Managing a

Microsoft Windows 2000 Network Environment

Version 3.0.1

Managing a

Microsoft Windows 2000 Network Environment

Version 3.0.1

Abstract:

This study guide will help you to prepare for Microsoft exam 70-218, Managing a Windows 2000 Network Environment. Topics include: publishing resources in Active Directory, managing data storage, creating shared resources, configuring & troubleshooting IIS, monitoring & managing network security, troubleshooting routing, configuring & troubleshooting TCP/IP, configuring & administering DHCP, configuring & administering DNS, installing & configuring hardware, troubleshooting start-up problems,

Find even more help here:

Contents:

Creating, Configuring, Managing, Securing, and Troubleshooting File, Print, and Web Resources

Publish resources in Active Directory. Types of resources include printers and shared folders.

Publish printers in Active Directory (KB# Q234619, Q245584, Q278504, Q234270)

By default, all printers that are installed on Windows 2000 systems that participate in an Active Directory domain are published in the Active Directory catalog so long as they are shared. (As with all default actions, this one too can be disabled if you chose to.) You can search for printers in the Active Directory as shown in Figure 1. More information on this is found in the Server Documentation.

- You can also manually publish printers in the Active Directory; this would be used when the printer is attached to a non-Windows 2000 machine. Open **Active Directory Users and Computers**, select the location (OU, etc.) where you want to locate the new printer at, right click on that object, select **New** and then select **Printer**. Enter the UNC address where the printer is located at and click **OK** to complete the process as shown in Figure 2. More information on this can be found in the Server Documentation.
- You must be logged in with directory service administration rights in order to publish printers in the Active Directory.

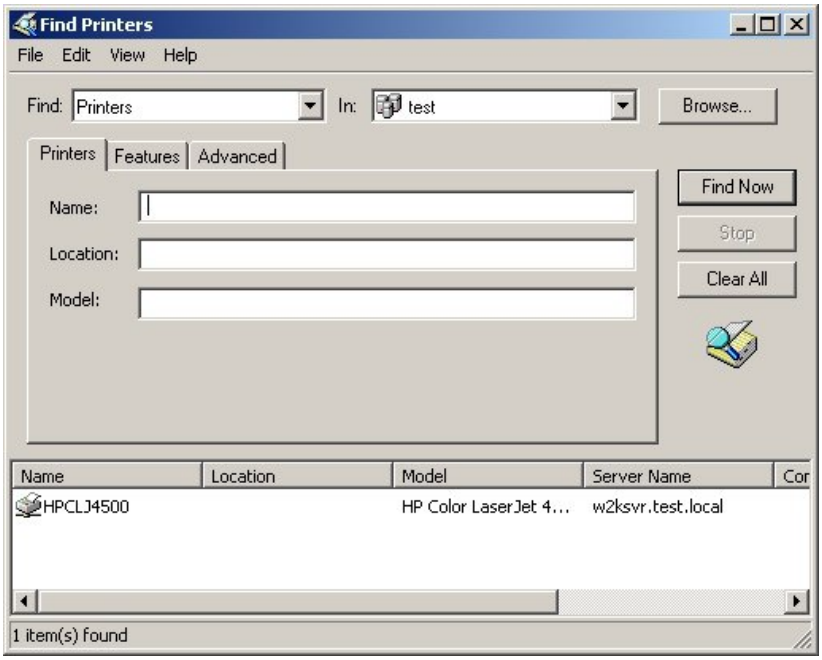

Figure 1 – Searching for printers in Active Directory.

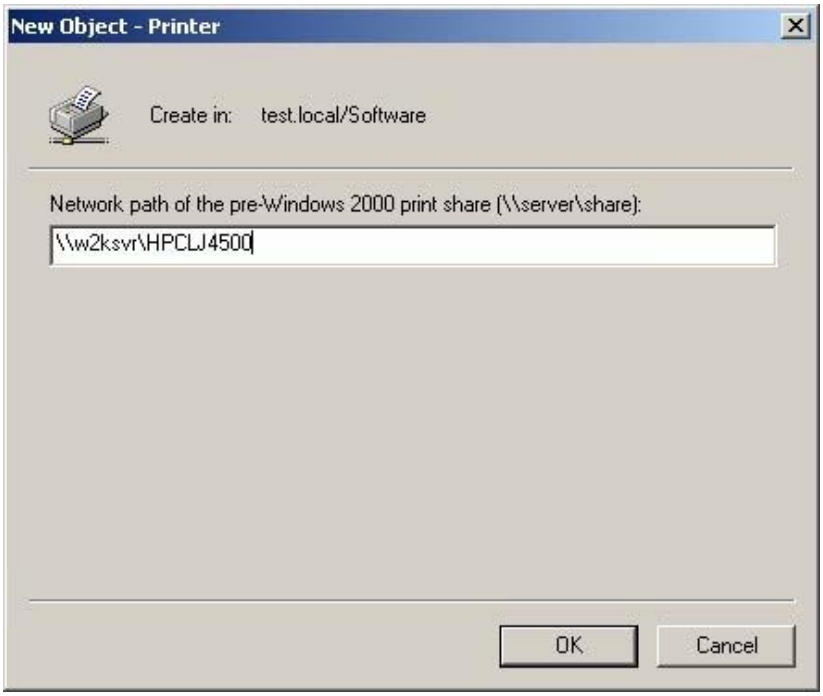

Figure 2 – Publishing printers on pre-Windows 2000 shares in Active Directory.

Publish shared folders in Active Directory (KB# Q234582)

- Open **Active Directory Users and Computers**, select the location (OU, etc.) where you want to locate the new share at, right click on that object, select **New** and then select **Shared Folder**. Enter a descriptive name and the UNC address where the folder to be shared is located at and click **OK** to complete the process as shown in Figure 3. Additional information can be found in the Server Documentation.

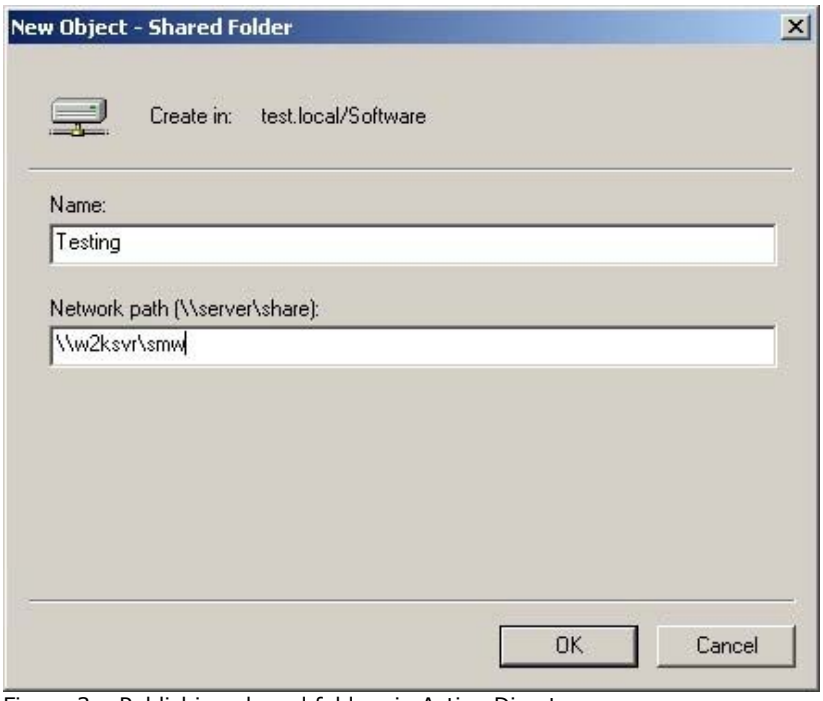

Figure 3 – Publishing shared folders in Active Directory.

Manage data storage. Considerations include file systems, permissions, and quotas.

File systems

- NTFS 5.0 provides the following features that are not available in the FAT32 or FAT file systems (KB# Q183090, MSDN SDK):
  - **Disk quotas:** Disk quotas allow administrators to control the amount of data that each user can store on an NTFS volume. Administrators can

optionally configure the system to log an event when users are near their quota, and to deny further disk space to users who exceed their quota. Quotas can be set on both Basic and Dynamic disks (KB# Q183322, Q300979)

- **Encryption:** The Encrypting File System (EFS) provides cryptographic protection of files. EFS provides file encryption on an individual file or folder basis using a public-key system. File encryption and file compression are mutually exclusive. (KB# Q222054, Q230520, Q243035, Q243756, Q223093)
- **Reparse points:** Programs can trap open operations against objects in the file system and run their own code before returning file data. This feature can be used to extend file system features such as mount points, which you can use to redirect data read and written from a folder to another volume or physical disk. (KB# Q262797)
- **Sparse files:** A large file in which a lot of data is all zeros is a sparse data set, such as a matrix in which much of the data is zeros. The NTFS file system works to prevent wasting hard drive space on these zero values. The file system does not allocate hard drive to a file except in regions of the file that contain some data other than zeros. Sparse files will be allocated their entire file size when using disk quotas, as the file can grow (KB# Q231388).
- **NTFS file permissions:** This allows for the settings of permissions from a very granular level (individual files) to a broad, wide-sweeping level (entire directories) to allow / prevent access to files and folders.
- **Volume mount points:** Volume Mount Points allow new volumes to be added to the file system without needing to assign a drive letter to it. Instead of mounting a CD-ROM as drive E:, it can be mounted and accessed under an existing drive (e.g., C:\CD-ROM). (KB# Q205524, Q260566).
- **File compression:** File compression is supposed on an individual file or folder basis with the NTFS file system. The file compression algorithm used is a lossless compression algorithm, which means that no data is lost when compressing and decompressing the file, as opposed to lossy compression algorithms, where some data is lost each time data compression and decompression occur. File compression and file encryption are mutually exclusive (KB# Q281186, Q223093).

- FAT and FAT32 are only used for dual booting between Windows 2000 and another Operating Systems, such as MS-DOS, Windows 3.1 or Windows 95/98. The use of FAT and FAT32 under Windows 2000 is not recommend and has limitations (KB# Q184006).
- Existing Windows NT 4.0 NTFS system partitions will be upgraded to Windows 2000 NTFS automatically during the installation process. If you wish to dual-boot between NT 4.0 and Windows 2000 you must first install Service Pack 4 on the NT 4.0 machine. This will allow it to read the upgraded NTFS

partitions, but advanced features such as EFS and Disk Quotas will be disabled (KB# Q184299, Q183090).

- Use **convert.exe** to convert a FAT or FAT32 file system to NTFS after the installation of Windows 2000 has been completed. NTFS partitions cannot be converted to FAT or FAT32 - the partition must be deleted and recreated as FAT or FAT32 (KB# Q156560, Q214579).
- You cannot convert a FAT partition to FAT32 using **convert.exe**. (KB# Q197627).
- Files and folders moved from an NTFS volume to a FAT or FAT32 volume lose all attributes they possessed under NTFS that are NTFS dependant.
- FAT / FAT32 features:

Feature	FAT	FAT32
File allocation table size	16 bit	32 bit
Maximum volume size	4 GB (best is 2 GB or less)	2 TB (limited to 32GB in Windows 2000 – KB# Q184006)
Maximum file size	2 GB	4 GB
Operating Systems supported	MS-DOS, all versions of Windows	Windows 95 OSR2, Windows 98, Windows Me, Windows 2000, Windows XP
Supports small cluster size?	No	Yes
Supports NTFS 4.0 features?	No	No
Supports NTFS 5.0 features?	No	No
Use on floppy disks?	Yes	Yes
Use on removable disks?	Yes	Yes

- Additional NTFS 4.0 / NTFS 5.0 features:

Feature	NTFS 4.0	NTFS 5.0
Maximum volume size	32 GB	2 TB
Maximum file size	32 GB	Limited by volume size
Operating Systems supported	Windows NT 4.0, Windows 2000, Windows XP	Windows 2000, Windows XP, Windows NT 4.0 (minimal support)
Use on floppy disks?	No	No
Use on removable disks?	Yes	Yes

NTFS file and folder permissions: (KB# Q183090, Q244600, Q300691)

- There are two types of permissions: explicit and inherited.
  - Explicit permissions are those that are directly assigned to an object, either when the object is created or by user actions.
  - Inherited permissions are those that have been propagated to a child object from a parent object.
- If no access to an object is specifically Allowed or Denied, then user access to the object is denied.
- By default, all child objects of a folder inherit the permissions assigned to the parent folder. Permission inheritance makes it easier for Administrators to assign permissions, as it can now be done at a high level, such as a folder, and thus will apply by default to all objects (files and subfolders) contained within that folder. This behavior can be turned off and is required to be turned off to change the inherited permissions on an object. Figure 4 shows inherited (grayed out check boxes) file permissions on an object.

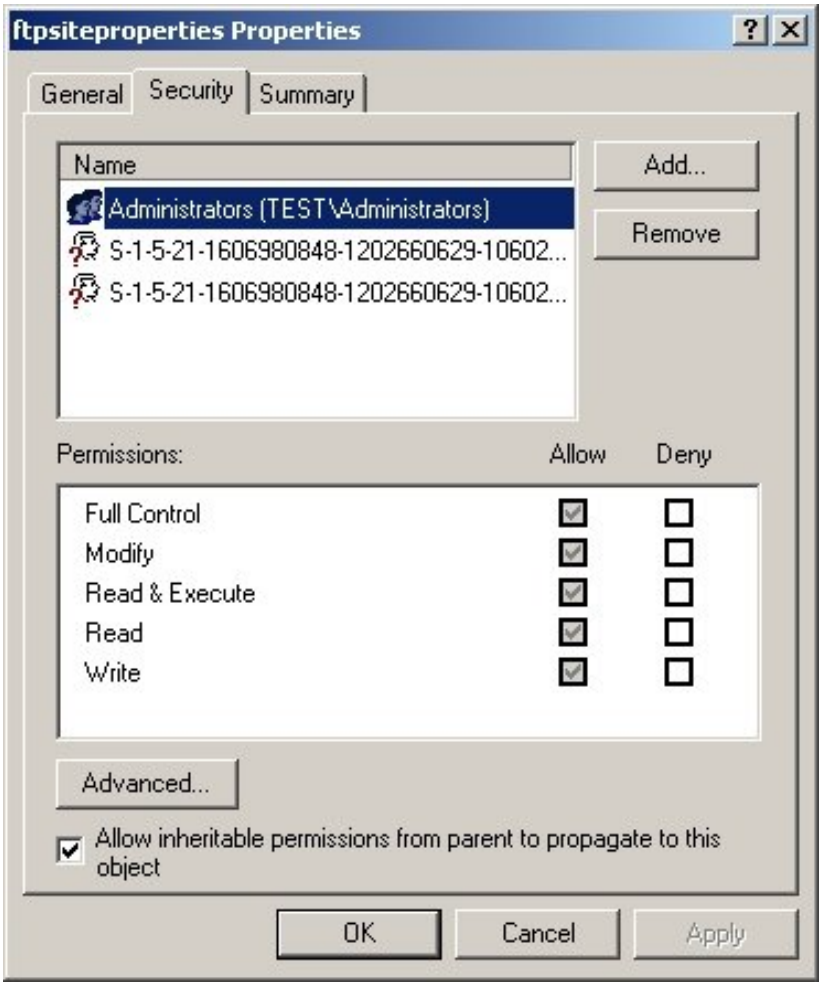

Figure 4 – Inherited file permissions (the SIDs listed numerically actually belong to another installation of Windows [XP in this case]—they would be treated as foreign security principals).

- Turn off file permission inheritance from the Advanced Security Settings window as shown in Figure 5 by unselecting the **Allow inheritable permissions from parent to propagate to this object** checkbox.

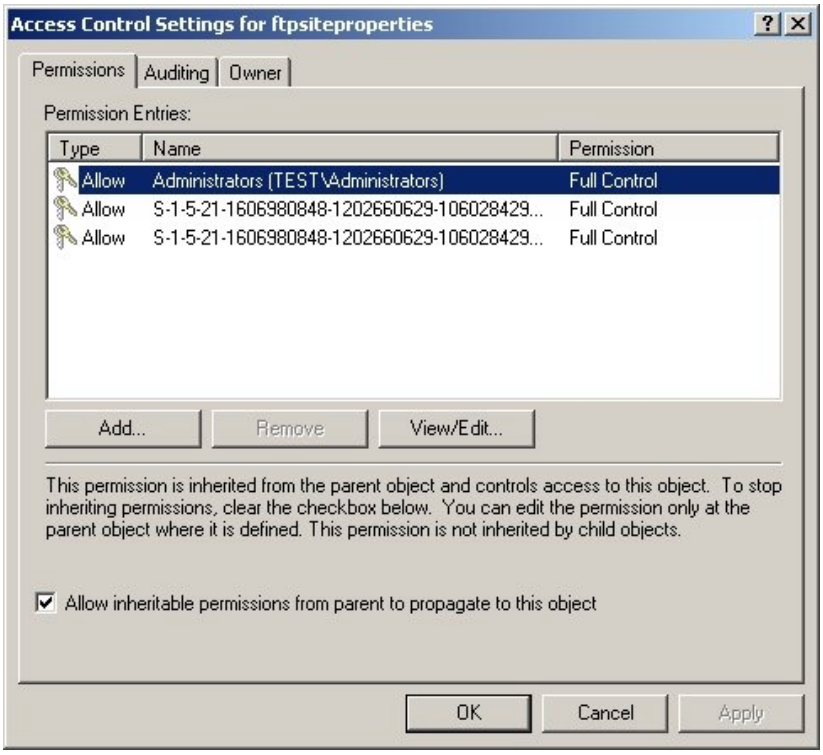

Figure 5 – The Advanced Security Settings window.

- Permissions explicitly assigned to a file or sub-folder over ride those implicit permissions possessed via inheritance.
- Permissions are cumulative, except for Deny, which overrides all other permissions. To determine users permissions on a specific object, add all Allow permissions from the volume root to the object in question and then subtract all permissions Denied from the volume root to the object. This is the cumulative object permission the user possesses.
- Folder permissions, which can be set to either Allow or Deny, include Full Control, Modify, Read & Execute, List Folder Contents, Read, and Write. Each of these permissions consists of a logical group of special permissions as outlined in the table below. Each of the special permissions can be set from the Advanced Security Settings window by selecting a user and then clicking **Add...**.
- File permissions, which can be set to either Allow or Deny, include Full Control, Modify, Read & Execute, Read, and Write. Each of these permissions consists of a logical group of special permissions as outlined in the table below (List Folder Contents does not apply to file permissions). Each of the special permissions can be set from the Advanced Security Settings window by selecting a user and then clicking **Add...**.

Special Permissions	Full Control	Modify	Read & Execute	Read	Write	List Folder Contents
Traverse Folder/Execute File	x	X	x			X
List Folder/Read Data	x	X	x	x		X
Read Attributes	x	X	x	x		X
Read Extended Attributes	x	X	x	x		X
Create Files/Write Data	x	X			x	
Create Folders/Append Data	x	X			x	
Write Attributes	x	X			x	
Write Extended Attributes	x	X			x	
Delete Subfolders and Files	x					
Delete	x	X				
Read Permissions	x	X	x	x	x	X
Change Permissions	x					
Take Ownership	x					
Synchronize	x	X	x	x	x	

Disk Quotas (KB# Q183322, Q300979)

- Administrators can use disk quotas to both control disk space usage and also to monitor disk space usage. You must be logged as a member of the Administrators group on the computer that houses the disk drive in order to implement Disk Quotas.
- Disk quotas can only be implemented on a per-volume basis; they cannot be implemented on a folder directly. Figure 6 shows the window for implementing Disk Quotas.

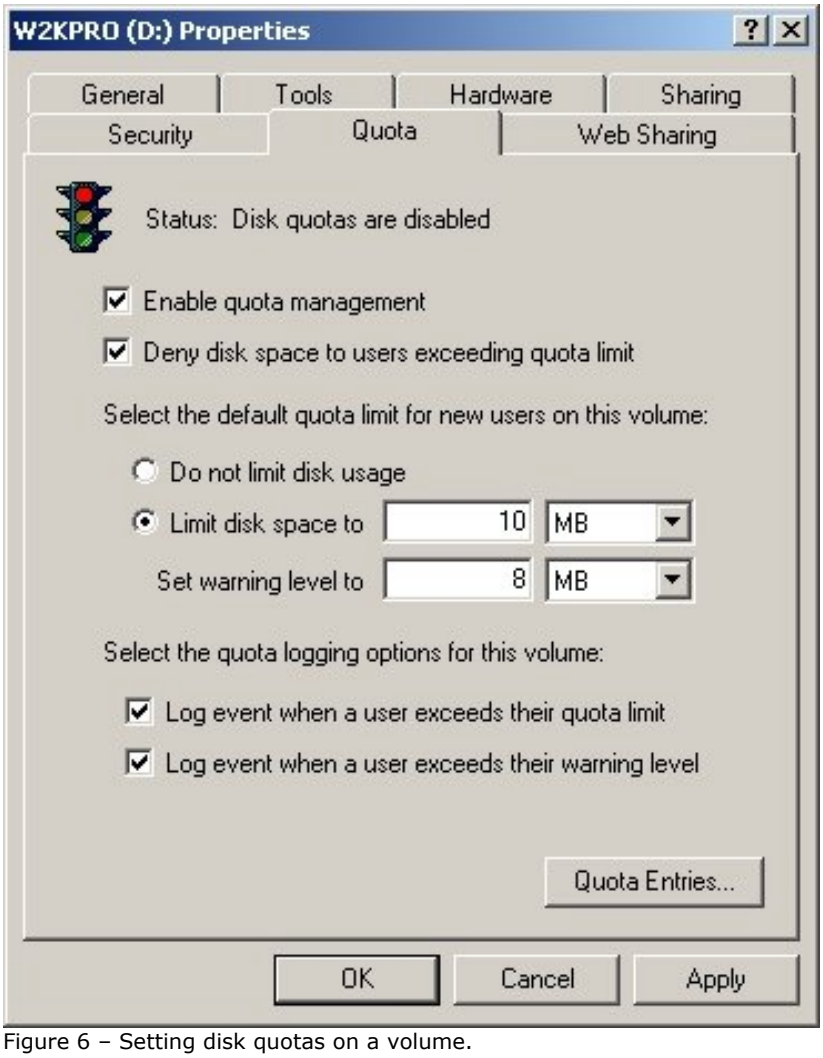

Figure 6 – Setting disk quotas on a volume.

- Disk quotas are based on uncompressed file sizes. If you had a 30 MB disk quota that contained 27 MB of data, implementing NTFS compression would not enable you to increase the amount of free space.
- Disk quotas can be applied to both basic and dynamic disks.
- Visual indication is provided to monitor disk space usage on volumes with Disk Quota in effect. The three standard indicators (red **above limit** circles, yellow **warning** triangles and white **OK** circles) are used to help draw attention to the usage of each user as show in Figure 7.

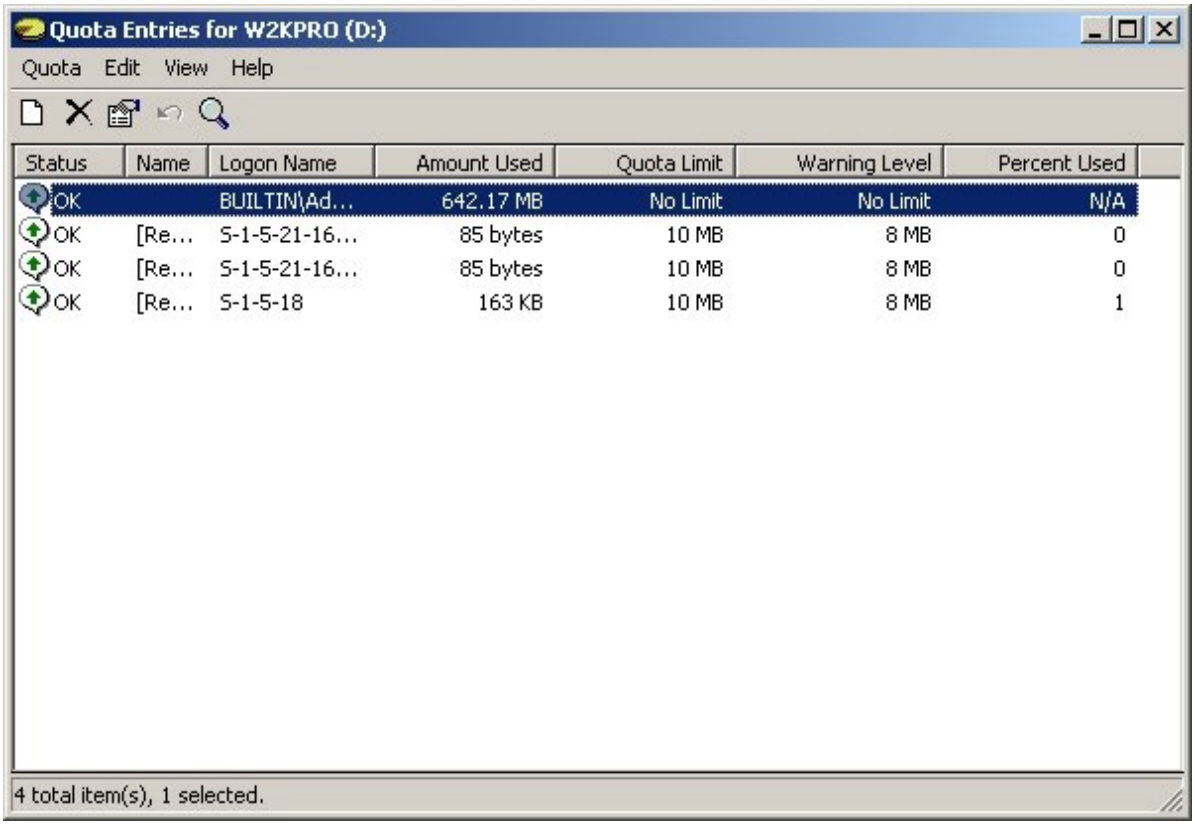

Figure 7 – Quota entries, notice the accounts over the quota limits and the one close to the limit.

- Disk quotas only apply to users created *after* the quota is enacted. Existing volume users will have no quotas applied to them by default. You can apply disk quotas to existing users by adding new quota entries for them in the Quota Settings window, as shown in Figure 8.

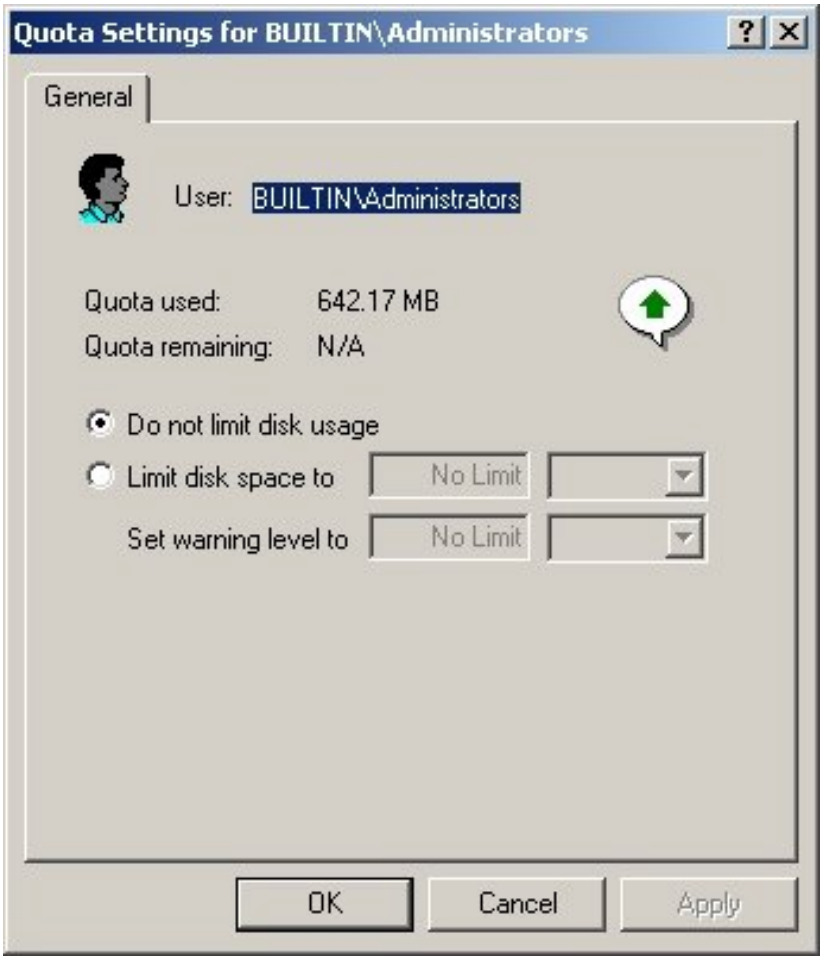

Figure 8 – Setting custom disk quotas for an individual user.

Create shared resources and configure access rights. Shared resources include printers, shared folders, and Web folders.

Configuring shared printers

- Sharing a printer will allow other users on the network to send print jobs to that printer. In large enterprises, shared printers should be hosted from a dedicated print server, but in many small setups the printer to be shared may be directly connected to a client workstation. KB# Q300392 describes how to set up a file or print server.

- Existing printers may be shared by selecting the printer from the **Printers** applet, right clicking on it and selecting **Sharing...** The printer properties window will open up (as shown in Figure 9) with the Sharing tab selected. From here you can choose to share or not share the printer, provide a descriptive name for it and enable any additional down-level drivers that other users on the network may require (such as Windows 98 or Windows NT 4.0 clients).

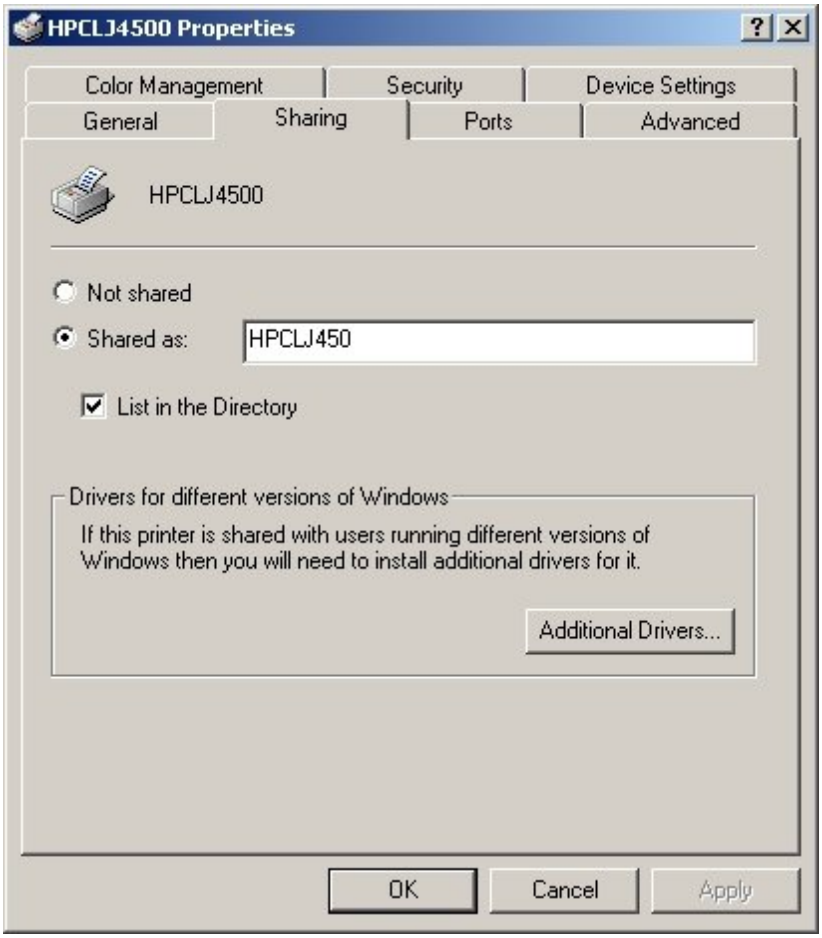

Figure 9 – Setting printer sharing properties.

- Some other points to remember about shared printers:
  - TCP/IP print services can only be provided for Windows and UNIX clients (KB# Q124734).

- Windows 2000 automatically downloads the printer drivers for clients running Windows XP, Win2000, WinNT 4, WinNT 3.51 and Windows 95/98 (KB# Q142667).
- Internet Printing (KB# Q248344) is a new feature that was introduced in Windows 2000. You have the option of entering the URL where your printer is located. The print server must be a Windows 2000 Server running Internet Information Server or a Windows 2000 Professional system running Personal Web Server (stripped down version of IIS). All shared printers can be viewed at: **http://servername/printers**.
- Print Pooling allows two or more identical printers to be installed as one logical printer.
- Print Priority is set by creating multiple logical printers for one physical printer and assigning different priorities to each. Priority ranges from 1, the lowest (default) to 99, the highest.
- Enabling "Availability" option allows the Administrator to specify the hours the printer is available.
- Use Separator Pages to separate print jobs at a shared printer. A template for the separator page can be created and saved in the %systemroot%\system32 directory with a .SEP file extension (KB# Q102712).
- You can select Restart in the printer's menu to reprint a document. This is useful when a document is printing and the printer jams. Resume can be selected to start printing where you left off.
- You can change the directory containing the print spooler in the advanced server properties for the printer (KB# Q123747).
- To remedy a stalled spooler, you will need to stop and restart the spooler services in the Services applet in Administrative Tools in the Control Panel (KB# Q240683).
- Use the **fixprnsv.exe** command-line utility to resolve printer incompatibility issues (KB# Q247196).

Configuring shared folders (KB# Q301198, Q301195, Q300856)

- To configure shared folders on a Windows 2000 Server, you will need to be a member of the **Administrators** or **Server Operators** group.
- To configure shared folders on a Windows 2000 Professional workstation, you will need to be a member of the **Administrators** or **Power Users** group.
- Shared folders can be created in three distinct ways:
  - Locally at the computer, you can share a folder by selecting it in Windows Explorer, right clicking it and then selecting **Properties**. Select the Share this folder option and configure options as desired and then click **OK** to complete the process. By default, the **Everyone** group has full control over shares created this way.

- Locally at the computer, you can share a folder by using Computer Management. Open the Shared Folders node (found inside the System Tools node) and then select **Shares**. Right click on **Shares** and select **New File Share...** This will bring up a window like the one shown in Figure 10. Provide the required information and then click **Next**. Set the share permissions as you desire and click **Finish**. You can control all shares from this MMC snap-in as shown in Figure 11.
- From any computer connected to the network you can share folders on other network computers by connecting to another computer. In the Computer Management console, click **Action** and then click **Connect to another computer...** The actions to perform will be the same after you are connected.

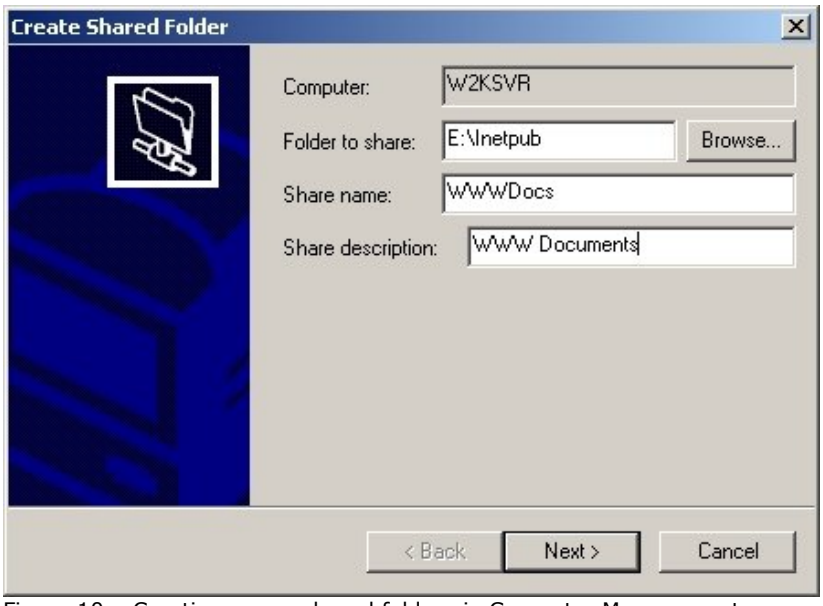

Figure 10 – Creating a new shared folder via Computer Management.

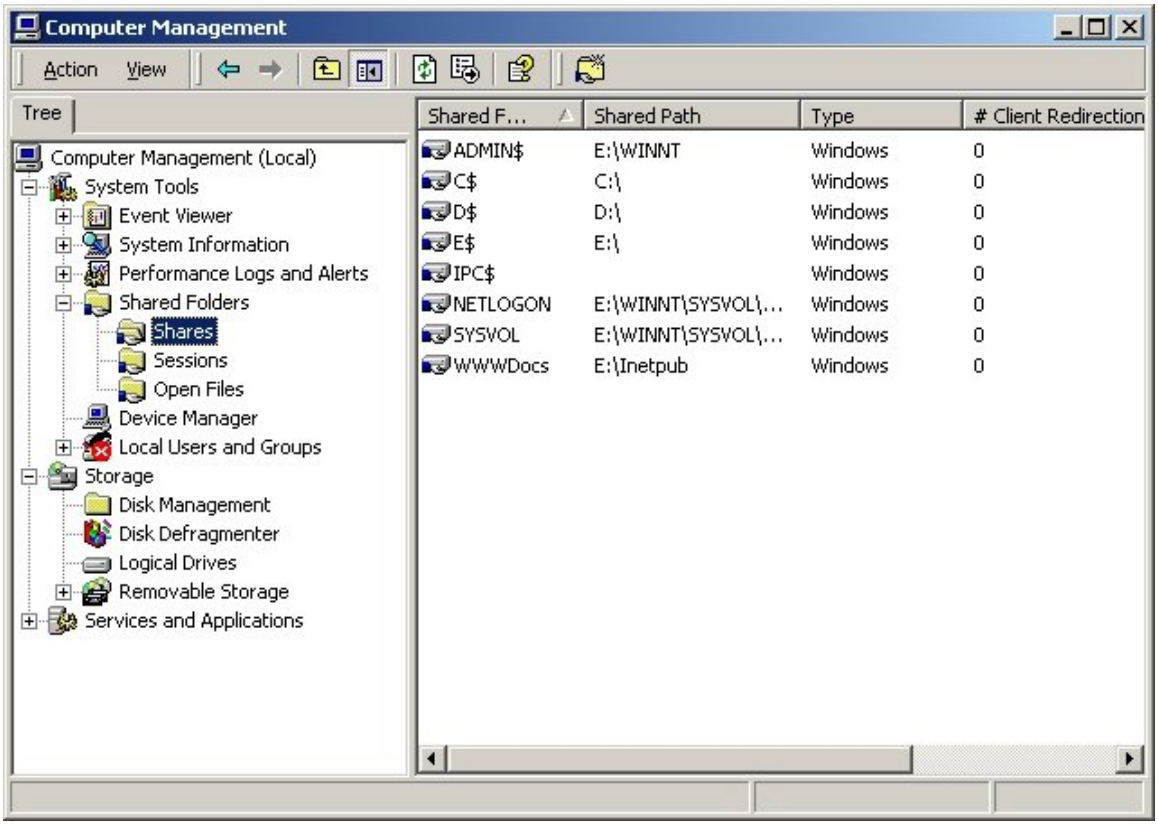

Figure 11 – Shared folders in Computer Management MMC console.

- Share access permissions include Full Control, Change and Read and are only used to determine access to the shared folder when it is accessed from the network. Share permissions are added to NTFS file permissions to determine the total cumulative permissions a user may have on an object.
- Shares that end with the dollar sign (**$**) are administrative shares and will not be seen by users exploring the system; however they can be mapped with the proper access permissions. These shares are designed to make system administration easier. You cannot set access permissions on special shares as they are assigned directly by Windows 2000. By default, the root of each NTFS volume is shared along with other special shares that depend on how the system is configured. All administrative shares are outlined in the table below.

Special share	Description
ADMIN$	Used during remote administration of a system, it provides access to the operating system at %systemroot%.
FAX$	Supports network faxes, and used by fax clients when sending faxes.
IPC$	Supports named pipes during IPC access. Used by programs for remote administration and remote resource access.
NETLOGON	Supports the NetLogon service. Used when processing domain logon events.
UAM Volume	Supports Macintosh file and printer services on a Windows 2000 domain. Used by File Server For Macintosh and Print Server For Macintosh.
PRINT$	Supports shared printer resources. Provides access to printer drivers for network printers.
SYSVOL	Supports the Active Directory. It is used to store all data and objects contained in the Active Directory.
X$	Allows Administrators to connect to the root of each volume, such as C$, D$, etc.

Configuring Web folders (KB# Q221600, Q287402, Q195851)

- Shortcuts to Web servers are known as Web or HTTP folders. The shortcuts are created automatically in My Network Places whenever you open resources on the servers, if you have read and write access to the server. You can also use the Add Network Place wizard to create shortcuts to Web servers and other computers.
- Web folders provide an easy way for you to view files and folders on Web servers. You can navigate from a Web page to a Web-folder view if you have read and write access to the Web server.
- You can view, manage, move, copy, save, and rename the files and folders on a Web server just as you would perform the same actions in Windows Explorer. However, when you view the contents of a Web folder, you see a list of files and folders and their associated Internet addresses.
- Before you can manage files and folders on a Web server, the Web server must support Web folders, which require the Web Extender Client (WEC) protocol and FrontPage extensions, or the WebDAV protocol and IIS, and you must have read and write access to the Web server.
- Web folders are created either through My Network Places or from Internet Explorer 5.0 and higher.
- To create a Web folder from My Network Places (shown in Figure 12):
    - Open My Network Places.
    - Double-click Add Network Place.
    - Provide the required information for the Wizard and click Finish when you are done. The new Web folder will show up in the My Network

Places folder. (Note that creating Web folders via this method will result in the actual selection being the final result.)

- To create a Web folder from Internet Explorer (shown in Figure 13):
  - Click File and then Open…
  - Place a check in the Open as Web Folder box.

Browse to the location containing the file you want to open. Click Open to select the file and then click OK to complete the process. The new Web folder will show up in the My Network Places folder. (Note that creating Web folders via this method will result in the root of the volume being the actual location of the Web folder shortcut.)

Figure 12 – Creating a Web folder from **My Network Places**.

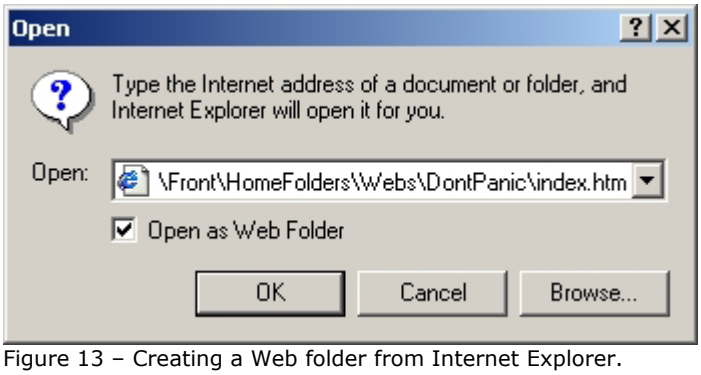

Figure 13 – Creating a Web folder from Internet Explorer.

Configure and troubleshoot Internet Information Services (IIS).

Configuring Virtual Servers

- Virtual Servers take on four different forms: Web Servers, FTP Servers, NNTP Servers and SMTP Servers. Any combination of the four can exist on the same machine. (It is important to note that on a Windows 2000 Professional machine, the option to implement NNTP Servers does not exist. NNTP Servers can only be created on a Windows 2000 Server machine. Additionally, the functionality of any Virtual Servers running on a Windows 2000 Professional machine will be limited when compared to a similar Windows 2000 Server Virtual Server. It is for these reasons that I recommend not using your Windows 2000 Professional machines to host Virtual Servers except perhaps for small internal Sites.)
- To create a Virtual Server (Web Site, FTP Site, SMTP Server or NNTP Server) perform the following set of actions:
    - In the Internet Services Manager console, select the computer or a site and click the **Action** button.
    - Click **New** and then the type of site or server you want to launch the site wizard with.
    - Follow the on-screen directions to assign identification information to your new site. You must provide the port address and the home directory path. If you are adding additional sites to a single IP address by using host headers, you must assign a host header name.
- In regards to **IP Address**, **All Unassigned** refers to IP addresses that are assigned to a computer but not assigned to a specific site. The default Web site uses all of the IP addresses that are not assigned to other sites. Only one site can be set to use unassigned IP addresses.
- For a Web Site, the Front Page Server Extensions must be configured separately after IIS has been installed and a Web Site created. Right click on the Web Site, select **All Tasks** and then select **Configure Server Extensions** to start the **Server Extensions Configuration Wizard**.

Configuring Web Site Virtual Servers

- A Virtual Server for a Web Site is configured from the *WebSiteName* Web Site Properties window as shown in Figure 14. Web Sites have the following configuration options:
    - From the **Web Site** tab, you can configure the Web Site description, IP Address to respond to, TCP port to use, SSL port to use, limited or unlimited connections, connection timeout, HTTP Keep-Alives allowed or not and Web Site logging options.

- From the **Operators** tab, you can add or remove user accounts that are to have operator privileges to this Web site.
- From the **Performance** tab, you can set performance tuning (how many connections you expect to have daily to the Web site), bandwidth throttling for the Web site and also process throttling for the Web site.
- From the **ISAPI Filters** tab, you can add, remove, edit or disable ISASPI filters for the Web Site.
- From the **Home Directory** tab, you configure the location of the home directory to be used for the Web Site, Read / Write / Directory Browsing permissions, logging, indexing (think twice about this), application settings, script executing permissions and application protection.
- From the **Documents** tab, you specify a default document or documents to be served (i.e., http://mysite.com/ becomes http://mysite.com/default.asp) and to set a document footer file (which should only contain the required HTML) that will be appended to every document sent by the Web server.
- From the **Directory Security** tab, you set your Web server's authentication and anonymous access control features, allow or prevent specific IP addresses or IP address ranges from connecting to the Web server, set / configure secure Server settings including SSL and use Directory Service client certificate mapping rather than the one-to-one or one-to-many mapping methods.
- From the **HTTP Headers** tab, you can configure controls for setting content expiration information for time sensitive information, provide custom HTTP Headers information that is returned in the header of a served HTML page, set and use content rating on your Web site and, lastly, configure MIME mappings for your Web site.
- From the **Custom Errors** tab, you can customize the HTTP errors that are sent to clients when Web server errors occur on your Web site. A full set of default error pages are provided and can be customized.
- From the **Server Extensions** tab (once the Front Page Server Extensions have been configured), you can select to enable authoring, choose a version control method, set performance options, set client scripting options, specify how e-mail should be set, configure Office collaboration features (only if Office Web Server is installed), log authoring actions, configure SSL properties, choose to allow authors to upload executes with their web sites and manually manage permissions.

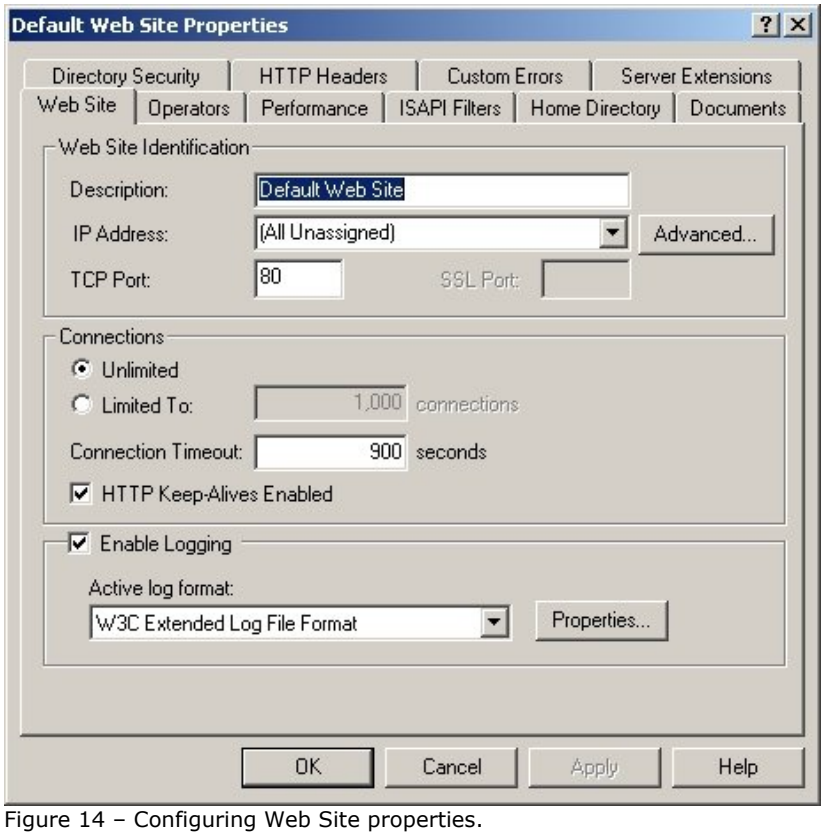

Figure 14 – Configuring Web Site properties.

Configuring FTP Site Virtual Servers

- A Virtual Server for an FTP Site is configured from the *FTPSiteName* Properties window as shown in Figure 15. FTP Sites have the following configuration options:
  - From the **FTP Site** tab, you can set the FTP site descriptive name, IP address, TCP port, number of allowed connections, inactive user timeout limits, current sessions on the FTP site, logging of FTP site activity (on or off) and also the type of logging to take place
  - From the **Security Accounts** tab, you can control how anonymous logins to the FTP site are to be handled, choose to let IIS control the password or not and add or remove FTP site operators.
  - From the **Messages** tab, you can create your own custom messages to be displayed to users. The messages are Welcome message, Exit message and Maximum connections message.

- From the **Home Directory** tab, you configure the location of the home directory to be used for the FTP site, Read and Write permissions, logging of visits and the directory listing style to be used.
- From the **Directory Security** tab, you can control access to FTP resources, such as sites, virtual directories, or files, by specifying the IP address, subnet mask, or domain name of the computer or computers to be granted or denied access.

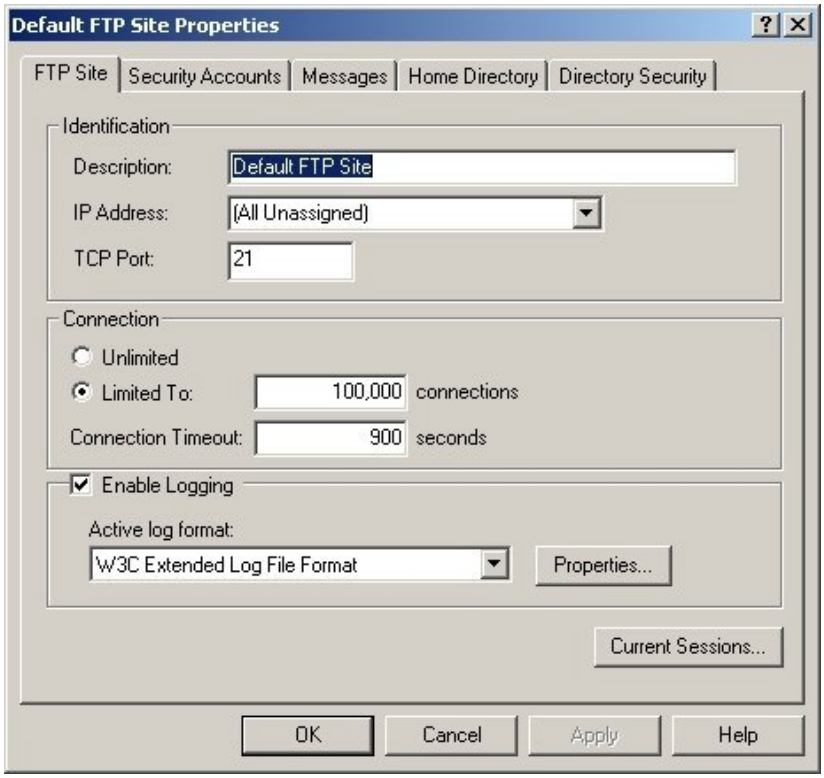

Figure 15 – Configuring FTP Site properties.

Configuring SMTP Virtual Servers

- The SMTP Server is configured from the *SMTPServerName* Properties window as shown in Figure 16. SMTP Servers have the following configuration options:
  - From the **General** tab, you assign the descriptive name to the SMTP server, IP address or IP addresses for the server to listen on, number of connections allowed, connection timeout value, whether or not logging will be performed on the server and what type of logging to use.

- From the **Access** tab, you configure the authentication methods to be used on the Server, create key pairs via the Certificate Wizard to allow TLS encryption, set the encryption level required on the Server, restriction of access by IP address or range and setting of relay features on the Server (caution with doing this as it may open your Server up to Spammers looking to hide their tracks).
- From the **Messages** tab, you configure settings for maximum message size, maximum session size, number of messages per session, number of recipients per message, specific routing for Non-Delivery Reports (NDR) and the location that a message should be sent to if it cannot be delivered after all retry intervals have been exhausted.
- From the **Delivery** tab, you specify the first, second, third and subsequent retry intervals for delivery, the delay notification and message expiration timeout settings, outbound security settings and other advanced delivery settings you wish to configure.
- From the **LDAP Routing** tab, you specify the name of the server running the LDAP service, the type of Schema (Active Directory, Site Server Membership Directory or Exchange LDAP Service), binding type that specifies how the SMTP Virtual Server is authenticated by the directory service, the domain name you want to bind to the LDAP directory, the distinguished name (DN) of the account that you want to use to bind to the LDAP directory, the password that corresponds to the chosen user name and the distinguished name of the container in the directory service that you will be accessing.
- From the **Security** tab, you can add or remove user accounts that you want to be designated as operators for the Virtual Server. Operators are allowed to access and make configuration changes on the Server.

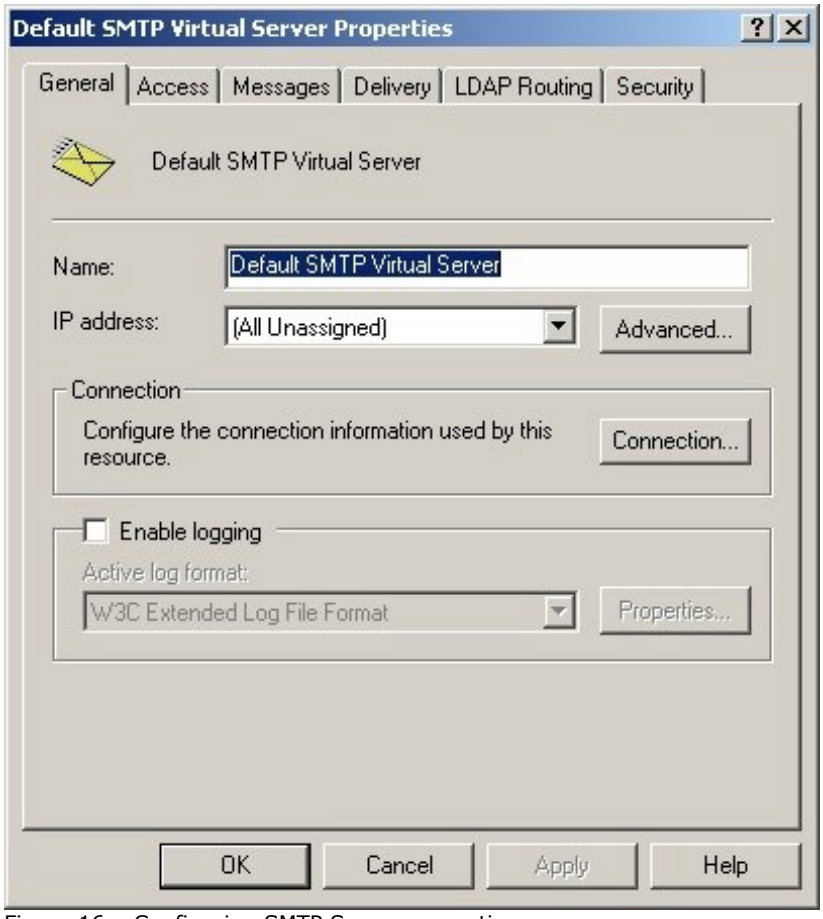

Figure 16 – Configuring SMTP Server properties.

Configuring NNTP Virtual Servers

- The NNTP Server is configured from the *NNTPServerName* Properties window as shown in Figure 17. FTP Sites have the following configuration options:
  - From the **General** tab, you can set the descriptive name of the Server, the IP address or addresses it is to listen on, number of simultaneous news connections allowed, turn logging on or off and set logging style, and the path string to be inserted into each message.
  - From the **Access** tab, you configure the authentication methods to be used on the Server, create key pairs via the Certificate Wizard to allow TLS encryption, set the encryption level required on the Server, and restrict access by IP address or range.
  - From the **Settings** tab, you: control posting of articles by clients, individual message size, maximum session size, posting of newsfeeds,

newsfeed individual post size, maximum newsfeed session size; allow or disallow other news servers to pull articles from your NNTP Virtual Server; and set the server to post messages for moderated groups to (by valid DNS entry or pathname), default moderator domain (this must be a qualified domain name) and administrator email account.

- From the **Security** tab, you can add or remove user accounts that you want to be designated as operators for the Virtual Server. Operators are allowed to access and make configuration changes on the Server.

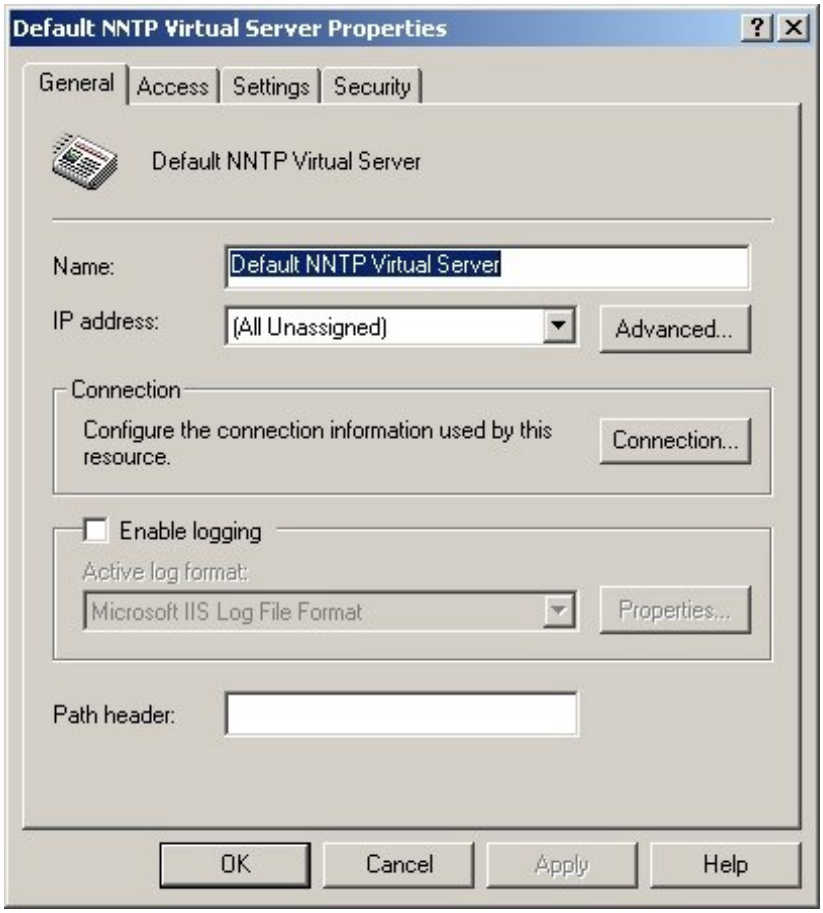

Figure 17 – Configuring NNTP Server properties.

Configuring Virtual Directories (KB# Q221600, Q172138)

- To create a Virtual Directory open the Internet Information Services console and perform the following sequence of actions:
  - Right-click on your default Web site, select **New** and then select **Virtual Directory…**
  - Dismiss the Wizard opening window by clicking **Next**. In the Alias text box, enter a description name for the new Virtual Directory.
  - Browse to or enter the directory that contains the content and click **Next**.
  - Select the applicable access permissions you wish to enable on the Virtual Directory from the following choices: Read, Run Scripts, Execute, Write and Browse. After making your selections, click **Next** and then click **Finish** to complete the Wizard.
- Right clicking on a Web Site Virtual Directory will bring up the properties window as shown in Figure 18. From here, you can customize your Virtual Directory to your requirements.
  - The **Virtual Directory** tab allows you to change the content location, log visits to the Web site, index the resource (might want to think twice about that option), set application settings, set execute permissions and set application protection.
  - The **Documents** tab allows you to specify a default document or documents to be served (i.e., http://mysite.com/ becomes http://mysite.com/default.asp) and to set a document footer file (which should only contain the required HTML) that will be appended to every document sent by the Web server.
  - The **Directory Security** tab allows you to set your Web server's authentication and anonymous access control features, allow or prevent specific IP addresses or IP address ranges from connecting to the Web server, set / configure secure Server settings including SSL and use the Directory Service client certificate mapping rather than the one-to-one or one-to-many mapping methods.
  - The **HTTP Headers** tab provides controls for setting content expiration information for time sensitive information, provide custom HTTP Headers information that is returned in the header of a served HTML page, set and use content rating on your Web site and, lastly, configure MIME mappings for your Web site.
  - The **Custom Errors** tab allows you to customize the HTTP errors that are sent to clients when Web server errors occur on your Web site. A full set of default error pages are provided and can be customized.

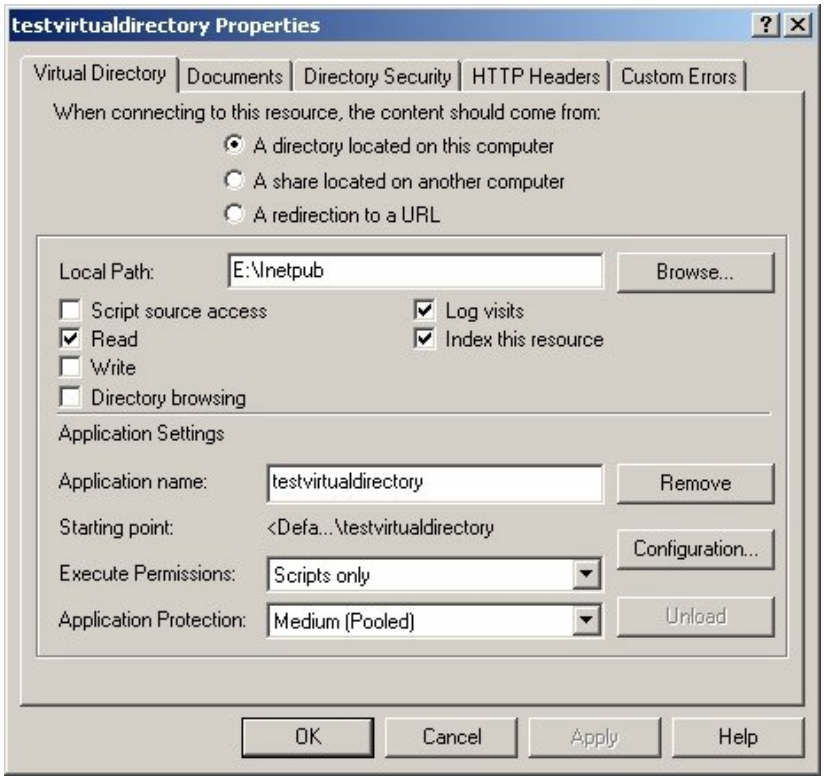

Figure 18 – Configuring Virtual Directory properties.

- A Virtual Directory for an FTP Site is created in the same fashion as that for a Web Site. The properties window for an FTP Site Virtual Directory allow you modify the following items:
  - Location of the home directory, either on the local computer or a network share.
  - The directory location of the FTP home directory.
  - Whether or not users have Read and Write access to the FTP Site and whether or not logging of visits is to take place.

Troubleshoot Internet browsing from client computers.

- The inability to browse the Internet from an internal client computer could be attributed to many possibilities or even a combination thereof.
- The first, and most simple, task to perform to see if the user is working online within Internet Explorer. The easiest way to check that this is not the case is to look at the title bar for **[Working Offline]** and also to look for, in the bottom left notification area, a disconnected folder icon. This is shown in Figure 19.

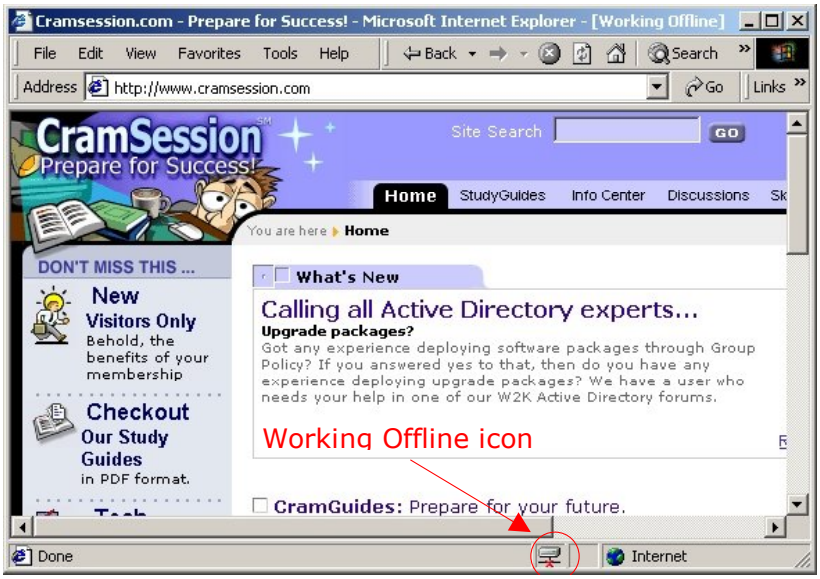

Figure 19 – Working offline in Internet Explorer.

- Another common cause of inability to connect to the Internet (i.e., outside of the local network) is the assignment of an incorrect default gateway or DNS Server address. This can happen in one of two ways:
  - The DHCP Server scope options are not set correctly. In this case, you will see this problem replicated across all client machines serviced by that particular DHCP Server, while clients holding leases from other DHCP Servers will report no connectivity issues.
  - An employee, with just enough knowledge to make him dangerous, has gone in and adjusted the TCP/IP settings for the machine manually. Manually assigned TCP/IP settings always override those obtained from a DHCP Server where there is a conflict. Note that Administrative privileges are required in Windows 2000 to adjust TCP/IP settings such as default gateway, DNS Servers, etc.

- If the client computer contains cached DNS information about the Internet location that is being accessed, it is possible that this information is no longer valid. From the command prompt type **ipconfig /flushdns** to clear the DNS cache on the local client.
- Access and/or privilege restrictions may be in place on the user account that are prompting the Proxy Server on the internal network to block outbound IP traffic for that particular user.
- Custom IP Filters, which prevent certain types of IP traffic from entering or exiting the internal network, may be in use on the network. This can be checked from the TCP/IP Filtering window (as shown in Figure 20), which can be accessed from the Options tab of the Advanced TCP/IP properties window. (The more likely scenario for IP Filtering is for it to actually be done via RRAS as filtering at the NIC level is not as effective. Filtering via RRAS takes place at the kernel level and is much more secure.)

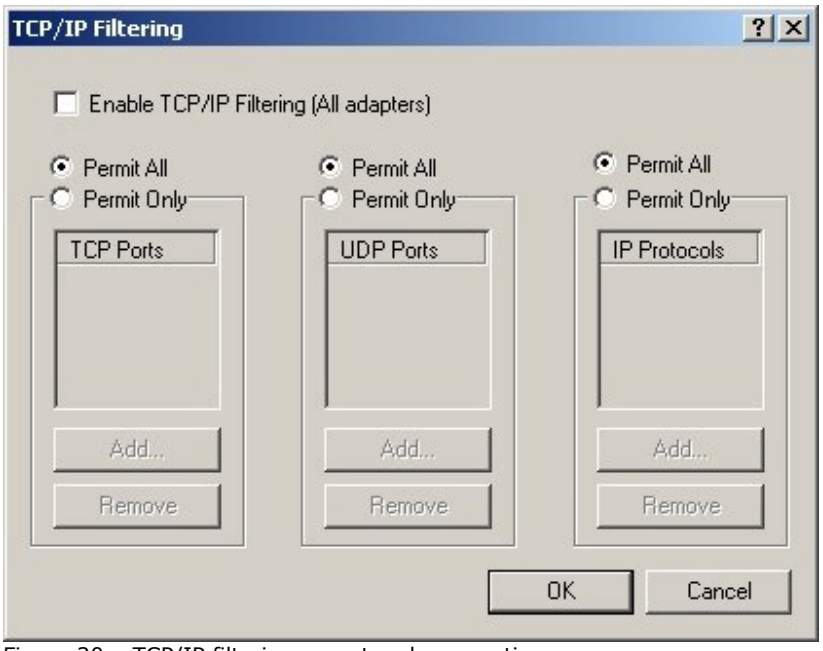

Figure 20 – TCP/IP filtering on network connections.

- It's always possible that a hardware failure may have occurred in the internal network, such as the failure of a DNS Server, Proxy Server or RAS Server. Testing them for connectivity via the **ping**, **pathping** and **tracert** commands should enable you to determine if this is the cause of the difficulties.
- If no access (including access to internal network resources) can be made from the client machine, the likely culprit is network hardware. Check that the network cable is attached and not damaged. Try moving the cable to a

different port on the hub or switch that it is attached to as ports can and will die. Ping the loop back address (**ping 127.0.0.1**) on the network adapter installed in the client machine to test that the NIC is functioning properly.

Configure authentication and SSL for Web sites.

- In order to authenticate users who log on with a client certificate, you must create mappings that tie the information contained in the user's certificate to a Windows user account. Mapping of certificates can be accomplished either via **one-to-one** mapping or **many-to-one** mapping. In either case, the **Internet Services Manager** console is used for establishing the mapping. The two types of mapping are defined below:
  - **One-to-one** mapping map individual client certificates to accounts. The server compares the copy of the client certificate it holds with the client certificate sent by the browser. The two must be absolutely identical for the mapping to proceed. If a client gets another certificate containing all of the same user information, it must be mapped again.
  - **Many-to-one** mapping uses *wildcard* matching rules that verify whether a client certificate contains specific information, such as issuer or subject. This mapping does not compare the actual client certificate, but rather accepts all client certificates fulfilling the specific criteria. If a client gets another certificate containing all of the same user information, the existing mapping will work.
- Alternatively, **Directory Service** (DS) mapping can be enabled. Directory Service (DS) certificate mapping uses native Windows 2000 Active Directory features to authenticate users with client certificates. There are both advantages (client certificate information is shared across many servers) and disadvantages (wildcard matching is not as advanced) to using DS mapping. You can enable DS mapping only at the Master properties level, and only if you are a member of a Windows 2000 domain. *Activating DS mapping will exclude the use of one-to-one and many-to-one mapping for the entire Web service.*
- A server certificate must be installed in order for certificate mapping to be enabled. If one does not exist, you can create it as follows:
  - Right-click the Web Site you are working with and select **Properties**. Change to the **Directory Security** tab and click **Server Certificate** in the **Secure Communications** area (as shown in Figure 21).
  - The Web Server Certificate Wizard will open. Click Next to dismiss the opening page. Select **Create a new certificate** and click **Next** to continue. Complete the Wizard to finish creating the new server certificate.
  - After completing the creation of the new server certificate the **View Certificate** and **Edit** buttons will become available for your use.

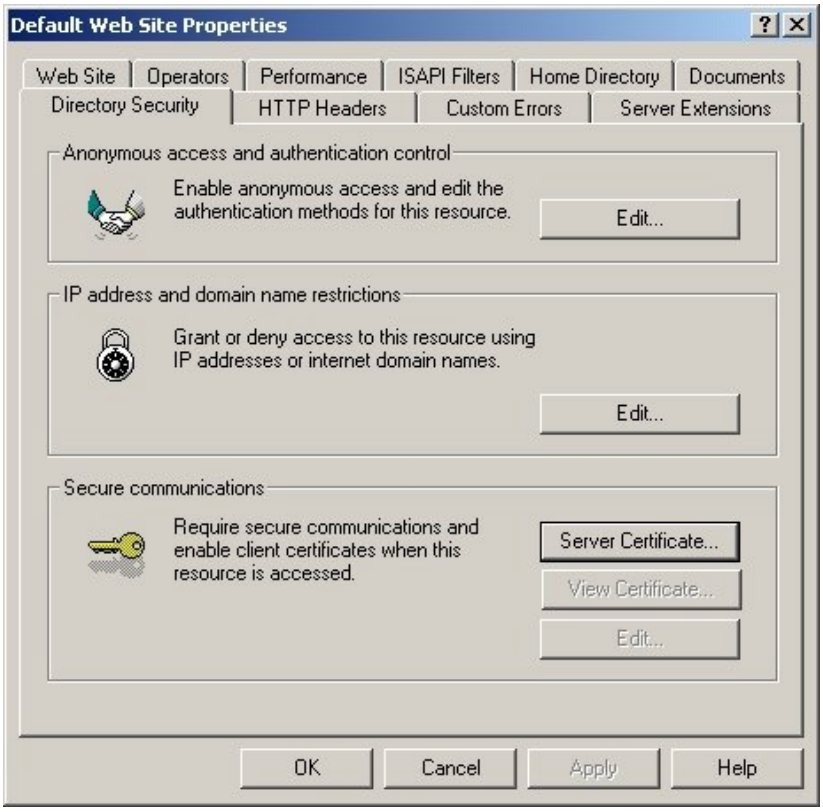

Figure 21 – Creating a Server Certificate for a Web Site.

- In order to ensure that changes to mapping rules take effect on the server, you much stop and restart the Web Site. From the **Internet Services Manager** console, right-click the Web Site and select **Stop**. Right-click the Web Site again and now select **Start** to complete the process.
- Certificate mapping is flexible in that you can use any of the three available methods to map certificates to users accounts. You could potentially map a client certificate to any number of users accounts and conversely, you could map any number of certificates to a single user account. Some mapping examples:
    - In a large network with a large number of certificates, many-to-one mapping could be utilized by creating one or more matching rules that map certificates to one or more user accounts.
    - In a smaller network with a small number of users, one-to-one mapping could be introduced to provide greater control of certificate usage. Similarly, many-to-one mapping could be used to create an easier administration situation.

  - For Internet sites that use certificate authentication, many-to-one mapping that accepts a variety of different certificates (such as customer certificates) could map all of the certificates to an account with permissions such as those of the **IUSR_computername** built-in account.
  - For high-security resources with a limited number of users, one-to-one mapping could be implemented to ensure that only certain certificates can be used.
  - For tracking of all users logging on with a certificate issued by a particular Certificate Authority (CA) or organization, a many-to-one mapping could be implemented with a matching rule that maps certificates issued by that CA or organization to a specific user account.
- Create a one-to-one mapping as follows:
  - From the **Directory Security** tab of the **Properties** window, click **Edit** in the **Secure Communications** section. Place a check mark in the box next to **Enable client certificate mapping** (if not already done) and click **Edit** (shown in Figure 22).
  - From the **1-to-1** tab of the **Account Mappings** window, you can add a new certificate by clicking **Add**, or edit an existing mapping by selecting the mapping and clicking **Edit Map**. If a new certificate is being adding, you will need to browse to the certificate file. If the certificate file cannot be found, then it will need to be exported first.
  - In the **Map to Account** dialog box, enter a map name for the mapping. This is the name that will be displayed in the selection list on the **Account Mappings** dialog box. Either type or browse to a Windows user account. Type the password of the account that the certificate is mapping to. Click **OK**.
  - Repeat these steps to map other certificates or to map this certificate to other accounts.

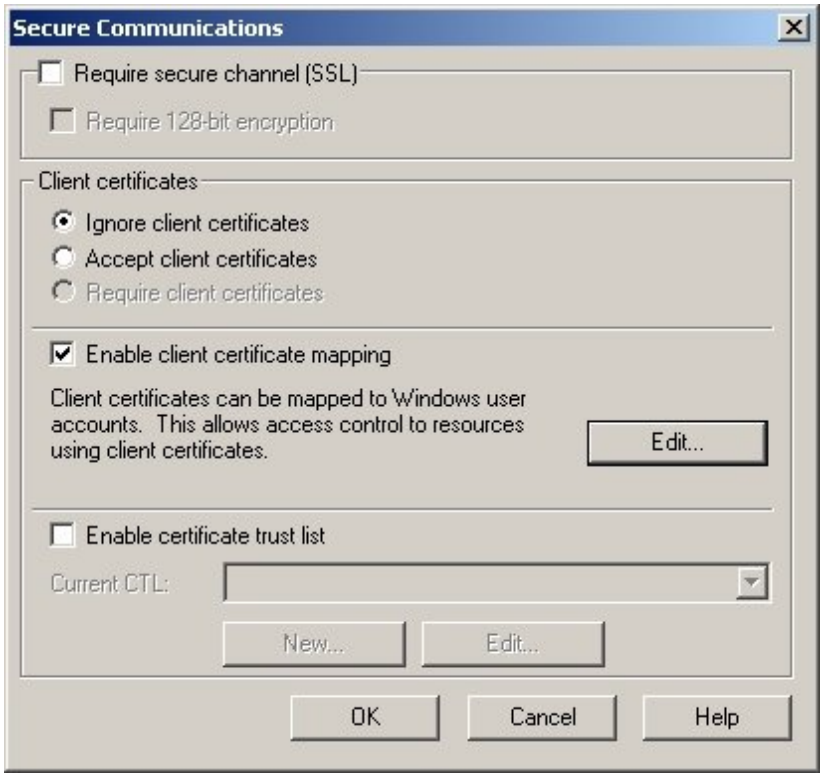

Figure 22 – Enabling client certificate mapping for a Web Site.

- Create a many-to-one mapping as follows:
  - From the **Directory Security** tab of the **Properties** window, click **Edit** in the **Secure Communications** section. Place a check mark in the box next to **Enable client certificate mapping** (if not already done) and click **Edit** (shown in Figure 22).
  - Switch to the **Many-to-one** tab of the **Account Mappings** dialog box and click **Add**. In the **General** dialog box, type a name for the rule. This is the name that will be displayed in the selection list on the **Account Mappings** dialog box. You can create rules for future use or disable rules without deleting them by selecting or clearing the **Enable this wildcard rule** check box. Click **Next**.
  - In the **Rules** dialog box click **New**. In the **Edit Rule Element** dialog box, select the appropriate criteria and click **OK**. A sample rule is shown in Figure 23. When you have finished defining the rule, click **Next**. In the **Mapping** dialog box, either type or browse to a Windows user account. Type the password of the account that the rule is mapping to. Click **OK** to complete the mapping creation.

- Repeat these steps to create other mapping rules. Use the **Move Up** and **Move Down** buttons to establish the precedence given to the rules. Rules higher in the list take precedence.

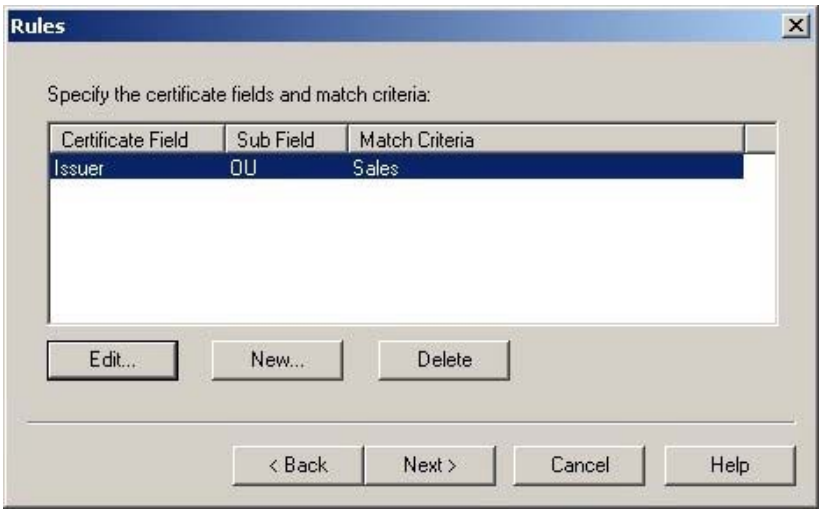

Figure 23 – Creating a many-to-one rule (this one is based on the Issuing OU).

Mappings with specific information will always take precedence over wildcard mappings.

Configure FTP services (KB# Q300662)

- You will need to ensure that Internet Information Services is installed on the Server that you want to use for your FTP Site. If IIS is not already installed, you must do so as follows:
  - Click Start > Settings > Control Panel. From the Control Panel, run the Add/Remove Programs applet and then select Add/Remove Windows Components. When the Windows Components Wizard window opens, select Internet Information Services (IIS), then click Details to allow selection of specific IIS services.
  - Select the following options: Common Files, Documentation, File Transfer Protocol (FTP) Server, and Internet Information Services Snap-In (as shown in Figure 24). Click OK and then click Next.
  - If you get a prompt to configure Terminal Services, click Next. If you are prompted for FTP root folder path, you can either accept the default (C:\Inetpub\Ftproot) or choose your own. Either way, the FTP root should be located on an NTFS volume to ensure maximum security. Click OK to continue. If prompted, supply the Windows 2000

Server CD or specify the location to the source files. Click OK and then click Finish to complete the procedure.

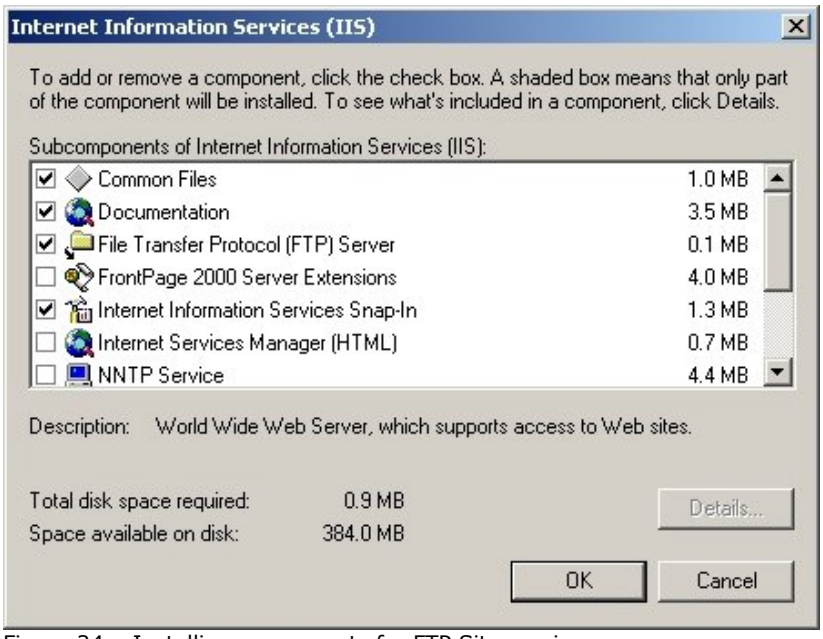

Figure 24 – Installing components for FTP Site services.

- At this point, you can now configure your FTP site. A basic (read: quick and dirty) configuration process is presented below. Using the information presented earlier in this Cramsession (**Configuring FTP Site Virtual Servers** and **Configuring Virtual Directories**) you can perform additional and advanced configuration of your FTP Site.
    - Click **Start > Programs > Administrative Tools > Internet Services Manager**. Click the "+" next to the server name to expand the node. Right click your FTP Site (the default Site is named, appropriately enough **Default FTP Site)** and click **Properties**.
    - To begin the configuration, change to the **Security Accounts** tab and select the following two options: **Allow Anonymous Connections** and **Allow Only Anonymous Connections**.
    - Enable logging by changing to the **Home Directory** tab and selecting the following options: **Read** and **Log Visits**. Unless you are going to allow uploading to your new FTP Site, clear the **Write** option.
    - Click OK to close the Properties window and save your settings. You have now configured a basic FTP Site that will allow anonymous connections for downloading only. If you have not done so already, you need to make the files available in the FTP root that you want to grant access to.

- Some other advanced options and scenarios for configuring FTP Sites are presented below:
  - Individual home directories for FTP users can be configured by creating a subdirectory with the same name as the user account inside the FTP root (KB# Q138698). This could be useful if the FTP server is used a central collection and distribution point for distant users.
  - An FTP Server can be set up behind an ISA Server or a Proxy Server (KB# Q209400) or on the same server as a Proxy Server (KB# Q210459).
  - Server-to-Server FTP transfers can be conducted (KB# Q247132).

Configuring and Implementing Auditing (KB# Q232714, Q301037, Q267556)

- While the fact still remains (and most likely always will) that network security starts with physical security, there are still a few things that an Administrator should do to harden their network against attack and detect attacks being conducted.
- Before we get any further into configuring and implementing auditing, we need to review three important terms: Discretionary Access Control List (DACL), System Access Control List (SACL) and Access Control Entry (ACE).
  - The *Discretionary Access Control List* is a list that represents part of an object's security descriptor and allows or denies permissions to specific users and groups.
  - The *System Access Control List* is a list that represents part of an object's security descriptor and specifies which events are to be audited per user or group.
  - An *Access Control Entry* is an entry in object's DACL that grants certain permissions to a user or a group. An ACE is also an entry in an object's SACL that specifies the security events to be audited for a user or a group.

- Auditing is a process that can be used to track what is going on in your network down to a very granular level. Some possible audit reasons are listed below:

Audit Event	Potential Threat
Failure audit for logon/logoff	Random password hack
Success audit for logon/logoff	Stolen password break-in
Success audit for user rights, user and group management, security change policies, restart, shutdown, and system events	Misuse of privileges
Success and failure audit for file-access and object-access events. File Manager success and failure audit of Read/Write access by suspect users or groups for the sensitive files.	Improper access to sensitive files
Success and failure audit for file-access printers and object-access events. Print Manager success and failure audit of print access by suspect users or groups for the printers.	Improper access to printers
Success and failure write access auditing for program files (.EXE and .DLL extensions). Success and failure auditing for process tracking. Run suspect programs; examine security log for unexpected attempts to modify program files or create unexpected processes. Run only when actively monitoring the system log.	Virus outbreak

- In order to use auditing, you must enable it; this can be done on the domain level or on a specific computer (in our example, we are configuring for the entire domain). If you choose to audit access to objects as part of your audit policy, you must turn on either the **Audit directory service access** category (for auditing objects on a domain controller), or the **Audit object access** category (for auditing objects on a member server). Enabling auditing via Group Policy is shown in Figure 25.

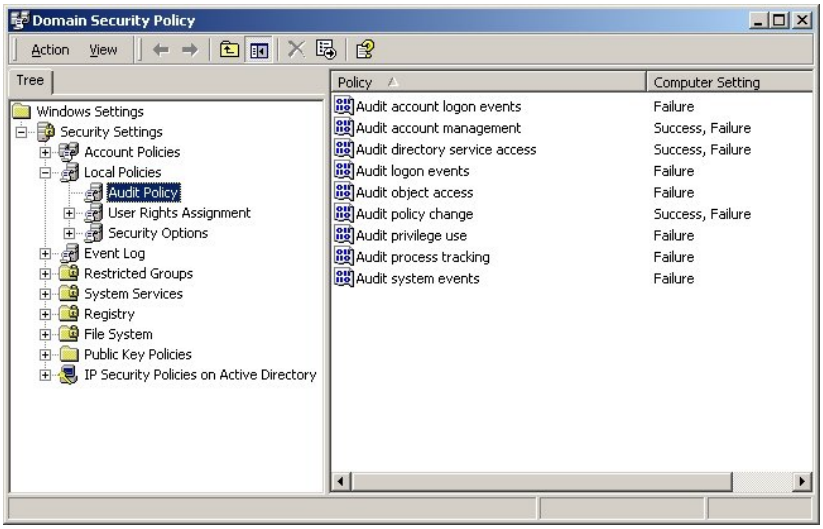

Figure 25 – Enabling auditing events via Domain Security Policy.

- Additionally, to allow auditing of file access, you will need to configure the auditing options for the folders and files of concern. To configure these auditing options, select the folder or file you want to audit and right-click. Select **Properties** and change to the **Security** tab. Click **Advanced** and then switch to the **Auditing** tab. Click **Add** to add a new auditing configuration. Select the users, groups or computers you want to apply the settings to and then click **OK**. You will now have a window like the one shown in Figure 26, where you can configure exactly what kind of auditing to perform on the folder or file in question. Make your selections and click **OK** three times to complete the configuration.
- When you audit a file or folder, an entry is written to the Event Viewer security log whenever the file or folder is accessed in a certain way (more on this later).

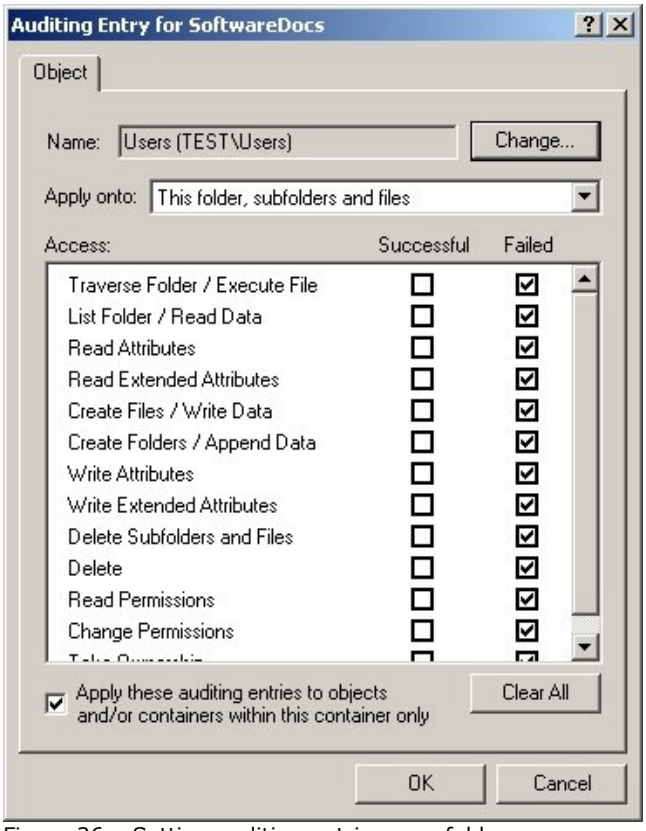

Figure 26 – Setting auditing entries on a folder.

Using Auditing and the Security Log to Find Security Issues

- Once you have configured your auditing policies, you now must let the system collect the data and then analyze it to detect security and privilege abuse problems.
- After the changes have been propagated to your machines, you can look in the **Security Log** of the **Event Viewer** console to see what is going on in your network. Notice that gold keys represent success audit events and gold locks represent failure audit events, as shown in Figure 27.
- Enabling too many items for auditing will result in your Security Log quickly filling up. Too much logging is not a good thing as it adds unnecessary overhead to your network and provides so much information, you have trouble picking out the items you are looking for.

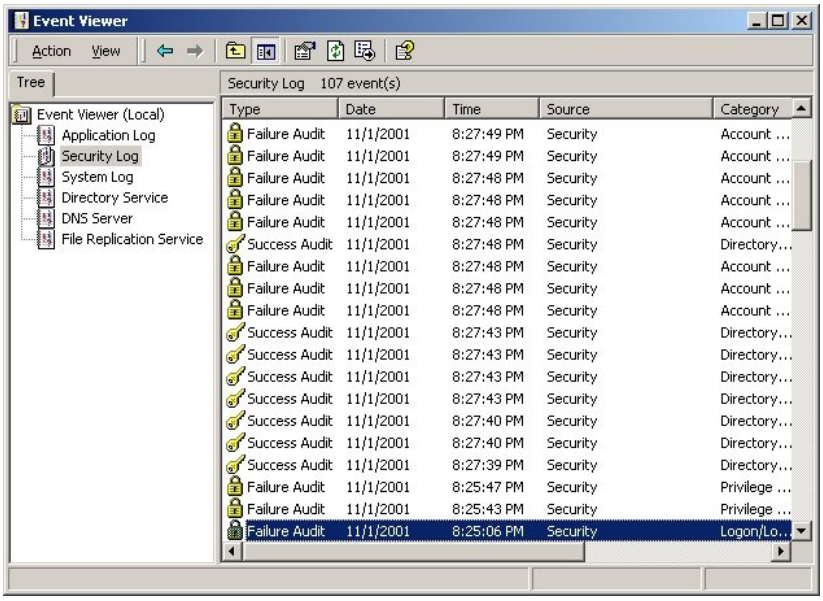

Figure 27 – Audit Events in the Security Log.

- An example of an Event in the **Security Log** is shown below in Figure 28. Here, a logon error occurred as a result of a bad password (brute force hacking?).

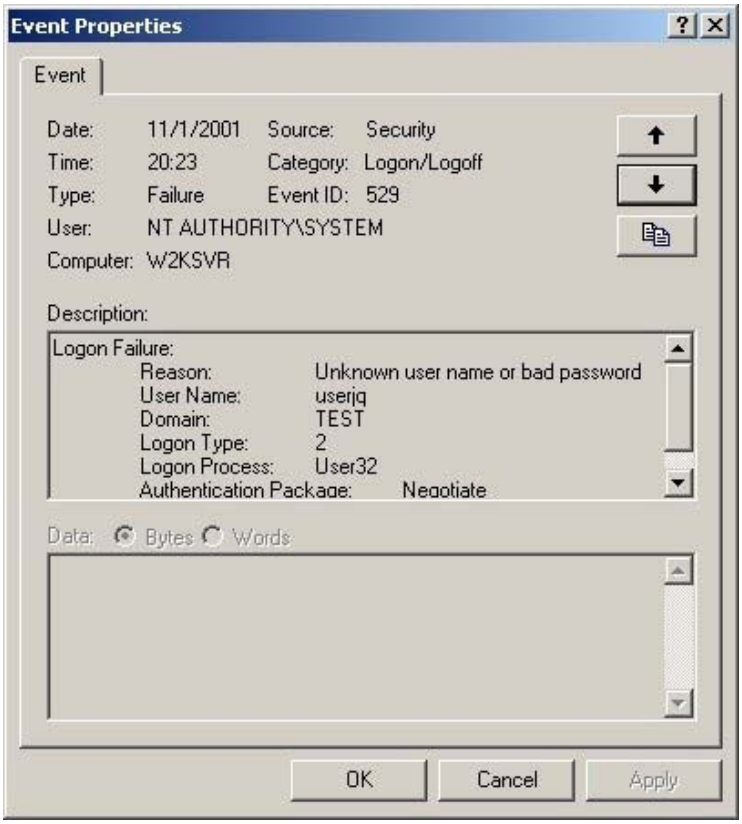

Figure 28 – Event Properties for a logon failure event.

- But how do you find specific entries in your Security Log that you are looking for. Fortunately, Microsoft has provided us with a filtering capability which is configured as follows:
    - To set up filtering, right click on log of interest (in this case, the **Security Log**) and select **Properties**. Change to the **Filter** tab and configure filtering to suit your needs as shown in Figure 29, where we have set up filtering to show only failure audit events from the logon process.

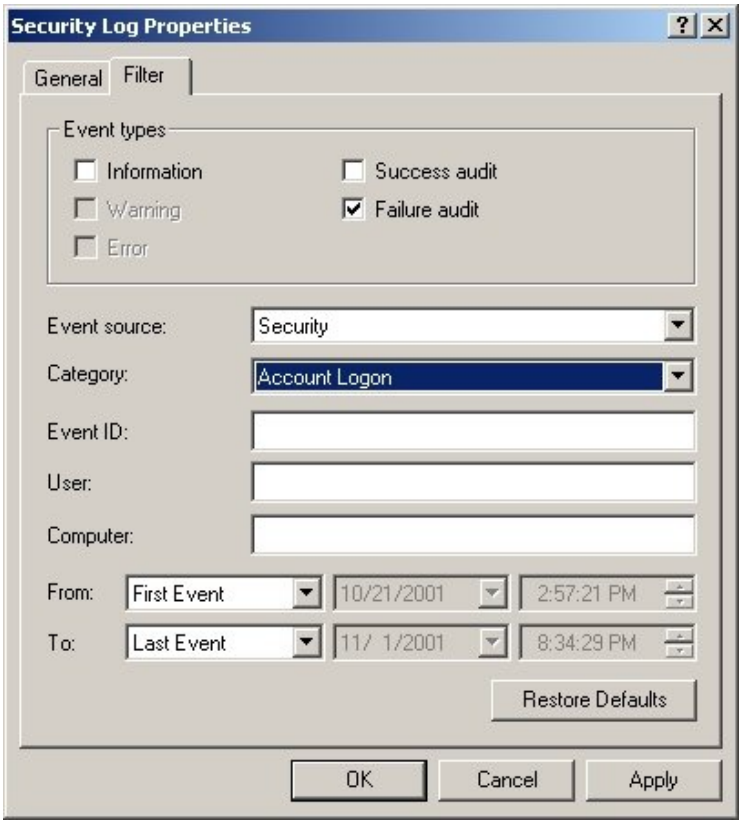

Figure 29 – Using log filtering to find desired information.

Configuring, Administering, and Troubleshooting the Network Infrastructure

Troubleshoot routing. Diagnostic utilities include the tracert command, the ping command, and the ipconfig command.

tracert (KB# Q162326, Q169206, Q217014, Q300986)

- This diagnostic tool determines the path taken to a destination by sending ICMP Echo Request messages with varying Time to Live (TTL) values to the destination. Each router along the path is required to decrement the TTL in an IP packet by at least 1 before forwarding it. Effectively, the TTL is a maximum link counter. When the TTL on a packet reaches 0, the router is expected to return an ICMP Time Exceeded message to the source computer.

- Usage: **tracert** [**-d**] [**-h** *MaximumHops*] [**-j** *HostList*] [**-w** *Timeout*] [*TargetName*]

Parameter	Description
-d	Prevents **tracert** from attempting to resolve the IP addresses of intermediate routers to their names. This can speed up the display of **tracert** results.
-h	Specifies the maximum number of hops in the path to search for the target (destination). The default is 30 hops.
-j	Specifies that Echo Request messages use the Loose Source Route option in the IP header with the set of intermediate destinations specified in *HostList*. With loose source routing, successive intermediate destinations can be separated by one or multiple routers. The maximum number of addresses or names in the host list is 9. The *HostList* is a series of IP addresses (in dotted decimal notation) separated by spaces.
-w	Specifies the amount of time in milliseconds to wait for the ICMP Time Exceeded or Echo Reply message corresponding to a given Echo Request message to be received. If not received within the time-out, an asterisk (*) is displayed. The default time-out is 4000 (4 seconds).
TargetName	Specifies the destination, identified either by IP address or host name.

ping (KB# Q217014, Q300986, Q102908)

- Verifies IP-level connectivity to another TCP/IP computer by sending Internet Control Message Protocol (ICMP) Echo Request messages. The receipt of corresponding Echo Reply messages are displayed, along with round-trip times. Ping is the primary TCP/IP command used to troubleshoot connectivity, reach-ability, and name resolution. Used without parameters, **ping** displays help.
- This command is available only if the **Internet Protocol (TCP/IP)** protocol is installed on the computer.
- Usage: **ping** [**-t**] [**-a**] [**-n** *Count*] [**-l** *Size*] [**-f**] [**-i** *TTL*] [**-v** *TOS*] [**-r** *Count*] [**-s** *Count*] [{**-j** *HostList* | **-k** *HostList*}] [**-w** *Timeout*] [*TargetName*]

Parameter	Description
-t	Specifies that ping continue sending Echo Request messages to the destination until interrupted. To interrupt and display statistics, press CTRL-BREAK. To interrupt and quit ping, press CTRL-C.
-a	Specifies that reverse name resolution is performed on the destination IP address. If this is successful, ping displays the corresponding host name.
-n	Specifies the number of Echo Request messages sent. The default is 4.
-l	Specifies the length, in bytes, of the Data field in the Echo Request messages sent. The default is 32. The maximum size is 65,527.
-f	Specifies that Echo Request messages are sent with the Don't Fragment flag in the IP header set to 1. The Echo Request message cannot be fragmented by routers in the path to the destination. This parameter is useful for troubleshooting path Maximum Transmission Unit (PMTU) problems.
-i	Specifies the value of the TTL field in the IP header for Echo Request messages sent. The default is the default TTL value for the host. The maximum TTL is 255.
-v	Specifies the value of the Type of Service (TOS) field in the IP header for Echo Request messages sent. The default is 0. TOS is specified as a decimal value from 0 to 255.
-r	Specifies that the Record Route option in the IP header is used to record the path taken by the Echo Request message and corresponding Echo Reply message. Each hop in the path uses an entry in the Record Route option. If possible, specify a Count that is equal to or greater than the number of hops between the source and destination. The Count must be a minimum of 1 and a maximum of 9.
-s	Specifies that the Internet Timestamp option in the IP header is used to record the time of arrival for the Echo Request message and corresponding Echo Reply message for each hop. The Count must be a minimum of 1 and a maximum of 4.
-j	Specifies that the Echo Request messages use the Loose Source Route option in the IP header with the set of intermediate destinations specified in HostList. With loose source routing, successive intermediate destinations can be separated by one or multiple routers. The maximum number of addresses or names in the host list is 9. The host list is a series of IP addresses (in dotted decimal notation) separated by spaces.
-k	Specifies that the Echo Request messages use the Strict Source Route option in the IP header with the set of intermediate destinations specified in HostList. With strict source routing, the next intermediate destination must be directly reach-able (it must be a neighbor on an interface of the router). The maximum number of addresses or names in the host list is 9. The host list is a series of IP addresses (in dotted decimal notation) separated by spaces.
-w	Specifies the amount of time, in milliseconds, to wait for the Echo Reply message that corresponds to a given Echo Request message to be received. If the Echo Reply message is not received within the time-out, the "Request timed out" error message is displayed. The default time-out is 4000 (4 seconds).
TargetName	Specifies the destination, which is identified either by IP address or host name.

ipconfig (KB# Q117662, Q223413, Q235272, Q300986)

- Displays all current TCP/IP network configuration values and refreshes Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) settings. Used without parameters, **ipconfig** displays the IP address, subnet mask, and default gateway for all adapters.
- This command is available only if the **Internet Protocol (TCP/IP)** protocol is installed on the computer.
- Usage: **ipconfig** [**/all**] [**/renew** [*Adapter*]] [**/release** [*Adapter*]] [**/flushdns**] [**/displaydns**] [**/registerdns**] [**/showclassid** *Adapter*] [**/setclassid** *Adapter* [*ClassID*]]

Parameter	Description
/all	Displays the full TCP/IP configuration for all adapters. Without this parameter, ipconfig displays only the IP address, subnet mask, and default gateway values for each adapter. Adapters can represent physical interfaces, such as installed network adapters, or logical interfaces, such as dial-up connections.
/renew [Adapter]	Renews DHCP configuration for all adapters (if an adapter is not specified) or for a specific adapter if the Adapter parameter is included. This parameter is available only on computers with adapters that are configured to obtain an IP address automatically. To specify an adapter name, type the adapter name that appears when you use ipconfig without parameters.
/release [Adapter]	Sends a DHCPRELEASE message to the DHCP server to release the current DHCP configuration and discard the IP address configuration for either all adapters (if an adapter is not specified) or for a specific adapter if the Adapter parameter is included. This parameter disables TCP/IP for adapters configured to obtain an IP address automatically. To specify an adapter name, type the adapter name that appears when you use ipconfig without parameters.
/flushdns	Flushes and resets the contents of the DNS client resolver cache. During DNS troubleshooting, you can use this procedure to discard negative cache entries from the cache, as well as any other entries that have been added dynamically.
/displaydns	Displays the contents of the DNS client resolver cache, which includes both entries preloaded from the local Hosts file and any recently obtained resource records for name queries resolved by the computer. The DNS Client service uses this information to resolve frequently queried names quickly, before querying its configured DNS servers.
/registerdns	Initiates manual dynamic registration for the DNS names and IP addresses that are configured at a computer. You can use this parameter to troubleshoot a failed DNS name registration or resolve a dynamic update problem between a client and the DNS server without rebooting the client computer. The DNS settings in the advanced properties of the TCP/IP protocol determine which names are registered in DNS.
/showclassid Adapter	Displays the DHCP class ID for a specified adapter. To see the DHCP class ID for all adapters, use the asterisk (*) wildcard character in place of Adapter. This parameter is available only on computers with adapters that are configured to obtain an IP address automatically.

/setclassid Adapter [ClassID]	Configures the DHCP class ID for a specified adapter. To set the DHCP class ID for all adapters, use the asterisk (*) wildcard character in place of Adapter. This parameter is available only on computers with adapters that are configured to obtain an IP address automatically. If a DHCP class ID is not specified, the current class ID is removed.

Configure and troubleshoot TCP/IP on servers and client computers. Considerations include subnet masks, default gateways, network IDs, and broadcast addresses.

Configuring TCP/IP on servers

- All servers should have a static IP address and other pertinent TCP/IP information. You can configure this information as follows:
  - From the **Network and Dial-up Connections** window, select the network adapter connection that you wish to configure, right-click and select **Properties**. Select **Internet Protocol (TCP/IP)** and then click **Properties**.
  - Select **Use the following IP address** radio button and enter a static IP address, subnet mask and default gateway address as shown in Figure 30. Click the **Advanced** button and change to the **DNS** tab.
  - From the DNS tab, select **Append primary and connection specific DNS suffixes**, **Append parent suffixes of the primary DNS suffix** and **Register this connection's addresses in DNS**.
  - Click **OK** three times to close all windows and save the changes.

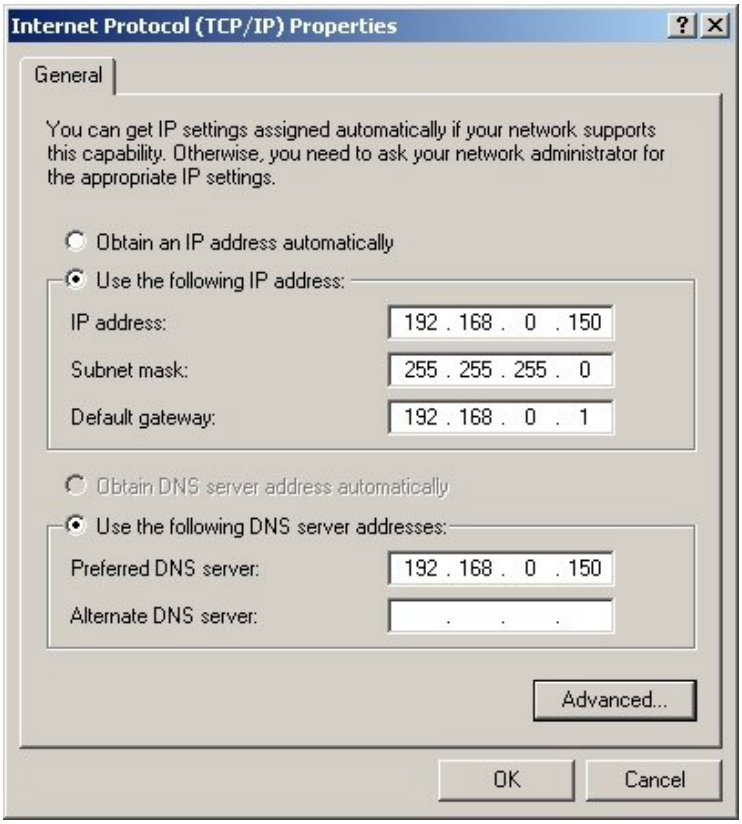

Figure 30 – Static IP address information for a server.

Configuring TCP/IP on clients

- The easiest (and most error-proof) method of configuring TCP/IP settings for network clients is by letting them obtain all required DHCP information from a DHCP Server via a lease.
- In order for a client to obtain a DHCP lease, the client must be able to contact the DHCP Server. For arrangements where the DHCP Server is on the same subnet as the client, no problems should typically be encountered unless the DHCP Server is out of leases to give.
- For clients that are not on the same subnet as a DHCP Server, one of two things must be in place to allow these clients to obtain a lease. Either the DHCP relay agent must be installed on a computer in the subnet or the router separating the subnet from the rest of the network must be BOOTP capable. These requirements exist because the DHCP process is carried out by broadcast messages. Routers do not pass broadcast messages out of the local subnet in an effort to decrease network traffic (KB# Q197197).

- To view the current TCP/IP settings for a client computer, use the **ipconfig** utility from the command line.
- Administrative privileges will be required to make any changes to the TCP/IP configuration on the machine, although users may be able to diagnose simple configuration problems via the **ipconfig** utility.

Configure, administer, and troubleshoot DHCP on servers and client computers.

Detecting unauthorized DHCP servers on a network (KB# Q244978, MSDN)

- Windows 2000 DHCP servers that have not been authorized in Active Directory will show up in the DHCP console with a red down arrow next to their name. Additionally they will not be able to hand out DHCP leases.
- Authorization does not work on Windows NT 4.0 DHCP servers and other DHCP server software. In this case, the detection of unauthorized servers rests squarely on the shoulders of the Network or System Administrator. The best bet is use a Windows 2000 only DHCP configuration on your network. The same is also true for DNS; it functions best when it's a Windows 2000 configuration.
- If you suspect non-Windows 2000 DHCP servers are on your network, you may be able to sniff them out by using the Network Monitor and running some **ipconfig/renew** commands from clients on the subnets where you suspect the unauthorized servers may be at. A twist on this issue is that the DHCP lease allocator that is built into Windows 2000 and Windows XP Internet Connection Sharing does not need authorization in Active Directory to begin handing out its DHCP leases.
- For the authorization process to work properly, it is critical that the first DHCP server on the network be a Windows 2000 Active Directory participant, either a Domain Controller or a Member Server. A stand-alone server is not an appropriate choice for your DHCP server.
- Windows 2000 DHCP has been specially modified to detect unauthorized DHCP servers on the network. The following process describes how a DHCP server determines if it is authorized on the network:
    - When the DHCP service starts, it sends a DHCP informational message (DHCPINFORM) request to the reachable network, using the local limited broadcast address (255.255.255.255), to locate the root domain on which other DHCP servers are installed and configured.
    - This message includes several vendor-specific option types that are known and supported by other DHCP servers running Windows 2000 Server. When received by other DHCP servers, these option types enable the query and retrieval of information about the root domain.

- When queried, other DHCP servers reply with DHCP acknowledgement messages (DHCPACK) to both acknowledge and answer with root domain information. In this way, the initializing DHCP server collects and compiles a list of all currently active DHCP servers on the reachable network, along with the root (of the root domain) used by each server.
- After a list of all DHCP servers running on the network is built, the next step in the detection process depends on whether a directory service is found to be available from the local computer.
- If the directory service is not available (such as where the initializing DHCP server is installed in a confined network environment used for testing) the initializing server can start if no other DHCP servers are discovered on the network that are part of any enterprise. Where this condition is met, the server successfully initializes and begins serving DHCP clients.
- However, the server continues every five minutes to collect information about other DHCP servers running on the network, using DHCPINFORM as it did at startup. Each time, it checks whether the directory service is available. If a directory service is found, the server ensures that it is authorized by following the procedure, depending on whether it is a member server or a standalone server.
- For member servers, the DHCP server queries the directory service for the DHCP server list of addresses that have been authorized. If the server finds its IP address in the authorized list, it initializes and starts providing DHCP service to clients. If it does not find itself in the authorized list, it does not initialize and stops providing DHCP services.
- For stand-alone servers, the DHCP server queries the directory service with the root of the enterprise returned by each of the other DHCP servers to see if it can find itself on the authorized list with any of the reported enterprises. The server initializes and starts providing DHCP services to clients *only if* the server finds its IP address in the authorized list for each of the enterprise roots reported by other DHCP servers. If it does not find itself in the authorized list for each of the reported enterprise roots, it does not initialize and the DHCP service is stopped.

Configuring authorization of DHCP servers (KB# Q303317, Server Documentation)

- Even though you may have configured a DHCP server in your network, it still must be authorized in the Active Directory before it can start giving out DHCP leases.
- After you have finished configuring the DHCP server, right click on it and select **Authorize**. (Note that this can also be done from the **Action** menu as well.) Wait a minute or so, refresh the console and you will see the red down arrow next to the server name change to a green up arrow—the DHCP server is now authorized and can begin handing out DHCP leases to requesting clients on the network.
- Another method to authorize servers in Active Directory is to right click on **DHCP** in the DHCP console, and select Manage Authorized Servers—this brings up a window as shown in Figure 31. Simply add the server(s) to be authorized, click **OK** and then **YES** if correct. You should now have something similar to what is shown in Figure 32.

Figure 31 – Authorizing servers in DHCP.

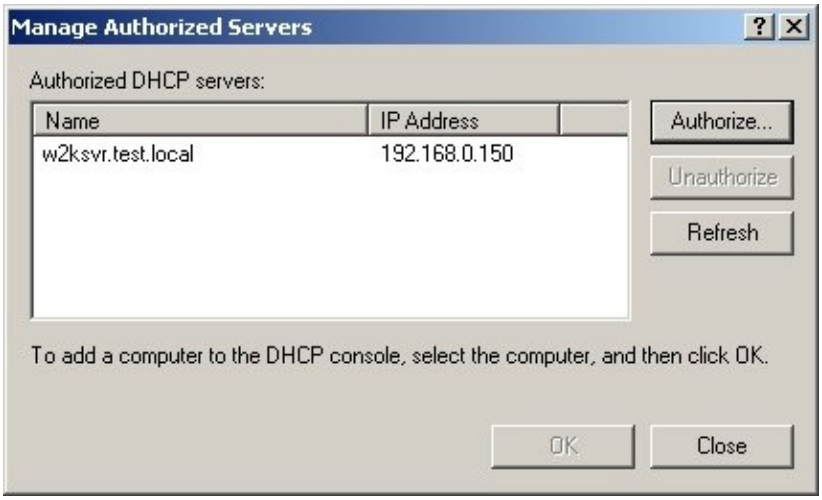

Figure 32 – Authorized DHCP servers on the network.

- For a DHCP server to be authorized in an Active Directory domain environment, you must first be logged on as a member of the Enterprise Administrators group for the enterprise where the server is being added. Alternatively, you may be delegated (done from Active Directory Sites and Services) to manage DHCP servers to be able to perform the authorization process.
- Servers that are to be used for Remote Installation Services (RIS) must also be authorized in this same manner before they can be used on the network to perform remote installations.

Configure, administer, and troubleshoot DNS

Domain Name System (KB# Q291382, Q300386, Q164054)

- The Domain Name System is a system for naming computers and network devices that is organized into a hierarchical system. DNS is the naming system that is used by the TCP/IP network because of its scalability and resiliency to locate computers and other network services through user-friendly names such as www.cramsession.com versus numerical IP addresses. When a DNS name is entered into a TCP/IP aware application, DNS services work to resolve the name to the IP address, thus facilitating communications.
- The following guidelines, if followed, should help prevent or minimize problems with DNS:
    - *Be conservative in adding alias records to zones.* Avoid using CNAME resource records (RRs) where they are not needed to alias a host name used in a host (A) resource record.

- *Use Active Directory-integrated zones for best results and simplified deployment and troubleshooting.* Active Directory integrated zones simplify network planning and troubleshooting because the same servers are used in replication for both services. Additionally, Active Directory integrated zones are much more secure from attack or compromise as well as bring more resilience to network failures.
- *Be aware of the points of failure and configuration issues that apply to using dynamic updates with standard primary type zones.* If not using Active Directory integrated zones, the use of standard primary type zones will be required for the DNS namespace. This results in one DNS server being designated as the primary server for a zone. Only the primary server, as determined in the SOA record properties for the zone, can process an update to the zone.
- *Use secondary or caching-only servers to reduce loading.* Secondary servers can be used as backups for DNS clients or as the preferred DNS servers for legacy DNS clients. For mixed-mode environments, this allows you to use secondary servers as a means to load balance DNS query traffic on your network, and reserve your DNS-enabled primary servers for use only by those clients that need them to perform dynamic registration and updates of their A and PTR RRs.

Configuring DNS (KB# Q237675)

- Before you can begin the process to effectively configure DNS services from your server, you must prepare the server itself. Doing so includes setting static entries for the IP address among other items as follows:
  - From the **Network and Dial-up Connections** window, select the network adapter connection that you wish to configure, right-click and select **Properties**. Select **Internet Protocol (TCP/IP)** and then click **Properties**.
  - Select **Use the following IP address** radio button and enter a static IP address, subnet mask and default gateway address as shown previously in Figure 30. Click the **Advanced** button and change to the **DNS** tab.
  - From the DNS tab, select **Append primary and connection specific DNS suffixes**, **Append parent suffixes of the primary DNS suffix** and **Register this connection's addresses in DNS**.
  - If this DNS server is to be used on a private network (Intranet), then it should point only to its own IP address for **DNS server address**. Should the server need to resolve names outside the private network, it should have a forwarder configured. (Configuring DNS forwarders is discussed later in this Cramsession.)
  - Click **OK** three times to close all windows and save the changes.

- Now the server is configured (TCP/IP wise at least) to support the DNS service, you will need to install it if it's not already present by following the process outlined below:
    - From the **Add/Remove Programs** applet in the **Control Panel**, click **Add/Remove Windows Components**. Click Network Services, then click Details to customize what components are installed. Select Domain Name Service (DNS). Click **OK** and then **Next** to complete the procedure for installing the DNS services.
    - Note that promoting a server to a Domain Controller (**dcpromo**) will prompt you to install DNS services on that server if not already enabled.
- Now that you have a DNS server, you will need to configure it to provide service to the network as follows (not all inclusive):
    - Click **Start > Programs > Administrative Tools** and select the **DNS** console. There will be two zones under the server name: a **Forward Lookup Zone** and a **Reverse Lookup Zone**.
    - To add a Forward Lookup Zone (DNS name to IP address), right-click **Forward Lookup Zone** and then click **New Zone**. Follow the New Zone Wizard to complete the creation of your new zone. It is important to remember that you must create a **Standard primary** zone if you want accept dynamic updates to the zone. If you are participating an Active Directory domain, the best choice would be to create an **Active Directory-integrated** zone, thus allowing for secure updates and integrated storage with the Active Directory information.
    - To add a Reverse Lookup Zone (IP address to DNS name), use the same process as for adding a Forward Lookup Zone.
    - Figures 33 and 34 show the completion of the New Zone Wizard.
    - If you are operating in mixed mode with Windows NT 4.0 DNS servers or UNIX BIND DNS servers, it is best to have your Primary DNS server (or Active Directory-integrated DNS server) on your Windows 2000 machines and use the legacy servers as **Standard secondary** zones only until you can phase them out of the network. (This is discussed in more detail later in this Cramsession.)

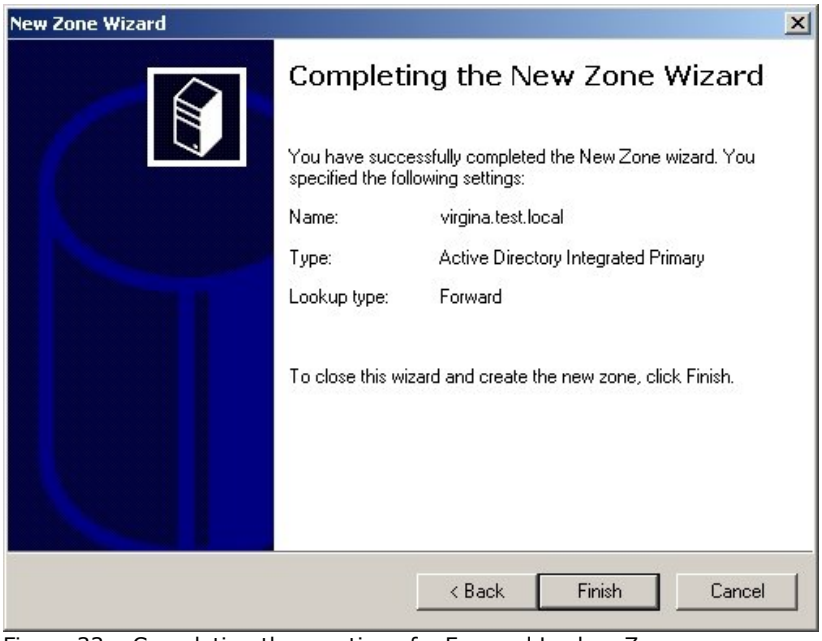

Figure 33 – Completing the creation of a Forward Lookup Zone.

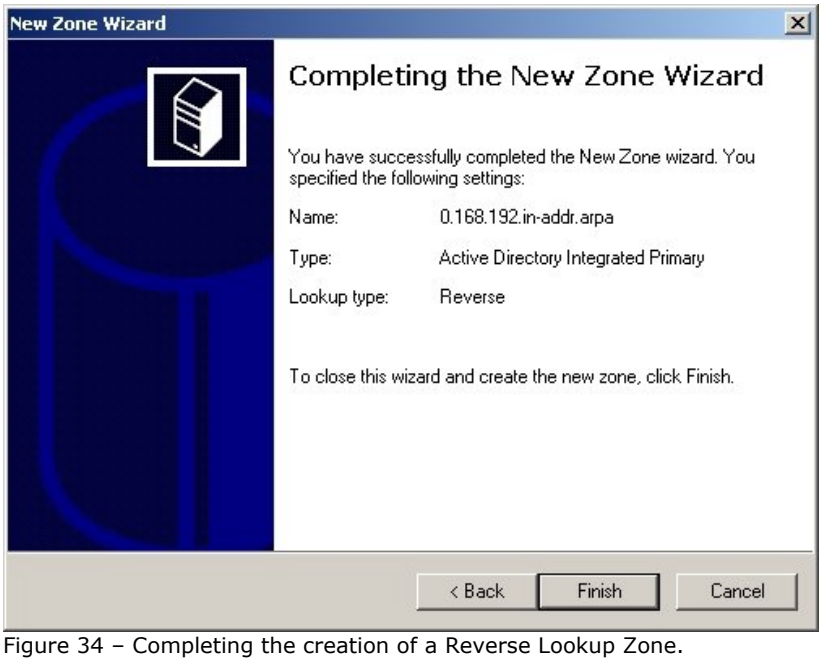

Figure 34 – Completing the creation of a Reverse Lookup Zone.

- If your DNS server must resolve addresses outside of the private network, then you must configure it for DNS forwarding. Right-click the DNS server in question, select **Properties** and change to the **Forwarders** tab. Add forwarders and set options as required as shown in Figure 35. If you want this DNS server to only use forwarders, place a check mark in the **Do not use recursion** box.

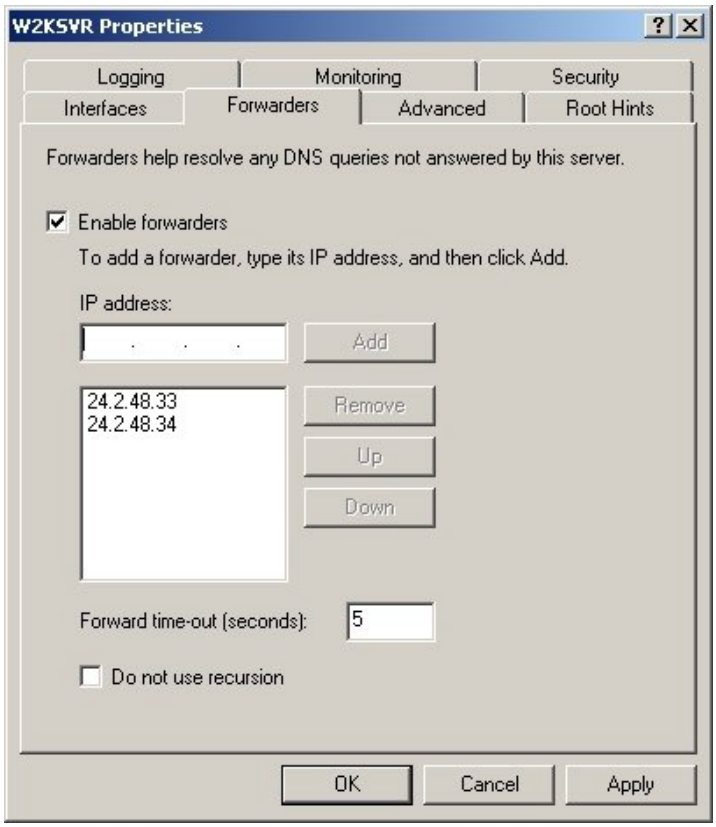

Figure 35 – Enabling DNS forwarders for a DNS server.

Additional DNS Configuration Options

- If you selected a Standard zone, you will now want to enable dynamic updates (KB# Q228803, Q222463) on the zone as follows:
  - Right-click the zone in question and then click **Properties**.
  - From the **General** tab, select **Yes** in the **Allow Dynamic Updates** box and then click **OK** to accept the change.
  - Root or "." zones cannot be configured for dynamic update (KB# Q232187).

- If you have an existing Standard zone that you wish to convert to an Active Directory-integrated zone, you may do so as follows:
  - Right-click the zone in question and then click **Properties**.
  - From the **General** tab, click the **Change....** button to bring up the dialog box shown in Figure 36. Select **Active Directory-integrated** and click **OK**. The DNS server will write the zone into Active Directory.
  - If not already done, change to **Allow Dynamic Updates**.

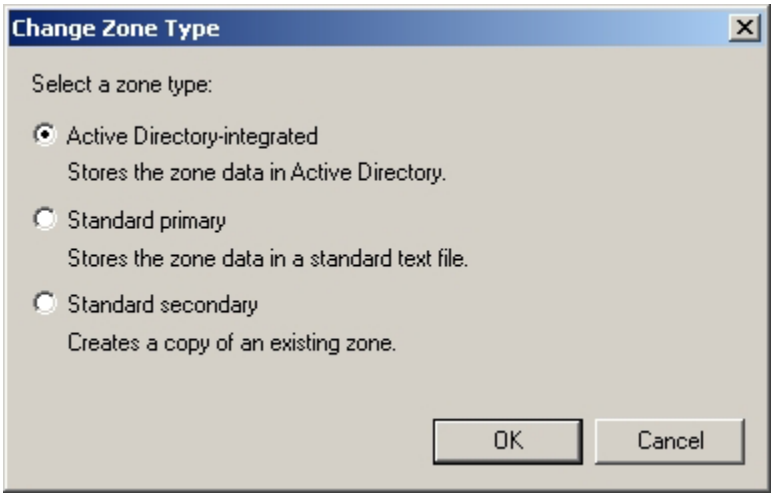

Figure 36 – Changing the zone type of an existing DNS zone.

- The following KB articles provide additional, advanced information and troubleshooting for DNS and Active Directory (KB# Q241505, Q241515, Q178169, Q254680).

Integrating Active Directory DNS zones with non-Active Directory DNS zones

- An Active Directory Integrated zone stores its data in Active Directory rather than on the local machine, thus providing greater fault-tolerance and secure updates (KB# Q227844).
- ACL editing provides granular access to either the zone or a specified resource record in the zone. (e.g., the ACL for a specific domain name can be set so that dynamic updates are only permitted for designated DNS clients or to authorize only specific groups with permissions for updating zone or record properties). This feature is not available for standard primary zones.
- Non Microsoft DNS servers can be used with AD so long as they support RFCs 2052 (SRV records) and 2163 (dynamic updates). The DNS server in Windows NT Server 4.0 cannot be used with AD; however, BIND versions 8.1.2 and later can.

DNS Miscellaneous Information (KB# Q217769)

- Resolves hostnames to IP addresses.
- Active Directory cannot run without it.
- **A** records are also called forward lookups or host records. An A record maps a domain name to an IP address.
- Start Of Authority (**SOA**) records names the primary DNS server for a domain, provides an e-mail address for the admin, and specifies how long it's okay to cache its data. Keeps track of data changes through serial numbers (KB# Q163971).
- **NS** records designate which servers are Name Servers in the domain.
- **CNAME** (Canonical Name) Records or Aliases used to provide an alias for the hostname of the server. For example, a Web server at brainbuzz.com may have the hostname "jaxx", but its CNAME alias allows it to respond to "www.brainbuzz.com" (KB# Q168322).
- **MX** (Mail Exchange) records allow an admin to designate which machines receive mail in a domain by order of preference (a lower number equals higher preference).
- **PTR** (Pointer) records are also called reverse records or reverse lookups. Allow an IP address to be resolved to a host name. Creates ".in-addr.arpa" entries (KB# Q164213).
- **SRV** records allow DNS to identify server types (KB# Q232025, Q178169).
- A Standard Primary zone stores a master copy of the zone in a text file. Used to exchange DNS data with other servers that use text-based storage methods.
- A Standard Secondary zone creates a copy of an existing zone - used for load balancing and fault-tolerance.
- A caching DNS server simply resolves requests and caches data from resolved requests until its TTL expires. This is handy for a location that needs DNS functionality but doesn't need a separate domain (KB# Q167234).

Managing replication of DNS data

- In MS speak, *Zone Transfer* refers to the duplication of data between DNS servers that do **not** participate in AD. *Zone Replication* refers to the replication of data between DNS servers (on domain controllers) that **do** participate in AD.
- Zone Transfer uses DNS Notification (RFC 1996) whereas in Zone Replication, DNS servers poll AD approx every 15 minutes (by default - depends on SOA refresh interval) for updates.
- There are two zone transfer types, full zone transfer (AXFR) and incremental zone transfer (IXFR):

- *AXFR* - supported by most DNS implementations. When the refresh interval expires on a secondary server it queries its primary using an AXFR query. If serial numbers have changed since the last copy, a new copy of the entire zone database is transferred to the secondary (KB# Q164017).
- *IXFR* - Also uses serial numbers, but only transfers information that has changed rather than the entire database. The server will only transfer the full database if the sum of the changes is larger than the entire zone, the client serial number is lower than the serial number of the older version of the zone on the server or the server responding to the IXFR request doesn't recognize that type of query (RFC 1995).

Troubleshoot name resolution on client computers. Considerations include WINS, DNS, NetBIOS, the Hosts file, and the Lmhosts file.

Troubleshooting WINS Issues (KB# Q272510, Q188001, Q119495)

- The Windows Internet Name Service (WINS) provides a dynamic, replicated database service that can register and resolve NetBIOS names to IP addresses.
- The following guidelines, if followed, should help prevent or minimize problems with WINS:
  - *Use default settings to configure WINS servers.* Using the default WINS settings provide the optimal configuration for most conditions and should be used in most WINS network installations.
  - *Avoid using static WINS entries.* The use of static WINS entries will require further administrative action to ensure their successful and intended use. A situation where static entries would be appropriate is the WINS registration of the names used by servers.
  - *Schedule consistency checking for an off-peak time.* WINS database consistency checking is network and resource intensive for the WINS server computer. For this reason, run WINS consistency checks during times of low traffic, such as at night or on weekends.
  - *Select Push/Pull when configuring replication partners.* Avoid the use of limited replication partnerships (Push Only or Pull Only) between WINS servers, except in special cases where replication must occur over slow WAN links.
  - *Use only as many WINS servers as you need.* As with all network services, seek to avoid having too many WINS servers on the network

as too many WINS servers on a network can complicate any problems that arise.
    - *Monitor and perform regular, offline compaction.* In order to help boost performance and minimize fragmentation of the WINS database, regular offline compaction is highly recommended.
    - *Perform regular backups of the WINS database.* Use the WINS console to perform WINS database backup and restoration if required.
    - *Configure clients with more WINS server IP addresses.* Avoid a Single Point Of Failure (SPOF) on the network by configuring clients with all WINS servers that are relevant to them.
    - *Configure each WINS server computer to point to itself.* To prevent problems that can occur if a WINS server doesn't register itself, each WINS server that you install on your network must register its own set of NetBIOS unique and group names in WINS.
- The following common problems may be encountered when dealing with WINS:
    - *Name resolution may fail at the client computer.* Determine whether WINS or DNS is being used for name resolution and if the name failure is occurring for a NetBIOS or fully qualified domain name (FQDN). This error can also be caused by incorrect configuration settings, whether the configuration has been set manually or via DHCP lease. To check a client IP configuration, use the **ipconfig /all** command. If the configuration is not correct, you can either supply the correct information manually or use the **ipconfig /renew** command to force the client to obtain a renewal of its DHCP lease and associated options.
    - *The client may not have basic connectivity with its configured WINS servers.* Try the **ping** command to test network connectivity between the client and server. If the WINS server responds positively to the **ping** command, try using the **nbtstat -RR** command at both the client and also at the resource server that the client is attempting to locate by name. Using **nbtstat –RR** will force the WINS service on both computers to send release and refresh requests to the WINS server.

The primary or secondary WINS server may not be able to service the client. Verify that the WINS service is started and running on the responsible WINS servers for the client. If the WINS servers are running, search for the name in the WINS database that the client requested. If the name does not appear in the database, investigation into replication between your WINS servers will be required to detect the problem.

Troubleshooting DNS Issues:

- The following common problems may be encountered when dealing with DNS:
  - *The DNS client received a "Name not found" error message.* This error can also be caused by incorrect configuration settings, whether the configuration has been set manually or via DHCP lease. To check a client IP configuration, use the **ipconfig /all** command. If the configuration is not correct, you can either supply the correct information manually or use the **ipconfig /renew** command to force the client to obtain a renewal of its DHCP lease and associated options.
  - *The DNS client cannot contact its configured DNS servers.* If the DNS client has basic connectivity to the network, verify that it can contact a preferred (or alternate) DNS server by using the **ping** command. A failure of DNS servers to respond to direct pinging is likely a network connectivity problem and not a DNS server issue.
  - *The DNS server is not running or responding to queries.* If the DNS client can ping the DNS server computer, verify that the DNS server is started and able to listen for and respond to client requests. Try using the **nslookup** command to test whether the server can respond to DNS clients.
  - *The DNS server is not responding to clients.* Verify that the server computer has a valid functioning network connection, including all network adapters, cables, etc. If no hardware problems can be found, check that it has connectivity with the rest of the network by pinging other computers that are on the same network as the affected DNS server.
  - *The DNS server is reachable through basic network testing but is not responding to DNS queries from clients.* If the DNS client can ping the DNS server computer, verify that the DNS server is started and able to listen to and respond to client requests. Try using the **nslookup** command to test whether the server can respond to DNS clients.
  - *The DNS server provides incorrect data for queries it successfully answers*. Some of the most likely causes include the following:
    - Resource records (RRs) were not dynamically updated in a zone.
    - An error was made when manually adding or modifying static resource records in the zone.
    - There are stale resource records in the DNS server database, left from cached lookups or zone records not updated with current information or removed when they are no longer needed.

- **Dnscmd.exe** is a command-line tool that you can use to view the properties of DNS servers, zones, and resource records. To be able to check your DNS server configuration, use the **Dnscmd** tool or the DNS Manager console to obtain information about the DNS server and obtain statistics about its performance. **Dnscmd** is also used to manually modify DNS server properties, to create and delete zones and resource records, and to force replication events between DNS server physical memory and DNS databases and data files.
- Use **nslookup** to troubleshoot problems with DNS (KB# Q200525).
- DNS server event messages are kept separate from events written by other applications and services in the DNS server log which can be viewed using Event Viewer (KB# Q235427).
- A log file, **dns.log**, can be enabled for debugging purposes. It is stored in the %systemroot\system32\dns folder by default. All debugging options are disabled by default because they can be resource-intensive. The logging options are as follows:

Option	Description
answers	Logs contents of answer section for each query message handled by the DNS server service.
full packets	Logs number of full packets written and sent by the DNS server service.
notify	Logs notification messages received from other servers by the DNS server service.
query	Logs queries received by the DNS server service from clients.
questions	Logs question section from each query message processed by DNS server service.
receive	Logs number of query messages received by the DNS server service.
send	Logs number of query messages sent by the DNS server service.
TCP	Logs number of requests received over a TCP port by the DNS server service.
UDP	Logs number of requests received over a UDP port by the DNS server service.
update	Logs dynamic updates received from other computers by the DNS server service.
write through	Logs number of packets written through and back to the zone by the DNS server service.

Troubleshooting NetBIOS Issues (KB# Q188001, Q188305, Q262963, Q227419, Q257942)

- Prior to Windows 2000, all MS-DOS and Windows-based operating systems required the NetBIOS naming interface to support network capabilities. With the release of Windows 2000 (and its default use of TCP/IP), support for the NetBIOS naming interface is no longer required for networking computers.
- NetBIOS is still supported in Windows 2000 to provide support for legacy operating systems that require its use. All Windows 2000 computers that use TCP/IP (and that should be all of them) are enabled to provide client-side support for registering and resolving NetBIOS names via NetBIOS over TCP/IP (**NetBT**), which can be manually disabled from the WINS tab of the TCP/IP Advanced settings window (shown in Figure 37). Additionally, Windows 2000 Server provides server-side support through the use of WINS.
- The exact mechanism by which NetBIOS names are resolved to IP addresses depends on the NetBIOS node type that is configured for the node. RFC 1001 defines the NetBIOS node types, which are discussed in the table below.

Node type	Description
B-node (broadcast)	B-node uses broadcast NetBIOS name queries for name registration and resolution. B-node has two major problems: (1) Broadcasts disturb every node on the network, and (2) Routers typically do not forward broadcasts, so only NetBIOS names on the local network can be resolved.
P-node (peer-peer)	P-node uses a NetBIOS name server (NBNS), such as a WINS server, to resolve NetBIOS names. P-node does not use broadcasts; instead, it queries the name server directly.
M-node (mixed)	M-node is a combination of B-node and P-node. By default, an M-node functions as a B-node. If an M-node is unable to resolve a name by broadcast, it queries an NBNS using P-node.
H-node (hybrid)	H-node is a combination of P-node and B-node. By default, an H-node functions as a P-node. If an H-node is unable to resolve a name through the NBNS, it uses a broadcast to resolve the name.

- By default, all computers running Windows 2000 are B-node but change over to H-node when they are configured with a WINS server.
- **Nbtstat** is a useful tool for troubleshooting NetBIOS name resolution problems. You can use the **nbtstat** command to remove or correct preloaded entries.
- Usage: **nbtstat** [**-a** *remotename*] [**-A** *IP address*] [**-c**] [**-n**] [**-R**] [**-r**] [**-S**] [**-s**] [*interval*]

Parameter	Description
–n	Displays the names that were registered locally on the system by programs such as the server and redirector.
–c	Shows the NetBIOS name cache, which contains name-to-address mappings for other computers.
–R	Purges the name cache and reloads it from the Lmhosts file.
–RR	Releases NetBIOS names registered with a WINS server and then renews their registration.
–a *name*	Performs a NetBIOS adapter status command against the computer specified by *name*. The adapter status command returns the local NetBIOS name table for that computer plus the media access control address of the adapter.
–S	Lists the current NetBIOS sessions and their status, including statistics.

Troubleshooting the Hosts file (KB# Q142309, Q108295)

- TCP/IP in Windows 2000 can be configured to search Hosts (the local host table file) for mappings of remote host names to IP addresses. The Hosts file format is the same as the format for host tables in the 4.3 Berkeley Software Distribution (BSD) UNIX /etc/hosts file.
- By using a text editor, you can create and change the Hosts file because it is a simple text file. An example of the Hosts format is provided in the file named Hosts in the Windows 2000 **%SystemRoot%\System32\Drivers\Etc** directory. Edit the Hosts file (created when you install TCP/IP) to include remote host names and IP addresses for each computer with which you communicate.
- The process by which the Hosts file is utilized for name resolution is as follows:
    - Computer A enters a command using the host name of Computer B.
    - The HOSTS file on Computer A (contained in the **%SystemRoot%\system32\drivers\etc** directory) is parsed. When the host name of Computer B is found, it is resolved to an IP address.
    - The Address Resolution Protocol (ARP) is then used to resolve the IP address of Computer B to its hardware address. If Computer B is on the local network, its hardware address will be obtained by using the ARP cache or by sending a local broadcast asking for a reply from Computer B with its hardware address. If Computer B is on a remote network, ARP will determine the hardware address of the default gateway for routing to Computer B.

Troubleshooting the Lmhosts file (KB# Q101927, Q102725, Q180099)

- The Lmhosts file is a static file that assists with remote NetBIOS name resolution on computers that cannot respond to NetBIOS name-query broadcasts. It contains NetBIOS name-to-IP addresses mappings. Its function is similar to that of the Hosts file; the difference is that the Hosts file can be used to map DNS domain names for host computers to their IP addresses.
- By default, the Lmhosts file does not exist. There is an **Lmhosts.sam** sample file that you can use as a basis for creating an Lmhosts file. Lmhosts can be enabled on the network by selecting it on the **WINS** tab of the **Advanced TCP/IP Settings** window as shown in Figure 37.

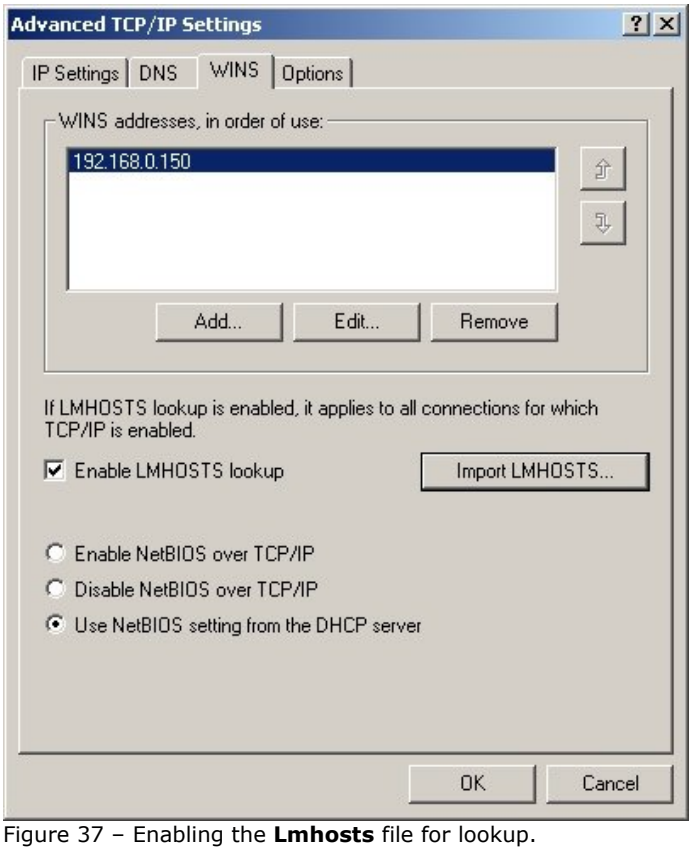

Figure 37 – Enabling the **Lmhosts** file for lookup.

- Computers in a Windows network can resolve NetBIOS names in several ways. If one method fails, they try the next method, in a fixed order. In a broadcast-based network, the computer first checks its NetBIOS name cache. If static name-to-address mappings are entered in the Lmhosts file using the

#pre notation, then these names are considered to be pre-loaded into the NetBIOS names cache and are used first to resolve name query, before a NetBIOS subnet broadcast or WINS query are used.

- After checking the local cache, WINS servers are contacted first before the name query is broadcast locally on the client subnet to further attempt resolution of the name.
- Like any static database, the Lmhosts file has its limitations. Because of its static nature, entries must be updated in the Lmhosts file if the name of IP address of a computer is changed as a result of (among other possible reasons) relocation on the network or DHCP lease changes.
- The use of a centrally managed Lmhosts file can reduce much of the manual administration required to propagate new or changed mappings to clients. However, this process is still labor intensive and quickly becomes too complicated to maintain on a growing or fluctuating network.

Managing, Securing, and Troubleshooting Servers and Client Computers

Install and configure server and client computer hardware.

- All hardware to be installed should be listed on the Hardware Compatibility List.
- Installing a new device typically involves three steps:
  - Connecting the device to your computer.
  - Loading the appropriate device drivers for the device.
  - Configuring device properties and settings.
- If the device is Plug and Play, detection usually happens automatically. If it is not Plug and Play compatible, then you will have manually install the device. It may be necessary to insert the Windows 2000 Server CD to complete this process. In some instances, a reboot of the machine will be required to finalize the process.
- You must be logged on as an Administrator or as a member of the Administrators group in order to install a device using the Add/Remove Hardware wizard in Control Panel (shown in Figure 38). If your computer is connected to a network, network policy settings may also prevent you from installing hardware. If an Administrator has already loaded the drivers for a device, you can install the device without Administrator privileges.

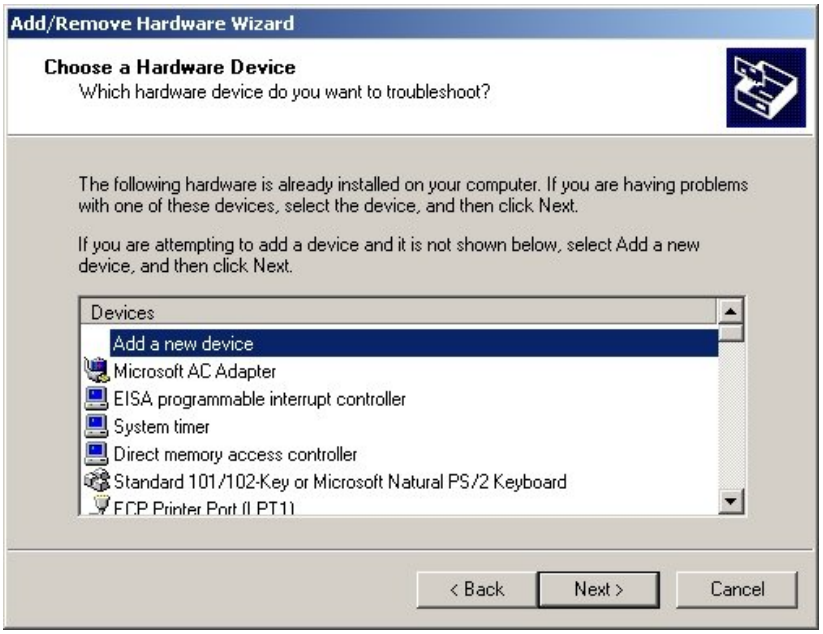

Figure 38 – Manually installing new hardware from the Add/Remove Hardware Wizard.

- If you add and set up a Plug and Play printer, you do not need to have administrative privileges.
- Configuring installed hardware is done from the hardware tree, which is accessed from the **System** applet of Control Panel, **Hardware** tab, **Device Manager** as shown in Figure 39.

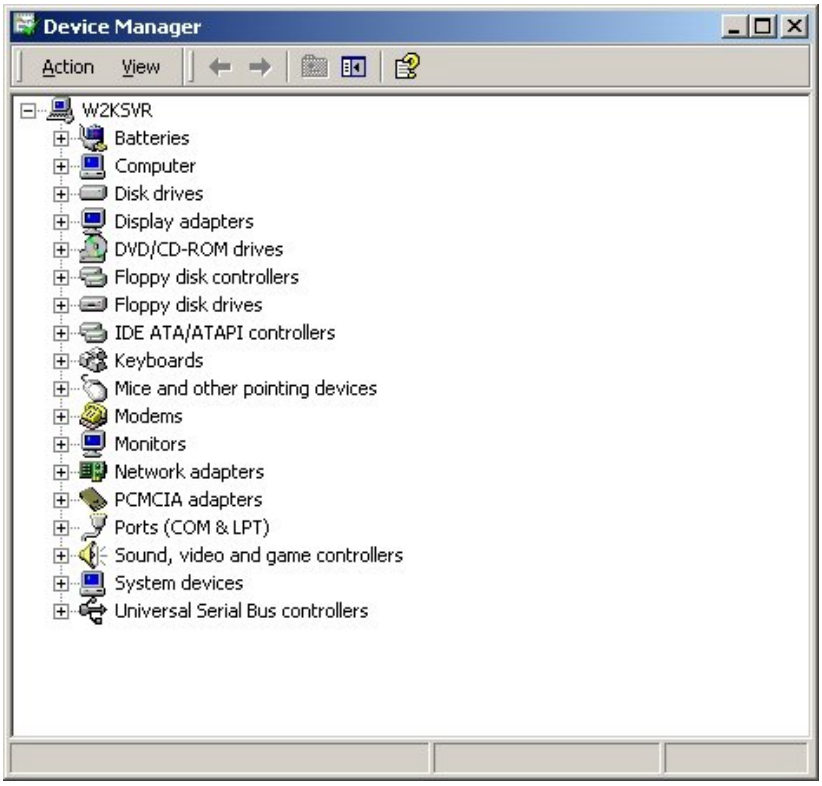

Figure 39 – Device Manager.

- Select a device to configure by opening the node in which it is found. For example, clicking the "+" next to Display adapters would open the node and display all installed display adapters on the machine. Double click on the device you wish to configure and you will get a new window similar to the one shown in Figure 40. Make your changes and close out all windows to implement the changes.

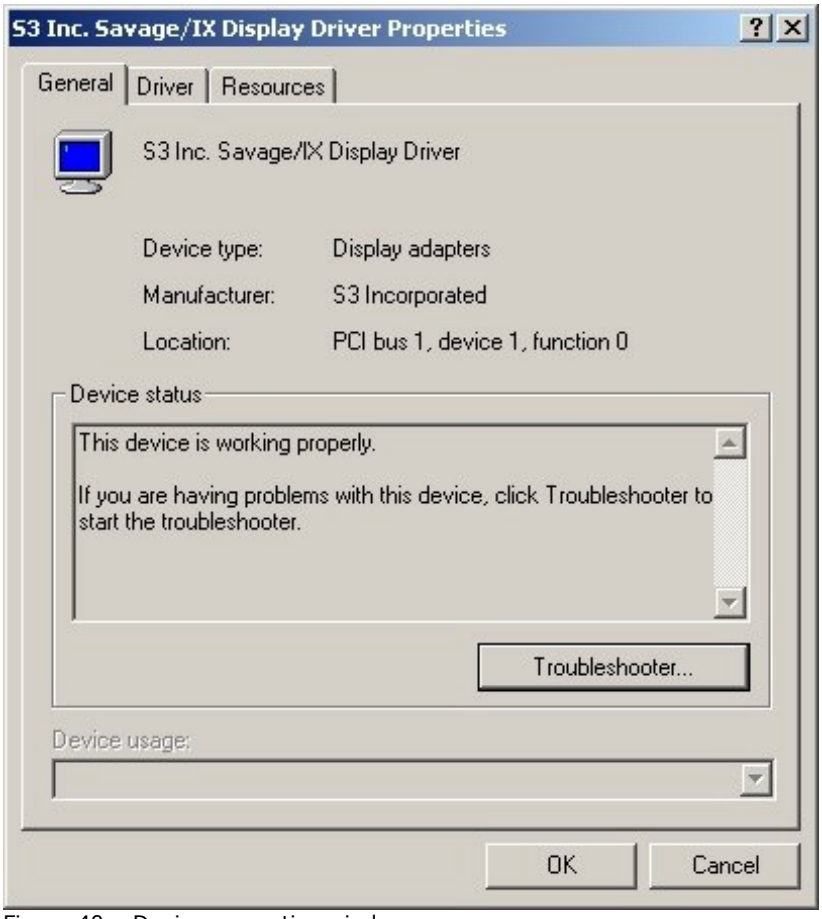

Figure 40 – Device properties window.

- The most common activity required when configuring hardware devices is the updating of drivers. Drivers are updated for any number of reasons, including new and enhanced features, correction of errors, and updates for newer Operating Systems. Driver management is done from the **Driver** tab of a device properties window.
    - From here you can choose to get the **Driver Details**, **Uninstall** the driver or **Update Driver**.
    - Microsoft recommends using Microsoft digitally signed drivers whenever possible (KB# Q244617).
    - The **Driver.cab** cabinet file on the Windows 2000 CD contains all of the drivers the OS ships with. Whenever a driver is updated, W2K looks here first (**c:\winnt\Driver Cache\i386\Driver.cab**). The location of this file is stored in a registry key and can be changed:

HKLM\Microsoft\Software\Windows\CurrentVersion\Setup\DriverCachePath (KB# Q230644).

- The Driver Verifier is used to troubleshoot and isolate driver problems. It must be enabled through changing a Registry setting. The Driver Verifier Manager, **verifier.exe**, provides a command-line interface for working with Driver Verifier (KB# Q244617).

- To prevent poorly written drivers from being installed on a system, Microsoft introduced Driver Signing. Driver signing is managed from the **Hardware** tab of the System applet by clicking **Driver Signing**. This opens a window as shown in Figure 41. Only **Administrators** have the option to apply the setting as a system default. (By default, Windows 2000 is set to **Warn**.)

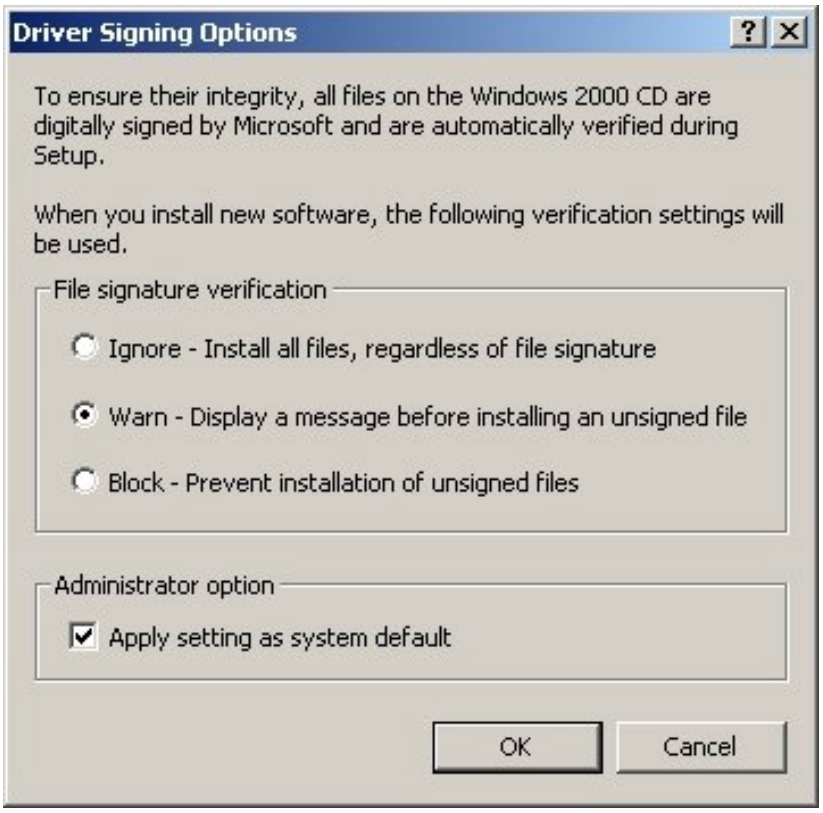

Figure 41 – Managing Driver Signing.

- The System File Checker (**sfc.exe**) (KB# Q222471) is a command line utility that scans and verifies the versions of all protected system files after you restart your computer. If System File Checker discovers that a protected file has been overwritten, it retrieves the correct version of the file from the **%systemroot%\system32\dllcache folder**, and then replaces the incorrect file. It has the following syntax:
    - sfc [/scannow] [/scanonce] [/scanboot] [/cancel] [/quiet] [/enable] [/purgecache] [/cachesize=x]

Parameter	Description
/scannow	Scans all protected system files immediately
/scanonce	Scans all protected system files at next startup
/scanboot	Scans all protected system files at every restart
/cancel	Cancels all pending scans
/enable	Sets Windows File Protection back to defaults
/purgecache	Purges file cache and forces immediate rescan
/cachesize=x	Sets file cache size

- Windows Signature Verification (**sigverif.exe**) (KB# Q259283) is another command line tool that can be used to identify unsigned third party drivers present on a system.
    - Running **sigverif** launches File Signature Verification. By default it only checks system files by default, but non-system files can also be checked as well. The search results are displayed onscreen and can also be saved to **c:\winnt\Sigverif.txt**.
- It is not generally recommend that you change resource settings manually, because when you do so, the settings become fixed, and Windows 2000 will then have less flexibility when allocating resources to other devices. If too many resources become fixed, Windows 2000 may not be able to install new Plug and Play devices.
- Working with multiple CPUs:
    - Adding a processor to your system to improve performance is called scaling. It's typically done for CPU intensive applications such as CAD and graphics rendering.
    - Windows 2000 Professional supports a maximum of two CPUs.
    - Windows 2000 Server supports a maximum of four CPUs. If you need more consider using Windows 2000 Advanced Server (up to 8 CPUs) or Datacenter Server (maximum of 32 CPUs).
    - Windows 2000 supports Symmetric Multiprocessing (SMP). Processor affinity is also supported. 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 (KB# Q234558).
- The Windows 2000 Driver and Hardware Development site discusses how Setup works to install devices.

Troubleshoot starting servers and client computers. Tools and methodologies include Safe Mode, Recovery Console, and parallel installations.

Safe Mode (KB# Q202485)

- Safe Mode exists to help you get a computer started that is starting with errors or perhaps not starting at all. The most common cause of this is bad drivers that are causing system conflicts. Safe Mode starts Windows with only a minimal set of drivers (basic mouse, video, keyboard, monitor and mass storage) to help resolve startup problems.
- By default, no networking drivers are loaded on a Safe Mode startup. Networking drivers can be loaded by using the **Safe Mode with Networking** option.
- In most cases, you will want to try correcting startup problems by using a Safe Mode startup before using the Recovery Console.
- To enter Safe Mode, restart the computer and press F8 when prompted (when you see the "Please Select The Operating System To Start").
- Use Safe Mode to remove a newly installed piece of hardware or software that may be the cause of startup problems. If the problem does not appear on the subsequent normal startup, you have found the problem.
- Choose from one of the following Safe Mode startup options to begin solving the problem:
  - **Safe Mode:** A minimal set of device drivers and services to start Windows.
  - **Safe Mode with Networking:** A minimal set of device drivers and services to start Windows plus the drivers necessary to load networking.
  - **Safe Mode with Command Prompt:** This is the same as Safe mode, with the exception that Cmd.exe is started rather than Windows Explorer.
  - **Enable VGA Mode:** This starts Windows in 640 X 480 mode using the current video driver (not Vga.sys). This mode is useful for cases in which the display was configured at a setting the monitor cannot display.

- **Last Known Good Configuration:** This starts Windows using a previous good configuration.
- **Directory Service Restore Mode:** This mode is valid only for Windows 2000 domain controllers. It performs a directory service repair.
- **Debug Mode:** This option enables debug mode in Windows 2000. Debugging information can be sent across a serial cable to another computer running a debugger. This mode is configured to use COM2.
- **Enable Boot Logging:** When the computer is started with any of the Safe Boot options except Last Known Good Configuration, logging is enabled. The Boot Logging text is recorded in the **Ntbtlog.txt** file in the **%systemroot%** folder.

Recovery Console (KB# Q229716)

- The Recovery Console is a DOS like command line tool that can be used to get a computer started that either will not start at all or is starting with errors.
- By default, you can copy from removable media to hard disk, but not vice versa – console can't be used to copy files to other media (KB# Q240831). As well, by default, the wildcards in the copy command don't work (KB# Q235364). You can't read or list files on any partition except for the system partition.
- Install the Recovery Console by inserting your Windows 2000 CD into the CD drive, change to the I386 folder and run **winnt32 /cmdcons** (KB# Q216417). You will need to be logged in with Local Administrative privileges to install the Recovery Console.
- After it is installed, it can be selected from the "Please Select Operating System to Start" menu.
- When starting Recovery Console, you must log on as the Local Administrator. (KB# Q239803).
- You can also start from the Windows 2000 Setup floppy disks or the Windows 2000 CD. When you get to the "Welcome to Setup" screen, press F10, or press R to repair, and then C to start the Recovery Console.
- While using the Recovery Console, access is limited to the following directories:
  - The root folder
  - The %SystemRoot% folder and the subfolders of the Windows 2000 installation you are currently logged in to
  - The Cmdcons folder
  - Removable media drives such as CD-ROM drives
- If you want to remove the Recovery Console from a computer, follow the following procedure:

- From **Windows Explorer**, click on the **Tools** menu, and then select **Folder Options**. From the **View** tab, select the radio button next to **Show Hidden Files and Folders** and also remove the checkbox next to **Hide Protected Operating System Files**. Click **OK** to close the window.
- From the root directory, delete the **Cmdcons** folder and the **cmldr** file.
- Edit the **Boot.ini** file (also found in the root directory) and remove the line that corresponds with the Recovery Console. Save and close the **Boot.ini** file.
- Restore file and folder viewing back to normal.

- Recovery Console commands:

Command	Description
Attrib	Changes attributes of selected file or folder
cd or chdir	Displays current directory or changes directories
Chkdsk	Run CheckDisk
Cls	Clears screen
Copy	Copies from removable media to system folders on hard disk. No wildcards
del or delete	Deletes service or folder
Dir	Lists contents of selected directory on system partition only
Disable	Disables service or driver
Diskpart	Replaces FDISK – creates/deletes partitions
Enable	Enables service or driver
Exit	Quits the Recovery Console and restarts your computer
Expand	Extracts components from .CAB files
Fixboot	Writes new partition boot sector on system partition
Fixmbr	Writes new MBR for partition boot sector
Format	Formats selected disk
Listsvc	Lists all services on WINXP workstation
Logon	Lets you choose which WINXP installation to logon to if you have more than one
Map	Displays current drive letter mappings
md or mkdir	Creates a directory
more or type	Displays contents of text file
rd or rmdir	Removes a directory
ren or rename	Renames a single file
Set	Allows you to display or modify four environment options: AllowWildCards, AllowAllPaths, AllowRemovableMedia,

	NoCopyPrompt
Systemroot	Makes current directory system root of drive you're logged into

Parallel Installations

- A Parallel Installation is a back door of sorts. It is a secondary installation of the Operating inside a different directory, on a different partition or most preferably, on a separate physical disk. Even on the most fault-tolerant and redundant installations, software corruption is still possible. A Parallel Installation, when performed *ahead* of time, is the best form of recovery when an Operating System installation is completely toasted.
- A Parallel Installation will allow you full control access to your NTFS formatted volumes in the event that disaster strikes and you need access to the files or Registry data contained on the primary installation. In this way, you can seek to repair problems yourself instead of relying on Windows recovery processes to do the work for you.
- A Parallel Installation should include all recovery tools (and system utilities such as network backup software) that you would find on the primary installation, but it should not include all of the services and functionality that the primary installation possesses. For example, if you were to create a Parallel installation on a Member Server that also served as a DNS / DHCP / WINS server, it would be unnecessary to install those additional services as they would simply taking up additional space. Also, it is not always necessary to keep your Parallel Installation updated with the most up to date Service Pack as long as you are comfortable with where it's at and it can perform its duties.

Monitor and troubleshoot server health and performance. Tools include System Monitor, Event Viewer, and Task Manager.

System Monitor

- With System Monitor, you can collect and view real-time data about memory, disk, processor, network, and other activity in graph, histogram, or report form.
- The System Monitor, shown in Figure 42, is accessed from the Performance console, found in Administrative Tools.

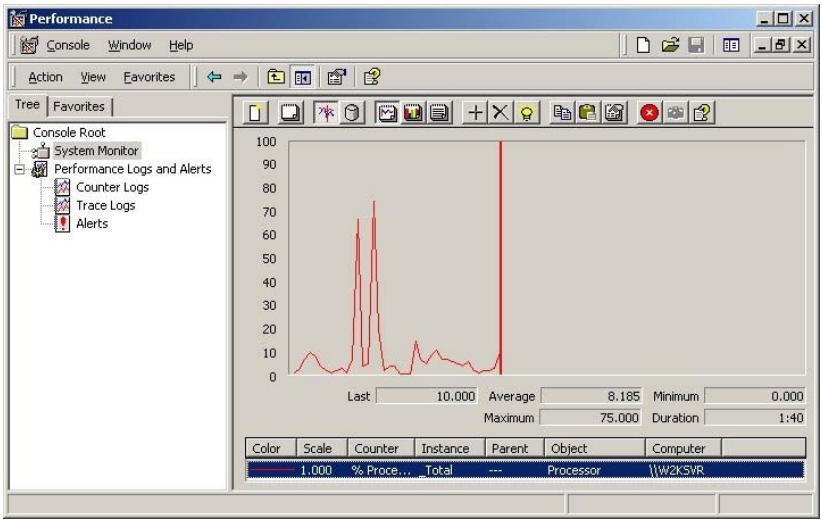

Figure 42 – The System Monitor console.

- To change between views, use the three icons immediately to the left of the add icon (the "+" sign).
- Initially, there are no counters installed in the System Monitor, thus you must add counters by clicking on the large "+" sign on the menu bar above the display area. This will bring up a new window, as shown in Figure 43, from which you can add counters for the local machine or any other machine on the network.
- Select the computer you want to monitor, and then select the category of counter to add from the drop down box and lastly select the counter(s) you wish to add to the System Monitor.

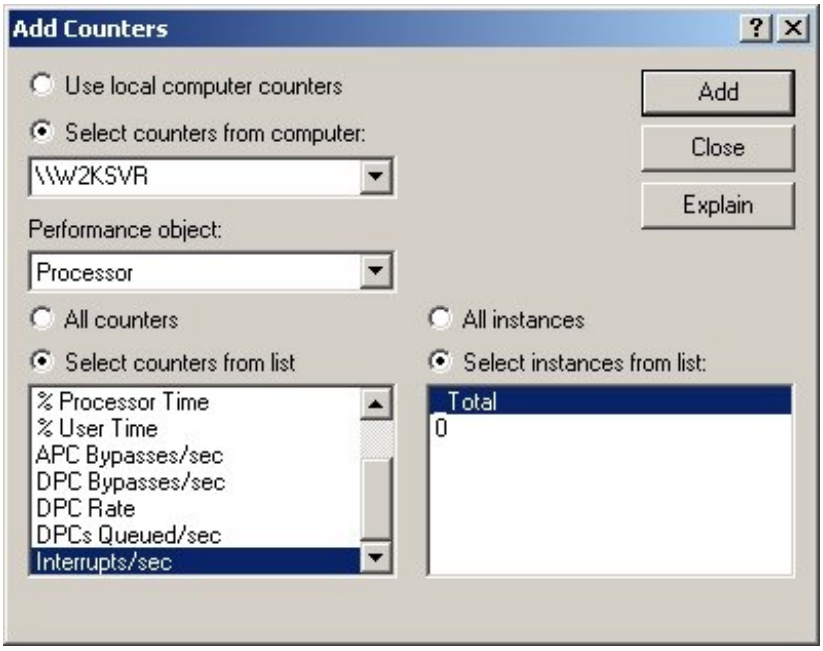

Figure 43 – Adding performance counters.

- Important objects to monitor are *cache* (file system cache used to buffer physical device data), *memory* (physical and virtual/paged memory on system), *physicaldisk* (monitors hard disk as a whole), *logicaldisk* (logical drives, stripe sets and spanned volumes), and *processor* (monitors CPU load). Specific objects to monitor:
  - *Processor - % Processor Time* counter measures time CPU spends executing a non-idle thread. If it is continually at or above 80%, a CPU upgrade is recommended.
  - *Processor - Processor Queue Length* – more than 2 threads in queue indicates CPU is a bottleneck for system performance.
  - *Processor - % CPU DPC Time* (deferred procedure call) measures software interrupts.
  - *Processor - % CPU Interrupts/Sec* measures hardware interrupts. If processor time exceeds 90% and interrupts/time exceeds 15%, check for a poorly written driver (bad drivers can generate excessive interrupts) or upgrade CPU.
  - *Logical disk – Disk Queue Length* – if averaging more than 2, drive access is a bottleneck. Upgrade disk, hard drive controller, or implement stripe set.
  - *Physical disk – Disk Queue Length* – same as above.

- *Physical disk - % Disk Time*- if above 90%, move data/pagefile to another drive or upgrade drive.
- *Physical disk – Split IO/sec* - reports the rate that I/Os (inputs/outputs) to the disk were split into multiple I/Os. A split I/O may result from requesting data in a size that is too large to fit into a single I/O or that (more commonly) the disk is fragmented.
- *Memory – Pages/sec* – more than 20 pages per second is a lot of paging – add more RAM.
- *Memory – Committed bytes* – should be less than amount of RAM in computer.
- *diskperf* command for activating disk counters has been modified in Windows 2000. Physical disk counters are now enabled by default, but you will have to type **diskperf –yv** at a command prompt to enable logical disk counters for logical drives or storage volumes (KB# Q253251).

- A log can also be created (KB# Q248345, Q253264, Q302509) and viewed (KB# Q243423) using System Monitor.

Event Viewer (KB# Q302542, Q300958)

- Using the event logs in Event Viewer (show in Figure 44), you can gather information about hardware, software, and system problems, and you can monitor Windows 2000 security events.
- The EventLog service starts automatically when you start Windows 2000. All users can view application and system logs. Only administrators can gain access to security logs.
- By default, security logging is turned off. You can use Group Policy to enable security logging. The administrator can also set auditing policies in the registry that cause the system to halt when the security log is full.

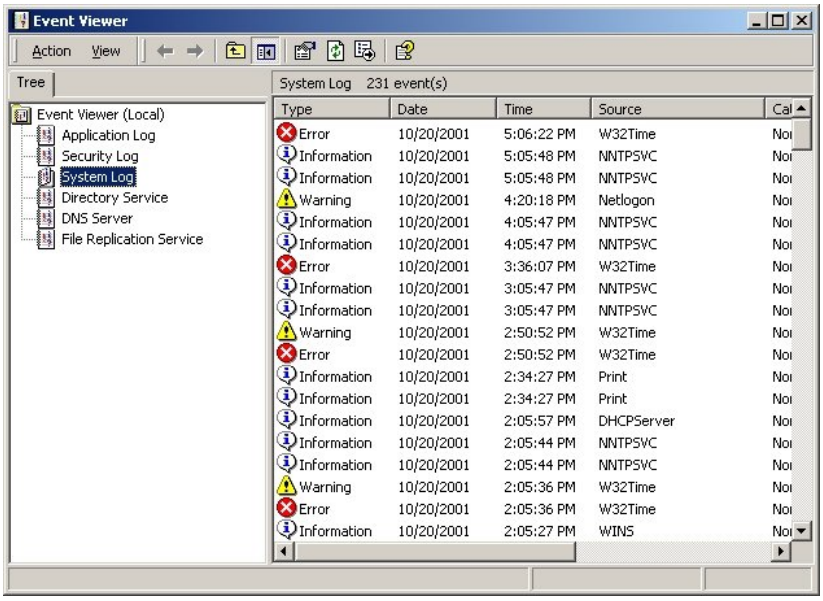

Figure 44 – Event Viewer.

- On a typical Windows 2000 machine, the following logs are created for Event Viewer (there may be others depending on what software the server is running):
  - The **Application Log** contains events logged by applications or programs. For example, a database program might record a file error in the application log. The program developer decides which events to record.
  - The **Security Log** can record security events such as valid and invalid logon attempts as well as events related to resource use such as creating, opening, or deleting files. An administrator can specify what events are recorded in the security log. For example, if you have enabled logon auditing, attempts to log on to the system are recorded in the security log.
  - The **System Log** contains events logged by the Windows 2000 system components. For example, the failure of a driver or other system component to load during startup is recorded in the system log. The event types logged by system components are predetermined by Windows 2000.

- A Domain Controller will have the following additional logs:
  - The **Directory Service** log records events logged by Active Directory and its related services.
  - The **File Replication Service** log records file replication activities on the system.
- A DNS Server will have the following additional log:
  - The **DNS Server** log records DNS queries, responses, and other DNS activities.
- Entries in Event Viewer will be one of the following types:
  - **Error (red circle):** A significant problem, such as loss of data or loss of functionality. For example, if a service fails to load during startup, an error will be logged.
  - **Warning (yellow triangle):** An event that is not necessarily significant, but may indicate a possible future problem. For example, when disk space is low, a warning will be logged.
  - **Information (white bubble):** An event that describes the successful operation of an application, driver, or service. For example, when a network driver loads successfully, an Information event will be logged.
  - **Success Audit (gold key):** An audited security access attempt that succeeds. For example, a user's successful attempt to log on the system will be logged as a Success Audit event.
  - **Failure Audit (gold lock):** An audited security access attempt that fails. For example, if a user tries to access a network drive and fails, the attempt will be logged as a Failure Audit event.

Task Manager (KB# Q243325, Q263201, Q155075)

- Windows Task Manager (shown in Figure 45) provides information about computer performance, and programs and processes running on the computer. Using Windows Task Manager, you can end programs or processes, start programs, and view a dynamic display of your computer's performance.
- To open Windows Task Manager, right-click an empty space on the taskbar, and then click **Task Manager** or select **Task Manager** from the **CTRL-ALT-DEL** menu.
- On computers equipped with two or more CPUs, processor affinity is set from within the Task Manager (Resource Kit, Server Documentation) by using the **Set Affinity** command.

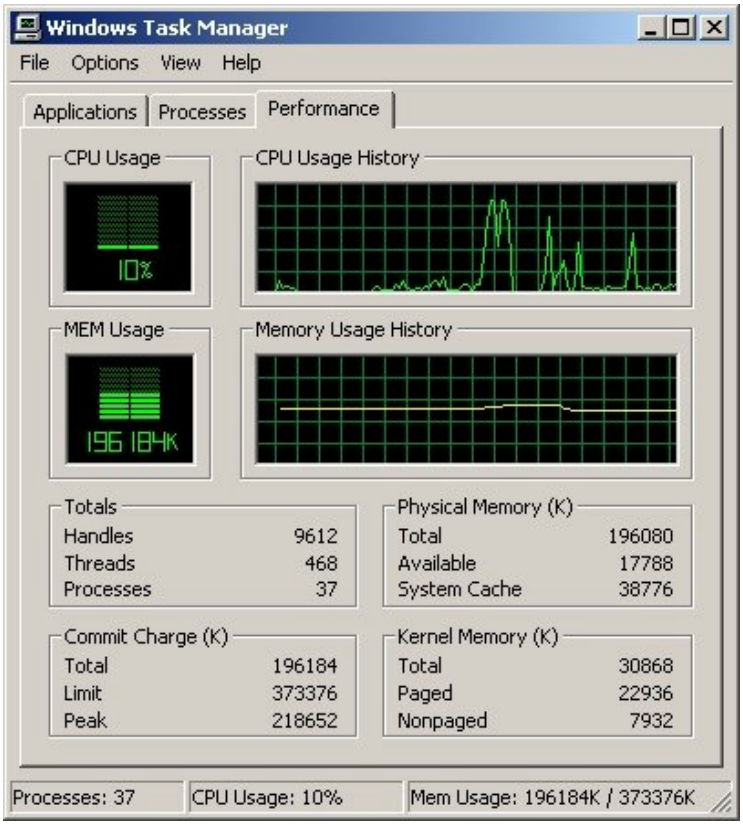

Figure 45 – Task manager in performance view.

Install and manage Windows 2000 updates. Updates include service packs, hot fixes, and security hot fixes.

Service Packs

- Service Packs are regularly scheduled maintenance releases to products that correct problematic issues with them and also occasionally add additional functionality to them.
- Typically, new Service Packs will include all fixes and updates that have been included in the Service Packs that preceded them, but this is not always the case.
- Installation of a Service Pack should always be followed by a reboot of the computer.
- Service Packs can be slipstreamed into new Operating System deployments.

- Service Packs can also be extracted to a file share and assigned to computers via Group Policy (use the update.msi file).
- Service Packs for Microsoft products can be located at the Service Packs home page.

Hot Fixes / Security Hot Fixes

- Hotfixes are small, problem specific executables whose purpose is to correct one specific flaw or security issue in an Operating System or other installed application (such as Internet Information Services or SQL Server). Hotfixes typically result from the discovery of an attack opportunity or weakness in a product. The timely application of a Hotfix is critical to properly secure the system or prevent degraded system performance.
- The Microsoft TechNet Security home page is the starting point for all security alerts and hotfixes.
- The Microsoft Network Security Hotfix Checker (KB# Q303215) provides a small executable file, **Hfnetchk.exe**, that can be used to check the status of required (and therefore, missing) security hot fixes on a computer. (Martin Grasdal has written an excellent article about this.)
- After the file has been installed on a computer, launch it from the command prompt by typing **hfnetchk**. You must be either logged in with Local Administrative privileges, on each machine to be scanned, for best results (KB# Q305385).
- **Hfnetchk** can be used to scan multiple machines on a network either by IP address, network boundaries or domain name.
- **Hfnetchk** will only display *required* hotfixes for the Operating System and additional supported Microsoft products that you have installed. It will not display any recommended or other optional hotfixes. The list of supported products that hfnetchk works for is listed in KB# Q305385.
- **Hfnetchk** will not automatically download or install any of the required hotfixes. Hotfixes will have to be downloaded and installed manually.
- Hotfixes can be chained together for installation on an existing Operating System installation using **Qchain.exe** (KB# Q296861), which allows for multiple hotfixes to be installed sequentially without rebooting the computer in between each Hotfix. Even for hotfixes that do not necessarily require a reboot after installation, chaining hotfixes via **Qchain.exe** will help to alleviate problems because of locked files or other issues.
- Hotfixes can be installed simultaneously with new Operating System deployments (KB# Q249149). The Windows 2000 installation files and Hotfix executables will need to be placed in a common distribution folder. To install the hotfixes during an unattended installation, you can either use the **Cmdline.txt** file (called out via the answer file, see the Resource Kit for more information) or directly via an answer file by putting the hotfixes in the Run

Once section by using Setup Manager Wizard (found at **Support\Tools\Deploy.cab\setupmgr.exe** on the Windows 2000 CD-ROM). If a hotfix requires a reboot of the computer, it should be installed via the Cmdline.txt file vice using the answer file. Figure 46 shows adding commands to the **Setup Manager Wizard** during the creation of an answer file.

- The Cmdline.txt file should look something like the code below. Additional information on **Cmdline.txt** creation is found in the Resource Kit.

```
[Commands]
"command_1"
"command_2"
.
.
"command_x"
```

- The pertinent section of a completed answer file will look like the code below.

```
[GuiRunOnce]
    Command0="Q123456 /q"
```

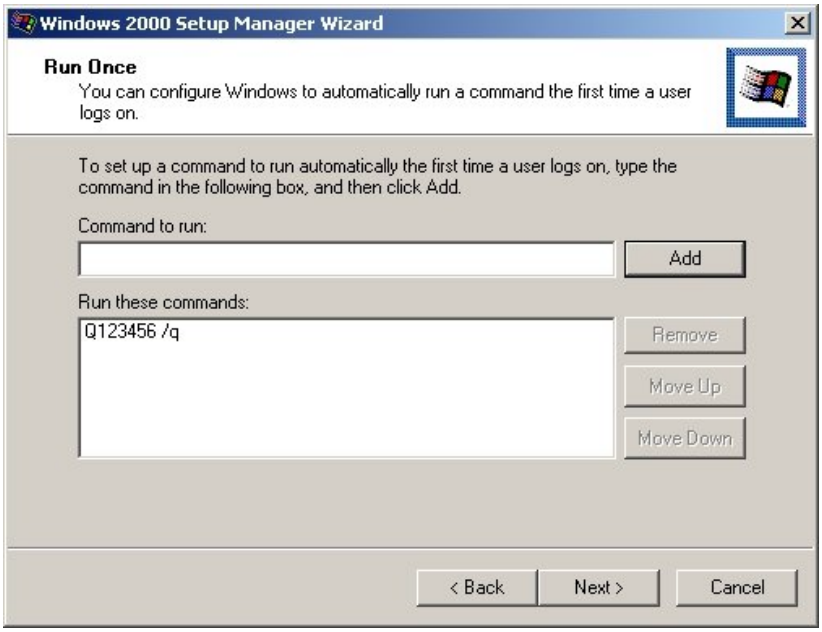

Figure 46 – Adding Run Once commands to an answer file from Setup Manager Wizard.

Windows Update

- The Windows Update site and Windows Update Corporate site provide updates and enhancements to the Windows Operating System.
- The Windows Update site, shown in Figure 47, is most useful when it is only required to update one computer. Local Administrative privileges are required to use Windows Update.
- The Windows Update Corporate site, shown in Figure 48, is useful for organizations where it is desired to update many computers without physically having to travel to each computer. Updates can be downloaded based on the needs of the hardware (this works best if all machines have the same hardware and software configurations) and then distributed by either Active Directory Group Policy Objects or using Systems Management Server 2.0.

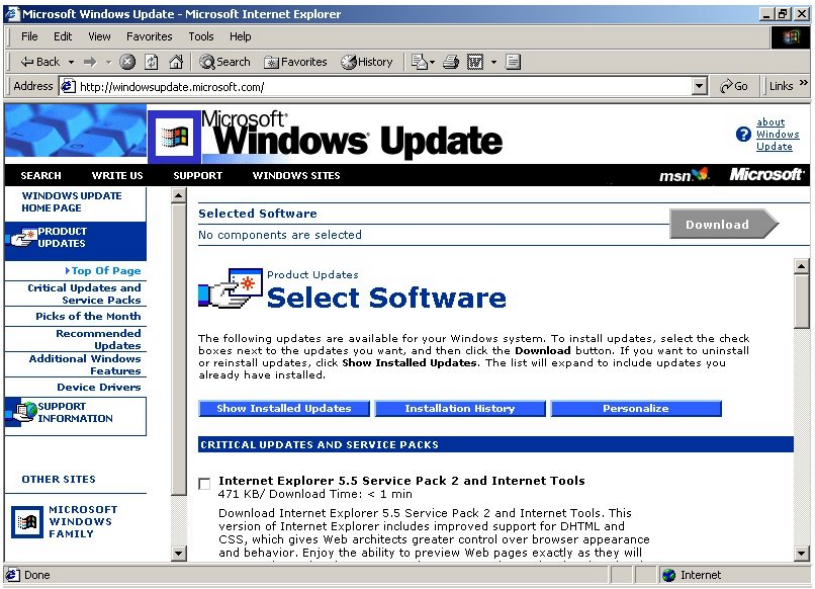

Figure 47 – Using the Windows Update to update a single computer.

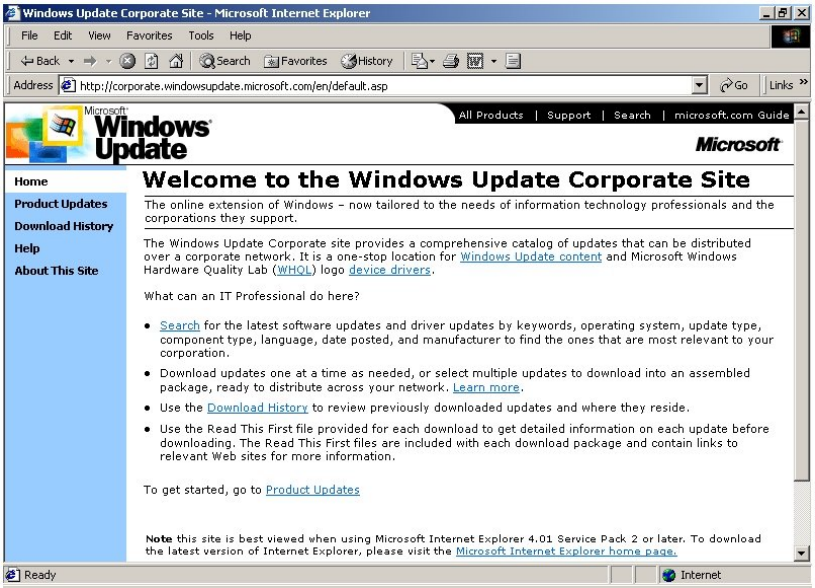

Figure 48 – Using the Windows Update Corporate Site to download updates for distribution.

Configuring, Managing, Securing, and Troubleshooting Active Directory Organizational Units and Group Policy

Create, manage, and troubleshoot User and Group objects in Active Directory.

Creating and configuring user accounts

- User accounts are created from the **Active Directory Users and Computers** console or the **Local Users and Groups** node of the **Computer Management** console, depending on whether or not the machine is participating in an Active Directory environment.
- To add users to a computer you must be in one of the following groups as appropriate for your situation:
  - Non Active Directory workgroup or standalone: **Administrators** or **Power Users**.
  - Active Directory participant: **Account Operators**, **Administrators**, **Domain Admins** or **Enterprise Admins**.
- All user accounts should be created using a predetermined naming convention that applies across your organization. The easiest way to do this is to create a user template, copy it as required and then make the appropriate changes to complete the process. In this way, you can assign the appropriate

permissions to the account (make several template accounts if you have several different groups of access requirements) one time and avoid giving a user too little in the way of permissions or worse yet, giving the user too much permission.

- Some examples of naming conventions for user *Joe Q. User* include:
  - Last name followed by initials: userjq
  - First name, middle initial(s) and last name: joequser
  - First and middle name initials followed by last name: jquser
  - Initials and numbers: jqu998
- To create a new user account, move to the location in the in the console (Organization Unit, etc.) where you wish to locate the new user and right click on it. Select **New > User** and supply the required information (see Figure 49). Clicks **Next** to continue and then set an initial password (highly recommend) and password options. Click **Next** again to review the settings and then click **Finish**.

Figure 49 – Creating a new user account.

- After the user account has been created, it will still require additional configuration (shown in Figure 50) as determined by your organization's directives.

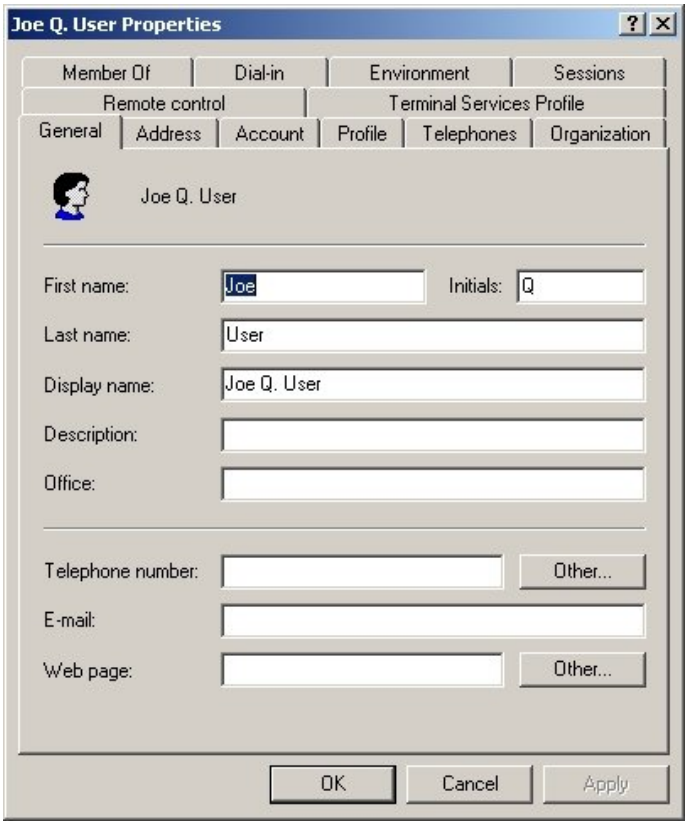

Figure 50 – Configuring user account properties.

- User account creation can be automated via use of the **NETDOM** tool (KB# Q222525).

Creating and configuring computer accounts

- Computer accounts can be created either at the time of joining a computer to the domain (requires appropriate permissions) or ahead of time from the **Active Directory Users and Computers** console.
- To add computers to a domain, you must have **Domain Admin** privileges or be delegated privileges to add computers.
- As with user accounts, naming of computer accounts should also follow an established naming convention that has been established for an entire organization. Some examples for computers located in a Site at Phoenix are given below:
  - PHO_WS4563 for a workstation located in Phoenix
  - PHO_DC1 for a Domain Controller located in Phoenix
  - PHO_RAS3 for a Remote Access Server located in Phoenix

- To create a computer account from the **Active Directory Users and Computers** console, move to the location in the console (Organization Unit, etc.) where you wish to locate the new user and right click on it. Select **New > Computer** and supply the required information (see Figure 51). Click **OK** to complete the procedure.

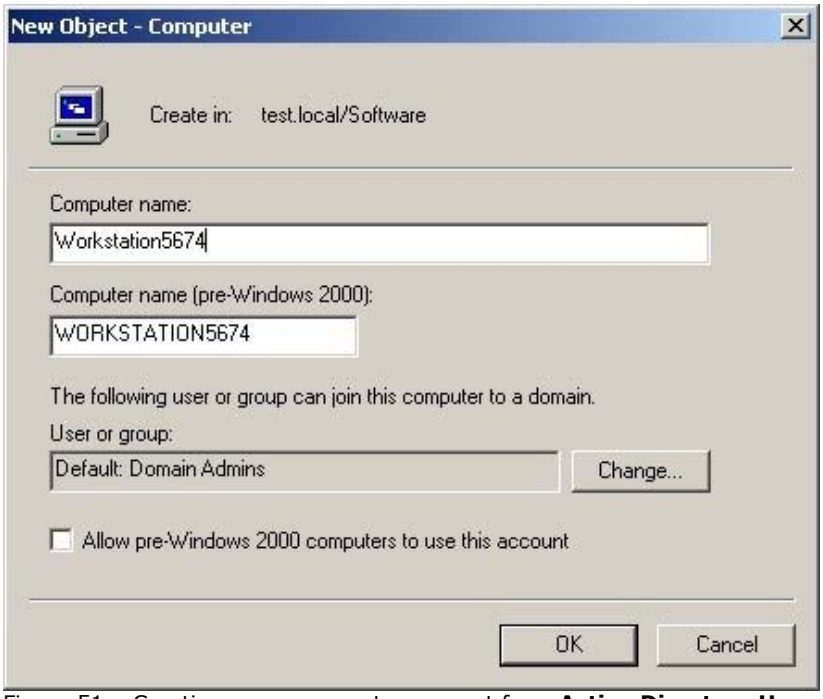

Figure 51 – Creating a new computer account from **Active Directory Users and Computers**.

- After the computer account has been created, it will still require additional configuration (shown in Figure 52) as determined by your organization's directives.

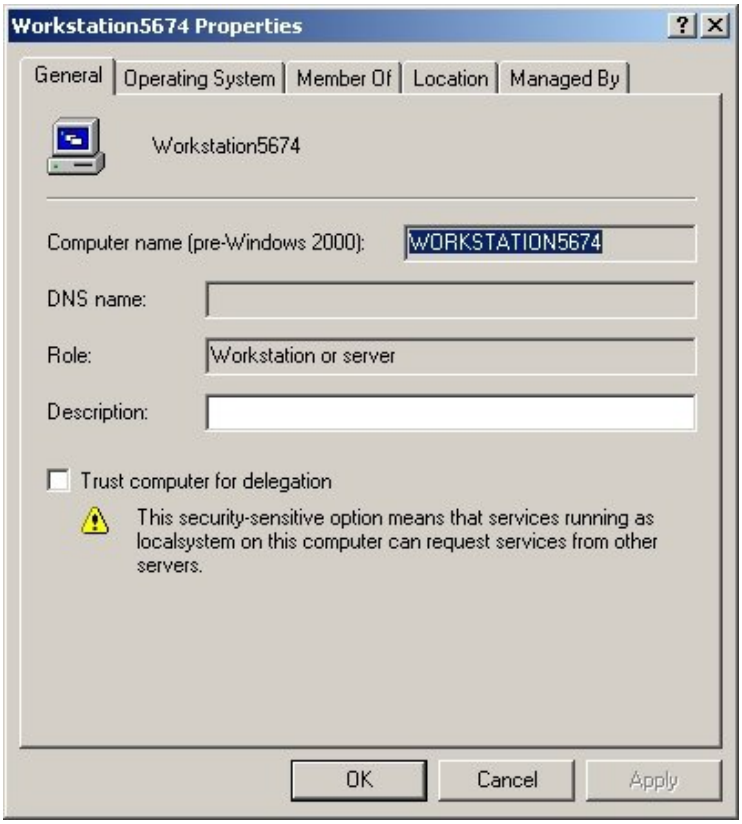

Figure 52 – Configuring computer properties.

- If you want to add the computer account at the time of joining to the domain, you must simply supply the appropriate credentials. You can change the domain / workgroup membership status of computers from the **Network Identification** tab of the **System** applet in the **Control Panel**. Note that Domain Controllers can not be renamed of moved into another domain without first demoting them and removing their Domain Controller functions.
- If the computer is to be a File or Print Server, then most likely you will have no further configuration to perform. A DNS Server, DHCP Server or similar will require those services installed, configured and authorized (as applicable). A computer that is to be a Domain Controller will need to be promoted to that job via the **dcpromo** command. KB# Q216899 provides a checklist for servers that are to be promoted to Domain Controllers.
- Always remember to set the IP address of all Servers manually. Ensure that the address you give it is in the excluded range for the scope you are assigning it from. This rule also applies to other network devices such as routers and printers.

Troubleshoot groups. Considerations include nesting, scope, and type.

Group Types

- Groups are Active Directory or local computer objects that can contain users, contacts, computers, and other groups. Use groups to:
  - Manage user and computer access to shared resources such as Active Directory objects and their properties, network shares, files, directories, printer queues, and so on.
  - Filter Group Policy settings.
  - Create e-mail distribution lists.
- There are two kinds of groups:
  - **Security groups** are used to collect users, computers and other groups into manageable units. When assigning permissions for resources (file shares, printers, and so on), administrators should assign those permissions to a security group rather than to individual users. The permissions are assigned once to the group, instead of several times to each individual user. Each account added to a group receives the rights and permissions defined for that group. Working with groups instead of with individual users helps simplify network maintenance and administration.
  - **Distribution groups** are not security-enabled. They cannot be listed in DACLs. They cannot be used to filter Group Policy settings. Distribution groups can be used only with e-mail applications (such as Exchange), to send e-mail to collections of users. If you do not need a group for security purposes, create a distribution group instead of a security group.
- Although a contact can be added to a security group as well as to a distribution group, contacts cannot be assigned rights and permissions. Contacts in a group can be sent e-mail.
- A group can be converted from a security group to a distribution group, and vice versa, at any time, but only if the domain is in native-mode. No groups can be converted while a domain is in mixed-mode.

Group Scopes

- Each security and distribution group has a scope that identifies the extent to which the group is applied in the domain tree or forest. There are three different scopes: universal, global, and domain local.
  - Groups with **universal scope** can have as their members groups and accounts from any Windows 2000 domain in the domain tree or forest

and can be granted permissions in any domain in the domain tree or forest. Groups with universal scope are referred to as **universal groups**.
    - Groups with **global scope** can have as their members groups and accounts only from the domain in which the group is defined and can be granted permissions in any domain in the forest. Groups with a global scope are referred to as **global groups**.
    - Groups with **domain local scope** can have as their members groups and accounts from a Windows 2000 or Windows NT domain and can be used to grant permissions only within a domain. Groups with a domain local scope are referred to as **domain local groups**.
- If you have multiple forests, users defined in only one forest cannot be placed into groups defined in another forest, and groups defined in only one forest cannot be assigned permissions in another forest.
- When creating a new group, by default, the new group is configured as a security group with global scope regardless of the current domain mode. Although changing a group scope is not allowed in mixed-mode domains, the following conversions are allowed in native-mode domains:
    - **Global** to **universal**. However, this is only allowed if the group is not a member of another group having global scope.
    - **Domain local** to **universal**. However, the group being converted cannot have as its member another group having domain local scope.

Nesting Groups (KB# Q268277, Q231273)

- Using nesting, you can add a group as a member of another group. You can nest groups to consolidate group management by increasing the affected member accounts and to reduce replication traffic caused by replication of group membership changes.
- Your nesting options depend on whether the domain is in native mode or mixed-mode. Groups in native-mode domains or distribution groups in mixed-mode domains have their membership determined as follows:
    - Groups with **universal scope** can have as their members: accounts, computer accounts, other groups with universal scope, and groups with global scope from any domain.
    - Groups with **global scope** can have as their members: accounts from the same domain and other groups with global scope from the same domain.
    - Groups with **domain local scope** can have as their members: accounts, groups with universal scope, and groups with global scope, all from any domain. They can also have as members other groups with domain local scope from within the same domain.

- Security groups in a mixed-mode domain are restricted to the following types of membership:
  - Groups with global scope can have as their members only accounts.
  - Groups with domain local scope can have as their members other groups with global scope and accounts.
- Security groups with universal scope cannot be created in mixed-mode domains because universal scope is supported only in Windows 2000 native-mode domains.
- The effect of domain modes is summarized in the table below:

	Native-mode domains	**Mixed-mode domains**
Universal Groups	Both security and distribution groups can have universal scope.	Only distribution groups can have universal scope.
Nesting	Full group nesting is allowed.	For security groups, group nesting is limited to groups with domain local scope having as their members groups with global scope (Windows NT 4.0 rule). Full group nesting is allowed for distribution groups.
Conversions	Groups can be converted freely between security groups and distribution groups. Groups having global or domain local scope can be converted to groups with universal scope.	No group conversions are allowed.

Manage object and container permissions (KB# Q218596, Q178170, Q221241, Q220167)

- As with all things in Windows 2000, you can manage object and container permissions on an extremely granular level. This allows Administrators to exercise great control over what users can and cannot do.
- To set object and container permissions, you will need to be logged onto a Domain Controller with Domain Admin privileges. The procedure to get started is given below:
  - From the **Active Directory Users and Computers** console, click the **View** menu and then select **Advanced Features** (neglecting to turn this on will prevent you from viewing the Security tab).
  - In the Active Directory tree view, find the specific object that you want to configure access control permissions for (I will use the "Software" Organizational Unit in my domain in this example). Right-click on the object or container and select **Properties**.

- In the **Properties** window, select the **Security** tab and then click **Advanced** to begin some very granular configuration. Click **View/Edit** to edit an existing entry or **Add** to create a new entry (you will have to supply groups, users or computers if you **Add**).
- From here, you have two tabs to choose from (and further complicate the situation) as shown in Figure 53. The **Object** tab deals with access permissions to objects on the network. The **Properties** tab deals with properties pertaining to the object or user.

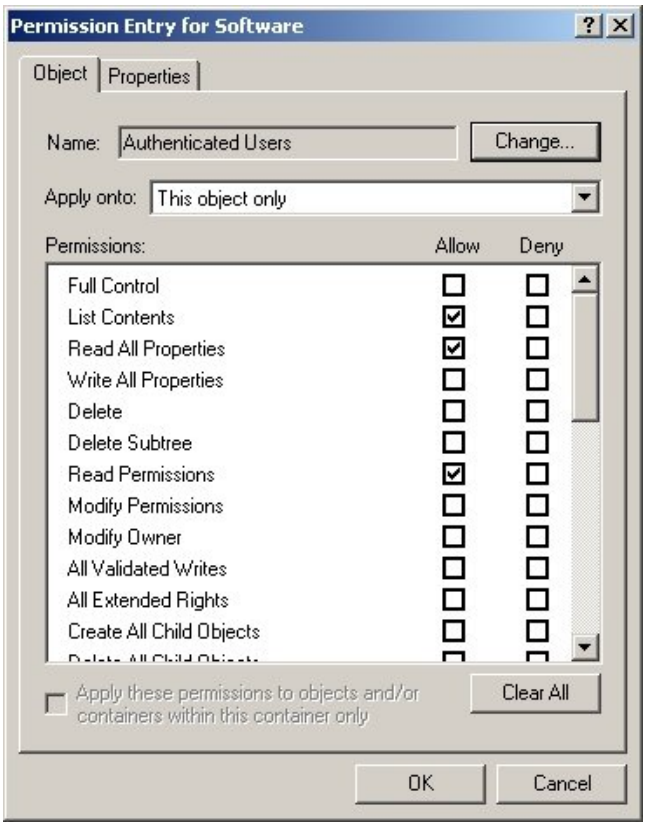

Figure 53 – Configuring permissions on an Object or Container.

Diagnose Active Directory replication problems (KB# Q244368, Q228866)

Understanding Active Directory Replication

- Active Directory is perhaps the single greatest improvement in Windows 2000 over previous versions of Windows NT. Active Directory provides the following new features in Windows 2000 that have not been seen prior:
  - Simplified user and network-resource management
  - Group Policy
  - Flexible, secure authentication and authorization
  - Directory consolidation
  - Directory-enabled applications and infrastructure
  - Scalability without complexity
  - Use of Internet standards
  - A powerful development environment
- Of course, even the best directory service would be useless if users and services can not readily access the directory information at any time from any computer in the forest. In order to make this possible, additions, modifications and deletions of any directory data must be relayed to other Domain Controllers in a timely and cost effective manner. The process of relaying this information is known as replication and it provides the following critical features to the network:
  - Improved information availability
  - Fault tolerance
  - Load balancing
  - Performance improvement
- Windows 2000 Active Directory uses a multimaster replication system, which enables updates to the directory to be made from any Domain Controller rather than from a single Primary Domain Controller (PDC), as in Windows NT 4.0. This new multimaster system directly contributes to the four critical features mentioned earlier, since, with multiple Domain Controllers, replication will continue even if a single (or several) Domain Controllers cease to function.
- Although Windows 2000 Active Directory uses multimaster replication, which allows changes to be made at any Domain Controller, there is really only one copy of the Active Directory database. Changes are simply replicated from the Domain Controller that originally received the changes to all Domain Controllers in the domain (or site); so all Domain Controllers have the same, current directory information. To this end, only changed directory information will be replicated, thus improving replication speed and reducing network loading.

- As with any system that can accept changes from more than one location, there is the possibility for changes to occur from multiple Domain Controllers that affect the same object at the same time. Active Directory has been designed to take this into account and has processes in place to solve conflicts between Domain Controllers during replication, and does this automatically in nearly all cases.

Diagnosing and Troubleshooting Active Directory Replication Problems

- There are two means by which Active Directory is replicated amongst Domain Controllers. RPC over IP and SMTP. They each have their specific use and are further explained below. It is important to understand that different errors and troubleshooting procedures will be required for each of the two different replication methods.
    - **SMTP replication** is only used for replication over site links (inter-site), and not for replication within a site (intra-site). Because SMTP is asynchronous, it typically ignores all schedules. SMTP replication is most often used where the WAN connectively is in doubt and using IP replication may lead to problems with lost or delayed data. SMTP replication requires the use of a Certificate Authority, as well, in order to validate the authenticity of the data being received.
    - **IP replication** uses remote procedure calls (RPC) for replication over site links (inter-site) and within a site (intra-site). Inter-site IP replication, by default, does adhere to replication schedules, although you may configure Active Directory replication to ignore schedules. IP replication does not require the use of a Certificate Authority as all Domain Controllers are on the same, connected, network and can validate each other via Kerberos.
- There are two tools available for diagnosing and troubleshooting IP replication. They are the Active Directory Replication Monitor (**Replmon.exe**) and **Repadmin.exe**. These two tools are briefed explained below.
- Active Directory Replication Monitor, **Replmon.exe** (KB# Q301423, Q290149, Q297230) is a graphical tool that you can use to view low-level status and performance of replication between Active Directory domain controllers. Active Directory Replication Monitor must be installed on a computer that is running Windows 2000 Professional or Windows 2000 Server. The computer can be a domain controller, member server, member workstation, or stand-alone computer. In addition, **Replmon** can be used to monitor domain controllers from different forests simultaneously. Some of the features of Replmon are:
    - Displays servers with which the computer is replicating both directly and transitively.

  - For direct replication partners, displays each USN value, number of failed attempts, reasons, and flags used for each partner.
  - Displays a graphical view of the intra-site topology and, by using the context menu for a specific domain controller in the view, allows the administrator to quickly display the properties of the server and any inter-site connections that exist for that server.
  - Allows an administrator to display how remote domain controllers are configured (for example, whether they have the PDC emulator role).
  - Generates reports that can aid in technical support calls. Allows the administrator to generate a status report for the monitored server, which includes a listing of the directory partitions for the server, the status of each replication partners (direct and transitive) for each of the directory partitions, the status of any Group Policy objects, the domain controllers that hold the FSMO roles, a snapshot of the performance counters on the computer, and the registry configuration of the server (including parameters for the KCC, Active Directory, Jet, and LDAP).
- **Repadmin.exe** (KB# Q301423, Q229896) is a command-line tool that lets you view and change replication status on domain controllers when you need to diagnose and troubleshoot replication between Windows 2000–based domain controllers. You can use **Repadmin** to view the current replication topology, manually create the replication topology, and force replication events.
- Troubleshooting SMTP replication is an entirely separate and complicated game in and of itself. The Resource Kit goes into great detail about troubleshooting SMTP replication, and is summarized briefly here.
  - Check the event log for relevant messages.
  - Verify that the KCC setup is on SMTP-based connections between the servers in the sites you want.
  - Verify that the replication links are established by using the correct transport.
  - Each server is configured to receive mail. The IIS must have been installed on both servers.
  - Communication between sites is by definition between bridgehead servers. The KCC chooses the bridgehead for each site unless they are set explicitly. Verify that if you are using explicit bridgeheads, that they hold the domain you are trying to replicate.
  - Determine whether mail-based replication is succeeding or not by checking the display from **repadmin /showreps**. This shows the current error code and the last success time.
  - A certificate authority must be installed in your enterprise on one of the domain controllers and must be an Enterprise Certificate Authority.

- Additional replication troubleshooting and help can be found in these Knowledge Base articles (KB# Q257187, Q232072, Q232538, Q262561, Q257844).

Deploy software by using Group Policy. Types of software include user applications, anti-virus software, line-of-business applications, and software updates.

Introduction to Group Policy

- Group policies are collections of computer and user configuration settings that are linked to domains, sites, computers, and organizational units. They are not linked directly to groups but are used extensively with OUs. GPOs (Group Policy Objects) can contain Software Settings, Windows Settings, and Administrative Templates:
  - **Software Settings** contains only information on software installation settings by default.
  - **Windows Settings** holds scripts and security settings (used for both computer configuration and user configuration).
  - **Windows Settings** also hold settings for RIS, Internet Explorer (IE) Maintenance, and folder redirection (used for user configuration only).
  - **Administrative Templates** hold all registry-based group policy settings for Windows Components, System, and Network.
  - **Windows Components** include NetMeeting, IE, Windows Explorer, MMC, Task Scheduler, and Windows Installer.
  - **System** controls logon and logoff functions.
  - **Network** controls settings for Offline Files, Network, and Dial-up Connections.
- **Computer configuration** settings *apply group policies to computers, regardless of* what user logs on to them. These settings are applied when Windows initializes.
- **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 are removed when the user logs off.

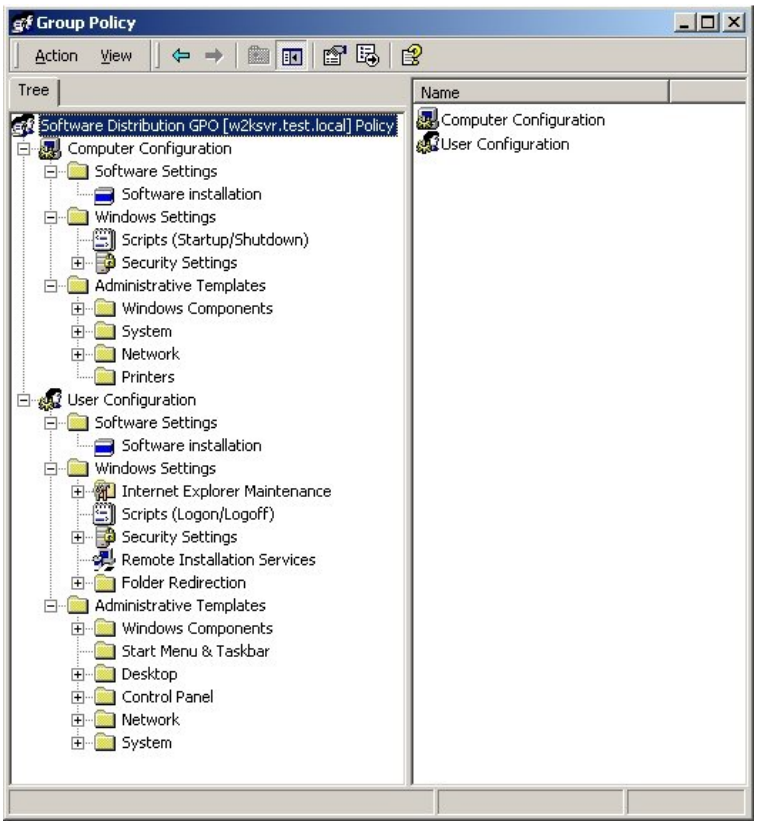

Figure 54 – Options available for configuration via Group Policy.

- The more GPOs you apply, the longer it takes to startup and/or logon to a system. GPOs are handy, but don't go completely nuts with them.

Creating a Group Policy Object (GPO):

- Each W2K computer can have one local GPO. These 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.
- Local GPOs are opened/created using the Group Policy snap-in for the MMC. Make sure that Local Computer appears in the Group Policy Object box.
- The Local Users and Group snap-in is disabled on DCs.
- Site GPOs are opened/created using **Administrative Tools** > **AD Sites & Services** > ***site_name*** (right-click) > **Properties** > **Group Policy** tab.

- Domain/OU GPOs are opened/created using **Administrative Tools** > **AD Users & Computers** > ***domain or OU*** (right-click) > **Properties** > **Group Policy** tab.

Linking to an existing Group Policy Object

- To link a GPO to an existing domain or OU, use **Administrative Tools** > **AD Users & Computers** > ***domain or OU*** (right-click) > **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 & Services** > ***domain or OU*** (right-click) > **Properties** > **Group Policy** tab. Click **Add** then choose the policy and click **OK**.

Delegating administrative control of Group Policy

- Allows you to specify which groups of Administrators have access permissions to the GPO. 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

- Steps to follow to delegate control:
  - Open the GPO's Group Policy snap-in
  - Right-click the root node of the console and select **Properties**
  - Click the **Security** tab
  - Choose the security group you wish to edit
- Write access is required to open and view the Group Policy snap-in and see the settings it contains.

Modify Group Policy inheritance (KB# Q231903, Q221241)

- Group policy settings are processed (inherited) in the following order:
  - *Local GPO* – there can be only one local GPO and it is processed first.
  - *Site GPOs* – these are processed next – administrator can specify the order they are processed in. Overwrites local.

  - *Domain GPOs* – multiple GPOs are processed synchronously in the order specified by the administrator. Overwrites site and local.
  - *OU GPOs* – GPOs linked to the OU highest in AD are processed first followed by GPOs linked to any child OUs. 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 processing (inheritance) order:
  - *Block inheritance* – 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. Block inheritance cannot be applied to GPOs or GPO links.
  - *No override* – any GPO linked to a site, domain or OU can be set to no override so that none of its policies will be overridden by a child container it is linked to.
  - *Loopback setting* – only used in closely managed environments like kiosks, labs, classrooms and reception areas. Can only be set to merge or replace modes.

Filter Group Policy settings by associating security groups to GPOs (KB# Q221930, Q273857)

- Setting permissions for security groups allows an administrator to filter group policy so that it only applies to the users and computers specified.
- Removing GPO Links vs. Deleting GPOs:
  - When a GPO link is removed, the GPO remains in AD until it is deleted, but it is no longer applied.
  - Deleting a GPO removes it from any sites, domains or OUs it was linked to. You can simply remove the GPO link if you no longer want it applied and it remains in AD so that you can modify it or use it again in the future.

Deploying software by using Group Policy (KB# Q240790)

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

Maintaining software by using Group Policy

- A software package is installed on a Windows 2000 system or in a shared directory. A Group Policy Object (GPO) is created. Behavior filters are set in the GPO to determine who gets the software. Then the package is added to the GPO under **User Configuration > Software Settings > Software Installation** (this is done on the server). You are prompted for a publishing method – choose it and say OK.
- Set up Application Categories in **Group Policy > *computer or user config* > 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. Windows does not ship with any categories by default.
- When upgrading deployed software, 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 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 the software.
- 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-clicks 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.

- The software settings of a Group Policy are not refreshed like the rest of the settings. The user may need to logoff/logon or the system may need to be restarted for the new settings to take place (depending on type of software installation).
- 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.
- Figures 55 and 56 show distribution of software via a GPO to a Computer and to Users.

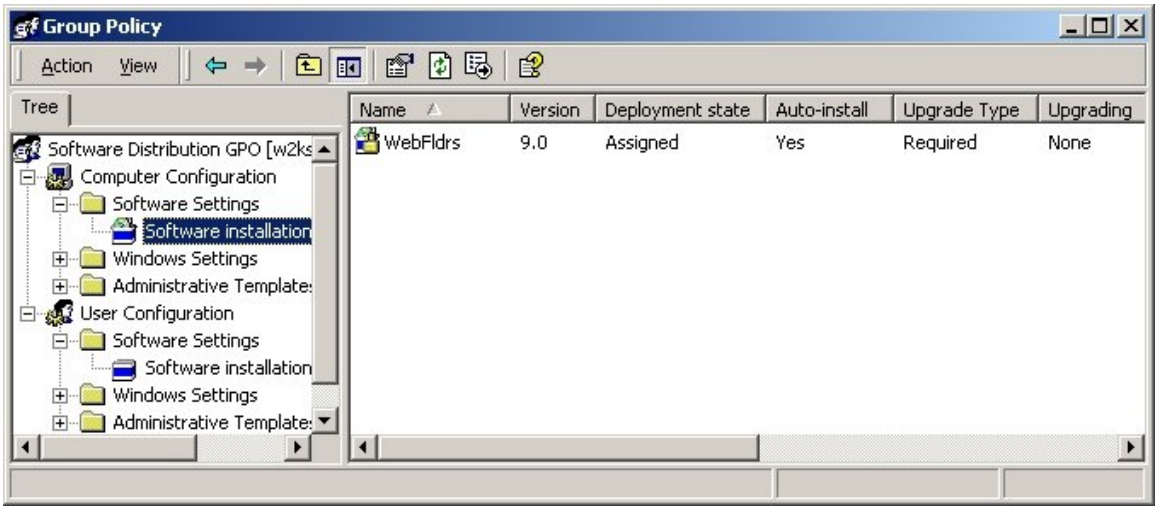

Figure 55 – Assigning software to a computer via a Group Policy Object.

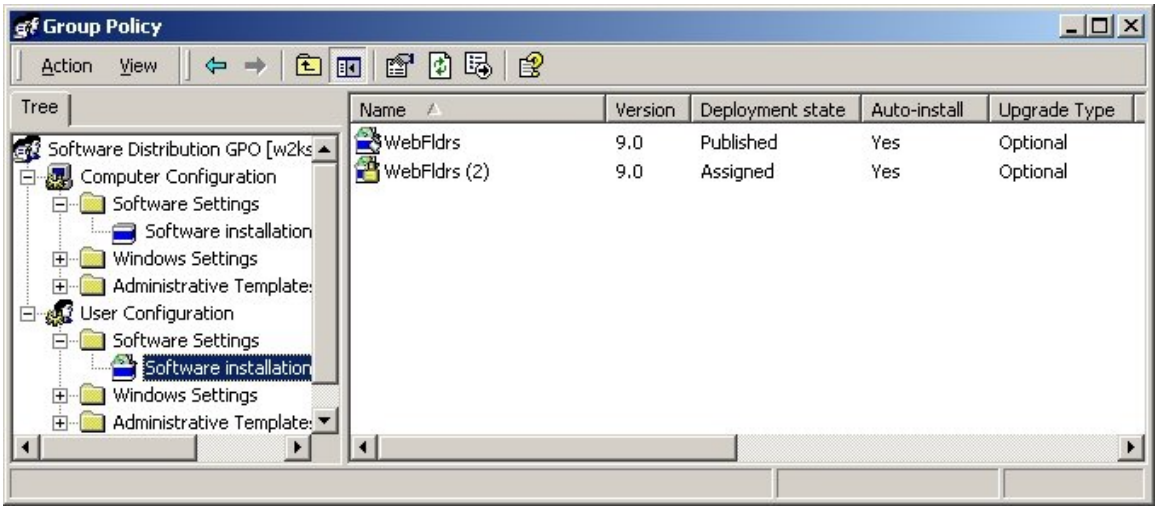

Figure 56 – Publishing and Assigning software to a user via a Group Policy Object.

- 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 invoked (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. (KB# Q231747) .ZAP files can only be published, not assigned.
- Non-MSI programs can be repackaged using a 3rd party tool called WinINSTALL by Veritas software. There is a lite version of this software that was included on the Windows 2000 product CDs that you can use. It lets you take a snapshot of a system, install your application, take another snapshot and create a difference file that becomes your MSI install package. If you wish to assign a non-MSI program to a user or computer, you must first repackage it as an MSI file (KB# Q236573).
- 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*]"** (KB# Q223393).
- 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 (KB# Q236943).
- Patches are deployed as .MSP files (KB# Q226936).

Troubleshoot end-user Group Policy

Troubleshooting Group Policy application (KB# Q250842)

- When troubleshooting Group Policy problems, always consider the dependency between components. For example, a problem with Software Installation would be looked at as follows: Software Installation relies on Group Policy to function, and Group Policy relies on the Active Directory. Active Directory relies on the proper configuration of various network services. When attempting to solve a problem with one component, always make a point to check the components and services on which it relies to ensure that they are not the root cause of the problem at hand. The Event Viewer will often contain clues to solving these type of problems with hierarchical dependencies.
- Always remember the order of Group Policy processing: Local, Site, Domain, Organizational Unit. Applying the correct GPO at the correct level can solve a large number of problems.
- Group Policies should only be created for one specific reason, such as security or perhaps software distribution and then named appropriately. This will help in applying them correctly and also in subsequent troubleshooting efforts when trying to figure out what GPO does what.
- If a GPO is not being applied as it should be, the following are items to investigate:
    - Make sure that the intended policy is not being blocked. Make sure no overriding policy set at a higher level of Active Directory has been set to **No Override**. If **Block** and **No Override** are both used, keep in mind that **No Override** takes precedence.
    - Verify that the user or computer is not a member of any security group for which the Apply Group Policy Access Control Entry is set to **Deny**.
    - Verify that the user or computer is a member of at least one security group for which the Apply Group Policy Access Control Entry is set to **Allow**.
    - Verify that the user or computer is a member of at least one security group for which the Read Access Control Entry is set to **Allow**.
    - Verify that the GPO is linked to an Organizational Unit only, not an Active Directory container. (An OU will have the icon with the "phone book" on it whereas a container will not.) If you want to have a GPO apply to a container, place the contained inside of an OU. The GPO will then be applied to all objects via inheritance.
    - If the GPO that is not taking effect is the local one, remember that local GPOs have the lowest priority. Check that a higher level GPO is not in conflict with the local GPO.

Troubleshooting software distribution via Group Policy

- If a Published application does not appear in the Add/Remove Programs window, investigate and troubleshoot the following items as required:
  - Group Policy was not applied.
  - Active Directory cannot be accessed.
  - User does not have any published applications in the Group Policy objects that apply to them.
  - Client is running Terminal Server (software installation is not supported for Terminal Services clients).
- If document invocation for published applications is not working properly, check to ensure that **Auto-Install** (from the **Deployment** tab of the GPO) is set for that file extension.
- If the error message "The feature you are tying to install is cannot be found in the source directory" is received, check the network condition and also permissions on the share where the distribution folder is located.
- If after removing an application, the shortcuts still appear on the user's desktop, then you must manually delete them. This occurs when the user installs an application and thus the Windows Installer is not aware of them.
- If the error message "Active Directory will not allow the package to be deployed" or "Cannot prepare package for deployment" is received, check the network status and determine if the package has been corrupted. Corrupt installation packages must be replaced before they will operate properly.

Implement and manage security policies by using Group Policy

Implement security policies via Group Policy

- Security policies can be applied via Group Policy easily across an entire organization or major part of an organization. There are two basic ways to go about implementing security policies: creating your own GPO from scratch or importing of the supplied **.INF** templates that ship with Windows 2000.
- Implementing security policy from scratch via GPO is done by using the **Group Policy** snap-in and setting options as desired in the following two locations:
  - Computer Configuration > Windows Settings > Security Settings
  - User Configuration > Windows Settings > Security Settings
- Implementing security policy by using the pre-defined templates is done from the following locations depending on the situation at hand:
  - **Local Security Policy** snap-in, for a stand-alone server.
  - **Domain Security Policy** snap-in, to apply the settings to the entire domain.

  - **Domain Controller Security Policy** snap-in, to apply the settings to Domain Controllers in the domain.
  - **Group Policy** snap-in, to apply the settings to a specific GPO.
- To implement policy by importing a template, right click on **Security Settings** and click on **Import Policy…** as shown in Figure 57.

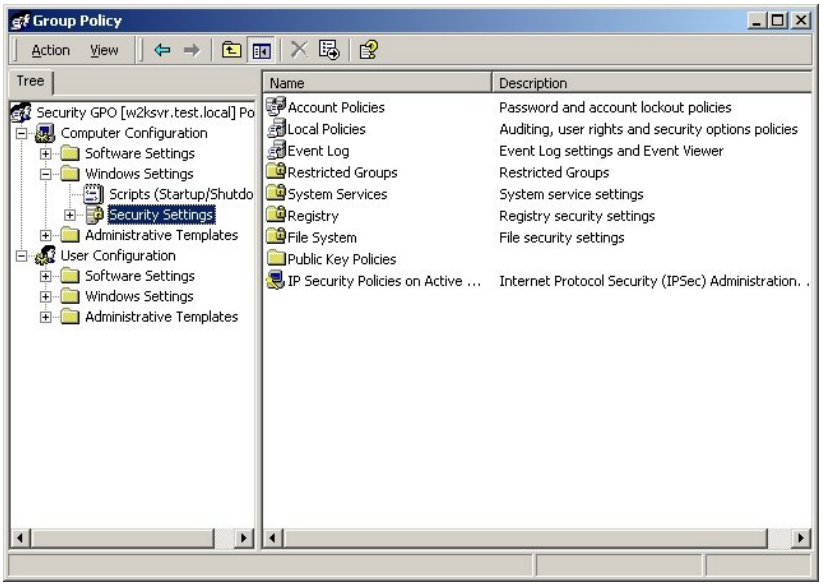

Figure 57 – Starting the process to import a security template.

- In regards to security templates, keep these two items in mind:
  - They should only be applied to Windows 2000 systems that have been clean installed onto an NTFS partition. For NTFS computers that have been upgraded from NT4 or earlier, only the Basic security templates can be applied.
  - Security templates are imported/exported using **.INF** files. The Group Policy snap-in can be focused on a local or remote system.

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

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

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

Analyzing security after application (KB# Q258595)

- The Security Configuration and Analysis snap-in can be used to determine the net effect of applied security policies versus the pre-defined template.
- To start the snap-in, open an empty MMC console by typing mmc from the RUN line. When the empty console opens, click **Console** > **Add/Remove snap-in** > **Add** to bring up the windows as shown in Figure 58. Select **Security Configuration and Analysis** and click **Add** > **Close** > **OK** to finalize the process.

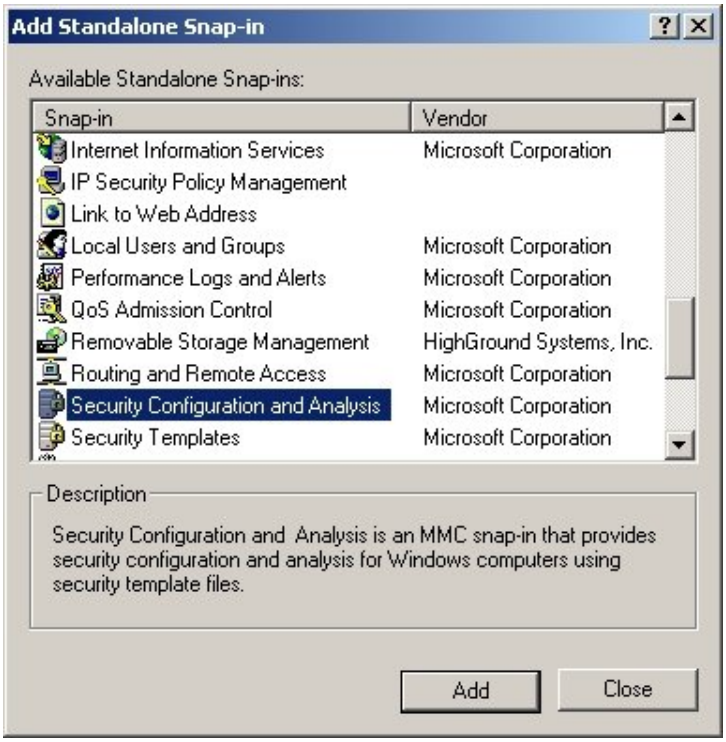

Figure 58 – Adding the **Security Configuration and Analysis** snap-in.

- After the snap-in is in place, you can begin the process for analyzing system security policies. Analyze security as follows:
  - Right click **Security Configuration and Analysis** and select **Open database**. Choose an existing personal database, or type a file name to create a new personal database. Click **Open**. If this is not the database used for the current configuration, you are prompted to select the security template you want to load into your database. If you chose an existing personal database that may already contain a template, and you want to *replace* that template rather than merge it into the stored template, select **Overwrite existing configuration in database**. Click **Open**. You now have a security database to work within for the analysis.
  - Right-click Security Configuration and Analysis, and then click Configure **System Now**. This begins the configuration portion of the analysis process.
  - Right-click Security Configuration and Analysis, and then click Analyze System **Now**. Click **OK** to use the default analysis log, or enter a file name and valid path. The different security areas are displayed as they are analyzed. This completes the procedure for reviewing security

policies. You can view the output in the console window (as shown in Figure 59) or in the log file by right clicking **Security Configuration and Analysis** and then clicking **View Log File**.

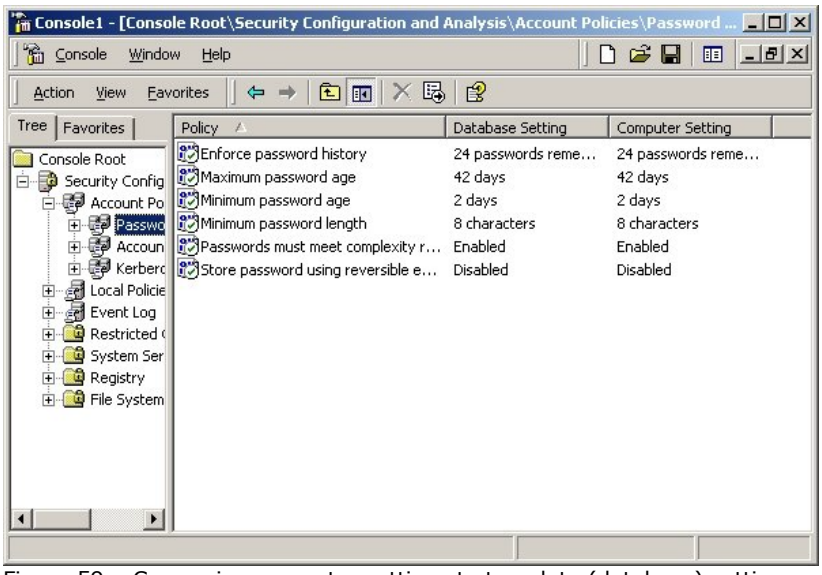

Figure 59 – Comparing computer settings to template (database) settings.

Configuring, Securing, and Troubleshooting Remote Access

Configure and troubleshoot remote access and virtual private network (VPN) connections

Configuring Remote Access and VPN Servers

- Installing and configuring a VPN Server is discussed in KB# Q308208, and is briefly outlined below:
  - Ensure that the configuration for the connection to the Internet and the connection to the LAN are correctly configured on the computer that will serve as the VPN Server.
  - Click **Start > Administrative Tools > Routing and Remote Access**. Pick a server name from the console tree, right-click it and select **Configure and Enable Routing and Remote Access**. The Routing and Remote Access Server Setup Wizard starts, click **Next** to start the setup process.

  - Select **Virtual private network (VPN server)** and then click **Next**.
  - Confirm that TCP/IP is included in the list of **Remote Client Protocols** and click **Yes, all of the available protocols are on this list** and then click **Next**. If TCP/IP is not included, you will install the required protocols from the Network and Dial-up Connections applet and re-run the Wizard again at a later time.
  - Select the Internet connection that will connect to the Internet and then click **Next** to continue. When asked about how you wish to assign IP addresses to remote access clients, select **Automatically** unless specific conditions in your organization require other considerations. This will allow the DHCP Servers on your network to service the remote clients with a DHCP lease (including all pertinent network configuration information). Click **Next** to continue.
  - Select **No, I don't want to set up this server to use RADIUS now**. Click **Next** and then **Finish** to complete the process.
- Next, you must configure the DHCP Relay Agent with the IP address of the DHCP Servers on your network (KB# Q232703, Q160699). Failure to do will result in remote access clients obtained incomplete and incorrect DHCP lease information.
  - From the **IP Routing** node of your new VPN Server, right-click on **DHCP Relay Agent** and select **Properties**.
  - Enter the IP address of the DHCP Servers on your network and click **OK** to close out the dialog box.
- The last major step in setting up the remote access and VPN server involves the configuration of the VPN ports as follows:
  - Right-click on the **Ports** node and select **Properties**. From the window that opens, click **WAN Miniport (PPTP)** and click **Configure** (shown in Figure 60).
  - If you need to support client dial-up VPN access to modems installed on the VPN server, ensure that the **Demand-Dial Routing Connections (Inbound and Outbound)** option is checked, otherwise uncheck it.
  - Set the maximum number of connections that you want to allow in the **Maximum Ports** text box. (This may depend on the number of available IP addresses.) Click OK to complete the configuration of PPTP ports.
  - Configure the **WAN Miniport (L2TP)** options using the same process.

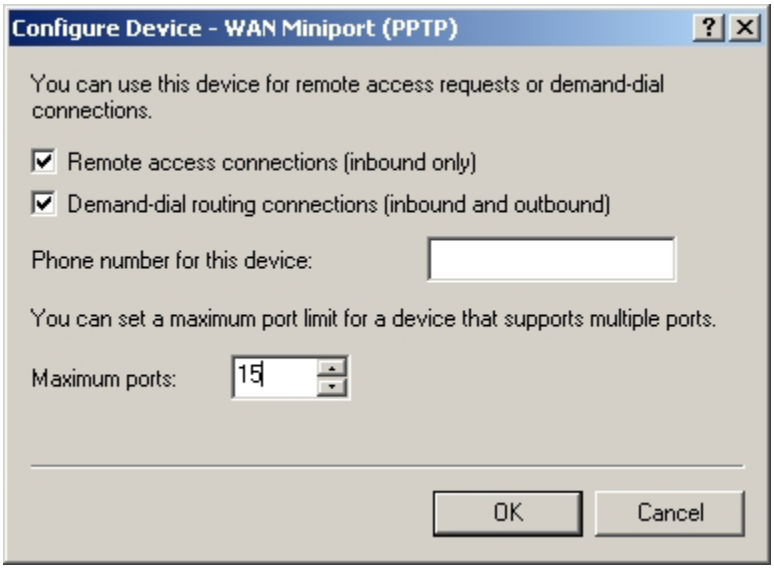

Figure 60 – Configuring VPN port properties.

- In the event that you already have an existing remote access server and you want to verify its configuration to allow routing, do so as follows (shown in Figure 61):
  - From them **Routing and Remote Access** console, right-click the server name and click **Properties**.
  - From the General tab, verify that **Enable This Computer As A Router** is selected as well as either **Local area network (LAN) routing only** or **LAN and demand-dial routing**. Click **OK** when done.
- Additional help for setting up remote access is found in KB# Q301193.

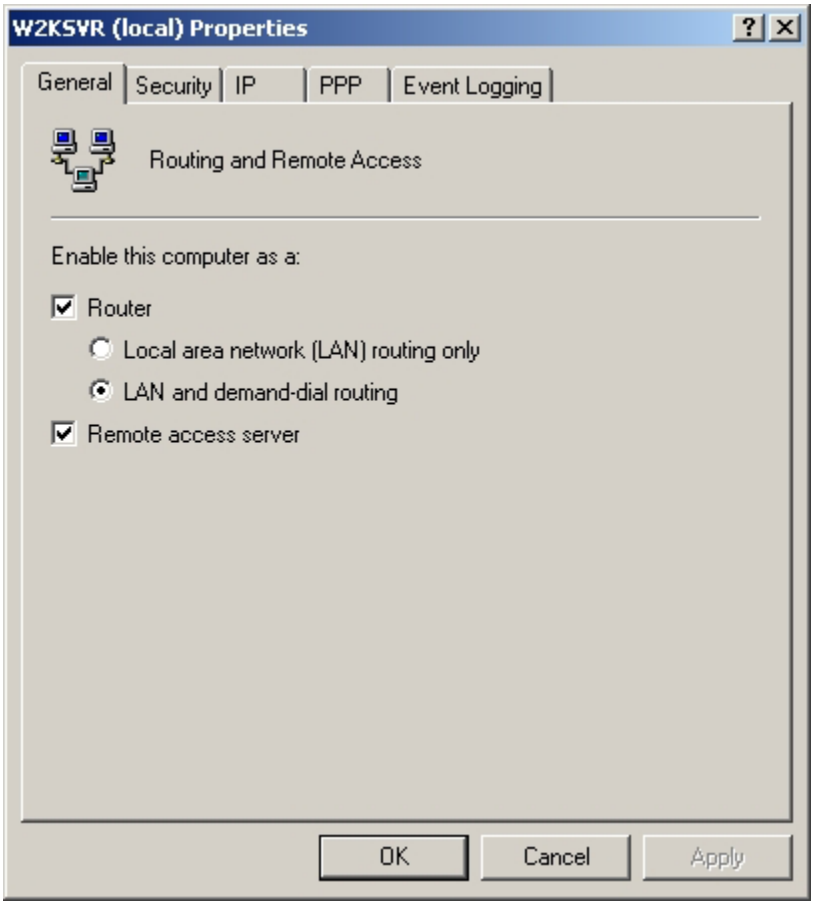

Figure 61 – Verifying remote access properties for routing.

Troubleshooting VPN Servers

- When attempting to troubleshoot VPN connections, it is critical to understand the different tunneling protocols and authentication methods and how they are supported in not only Windows 2000, but also by the Operating Systems that client machines may be running.
- A summary of tunneling protocols supported by Microsoft Windows Operating Systems:

Operating System	Supported tunneling protocols	Unsupported tunneling protocols
Windows 2000	Point-to-Point Tunneling Protocol (PPTP) and Layer Two Tunneling Protocol (L2TP)	None
Windows NT 4.0	PPTP	L2TP
Windows NT 3.51	None	L2TP, PPTP
Windows 98	PPTP	L2TP
Windows 95	PPTP with the Windows Dial-Up Networking 1.3 Performance & Security Upgrade for Windows 95	L2TP

- A summary of authentication methods supported by Microsoft Windows Operating Systems:

Operating System	Supported remote access authentication protocols	Unsupported remote access authentication protocols
Windows 2000	Microsoft Challenge Handshake Authentication Protocol (MS-CHAP), Challenge Handshake Authentication Protocol (CHAP), Shiva Password Authentication Protocol (SPAP), Password Authentication Protocol (PAP), MS-CHAP version 2 (MS-CHAP v2), and Extensible Authentication Protocol (EAP)	
Windows NT version 4.0	MS-CHAP, CHAP, SPAP, PAP, and MS-CHAP v2 (with the Windows NT 4.0 Service Pack 4 and later)	EAP
Windows 98	MS-CHAP, CHAP, SPAP, PAP, and MS-CHAP v2 (with the Windows 98 Service Pack 1 and later)	EAP
Windows 95	MS-CHAP, CHAP, SPAP, PAP, and MS-CHAP v2 (with the Windows Dial-Up Networking 1.3 Performance & Security Upgrade for Windows 95)	EAP

- Perhaps the most common problem with VPN Servers is the inability to connect to the server. This is understandable, as the list of possible causes is extensive and summarized below:
  - The credentials of the VPN client (user name, password, and domain name) are incorrect and cannot be validated by the VPN server.
  - The Routing and Remote Access service is not started on the VPN server.
  - Remote access is not enabled on the VPN server.
  - The VPN server cannot access Active Directory.
  - PPTP or L2TP ports are not enabled for inbound remote access requests.
  - The LAN protocols being used by the VPN clients are not enabled for remote access on the VPN server.
  - All of the PPTP or L2TP ports on the VPN server are already being used by currently connected remote access clients or demand-dial routers.
  - The VPN server does not support the tunneling protocol of the VPN client.
  - The VPN client and the VPN server, in conjunction with a remote access policy, are not configured to use at least one common authentication method.
  - The VPN client and the VPN server, in conjunction with a remote access policy, are not configured to use at least one common encryption method.
  - The VPN connection does not have the appropriate permissions through dial-in properties of the user account and remote access policies.
  - The settings of the remote access policy profile are in conflict with properties of the VPN server.
  - There are not enough addresses in the static IP address pool (this is one good reason to use DHCP Servers on your network).
  - The authentication provider of the VPN server is improperly configured.
- Another common problem you may encounter with a VPN Server is the inability of remote access clients to see resources inside the network (think DHCP Relay Agent). Some possible causes are:
  - The LAN protocols used by remote access VPN clients are not enabled to allow access to the network to which the VPN server is attached.
  - A static IP address pool is configured but there are no routes back to the remote access VPN clients.
  - Packet filters on the remote access policy profile are preventing the flow of IP traffic.
- NAT and IPSec are incompatible technologies because of IPSec encrypting the headers, the NAT Translator cannot examine the packet (KB# Q259335).

- Basic L2TP/IPSec troubleshooting guidance is provided in KB# Q259335 and basic IPSec troubleshooting help can be found in KB# Q257225.
- Guidance on providing secure point-to-point communications across the Internet can be found in KB# Q301194.

Troubleshooting Remote Access Servers

- Troubleshooting Remote Access Servers is similar to troubleshooting VPN Servers. The most common problem is the inability to connect to the Remote Access Server and some possible reasons are:
  - The credentials of the remote access client (user name, password, and domain name) are incorrect and cannot be validated by the remote access server.
  - The modem is not working properly on one or both ends of the connection.
  - The Routing and Remote Access service is not started on the remote access server.
  - Remote access is not enabled on the remote access server.
  - The remote access server cannot access Active Directory.
  - Dial-in, PPTP, or L2TP ports are not enabled for inbound remote access connections.
  - The Windows 2000 Fax service is enabled and your modem does not support adaptive answer.
  - You are using MS-CHAP v1 and a user password over 14 characters long.
  - The LAN protocols being used by the remote access clients are not configured on the remote access server to allow remote access connections.
  - Currently connected remote access clients or demand-dial routers are already using all of the remote access ports on the remote access server.
  - The remote access client and the remote access server in conjunction with a remote access policy are not configured to use at least one common authentication method.
  - The remote access client and the remote access server in conjunction with a remote access policy are not configured to use at least one common encryption strength.
  - The remote access connection does not have the appropriate permissions through dial-in properties of the user account and remote access policies.
  - The settings of the remote access policy profile are in conflict with properties of the remote access server.
  - There are not enough addresses in the static IP address pool.

- Another issue you may run into with Remote Access Servers is the inability of the remote access client to see network resources inside of the network. Some possible problems are:
  - For IP-based remote access clients, IP routing is not enabled.
  - A static IP address pool is configured but there are no routes back to the remote access clients.
  - Packet filters on the remote access policy profile are preventing the flow of IP traffic.
  - For IPX, AppleTalk, or NetBEUI-based remote access clients, these protocols might not be installed on the server.
- If callback is not working properly, look at these points to determine the cause of the problem:
  - Callback is improperly configured on the dial-in properties of the user account.
  - **Link control protocol (LCP) extensions** is disabled on the **PPP** tab for the properties of the remote access server.
  - Callback numbers may be truncated when a remote access server running Windows NT 4.0 requests dial-in properties of a user account in a Windows 2000 native-mode domain.
- You can troubleshoot modem commands sent from the Remote Access Server or client by using a modem log file (KB# Q162694).
- LabMice.net provides a fairly large resource of RAS troubleshooting articles.

Troubleshoot Routing and Remote Access policy

- A remote access policy profile is a set of properties that are applied to a connection when the connection is authorized—either through the user account permission setting or the policy permission setting.
- Remote access policy conditions are one or more attributes that are compared to the settings of the connection attempt. If there are multiple conditions, then all of the conditions must match the settings of the connection attempt in order for the connection attempt to match the policy.
- Before troubleshooting RRAS policy on your Remote Access Server, first determine if you are operating in native-mode or mixed-mode…it matters.
  - In a native-mode network, the remote-access permission on every user account is set to **Control access through Remote-Access Policy**, which means that the remote-access permission setting on the remote-access policy controls whether remote-access permission is allowed or denied. You can allow or deny access on a per-group basis by creating a remote-access policy using the **Windows Group** condition and setting the remote-access permission on the remote-access policy to either **Grant remote-access permission** or **Deny remote-access permission**.

  - In a mixed-mode network, the remote-access permission on every user account is set to **Allow access**, and the default remote-access policy, called **Allow access if dial-in permission is enabled**, is deleted. On a remote-access server running Windows 2000 that is a member of a Windows 2000 mixed-mode domain, the **Control access through Remote-Access Policy** setting on the user account is not available. You can allow or deny access on a per-group basis by creating a remote-access policy using the **Windows Group** condition. However, in order to deny access, you must specify, within the profile properties, a connection constraint that cannot be met. To do this, enable the **Restrict Dial-in to this number only** dial-in constraint and type a number that does not correspond to any dial-in number being used by the server.

- Another, however more difficult to administer and less dependable, method to control remote access permissions is directly via a user's account. Permissions are controlled through the **Allow access** and **Deny access** options on the **Dial-in** tab of the user account's properties in the Active Directory Users and Groups Snap-in. Remote-access permission can be enabled or disabled on a per-user basis by selecting **Allow access** or **Deny access**. You can allow access on a per-group basis by creating a remote-access policy using the **Windows Group** condition. However, only the members of the group who have the remote-access permission option set to **Allow access** will be granted access. You can deny access on a per-group basis, regardless of the user account's remote-access permission setting, by creating a remote-access policy using the **Windows Group** condition. However, you must specify, within the profile properties, a connection constraint that cannot be met. To do this, enable the **Restrict Dial-in to this number only** dial-in constraint and type a number that does not correspond to any dial-in number being used by the server.
- You cannot use the built-in local groups of a stand-alone remote access server running Windows 2000 for the Windows Groups attribute.
- Remote access policies are processed as shown in Figure 62.

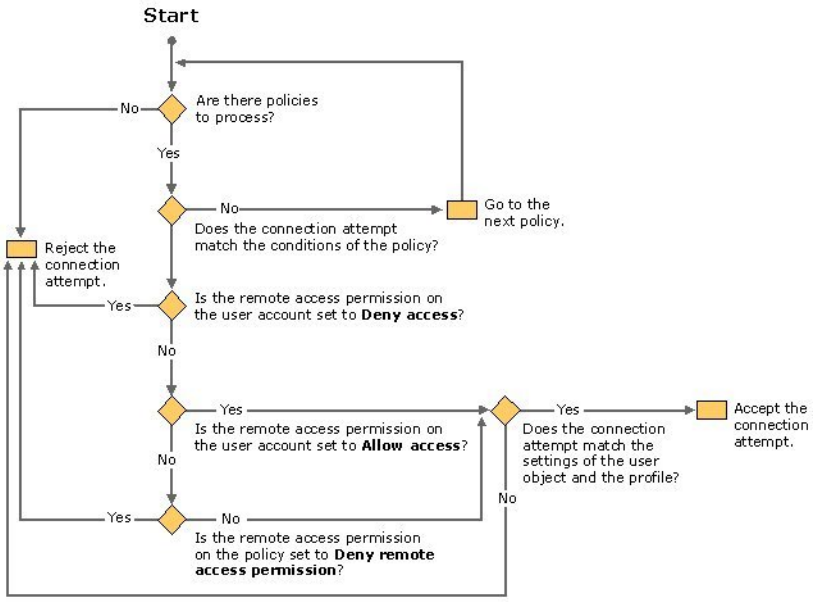

Figure 62 – Remote access policy processing flowchart (Windows 2000 online help system).

Implement and troubleshoot Terminal Services for remote access

Configuring Terminal Services (KB# Q306626, Q270897, TechNet, Server Documentation)

- Terminal Services provides remote access to a server desktop through "thin client" software, serving as a terminal emulator. Terminal Services transmits only the user interface of the program to the client, while the application itself runs from the server. The client then returns keyboard and mouse clicks back to be processed by the server.
- Terminal Services can be deployed on the server in either application server or remote administration mode. As an application server, Terminal Services provides an effective and reliable way to distribute Windows-based programs with a network server. In application server mode, Terminal Services delivers the Windows 2000 desktop and the most current Windows-based applications to computers that might not normally be able to run Windows. When used for remote administration, Terminal Services provides remote access for administering your server from virtually anywhere on your network.
- To deploy Terminal Services in Remote administration mode, open the **Add/Remove Programs** applet in the **Control Panel**. Choose the **Add/Remove Windows Components** option and then place a check next to

Terminal Services and click **Next**. This will bring up the window as shown in Figure 63. Select Remote administration mode and click **Next**. Configuration for Remote administration mode is complete.

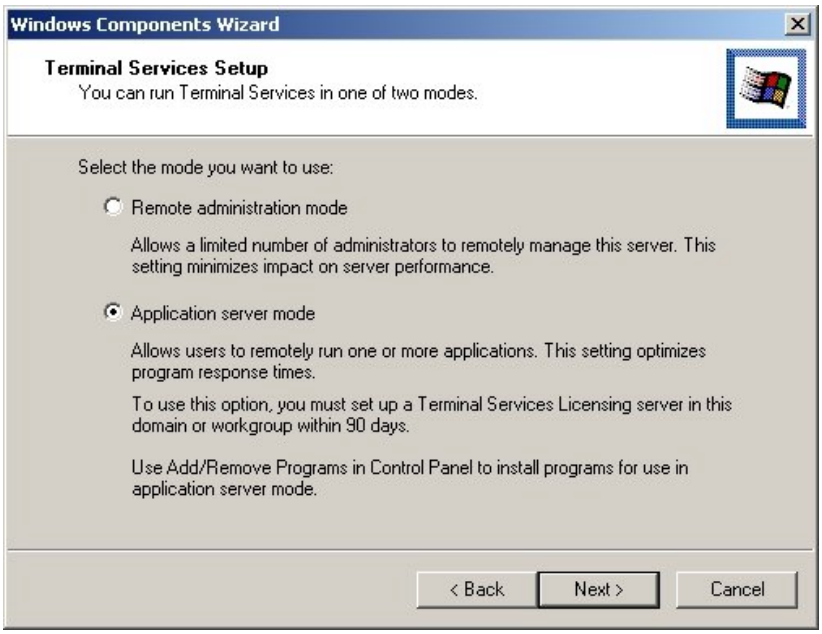

Figure 63 – Installing Terminal Services.

- To deploy Terminal Services in Application server mode, open the **Add/Remove Programs** applet in the **Control Panel**. Choose the **Add/Remove Windows Components** option and then place a check next to Terminal Services and click **Next**. This will bring up the window as shown in Figure 63. Select Remote administration mode and click **Next.** Select **Permissions compatible with Windows 2000 Users** (preferred) or **Permissions compatible with Terminal Server 4.0 Users** as your organization requires. You will now be presented with a window detailing all applications that may cease to function properly (shown in Figure 64). These applications will need to be reinstalled after the installation of Terminal Services by using the **Add New Programs** option of the **Add/Remove Programs** applet.

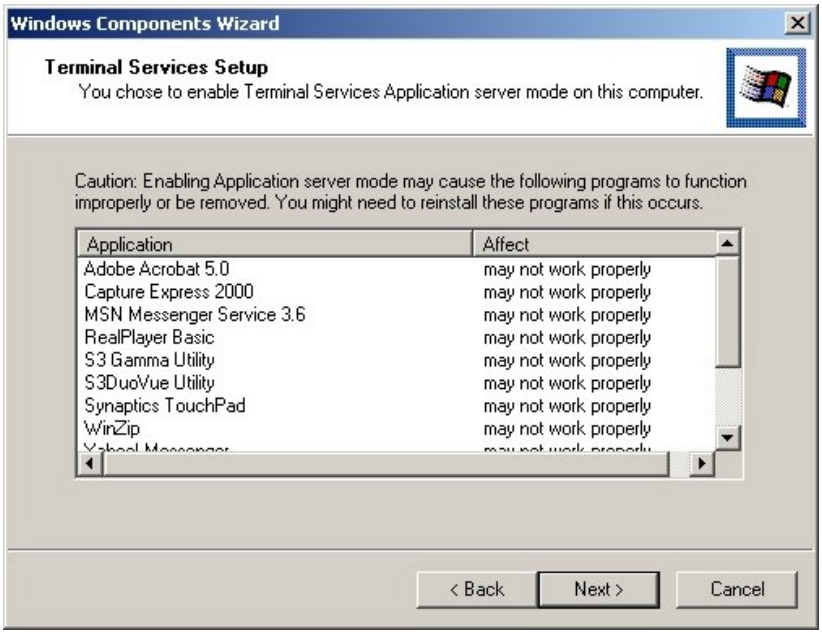

Figure 64 – Applications that may cease to function properly after installation of Terminal Services application server.

Troubleshooting Terminal Services

- If an installed program is not functioning properly, there are several possible solutions:
  - If the program was installed before Terminal Services was enabled, it will have to be uninstalled. To correct this problem, uninstall the program, and reinstall using either **Add/Remove Programs** or the **change user** command.
  - If the program was installed using **change user /execute** rather than **change user /install**, it will have to be uninstalled. To correct this problem, uninstall the program, and reinstall using either **Add/Remove Programs** or the **change user** command.
  - If the program compatibility scripts were not run properly, try running them again.
- If you need to determine the type of Terminal Services Server you have configured, follow these steps (KB# Q243212):
  - Click Start > Programs > Administrative Tools. Click Terminal Services Configuration. Click Server Settings. Locate the Terminal server mode row in the right pane. The mode is listed in the Attributes column.

  - If you double-click Terminal server mode, Windows 2000 calls the ShellExecute API function and a dialog box opens. This dialog box describes how to change modes (KB# Q238162).
- If you receive the following message when logging on to a Terminal Services Server running in Remote Administration mode

```
Logon Message
You do not have access to logon to this Session.
OK
```

  Then the account you are attempting to log on with does not have **Administrative** privileges (KB# Q253831). To correct this issue, you must grant additional security groups (such as the **Server Operators** group) permissions enabling them to log onto the Remote administration Server as follows:
  - Click **Start > Programs > Administrative Tools**, and then click **Terminal Services Configuration**. In the tree in the left pane, click **Connections**. Click the **RDP-TCP** connection in the right pane, and then click **Properties** on the **Action** menu. Click the **Permissions** tab. (NOTE: Only **Administrator** and System accounts appear.)
  - Click **Add**. Search for the groups or users that are appropriate for your Terminal Services management (such as the Server Operators group). Click **Add** to place them in the bottom pane. Click **OK**. (NOTE: The Server Operators group appears in the RDP-TCP properties; the permissions in the bottom pane are not enough to manage the server because only **Guest Access** is selected by default.)
  - Click to select the **User Access** check box for basic tasks or both the **User Access** and **Full Control** check boxes to fully manage the server, and then click **Apply**. Click **OK**. Test by logging on the accounts in the **Server Operators** group.
- If you are experiencing problems with a Terminal Services profile that is inconsistent or overwritten (KB# Q243535), this may be from logging in with that profile in more than one instant simultaneously. The correction for this problem is to cease the use of roaming profiles and use only local profiles when using Terminal Services.
- Many additional Terminal Services troubleshooting articles can be found at LabMice.net.

Configure and troubleshoot Network Address Translation and Internet Connection Sharing

Network Address Translation (KB# Q299801, Q254018, Q254322)

- With **Network Address Translation** in Windows 2000, you can configure your home network or small office network to share a single connection to the Internet. Network address translation consists of the following components:
  - **Translation component**: The Windows 2000 router on which network address translation is enabled acts as a network address translator (NAT), translating the IP addresses and TCP/UDP port numbers of packets that are forwarded between the private network and the Internet.
  - **Addressing component**: The network address translation computer provides IP address configuration information to the other computers on the home network. The addressing component is a simplified DHCP server (referred to as the DHCP Allocator) that allocates an IP address, a subnet mask, a default gateway, and the IP address of a DNS server. You must configure computers on the private network as DHCP clients in order to receive the IP configuration automatically. (You can disable the addressing component of NAT and use existing Windows 2000 DHCP servers on the network—a recommended action).
  - **Name-resolution component**: The network address translation computer becomes the DNS server for the other computers on the home network. When the network address translation computer receives name resolution requests, it forwards the name-resolution requests to the Internet-based DNS server for which it is configured and returns the responses to the home network computer.
- The following items require consideration before attempting to implement NAT on a network:
  - *Private network addressing*: You should use one of the following IP addresses from the InterNIC private IP network IDs: 10.0.0.0 with a subnet mask of 255.0.0.0, 172.16.0.0 with a subnet mask of 255.240.0.0, or 192.168.0.0 with a subnet mask of 255.255.0.0. By default, network address translation uses the private network ID 192.168.0.0 with the subnet mask of 255.255.255.0 for the private network.
  - *Single or multiple public addresses:* If you are using a single public IP address allocated by your ISP, no other IP address configuration is necessary. If you are using multiple IP addresses allocated by your ISP, then you must configure the network address translation (NAT) interface with your range of public IP addresses.

- *Allowing inbound connections:* Normal NAT usage from a home or small business allows outbound connections from the private network to the public network. Programs such as Web browsers that run from the private network create connections to Internet resources. The return traffic from the Internet can cross the NAT because the connection was initiated from the private network. To allow Internet users to access resources on your private network, you must perform additional configuration as follows:
  - Configure a static IP address on the resource server inside the private network.
  - Exclude the IP address being used by the resource computer from the range of IP addresses being allocated by the NAT computer.
  - Configure a special port. A special port is a static mapping of a public address and port number to a private address and port number. A special port maps an inbound connection from an Internet user to a specific address on your private network. This comes into play if you have resources on your private network (such as a Web Server or a FTP Server) that you wish to make publicly available.
- *Configuring applications and services:* You may need to configure applications and services to work properly across the Internet. For example, if users on your small office or home office (SOHO) network want to play a game with other users on the Internet, network address translation must be configured for that application (i.e., a specific port will most likely need to be opened).
- *VPN connections from a translated SOHO network:* To access a private intranet using a VPN connection from a translated NAT network, you must use the PPTP protocol as NAT does not support L2TP with IPSec.

- To implement NAT on your network, the easiest way is to use the **Routing and Remote Access** console. Right click the server in the window and select **Configure and Enable Routing and Remote Access**. This will launch the Routing and Remote Access Server Setup Wizard. Click **Next** to start the procedure. Choose **Internet connection server** (as shown in Figure 65) and click **Next**. Choose **Set up a router with the Network Address Translation (NAT) protocol** and click **Next** again. Pick the connection that will be used and click **Next**. If you chose to use a demand-dial connection, then the Demand Dial Interface Wizard will start and you will follow it to create the demand-dial interface. Click Finish on the Routing and Remote Access Server Setup Wizard and you will have configured your server for **NAT**.

Figure 65 – Setting up a NAT Server.

- If the Routing and Remote Access service has already been enabled on the machine, you will have to do some of the configuration manually (KB# Q299801).

Internet Connection Sharing (KB# Q234815, Q307311, Q237254)

- Internet Connection Sharing (ICS) is a watered down version of Network Address Translation that is intended for small networks, typically those found in the home or small business.
- Using ICS, one computer, called the ICS host, shares its Internet connection with the rest of the computers on the private network. Other computers on the private network can force the ICS host to initiate a connection to the Internet (if not already active) by beginning a task that required Internet access, such as starting Internet Explorer or Outlook Express.
- The ICS host must have at least one Network Interface Card (NIC) connected to the rest of the private network through a switch or hub and one other network interface that connects to the Internet. This can be either broadband (Cable, DSL, etc) or a standard dial-up modem.
- When ICS is enabled it will reassign the private adapter the IP of 192.168.0.1 with subnet of 255.255.255.0. All of the computers inside the private network must be configured to request IP addresses using DHCP. The ICS host will act as its own DHCP and DNS server for the internal private network.

- To configure a connection for ICS, open the **Network and Dial-Up Connections** applet in the **Control Panel**. Right-click the connection you want to share, and then click **Properties**. Click the **Sharing** tab (shown in Figure 66), and then click to select the **Enable Internet Connection Sharing for this connection** check box. If the connection you are sharing is a Dial-up connection and you want the connection to dial automatically when another computer on your home network attempts to use external resources, click to select the **Enable on-demand dialing** check box.

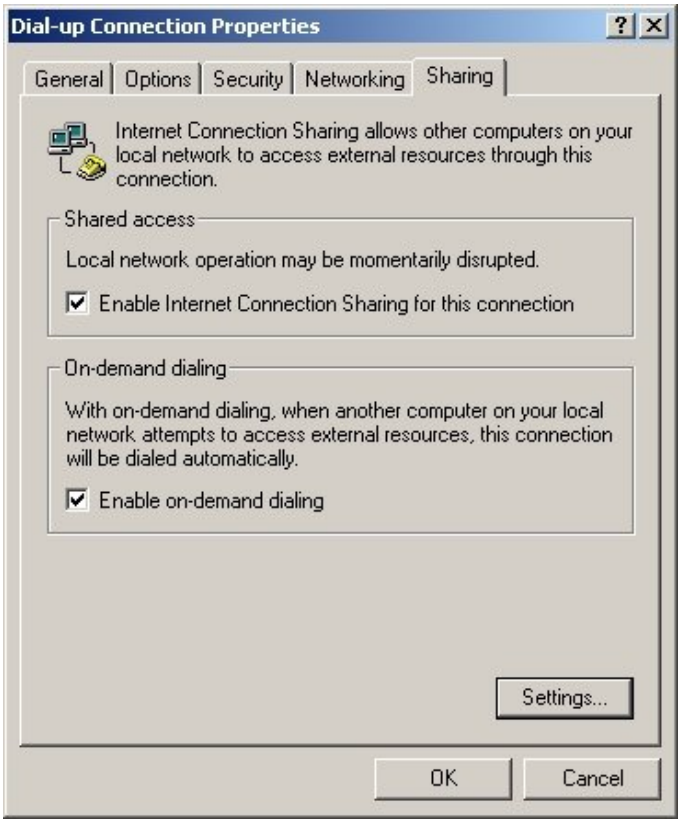

Figure 66 – Setting up Internet Connection Sharing.

- You can customize your ICS settings by clicking on the **Settings…** button. A new window will open up as shown in Figure 67. From the **Applications** tab, you can add applications for use with ICS. To add applications, you will need to provide the following information: application name, remote port number, remote port type, local port number and local port type. From the **Services** tab, you can enable or disable standard Internet applications, such as FTP Servers, SMTP Servers or Web Servers. You can also customize the setup of these services as required for your network configuration.

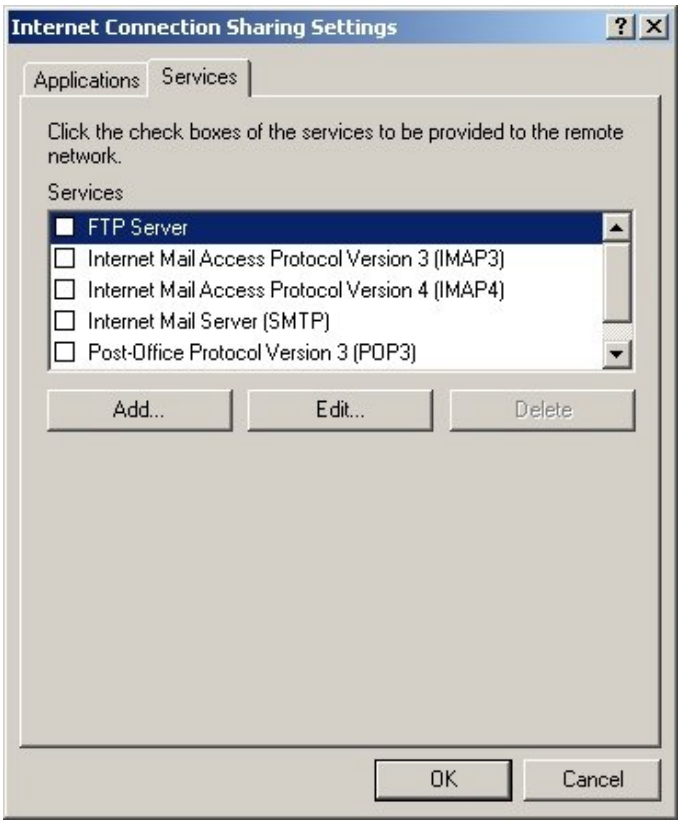

Figure 67 – Configuring settings for Internet Connection Sharing.

- To enable ICS, you must have **Administrative** privileges.
- Additional help on setting up ICS can be found in the Windows 2000 Professional Documentation, the Windows 2000 Server Documentation and also in KB# Q237254.
- Additional information on NAT versus ICS is found online in the Server Documentation.

Special thanks to Will Schmied for contributing this Cramsession.
To send feedback to Will, please post a message
labeled "Attention Cramsession Author" here:

Managing W2K Network Environment Forum

Make sure to visit his site at:

http://www.soitslikethat.com/

Will would like to acknowledge the following
individual for his tremendous assistance in
the preparation of this Cramsession:

Sean McCormick