Windows 2000 domain operates in native mode. The server uses the default remote access policy. You want the remote access permissions for new user accounts to automatically allow access. What should you do?

A: Change the setting from Control Access through Remote Access Policy to Allow Access.

110. All subnets on your network use a /24 subnet addressing scheme. Your router that connects a subnet to the network has an IP address of 158.25.64.1. The next router in line has an IP address of 158.23.65.2. Which subnet mask and default gateway should you use to configure the client computer?

A: 255.255.255.0
158.25.64.1

111. Your Windows 2000 network is configured with Active Directory and Group Policies. You create a Group Policy object linked to an Organizational Unit. You do not want the GPO to use any policies from the domain. What should you do?

A: Check the "Block Inheritance" box in the main screen of the OU's Group Policy editor.

112. On your Windows 2000 Active Directory domain controller, you are backing up the system boot files, the registry, the COM+ class registration database, the Certificate Server database, the Active Directory Services database, and the SYSVOL directory. Your domain controller is a Pentium 200 MHz with a RAID 5 array with ten 3-GB partitions. Minimizing backup time, how can you backup these files?

A: Use Windows Backup to back up the System State data.

113. How can you assign an application to one processor exclusively?

A: Right-click the application process, select Set Affinity, and select the appropriate processor.

114. You have an Active Directory-enabled Windows 2000 server. You create an Organizational Unit with a child OU named Designers. The child object must have explicit rights assigned to it, but the OU's permissions must propagate to the OU and all its other child objects. What should you do? (Choose all that apply)

A: Configure permission inheritance on the OU.
From the Security tab, clear the Allow Inheritable Permissions From Parent to Propagate To This Object on the Designer's object.

115. You must prevent any unsigned drivers from being installed on any computer in your Windows 2000 network. The network consists of Windows 2000 domain controllers, Windows 2000 file and print servers, and Windows 2000 Professional computers. What should you do?

A: Configure the domain controllers, file and print servers, and client computers to Block unsigned drivers.

116. Your network contains two routed subnets: Subnet A and Subnet B. Subnet B contains a Windows 2000 server configured as a DHCP server. This server has scopes created for both Subnet A and Subnet B. Subnet A does not contain a DHCP server. The clients on Subnet A are not receiving IP addresses from the DHCP server. What can you do to enable clients in Subnet A to receive dynamically assigned IP addresses? (Choose all that apply)

A: Configure an RFC 1542-compliant router to forward BOOTP messaging between subnets.
Configure an RFC 1560-compliant router to pass all UDP traffic on ports 2151, 2152, 2153 and 2154.
Configure a DHCP relay agent on Subnet A to forward DHCP messages to Subnet B.

117. You configure several Group Policies to restrict user's desktop configuration changes. You want them to be applied immediately. What should you do?

A: Run the SECEDIT.EXE command to refresh the policy.

118. On the Windows 2000 computers you install the NWLink IPX/SPX/NetBIOS Compatible Transport Protocol. After installing the protocol you discover that the Windows 2000 machines can communicate with some but not all of the NetWare servers. What should you do?

A: The frame type is not set correctly. Reconfigure the Windows 2000 computers for Manual Frame Detection.

119. You are backing up all of the data on a computer on your network using the following strategy.

Day of the Week	Backup Type
Saturday	Normal Backup
Monday	Differential Backup
Tuesday	Differential Backup
Wednesday	Differential Backup
Thursday	Differential Backup

On Friday at 2:15 PM, you experience a hard drive failure on the computer. What should you do to restore your data?

A: Restore data from Saturday, then Thursday.

120. You wish to install Recovery Console on a computer that has a mirrored volume. How do you do this?

A: Break the mirror, then install the Recovery Console using x:\I386\winnt32.exe /cmdcons. Reestablish the mirrored volume.

121. You are concerned that someone is accessing confidential data files on a Windows 2000 Professional computer. You would like to configure the system so that all attempts to access those files, whether successful or failed, are tracked. What should you do? (Choose all that apply)

A: Right-click on the files to be audited. From the Security tab, click Advanced. From the Auditing tab click Add and select the user or group whose actions you want to audit. In the Local Computer Policy, choose Audit Policy and select the checkboxes for "Success" and "Failure" under "Audit object access".

122. You use Network Address Translation to provide Internet access for the client machines on your network. You have a Windows 2000 Professional machine that you would like to establish a secure Virtual Private Networking session with another Windows 2000 machine at a remote office using L2TP. You are unable to establish an L2TP connection with the remote office, but are successful when you try to connect to another machine in the same office. Why are you unable to connect to the remote office?

A: You cannot establish a L2TP session behind a device performing NAT. The L2TP session fails because the IP Security packets have become corrupted.

123. You are installing a new computer named Svr2.troytec.com on your Windows 2000 network. You want to enter the appropriate TCP/IP addresses for the subnet mask and the default gateway for Svr2.troytec.com. Which subnet mask and default

gateway should you use? To answer, drag the appropriate addresses to the appropriate boxes in the Internet Protocol (TCP/IP) Properties dialog box.

A: Drag 255.255.0.0 to the subnet mask, and the IP address of the router to the default gateway.

Implementing, Managing and Supporting
Windows 2000 Network Infrastructure Concepts

DNS in a Windows 2000 Network Infrastructure

DNS Overview
DNS is the name service for Internet addresses used to translate friendly domain names to numeric IP addresses. Microsoft's web page, http://www.microsoft.com translates to 207.46.130.149. A host computer queries the name of a computer and a domain name server cross-references the name to an IP address.

Windows 2000 clients use DNS for name resolution and locating domain controllers for logon. In the DNS, the clients are resolvers and the servers are name servers. DNS uses three components: resolvers, name servers, and the domain name space. A resolver sends queries to a name server. The name server returns the requested information, a pointer to another name server, or a failure message, if the request cannot be satisfied.

Resolvers
Resolvers pass name requests between applications and name servers. The name request contains a query, such as the IP address of a Web site. The resolver can be built into the application or may be running on the host computer as a library routine.

Name Servers
A name server contains address information about other computers on the network. Name servers are grouped into domains. Access to each computer in a given group is controlled by the same server. If the name server is not able to resolve the request, it can forward the request to another name server.

Root-Level Domains
Domains define levels of authority in a hierarchical structure. The top of the hierarchy is called the root domain. References to the root domain are expressed by a period (**.**).

Top-Level Domains
Top-Level Domains include the following:

Identifier	Organization
arpa	Reverse DNS
com	Commercial organizations
edu	Educational institutions and universities
gov	Nonmilitary government organizations

mil	Military government organizations
net	Networks (the backbone of the Internet)
num	Phone numbers
org	Non-profit organizations
xx	Two-letter country code

Second-Level Domains
Second-level domains contain hosts and other domains, called subdomains.

Host Names
The domain name is used with the host name to create a fully qualified domain name (FQDN). The FQDN is the host name followed by a period (.), followed by the domain name.

Zones
A zone is the administrative unit for DNS. It is a subtree of the DNS database that is administered as a single, separate entity. It can consist of a single domain or a domain with subdomains. The lower-level subdomains of a zone can also be split into separate zones.

Name Server Roles
The minimum number of DNS servers for each zone is two – a primary and a secondary. The existence of both servers provides for database redundancy and a level of fault tolerance.

Primary Name Servers
Primary name servers get the data for their zones from the local DNS database files. When a change is made to the zone data the change must be made on the primary DNS server so that the new information is entered in the local zone file.

Secondary Name Servers
Secondary name servers get their zone data file from the primary DNS server that is authoritative for that zone. Zone transfer is the process of the primary DNS server sending a copy of the zone file to the secondary DNS server. Secondary servers allow for redundancy, quicker access for remote locations, and load balancing. Primary or secondary designation is defined at a zone level because information for each zone is stored in separate files. A particular name server may be a primary name server for certain zones and a secondary name server for other zones.

Caching-Only Servers
Caching-only servers are DNS name servers that perform queries, cache the answers, and return the results. No zone data is kept locally. They contain only information that they have cached while resolving queries. Less traffic is generated between servers because the server is not doing a zone transfer. Caching-only servers can be used if you have a slow connection between sites.

DHCP in a Windows 2000 Network Infrastructure

DHCP Overview

DHCP centralizes and manages the allocation of TCP/IP configuration information by automatically assigning IP addresses to computers configured to use DHCP. Each time a DHCP client starts, it requests IP address information from a DHCP server, including the IP address, the subnet mask, and optional values. The optional values may include a default gateway address, Domain Name System (DNS) address, and Windows Internet Name Service (WINS) server address. When a DHCP server receives a request, it selects IP addressing information from a pool of addresses defined in its database and offers it to the DHCP client. If the client accepts the offer, the IP addressing information is leased to the client for a specified period of time. If there is no available IP addressing information in the pool to lease to a client, the client cannot initialize TCP/IP.

Windows 2000-based clients can automatically configure an IP address and subnet mask if a DHCP server is unavailable at system start time through Automatic Private IP Addressing (APIPA). The Windows 2000 DHCP client service goes through the following process to autoconfigure the client:

- The DHCP client tries to locate a DHCP server and obtain an address.
- If a DHCP server does not respond or cannot be found, the DHCP client autoconfigures its IP address and subnet mask using a selected address from reserved Class B network, 169.254.0.0, with the subnet mask 255.255.0.0.
- The DHCP client then tests for address conflicts. If a conflict is found, the client will retry autoconfiguration for up to 10 addresses.
- Once the DHCP client succeeds in selecting an address, it configures its network interface with the IP address. The client continues to check for a DHCP server every 5 minutes. If a DHCP server is later found, the client will use an address offered by the DHCP server.

Installing and Configuring a DHCP Server

The DHCP Server service must be running to communicate with DHCP clients. Once installed, several options must be configured:

- Install the Microsoft DHCP Server service.
- Authorize the DHCP server.
- Configure a scope or pool of valid IP addresses before a DHCP server can lease IP addresses to DHCP clients.
- Configure Global scope and client scope options for a particular DHCP client.

You should manually configure the DHCP server computer to use a static IP address. The DHCP server cannot be a DHCP client. It must have a static IP address, subnet mask, and default gateway address.

Installing DHCP Server Services

1. Clicking Start, Settings, and Control Panel.

2. Double-click Add/Remove Programs, then click Add/Remove Windows Components.
3. Click Networking Services.
4. Click Details.
5. Under Subcomponents of Networking Services, select Dynamic Host Configuration Protocol (DHCP), click OK, then click Next.
6. Type the full path to the Windows 2000 distribution files and click Continue. Required files will be copied to your hard disk.
7. Click Finish to close the Windows Components Wizard.

Authorizing a DHCP Server

An unauthorized DHCP server may either lease incorrect IP addresses to clients or negatively acknowledging DHCP clients. Clients that obtain a configuration lease from the unauthorized server can fail to locate valid domain controllers, preventing clients from successfully logging on to the network. For the directory authorization process to work properly, it is necessary that the first DHCP server introduced onto your network participate in the Active Directory service. The server must be installed as either a domain controller or a member server. The authorization process for DHCP server computers in Active Directory depends on the installed role of the server on your network; domain controller, member server, or stand-alone server. If Active Directory is deployed, all computers operating as DHCP servers must be either domain controllers or domain member servers.

Authorizing as a DHCP Server in Active Directory

You must log on to the network using an account that has membership in the Enterprise Administrators group that allows you Full control rights to the NetServices container object as it is stored in the Enterprise Root of the Active Directory service.

9. Install the DHCP service on this computer (if necessary).
10. Click Start, Programs, Administrative Tools, then click DHCP.
11. On the Action menu, click Manage Authorized Servers.
12. Click Authorize.
13. When prompted, type the name or IP address of the DHCP server to be authorized, then click OK.

Creating a DHCP Scope

A scope is a pool of valid IP addresses available for lease to DHCP clients. It must be created before a DHCP server can lease an address to DHCP clients. One scope for every DHCP server must be created. Static IP addresses must be excluded from the scope. To centralize administration and to assign IP addresses specific to a subnet, create multiple scopes on a DHCP server. Only one scope can be assigned to a specific subnet. Because DHCP servers do not share scope information, you must ensure that the same IP addresses do not exist in more than one scope to prevent duplicate IP addressing.

Creating a New Scope

1. Click Start, Programs, Administrative Tools, then click DHCP.
2. Click the applicable DHCP server.
3. On the Action menu, click New Scope.
4. Follow the instructions in the New Scope Wizard. After creating a new scope, you need to activate the scope for use or for assigning scope options.

Configuring DHCP for DNS Integration

A Windows 2000 DHCP server can register with a DNS server and update pointer (PTR) and address (A) resource records (RRs) on behalf of its DHCP-enabled clients using the Dynamic DNS update protocol. DHCP option code (Option Code 81) enables the return of a client's FQDN to the DHCP server. The DHCP server can dynamically update DNS to modify an individual computer's RRs with a DNS server using the dynamic update protocol.

Dynamic Updates for Non-Supported Dynamic DNS Updates

1. Click Start, Programs, Administrative Tools, then click DNS.
2. Click the applicable zone.
3. On the Action menu, click Properties.
4. In the DNS Property tab, select Enable Updates For DNS Clients That Do Not Support Dynamic Update.
5. Select Only Secure Updates If Your Zone Type Is Active Directory-Integrated.

Troubleshooting DHCP Clients

Most DHCP-related problems start as a failed IP configuration at a client. If the client is not the clause, check the system event log and DHCP server audit logs. These logs contain the source of the service failure or shutdown. Use the IPConfig TCP/IP utility to get information about the configured TCP/IP parameters on local or remote computers on the network.

DHCP Errors

Symptom	Solution
Invalid IP address configuration	Possible network hardware failure or the DHCP server is unavailable. Verify the client computer has a valid, functioning network connection.
Autoconfiguration problems on the current network	Use the ping command to test connectivity. Manually renew the client lease. If the client hardware appears to be functioning properly, ping the DHCP server from another computer on the same network. Release or renew the client's address lease.
Missing configuration details	DHCP server is not configured to distribute options or the client does not support the options distributed by the server. Verify that the most commonly used and supported options have been configured at either the server, scope, client, or class level of option assignment. Check the DHCP option settings. Check to see if the DHCP server is configured with an incorrect DHCP router option (Option Code 3).

The IP address of the DHCP server was changed	Make sure that the DHCP server IP address falls in the same network range as the scope it is servicing.
DHCP clients unable to receive an address from the server.	A DHCP server can provide IP addresses to client computers on remote multiple subnets only if the router that separates them can act as a DHCP relay agent. Configure a BOOTP/DHCP relay agent on the client subnet. The relay agent can be located on the router itself or on a Windows 2000 Server computer running the DHCP Relay service component.
Multiple DHCP servers exist on the same LAN.	Do not configure multiple DHCP servers on the same LAN with overlapping scopes. The DHCP service, when running under Small Business Server, automatically stops when it detects another DHCP server on the LAN.

Troubleshooting DHCP Servers
Make sure that the DHCP services are running by opening the DHCP service console to view service status, or by opening Services and Applications under Computer Manager.

DHCP Relay Agent
A relay agent is a program that relays DHCP/BOOTP messages between clients and servers on different subnets. For each IP network segment that contains DHCP clients, either a DHCP server or a computer acting as a DHCP relay agent is required.

Adding DHCP Relay Agent

1. Click Start, Programs, Administrative Tools, Routing And Remote Access.
2. Click Server name\IP Routing\General.
3. Right-click General, then click New Routing Protocol.
4. In the Select Routing Protocol dialog box, click DHCP Relay Agent, then click OK.

Remote Access in a Windows 2000 Network Infrastructure

Creating a Remote Access Policy (RAP)
RAPs are used to define who has remote access to the network and what the characteristics of that connection will be. Conditions for accepting or rejecting connections can be based on many different criteria, such as day and time, group membership, and type of service. Remote Access Policies are stored locally in the IAS.MDB file. Policies are created manually on each server. Remote Access Policies are applied to users in a mixed-mode domain. Control Access Through Remote Access Policy is not available on mixed-mode domain controllers. If the user's permission is Allow Access, the user still must meet the conditions set forth in a policy before being allowed to connect.

Creating a New Remote Access Policy

1. Right-click Remote Access Policies using the Routing and Remote Access Administration Tool, and select New Remote Access Policy.
2. Add a friendly name of “Allow Domain Users”, and then click Next.
3. Click Add to add a condition.
4. Select Windows-Groups, then click Add.
5. Click Add, select Domain Users, and then click Add. Click OK.
6. Click OK to exit Groups.
7. Click Next, then select Grant Remote Access Permission.
8. Click Next, then click Finish.

Configuring a Remote Access Profile

The profile specifies what kind of access the user will be given if the conditions match. There are six different tabs that can be used to configure a profile. The tabs are Dial-in Constraints, IP, Multilink, Authentication, Encryption, and Advanced.

Dial-In Constraints

Constraints are configured in the Edit Dial-In Profile dialog box, on the Constraints tab. Possible settings include idle time disconnect, maximum session time, day and time, phone number, and media type.

Enabling IP Routing

1. Right-click Properties from the Routing and Remote Access Manager. Choose enable This Computer as a Router, then click OK.
2. Click Yes at the warning.

Enabling and Configuring a Routing and Remote Access Server

1. Open the Routing and Remote Access Manager.
2. Right-click the machine name and choose Configure and Enable Routing and Remote Access.
3. Click Next in the Routing And Remote Access Server Setup Wizard.
4. Select the Network Router radio button on the Common Configurations page, then click Next.
5. On the Remote Client Protocols page, under Protocols, make sure that TCP/IP is listed, verify that Yes, All The Required Protocols are on This List is selected, then click Next.
6. On the Demand Dial Connections page, make sure that No is specified from You Can Set Up Demand-Dial Routing Connections After This Wizard Finishes, then click Next.
7. Click Finish.

Updating the Routing Tables

The routing table is a series of entries called routes that contain information on where the network IDs of the internetwork are located. The routing table is not exclusive to a router. Hosts (nonrouters) also have a routing table that is used to determine the

optimal route. There are three types of entries in the routing table; network route, host route, and default route.

Implementing Demand-Dial Routing
A demand-dial interface is a router interface that will be brought up on demand based on network traffic. The demand-dial link is only initiated if the routing table shows that this interface is needed to reach the IP destination address. Filters can be set to permit or deny particular source or destination IP addresses, ports or protocols. Time-of-day restrictions can further control access.

Virtual Private Networks
A VPN is the ability to send data between two computers across an internetwork in a manner that mimics the properties of a dedicated private network. VPNs allow users working at home or on the road to connect securely to a remote corporate server using the routing infrastructure provided by a public internetwork such as the Internet.

Routing and Remote Access for DHCP Integration
Routing and Remote Access uses DHCP to lease addresses in blocks of 10, and stores them in the registry. When a Routing and Remote Access address pool is configured to use DHCP, no DHCP packets will go over the wire to the Routing and Remote Access clients. The network information center (NIC) used to lease these DHCP addresses is configurable in the user interface if two or more NICs are in the server. The DHCP leases are released when Routing and Remote Access is shut down.

DHCP Relay Agent
The Routing and Remote Access client will receive an IP address from the Routing and Remote Access server, but may use DHCPINFORM packets to obtain Windows Internet Name Service (WINS) and Domain Name System (DNS) addresses, domain name, or other DHCP options. DHCPINFORM messages are used to obtain option information without getting an IP address.

Configuring a DHCP Relay Agent

1. Right-click General under IP Routing in the Routing and Remote Access Manager. Select New Routing Protocol.
2. Choose DHCP Relay Agent, then click OK.
3. Highlight DHCP Relay Agent, and then right-click Properties. Configure the IP addresses of any DHCP server.
4. Click OK to close the dialog box.
5. Right-click the DHCP Relay Agent and choose New Interface.
6. Select Internal, then click OK.
7. Click OK to close the DHCP Relay Agent Internal Properties dialog box.

Managing and Monitoring Remote Access
IAS can create log files based on the authentication and accounting requests received from the NASs. These logs can be used to track accounting information, such as logon and logoff records, and to help maintain records for billing purposes. You can specify

whether new logs are started daily, weekly, monthly, or when the log reaches a specific size. By default, the log files are located in the %systemroot%\system32\LogFiles folder.

Network Protocols in a Windows 2000 Network Infrastructure

Installing and Configuring TCP/IP

TCP/IP is installed as the default network protocol if a network adapter is detected when you run Windows 2000 Setup.

Installing TCP/IP

1. Click Start, Settings, Network and Dial-Up Connections.
2. Right-click Local Area Connection and then click Properties.
3. Click Install.
4. Click Protocol and then click Add.
5. Click Internet Protocol (TCP/IP), and then click OK.
6. Click Close.

Configuring TCP/IP

TCP/IP network addressing schemes can include either public or private addresses. Devices connected directly to the Internet require a public IP address. InterNIC assigns public addresses to Internet Service Providers (ISPs). ISPs assign IP addresses to organizations when network connectivity is purchased. IP addresses assigned this way are guaranteed to be unique and are programmed into Internet routers in order for traffic to reach the destination host. By configuring private addresses on all the computers on your private network (or Intranet) you can shield your internal addresses from the rest of the Internet. Private addresses are not reachable on the Internet because they are separate from public addresses, and they do not overlap. You can assign IP addresses in Windows 2000 dynamically using Dynamic Host Configuration Protocol (DHCP), address assignment using Automatic Private IP Addressing or configuring TCP/IP manually.

Dynamic Configuration

Windows 2000 computers will attempt to obtain the TCP/IP configuration from a DHCP server on your network by default. If a static TCP/IP configuration is currently implemented on a computer, you can implement a dynamic TCP/IP configuration.

1. Click Start, Settings, Network And Dial-Up Connections.
2. Right-click the Local Area Connection, and then click Properties.
3. On the General tab, click Internet Protocol (TCP/IP), and then click Properties.
4. Click Obtain An IP Address Automatically, and then click OK.

Manual Configuration

Some servers, such as DHCP, DNS, and WINS servers should be assigned an IP address manually. If you do not have a DHCP server on your network, you must configure TCP/IP computers manually to use a static IP address.

Configuring TCP/IP to use Static Addressing

1. Click Start, Settings, Network and Dial-Up Connections.
2. Right-click Local Area Connection, and then click Properties.
3. On the General tab, click Internet Protocol (TCP/IP), and then click Properties.
4. Select Use the Following IP Address.
5. Type in an IP, subnet mask, and default gateway address. If your network has a DNS server, you can set up your computer to use DNS.

Automatic Private IP Address Assignment

Automatic Private IP Addressing automates the process of assigning an unused IP address when DHCP is not available. The Automatic Private IP Addressing address is selected from the Microsoft reserved address block 169.254.0.0, with the subnet mask 255.255.0.0. The assigned IP address is used until a DHCP server is located.

Testing TCP/IP with IPConfig and Ping

You can perform basic TCP/IP configuration and connectivity testing using IPConfig and ping utilities. IPConfig verifies the TCP/IP configuration parameters on a host, including the IP address, subnet mask, and default gateway. This can determine whether the configuration is initialized, or if a duplicate IP address is configured. The ping utility diagnostic tool tests TCP/IP configurations and diagnoses connection failures. Ping uses the Internet Control Message Protocol (ICMP) Echo Request and Echo Reply messages to determine whether a particular TCP/IP host is available and functional.

Configuring TCP/IP packet filters

IP packet filtering can be used to trigger security negotiations for a communication based on the source, destination, and type of IP traffic. You can define which specific IP and IPX traffic triggers will be secured, blocked, or allowed to pass through unfiltered. IP packets can be filtered on the TCP port number, the UDP port number, and the IP protocol number.

NWLink and Windows 2000

NWLink must be installed if you want to use Gateway Service for NetWare or Client Services for NetWare to connect to NetWare servers. Use Client Services for NetWare or Novell Client for Windows 2000 to log on to a NetWare network from a Windows 2000 Professional-based computer.

Configuring Client Services for NetWare

When you install Client Services for NetWare on a Windows 2000 Professional, the NWLink IPX/SPX/NetBIOS Compatible Transport Protocol is automatically installed. To install Client Services for NetWare, you need Administrator rights to the computer running Windows 2000 Professional. Microsoft Unattended Setup Mode can be used for large deployments of Windows 2000 Professional and Client Services for NetWare.

Installing Client Services for NetWare

1. Click Start, Settings, Network and Dial-Up Connections.
2. Right-click the Local Area Connection, then click Properties.
3. In the General tab, click Install.
4. In the Select Network Component Type dialog box, click Client, then click Add.
5. In the Select Network Client dialog box, click Client Services for NetWare, then click OK.

Installing NWLink

1. Click Start, Settings, Network And Dial-Up Connections.
2. Right-click a Local Area Connection, then click Properties.
3. In the General tab, click Install.
4. In the Select Network Component Type dialog box, click Protocol, then click Add.
5. In the Select Network Protocol dialog box, click NWLink IPX/SPX/NetBIOS Compatible Transport Protocol, then click OK.

Configuring NWLink

You must first install the NWLink IPX/SPX/NetBIOS Compatible Transport Protocol and be a member of the Administrators group.

1. Click Start, Settings, Network And Dial-Up Connections.
2. Right-click a Local Area Connection, then click Properties.
3. In the General tab, click NWLink IPX/SPX/NetBIOS Compatible Transport Protocol, then click Properties.
4. In the General tab, type a value for Internal Network Number or leave this setting at the default value of 00000000.
5. If you want Windows 2000 to automatically select the frame type, click Auto Frame Type Detection, and then click OK. Skip Steps 6 through 9.
6. To manually set the frame type, click Manual Frame Type Detection.
7. Click Add.
8. In the Manual Frame Detection dialog box, in Frame Type, click a frame type.
9. In Network Number, type a network number, then click Add, then click OK.

Configuring and Troubleshooting Network Protocol Security

Configuring and Troubleshooting IPSec

IPSec protects IP packets, and provides a defense against network attacks through the use of cryptography-based protection services, security protocols, and dynamic key management. IPSec can be used to filter data packets on a network.

Implementing IPSec

You can view the default IP Security policies in the Group Policy snap-in to MMC. The policies are listed under IP Security Policies on Active Directory: Group Policy Object\Computer Configuration\Windows Settings\Security Settings\IP Security

Policies on Active Directory. You can also view IPSec policies by using the IP Security Policy Management snap-in to MMC. Each IPSec policy is governed by rules that determine when and how the policy is applied. Right-click a policy and select Properties. The Rules tab lists the policy rules. Rules can be further subdivided into filter lists, filter actions, and additional properties. The default snap-in is started from the Administrative Tools menu; this allows configuration of the local computer only. To centrally manage policy for multiple computers, add the IP Security Management snap-in to an MMC.

Configuring IPSec Policies

There are three predefined policy entries: Client (Respond Only), Secure Server (Require Security), and Server (Request Security). By default, none of these policies are enabled.

Respond Only

The Client (Respond Only) policy allows communications in plain text but will respond to IPSec requests and attempt to negotiate security. It uses Kerberos V5 for authentication.

Request Security

The Server (Request Security) policy causes the server to attempt to initiate secure communications for every session. If a client who is not IPSec-aware initiates a session, it will be allowed.

Require Security

The Secure Server (Require Security) policy requires Kerberos trust for all IP packets sent from the computer, with the exception of broadcast, multicast, Resource Reservation Setup Protocol (RSVP), and ISAKMP packets. This policy does not allow unsecured communications with clients. Any clients who connect to a server must be IPSec-aware.

Authentication Methods

Windows 2000 supports three authentication methods:

- **Kerberos.** The Kerberos V5 security protocol is the default authentication technology. The Kerberos protocol issues tickets, or virtual proof-of-identity cards, when a computer logs on to a trusted domain. This method can be used for any clients running the Kerberos V5 protocol (whether or not they are Windows-based clients) who are members of a trusted domain.
- **Certificates.** This requires that at least one trusted certificate authority (CA) has been configured. Windows 2000 supports X.509 Version 3 certificates, including CA certificates generated by commercial certifying authorities. A rule may specify multiple authentication methods. This ensures that a common method can be found when negotiating with a peer.
- **Preshared Key.** This is a shared key that is secret and is previously agreed on by two users. It is quick to use and does not require the client to run the Kerberos protocol or have a public key certificate. Both parties must

manually configure IPSec to use this preshared key. This is a simple method for authenticating non-Windows-based hosts and stand-alone hosts.

IPSec Policies and Rules
An IPSec policy is a collection of rules and key exchange settings. The policy may be assigned as a domain security policy or an individual computer's security policy. A domain computer will automatically inherit the IPSec policy assigned to the domain security policy when it logs on to the domain. If a computer is not connected to a domain, IPSec policies are stored in and retrieved from the computer registry. One security policy can be created for all users on the same network or all users in a particular department. IPSec policies are created with the IPSec Management snap-in for a Windows 2000 member server.

Rules
Rules govern how and when IPSec is used. A rule contains a list of IP filters and specifies the security actions that will take place when a filter match occurs. A rule is a collection of IP filters, negotiation policies, IP tunneling attributes, adapter types and authentication methods. Each policy may contain multiple rules.

Monitoring and Troubleshooting Tools
IP Security Monitor (IPSECMON.EXE), monitors IP SAs, rekeys, negotiation errors, and other IP Security statistics.

Using Network Monitor
Network Monitor captures all information transferred over a network interface at any given time. Network Monitor version 2.0 contains parsers for IPSec packets. If IPSec is encrypting the packets, then the contents will not be visible, but the packet itself will. If only authentication is being used, the entire packet, including its contents, will be visible.

WINS in a Windows 2000 Network Infrastructure

Resolving NetBIOS Names with WINS
When a client needs to contact another host on the network, it first contacts the WINS server to resolve the IP address using mapping information from the database of the server. The relational database engine of the WINS server accesses an indexed sequential access method (ISAM) database. The ISAM database is a replicated database that contains NetBIOS computer names and IP address mappings. For a WINS client to log on to the network, it must register its computer name and IP address with the WINS server. This creates an entry in the WINS database for every NetBIOS service running on the client. Because these entries are updated each time a WINS-enabled client logs on to the network, information stored in the WINS server database remains accurate.

Installing WINS
1. In Control Panel, double-click Add/Remove Programs.

2. Click Add/Remove Windows Components.
3. Under Components, click Networking Services, then click Details.
4. Select the Windows Internet Name Service (WINS) check box, click OK, then click Next.

Using Static Mappings

Mapped name-to-address entries can be added to WINS in either of two ways: dynamically or manually. Dynamically, WINS-enabled clients directly contact a WINS server to register, release, or renew their NetBIOS names in the server database. Manually, an administrator uses the WINS console or command-line tools to add or delete statically mapped entries in the server database.

Troubleshooting WINS

Initially, verify that the appropriate services are running from either the WINS server or WINS client. Failed name resolution is the most common WINS client problem. When name resolution fails at a client, verify if the client computer is able to use WINS, and is it correctly configured. If the WINS server does not respond to a direct ping, check network connectivity between the client and the WINS server. The inability to resolve names for clients is the most common WINS server problem. When a server fails to resolve a name for its clients, the failure most often is discovered by clients with "Name not found" error messages, or the server sending a positive response back to the client, but the information contained in the response is incorrect. Use Event Viewer or the WINS management console to see if WINS is currently running. If WINS is running on the server, search for the name previously requested by the client to see if it is in the WINS server database. If the WINS server is failing or registering database corruption errors, use WINS database recovery techniques to restore WINS operations. You can back up the WINS database by using the WINS administrative console. To do this, specify a backup directory for the database, and then WINS will execute database backups. By default, backups are performed every three hours. To restore a local server database, replicate data back from a replication partner. If the corruption is limited to a certain number of records, you can repair them by forcing replication of uncorrupted WINS records. This will remove the affected records from other WINS servers. If changes are replicated among WINS servers quickly, restore a local WINS server database by using a replication partner.

Configuring WINS Replication

Replicating databases enables a WINS server to resolve NetBIOS names of hosts registered with another WINS server. To replicate database entries, each WINS server must be configured as either a pull or a push partner with at least one other WINS server. A push partner is a WINS server that sends a message to its pull partners notifying them when its WINS database has changed. When a WINS server's pull partners respond to the message with a replication request, the WINS server sends a copy of its new database entries (replicas) to its pull partners. A pull partner is a WINS server that requests new database entries (replicas) from its push partners. This is done by requesting entries with a higher version number than the last entries it

received during the last replication. Database replication requires that you configure at least one push partner and one pull partner. The four methods of starting the replication of the WINS database are:

1. **At system startup.** Once a replication partner is configured, by default, WINS automatically pulls database entries each time WINS is started. The WINS server can also be configured to push on system startup.
2. **At a configured interval**, such as every eight hours.
3. When a WINS server has reached a **configured threshold** for the number of registrations and changes to the WINS database.
4. By **forcing replication** in the WINS administrative console.

WINS Automatic Replication Partners

The WINS server can be configured to automatically find other WINS servers on the network by multicasting to the IP address 224.0.1.24, if your network supports multicasting. This multicasting occurs by default every 40 minutes. Any WINS servers found on the network are automatically configured as push and pull replication partners, with pull replication set to occur every two hours. If network routers do not support multicasting, the WINS server will find only other WINS servers on its subnet. Automatic WINS server partnerships are turned off by default. To manually disable this feature, use the Registry Editor to set UseSelfFndPnrs to 0 and McastIntvl to a large value.

Backing Up the WINS Database

The WINS console provides backup tools so that you can back up and restore the WINS database. When WINS backs up the server database, it creates a \Wins_bak\New folder under the backup folder you have specified as the Default backup path in Server Properties. By default, the backup path is the root folder on your system partition. After you specify a backup folder for the database, WINS performs complete database backups every three hours using the specified folder. WINS can also be configured to back up the database automatically when the service is stopped or the server computer is shut down.

IP Routing in a Windows 2000 Network Infrastructure

Overview of Routing

Each packet sent over a LAN has a packet header that contains source and destination address fields. Routers match packet headers to a LAN segment and choose the best path for the packet, optimizing network performance. A routing table contains entries with the IP addresses of router interfaces to other networks that it can communicate with. A routing table is a series of entries, called *routes*, that contain information on where the network IDs of the internetwork are located.

Routing Protocols

Dynamic routing is a function of routing protocols, such as the Routing Information Protocol (RIP) and Open Shortest Path First (OSPF). Routing protocols periodically

exchange routes to known networks among dynamic routers. If a route changes, other routers are automatically informed of the change. You must have multiple network adapters (one per network) on a Windows 2000 Server or Windows 2000 Advanced Server. In addition, you must install and configure Routing and Remote Access because dynamic routing protocols are not installed by default when you install Windows 2000.

Routing Information Protocol (RIP)

RIP is a distance-vector routing protocol provided for backwards-compatibility with existing RIP networks. RIP allows a router to exchange routing information with other RIP routers to make them aware of any change in the internetwork layout. RIP broadcasts the information to neighboring routers, and sends periodic RIP broadcast packets containing all routing information known to the router. These broadcasts keep all internetwork routers synchronized.

Open Shortest Path First (OSPF)

OSPF is a link-state routing protocol that enables routers to exchange routing information and create a map of the network that calculates the best possible path to each network. Upon receiving changes to the link state database, the routing table is recalculated. As the size of the link state database increases, memory requirements and route computation times increase. OSPF divides the internetwork into collections of contiguous networks called areas. Areas are connected to each other through a backbone area. A backbone router in OSPF is a router that is connected to the backbone area. Backbone routers include routers that are connected to more than one area. Backbone routers do not have to be area border routers. Routers that have all networks connected to the backbone are internal routers. Each router only keeps a link state database for those areas that are connected to the router. Area Border Routers (ABRs) connect the backbone area to other areas.

Installing, Configuring, and Troubleshooting Network Address Translation (NAT)

Network Address Translation

NAT enables private IP addresses to be translated into public IP addresses for traffic to and from the Internet. It allows computers on a network to share a single Internet connection with only a single public IP address. The computer on which NAT is installed can act as a network address translator, a simplified DHCP server, a Domain Name System (DNS) proxy, and a Windows Internet Name Service (WINS) proxy. NAT allows host computers to share one or more publicly registered IP addresses, helping to conserve public address space.

Certificate Services

Overview of Certificates

A certificate is a digital document that verifies that the public key contained in the certificate actually belongs to the entity named in the certificate. Certificate Services

includes two policy modules that permit two classes of CAs: Enterprise CAs and Stand-Alone CAs. The policy modules define the actions that a CA can take when it receives a certificate request, and can be modified if necessary.

Enterprise CAs
In an enterprise, the enterprise root CA is the most trusted CA. There can be only one enterprise root CA in any given hierarchy, but there can be more than one enterprise root CA in a Windows 2000 domain. All other CAs in the hierarchy are enterprise subordinate CAs.

Stand-Alone CAs
An organization that issues certificates to users or computers outside the organization should install a stand-alone CA. As with Enterprise CAs, there can be only one stand-alone CA per hierarchy, but multiple Stand-Alone CAs can exist. All other CAs in a hierarchy are either stand-alone subordinate CAs or enterprise subordinate CAs. A stand-alone CA has a simple default policy module. It does not store any information remotely.

Installing a Stand-Alone Subordinate CA

1. From Control Panel, select Add/Remove Programs.
2. Click Add/Remove Windows Components.
3. Check the box next to Certificate Services, then click Next.
4. Select Stand-Alone Root CA, then click Next.
5. Fill in the CA identifying information. For CA name, type ComputernameCA. Click Next.
6. Use the default data storage locations, then click Next.
7. During the CA installation process, you will need to give the location of the CERTSRV.* installation files.
8. Click Finish.
9. Close the Add/Remove Programs window.

Requesting and Installing a Certificate From The Local CA

1. Run Certificate Authority Manager.
2. Run Internet Explorer and connect to *http://<your_server>/certsrv/default.asp*.
3. Request a Web browser certificate. The request will be pending. Close Internet Explorer.
4. Open Certificate Authority and select the Pending Requests folder. Right-click your request and choose Issue from the All Tasks menu.
5. In the left pane select the Issued Certificates folder, your request has been issued.
6. Run Internet Explorer, connect to *http://<your_server>/certsrv/default.asp*, check on the Pending Certificate Request, then install the certificate.
7. From the Tools menu, click Internet Options, Content, then Certificates.

Revoked Certificates

When a certificate is marked as revoked, it is moved to the Revoked Certificates folder. The revoked certificate will appear on the CRL the next time it is published. Certificates revoked with the reason code Certificate Hold can be unrevoked, left on Certificate Hold until they expire, or have their revocation reason code changed. This is the only reason code that allows you to change the status of a revoked certificate.

EFS Recovery Policy

EFS requires an encrypted data recovery agent policy before it can be used. Only members of the Domain Administrators group can designate another account as the recovery agent account. If there are no domains, the computer's local Administrator account is the default recovery agent account. A recovery agent account is used to restore data for all computers covered by the policy. If a user's private key is lost, a file protected by that key can be backed up, and the backup sent by means of secure e-mail to a recovery agent administrator. The administrator restores the backup copy, opens it to read the file, copies the file in plain text, and returns the plain text file to the user using secure e-mail again. As an alternative, the administrator can go to the computer that has the encrypted file, import his or her recovery agent certificate and private key, and perform the recovery locally.

Implementing and Administering a Microsoft Windows 2000 Network Infrastructure Exam Questions

1. **You configure your Windows 2000 Server to route all network traffic on your Intranet. Users on both segments need access to files on the other segment. The route table shows:**

Network Destination	Subnet Mask	Gateway	Interface	Metric
10.0.0.0	255.0.0.0	10.0.0.169	10.0.0.169	1
10.0.0.169	255.255.255.255	127.0.0.1	127.0.0.1	1
192.168.0.0	255.255.0.0	192.168.0.200	192.168.0.200	1
192.168.0.200	255.255.255.255	127.0.0.1	127.0.0.1	1

You install and start IIS Web Service on the server. Users on both segments report that they cannot access the Web service. What must you do?

A: Disable all TCP/IP port filters.

2. **Your company policy is to allow only Administrators in your Houston office to install and use Network Monitor. You have been informed that Administrators in New York are installing and using Network Monitor. After you install Network Monitor, what should you do to monitor how many copies of Network Monitor are currently running? (Choose two)**

A: On the Tools menu in Network Monitor select Identify Network Monitor Users. Install Network Monitor on a computer on the second segment.

3. **Your network has 1,900 hosts, and requires Internet connectivity. Your network is not routed, except for the connection to the Internet. You have been assigned the following eight network addresses from your ISP:**

192.24.32.0/24
192.24.33.0/24
192.24.34.0/24
192.30.35.0/24
192.30.36.0/24
192.30.37.0/24
192.30.38.0/24
192.30.39.0/24

Your goal is to minimize the complexity of the routing tables, while maintaining Internet connectivity for all hosts. What subnet mask should you use?

A: 255.255.248.0

4. **On your Windows 2000 Server, you install Client Services for NetWare and NWLink with the default settings. How should you configure your Windows 2000 server to connect to all NetWare servers, regardless of their version?**

   A: Set the adapter to Manual Frame Type Detection. Add the frame type of each NetWare server.

5. **You are planning to migrate your 100 network computers from IPX/SPX to TCP/IP and establish connectivity with the Internet. Your ISP assigns the address 192.168.16.0/124 to your network. You require 10 subnets with at least 10 hosts per subnet. What subnet mask should you use?**

   A: 255.255.255.240.

6. **Your network consists of Windows 2000 Server computers, Windows 2000 Professional computers, and one NetWare server. Administrators must have complete access to the Sys volume on the NetWare server. All other users should have read only access. Configuring Gateway Service for NetWare on a Windows 2000 Server computer, what should you do to configure the appropriate access to the NetWare server? (Choose two)**

   A: Add the NT Gateway User Account to the NTGateway Group on the NetWare server.
   Grant Full Control permission to Administrators and Read permission to users on the Windows 2000 Server computer.

7. **Your network has two Windows 2000 based WINS servers. How should you configure the network to automatically backup the WINS database of both WINS servers?**

   A: Configure the General properties of the WINS server to specify a default backup path in the WINS console on both WINS servers.

8. **Your network has three Windows 2000 based WINS servers. How should you perform a manual compaction of the WINS database on one of the WINS servers?**

   A: Stop the server's WINS server. Use the jetpack command line tool to compact the WINS database. Restart the server's WINS server.

9. **Your network contains 12 Windows 2000 Servers and 100 Windows 2000 Professional computers distributed across the four subnets connected by a router. The servers are used to serve file and print resources to the clients. You install the WINS Server service on a server on one subnet. You configure the WINS option in a DHCP scope to configure all of the other computers on the network to register with and query the WINS server for NetBIOS name resolution. Users on**

the remote subnets report that they cannot access resources located on the WINS server by NetBIOS name. Other TCP/IP connectivity is not affected. Users located on the same subnet as the WINS server are not having any problems. What should you do?

A: Configure the WINS server to include its own IP address as a WINS client computer.

10. **You use a computer running Windows 2000 Server and the DHCP Server service to create a DHCP scope with a lease length of 15 days and a subnet mask of 21 bits. You now want to reconfigure the scope to have an unlimited lease and a subnet mask of 28 bits. What steps must you take?**

    A: Delete the scope. Use the new scope wizard to create a new scope with a subnet mask of 28 bits. Edit the properties of the new scope to set an unlimited lease. Activate the new scope.

11. **Administrators of your Sales organizational unit want to be able to manage EFS for the users in their department. These administrators belong to a group named SalesAdmin which has full administrative privileges to the OU. You install an Enterprise Certificate Authority for use by the entire company. However, the administrators of the Sales department notify you that they are unable to create a Group Policy that allows them to manage EFS for their department. What should you do? (Choose two)**

    A: Add a new policy setting for an EFS Recovery Agent certificate in the Certification Authority console for the CA.
    Grant the enroll permission to the SalesAdmin group for the Recovery Certificate Template.

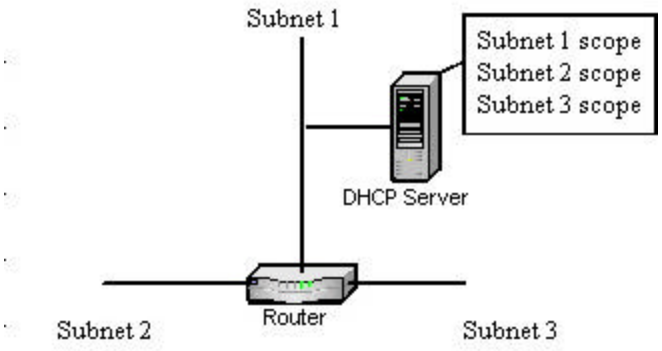
12. **Your network consists of 90 client computers and 50 portable computers. Computers in your network only run Windows 2000 Professional. Only 20 of the users of the portable computers will ever be in the office at the same time. You have purchased a subnetted Class B subnet with a 25-bit mask to accommodate the number of users for your network. All users need access to the Internet while in the office. How should you configure DHCP?**

    A: Create one scope that has two user classes, each with a different lease duration.

13. **You install the Windows 2000 DHCP server service on a member server in your Windows 2000 domain. The domain contains only Windows 2000 Professional computers. The DHCP server is located on the same network segment as the Windows 2000 Professional computers. You create and activate a DHCP scope for the network segment. The Windows 2000 Professional computers are configured as DHCP client computers but they do not receive IP addresses. What should you do so that each DHCP client computer receives an IP address?**

A: Authorize the DHCP server in Active Directory.

14. **Your network consists of three network segments connected by a router. You install the DHCP Server service on a Windows 2000 Server computer. You create scopes for each subnet's range of addresses and activate each scope. Users from the second and third subnet report that they cannot connect to the network. Users from the first subnet report no connectivity problems. After investigation, you realize that computers on subnets 2 and 3 are not receiving a TCP/IP configuration from the DHCP server. What should you do?**



A: Install the DHCP Relay Agent service on a computer on each remote subnet.

15. **All client computers in your domain are Windows 98 computers or Windows 2000 computers. Windows 2000 users run an Internet application that accesses files from a Windows NT computer. None of your Windows 2000 computers can connect to this Windows NT computer, but it can connect to every Windows 2000 computer. What should you do?**

A: Select the Enable Updates for DNS Clients That Do Not Support Dynamic Update check box.

16. **Your network consists of two Windows 2000 Server computers, and 75 Windows 2000 Professional computers. One server is a DHCP server which provides TCP/IP configuration to all of the Windows 2000 Professional computers. You want to allow your help desk support personnel to have only Read access to the DHCP console and the DHCP leases information. What should you do?**

A: Place the global group of the help desk support personnel in the DHCP Users group.

17. **Your network consists of two Windows 2000 Server computers and 50 Windows 2000 Professional computers. You configure your DHCP server to automatically update your DNS server's forward and reverse lookup zone files with the DHCP client information. In the reverse lookup zone, some of the client computers are**

referenced by PTR (pointer) records. But, there are no PTR records for the remaining client computers. What should you do?

A: Configure the DHCP server to always update DNS, even if a client computer does not request it.

18. **Your network consists of a single Windows 2000 domain and uses TCP/IP. You use DHCP to assign addresses to your Windows 2000 Professional client computers. You add several new Windows 2000 Professional client computers to your network. Users report that occasionally they cannot access network resources located on servers, but workgroup resources are sometimes available. The TCP/IP configuration of a computer that is experiencing this problem shows that it is using the address 169.254.0.16 – an invalid address in your network. What should you do?**

    A: Add enough new addresses to the existing DHCP scope to include the new client computers.

19. **You install Certificate Services on two computers running Windows 2000 Server. CertRoot is an Enterprise Root Certificate Authority. CertSub is an Enterprise Subordinate CA. You have two domains: troytec.com and suppport.troytec.com. You add a new domain, products.troytec.com. You attempt to issue a certificate from CertSub for a user account in products.troytec.com. The Event Viewer shows the CA was unable to publish a certificate for products.troytec.com\DC. DC is a domain controller for products.troytec.com. What is the most likely reason you receive this error message?**

    A: CertSub is not a member of the group products.troytec.com\Cert Publishers.

20. **All client computers in your domain use DHCP for their TCP/IP configuration. Your network Administrator installs a new T1 line and router for Internet access. This router is to be used by administrative staff only. You want to configure the administrative staff's client computers to use this new router, and ensure that non-administrative staff cannot gain Internet access through the router. You must ensure that each targeted client computer will only need to be configured once. What should you do?**

    A: Use the route add – p command at each administrative client computer to enter new router information.

21. **Your network consists of two locations containing a Windows 2000 Server computer and 45 Windows 2000 Professional computers. The two servers are Windows 2000-based routers. Although the two routers are not connected directly to each other, they are connected to a third router. This third router is administered by a different company. Users in both locations want to provide multicast-based datacasting of information to the other location. You add the**

Internet Group Management Protocol (IGMP) routing protocol to both servers. However, the third router does not support multicast forwarding or routing. How should you configured the network to allow IP multicast traffic to pass between the two locations?

A: Create an IP-in-IP interface between the servers.
Assign the interface to the IGMP routing protocol.
Run the interface in IGMP proxy mode.

22. Your network is connected to the company network via a Windows 2000 Routing and Remote Access two-way demand-dial connection over ISDN. The ISDN link must only be used once each day to transfer sales information to or from the main office during non-business hours. Several times a day, an ISDN link is initiated between the networks. You analyze the traffic and discover that it is composed of router announcement broadcasts. What should you do to prevent the link from being used during business hours? (Choose two)

A: Schedule the demand-dial interface to dial only during specified hours.
Create a demand-dial filter on the interface.

23. Your network has one primary internal and external DNS server. It has secondary DNS servers that transfer zone information from the primary external DNS server. The secondary DNS servers are installed on two Windows 2000 Server computers and one Windows NT Server 4 0 computer. The primary external DNS server has only a limited number of resource records in its zone file, and is used to host records for your company's Web and mail servers. The Web server and the mail server have static IP addresses. When you monitor the secondary DNS servers by using System Monitor, you notice a high number of hits when monitoring the counter DNS: Zone Transfer SOA Requests Sent. How should you minimize the bandwidth that is required for this traffic? (Choose two)

A: Configured the notify list on the primary external DNS server to notify the secondary DNS servers when there are changes to be replicated.
Increase the value of the Refresh interval in the SOA record.

24. You have three Windows 2000 domain controllers in a single domain. Your primary DNS server is installed on a domain controller named dc1.troytec.com. You have two secondary DNS servers installed on member servers named srvl.troytec.com and srv2.troytec.com. You want to increase fault tolerance for your DNS infrastructure. You also want to optimize and simplify replication and zone transfer management on your network. What should you do?

A: Remove the DNS server service from the member servers. Install the DNS server service on the DCs. Convert the zone to an Active Directory integrated zone.

25. **You configure DHCP to dynamically update the PTR record for clients who lease addresses from the server. From where is the domain name to be used in the PTR record obtained?**

    A: From the DHCPREQUEST message.

26. **Your network consists of one Windows 2000 domain named troytec.local. You want to ensure that internal name resolution traffic never passes outside the network. External name requests must be handled by an external DNS server. What should you do?**

    A: Delete the root zone for your local namespace and configure all internal DNS servers to forward name resolution requests to the external DNS server.

27. **Your internal DNS server is located behind a firewall. When you test this DNS server the DNS server passes the simple test but fails the recursive test. What should you do to resolve this problem?**

    A: Copy the Systemroot\system32\dns\samples\cache.dns file to the Systemroot\system32\dns\cache.dns file.

28. **Your network consists of computers running Windows 2000 Server, Windows 2000 Professional, Windows 95, and OS/2 with LAN Manager 2.2c. All are on the same subnet. You want applications on the OS/2 client that use NetBIOS names to be able to resolve the NetBIOS names to IP addresses from a WINS database. You install WINS on one of the computers that is running Windows 2000 Server. What should you do to enable applications on the computer running OS/2 to resolve names to IP addresses from the WINS database?**

    A: Configure one of the computers running Windows 2000 Professional as a WINS proxy.

29. **Your network consists of one Windows 2000 domain. All servers and client computers are running Windows 2000. You have configured your DNS standard primary zone to include the addresses of all of your servers. After adding new member servers to your network, users report that they can find these servers in the directory, but cannot access them. What should you do?**

    A: Set the Allow Dynamic Updates setting for the DNS standard primary zone to Yes.

30. **Your Windows 2000-based network has three subnets. SubnetA is at the corporate headquarters. SubnetB is used to connect a router at the headquarters office to a router at the remote office. The remote office has one subnet called SubnetC. You use two computers running Windows 2000 Server as routers: RouterAB connects SubnetA and SubnetB. RouterBC connects SubnetB and SubnetC. You configure RouterAB and RouterBC to communicate using demand-**

dial connections. What two steps should you take to allow a user whose computer is on SubnetC to access a share on a computer on SubnetA?

A: Configure a static route for SubnetA on the demand-dial interface of RouterBC.
Configure a static route for SubnetC on the demand-dial interface of RouterAB.

31. Your DNS server runs on Windows 2000 Server, and provides name resolution within your Internet domain. You have five Web servers to handle company information and client reservations. Each Web server is configured to maintain exactly the same content as all the other Web servers. All the Web servers respond to the same host name. Customers are complaining about response times from your Web server. After monitoring your Web servers, you discover that four of the servers are idle. In the DNS Management console, what should you do to ensure load balancing and improve response times? (Choose two)

A: Verify that A (host) records have been created for each Web server.
Enable Round Robin in the DNS server's properties.

32. You are configuring a Windows 2000 network for dial-up access. Your company issues smart cards to all users who have dial-up access. What should you do to configure your Routing and Remote Access server? (Choose two)

A: Select the Extensible Authentication Protocol (EAP) check box.
Install a smart card logon certificate on the Routing and Remote Access server.

33. Your domain has a Windows 2000 member server computer named Srv1. Routing and Remote Access and CHAP is enabled for remote access on Srv1. You have also configured the appropriate remote access policy to use CHAP. However, users who require CHAP report that they are not able to dial in to Srv1. What should you do?

A: Configure Srv1 to disable LCP extensions.

34. You are configuring your users' portable computers to allow users to connect to the company network by using Routing and Remote Access. You test the portable computers on the LAN and verify that they can successfully connect to resources on the company network by name. When you test the connection through Remote Access all of the portable computers can successfully connect but they cannot access files on computers on different segments by using the computer name. What should you do to resolve this problem?

A: Install the DHCP Relay Agent on the Remote Access server.

35. Your domain has a Windows 2000 member server computer named London and a DHCP server. Routing and Remote Access is enabled for remote access on London. The domain is in native mode. Users in the domain dial in to the network

by using Windows 2000 Professional portable computers. Dial-up connection configuration for the Windows 2000 Professional computers is set to obtain an IP address automatically. You do not want to change this configuration. You want to designate a fixed IP address for each of the users. All users should receive a different fixed IP address when a dial-up connection is made. How should you configure the network to accomplish this goal?

A: In the Active Directory Users and Computers console, assign a static IP address for each user.

36. **You configure your remote access server to allow DHCP to assign addresses and configurations to the client computers. Users report that they cannot access network resources by using the server name or by searching Active Directory. You discover that when you connect to the remote access server, your client computer is receiving its IP address configuration but none of the DHCP options. What should you do to resolve this problem?**

    A: Configure the remote access server to act as a DHCP Relay Agent.

37. **Your domain is in mixed mode. Routing and Remote Access is enabled for remote access on Srv1. The domain also has a Windows NT 4.0 member server computer named Srv2. Srv2 is running Remote Access Service (RAS). Users in the domain use Windows 2000 Professional computers to dial in to the network through Srv1 or Srv2. However, Srv2 is not able to validate remote access credentials of domain accounts. How should you configure the network to enable Srv2 to validate remote access domain users?**

    A: Add the Everyone group to the Pre-Windows 2000 Compatible Access group.

38. **You have Macintosh users who inform you that they cannot request valid user certificates from your Enterprise Certificate Authority. What should you do to allow these users to request certificates by using Web based enrollment?**

    A: In the Internet Information Services (IIS) console, access the properties for the CertSrv virtual directory. On the Directory Security tab, set the authentication type to Basic Authentication.

39. **You are the administrator of a Web server hosted on the Internet that runs on a Windows 2000 Server computer. You want to download ActiveX controls automatically to your customers' browsers. The default security settings on your customers' browsers prevent this. What should you do to automate the downloading of your ActiveX controls?**

    A: Install an Enterprise Subordinate Certificate Authority (CA) that uses a commercial CA as the parent. Create a policy on the CA that allows the Web developers to request a certificate for code signing.

40. You configure a Windows 2000 Server as the DNS server for your network. You create both standard primary forward lookup and reverse lookup zones. When you use the NSLOOKUP utility, you cannot resolve host names from IP addresses on your network. When you run TRACERT.EXE, you receive the error message: "Unable to resolve target system name". What should you do?

A: Create PTR (pointer) records in the reverse lookup zone.

41. Your Windows 2000 Server computer named Srv2 cannot communicate with your UNIX server named Srv1. Srv2 can communicate with other computers on your network. You try to ping Srv1 but you receive the following error message: "Unknown host Srv1". After creating an A (host) record that has the correct name and IP address, you still receive the same error message. What should you do to resolve this problem?

A: Run the ipconfig/flushdns command on Srv2.

42. In your domain, Srvl is configured as the primary server, and Srv2 and Srv3 are configured as caching-only servers. Both servers forward requests to Srvl. Users on networks 10.107.2.0 and 10.107.3.0 use an Internet application that gathers stock market quotes from various servers on the troytec.com domain. You want to reduce network traffic. What should you do?

A: Increase the Time to Live (TTL) for the SOA (start of authority) record on Srvl.

43. Your Web server is configured to run a third party Web application for users on your network. Users complain that each time they try to connect to a secure Web page stored on the Web server, they receive the error message "Web page requested is not available". They have no problem connecting to FTP. You have verified that the Web service has started. What should you do to diagnose this problem?

A: Verify that port 443 is permitted in your TCP/IP filter.

44. Your network has a main office and one branch office. You use PPTP to connect the main office to the branch office. What is the strongest possible level of data encryption for the connection?

A: MS-CHAP v2.

45. Your network consists of two Windows 2000 Server computers named Houston and Sacramento and 350 Windows 2000 Professional computers. Sacramento is a DHCP server. The DHCP server provides the TCP/IP configuration of all the Windows 2000 Professional computers. Houston and Sacramento have IP addresses that are manually configured. Houston frequently hosts multicast-based

video and audio conferences. How should you configure the networks to dynamically allocate multicast addresses?

A: On the DHCP server, create and activate a scope so that it has a range of Class D addresses.

46. You manage Srv1, a computer running Windows 2000 Server that has two network adapter cards, one connected to the Internet and one connected to your internal network. You install NAT protocol to provide Internet access to client computers. Srv1 and the client computers are located at one of your remote offices. When configuring NAT, you choose "Resolve IP addresses for clients using DNS". What else should you do?

A: The network adapter connected to the Internet should be configured with the address of a DNS server.

47. Your network consists of a single IP subnet that uses DHCP to automate client computer configuration. You install a WINS server on the network. Users report that the network response time is slow. You discover that the levels of broadcast traffic have not been reduced. When you view the WINS database, you also find that the only entry is for the WINS server itself. What should you do?

A: Configure a DHCP scope option to include the address of the WINS server.

48. Your network consists of Windows 2000 Servers, Windows NT Workstations, and Windows for Workgroups 3.11 clients distributed across three subnets. All client computers are configured as DHCP client computers. You install a WINS server on one subnet on your network. You define a DHCP setting option to include the WINS server's address. Users report that they can access resources on servers on their own subnet but they cannot access resources on other subnets. What should you do?

A: Use the IPConfig/renew command to refresh the client computer's configuration.

49. Your network has three segments connected by a router. Each segment contains a Windows 2000 based WINS server and two other Windows 2000 Server computers. The network has 300 Windows NT Workstations, and 40 WINS clients distributed evenly over the three segments. Users in each network segment inform you that they cannot browse any network resources on the other network segments, but can browse their own segment. What should you do to enable users to browse for network resources on all three network segments?

A: Configure the three WINS servers as replication partners of each other.

50. Your Windows 2000 Server computer is configured with a static IP address. You want to configure the computer as a DNS resolver. What step should you take?

A: Configure the address of the preferred DNS server in the TCP/IP properties of the Local Area Connection.

51. Your company has a main office in Orlando and branch office locations in Miami, Tampa and Jacksonville. The branch offices are connected to Orlando by Windows 2000 based routers. All four locations have a Windows 2000 based DHCP server. Each Friday, the Orlando location hosts a multicast video presentation that is broadcast to all four locations. The Orlando location also frequently hosts multicasting video presentations intended for the sales staff in the Orlando and Miami locations only. You want to ensure that these sales staff multicasting video presentations are not sent to the Tampa and Jacksonville locations. You assign specific IP multicast addresses for use with the sales staff multicasting video presentations. How should you configure the network to prevent the forwarding of the sales staff multicasting video presentations to the Tampa and Jacksonville locations?

A: Configure a multicast setting boundary for the sales IP multicast addresses on the Tampa and Jacksonville interfaces of the Orlando router.

52. You have been given the network ID of 172.24.8.0/22 from your ISP. All of the routers in your network use either RIP V2, or OSPF. Each of the two subnets you will be creating will contain only 75 computers. You want to use the most specific number of bits and the first two available network ID numbers in your subnet mask.

A: Drag 172.24. 8.128/25 and 172.24.9.0/25 to the appropriate position.

53. You use an IPSec policy to encrypt data. You want to prevent the re-use of the previous session keys, and limit performance degradation. What should you do?

A: Select the Session key Perfect Forward Secrecy check box.

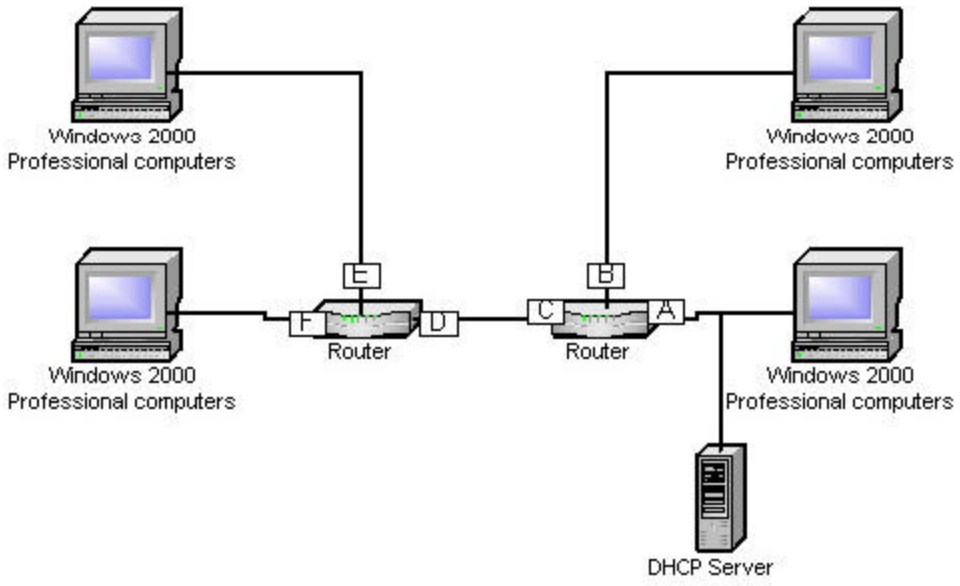
54. Your network router has SNMP enabled. You want to monitor all SNMP traffic generated by this router. You install Network Monitor on a Windows 2000 Server on your network. You have configured your router to trap to an SNMP Manager installed on another server. What should you do to receive a notification when the network router raises a SNMP trap? (Choose two)

A: Create a Network Monitor filter that has a pattern match for SNMP traffic.
Create a Network Monitor trigger to run the net send command.

55. You want to encrypt traffic and prevent unnecessary connections over your 128-Kbps ISDN line. This line connects your main office to a branch office. You have configured Routing and Remote Access on a stand-alone Windows 2000 Server in each office to provide a demand-dial connection. What should you do?

A: Configure a PPTP demand-dial connection.
Set the IP Demand Dial Filters to exclude NetBIOS broadcast traffic.

56. You have the following network configuration. You want to enable and configure the DHCP Relay Agent to allow all Win2000 Profession computers to receive an IP address from the DHCP server. On which interfaces should you enable and configure the DHCP Relay Agent?



A: Drag the interface with DHCP Relay Agent to B, E, and F.

57. You have one standard primary and two secondary DNS servers in your Windows 2000 domain. The DNS zones for the domain are configured to allow for dynamic updates. All three DNS servers are located on domain controllers. What should you do to allow client computers to be able to register with any DNS server?

A: Change the zone type to the DNS zone for the Win2000 domain on all 3 DNS servers to Active Directory Integrated.

58. You have mirrored the contents of an Intranet Web application on three Web servers that contain IIS. Using the fewest possible resources, how should you configure DNS to allow access to all Web servers in the event of a failure?

A: Configure one DNS server so that it has one DNS zone.
Enable Round Robin.
Create an A (host) record for the application on each Web server's IP address.

59. Routing and Remote Access is enable for remote access to your member server. The domain is in native mode. All users should be allowed to dial in during the workday. The global security group name Support must be allowed to dial in

between 6:00 p.m. and 8:00 a.m. You do not want to allow them to dial in when the log files are made between 7: 00 a.m. and 8:00 a.m. You create four remote access polices as shown:

Name	Condition	Permission
Domain Users All	Windows-group= Domain users	Access
Support All	Windows-group= Support	Access
Domain Users 6-8	Day-and-Time=6pm-8am Windows-group= Domain users	Deny
Support 7-8	Day-and-Time=7am-8am Windows-group= Support	Deny

In what order should the remote access policies be placed?

A: Support 7-8
Support All
Domain Users 6-8
Domain Users All

60. Routing and Remote Access is enabled for remote access to your member server. Users dial into the network by using their Windows 2000 Professional computers. Members of the Accounting group use smart cards for remote authentication. Their dial-in permission is set to Control access through Remote Access Policy. You create a new remote access policy named Accounting Access. It grants the Accounting group access any time of the day. It's the first policy on the list. When Accounting dials into they network, they report that they are unable to use the smart card for remote authentication. What should you do?

A: Enable EAP on the member server and the Windows 2000 remote access clients. Enable EAP in the profile for the Accounting group remote access policy.

61. Your network consists of one Windows 2000 domain running in native mode. You are not running Certificate Services. Salespeople in the field require file and print services, e-mail, and access to the company's database. You have dedicated T1 access to the Internet. You use VPN. You want to accomplish the following goals

- **Required network resources will be available to all Accounting people.**
- **Only the Accounting people will be able to make connections to the network.**
- **Confidential data should not be compromised.**
- **Network access will only occur during business hours.**
- **All Accounting staff are able to simultaneously connect to the network.**

You take the following actions:

- **Install Routing and Remove Access and configure virtual private networking.**

- **Grant the Accounting staff Allow Access dial-in permission.**
- **Edit the default remote access policy to grant remote access permission.**
- **Edit the default remote access profile to require strong encryption of data.**

What results do these actions produce? (Choose all that apply)

A: Required network resources are accessible to all accounting people.
Connections to the network are made by accounting people only.
Sensitive company data is kept confidential over the VPN.

62. Your executives need access when mobile, regardless of where the call originates. You allow vendors access to the network by Routing and Remote Access. You want to be able to specify the locations from which vendors can connect. What three actions should you take to enable both the executives and vendors access to your network? (Choose three)

A: Set the Callback option to Always Callback to for the vendors.
Enable LCP extensions.
Set the Callback option to Set by Caller to for the executives.

63. To allow Internet access through a dial-up connection to Server A, you install NAT routing protocol. All computers in your network use Automatic Private IP addressing. There is no DHCP server in the network. How should you configure Server A to use the IP address 172.16.65.1 through 172.16.65.250? (Choose all that apply)

A: Assign an IP address of 172.16.65.1 to the LAN interface of Server A.
Configure the NAT routing protocol to automatically assign addresses in the range of 172.16.65.2 through 172.16.65.250 to computers on the private interface.

64. To allow Internet access through a dial-up connection to London, you install NAT routing protocol. All computers in your network use a dynamically assigned IP address. You have one DHCP server in the network. Your ISP has allocated four IP addresses 207.46.179.4 through 207.46.179.7 to your network. How should you configure London to use these addresses?

A: Configure the public interface of the NAT routing protocol to use an address pool with a starting address of 207.46.179.4 and a mask of 255.255.255.252.

65. Your Public Key Infrastructure consists of an offline root CA and several subordinate CAs. One of your divisions that used to issue certificates is being sold. You do not want applications and other CAs on your network to accept certificates from this CA. What should you do?

A: On the company's root CA, revoke the certificate of the division's subordinate CA.

Publish the CRL.
Copy the EDB.log file from the root CA to the CDP.

66. Your network contains ten segments connected by four server-based routers. Routing and Remote Access is enabled as a router on these servers. These servers, Router1, Router2, Router3, and Router4 use RIP V2 for IP. You have additional routers that use RIP V2. These other servers may have incorrect routing information. How can you ensure the first four routers do not process routes received from any other router but from Routers1-4? (Choose all that apply)

A: Configure the RIP routing protocol on the four routers to use RIP peer filters. List the other three routers as RIP peers.
On each RIP interface on the four routers, configure route filters for outgoing routes. Announce only routes that are connected to the four routers.
Configure each RIP interface on the four router to unicast announcements to RIP neighbors.
Configure each RIP interface to use password authentication.

67. Your network consists of two segments connected by a router. It has one DHCP server that has active scopes for both segments. The IP address configured in the two scopes are 10.65.1.0/24 for the first segment, and 10.65.2.1/24 for the second segment. The DHCP server's IP address is 10.65.1.2. Users in the segment without the DHCP server report they are using IP addresses in the range of 169.254.0.0/16. The other segment is using IP address in the range of 10.65.1.0/24. What should you do to ensure the computers in the segment that does not have the DHCP server to automatically use IP address in the range of 10.65.2.0/24?

A: Enable and configure the DHCP Relay Agent service on a server in the segment that does not have the DHCP server.

68. Your WAN network consists of ten internal subnets in two physical buildings connected by routers. An additional subnet is configured for Internet access. All routers on the network will be multihomed Windows 2000 Servers running Routing and Remote Access. You want to accomplish the following goals:

- **Administrative overhead for routing tale configuration is minimized.**
- **Broadcast traffic for routing table configuration is minimized.**
- **Link redundancy within ten minutes is ensured in case of router failure.**
- **Ensure convergence times of less than one minute for all known routes.**
- **Internal routing information will never be exposed to external routers.**

You take the following actions:

- **Install RIP version 1.**

- **Configure RIP to use all interfaces on all multihomed computers.**
- **Enable RIP authentication by specifying a password on each interface.**

What results do these actions produce? (Choose all that apply)

A: Administrative overhead is minimized.
Internal routing is never exposed.

69. You are migrating your network from WINS to DNS. You remove one WINS server by performing the following actions:

- **On the WINS server, stop the WINS Service and uninstall WINS.**
- **On the DHCP servers, reconfigure the options to no longer specify that WINS server as a WINS server. Configure the DHCP options to instead use the other WINS servers equally.**
- **On WINS clients that are manually configured to use TCP/IP, reconfigure them to no longer use that WINS server. Configure them instead to use the other WINS servers.**
- **On one of the remaining WINS servers, delete the static mappings originally made on the deleted WINS server.**

After several weeks, you notice that static mappings originally made on the WINS server are still present on all the remaining WINS servers. What should you do?

A: Manually tombstone the WINS owner from the database.

70. Your network consists of many Windows 2000 Professions WINS client computers and several Windows 2000 based WINS servers. The client computers are portables that connect from different locations, and access NetBIOS-based resources. DHCP servers provide the TCP/IP configuration of the WINS clients. How do you ensure that all the client computers are able to resolve NetBIOS names, even if some of the WINS servers are not available?

A: Configure the DHCP servers to provide each client with a list of WINS servers.

71. Your network has two IP subnets. Two domain controllers are located on subnet1. Each domain controller is also a DNS server hosting an Active Directory integrated zone. You implement WINS on a server on subnet2. Windows NT Workstations on subnet 2 are receiving the following error: "Domain Controller cannot be located". Workstation users on subnet1 are not having the same problem, but are complaining about logon response times. No Windows 2000 Professional users report any problems. What must you do to ensure Workstation users on subnet2 can be validated, and improve Workstation users' response time on subnet1?

A: Configure the Windows 2000 Server domain controller computers as WINS clients.

72. Your network has two sites, Sacramento and Phoenix, and two DNS zones. The primary DNS server in Sacramento is named ns1.troytec.com, and is authoritative for the root zone in troytec.com. The primary DNS server in Phoenix is named ns2.phoenix.troytec.com. This server is authoritative for the delegated subdomain phoenix.troytec.com. You notice several Knowledge Consistency Checker (KCC) warnings. They indicate that the KCC cannot establish a replication link with the directory partitions in Phoenix. What should you do?

A: Change the NS record that points to the ns2.phoenix.troytec.com to phoenix.troytec.com. NS ns2.phoenix.troytec.com.

73. Your company owns the Class B subnet 172.41.48.0/24. All your servers and clients are configured as DHCP clients. The DHCP server's hard disk fails. It was not backed up. You are installing a new DHCP server to prevent any connectivity problems. What should you do? (Choose two)

A: Decrease Conflict Detection attempts.
Create a scope of 172.41.48.1 to 172.41.48.254.

74. Your network consists of two Windows 2000 Servers and 200 Windows Professional computers on one segment. The first server, a DHCP server, has an IP address of 192.168.2.1. It provides TCP/IP configuration for all the client computers. The range used is 192.168.2.0/24, with a lease duration of 15 days. You want to change the address to 10.17.8.0/24. The second server as an IP address of 10.17.8.1, and it is installed with DHCP. It's range is 10.17.8.0/24, and lease duration is 15 days. The two address ranges will be used concurrently on the same segment for three months. A router provides routing. After you activate the DHCP scope on the second server, users report they are unable to obtain an IP address. Each of the two DHCP servers respond with negative acknowledgment messages to lease requests. What should you do?

A: On both DHCP servers, configure a superscope so that it has both address ranges. Define an exclusion range for the entire address range of 10.17.8.0/24 on the first server, and 192.168.2.0/24 on the second server.

75. You run dcpromo.exe to promote SrvA, a computer running Windows 2000 Server, to the first domain controller for troytec.com. You install the DNS service on SrvA. You assign a static IP address to ten Windows 2000 Professional computers and configure the IP address of SrvA as the DNS server for these computers. What should you do to insure that the A records and the PTR records for the computers running Windows 2000 Professional are recorded correctly on SrvA?

A: Enable the zone for troytec.com to accept dynamic updates and create a reverse lookup zone for the network and enable the zone to accept dynamic updates.

76. Your main office and two branch offices are connected by dedicated T1 lines. Two additional branch offices use 128-Kbps ISDN lines and Routing and Remote Access over the Internet to connect to the company's network. You are designing your DNS name resolution environment, and want to accomplish the following goals:

- **Name resolution traffic across the WAN should be minimized.**
- **Replication traffic across the WAN should be minimized.**
- **Replication traffic across the public WAN should be secure.**
- **Name resolution performance for client computers should be optimized.**

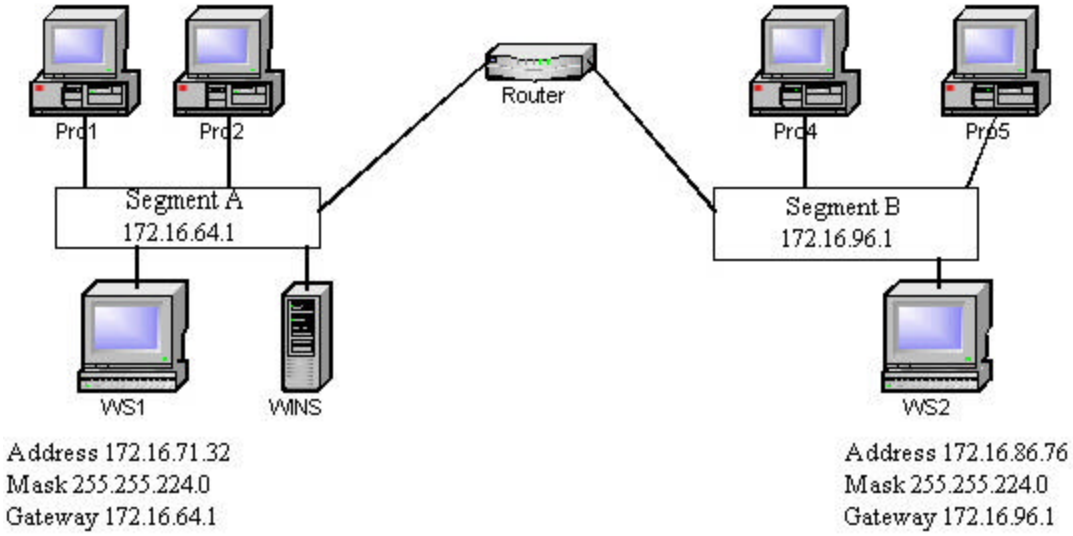
You take the following actions:

- **Install the DNS Server service on one DC at each office.**
- **Create an Active Directory integrated zone on each DNS server at each office.**
- **Configure client computers to query their local DNS server.**
- **Configure the zones to allow dynamic updates.**

What results do these actions produce? (Choose all that apply)

A: Name resolution traffic is minimized.
Replication traffic is minimized.
Name resolution performance for client computers is optimized.
Replication traffic across the public WAN is secure.

77. You have four Windows 2000 Professional computers and two Windows 2000 Servers. Pro1 can ping 172.16.96.1. Pro4 can ping 172.16.64.1. All Windows Professional computers can communicate with each other, but WS1 cannot ping WS2. What should you do to ensure WS1 communicates with WS2?



A: Change the IP address of WS2 to 172.16.103.76.

78. You have seven Windows 2000-based WINS servers in separate locations. How should you configure these servers to have a convergence time of less than 60 minutes?

A: Designate one of the WINS servers as the central WINS server.
Configure the other WINS servers as push/pull partners with the central server.
Configure the central WINS server as push/pull partner with the other WINS servers.
Use a replication interval of 25 minutes.

79. Your network consists of Windows 2000 Servers, Windows 2000 Professional computers, Windows 98 computers, and UNIX workstation computers running SMB server software. TCP/IP is your only protocol. You implement WINS, but the Windows-based clients report they cannot access resources based on the UNIX computers by NetBIOS names. They are not experiencing problems accessing Windows-based resources by NetBIOS name. What should you do?

A: On the WINS server, create static mappings for the UNIX computers.

80. Your network has two locations that contain two 2000-based WINS servers each. You want to accomplish the following replication goals:

- **The Sacramento WINS server must replicate changes in the local database to each other immediately following each new registration or IP address change registration.**
- **The Houston WINS servers must replicate changes in the local database to each other every 30 minutes.**
- **Changes in the WINS database in either location should be replicated to the other location every three hours.**

How should you configure the WINS server to accomplish these goals? (Choose three)

A: Configure the Sacramento WINS servers as push/pull partners of each other. Configure both WINS server to use persistent connections for push replication partners. Set the number of changes before replication to 1.
Configure the Houston WINS servers as push/pull partners of each other. Specify a replication interval of 30 minutes.
Configure the Sacramento1 and Houston1 WINS servers as push/pull partners of each other. Specify a replication interval of three hours.

81. Your DHCP server provides TCP/IP configuration to all client computers in your network, which consists of the Windows 2000 Professional computers, Windows 2000 Servers, and Windows NT Workstation computers. All client computers

have file and print sharing services enabled. You want to accomplish the following goals:

- **FQDN will be utilized to locate all client computers.**
- **A records for all clients will be automatically added to the DNS zone files.**
- **PTR records for reverse name lookup for clients will be automatically added the DNS zone files.**
- **A records and PTR records will be automatically removed from the DNS zone files when the DHCP lease expires.**

You take the following actions:

- **Configure the DHCP server to never update client information in DNS.**
- **Configure the DHCP server to discard forward lookups when the lease expires.**
- **Configure the DHCP scope to configure the domain name for all DHCP clients.**

Which results do these actions produce? (Choose all that apply)

A: A records and PTR records will be automatically removed from the DNS zone files when the DHCP lease expires.

82. Your network consists of three segments connected by a router. Each segment contains one Windows 2000 Server. London is a DHCP server which provides TCP/IP configuration to all clients in the three segments. The DHCP server ahs three scopes, one for each segment. The lease duration is eight days for all three scopes. You want to move the DHCP Server from London to Bristol. You take the following actions:

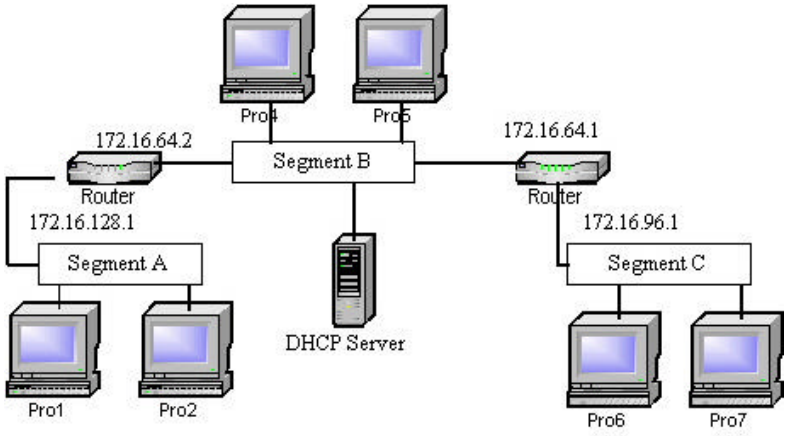
- **On London, stop and disable the DHCP Server service.**
- **On Bristol, install, authorize, and stop the DHCP Server service.**
- **Copy the entire Systemroot\system32\dhcp folder from London to Bristol.**

You want to configure Bristol to use the scope information and the lease address currently in use by the Windows 2000 Professional computers. What should you do next on Bristol? (Choose two)

A: Start the DHCP server and reconcile all scopes.
Use the registry editor to restore the DHCP registry configuration from the Systemroot\system32\dhcp\backup location.

83. All your client computers receive their IP address information from the DHCP server on your network. Users on Pro4 access most of their resources from computers on Segment A. Users on Pro5 access their resources from computers

on Segment C. How should you configure your DHCP server to issue gateway addresses to Pro4 and Pro5 to offer optimum access time? (Choose two)



A: Create a reservation for Pro4. Configure the router option that has the value of 172.16.64.2.
On the DHCP server's scope for Segment B, configure the Router option of 172.16.64.1.

84. Your network consists of five subnets that are connected by a BOOTP relay-enabled router. You have Windows 2000 Servers, Professional client computers, and several UNIX servers and DHCP-enabled network printers. You want to accomplish the following goals:

- **Automatically assign the correct IP address to clients.**
- **Prevent address conflicts between clients and servers.**
- **Correct scope options should be applied to each client on each subnet.**
- **Clients not in use will not be allowed to keep an IP addresses for more than 3 days.**
- **Each network printer will always receive the same IP address.**

You take the following actions:

- **Install DHCP Server service on a Windows 2000 Server computer.**
- **Create five scopes, each containing the address range for a specific subnet.**
- **From the DHCP console, set optional client configurations for each scope in the Scope Options container.**
- **Exclude the range of address in use by the server.**
- **Exclude the range of addresses in use by network printers.**

Which results do these actions produce? (Choose all that apply)

A: Automatic assignment of the correct IP address to clients.
Address conflicts between clients and servers prevented.

Correct scope options are applied to each client on each subnet.

85. Your DHCP server provides TCP/IP configuration to all client computers in your network, which consists of the Windows 2000 Professional computers, Windows 2000 Servers, and Windows NT Workstation computers. All client computers have file and print sharing services enabled. You want to accomplish the following goals:

- **FQDN will be utilized to locate all client computers.**
- **A records for all clients will be automatically added to the DNS zone files.**
- **PTR records for reverse name lookup for clients will be automatically added the DNS zone files.**
- **A records and PTR records will be automatically removed from the DNS zone files when the DHCP leas expires.**

You take the following actions:

- **Configure the DHCP server to always update client information in DNS.**
- **Configure the DHCP server to discard forward lookups when the lease expires.**
- **Configure the DHCP score to configure the domain name for all DHCP clients.**
- **Configure the DHCP server to update DNS for client computers that do not support dynamic updates.**

Which results do these actions produce? (Choose all that apply)

A: FQDN will be utilized to locate all client computers.
A records for all client computers are automatically added to the DNS zone files.
PTR records for reverse name lookup re added to the DNS zone files.
A records and PTR records are automatically removed from the DNS zone files.

86. To allow Internet access through a dial-up connection to Server A, you install NAT routing protocol. All computers in your network use Automatic Private IP addressing. There is no DHCP server in the network. Your server is configured to use the IP address 192.168.0.1. Routing and Remote Access and all the ports on this server are enabled for demand-dial routing. What should you do to enable your Windows 2000 Professional clients to access the Internet through a translated demand-dial connection on the server? (Choose four)

A: Create a new demand-dial interface for the dial-up connection.
Add a public and a private interface to the NAT routing protocol.
Add a default static route that uses the public interface.
Configure the NAT routing protocol to enable NAT assignment and name resolution.

87. You use the Group Policy Editor to create an IPSec policy for the Group Policy Object linked to an OU in your Windows 2000 domain. What should you do to insure the policy is applied to the computers in the OU?

A: Use the IP Security Policies node in Group Policy Editor to assign the policy.

88. You want to configure your DNS server to allow users to type a host name in their browsers to connect to the Web server that is on the same subnet. The host name that all users will type in will be identical regardless of the subnet they are on. You have three subnets in your network, and each Web server on your network contains the same content as all of the Web servers. How should you configure your DNS server?

A: On the primary DNS server, create three A (host) records that map the same host name to IP address of the Web server on each subnet.

89. You have a primary external DNS server, and a secondary DNS server located on your ISP's UNIX server in order to provide fault tolerance. Users are unable to connect to the URL when using the secondary DNS server. What should you do?

A: Click the BIND secondaries check box in the Advanced tab of the Properties box.

90. Your administrators perform remote monitoring and administration which requires an excessive amount of network bandwidth. You want to limit all users to use a single phone line, but allow administrators to use multiple lines. You want to configure multiple phone-line connections to adapt to changing bandwidths. When they fall below 50 percent, you want to reduce the number of phone lines utilized. All users should have the ability to connect to he network by Routing and Remote Access. No default remote access policies currently exists. What should you do? (Choose three)

A: Create two remote access policies on the Routing and Remote Access server.
Allow Multilink.
Select Requires BAP for Dynamic Multilink Requests.

91. To enable connections for remote administration, you install Routing and Remote Access on a Windows 2000 domain controller. You want to accomplish the following goals:

- **Only administrators will have dial-up access.**
- **Connections will be accepted only from 4:00 p.m. to 7:00 a.m.**
- **Connections will automatically disconnect after 20 minutes of inactivity.**
- **All connections will encrypt all communications.**
- **Connections will be limited to one hour.**

You take the following actions:

- **Set the level or levels of encryption to No Encryption and Basic.**

- **Add Domain Admins to the Windows Group Policy condition.**
- **Set Disconnect if idle to 60 minutes. Set Restrict maximum sessions to 20 minutes. Set Restrict access for Days-and-Times to Sunday – Saturday, 07:00 – 16:00 each day.**

Which results do these actions produce? (Choose all that apply)

A: Connections are forcibly disconnected after 20 minutes of inactivity.
Only Administrators have dial-up access.
Dial-up connections are accepted from 4:00 p.m. to 7:00 a.m.

92. To centralize administration you implement a Remote Authentication Dial-In Service (RADIUS) server. Each of your branch offices will support their own Routing and Remote Access Server. You remove the default remote access policy. What should you do to implement one company policy that requires all dial-up communications to use 40-bit encryption, and require secure communications? (Choose two)

A: Create one remote access policy on the RADIUS server.
Set encryption to Basic in the remote access policy.

93. Your network consists of a computer running Windows 2000 Server, NWLink, and SQL Server named SQL1. It has one network adapter card. You need to enable access to SQL for clients running Windows 98 and NetWare clients from Novell. The NetWare servers on your network are running NetWare version 4.11. What should you do?

A: Configure a unique internal network number for SQL1.

94. Your domain has a Windows 2000 member server named Ras1 and a Windows 2000-based DHCP Server named Dhc1. Routing and Remote Access is enabled on Ras1. Two DNS servers use IP addresses of 10.1.5.2 and 10.1.5.3. Ras1 is configured to use DHCP to assign IP addresses to remote access clients. DHCP server scope options include: Vendor: Standard, Value: 10.1.5.3, Class: None. It does not have any client reservations. When remote access clients dial into Ras1, they receive an IP address from the DHCP scope range, but they do not receive the DNS address configured in the DHCP scope. They receive a DNS server address of 10.1.5.2. How should you configure your network to allow remote access clients to receive the DNS option from the DHCP server?

A: Install and configure the DHCP Relay Agent routing protocol on the internal interface on Ras1.

95. Your network consists of Windows NT 4.0 and Windows 2000 computers. All Windows 2000 Server computers are member servers of a single Windows NT 4.0

domain. You would like to use two of these servers to test IPSec configurations that are using Kerberos authentication protocol. What should you do?

A: Promote one of the servers to a domain controller.
Assign the domain controller the default Secure Server IPSec policy.
Assign the other server the default Client IPSec policy.

96. To monitor traffic on your network, you install Network Monitor. You want to monitor the source IP address, destination port number of every TCP/IP frame, and destination IP address. This information will be logged for three hours. What should you do? (Choose two)

A: On the Capture Buffer Settings menu, increase the buffer size.
Change the Temporary Capture Directory.

97. Your Windows 2000 Server runs IIS and uses an IP address of 131.107.2.2 to support Internet users, and 10.1.1.2 to support an Intranet application. You want to configure this server to permit only Web communications from the Internet, and to allow access to shared folders and other resources for users on the Intranet. What should you do? (Choose two)

A: Enable TCP/IP filter. Permit only port 80 on the network adapter that uses the IP address of 131.107.2.2.
Permit all ports on the network adapter that uses the IP address of 10.1.1.2.

98. Your Windows 2000 Server has Routing and Remote Access enabled, and it configured as a Virtual Private Network (VPN) server. You want to limit access to the VPN server to employees who belong to the Windows 2000 domain local security group GroupA. Each GroupA member account is configured using the setting "Control access through remote access policy". You have removed the default remote access policy. What do you need to do to limit access to the VPN to only members of GroupA?

A: Create a remote access policy and set the condition Windows-Groups to VPN-Access in the policy.

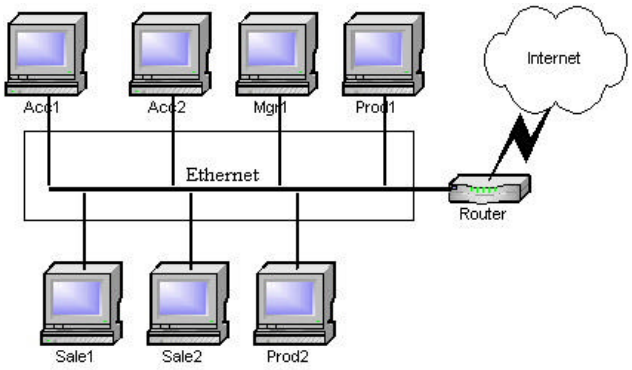
99. You install and configure both TCP/IP and NWLink IPX/SPX on a Windows 2000 Professional computer. Your network consists of Windows 2000 Servers, Windows NT Server 4.0, and NetWare 3.11 and 4.1 servers. You install the client software for both Microsoft and NetWare networks. But, when you attach to the Windows 2000 Professional computer to the network, you are unable to see the NetWare 3.11 servers in My Network Places. You also cannot map drives by using either Microsoft-specific or NetWare-specific commands. What should you do?

A: Edit the PktType value in the registry to include the hexadecimal values for both 802.3 and 802.2 frame types.

100. You need to assign network ID numbers and host addresses to the computers in one of your branch offices. A single route to the branch office is advertised as 192.168.16.0/24. You must be able to add 2,000 additional computers to the branch. What steps must you take to be able to accommodate all computers in the branch, while taking advantage of route summarization? (Choose all that apply)

A: In the branch office, add additional network ID numbers 192.168.17.0/24 – 192.168.23.0/24.
Change the advertisement to the branch office to 192.168.16.0/20.

101. Your network is configured as shown:

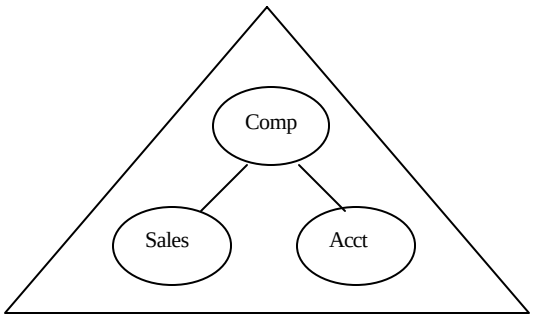


The Accounting computers do not need access to the Internet. You want to accomplish the following goals:

- **All communications involving Acct1 and Acct2 should be encrypted.**
- **Internet communications should not be encrypted.**
- **Communications between the sales and management clients should be encrypted.**
- **Performance overhead for encryption should be minimized.**

You take the following actions:

- **Create the following OU structure:**



- **Add Acct1 and Acct2 to the Acct OU.**
- **Add Sale1 and Sale2 to the Sales OU.**
- **Add all other computers to the Comp OU.**
- **Assign the default Secure Server IPSec Policy to the domain.**

Which results do these actions produce? (Choose all that apply)

A: All communications between Acct1 and Acct2 are encrypted.
Communications between Sales and Management are encrypted.
Internet communications are not encrypted.

102. You are a branch office network administrator. You are connected to the company network via a Windows 2000 Routing and Remote Access two-way demand-dial connection over ISDN. Sensitive company data, e-mail, and application traffic is sent across the connection. You want to accomplish the following goals:

- **All data should be secure.**
- **Rogue routers will be prevented from exchanging router information with either router.**
- **Both routers will be able to validate each other.**
- **Both routers will maintain up-to-date routing tables.**
- **Traffic over the link during peak business hours will be minimized.**

You take the following actions:

- **Install a Certificate Services server at the main office.**
- **Enable EAP-TLS as the authentication protocol on both Routing and Remote Access servers.**
- **Enable RIP version 2 on the demand-dial interfaces.**

Which results do these actions produce? (Choose all that apply)

A: Routers maintain up-to-date tables.

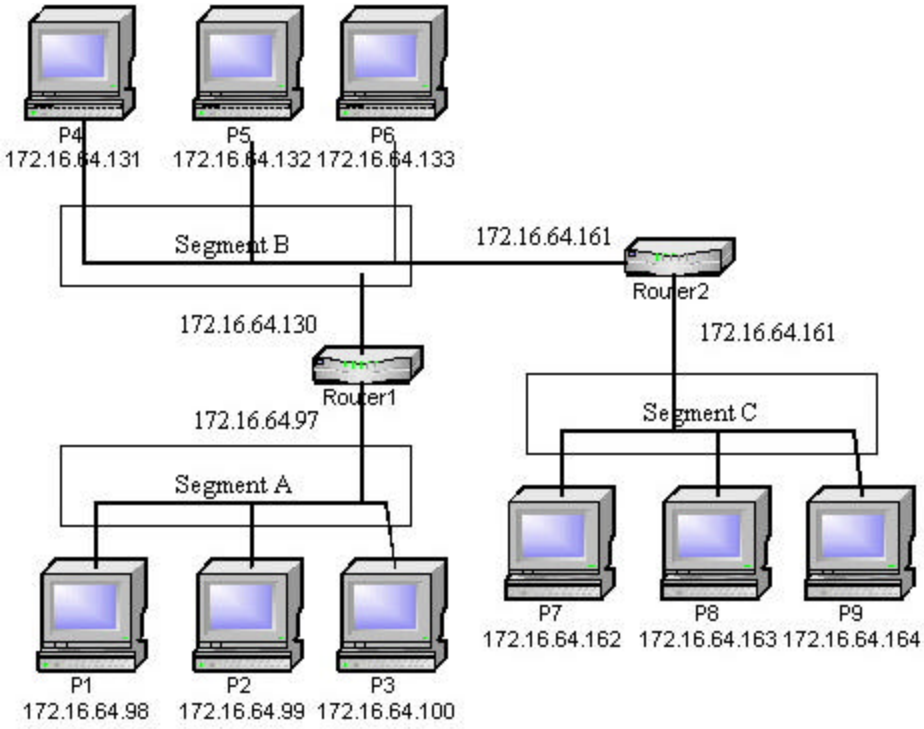
103. Your network contains a Windows 2000 Server that has two network interfaces, East and West. Routing and Remote Access is enabled as a router on the server. Only the network segment connected to the West interface has a DHCP server hosted on a Windows 2000 Server. You want to allow computers on the East interface to receive IP address from the DHCP server. What should you do? (Choose all that apply)

A: Configure the DHCP Relay Agent routing protocol to run on the East interface.
Configure the DHCP Relay Agent routing protocol to use the IP address of the DHCP server as the server address.

104. Your network has ten segments connected by routers. Only four segments have Windows 2000-based WINS servers. Throughout the network are several NetBIOS b-node client computers. NetBIOS b-node clients cannot browse any other network segments, but are having no problems browsing their own. What should you do?

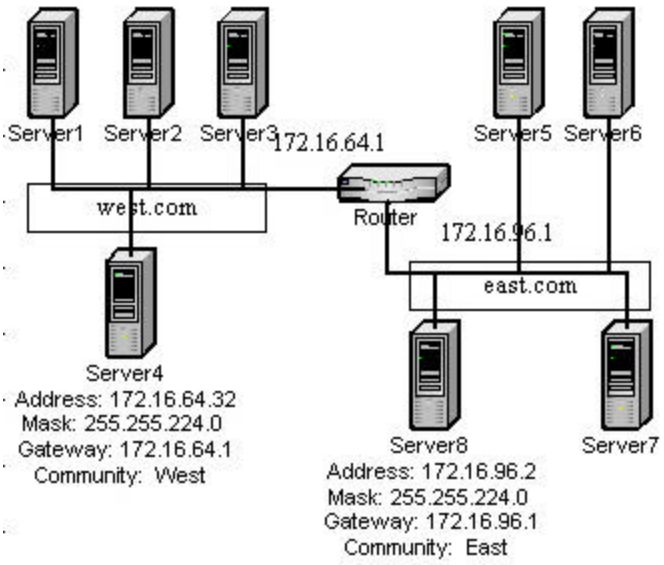
A: On each segment, configure a computer as a WINS proxy.

105. Your company has three offices, but plans to expand. You are replacing your bridges with two routers named Router1 and Router2 to accommodate increased traffic. You are configuring Router1. What routing entry should you add?



A: Execute route add 172.16.64.96 mask 255.255.255.224 172.16.64.130 –p.

106. You are configuring your network to support a SNMP management application. The network is configured as shown:



The SNMP management application is installed on Server8. Even though the servers in the west.com domain have the identical SNMP setting, the application cannot manage any of the servers in the west.com domain. What should you do?

A: Configure all the servers to have the same community name.

107. Routing and Remote Access is enabled on Router A in your network. Router A has a LAN interface which uses an IP address of 192.168.1.2. The only traffic that you want allowed into this interface is HTTP traffic. You configure two input packets with the "Receive all packets except those that meet the criteria below" option, and specify the Destination Address of 192.168.1.2 for both filters, and Destination port of 80 for the first filter, and 443 for the second filter. You notice that other network traffic is still allowed into the router though the interface. What should you do?

A: Configure the input packet filters to "Drop all packets except packets allowed by the filters".

108. You are a branch office network administrator. You are connected to the company network via a Windows 2000 Routing and Remote Access two-way demand-dial connection over ISDN. Sensitive company data, e-mail, and application traffic is sent across the connection. You want to accomplish the following goals:

- **All data should be secure.**
- **Rogue routers will be prevented from exchanging router information with either router.**
- **Both routers will be able to validate each other.**
- **Both routers will maintain up-to-date routing tables.**
- **Traffic over the link during peak business hours will be minimized.**

You take the following actions:

- **Enable MS-CHAP as the authentication protocol on both Routing and Remote Access servers.**
- **Enable OSPF on the demand-dial interfaces.**
- **Set the Require Encryption option on both Routing and Remote Access servers.**

Which results do these actions produce? (Choose all that apply)

A: All data transmitted over the connection is secure.
Both routers maintain up-to-date routing tables.

109. Your Windows 2000 Server runs IIS and uses an IP address of 131.107.2.2 to support Internet users, and 10.1.1.2 to support an Intranet application. You want to configure this server to permit only FTP communications from the Internet, and to allow access to shared folders and other resources for users on the Intranet. What should you do? (Choose two)

A: Enable TCP/IP filter. Permit only port 21 and 20 on the network adapter that uses the IP address of 131.107.2.2.
Permit all ports on the network adapter that uses the IP address of 10.1.1.2.

110. Your company has three subnets connected by a router. They are configured as follows:

Interface	Subnet	IP Address	Subnet Mask
Interface 0	Subnet 0	172.30.4.1	255.255.255.0
Interface 1	Subnet 1	172.30.5.1	255.255.255.0
Interface 2	Subnet 2	172.30.6.2	255.255.255.0

The following Subnet Scope Properties exist:

Scope Name	Start IP	End IP	Subnet Mask
Subnet 1 Scope	172.30.5.100	172.30.5.254	255.255.0.0
Subnet 2 Scope	172.30.6.100	172.30.6.254	255.255.255.0

Only subnet 1 and Subnet 2 contain clients. Each contains a Windows 2000 DHCP server. Computers on Subnet 1 can only communicate with their own host. Computers on Subnet 2 cannot communicate with hosts on Subnet 1, but have no problems connecting to Subnet 0. What should you do?

A: Delete and re-create the scope on the DHCP server on Subnet 1 to reflect the correct subnet mask.

111. Your network consists of two segments. The first segment contains Windows 2000 server computers and the second segment contains NetWare 4.1 servers. On

subnetwork 1, you want the Windows 2000 Server computer to provide file and print services to Windows-based clients that use TCP/IP. On subnetwork 2, you want the Windows 2000 Server to provide application services to NetWare clients that use only IPX/SPX. The Windows 2000 Server has two network adapter cards, and it will not function as a router for either subnetworks. What should you do? (Choose two)

A: Unbind TCP/IP to the adapter connected to subnetwork 2.
Unbind NWLink to the adapter connected to subnetwork 1.

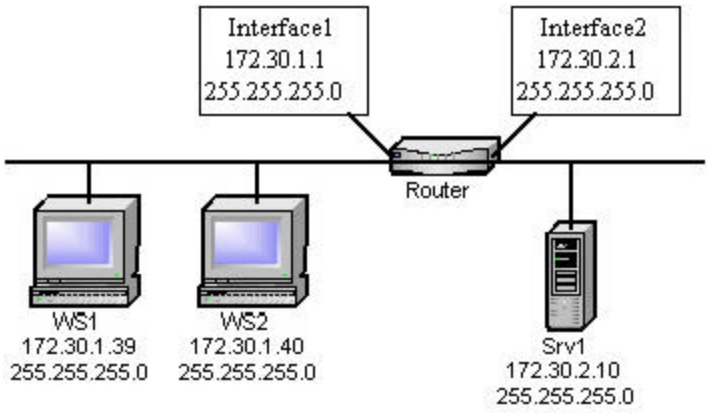
112. Your network uses an address of 172.30.0.0/16. Your projected growth for the network indicates a need for at least 25 subnets with a minimum of 1,000 hosts per subnet. What subnet mask should you configure to meet these needs?

A: 255.255.252.0

113. You install Network Monitor on a Windows 2000 Server to analyze ISO and TP4 communications to the Microsoft Exchange Server on your network. How should you configure Network Monitor? (Choose two)

A: Copy ISO.DLL and TP4.DLL to the NetMon\Parsers subdirectory.
Modify the Parser.ini.

114. Your network is configured as shown:



WS1 reports that it cannot access resources on Srv1. WS1 is able to communicate with any host on its own subnet, and can ping the router. But, WS1 cannot ping hosts on the second subnet. WS2 is not having problems.

The route print command from WS1 shows:

Network Destination	Netmask	Gateway	Interface
0.0.0.0	0.0.0.0	172.30.1.39	172.30.1.39
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1

172.30.1.0	**255.255.255.0**	**172.30.1.39**	**172.30.1.39**
172.30.1.39	**255.255.255.255**	**127.0.0.1**	**127.0.0.1**
172.30.255.255	**255.255.255.255**	**172.30.1.39**	**172.30.1.39**
224.0.0.0	**224.0.0.0**	**172.30.1.39**	**172.30.1.39**
255.255.255.255	**255.255.255.255**	**172.30.1.39**	**172.30.1.39**

What should you do?

A: The default gateway parameter on WS1.

115. You are creating a DHCP scope for your 192.168.1.32/28 subnet. The subnet consists of Windows 2000, Windows 98, and Windows 95 computers. You have two UNIX computers on this subnet that will be assigned the two highest available static IP addresses. The subnet's default gateway will be assigned the lowest available IP address on the subnet. Which scope should you create on your DHCP server?

A: 192.168.1.34 – 192.168.1.44

116. What two utilities should you use to determine the number of DNS requests submitted to a DNS server over both TCP and UDP?

A: DNS console and System Monitor

117. To allow Internet access through a dial-up connection to Server A, you install NAT routing protocol. All computers in your network use Automatic Private IP addressing. There is no DHCP server in the network. Server A is configured as follows:

- **LAN interface has an IP address of 10.65.3.1 and a subnet mask of 255.255.255.0.**
- **NAT automatically assign IP addresses of 10.65.3.2. through 10.65.3.60 to computers on the private interface.**
- **NAT uses a demand-dial interface named Dial ISP to connect to the ISP.**
- **The demand-dial interface uses an address pool of 207.46.179.33 through 207.46.179.36.**
- **The routing table has a default static route for the public interface.**

What configuration should you use for the static route for the public interface?

A: Interface: Dial ISP
Destination: 0.0.0.0
Network Mask: 0.0.0.0
Gateway: None

118. You have two Windows 2000 Servers named London and Bristol. London has a permanent cable modem connection to the Internet. Windows 2000 Professional computers on your network use APIPA. The network does not contain a DHCP server. You install and configure the NAT routing protocol on London to allow the Windows 2000 Professional computers access to the Internet through the cable modem. You use the IP range of 172.20.20.1 through 172.20.20.150 for the network. London uses an IP address of 172.20.20.1. Bristol is a Web server with an IP address of 172.20.20.2 and a default gateway of 172.20.20.1. You want to allow Internet users from outside your internal network to access the resources on Bristol through the NAT on London. What should you do?

A: Configure the public interface NAT routing protocol to use a special port that maps to the Web port and an IP address of 172.20.20.2.

119. You are the administrator of your domain. You have client computers evenly distributed across five sites. Atlanta.troytec.com recently upgraded their two DNS servers that service the subdomain. You suspect the upgrade has resulted in an incorrect configuration of your zone delegation. What should you do to verify proper zone delegations?

A: Run the nslookup –querytype=ns atlanta.troytec.com command with the server option set to query the atalanta.troytec.com server. Ping the records displayed in the output of the nslookup command.

120. Your network consists of a Windows 2000 domain that spans multiple locations. They are connected over the Internet by using Routing and Remote Access. Resources are located on TCP/IP hosts on your network. You implement Windows 2000 DNS server on your network for name resolution. What should you do to ensure when the zone transfer traffic between your DNS servers crosses the Internet links between the locations, it cannot be compromised?

A: Allow zone transfers only to servers listed on the Name Servers tab.

121. Your network consists of Windows 2000 computers, and UNIX servers. Your DNS zone is configured as an Active Directory integrated zone, and allows dynamic updates. Users can access the Windows 2000 computers by host name, but not the UNIX servers. What should you do?

A: Manually enter A (host) records for the UNIX servers to the zone database.

122. Your main office and two branch offices are connected by dedicated T1 lines. Two additional branch offices use 128-Kbps ISDN lines and Routing and Remote Access over the Internet to connect to the company's network. You are designing your DNS name resolution environment, and want to accomplish the following goals:

- **Name resolution traffic across the WAN should be minimized.**

- **Replication traffic across the WAN should be minimized.**
- **Replication traffic across the public WAN should be secure.**
- **Name resolution performance for client computers should be optimized.**

You take the following actions:

- **Install the DNS Server service on one server at each office.**
- **Create a standard primary zone at the main office.**
- **Create a standard secondary zone at the four other offices.**
- **Configure client computers to query their local DNS server.**

What results do these actions produce? (Choose all that apply)

A: Name resolution traffic across the WAN should be minimized.
Name resolution performance for client computers should be optimized.

123. A user who uses a Windows 2000 Professional computer must access data on a server that requires communication using IPSec. The Event Viewer indicates the IPSec Policy Agent cannot be started. What should you do to insure the IPSec Policy Agent is installed correctly on this computer?

A: Remove and reinstall the TCP/IP protocol.

124. You are configuring the Routing and Remote Access server for remote access. You are requested to provide a record of everyone who will access the company network by Routing and Remote Access. What should you do to log all logon activity on the Routing and Remote Access Server?

A: On the Routing and Remote Access server, enable log authentication requests in Remote Access Logging.

125. You configure remote access services in your native mode Windows 2000 domain to allow users to access the network remotely. You do not want to apply any time or authentication restrictions. You delete the default remote access policy. However, you want to restrict access by unauthorized uses. You grant all users in the domain the Allows Access dial-in permission, but immediately are notified that users are not able to make a connection. What should you do?

A: Create a new remote access policy that has the condition to grant all members of the Domain Users group dial-in access.

126. You are implementing a remote access policy that is highly available and highly secure. Your company utilizes a T3 connection to the Internet. All the servers are running Windows 2000 Advanced Server, and all clients are running Windows 2000 Professional. You want to accomplish the following goals:

- **No single point of failure will result in total loss of remote access connectivity.**
- **No authentication traffic will be carried as clear text.**
- **No data traffic will be carried as clear text.**
- **Support for 200 simultaneous remote users must be available at all times.**

You take the following actions:

- **Install a VPN server at the main office.**
- **Configure the VPN server to support 250 PPTP connections.**
- **Configure the client computers to use CHAP as the authentication protocol.**

Which results do these actions produce? (Choose all that apply)

A: Support for 200 simultaneous remote users must be available at all times.
No authentication traffic will be carried as clear text.
No single point of failure.

127. Your WINS server's hard disk fails, and you replace it, and restore the WINS database from a backup that is one week old. Now, users report they cannot browse any of the resources in the other locations. What should you do?

A: On the Windows 2000 Server computers, use the NBTStat –RR command to release and refresh the WINS registrations.

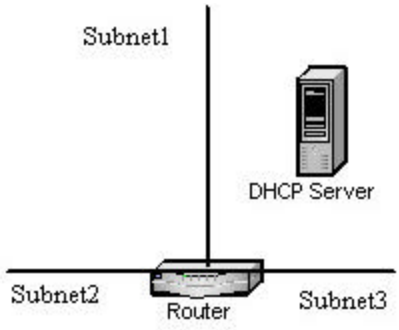
128. Your network consists of three DHCP servers and three DNS servers. TCP/IP configuration for your Windows 2000 Professional and NT Workstation clients is provided by the DHCP servers. All three DHCP servers are configured so that they have scopes for all the computers in the network, and always register and update client computer information on the DNS servers. You configure the DNS zones on all DNS servers to only allow secure updates. After you complete the configuration, you notice the client computer information in the DNS zones is no longer updated correctly after IP changes. What should you do?

A: Add the computer accounts of the three DHCP servers to the DnsUpdateProxy global security group.

129. Your client computers are configured as proxy client computers. Your DHCP server uses a scope of 172.41.48.0, and has been configured with the range of 172.41.48.1 to 172.41.48.255 with a 20-bit mask. Users complain that they cannot access any computers on the network. What should you do? (Choose two)

A: Re-create the scope that uses the subnet mask of 255.255.248.0.
Activate the scope.

130. Your network consists of three subnets that are connected by a BOOTP relay-enabled router. DHCP automates the TCP/IP configuration of your Windows 2000 Professional clients. The DHCP server is configured with a scope for each subnet.



Users on subnet2 and subnet3 periodically cannot access network resources. During high network usage times, client computers on the remote subnets are being configured with the addresses in the range of 169.254.0.0 – an invalid range. What should you do?

A: Install a DHCP Server on each remote subnet, and configure a subnet-specific scope.

131. DHCP automates the TCP/IP configuration of your Windows 2000 Professional clients. You configure options at the scope level to provide router and DNS server information to the clients. As your network has certain computers that always require a specific address and configuration, you configure reservations in your scope. Your Internet gateway has changed due to the ISP bringing a new router online. You then reconfigure your scope options to reflect the new router address. The users who have reserved addresses report that they can no longer access the Internet. What should you do? (Choose two)

A: Use the ipconfig/renew command at each client computer.
Configure the scope options to include the Perform Router Discovery option.

132. You install a DHCP server at one of your company's branch offices, and create a scope. Users in the branch inform you that each time they restart their computers, they receive the message: "DHCP in unavailable". What should you do?

A: Authorize the DHCP server.

133. You install and configure DHCP Server service on a Windows 2000 Server to automate TCP/IP client configuration. You create a scope that contains the range of valid IP addresses. You create an exclusion range, and address reservations for your TCP/IP network printers so they will always receive the same address. None

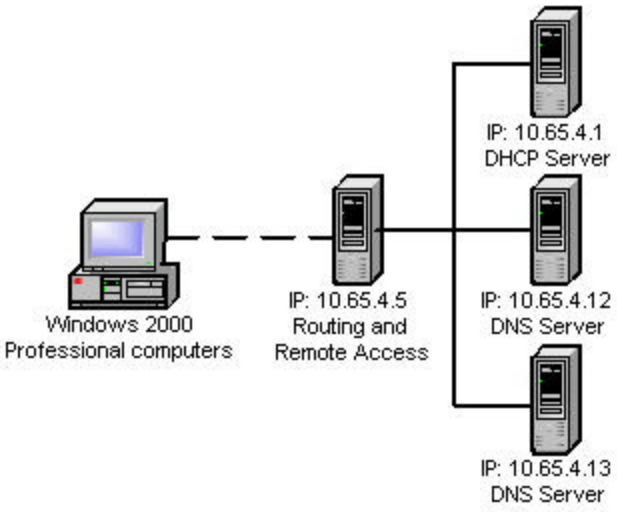
of your printers are receiving addresses from the DHCP server. Client computers are not experiencing problems. What should you do?

A: Remove the exclusion range for the addresses that are in use by the printers.

134. Your company's portable computers are frequently utilized by users at locations that are not on the network. Two DHCP servers provide TCP/IP configuration to your Windows 2000 Professional clients. You want to configure different lease times for the desktop computers and portable computers. Desktop clients should use the default lease time. Portable computes should use a lease time of four hours. What should you do? (Choose three)

A: On the DHCP servers, configure the scope options to use a lease time of four hours for the portable computers.
On the portable computers, set the DHCP class ID setting to Windows 2000 portable computers
On the DHCP servers, define a new user class that has the ID specified on the portable computers.

135. Your network is configured as follows:



The DHCP server has a scope range of 10.65.4.20 through 10.65.4.80 with a subnet mask of 255.255.255.0. Portable computers should use the DNS server when they dial in to the Routing and Remote Access server. The DHCP server sends IP address to the Routing and Remote Access server for the portable computers. You configure the DHCP scope so that it has an IP address of 10.65.4.12 for the DNS Servers scope option. When users dial in, all portable computers receive the IP address of 10.65.4.13. What should you do to ensure the portable computers will receive the IP address of 10.65.4.12 for the DNS server?

A: Configure the DHCP server to always register and update client computer information to contain the configured DNS server.

136. Your Web server is not a member of your domain. You want to allow your customers to connect to the Web server to make encryption secured online transactions. You also want to assure customers of the identity of your Web server when they make online transactions. What should you do?

A: Install a Subordinate Stand-Alone CA that uses a commercial CA as the parent.

137. Your network consists of a single domain with three Windows 2000 domain controllers, and 1,000 Windows 2000 Professional workstations. You want to use digital certificates by installing your own CA. You must protect the root CA and the private key. You must also ensure that you can manage the Public Key Infrastructure. You want to accomplish the following goals:

- **The server hosting the root CA will have maximum protection.**
- **The server hosting the root CA will certify other CAs and revoke certificates.**
- **All servers in the domain will be able to access the revocation status of all certificates in the Public Key Infrastructure.**
- **Certificate requests will be immediately processed.**

You take the following actions:

- **Install a stand-alone root CA on a member server.**
- **Disconnect the member server, and place it in a secure and separate location.**

Which results do these actions produce? (Choose all that apply)

A: The server that is hosting the root CA is protected from security breaches.
All servers in the domain can access the revocation status of all certificates.
Certificate requests are made immediately.

138. Your company wants to be able to connect to its Web server to make credit card transactions. These transactions should be encrypted. You must assure the identity of the Web server when customers make online transactions. You must be able to support certificate-based logons for employees of your company who need access to private areas on your Web server. What should you do?

A: Install a Subordinate Enterprise CA that uses a commercial CA as the parent.

139. Your company receives faxes via a Windows 2000 Server computer that has a modem installed. You install Routing and Remote Access on the server. You configure the server to connect to a branch office every six hours to synchronize the branch offices files. You automate this process by using command-line statements and the Windows scheduler. Each time your scheduled synchronization begins, your server fails to start. What should you do?

A: Stop the fax service before making the connection.

140. You have two Windows 2000 Servers named London and Bristol. London has a permanent cable modem connection to the Internet. Windows 2000 Professional computers on your network use APIPA. The network does not contain a DHCP server. You install and configure the NAT routing protocol on London to allow the Windows 2000 Professional computers access to the Internet through the cable modem. You use the IP range of 192.168.40.1 through 192.168.40.50 for the network. London uses an IP address of 19.168.40.1. Bristol is a Web server with an IP address of 192.168.40.2 and a default gateway of 192.168.40.1. Your ISP has allocated 207.46.179.16 and 207.46.179.17 to your network. You want to allow Internet users from outside your internal network to use an IP address of 207.46.179.17 to access the resources on Bristol through the NAT on London. What should you do?

A: Configure the public interface NAT routing protocol to use an address pool starting with 207.46.179.16 and a mask of 255.255.255.254. Reserve a public IP address of 207.46.179.17 for the private IP address of 192.168.40.2.

141. Your network has a Windows 2000 Server computer that has a dial-up connection that connects to the Internet. Your Windows 2000 Professional computers are configured for static TCP/IP addressing. The IP addresses are 192.168.0.1 through 192.168.0.12, and the subnet mask is 255.255.255.0. The Windows 2000 Professional computers have no default gateway configured. You realize your Windows 2000 Professional computers are not able to access the Internet through the dial-up connection. You confirm that the preferred DNS server on the client computers is configured correctly. What should you do?

A: Change the IP address on all Windows 2000 Professional computers to 169.254.0.2 through 169.254.0.13.
Change the subnet mask on the client computers to 255.255.0.0.
Change the default gateway on the client computers to 169.254.0.1.

142. Your network consists of 50 Windows 2000 Server computers, 2,5000 Windows 2000 Professional computers, 3,000 Windows 98 computers and 50 UNIX servers. You have a single Windows 2000 domain. Users store data on their client computers and on the server. You have five subnets, and a sixth subnet connecting two BOOTP routers. You use DHCP to configure TCP/IP configurations. You want to accomplish the following goals:

- **All users will be able to access resources on all servers.**
- **All users will be able to access resources on all clients.**
- **Network traffic between subnets will be minimized.**
- **You must allow for 100 percent growth over the next year with minimal reconfiguration.**

You take the following actions:

- **Place all Windows 2000 Servers on Subnet 1.**
- **Place all UNIX servers on Subnet 2.**
- **Distribute clients evenly across Subnets 3, 4, and 5.**
- **Install the DHCP Server service on one of the Windows 2000 Servers, and configure a scope for each subnet.**
- **Install and configure DNS Server service on one of the Windows 2000 Servers.**
- **Configure all Windows-based computers to use DHCP.**
- **Subnet the network address space by using 255.255.248.0.**

Which results do these actions produce? (Choose all that apply)

A: All users are able to access resources on all servers.
All users are able to access resources on all clients.

143. To distribute administrative control of the DNS namespace, you use a single standard primary DNS zone to handle all name resolution for three domains. What should you do to optimize name resolution time, while maintaining centralized control?

A: Create a new secondary zone for the east and west domains.

144. Your network has two Windows 2000 Servers named Router1 and Router2. You want to enable RIP for IP on Router1 and Router2. You configure RIP for IP on Router1 and Router2 as follows:

- **Set operation mode to Periodic update mode.**
- **Set outgoing packet protocol to RIP version 1 broadcast.**
- **St incoming packet protocol to RIP version 1 and 2.**
- **Specify Router1 and Router2 as unicast neighbors of each other.**

What should you do to guarantee the correct routes are being received?

A: Set the RIP for IP outgoing packet protocol to RIP version 2 broadcast.

145. Your network consists of a Windows 2000 Server and several Windows 2000 Professions computers. Your server has a dial-up connection to the Internet. Your Windows 2000 Professional computers are configured to use APIPA. There is no DHCP server on the network. You want to implement Internet Connection Sharing to allow the Windows 2000 Professional computers to access the Internet. How should you configure the server? (Choose all that apply)

A: Enable Internet Connection Sharing on the dial-up connection of the server.
Configure the server to use APIPA for the LAN interface.

146. Your domain has six Windows 2000-based Routing and Remote Access servers and two Windows 2000-based Internet Authentication Service servers. The Routing and Remote Access servers use the IAS server to authenticate remote access credentials. You change the remote access policies on the first IAS server. How do you ensure that this change is enforced on the second IAS server?

A: Use the Netsh command-line utility to copy the IAS configuration from the first IAS server to the second IAS server.

Microsoft Windows 2000
Directory Services Infrastructure Concepts

Active Directory Overview

The Microsoft Windows 2000 Active Directory (AD) is the central repository in which all objects in an enterprise and their respective attributes are stored. It is a hierarchical, multimaster enabled database, capable of storing millions of objects. Because it is multimaster, changes to the database can be processed at any given domain controller (DC) in the enterprise regardless of whether the domain controller is connected or disconnected from the network.

Windows 2000 Domain Hierarchy

Windows 2000 domains use a hierarchical model with a parent domain and child domains under it. A single domain tree consists of a parent domain and all of its child domains. Domains are named in accordance with the Internet's Domain Name System standard. If the parent (root) domain is called "troytec.com", a child may be called "support.troytec.com". In a Windows 2000 domain, trust relationships between domains are made automatically either by two-way, or transitive trusts. Domain A can trust Domain B, Domain A can trust Domain C, and Domain B can trust Domain C. In addition, you have the option of only having one way trusts, or no trust. The act of permissions flowing downward from parent to child is called inheritance. It is the default, but can be blocked for specific objects or classes of objects.

AD Database Overview

Forest and Trees

The AD database contains all information about objects in all the domains from logon authentication to objects in the directory. A hierarchical structure made up of multiple domains that trust each other is called a tree. A set of object definitions and their associated attributes is called a schema. All domains in a tree will share the same schema and will have a contiguous namespace. A namespace is a collection of domains that share a common root name. An example of this is support.troytec.com, marketing.troytec.com, and troytec.com. A disjointed namespace contains domains that are interrelated, but don't share common root name. This might occur when a company merges with another company. An example of this is troytec.com, and abc.com. A forest is one or more domain trees that have separate contiguous namespaces. All the trees in a forest share a common schema and trust one another because of transitive trusts. If you have multiple forests, you must set up an explicit trust between them.

Sites

Use the Active Directory Sites And Services Microsoft Management Console (MMC) snap-in to configure sites. To create a site, add the subnets the domain controllers are in to the site object. A site object is a collection of subnet addresses that usually share a geographic location. Sites can span domains, and domains can span sites. If the subnet address of a client or domain controller has not been included in any site, it is assigned to the initial site container created by

AD, named Default-First-Site. If a subnet requires fast access to the directory, it should be configured as a site. In every site, at least one global catalog server should be installed for fast directory access, and at least one domain controller should be installed.

Dynamic Domain Name System (DDNS)
AD requires Dynamic Domain Name System (DDNS) for name resolution of objects. The records in the DNS database are automatically updated instead of the normal DNS manual methods.

Organizational Units (OUs)
An Organizational Unit is a container object that can hold users, groups, printers, and other objects, as long as these objects are members of the same domain as the OU. You can organize the domain into logical administrative groups using OUs. OUs allow you to delegate the management of the objects in the OU to other users. You can assign separate sets of permissions over the objects in the OU, other than the permissions in your domain. The Active Directory Users And Computers MMC snap-in is used to create and manage OUs. To delegate the control of an OU, use the Delegation of Control Wizard.

Global Catalog
A global catalog contains all the objects in the AD, with only a subset of their attributes. This allows you to find object quickly even in a large multi-domain environment. The global catalog serves as an index to the entire structure of all domains and trees in a forest. It is also used for user authentication, so a user can log on at any location without having to perform a lookup back to the user's home domain. The first server installed in a tree is called the global catalog server. Additional global catalog servers will improve the response time of queries for AD objects. Use the Active Directory Sites And Services MMC snap-in to create additional global catalog servers.

Domain Controllers
All domain controllers in a Windows 2000 domain have a writeable copy of the AD database. All changes performed on any domain controller are replicated to all the other domain controllers within the domain via multimaster replication. Multimaster replication occurs when there is no master domain controllers, and all domain controls are considered equal. Domain controllers are not required to replicate directly with each other. Domain controllers that are in close proximity to each other can replicate with each other, and then one of them can send all the changes to a remote domain controller.

Replication
A connection object is a connection that AD uses for replication. Connection objects are fault tolerant. When a communication fails, AD will automatically reconfigure itself to use another route to continue replication. The process that creates connection objects is called Knowledge Consistency Checker (KCC). It runs on all domain controllers every 15 minutes by default. It creates connection objects that provide the most favorable route for replication at the time of replication. KCC uses the network model that has been defined to determine connectivity

between sites, but it will configure the links between domain controllers in the same site without assistance. Changes that need to be replicated are based on the update sequence number (USN). Each domain controller maintains a table of its own USNs, which is updated whenever it makes a change to an AD object. The USN is written to the AD database with the attribute that has changed. Other domain controllers use this USN to determine whether a change has occurred on a replication partner. To reduce network traffic, only the changed attribute will be transferred. After a domain controller fails, it attempts to replicate with all of the domain controllers when brought back online. It only requests updates with USNs greater than the last USN that was applied.

Sites
AD uses sites to control replication traffic over a WAN. A site is a group of domain controllers joined by a fast connection. Intrasite replication traffic can consume a large amount of bandwidth. Intersite traffic is compressed at a rate of 10:1.

Site Links
Site links are created using either Remote Procedure Call (RPC), or Simple Mail Transfer Protocol (SMTP) after sites are created. These links facilitate the replication between sites. If not created, domain controllers will not be able to send or receive directory updates. Replication availability, cost, and replication frequency can be configured for greater efficiency. The KCC uses settings from the site links to determine which connection objects to create to replicate directory data. SMTP transport is generally used for connections that are intermittent, such as dial-up links. Replication can be set up for a specific schedule by specifying when replication over that site link cannot take place, or by default, which allows replication to occur at any time. The default replication time is every three hours. Cost value determines which link to use when there are multiple links between sites. AD always uses the lowest cost path available. You can designate a domain controller as a bridgehead server to act as a replication gateway. It accepts all replication data from other sites via slow links and distributes it to other domain controllers in the site via fast links. Bridgehead servers are commonly used when sites are separated by firewalls, proxy servers, or Virtual Private Networks (VPNs).

Site Link Bridge
A site link bridge specifies a preferred route for replication traffic. It is the process of building a connection between two links. It is not needed in a fully routed IP network. If you set up site link bridges, you must turn off the default option to bridge all site links automatically.

Installing, Configuring, and Troubleshooting Active Directory

Microsoft Management Console (MMC)

MMC is a framework in which you can add custom utilities called snap-ins to administer system components. Preconfigured MMCs that are used to work with AD are:

Snap-in	Description
AD Domains And Trusts	Configures and manages trust relationships.

AD Sites And Services	Creates and manages sites, site links, site link bridges, replications and OUs.
AD Users And Computers	Creates and Manages user accounts, resource objects and security groups.
DNS	Manages DNS.
Domain Security Policy	Manages security policy for domains.

Active Directory

Installing Active Directory

Servers install as member servers (standalone) by default. Active Directory services can be only installed on a Windows 2000 Server, an Advanced Server or a Datacenter Server. You must have at least 256 MB of memory available, and at least one NTFS 5.0 partition. The Directory Services database is installed to %systemroot%\ntds\ntds.dit by default. AD depends on DNS, and as such, cannot be installed without it. During the installation program, if DNS is not found, you are given the choice of aborting the installation or installing DNS on the server you're upgrading to a domain controller.

> You do not have to reinstall the operating system to create a domain controller. A member server can be promoted to a domain controller or demoted to a member server at any time by using dcpromo. The answer file contains only the [DCInstall] section. Use the /answer**:**<answer_file> switch to specify the answer file. To remove AD and demote a domain controller to a member server, log on as an Administrator, then supply Enterprise Administrator credentials during the demotion process.

Use mixed mode (installed by default) if your domain consists of both AD and pre-Windows 2000 domain controllers. If Windows 2000 is being installed into an infrastructure where all domain controllers will be running Windows 2000, then domain controllers should utilize native mode.

Creating Sites

By default, all domain controllers are placed in the default site, Default-First-Site-Name, and the KCC handles all replication. To create a site go to Start | Programs | Administrative Tools | AD Sites And Services. Right-click Sites, and choose New Site. Type the name of your site and select a site link. If the IP address of a newly installed domain controller matches an existing subnet in a defined site, it is automatically added to that site. Otherwise, it is added to the site of the source domain controller.

Creating Subnets

Subnets are the objects used by AD to determine the boundaries of sites. Workstations use subnets to determine the closest domain controller for logons. AD uses IP subnets to find a domain controller in the same site as the system that is being authenticated during a logon and to determine the best routes between domain controllers. To create a subnet go to Start | Programs | Administrative Tools | AD Sites And Services | Sites. Right-click Subnets, and choose New Subnet. Enter the subnet address and subnet mask. Associate the subnet with a site.

Creating Site Links

Creating a site link between two or more sites influences replication. In creating a site link, you can specify what connections are available, which ones are preferred, and how much bandwidth is available. AD can use this information to choose the most efficient times and connections for replication. Site links are not created automatically, they must be manually created. Computers in different sites cannot communicate with each other or replicate data until a site link has been established between them. To create a new site link go to Start | Programs | Administrative Tools | AD Sites And Services Right-click the Inter-Site Transports folder (IP or SMTP), then click New Site Link. Provide a link name and choose the sites you want to connect. The DEFAULTIPSITELINK object is created in the IP container when AD is installed on the first domain controller in a site. Default site link cost is 100. The slower a connection, the more it should cost. The replication interval must be at least 15 minutes and cannot exceed 10,080 minutes.

Replication protocols over site links:

Protocol	Description
SMTP Replication	Only used for intersite replication. Is synchronous and ignores all schedules. Requires installation of a Certificate Authority (CA).
IP Replication	Uses Remote Procedure Calls (RPCs) for both intersite and intrasite replication. Intersite IP replication uses schedules by default. Does not require a CA.

Creating Site Link Bridges

In a fully routed network, it is not necessary to create site link bridges as all site links using the same protocol are bridged by default. When a network is not fully routed it is necessary to disable the default site link bridging. To create a new site link bridge, go to Start | Programs | Administrative Tools | AD Sites And Services. Right-click the Inter-Site Transports folder (IP or SMTP), then click New Site Link Bridge. Provide a site link bridge name and choose the site links you want to connect. To disable default site link bridging, go to Start | Programs | Administrative Tools | AD Sites And Services. Right-click the Inter-Site Transports folder (IP or SMTP), then click Properties. Uncheck the Bridge All Site Links check box.

Creating Connection Objects

Connection objects are automatically created by the Knowledge Consistency Checker (KCC). Manually adding connection objects may increase replication performance. To create a connection object, go to Start | Programs | Administrative Tools | AD Sites And Services. Open the Site folder. Next, open the Servers folder, then expand the server object to get to the NTDS Settings. Right-click NTDS Settings, and choose New Active Directory

Connection. In the Find Domain Controllers box, select the desired domain controller. In the New Object – Connection window, name the new connection.

Creating Global Catalog Servers

There should be at least one global catalog server located in every site. If your network has multiple sites, you may wish to create additional global catalog servers to prevent queries from being performed across slow Wide Area Network (WAN) links. AD creates one global catalog server per forest by default. To create a global catalog server, go to Start | Programs | Administrative Tools | AD Sites And Services. Open the Site folder, and open the Servers folder, then expand the server object to get to the NTDS Settings. Right-click NTDS Settings, and choose Properties. Select the Global Catalog Server checkbox on the General tab.

Moving Server Objects between Sites

When a server is created, it becomes a member of the site in which it's installed. To move server objects between sites go to Start | Programs | Administrative Tools | AD Sites And Services. Open the Site folder, and open the Servers folder where the server is currently located. Right-click the server to be moved, and select Move. Select the site you want to move the server object to then click OK.

Operations Master Roles

AD uses multimaster replication of the directory to make all domain controllers equal. Some operations are impractical to perform in a multimaster environment. In a single-master model, only one DC in the entire directory is allowed to process updates. The Windows 2000 Active Directory has the ability to transfer roles to any domain controller (DC) in the enterprise. Because an Active Directory role is not bound to a single DC, it is referred to as operations masters roles. There are five operations masters roles:

Role	Description
Domain naming master	Forest-level master that controls adding/deleting of domains to the forest. Responsible for domain name uniqueness.
Infrastructure daemon	Domain-level master that maintains inter-domain consistency.
PDC emulator	Domain-level master that provides support for non-AD compatible clients. Handles the replication of data to Windows NT BDCs.
Relative Identifier (RID) pool operations master	Domain-level master that allocates relative IDs to domain controllers.
Schema master	Forest-level master responsible for write updates and changes to the schema.

Transferring Operations Master Roles

In transferring operations master roles, you are moving the role from one domain controller to another. This may occur when one of the domain controllers hosting the master role should fail. Depending on the role, you must transfer the role using one of three AD snap-ins:

Role	Snap-in
Domain naming master	Active Directory Domains And Trusts
Infrastructure daemon	Active Directory Users And Computers
PDC emulator	Active Directory Users And Computers
Relative Identifier pool operations master	Active Directory Users And Computers
Schema master	Active Directory Schema

Verifying Active Directory Installation

You can verify promotion of a server to a domain controller by checking for the following items after an upgrade:

Item	Description
Default containers	Created automatically when the first domain is created.
Default domain controllers OU	Contains the first domain controller.
Default-First-Site-Name	First site is automatically created when you install the first domain controller.
Directory services database	The file Ntds.dit is installed in the %systemroot%\ntds directory.
Global catalog server	First domain controller becomes a global catalog server by default.
Root domain	Forest root is created when the first domain controller is installed.
Shared system volume	Default location is %systemroot%\Sysvol directory. Exists on all Windows 2000 domain controllers.
SRV resource records	Check the Netlogon.dns file for the LDAP SRV entry.

Implementing an Organizational Unit Structure

OUs are AD containers into which users, groups, resources, and other OUs are placed. The objects must be members of the same domain as the OU. OUs allow you to assign separate sets of permissions over the objects in the OU, and allow you to delegate administrative rights to objects. To create OUs, go to Start | Programs | Administrative Tools | AD Users And Computers. Select the domain name or in another OU. Right-click it, then choose New from the Action menu then select Organizational Unit. Enter the name of the new OU, then click OK.

OU Properties:

Property	Description
General	Description, street address, city, state or province, zip or postal code, and country or region.
Managed By	OU manager's name, office location, street address, city, state or province, country or region, phone number, and fax number.
Group Policy	OU's group policy links.

Backing Up and Restoring Active Directory

The data in AD that is backed up is called System State data. It contains the Registry, system boot file, the AD database, the SYSVOL directory, and the COM+ Class Registration database. To use the Windows 2000 Backup utility to back up the System State data, you must be a member of the Administrators or the Backup Operators group.

Performing a Nonauthoritative Restore of Active Directory

By default, when restoring System State data to a domain controller, you are performing a nonauthoritative restore. All System State components that are older than the replicated components on the other domain controllers will be brought up to date by replication after the data is restored. If you do not want this information to be updated by replication, you must perform an Authoritative Restore. Nonauthoritative restore is used for restoring System State data on a local computer only. If you do not specify an alternate location for the restored data, Backup will erase your current System State data. Only the registry files, SYSVOL directory files, and system boot files are restored to the alternate location. The AD database, Certificate Services database, and COM+ are not restored when an alternate location is selected. To restore System State data, you must first start the system in safe mode.

Performing an Authoritative Restore of Active Directory

An authoritative restore is performed immediately after a nonauthoritative restore and designates the information that is authoritative. A value of 100,000 is added to the Property Version number of every object on the domain controller. This ensures the objects on this domain controller will overwrite the copies of these objects on other domain controllers. To perform an authoritative restore, perform the standard restore procedure, but do not allow the domain controller to reboot at the end of the procedure. Click No to bypass the restart option, then close Backup. From a command prompt, type Ntdsutil. From the Ntdsutil: prompt, type Authoritative Restore. Then type Restore Database.

Startup and Recovery Settings

The paging file must be on the system partition and the pagefile itself must be at least 1 MB larger than the amount of RAM installed for the Write debugging information option to work. Use dumpchk.exe to examine contents of memory.dmp. A small memory dump needs 64K of space. Found in %systemroot%\minidump. Memory dumps are saved with the filename memory.dmp. Startup and recovery settings are accessed through Control Panel | System. Choose the Advanced tab, Startup and Recovery.

DNS for Active Directory

Installing, Configuring and Troubleshooting DNS for Active Directory

Integrating Active Directory DNS Zones With Non-Active Directory DNS Zones

The Domain Name System (DNS) is the Active Directory locator in Windows 2000. Active Directory clients and client tools use DNS to locate domain controllers for administration and logon. You must have a DNS server installed and configured for Active Directory and the associated client software to function correctly. Non-Microsoft DNS servers can be used with AD if they support SRV records and dynamic updates. The DNS server in Windows NT Server 4.0 cannot be used with AD, but BIND versions 8.1.2 and later can. Active Directory Integrated DNS uses the directory for the storage and replication of DNS zone databases. If you use Active Directory Integrated DNS, DNS runs on one or more domain controllers and you do not need to set up a separate DNS replication topology.

Configuring Zones for Dynamic DNS (DDNS) Updates

Zones can be configured for dynamic updates. Resource records will then be updated by the DHCP clients and or server without administrator intervention. The Only Secure Updates option is only available in Active Directory integrated zones. To configure DDNS, from the DNS console, select the server you want to administer and then select Forward Lookup Zones. Right-click the domain name and choose Properties. Check the Allow Dynamic Updates box on the General tab. You must do the same for the Reverse Lookup Zones. Root or "." zones cannot be configured for dynamic updates.

Managing Replication of DNS Data

Zone Transfer is the duplication of data between DNS servers that do not participate in AD. Zone Replication is the replication of data between DNS servers (on domain controllers) that participate in AD. Zone Replication DNS servers poll AD every 15 minutes for updates. Zone Transfer uses DNS Notification. There are two zone transfer types, full zone transfer (AXFR) and incremental zone transfer (IXFR):

- AXFR: When the refresh interval expires on a secondary server it queries its primary using an AXFR query. If serial numbers have changed since the last copy, a new copy of the entire zone database is transferred to the secondary.
- IXFR: Uses serial numbers, but transfers only information that has changed. The server will only transfer the full database if the sum of the changes is larger than the entire zone, the client serial number is lower than the serial number of the old version of the zone on the server or the server responding to the IXFR request doesn't recognize that type of query.

Troubleshooting

Dcpromo creates an installation log during the installation procedure that records every step, including success or failures. The file created is Dcpromo.log, and is stored in the %systemroot%\Debug directory Dns.log can be enabled for debugging purposes. It is stored in the %systemroot%\system32\dns folder. All debugging options are disabled by default because they can be resource-intensive. Use nslookup to troubleshoot problems with DNS.

Change and Configuration Management

Implementing and Troubleshooting Group Policy

Group policies are collections of computer and user configuration settings that are linked to domains, sites, computers, and organizational units. When applied, a Group Policy affects all users and computers within a container. Group Policy settings define what controls, freedoms, or restrictions are placed over an OU. Group Policy Objects can contain seven types of settings:

Setting	Description
Administrative Templates	Defines application and desktop configurations via Registry controls.
Security	Controls access and security (account policies, lockout policies, audit policies, user rights, etc.)
Software Installation	Controls installation, update, and removal of software.
Scripts	Controls when Windows 2000 will execute specific scripts.
Remote Installation Services	Controls options when Client Installation Wizard is used by RIS.
Internet Explorer Maintenance	Manages and customizes Internet Explorer.
Folder Redirection	Defines folder redirection for user profile home directories and folders.

User configuration settings apply group policies to users, regardless of what computer they have logged on to. Settings are only applied at time of logon and removed when the user logs off. Computer configuration settings apply group policies to computers, regardless of what user logs on to them. Settings are applied when Windows initializes.

Creating a Group Policy Object (GPO)

A GPO is stored in two locations; a Group Policy template (GPT), and a Group Policy container (GPC). Local GPOs are created using the Group Policy snap-in for the MMC. Site GPOs are created by Start | Programs | Administrative Tools | AD Sites And Services. Right-click the Site folder, and choose Properties, Group Policy tab. Each Windows 2000 computer can have one local GPO. Local GPOs can have their settings overridden by non-local GPOs when used in conjunction with AD. In a peer-to-peer environment, local GPOs are not overwritten by non-local GPOs. Domain/OU GPOs are created by Start | Programs | Administrative Tools | AD Users And Computers. Right-click domain or OU, and choose Properties, Group Policy tab.

Linking an Existing GPO

GPOs are linked with a container. It's through the container that GPOs are applied to individual users and computers. GPOs cannot be tied directly to users or computers. A single GPO can be linked to multiple OUs, or multiple GPOs can be linked to a single OU. Only Domain Admins and Enterprise Admins have the ability to link GPOs to domains, OUs, or

sites. To link a GPO to an existing, domain or OU, use Administrative Tools | AD Users And Computers | Right-click domain or OU, and choose Properties, Group Policy tab. Click Add then choose the policy and click OK. To link a GPO to an existing, site use Administrative Tools | AD Sites And Services | Right-click domain or OU, and choose Properties, Group Policy tab. Click Add then choose the policy and click OK.

Delegating Administrative Control of Group Policy

Delegating a GPO to a user grants that user control over the GPO, not the container to which the GPO applies. GPO management delegation includes; GPO links to sites, domains and OUs, creating GPOs, and editing GPOs. The default permissions are:

Security Group	Default Settings
Authenticated users	Read, Apply Group Policy, Special Permissions
Creator Owner	Special Permissions
Domain Admins	Read, Write, Create All Child Objects, Delete All Child Objects, Special Permissions
Enterprise Admins	Read, Write, Create All Child Objects, Delete All Child Objects, Special Permissions
System	Read, Write, Create All Child Objects, Delete All Child Objects, Special Permissions

Modifying Group Policy Inheritance

When multiple Group Polices apply to an object, the inheritance rules (order in which applied) of Group Policy apply. The order is Local GPO, Site GPO, Domain GPO, and OU GPO. Each previous GPO is overwritten by the next in line. When several GPOs are linked to a single OU, they are processed synchronously, in the order specified by the administrator.

Exceptions to Inheritance Order

Any site, domain or OU can block inheritance of group policy from above, except when an administrator has set No Override to the GPO link. No override can be set so that none of its policies will be overridden by a child container it is linked to. Loopback setting is used to merge or replace modes.

Filtering Group Policy Settings by Associating Security Groups to GPOs

By default, a GPO is applied to all members of its linked container. Filtering grants or restricts Read access to the GPO. If a user/group has Read access, the GPO can be applied; if not, it has been filtered. To apply the GPO to specific uses, modify the GPO's Access Control List (ACL). To prevent a GPO from applying to a listed group, remove the Allow setting for the Apply Group Policy setting from the Security tab. To prevent a GPO from applying to a specific user within a listed group, add the user to the list of names and then select the Deny setting for the Apply Group Policy setting.

Removing and Deleting GPOs
Deleting a GPO removes it from any sites, domains or OUs it was linked to. When a GPO link is removed, it is no longer applied, but still exists.

Managing and Troubleshooting User Environments by Using Group Policy

Group policies can be used to control the abilities of a user to perform tasks or access portions of the operating system or network. System Policies are a collection of user environment settings that are enforced by the operating system and cannot be modified by the user. User profiles refer to the environment settings that users can change. Environment control takes place via Administrative Templates. Administrative Templates control a system through editing or overwriting portions of the Registry.

Using Incremental Security Templates
Settings can be stored locally or in AD. They are secure and can only be changed by Administrators. Templates can be filtered using Active Directory. Settings are imported/exported using .INF files.

Incremental Security Templates for Windows 2000

Template	Filename	Description
Compatibility	compatws.inf compatsv.inf compatdc.inf	Sets up permissions for local users group to ensure viability of legacy programs.
Secure	securews.inf securesv.inf securedc.inf	Increases security settings for Account Policy and Auditing. Removes all members from Power Users group.
High Secure	hisecws.inf hisecsv.inf hisecdc.inf	For Workstations running in Windows 2000 native mode only. Requires all communications to be digitally signed and encrypted. Cannot communicate with downlevel Windows clients. Changes ACLs to give Power Users ability to create shares and change system time.

Assigning Script Policies to Users and Computers
Startup/shutdown scripts are assigned to computers. Logon/logoff scripts are assigned to users and run when a user logs on or off the system. When a system is shut down, Windows 2000 processes the logoff scripts then the shutdown scripts. Multiple scripts can be assigned to the same user or computer and Windows processes them using top-down logic.

Managing and Troubleshooting Software by Using Group Policy

Deploying Software by Using Group Policy
Group Policy integrates software installation into Windows 2000 in a feature known as Software Installation and Maintenance. Administrators can automate the process of installing, upgrading,

managing, and removing software from systems on the network. Windows Installer packages have a .MSI file extension.

Maintaining Software by Using Group Policy

Software packages are installed on a Windows 2000 Server in a shared directory. A Group Policy Object is created. Behavior filters are set in the GPO to determine who gets the software. The package is added to the GPO under User Configuration, Software Settings, Software Installation. Choose the publishing method, then choose OK. AD can either uninstall the old application first or upgrade over top of it. When publishing upgrades, they can be optional or mandatory for users but are mandatory when assigned to computers. When applications are no longer supported, they can be removed from software installation without having to be removed from the systems of users who are using them. They can continue using the software until they remove it themselves, but no one else will be able to install the software through the Start menu, Add/Remove Programs, or by invocation. Applications that are no longer used can have their removal forced by an administrator. Software assigned to the user is automatically removed the next time that user logs on. When software is assigned to a computer, it is automatically removed at start up. Users cannot re-install the software. Selecting the "Uninstall this application when it falls out of the scope of management" option forces the removal of the software when a GPO no longer applies.

Configuring Deployment Options

You can assign or publish software packages. Software that is published can be installed from the Control Panel, Add/Remove programs. Assigned software is installed the next time the user logs on regardless of whether or not they run it.

When software is assigned to a user, the new program is advertised when a user logs on, but is not installed until the user starts the application. Software assigned to a computer is installed automatically. A local administrator can only remove software when it is assigned to a computer. Users can repair software assigned to computers, but not remove it.

Published applications are not advertised. Applications can only be published to users, not computers. They are only installed through Add/Remove Programs or through invocation. Published applications do not self-repair or re-install if deleted.

With invocation, when a user launches an unknown file type, the client computer queries Active Directory to see what is associated with the file extension. If an application is registered, AD checks to see if it has been published to the user. If it has, it checks for the auto-install permission. If all conditions are met, the application is installed.

Non-MSI programs are published as .ZAP files. .ZAP files can only be published, not assigned.

Managing Network Configuration by Using Group Policy

Used with roaming profiles to redirect folders to a central server to prevent files from being copied back and forth from the server to the workstation every time the user logs on and off. Data that is centrally stored on a network server can be backed up regularly and does not require action on the part of the user. Use Group Policy to set disk quotas, limiting the amount of space used by special folders.

Deploying Windows 2000 Using Remote Installation Services

Deploying Windows 2000 Using Remote Installation Services (RIS)

Remote Installation Services allows you to support the installation of Windows 2000 Professional (only) onto network clients that don't have an operating system installed. A destination client can be a system with only a DHCP Preboot Execution Environment-based (PXE-based) remote boot ROM NIC, or a RIS boot disk. RIS can initiate a typical network share type of installation or use a system image transfer type of installation. A RIS Server requires DHCP Server Service, Active Directory, DNS Server Service and at least 2 GB of disk space. Hard disk must have at least two partitions, one for the Operating System and one for the images. The image partition must be formatted with NTFS. RIS packages cannot be installed on either the system or boot partitions.

Setting Up a RIS Server

Setup Wizard creates the folder structure, copies needed source files to the server, creates the initial CD-based Windows 2000 Professional image in its designated folder along with the default answer file (Ristandard.sif), and starts the RIS services on the server. To authorize the server, open Administrative Tools, DHCP. Right-click DHCP in the console tree and choose Manage authorized servers. Click Authorize and enter name or IP of the RIS server. Assign users/groups that will be performing RIS installations permissions to Create Computer Objects in Active Directory. The Client Computer Naming Format is defined through Active Directory Users And Computers. Right-click the RIS Server and click Properties, Remote Install, Advanced Settings, New Clients. Choose a pre-defined format or create a custom one. Associate an answer file (.SIF) with your image.

Install Remote Installation Services using Control Panel | Add/Remove Programs | Windows Components. Start the RIS Setup Wizard by running Risetup. Specify the Remote Installation Folder Location. For Initial Settings, choose Do not respond to any client requests. Specify the location of the Windows 2000 Professional source files for building the initial CD-based image. Designate a folder inside the RIS folder where the CD image will be stored. Provide a text name for the CD-based image.

Creating A RIPrep Image

Install Windows 2000 Professional on a source computer. Configure all components and settings for the desired client configuration. Install and configure applications. Copy the configuration to the Default User profile. To launch the RIPrep Wizard, click Start, Run and

enter: *RISServerName*\reminst\admin\i386\riprep.exe. Provide the name of the RIS Server where the image will be stored.

Installing an Image on a RIS client

Custom RIS images can be built using the RIPrep tool. It creates an installation image from a preinstalled and configured system. You can use Remote Installation Services (RIS) for Windows 2000 to install a local copy of the OS throughout the organization from remote locations. Using existing network technologies, after booting, personal computers contact a Dynamic Host Configuration Protocol (DHCP) server for an Internet Protocol (IP) address, and then contact a boot server to install the OS. Using RIS, you can send personal computers directly to an end user or staging area and install an automated, customized version of Windows 2000. The client initiates the protocol by broadcasting a DHCP Discover packet containing an extension that identifies the request as coming from a client that implements the PXE protocol. The boot server sends an offer containing the IP address of the server that will service the client. The client uses TFTP to download the executable file from the boot server. The client then initiates execution of the downloaded image.

Creating A RIS Boot Disk

If the destination desktop does not have PXE-based remote-boot ROM on its NIC, you must create a boot disk to initiate the remote installation. The boot disk creates a PXE emulator that works on supported PCI network adapters that allow them to connect to the RIS server. Since one disk works for all network adapters, a specific network boot disk is no longer required. The supported network adapters are listed in the utility that creates the boot disk. This utility is named Rbfg.exe and can be found in the network folder: \reminst\admin\i386.

Configuring Remote Installation Options

Once installed, the RIS system can be re-created and altered via the RIS host's Properties dialog box from the Active Directory Users And Computers tool. RIS can be configured to respond to clients requesting server, to respond only to authorized and known clients, to verify that the server is properly configured, and to view the current RIS clients.

Troubleshooting Remote Installations

Error	Solution
Computer displays a BootP message but doesn't display the DHCP message.	Make sure the RIS server is online and authorized and that DHCP packets are being routed.
Computer displays the DHCP message but does not display the Boot Information Negotiations Layer (BINL) message.	Make sure the RIS server is online and authorized and that DHCP packets are being routed.
BINL message is displayed but system is unable to connect to RIS server.	Restart the NetPC Boot Service Manager (BINLSVC) on the RIS Server.
Client cannot connect to RIS Server using the Startup disk.	Check network adapter driver in rbfg.exe.
Installation options are not available.	Possible Group Policy conflicts. Check to

	make sure another Group Policy Object is not taking precedence.

Managing Images for Performing Remote Installations
You can customize existing CD-based installs by modifying the associated answer file (*.SIF). For RIPrep images, the files are stored as individual source files. If modifications need to be made to the RIPrep image, apply the existing image to a client, make any required changes, and rerun the RIPrep wizard from the RIS server Admin folder to upload the new, updated image to the RIS server. You can still modify the *.SIF file associated with a RIPrep-based install, but you'll only be able to modify options that can be configured via the answer file. The RIPrep answer file, named RISETUP.SIF by default, will be located under the I386\Templates subfolder of the folder created for the RIPrep image.

Managing, Monitoring, and Optimizing the Components of Active Directory

Managing Active Directory Objects

Moving Active Directory Objects within a Domain

Objects can be moved within a domain using the AD Users And Computers console. Permissions that have been assigned directly to an object will not change when it is moved. Objects without permissions inherit the permissions of the parent container they are moved to.

Moving Active Directory Objects between Domains

An OU can be moved from one domain to another without damaging any of its GPOs. The GPO link is automatically updated. Use the Movetree command-line utility to move objects between domains. Use the Netdom command-line utility to move workstations or member servers between domains. When objects are moved their GUID remains unchanged but they receive a new SID. User objects that contain any other objects cannot be moved.

Resource Publishing in Active Directory

Publishing a resource refers to the process of creating an object in the directory that either contains the information you want to make available or that provides a reference to the object. General information is automatically published for all network users while account security information is only available to select administrator groups. Printers must be installed before they are added to AD. Use Administrative Tools, AD Users And Computers, domain node to find the container you want to add the printer to. Right-click the container and choose New, Printer. When the New Object-Printer dialog appears, type the UNC name of the printer in the Network Path box then click OK. Shared folders are published using Administrative Tools, AD Users And Computers, domain node. Right-click the container you want to add the shared folder to and choose New, Shared Folder. Enter the name of the folder in the Name box and the UNC name that you want to publish in AD in the Network Path box.

Locating Objects in Active Directory

Object	Description

Computer	Information on a computer that belongs to the domain.
Contact	A person connected to the organization. Includes phone number, e-mail, address, home page, etc.
Domain Controllers	Information on domain controllers including their DNS name, NetBIOS name, OS version, location, manager, etc.
Group	Collections of users, groups, or computers used to simplify administration.
OU	Container used to organize AD objects including other OUs.
Printer	Pointer to a printer. Windows 2000 automatically adds printers created on domain computers to AD.
Shared Folder	Pointer to a shared folder on a computer.

Using the Find Tool

Administrators can search AD via an LDAP query against the global catalog. To find objects in AD use Administrative Tools | AD Users And Computers. Right-click a domain or container in the console tree and select Find. Users can access directory objects via the search command from the Start menu, through My Network Places, or via the Find command from the AD Users And Computers snap-in. Users can search for computers, shared folders, printers, and users.

Creating and Managing Accounts Manually or by Scripting

	Description
Local accounts	Created in the local computer's Security Accounts Manager (SAM) database. Local accounts are not recognized by Active Directory. Added through Administrative Tools, Local Users and Groups.
Domain user accounts	Used by users to logon to the domain to gain access to network resources. Receive an access token from AD at logon that is checked against ACLs when accessing objects. Added through Administrative Tools, AD Users And Computers.
Built-in user accounts	Administrator and Guest.
Local user profile	Created on a computer the first time a user logs on. Stored on the local hard drive.
Roaming user profile	Created by system administrator. Stored on a server. Available from any computer on the network. Changes are saved to the profile on the remote server.
Mandatory user profile	Created by system administrator. Only administrators can change mandatory profiles.

Accounts should only be deleted when they will no longer needed. Renaming an account retains all rights, permissions and group memberships and assigns them to a different user. Disable accounts when they are not going to be needed for an extended period but may be needed again.

Creating and Managing Groups

Security groups are used to assign permissions for accessing objects in AD. Distribution groups are used for non-security related functions, and can only be accessed by AD-aware programs such as Exchange Server 2000. Accounts go into global groups which then go into local groups that are assigned permissions to a resource. Global groups can only contain members from the domain in which the group was created. Use global groups to assign permissions for gaining access to resources located in any domain in the tree or forest. They contain other global groups when running in native mode. Domain Local groups can contain members from any domain. They only access resources in the domain where the group was created. They contain global groups, and should not be used to assign permissions to AD objects. Universal groups can include members from any domain. They contain other global and universal groups. Putting users in universal groups affects logon performance. Universal groups are not available in mixed-mode. Objects with identical security requirements should be placed into OUs. All objects inside the OU will inherit the same permissions.

Controlling Access to Active Directory Objects

The Access Control List (ACL) is a list of user access permissions for every AD object. Permissions can be used to assign administrative privileges to users, groups, OUs, or any other object without giving control over other AD objects. Permissions are cumulative, except for Deny. A user with read access to an object in one group and write access to the same object in another group would have a cumulative access of read and write. The exception to this is deny, which overrides all other permissions.

Standard permissions include:

Permission	Description
Read	Can view objects and their attributes, the owner of the object and AD permissions.
Write	Modify attributes of object.
Full Control	Change all permissions and take ownership.
Create All Child Objects	Can add any type of child object to an OU.
Delete All Child Objects	Can delete any type of object from an OU.

Delegating Administrative Control of Objects in Active Directory

Permissions flow from the parent container to the child container unless inheritance has been prevented. Delegations should be accomplished using the Delegation of Control Wizard. Options include:

Option	
AD Object Type	Selects scope for tasks being delegated: This folder, Existing Objects In This Folder, and Creation of Objects In This Folder, or Only The Following Objects In This Folder.
Permissions	General is the most common. Property Specific includes

	permissions that can be assigned to the attributes of the object. Creation/Deletion of Specific Child Objects is the ability to create and delete child objects.
Tasks to Delegate	Select tasks from a list or create custom tasks you want to delegate.
Users or Groups	Select the users/groups you want to delegate control to.

Managing Active Directory performance

Domain Controller Performance

Performance Console:

Object	Description
Cache	File system cache used to buffer physical device data.
diskperf	Command for activating disk counters. Is not supported in Windows 2000.
Logical disk - Disk Queue Length	If averaging more than 2, drive access is a bottleneck. Upgrade disk, hard drive controller, or implement stripe set.
Logicaldisk	Logical drives, stripe sets and spanned volumes.
Memory	Physical and virtual/paged memory on system.
Memory - Committed bytes	Should be less than amount of RAM in computer.
Memory - Pages/sec	Add more RAM if more than 20 pages per second.
Physical disk - % Disk Time	If above 90%, move data/pagefile to another drive or upgrade drive.
Physical disk - Disk Queue Length	If averaging more than 2, drive access is a bottleneck. Upgrade disk, hard drive controller, or implement stripe set.
Physicaldisk	Monitors hard disk as a whole.
Processor	Monitors CPU load.
Processor - % CPU DPC Time	Measures software interrupts.
Processor - % CPU Interrupts/Sec	Measures hardware interrupts. If processor time exceeds 90% and interrupts/time exceeds 15%, check driver.
Processor - % Processor Time	Measures time CPU spends executing a non-idle thread. If continually at or above 80%, upgrade CPU.
Processor - Processor Queue Length	More than 2 threads in queue indicates CPU is a bottleneck for system performance

Performance Alerts and Logs

By default, log files are stored in the \Perflogs folder in the system's boot partition. Log types include Alert logs, Counter logs, and Trace logs. Alert logs log an event, send a message or run a program when a user-defined threshold has been exceeded. Counter logs record data

from local/remote systems on hardware usage and system service activity. Trace logs are event driven and record monitored data such as disk I/O or page faults.

Troubleshooting Active Directory Components

Problem	Solution
Cannot add/remove domain.	Domain Naming Master is not available. Network problem or failure of computer holding the master role. Seize the role to another system.
Cannot create objects in AD.	Relative ID master is not available due to failure of the computer holding master role or a network problem. If the network problem or the computer holding the master role cannot be repaired, seize the role to another system.
Cannot modify the schema.	Schema master is not available due to failure of computer holding master role or network problem. If problem cannot be resolved, seize the role to another computer.
Clients cannot access resources in a different domain.	Trusts may have failed between domains. Reset and verify trusts.
Clients without AD client software cannot logon.	PDC emulator not available possibly caused by network problem or failure of system holding master role. If problem cannot be resolved, seize the role to another system.

Managing and Troubleshooting Active Directory Replication

Managing Intersite Replication

Replication takes place for domain controllers between sites (intersite replication) based upon a schedule, the amount of network traffic, and costs. The replication schedule, defined by site link and connection objects, is used to define the time that replication is allowed to occur. The replication interval is used to define how often replication should occur during a "window of opportunity" based on the schedule. Bridgehead servers are computers with additional hardware or network capacity that are specified as preferred recipients for intersite replication. The bridgehead server subsequently replicates its AD information to its replication partners. Using bridgehead servers improves replication performance between sites. When using a firewall proxy server, you must establish it as a bridgehead server and allow it to replicate AD information to other domain controllers outside the firewall.

Managing Intrasite Replication

Replication takes place between domain controllers within a site (intrasite replication) as needed without regard to cost or schedules. Domain controllers in the same site replicate using notification. When one domain controller has changes, it notifies its partners. The partners then request the changes and the replication occurs.

Urgent replication triggers:

Events replicated immediately in native-mode domains:

- changing an LSA secret
- newly locked-out account
- RID manager state changes

Events replicated immediately in mixed-mode domains:

- changes to account lockout policy
- changes to domain password policy
- changing an LSA secret
- changing the password on a machine account
- inter-domain trust password changes
- newly locked-out account
- RID manager state changes

Active Directory Security Solutions

Configuring and Troubleshooting Security in a Directory Services Infrastructure

Applying Security Policies by Using Group Policy

You must have the Manage Auditing and Security Log user right on the system where you need to implement an audit policy or review the audit log. Used to track success/failure of events like logon attempts, accesses to a specific file, modifications to a user account, group memberships, and security setting modifications. Audited events are written to the Event Viewer.

Security Configuration and Analysis and Security Templates

The security database (mysecuresv.mdb) is compared to an incremental template (hisecsv.inf) and the results displayed in the right pane. The log of the analysis will be placed in %systemroot%\security\logs\mysecure.log.

Implementing an Audit Policy

Type secedit /refreshpolicy machine_policy at a command prompt to start policy propagation. By default policy propagation takes place every 8 hours.

Auditable Events:

Event	Description
Account logon events	A domain controller received a request to validate a user account.
Account management	An administrator created, changed, or deleted a user account or group. A user account was renamed, disabled, or enabled, or a password was set or changed.
Directory service access	A user gained access to an Active Directory object. Configure specific Active Directory objects for auditing to log this type of event.

Logon events	A user logged on or logged off, or a user made or canceled a network connection to the computer.
Object access	A user gained access to a file, folder, or printer. Configure specific files, folders, or printers for auditing. Directory service access is auditing a user's access to specific Active Directory objects. Object access is auditing a user's access to files, folders, and printers.
Policy change	A change was made to the user security options, user rights, or audit policies.
Privilege use	A user exercised a right, such as changing the system time.
Process tracking	A program performed an action.
System	A user restarted or shut down the computer, or an event occurred that affects Windows 2000 security or the security log.

Monitoring and Analyzing Security Events

Logs are accessed through Administrative Tools, Event Viewer. Logs include the Application log which contains errors, warnings, or information generated by programs running under Windows, the System log which contains errors, warnings, or information generated by Windows 2000, and the Security log which contains information about success/failure of audited events. The Event Viewer contains entries of events related to the operation of the operating system and various applications. A Windows 2000 domain controller has six logs available. These include:

Log	Description
Application log	Contains events generated by application programs. Contain errors, warnings, informational events, and events generated by the Alert log.
Directory Service	Contains events relating to the operation of AD.
DNS Server	Contains events relating to the operation of the DNS server.
File Replication Service	Contains errors and events that occur when domain controllers are updating.
Security Log	Contains information on security events, such as logon attempts and accessed resources.
System Log	Contains events generated by Windows 2000 components, drivers, and services.

Implementing and Administering a Microsoft Windows 2000 Network Infrastructure Practice Questions

1. **All users in your Support OU use an application named LocatorID. The LocatorID application was deployed using a GPO named Locator App, which was configured to publish the LocatorID application to the Support OU by using the Windows Installer package. Only users in the Support OU can start the LocatorID application. What should you do to ensure all users in the domain can install the locator application by using the Start menu shortcut?**

   A: Remove the Locator App GPO link to the Support OU.
   Assign the Locator App GPO to the domain.
   Change the configuration of the Locator App GPO to assign the LocatorID application to users.

2. **You are using Microsoft Systems Management Server to install applications on all of your client computers. A custom configuration is required for each of them. What do you need to do to use RIS to install Windows 2000 on all the client computers?**

   A: Create a CD-based RIS image and different answer files for each custom configuration.

3. **You are deploying an application named Accounting that will be used by all users in your domain. You have been given a Windows Installer package for the installation. During the initial deployment, only members of a security group named Accounting Pilot will use the application. In the second half of the deployment, all users in the domain will install and use the application. You want to accomplish the following Phase 1 goals:**
   - **Only members of the Accounting Pilot group will be able to install the application using a Start menu shortcut – no other users can.**
   - **The application will not be automatically installed when users log on.**
   - **After Phase 1, the application will be installed automatically the first time any user logs on.**

   You take the following actions:
   - **Create a GPO named Deploy Accounting and link the Deploy Accounting GPO to the domain.**
   - **Configure the Deploy Accounting GPO to assign the Accounting application to users.**
   - **For Phase 1, create a software category named Accounting Pilot. Assign the Accounting application to it.**
   - **For Phase 2, remove the Accounting application from the Accounting Pilot software category.**

Which results do these actions produce? (Choose all that apply)

A: During Phase 1, the Accounting application is not installed automatically when users log on.

During Phase 1, users who are members of the Accounting Pilot group can install the Accounting application by using a Start menu shortcut.

4. What actions should you audit to identify users who have been deleting files from your server? (Choose two)

A: Directory services access.
Process tracking.

5. Users in your Boston domain use different Windows 2000 Professional computers. You want to accomplish the following goals:

- **Changes made to the desktop settings will not be saved when users log off.**
- **All users in the domain will be able to work on all Windows 2000 Professional computers and have their own predefined desktop settings available.**
- **Users can make changes to their desktop settings.**

What should you do?

A: Configure a roaming profile for each user in the domain. Use \\Boston\Profiles\%Username% as the profile path. On the Boston server, rename the Ntuser.dat file to Ntuser.man for each user.

6. All users in your domain are members of the Power Users group, and use Windows 2000 Professional computers. Randy has dial-up access to the Internet. You do not want other users to share Randy's Internet connection. What should you do?

A: Create a GPO that disables the configuration of connection-sharing. Grant Randy Read and Apply Group Policy permissions to the GPO.

7. You have a single top-level OU named HQ, and five child OUs named after your company's internal departments, Sales, Marketing, Accounting, Shipping and Support. Users in the first four departments require the same desktop settings. Users in the Support OU require a less restrictive setting. You want to accomplish the following goals:

- **Group Policy will be automatically applied when new child OUs are added to the domain.**
- **Group Policy from the HQ OU will not be applied to the Support OU.**
- **All assigned Group Policy settings in the HQ OU will be applied to all users and computers in the Sales, Marketing, Accounting and Shipping OUs.**

- **Users should not be able to change their Group Policy settings.**
- **Administrators in the Support OU will be able to change the Group Policy settings.**

You take the following actions:

- **Create and configure the GPO, and link the GPO to the HQ OU.**
- **Select No Override in Group Policy Options for the HQ OU.**
- **For the Support OU, select Block Policy inheritance in the Group Policy dialog box.**
- **Assign the Authenticated Users group Full Control permission to the GPO.**

Which results do these actions produce? (Choose all that apply)

A: All assigned Group Policy settings in the HQ OU are applied to all users and computers in the Sales, Marketing, Accounting and Shipping OUs.
Group Policy from the HQ OU is not be applied to the Support OU.
Administrators in the Support OU are able to change the Group Policy settings.
Group Policy is automatically applied when new child OUs are added to the domain.

8. You have RIS installed on your Windows 2000 domain server. You want to use RIS to install new client computers. When you start a test client computer, the Client Installation Wizard does not appear. Your network adapter cards are not PXE compliant. What should you do to connect to the RIS server?

A: Run Rbfg.exe to create a RIS boot disk.

9. You want to standardize the Start menu for users in your Main OU. Some members of the Domain Admins group are in the Main OU. Folders and shortcuts are on the network at \\Srv1\Menu. The Everyone group has Change permissions on the Menu share. You want to accomplish the following goals:

- **Each user who is not a member of the Main OU will have a separate Start Menu that they can change.**
- **Users who use the \\Srv1\Menu Start menu will not be able to change the contents of the Start menu.**
- **Each Domain Admin member should have a separate Start menu that they can change.**
- **All users except Domain Admin members will use the \\Srv1\Menu Start menu.**

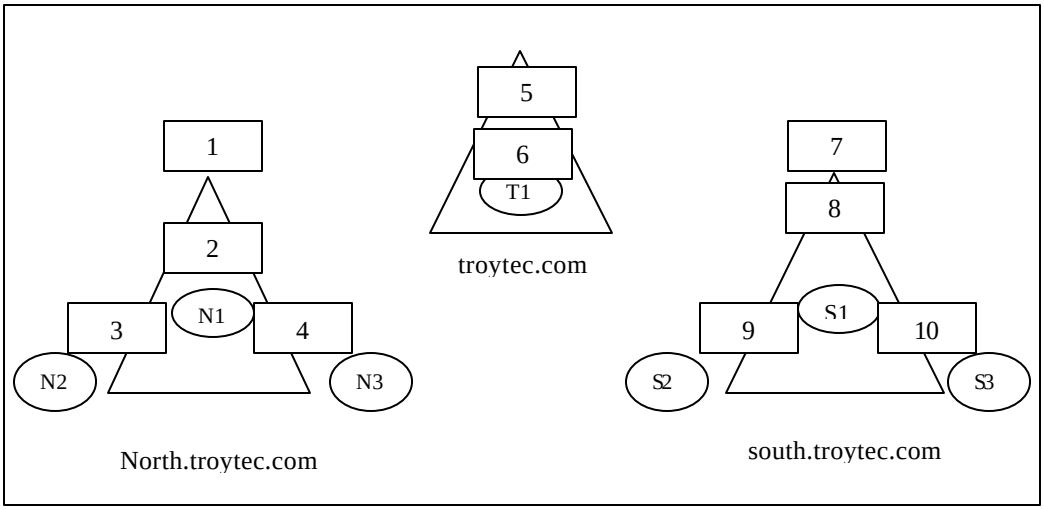
You take the following actions:

- **Create a GPO named Menu. Assign the Menu GPO to the Main OU.**
- **Configure the Menu GPO to redirect the Start menu folder for the Domain Users group to \\Srv2\Menu.**
- **Change the permissions on the Menu GPO to deny Apply Group Policy permission to the Domain Admins group.**

Which results do these actions produce? (Choose all that apply)

A: Each Domain Admin member has a separate Start menu that they can change.
All users except Domain Admin members use the \\Srv1\Menu Start menu.
Users who use the \\Srv1\Menu Start menu are not able to change the contents of the Start menu.
Each user who is not a member of the Main OU has a separate Start Menu that they can change.

10. Your network has three domains named troytec.com, north.troytec.com, and south.troytec.com. All are in a site named Sacramento, and contain OUs. You are implementing a new desktop policy for all users on the network in a GPO named Troydesktop. You are also implementing a logon script, which in configured in a GPO named Troyscript, for users from the N2 OU. Users in the N2 OU always log on to Windows 2000 Professional computers defined in the N3 OU. You do not want Group Policy filtering. What should you do to have the fewest GPO assignments possible? (Drag and drop each GPO only once)



A: Drag Troydesktop to position number 6, and drag Troyscript to position number 2.

11. You have four RIS servers in two segments. RIS server 1 and 2 are in segment A, and RIS server 3 and 4 are in segment B. The segments are linked by a router. Each segment has approximately the same number of Windows 2000 Professional clients. Using RIS, you deploy Windows 2000 Professional on 100 computers. RIS servers 1 and 3 are responding slowly, and are overworked. What should you do for a more consistent performance?

A: Create prestaged computer accounts for all the computers. Specify which RIS server will control each computer.

12. You have a script file that changes settings to users' desktops in the current user profile. It is deployed as a logon script for all users in the domain. What should you do to ensure that each user's desktop only appears after the script file completes its work?

A: Create a new GPO.
Assign the GPO to the domain.
Add the script to the GPO as a logon script.
Configure the GPO to run logon scripts synchronously.

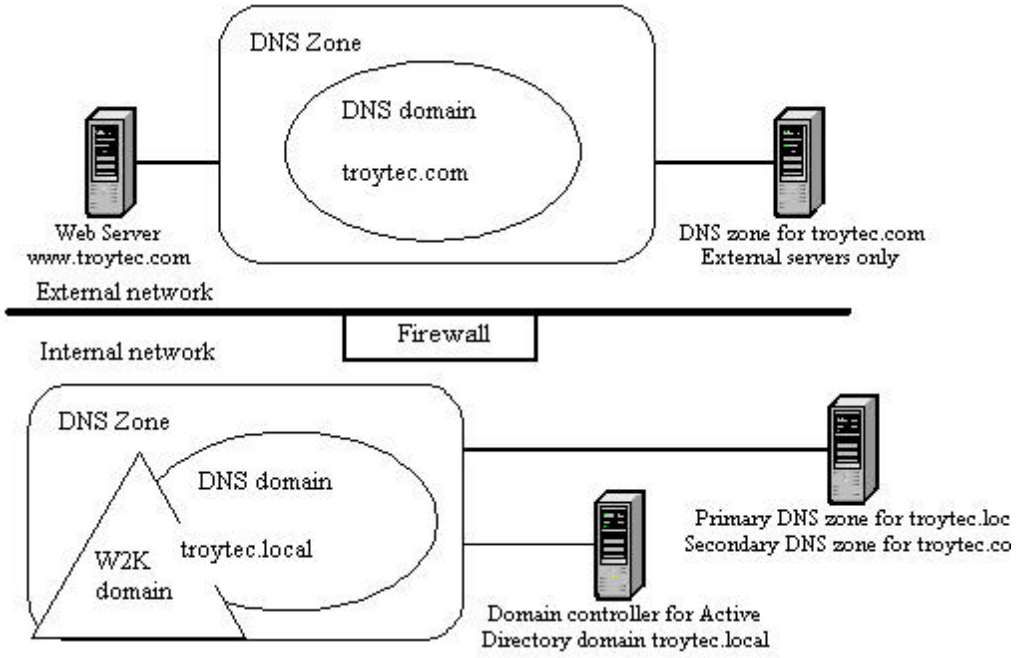
13. You want to use a GPO to assign a logon script to users in your Sales OU. What should you do?

A: Create a new GPO named Script and assign the Script GPO to the Sales OU.
Copy the logon script to the folder that is shared as Netlogon on the PDC emulator.
Add the script as a logon script to the Script GPO.

14. You are designing a Windows 2000 domain. Your company owns troytec.com, a registered domain name. The existing DNS zone is hosted on Windows NT 4.0 servers. You want to accomplish the following goals:

- **The existing DNS servers will not be upgraded.**
- **Internal users will resolve external names for access to Internet resources.**
- **Internal host names will not be exposed to the Internet.**
- **Depth of domain names and complexity for Active Directory will be minimized.**

You design a DNS implementation as shown:



Which results do these actions produce? (Choose all that apply)

A: Internal host names are not exposed to the Internet.
Internal users resolve external names for access to Internet resources.
Depth of domain names and complexity for Active Directory are minimized.

15. Your network consists of two segments connected by a router. Segment A contains downlevel client computers and a server serving as a DHCP relay. Segment B's client computers are all Windows 2000 Professional computers. All client computers in the network use DHCP. Segment B also contains a server serving as a domain controller and DNS server, a server serving as a DHCP server, and a server serving as a DNS server. Several days after you share some resources on client computers on Segment A, you are unable to resolve the host names of client computers when you attempt to connect to those resources from computers on Segment B. What should you do?

A: On the DHCP server in segment B, enable updates for DNS clients that do not support dynamic updates.

16. Server1 in your Windows 2000 network is configured with the primary zone for troytec.com. A DNS server in Boston and in Tampa are configured with secondary zones for troytec.com. You discover an error in several host records that prevents clients in Tampa from accessing shared resources. You make the necessary corrections on Server1. You want these changes to be propagated to Tampa immediately. What should you do?

A: On the DNS server in Tampa, perform the Transfer from master action for the troytec.com zone.

17. You are configuring DNS throughout your Windows 2000 domain which spans multiple subnets. You want to accomplish the following goals:

- **Zone transfer information will be secure.**
- **Administrative overhead for DNS zone files is minimized.**
- **DNS zone transfer traffic is minimized.**
- **Unauthorized host computers will not have records created in the zone.**
- **Zone updates will come only from authorized DNS servers.**

You take the following actions:

- **Create an Active Directory integrated zone.**
- **Set Allow Dynamic Updates to Yes.**
- **Enter the names and addresses of all DNS server on the network in the Name Servers tab of the Zone Properties dialog box.**

Which results do these actions produce? (Choose all that apply)

A: DNS zone transfer traffic is minimized.
Administrative overhead for DNS zone files is minimized.

18. Your network has four servers located in two cities. Server1 and Server2 are in Boston, and Server3 and Server4 are in Dallas. You install Server2 and Server4 as domain controllers, and Server1 and Server3 as DNS servers for troytec.com. Each server has a standard primary zone named troytec.com, and the domain runs in native mode. When you attempt to contact Server4 by name from Server2, you cannot connect. But, you can ping Server2 and Server4 from any computer in either site. You want information to be regularly updated. What should you do to be able to resolve names of servers in both sites?

A: Re-create the troytec.com zone on Server3 as a secondary zone. Configure Server3 to replicate DNS data from Server1.

19. A user's account has been deleted. You have been auditing all objects in Active Directory since the domain was created. You are not able to find a record of the deletion. What should you do to identify the person who deleted the account?

A: Search the security event logs on each domain controller for account management events.

20. You have edited the Default Domain Controllers Group Policy to require passwords to be at least ten characters long. But, users are still able to create passwords with less than ten characters. What should you do?

A: Edit the Default Domain Group Policy to require passwords to be at least ten characters long.

21. You want to implement a stricter network security policy that requires encrypted TCP/IP communication. What should you do?

A: Create a GPO for the domain, and configure it to assign the Secure Server IPSec Policy.

22. You want to configure security auditing on your servers to monitor access to specific folders. When the security logs become full, you want to prevent users from gaining access to these servers. What should you do?

A: Create a GPO that applies to the servers. Configure the GPO to enable auditing for object access. Set up the individual objects to be audited in Windows Explorer. Configure the security event log so that it does not overwrite events. Configure the GPO to enable the Shut down the system immediately if unable to log security audits setting.

23. You implement a security policy to be in effect at all times on all clients in your network. Administrators periodically change security settings on computers when they are troubleshooting. How can you automate the security analysis and configuration of client computers so that you can track changes to the security policy and reapply the original security policy when it is changed?

A: Schedule the secedit command to run on the client computers.

24. You want to use a custom built security template on five domain controllers in your domain. What should you do? (Choose two)

A: Import the custom-built template file.
Create a GPO on the Domain Controllers OU.

25. Using the least amount of administrative effort, how can you duplicate security settings from one domain controller to four other domain controllers?

A: Create a GPO for the Domain Controllers OU. Configure the GPO settings to match the settings of the secured domain controller.

26. Your domain has four OUs. In an effort to centralize security policy in your domain, you create three security template and GPOs:

- **SecPol1 defines Password, Audit and User Rights policies.**
- **SecPol2 defines User Desktop policy, File System security, and Registry security.**
- **SecPol3 defines a High Security User Desktop policy for network administrators.**

You want the GPOs to apply the security policies to users and computers in the domain with the fewest assignments possible. You want Group Policy to apply at the OU level for more granular administrative control. What should you do? (Select and Place)

A: Drag SecPol1 to all locations.

27. The volume that contains the Active Directory database file on Server1 is running out of disk space. What should you do to move the database file to an empty volume on a different disk on Server1?

A: Restart Server1 in directory services restore mode. Use Ntdsutil to move the database file to the empty volume.

28. Your network consists of two domains and six sites. Site A and Site C are connected by a T1 line. Site A and Site B are connected by a T1 line. Site C and Site F are connected by a T1 line. Site B and Site D utilize a 56 Kbps connection. Site C and Site E utilize a 128 Kbps connection. Each site has one or more domain controllers. One domain controller in each site is configured as a global catalog server. Network performance and data transfer for an application located in Site A are extremely poor. What should you do to improve performance?

A: Create site links between all sites and set less frequent replication schedules.

29. Your domain contains three domain controllers. DC1 does not hold any operations master roles. You backed up the System State data of DC1 two weeks ago. The hard drive on DC1 fails. You want to replace DC1 with a new computer that you've installed Windows 2000 Server on. What should you do next?

A: Use the Active Directory Installation wizard to make the new computer a replica in the domain.

30. One of your administrators has deleted an empty OU named Remote1 from ServerA. Before the deletion is replicated to ServerB, another administrator moves users into Remote1 from ServerB. What should you do to reinstate the configuration where users are moved into Remote1?

A: At ServerB, create a new Remote1 OU. Move the users from the LostAndFound container to the new Remote1 OU.

31. Your domain has three domain controllers name DC1, DC2, and DC3. You want to replace DC1 with a newer computer named DC4. DC4 should be a domain controller in the domain, and DC1 should no longer function as a domain controller. What should you do?

A: Install DC4 as a member server in the domain.
On DC4, use the Active Directory Installation wizard to install Active Directory on DC4.
On DC1, use the Active Directory Installation wizard to remove Active Directory from DC1.

32. Your Windows 2000 Server servers as a domain controller and a DNS server. When Windows 2000 Professional clients attempt to log on, they receive an error message that the domain controller cannot be located. Active Directory is installed and functioning. What should you do?

A: Check DNS for the addition of an appropriate SRV (service) record in the zone.

33. You want to create an Active Directory structure to allow local administrators at branch offices to control users and local resources. They should be prevented from controlling resources in branch offices other than their own. What should you do?

A: Create a child OU for each office. Delegate control of each OU to the local administrators at each office.

34. You want to create an Active Directory structure to allow local administrators at each branch office to be able to only control their own local resources. Only administrators from the main office should be allowed to create and manage user accounts. What should you do?

A: Create a single domain. Create an OU for each branch office and an additional OU named MainUsers. Delegate authority for resource administration to the local administrators for their own OUs. Delegate authority to the MainUsers OU only to the Domain Admins group.

35. You manage a multi-domain Windows 2000 network for two companies; Troytec and Support Systems. Each of the six departments has an OU in Active Directory. Each domain and OU has specific Group Policy settings that must be applied to all of its members. Some users have moved to different departments, and some have changed domains. You want to accomplish the following goals:

- **No user access disruption.**
- **Place user accounts in the appropriate domains.**
- **Apply existing policies for each domain or OU to the moved accounts.**

What should you do?

A: Use the Movetree utility for the users moving between domains. For users moving between OUs in the same domain, select the accounts, then from the Action menu, choose Move.

36. Your single domain contains three sites with two domain controllers each. You have two IP site links: Boston_Chicago, and Salem_Chicago. You want to add another domain controller in each site to handle all replication from each site. What should you do?

A: Configure each new domain controller to be the IP preferred bridgehead server for its site.

37. You hire a LAN administrator for your Salem office. Your network consists of one domain. Each office has its own OU. The new LAN administrator needs to be able to create child OUs under only ou=Salem,dc=troytec,dc=com and verify the existence of the created OUs. What permissions should you assign the LAN administrator? (Choose three)

A: List Contents
Create OU Objects
Read

38. Your network has three native mode domains: troytec.com, sales.troytec.com, and support.troytec.com. You want to remove sales.troytec.com. How should you move the sales.troytec.com users at the same time to troytec.com?

A: At the command prompt, type:
Movetree /start /s dc1.sales.troytec.com /d dc1.troytec.com /sdn cn=users,dc=sales,dc=troytec,dc=com /ddn cn=users,dc=troytec,dc=com

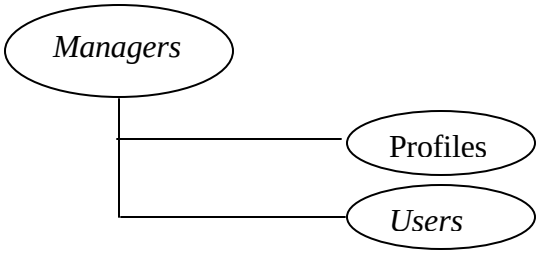
39. Your Ntds.dit file remains the same size over the course of a year, even though you have deleted numerous objects. How do you reduce the size of the Ntds.dit file? (Choose two)

A: Restart the server in directory services restore mode.
Use the Ntdsutil utility to compress the database to another drive.

40. All five of your domains run in native mode. Each domain has at least one Support personnel member. Each domain has a global group named Support Members that contains the Support personnel from each domain. You want all the Support staff to be able to reset passwords in an OU named Accountants. What should you do?

A: In the root domain create a new universal security group named Support Staff.
Place the five Support Members groups in the Support Staff group.
In the root domain create a new local security group named Reset Accountants. Place the Support Staff in this new local security group.
On the Accountants OU, assign the Reset Password permission to the Reset Accountants group.

41. Your OU structure is as follows:



You grant Create User Objects permissions to Lane for the Managers OU, but he is unable to create users objects in the Users OU. Lane is able to create users objects in the Profiles OU. What should you do?

A: In the Users OU, select Allow inheritable permissions from parent to propagate to this object.

42. You recently added three new SCSI hard disk drives to your domain controller which already had two physicals disks. The SCSI disks are configured in a RAID-5 array. How should you optimize the speed of the Active Directory database? (Choose two)

A: Move the Ntds.dit file to the RAID-5 array.
Move the log files to a separate physical disk from the operating system.

43. You enable a new domain controller name G1 as a global catalog. It will take the place of your existing G0 global catalog server. You want to use G0 only as a domain controller, and increase its disk space. What should you do? (Choose all that apply)

A: Use Active Directory Sites and Services.
Select the NTDS Setting object for the G0 server to clear the Global Catalog check box.
On the G0 server, run the Ntdsutil utility to defragment Active Directory.

44. You install a new Windows 2000 Server computer on your existing Windows NT network. To promote the server to a domain controller named domain.local, you run DCPromo.exe. There are no other Windows 2000 domains on your network, but you receive the error: "The domain name specified is already in use". What should you do?

A: Change the downlevel domain name to domain1.

45. Your network has two native mode domains in six sites. Each site has at least one domain controller. Authentication and directory searches are slow during high network usage. What should you do to improve network performance?

A: Designate a domain controller in each site as a global catalog server.

46. What should you do to automatically back up the Active Directory database files for your domain controllers once a week?

A: Schedule a backup job that will back up the System State data once a week.

47. You are installing a new domain named troytec1.local. You receive the error: "The domain name specified is already in use" during the promotion process. What is the cause of the problem?

A: The default-generated NetBIOS domain name is already in use.

48. Your company has four locations connected by 256 Kbps leased lines. You have a Windows 2000 domain controller at each location. What should you do to control bandwidth usage and the replication schedule of directory information to each domain controller in each location? (Choose two)

A: Create a site for each location.
Move each server object from Default-First-Site-Name to the appropriate site.

49. What should you do to strengthen your security to protect against brute force attacks? (Choose two)

A: Enable Password must meet complexity requirements.
Increase minimum password length.

50. You suspect someone has been modifying the properties of user accounts in Active Directory. You need to isolate and review events pertaining to a user reporting that they are unable to change their password. Using the least possible amount of time, how can you review the event logs for an isolated event?

A: In the security log, create a filter for events matching the criteria: Event source: Security, Category: Account Management. Search the remaining items for events referencing the user's account.

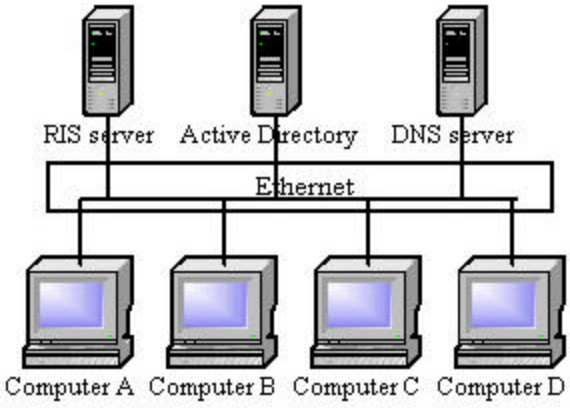
51. You have delegated the authority to create and delete computer accounts to one of your users. A second user is delegated with change user account information. A third user is delegated the ability to add client computers to the domain. What should you do to track the changes made to the directory by these three users?

A: Create a GPO for the domain controllers.
Assign Read and Apply Group Policy permissions to the three users.
Configure the GPO to audit directory services access and account management.

52. Users in your OU need to have a drive mapped during logon. Using a logon script, what should you do to implement this drive mapping for all current and future users in the OU?

A: Create a GPO that enforces the logon script as a logon script.
Assign the GPO to the OU.

53. You install a RIS server to expedite the deployment of Windows 2000 Professional on your network. When you attempt to use the RIS server to deploy Windows 2000 Professional on computers A and B, you cannot establish a connection. Computers C and D installed Windows 2000 from CD-ROM without any problems. What should you do?



A: Install a DHCP server and authorize it in Active Directory.

54. You have created a GPO and filter it to users in your Windows 2000 network. You discover that users are re-using the same password. You want to configure the GPO to require users to create different passwords periodically for security. What two settings should you enable to accomplish this goal? (Choose two)

A: Minimum password length.
Enforcement of password history.

55. Your Windows 2000 domain is running in native mode. You are going to implement a policy to disable the Shutdown command for all users, except for members of the Domain Admins security group. You create a new GPO named Shutdown, and configure it to disable the Shutdown option. You assign it to the domain. What should you do to ensure that the Domain Admins group is not affected by the policy?

A: Deny the Apply Group Policy permission to the Domain Admins group on the Shutdown GPO.

56. Your domain has an OU named HelpDesk. Users in the HelpDesk OU use their portable Windows 2000 Professional computers when they are not connected to the network. You have a Windows 2000 Server named Data1. Files used by the HelpDesk OU are contained in the \\Data1\SupFiles share. You want to accomplish the following goals:

- **Users of the HelpDesk OU can access the shared files when they are not connected to the network.**
- **Total disk space on the portable computers to automatically store files will not exceed 5 percent of the hard disk space.**

What should you do? (Choose all that apply)

A: Configure the SupFiles share on the Data1 server to cache documents automatically.
Create a new GPO named Maxdisk.
Assign the Maxdisk GPO to the HelpDesk OU.
Configure the Maxdisk GPO to limit the automatically cached offline files to 5 percent of the hard disk space.

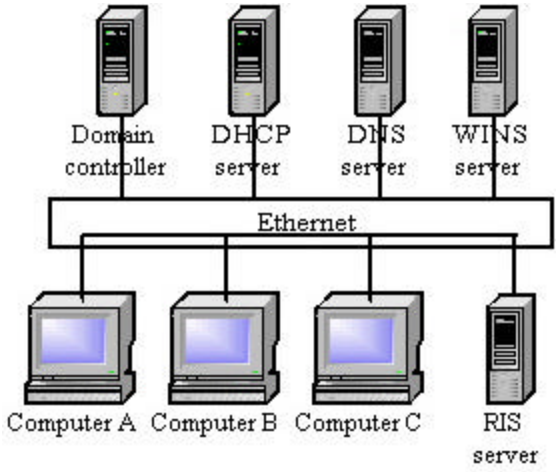
57. Your Windows 2000 domain has a Windows 2000 Server named Boston. You want to enable roaming profiles for all users, as they use different Windows 2000 Professional computers. You want to accomplish the following goals:

- **All users can use any Windows 2000 Professional computer utilizing their own desktop settings.**
- **Users can make changes to their desktop settings.**
- **Users can access their documents in the My Documents folder from any computer.**
- **The amount of data copied between the server and the My Documents folder will be minimized during log on or log off.**

What should you do? (Choose two)

A: Configure a roaming profile for each user. For the profile path, use \\Boston\Profiles\%Username%.
Create a new GPO named Docs. Assign the Docs GPO to the domain. Configure the Docs GPO to redirect the My Documents folder to the \\Boston\Docs\%Username% location.

58. You recently install a RIS server to deploy installation of Windows 2000 Professional. Client computers meet requirements for RIS deployment. You cannot connect the RIS client computers to the RIS server. Existing clients are able to connect to all the servers for network resources. What is the problem? (Choose all that apply)



A: The RIS server is not authorized in Active Directory.
The RIS server is not configured to respond to client computers.

59. You are deploying an application named Accounting that will be used by all users in your domain. You have been given a Windows Installer package for the installation. During the initial deployment, only members of a security group named Accounting Pilot will use the application. In the second half of the deployment, all users in the domain will install and use the application. You want to accomplish the following Phase 1 goals:

- **Only members of the Accounting Pilot group will be able to install the application using a Start menu shortcut – no other users can.**
- **The application will not be automatically installed when users log on.**
- **After Phase 1, the application will be installed automatically the first time any user logs on.**

You take the following actions:

- **Create a GPO named Deploy Accounting and link the Deploy Accounting GPO to the domain.**
- **Configure the Deploy Accounting GPO to publish the Accounting application to users.**
- **For Phase 1, configure the Deploy Accounting GPO permissions. Remove the Apply Group Policy permission for the Authenticated Users group. Grant the Apply Group Policy permission for the Accounting Pilot group.**
- **For Phase 2, configure the Deploy Accounting GPO permissions. Grant the Apply Group Policy permission for the Authenticated Users group. Remove the Apply Group Policy permission for the Accounting Pilot group.**

Which results do these actions produce? (Choose all that apply)

A: During Phase 1, the Accounting application is not installed automatically when users log on.

During Phase 1, users who are not members of the Accounting Pilot group cannot install the Accounting application by using a Start menu shortcut.

60. Your finance staff use portable computers and Routing and Remote Access to connect to your network. They need local administrator rights to their computers so they can run a third-party application. What should you do to configure their computers to prevent users from modifying their existing network connections?

A: Create a GPO for the domain. Filter the GPO for the finance users. Configure the GPO to deny the finance users access to the properties of a LAN or Routing and Remote Access connection.

61. All users in your Finance OU use an application named Accounting. It is deployed by using a GPO named Account App on the Finance OU. The Accounting App GPO is configured to assign the Accounting application to users by using a Windows Installer package. The Accounting application will be replaced in the near future. You want to accomplish the following goals:

- **Users who have not yet installed the Accounting application will be prevented from installing the application.**
- **Users who already have the application will be able to continue to use it.**
- **If key application files are missing, they will be reinstalled automatically when the Accounting application starts.**
- **If a software patch is released, you will be able to assign the patch to only users who have already installed the application.**

You take the following actions:

- **Create a new software category named Ledger Apps.**
- **Configure the Accounting App GPO to add the Accounting application to the Ledger Apps software category.**
- **Configure the Accounting App GPO to remove the Accounting application, but select the option to allow uses t continue to use the software.**

Which results do these actions produce? (Choose all that apply)

A: Users who have not yet installed the software are prevented from installing it.
Users who have already installed the software can continue to use it.

62. Your Windows 2000 Server is not a domain controller. Members of the domain Users group have the right to log on locally at this server. When one of these members logs on locally, you want a script named Params.vbs to be executed. It defines environment variables in the current user profile that are need for the Windows 2000 Server. What should you do?

A: Add the Params.vbs script to the local Group object as a logon script.

63. You are deploying a custom application named Painting. You need to set a custom policy setting in the HKCU\Software\Policies location in the registry for every user in the domain to configure the Painting application. What should you do?

A: Create a GPO named Paint Setting.
Assign the Paint Setting GPO to the domain.
Create a new administrative template that defines the custom policy setting.
Add the new administrative template to the Paint Setting GPO.
Configure the Paint Setting GPO to set the appropriate policy.

64. Your network consists of a Windows 2000 domain with three OUs. The Support OU has a Windows 2000 Server running RIS, and client computers. The Sales OU has 250 client computers, and the Research OU has 200 client computers. You are deploying Windows 2000 Professional on the computers in the Support and Sales OUs. You create a group named RIS Install which contains users from the Support OU. Only these members will use RIS to deploy Windows 2000. You want to accomplish the following goals:

- **Computers in the Research OU will not be able to download images during RIS deployment.**
- **New computer accounts will be organized into their appropriate OUs.**
- **The RIS Install group should be able to choose client computer names during installation.**
- **The existing company naming convention will be applied to new computers.**

You take the following actions:

- **Place Research computers in a different IP subnet from Support and Sales.**
- **Create an OU. In the RIS properties sheet, specify the client account location.**
- **In the RIS properties sheet, specify a custom Client computer naming format.**

Which results do these actions produce? (Choose all that apply)

A: The RIS Install group is able to choose client computer names during installation.
The existing company naming convention is applied to new computers.

65. Your network consists of two Windows 2000 domains named troytec.com and support.troytec.com. On your DNS server, you create separate zones for each domain. You then add a second DNS server which also functions as a domain controller. After you convert the troytec.com zone to an Active Directory integrated zone, and set the zone to allow only secure updates, you discover that unauthorized computers are registering themselves in the support.troytec.com domain. The zone's properties sheet

shows that the zone is allowing dynamic updates, and the option to select secure dynamic updates is not available. What should you do?

A: Convert support.troytec.com to an Active Directory integrated zone.

66. You are configuring DNS throughout your Windows 2000 domain which spans multiple subnets. You want to accomplish the following goals:

- **Zone transfer information will be secure.**
- **Administrative overhead for DNS zone files is minimized.**
- **DNS zone transfer traffic is minimized.**
- **Unauthorized host computers will not have records created in the zone.**
- **Zone updates will come only from authorized DNS servers.**

You take the following actions:

- **Create an Active Directory integrated zone.**
- **Set Allow Dynamic Updates to Only Secure Updates.**
- **Enter the names and addresses of all DNS server on the network in the Name Servers tab of the Zone Properties dialog box.**
- **Select Allow zone transfers only to servers listed on the Name Servers tab on the Zone Transfers tab of the Zone Properties dialog box.**

Which results do these actions produce? (Choose all that apply)

A: DNS zone transfer traffic is minimized.
Zone updates come only from authorized DNS servers.
Administrative overhead for DNS zone files is minimized.
Unauthorized host computers do not have records created in the zone.

67. You are configuring your Windows 2000 DNS server which resides on one Windows NT domain. DNS on a Windows NT Server already exists. You are going to use dynamic updates on the DNS database. Current policy prohibits you from upgrading or decommissioning the Windows NT DNS server. All DNS information must be synchronized between your two DNS servers. What should you do? (Choose three)

A: Create a standard primary zone on the Windows 2000 DNS server and import the existing zone file.
Delete the existing zone and create a new secondary zone on the Windows NT DNS server.
Configure the secondary zone on the Windows NT DNS server to use the Windows 2000 standard primary zone as its master zone.

68. You are the network administrator for a company that is planning a merger with another company. Your network segment consists of a DNS server, a domain controller, a WINS server, and a RAS server. The network segment of the company you will be merging with consists of a domain controller which serves as a DNS server

with Active Directory integrated zone, a domain controller, a WINS server, and a DHCP server. The two segments will be connected by routers. You want to host the merged domain on your DNS server. What should you do to host the merged company while retaining its domain structure after the merger is complete?

A: On the merged company's DNS server, configure DNS zone transfers to allow your DNS server to replicate data. On your DNS server, create a secondary zone with the domain name of the merged company.

69. Your Active Directory database is taking up too much space on your domain controller. What should you do to reduce the size of the Active Directory database file? (Choose three)

A: Restart the server in directory services restore mode.
Use the Ntdsutil utility to compact the database folder. Move the compacted file to the original location.
Restart the server and boot normally.

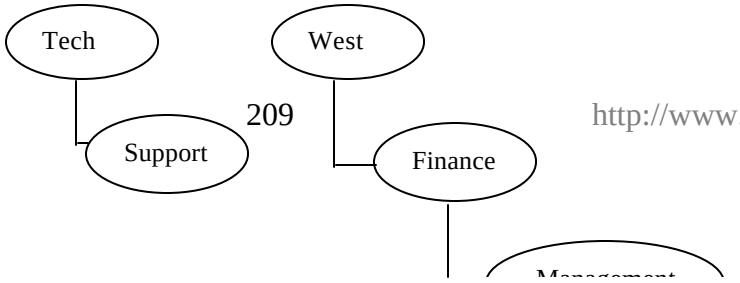
70. Your network has one domain, with three locations all connected by T1 lines. Each site contains a global catalog server. All site links have the same cost. You want users located in the West site to query the Central site if the West site global catalog server is offline. What should you do?

A: Configure the site link between the Central site and the West site to have a lower cost than the site link between the West site and the East site.

71. Your network consists of four domains named troytec.com, north.troytec.com, south.troytec.com, and salem.com. The root of the forest is troytec.com. Each domain has two Windows NT 4.0 BDCs. Technical Writers place documents for Salem, LLC in a shared folder on a domain controller named docs.salem.com. Read and Write permissions are granted to the Writers Domain Local group in the salem.com domain. Lane is a member of the Tech Writers global distribution group in the north.troytec.com domain. He is unable to gain access to the shared folder. What should you do?

A: Change the Tech Writers group type to Security and add it to the Writers Domain Local group.

72. A user in your network is moving from the Tech department to the Management department. You move his account from the Tech OU to the Management OU. You want him to be able to create user accounts in ou=finance,ou=west,dc=troytec,dc=com. What should you do?



A: Grant the user's account Create User Objects permission for the Finance OU.

73. The distinguished name for your Tech OU is ou=tech,ou=south,dc=troytec,dc=com. You want to assign a user the ability to manage all the objects in the Tech OU only. What should you do?

A: Grant the user Full Control permission to the Tech OU.

74. Your Windows 2000 network runs in native mode. It has two domains named troytec.com and support.troytec.com. Adam has a user account in the troytec.com domain, and needs to support files in the support.troytec.com domain. To accomplish this goal, you create a global group named Support in support.troytec.com. Support is a member of the Domain Local group named IS. IS has Read permission to the IS shared folder in the support.troytec.com domain. What should you do to grant Adam Read permission to the IS shared folder?

A: Create a new global group named Global IS in troytec.com. Add Adam to the new global group. Add the Global IS group to the IS group.

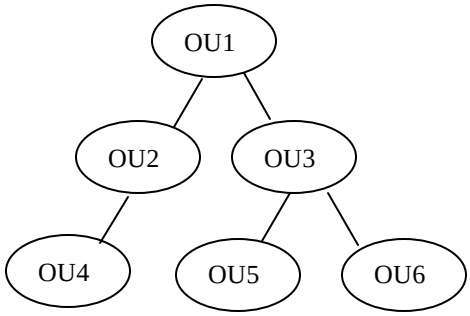
75. Your company has six locations. Three of these locations are in Europe, and three in South America. The European sites are in the eur.troytec.com domain. The South American sites are in the sa.troytec.com domain. The connection between one of the South American and one of the European sites is unreliable. You want to configure replication between these two sites. What should you do?

A: Create an SMTP site link between the two sites.

76. Your network consists of five sites in one domain. Cleveland, Louisville, and Newark will have DNS running on their domain controllers. Memphis and Salem will have DNS running on dedicated member servers. You want to allow client computers in Cleveland, Louisville, and Newark to perform secure dynamic updates to the DNS servers. The DNS servers should be configured so that each site has a replicated copy of the DNS database. What zone type should be designated for each site?

A: Drag Active Directory integrated to Louisville, Cleveland and Newark, and Secondary to Memphis and Salem.

77. You are designing a domain-wide security policy. Your OUs are organized as shown:



All domain controllers are in OU1. Resources for two buildings are in OU2 and OU3. Non-administrative users are in OUs 4 and 5. Administrative users are in OU6. You want to accomplish the following goals:

- **The number of GPO links will be minimized.**
- **All users will have the same password and account lockout policies.**
- **Only domain controllers and servers will have strict audit policies.**
- **Administrative and non-administrative computers will have different security settings.**

You take the following actions:

- **Create a single GPO.**
- **Create one security template that has all the required settings.**
- **Import the security template into the GPO.**
- **Link the GPO to the domain.**

Which results do these actions produce? (Choose all that apply)

A: All users have the same password and account lockout policies.
The number of GPO links is minimized.

78. You need to immediately implement a new security policy which renames the Administrator account on all computers in your network. You do not want to manually edit each account. What should you do? (Choose all that apply)

A: Use a Group Policy to implement a user logon script.
Use Group Policy to force all users to log off within 30 minutes.

79. You move a printer from your Sales OU to your Research OU. After you move the printer, the administrator of the Sales OU can still remove print jobs from it, although he is the administrator of resources only in the Sales OU. What should you do?

A: Remove the permission for the administrator from the printer.

80. Most of the resources your Sales team utilizes are in the west.troytec.com domain. You have a subsidiary of your company in South America with the domain salem.com. Members of the Sales team report that it is taking excessive time to access resources in the sa.salem.com domain. Network utilization is at 5 percent. What should you do to improve network performance?

A: Create an explicit trust between west.troytec.com and sa.salem.com.

81. Your na.troytec.com and eur.troytec.com domains are in mixed mode. Your troytec.com and salem.com domains are in native mode. Na.troytec.com has two Windows NT 4.0 BDCs that support legacy applications. Na.troytec.com users report when they try to access resources in a shared folder in the troytec.com domain, they are denied access. A universal group that has Read permissions to the Research folder exists. Research is assigned Read permission for the shared folder. When you log on as a member of the Research group from the troytec.com domain, you are able to access the shared folder. What should you do?

A: Create a global group in the na.troytec.com domain.
Add the user accounts from the na.troytec.com domain to the global group.
Grant Read permission to the global group for the shared folder.

82. Your company is installing a new network in Durango using 10.1.3.0/24. What should you do to prepare the network in advance so when your staff installs a new domain controller, it will automatically join the appropriate site?

A: Create a new subnet for the Durango network. Create a new site and associate the new subnet with the new site.

83. Your Domain Local group named WI has Change permissions for the Workorders In folder. The Workorders In folder is a subfolder of the Workorders folder. The Workorders In global group is a member of the WI Domain Local group. Amanda's user account is a member of the Workorders In global Group. Amanda moves to a different department. She needs to access only resources in that department. You remove Amanda's user account from Workorders In global group, but she is still able to access the Workorders In folder. What are two possible causes of this problem? (Choose two)

A: Amanda's user account has explicit permissions on the Workorders folder.

Amanda's user account belongs to another group that gives her permissions on the Workorders In folder.

84. While you run DCPromo.exe on a failing domain controller on your domain to remove Active Directory, the hard disk drive fails. The server will not reboot. Objects for the failed server are still appearing in Active Directory. What option should you use in Ntdsutil to remove the old server from Active Directory?

A: metadata cleanup.

85. You are deploying an application named Vacation that will be used by all users in your domain. The vendor of the application did not provide a Windows Installer package. You want to use Group Policy to deploy the application with the following goals:

- **If key application files are missing, the application will be automatically reinstalled.**
- **Users can install the application by using a Start menu shortcut.**
- **Users can install the application by using Add/Remove Programs.**
- **Users can install the application by using document invocation.**

You take the following actions:

- **Create a zero administration package text file.**
- **Copy the .zap file to a shared folder on the network.**
- **Create a new GPO named Install Vacation and assign the Install Vacation GPO to the domain.**
- **Configure the Install Vacation GPO to publish the Vacation application to users by using the .ZAP file.**

Which results do these actions produce? (Choose all that apply)

A: Users can install the application by using Add/Remove Programs.
Users can install the application by using document invocation.

86. You are using RIS to deploy Windows 2000 Professional on your network. You want to allow members of the Managers group access to create custom images and post them to the RIS server for deployment, and allow them to install client computers from the RIS server. What should you do?

A: Grant the Managers group Read and Write permissions to the RemoteInstall folder.

87. Your Windows 2000 domain has an OU named Management. Your Windows 2000 Server is named Boston. All of your Windows 2000 Professional computers are on the same domain, and each is shared by many users. You want to accomplish the following goals:

- **Management OU users can use any Windows 2000 Professional computer and receive their own user profile settings.**
- **Users can access their documents in the My Documents folder from any computer.**
- **Documents will not be automatically copied to or from the server and the user's My Documents folder when users log on or log off.**

What should you do? (Choose all that apply)

A: Configure a roaming profile for each user in the Management OU. For the profile path, use \\Boston\Profiles\%Username%.
Create a new GPO named Redirect. Assign the Redirect GPO to the Management OU. Configure the Redirect GPO to redirect the My Documents folder to \\Boston\Docs\%Username%.

88. Your domain is in native mode, and contains an OU named Support. You want to delegate the control of Group Policy settings for the Support OU to a global group named Tech Support. Members of the Tech Support group should be able to create and edit new GPOs and assign these GPOs to only the Support OU. What should you do? (Choose two)

A: On existing GPOs, assign Read and Write permissions to the Tech Support group.
On the Support OU, delegate the predefined task named Manage Group Policy links to the Tech Support group.

89. You are configuring RIS to deploy Windows 2000 Professional on your new client computers. But when new users attempt to install their computers, they report that they cannot receive an IP address. What should you do?

A: Authorize the DHCP server.

90. You have numerous departments in your company. Each department needs to use specific features of Windows 2000 and custom third-party applications. You want to provide customized software installations to your users, while minimizing the administrative time required to set up the client computers. What should you do?

A: Install and configure a RIS server.
User RIPrep.exe to create multiple images for each department.
Connect the client computers to the RIS server, and deploy the custom images.

91. Your Windows 2000 domain has a Windows 2000 Server named West. Users use different Windows 2000 Professional desktop and portable computers. You want to accomplish the following goals:

- **All users can use any Windows 2000 Professional computer or portable computer when they are traveling, and have their own desktop settings.**
- **Users can access their documents in the My Documents folder from any computer, including when users dial in to the network.**
- **When users dial in to the network, the logon, and logoff times will not be delayed because of the transfer of the contents of the My Documents folder.**

What should you do? (Choose two)

A: Configure a roaming profile for each user in the domain. For the profile path, use \\West\Profiles\%Username%.
Create a new GPO named Redocs. Assign the Redocs GPO to the domain. Configure the Redocs GPO to redirect the My Documents folder to the \\West\Docs\%Username% location.

92. Your company wants to minimize the number of GPOs that are processed at logon. The Support OU has a GPO named Disable Regedit that disables the use of registry editing tools. They have decided that the restriction on the use of the registry editing tools should no longer apply to the users in the Support OU. What should you do?

A: Remove the Disable Regedit GPO from the Support OU.

93. You have two Windows 2000 Servers and only enough Windows 2000 Professional licenses for 250 of your users. What should you do to minimize user intervention, centralize the installation files, and restrict the deployment so that Windows 2000 Professional can be installed only on the licensed computers?

A: Install RIS on one of the servers.
Create computer accounts for only the licensed computers.
Configure the RIS server to accept connections from only known computers.
Perform unattended installations for all connection computers.

94. What tools should you use to find the GUIDs on client computers to complete deployment of Windows 2000 Professional using RIS?

A: Use Network Monitor to capture the DHCPDiscover frames from the client computers. Search the data fields for the GUIDs in hexadecimal format.

95. You are designing the structure of your DNS servers in your Windows 2000 network which consists of five sites in your troytec.com domain. You have 15,000 users in Cleveland, 5,000 in Lacrosse, 2,000 in Memphis, 10,000 in Newark, and 2,000 users in Salem. You must allow secure dynamic updates to DNS in Cleveland, Lacrosse, and Newark. You want full DNS replication to occur in all the sites. You do not want

Memphis to have an editable copy of the DNS zone. What zone types and server types should be assigned to each of the sites?

A: Cleveland: Domain controller, Active Directory integrated; Lacrosse: Domain controller, Active Directory integrated; Memphis: Member server, Cache only; Newark: Domain controller, Active Directory integrated; Salem: Member server; Secondary.

96. What two things must you do to set up replication so that two domain controllers in separate sites replicate every half-hour between the hours of 5 a.m. and 4 p.m.

A: Configure the replication period with a setting of once every 30 minutes.
Configure the replication schedule to allow replication between 5 a.m. and 4 p.m.

97. What is the name given to a single server that is designated in each site to perform site-to-site replication?

A: Bridgehead Server.

98. What is true about Operations Masters' placement in a Windows 2000 network? (Choose all that apply)

A: The Schema Master should always be the same machine as the Domain Naming Master.
The Infrastructure Master should never be placed on a Global Catalog Server.

99. In what order do you restore an erroneously deleted organizational unit?

A: Restart the machine. Enter directory services restore mode for the domain controller. Restore the System State data from a recent tape backup. Using Ntdsutil.exe, perform an authoritative restore.

100. What tasks can Windows Installer perform? (Choose all that apply)

A: Monitoring of file resiliency.
Modifying an existing application.
Removing an existing application.

101. You use Active Directory Users and Computers to create a distribution group with Domain Local scope. When you attempt to assign permissions to the group you are unsuccessful. Why?

A: Distribution groups are not security principals and cannot be used to assign permissions.

102. You are in charge of administering all users within the Sales OU of a domain in a multinational company. You have been delegated Full Control permission for the Sales

OU. You are configuring Group Policies to deploy Office 2000 to the desktops in the OU, and would like the applications to be available to all users who access computers in the Sales OU regardless of whether their user accounts reside in the Sales OU. What should you do?

A: Create a policy for the Sales OU. Edit the policy and assign a new package under the Computer Configuration, Software Settings, Software Installation node.

103. Which of the following require the NTFS file system? (Choose all that apply)

A: A partition that you will be enforcing Windows 2000 disk quotas on.
A partition containing the SYSVOL folder structure.
A partition where you will install Remote Installation Services (RIS).

104. When should you establish non-transitive trust relationships? (Choose all that apply)

A: Between a Windows 2000 domain and a Windows NT domain.
Between a Windows 2000 domain and a Kerberos V5 protocol security realm.
Between a Windows 2000 domain in one forest and a Windows 2000 domain in another forest.

105. What is the best way to have a Group Policy apply only to a single user within an organizational unit?

A: Set a Group Policy at the Organizational Unit level. Configure the Discretionary Access Control List for the Group Policy so that only that user account has the Apply Group Policy permission allowed.

106. What are potential benefits of using SMTP replication versus RPC-based replication? (Choose all that apply)

A: Where end-to-end online IP connectivity is impossible mail can be used and routed appropriately.

107. You configure a password policy for your domain so that all users must have a minimum password length of 6 characters. Within the domain, there is an organizational unit (OU) named Support. Due to the sensitive nature of security within the Support OU, you want to set a more secure password restriction on users within Support. You set a password policy at the organizational unit level so that all accounts within Support must have a password of 10 characters or greater. When testing the policy, you discover that you can still use a password of less than 10 characters. What is the most likely the cause?

A: Group Policies for certain account settings such as password length can only be applied at the domain level. A policy applied at an OU level would affect local logons to computers located in the OU, but it would not affect domain logons.

108. If a user attempts to log on and the domain controller that is servicing the authentication request does not recognize the user's password, the authentication request is then passed on to the machine receiving preferred replication of password changes. What is the machine performing this role on the domain called?

A: PDC emulator.

109. You want to delegate administrative tasks to several users. You create two organizational units within your root domain called Main and Branch. You grant a user named Randy to have full administrative power over the Main OU and grant a user named Grace full administrative power over the Branch OU. You do not want them to configure settings which would override the security settings that you has configured at the domain level. What should you do?

A: Configure a group policy at the domain level with the security settings and give it the setting of "No Override".

110. You configure several Group Policies to be applied to users in your company whose desktops you want to restrict. You want the Group Policies to be applied immediately to all the users that they affect. What should you do?

A: Run the secedit command to refresh the policy.

111. After installing Active Directory, Mark sets up a Group Policy to place restrictions on some of the users in his company. Mark's company currently has a single domain with four organizational units (OUs) named Sales, Finance, Marketing and Research. There are ten scientists in the company that Mark would like to place restrictions on. The user accounts for these scientists are distributed among all four of the company's OUs. All of the scientists are members of a global group called Scientists which is located in the Research OU. Mark would like a policy to apply to members of the Scientists group but not to apply to anyone else in the company. He creates a policy for the Research OU and changes the permissions so that the Scientists group has the Read and Apply Group Policy permissions. He removes the default permissions for the Authenticated Users group. However, when testing the policy, Mark does not get the results he had expected. What is the most likely reason for this and how should Mark correct the problem?

A: All of the user accounts are not located in the Research OU. A user account will only have policies applied to it based on the location of its user object. Configure the policy to be applied at the domain level rather than at the organizational unit level.

112. You want to upgrade an NT 4.0 domain on your network to Windows 2000 and minimize the amount of time that a Primary Domain Controller is unavailable. You need the ability to roll back to your current environment. What should you do?

A: . Save a pre-Windows 2000 backup domain controller (BDC). Upgrade the Windows NT primary domain controller. Install Active Directory on the Windows NT PDC, and upgrade any remaining backup domain controllers.

113. There are several schema objects created on your Windows 2000 schema upon schema installation. You want to deactivate these objects you are trying to minimize schema replication traffic. When you try to deactivate them you are unsuccessful. What is the most likely reason for this?

A: You cannot deactivate objects that were created when the schema was installed.

114. Grace is trying to change the description of the mailboxes for seven user objects in Active Directory from her workstation. Every time she tries to enter the new description for each user, it fails. She has permission to modify the Active Directory schema. What is the most likely problem?

A: Her workstation does not have the Active Directory connector management components installed.

115. Troy's Windows 2000 network has only one class for user objects called "corporate users". He wants to subdivide the users into different departments such as sales, marketing, and support. Troy creates the child classes to "corporate users" and sets the attributes. How should he move the user objects to their new classes?

A: Delete the user objects and recreate them as new instances of the new classes.

116. Drew wants to create two new classes in separate trees that will be used to identify salesmen. The trees are in different sites and are not directly connected. The name for both classes is "IT" and they have different LDAP names and object identifiers. After creating the first class and adding it to the schema, Drew tries to create the second class and fails. What is the most likely reason why?

A: Two classes cannot share a common name.

117. Your single-domain organization currently has two organizational units (OUs) for the Sales and Support. Each division has multiple departments. You have developed a Group Policy for every job category within the organization. How can you structure your OU hierarchy for Active Directory to support delegation and group policy needs?

A: Within each division, create an OU for each job category. Create a GPO for each category-based OU.

118. You are creating an unattended answer file with Setup Manager. You type the name of your downlevel domain, troytec, in the Workgroup option box rather than selecting the domain name option. You will use this answer file to install Windows 2000 Server on ten computers. How will this impact your rollout when these servers join the upgraded domain, troytec.com?

A: The computers of this unattended installation can join the domain from their current workgroup status with the identical name.

119. You need to reinstall Windows 2000 Server on a domain controller because the operating system is corrupt. How can you get the Active Directory to automatically copy domain information to the new installation?

A: Remove all existing references to the old domain controller using Sites And Services snap-in. Reinstall Windows 2000 server, reinstall Active Directory with the wizard to promote the server to a domain controller.

Index