Chapter 6

Configuring New Windows 2000 Server Installations

Checking for Setup Problems 107

Configuring Devices 108

Configuring Networking Settings 114

Configuring Storage 125

Using the Windows 2000 Configure Your Server Tool 125

Performance and Memory Tuning 129

Updating Windows 132

Securing Windows 133

Summary 135
After installing Microsoft Windows 2000 Server, it’s important to check for installation errors or problems. Also, add (and possibly troubleshoot) any other devices, review the server’s network settings, and use the Configure Your Server Wizard to set up the server for its desired network role, such as Dynamic Host Configuration Protocol (DHCP) server or Active Directory service domain controller. Now is also the time to partition and format any additional disk drives and tune the server’s performance and memory options to best suit its desired role. You should also implement the appropriate security measures for the server’s desired role.

The goal of this chapter is to help get your system in basic working order, with information on fine-tuning to come in later chapters. For example, Chapter 14 has more information on the management of DHCP, Domain Name System (DNS), and Windows Internet Name Service (WINS). If you need to configure disks, see Chapter 15.

**Tip** In addition to the tasks covered in this chapter, you might want to set up security auditing (covered in Chapter 9 and Chapter 18) and remote administration using the Terminal Services feature (covered in Chapter 26).

**Checking for Setup Problems**

After your Windows installation is complete, you should check the system for setup errors or device problems. Check the following items:

- Check Event Viewer for errors (Event Viewer is discussed in Chapter 10).
- Review setup errors. To do so, open the \Winnt\setuperr.log file, if it exists. If it doesn’t, there were no errors.
Configuring Devices

Immediately after finishing an installation of Windows 2000, or any operating system for that matter, check to make sure devices are recognized and properly configured. Although Windows 2000 Setup generally does a good job of detecting and configuring, Setup isn’t able to resolve resource conflicts or overcome a lack of drivers. You’ll also need to enable devices, such as an uninterruptible power supply (UPS), that were disconnected or disabled before starting the installation.

Microsoft Windows NT 4 isn’t the best operating system for finding and troubleshooting device problems because it lacks Plug and Play (PnP) functions and supports a somewhat limited hardware base. In contrast, Windows 2000 handles these issues well, integrating PnP support along with a more centralized method of managing hardware devices, using Device Manager and the Add/Remove Hardware Wizard, and generally improving device driver support. Check the list of devices in Device Manager for conflicts and for devices that weren’t installed during setup, and then use the Add/Remove Hardware Wizard to make the necessary changes. You can use Device Manager if you prefer a more hands-on approach.

Using the Add/Remove Hardware Wizard

Although you can use Device Manager instead of the Add/Remove Hardware Wizard to handle most of the wizard’s functions, you do need to use the Add/Remove Hardware Wizard to add a device that Windows 2000 can’t recognize or to unplug or eject a device.

Removing and Adding a Device

To remove a device, select the Uninstall/Unplug A Device option in the Add/Remove Hardware Wizard, and then use the screens that follow either to temporarily unplug a hot-pluggable device or to permanently uninstall a device from your system. You can always add the device back later by using this same wizard or by using autodetection of PnP devices in Windows 2000.

To add a device to your system, make sure the device is physically connected and, if appropriate, turned on. Then double-click the Add/Remove Hardware icon in Control Panel, and when the Welcome screen appears, click Next to begin the wizard.

Select the Add/Troubleshoot A Device option, shown in Figure 6-1, and then click Next. Windows 2000 scans your system for PnP hardware and displays a list of detected hardware. If new PnP hardware is detected, Windows 2000 installs drivers, if it can locate them, and displays a list of devices that it installed. Click Finish to end the installation process.
Troubleshooting a Device

If, after you add a device, Windows 2000 doesn’t detect it or detects it incorrectly, you can troubleshoot the problem using the Add/Remove Hardware Wizard. When no new devices are found, Windows 2000 displays all the devices on your system—listing any disabled devices or devices with problems first (Figure 6-2).

Figure 6-2. The Choose A Hardware Device screen of the Add/Remove Hardware Wizard.
When troubleshooting a problem device, select the device from the list, and then click Next to see the status of the device and to start a troubleshooter. To add a device that Windows 2000 couldn’t detect, select Add A New Device from the list in the Choose A Hardware Device screen, and then follow these steps:

1. Choose whether you want Windows 2000 to search for your hardware or whether you want to select the device manually from a list.
2. Select from the list of devices detected, or select a type of hardware you want to install from the provided list, and click Next.
3. If you chose to select your device manually, select the manufacturer and device, or click Have Disk to supply your own drivers, and then click Next. Windows 2000 installs the drivers for your device and then displays a summary of its actions.
4. Click Finish to complete the wizard.

**Using Device Manager**

Device Manager is a central repository for device information in Windows 2000. If you’ve used Device Manager in Microsoft Windows 95/98, you’ll be at home with the Windows 2000 Device Manager. Use it to view or print the configuration and drivers loaded for any device on your system as well as to disable, uninstall, or change the configuration for a device.

**Opening Device Manager**

You can access Device Manager in one of several ways. Perhaps the most useful way is to launch Computer Management (Compmgmt.msc) from the Administrative Tools folder on the Programs menu. Click the plus sign next to System Tools to expand the tree, and then click Device Manager.

You can also access Device Manager by opening the System tool in Control Panel. Click the Hardware tab and then click Device Manager. The Hardware tab also contains the Hardware Wizard and the Driver Signing tool that you can use to specify whether you want to permit the use of unsigned device drivers.

**Tip** To use the Computer Management snap-in to remotely administer another computer running Windows 2000, select Computer Management in the console tree, and then choose Connect To Another Computer from the Action menu. Select the computer you want to manage, click OK, and you’re there.
Working with Device Manager

After opening Device Manager, you’ll see a list of all the devices that Windows 2000 has detected on your system (Figure 6-3). Any nonfunctioning devices are displayed with an exclamation point, indicating that a problem exists with the device; disabled devices are displayed with a small red “x” over the icon.

On the far right side of the toolbar, icons are available according to the device you’ve selected. In Figure 6-3, they are the following buttons (reading from left to right):

- **Scan For Hardware Changes**  Click this button to tell the system to look for changes in hardware. Use this button after adding new PnP devices or after swapping hardware.

- **Disable/Enable**  Select a device and click this button to disable it or enable it, depending on its current status. When a device is disabled, its resources are freed and its drivers remain but are not loaded during startup. Take care not to disable something you need to start the machine.

- **Uninstall**  Select a device and click this button to uninstall it. This should only be necessary for non-PnP devices. You can uninstall a PnP device by simply removing it from the computer. Uninstalling a device doesn’t remove its drivers from the hard disk.
To change the Device Manager display, choose a setting from the View menu (see Table 6-1). Use the different view settings for Device Manager to organize your system’s devices in a way that makes it easy to find the information you need.

Table 6-1. View settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Devices By Type</td>
<td>Shows devices categorized by device type; usually the most useful view (also the default)</td>
</tr>
<tr>
<td>Devices By Connection</td>
<td>Shows all devices in relation to how they’re connected to other devices</td>
</tr>
<tr>
<td>Resources By Type</td>
<td>Shows all system resources, organized by type of resource</td>
</tr>
<tr>
<td>Resources By Connection</td>
<td>Shows all system resources, organized and grouped by the device to which they’re connected</td>
</tr>
<tr>
<td>Show Hidden Devices</td>
<td>Includes devices that are not PnP plus devices that might have been physically removed but still have their drivers installed</td>
</tr>
</tbody>
</table>

**Working with Device Properties**

To display a device’s properties (Figure 6-4), select the device, and then click the Properties toolbar button or double-click the device. In the Device Properties dialog box, there might be several tabs. You can view the status and configuration information, as well as the device manufacturer, device type, and location, in the upper portion of the General tab.

**Tip** The device name shown in Device Manager is the name of the driver that Windows 2000 is using for the device and can actually be incorrect if the wrong driver is loaded for the device.

The Device Status box in the middle of the General tab displays the status of the device, including any errors. If the device has any problems, the Device Status box briefly describes the problem, and usually it also describes the appropriate course of action to correct the problem. Click Troubleshooter to use the built-in mechanisms for detecting the nature of the problem.
Other tabs include the Driver tab, which displays the details of the driver being used. This tab also lets you update or uninstall the driver. The Resources tab displays the hardware resources being used. This tab allows you to see and resolve any conflicts caused by non-PnP devices. Along with these tabs, some devices have additional advanced settings or tabs for device-specific settings.

**Tip** Device Manager works on remote computers in read-only mode. You can use Device Manager to diagnose problems, but you must make changes locally.

**Troubleshooting Devices**

Troubleshooting devices is not an exact science. Devices in Windows 2000 usually work with minimal installation headaches. If they don’t, it’s often difficult to make them work. With that said, here are some of the troubleshooting techniques we’ve learned from our many years of device-induced headaches:

- Open the properties for the device and see if the cause of the problem is listed in the General tab or the Resources tab. If there are any conflicts, remove or disable the conflicting device, or plug the device into a different slot (if possible).
Part II  Installation and Initial Configuration

Select the device in Device Manager and click the Uninstall toolbar button. Click Scan For Changes and let Windows redetect the device. Hopefully it will install properly. You can also uninstall the device and then reboot Windows for a more thorough but time-consuming attempt.

Try plugging external devices into a different port, or directly into the computer instead of through a hub. Only connect high-power, bus-powered Universal Serial Bus (USB) or Firewire devices such as scanners without external power supplies to self-powered hubs (hubs with external power supplies). To check the power consumption of USB devices, open the device properties for the USB hub and click the Power tab.

If the problem is persistent, remove all unnecessary devices from the system and see if the device works. If not, you’ve got real problems (try the device in another system to see if it’s faulty or if there is a conflict unique to your system). If the device works, add the removed devices back one by one until something doesn’t work, and then assess the situation (you might need to leave some cards or devices unplugged).

**Tip** If you disable something essential—like the mouse or keyboard—you can return to the previous hardware profile by rebooting. When the Loader menu appears, press F8, and choose Last Known Good Configuration. Then choose the version of Windows you have installed from the Loader menu and press Enter. This action enables the last good hardware profile.

**More Info** For more in-depth troubleshooting advice, consult Windows Help, or perform a search on the Microsoft Knowledge Base, accessible from Help or from [http://support.microsoft.com](http://support.microsoft.com).

### Configuring Networking Settings

Although most computers will be properly set up for network access during Windows Setup, you might need to change these settings at some point—possibly immediately if the specified settings were wrong or incomplete. This section explains how to get a server running properly on a network.

### Changing Your Network Identity

Change is sometimes necessary—although with a server, it’s better to spend your time planning first than to have to make changes later. However, as Robbie Burns might have said while reconfiguring his server, “The best laid schemes o’ mice and
men gang aft a-gley.” So even with careful planning, you can discover that a machine needs to have a different name or needs to be joined to a different domain.

To change the identity of a server that isn’t a domain controller, log on using an administrator’s account and follow these steps:

1. Open the System tool in Control Panel, and then click the Network Identification tab.

2. To change your computer name and domain or workgroup membership, select Properties. Then enter the new name for your computer in the New Computer Name text box in the Identification Changes dialog box, as shown in Figure 6-5.

3. To change the domain or workgroup you belong to, choose either the Domain option or the Workgroup option, and then type the domain or workgroup name in the text box.

4. Click More to manually specify the domain name for your computer and to preview the NetBIOS name for your system. Click OK when you’re finished.

Note Changing the identity of a domain controller is a multistep process. First you must demote the domain controller by running DCPROMO. Then you can change the identity, and finally you can promote the domain controller again. The steps for this process are detailed in Chapter 11.
Real World  Naming Computers
It’s a good idea to use a computer name that is both DNS-compatible and NetBIOS-compatible so that all types of clients see the same name for your computer. To do this, make the name 15 characters or fewer and don’t use asterisks or periods. To obtain the best application compatibility, try to avoid using spaces, underscores, and hyphens.

Configuring Network Components
To add or change the settings for core network components such as clients, services, and protocols, open the Network and Dial-Up Connections folder, right-click the Local Area Connection icon, and choose Properties from the shortcut menu. This procedure opens the Local Area Connection Properties dialog box shown in Figure 6-6, which you can use to view and change your server’s networking components.

Figure 6-6. The Local Area Connection Properties dialog box.
The top of the dialog box shows the network adapter to which you are binding networking services. Beneath that is the media access control (MAC) address for the network interface card, the unique identifier of your network card that is used for communications with other hosts in your subnet.

To install a network component, select Install, choose the type of component you want to install (Client, Service, or Protocol), and then click Add. Select the component from the list presented and click OK. To configure the component (if the component has a configurable option), select the component and click Properties.

**Tip** If you have a multihomed server (a server with more than one network adapter), give your local area connections a name indicating to which network the adapters are connected. To do so, right-click the connections in the Network and Dial-Up Connections folder and choose Rename from the shortcut menu.

### Configuring TCP/IP

TCP/IP is the most important protocol in today’s networks, and it’s the backbone for Microsoft’s vision of networking in Windows 2000 and beyond. The protocol is well suited to enterprise networking, and it’s required for accessing the Internet. If you’re unfamiliar with TCP/IP, see Chapter 13 for an introduction.

**Planning** Before installing and configuring protocols on your network, review the checklists in the Windows 2000 Help files. Once you understand the following three areas, you can install all the necessary interlocking pieces.

- TCP/IP concepts such as IP addressing, subnet masks, and gateways
- Whether your network supports DHCP to configure TCP/IP dynamically
- How computers on your network will handle name resolution

### Installing TCP/IP

TCP/IP is installed as the default network protocol if a network adapter was detected during installation. If the default was overridden during installation, you can add TCP/IP by following these steps:

1. Click Start, select Settings, and then choose Network And Dial-Up Connections.
2. Right-click the connection for which you want to install TCP/IP, and choose Properties from the shortcut menu.
3. If TCP/IP isn’t in the list of components used, as shown in Figure 6-6, click Install.
4. Select Protocol, and click Add.
5. In the Select Network Protocol box, select Internet Protocol (TCP/IP) and click OK.
6. Verify that the Internet Protocol (TCP/IP) check box is selected, and then click OK.

**Using Dynamic Addressing**

The easiest and most reliable way to configure machines on a network running the TCP/IP suite is to use a DHCP server to automatically distribute IP addresses. DHCP can also inform clients of the appropriate DNS servers and gateways to use. A DHCP server not only simplifies client configuration, but it also saves headaches for the poor soul who would otherwise have to track the use of IP addresses, because it manages the database of available IP addresses dynamically and automatically.

Dynamic addressing using DHCP is the Windows 2000 default setting. If you need to check this or change a statically assigned host to a dynamically configured host, follow these steps:

1. Select the Internet Protocol (TCP/IP) component in your Local Area Connection Properties dialog box, and click Properties (Figure 6-7).

![Figure 6-7. The General tab of the Internet Protocol (TCP/IP) Properties dialog box.](image)
2. Select the Obtain An IP Address Automatically option. However, don’t select this option on a machine that is to act as a DHCP server. A DHCP server must have a fixed, static IP address.

3. Select the Obtain DNS Server Address Automatically option if your DHCP server is set up to provide the DNS server addresses to clients; otherwise, select the Use The Following DNS Server Addresses option, and enter the IP addresses for the DNS servers you want to use.

Real World Assigning IP Addresses for DNS and WINS Servers

When setting up a DNS or WINS server, it’s tempting to use a static IP address. Although this is an acceptable use of static IP addresses, a better method for many networks is to allow the server to obtain an address from the DHCP server and then create an IP reservation for the server with an unlimited lease duration on the DHCP server. This step gives the server a permanent lease on the IP address it was assigned, ensuring that the IP address of the DNS server won’t change, at the same time allowing the DHCP administrator to easily take back the address if the server is moved or decommissioned. See Chapter 14 for information on creating reservations on a DHCP server.

Using Static Addressing

If your network doesn’t have a DHCP server or if you’re setting up a DHCP server, you need to manually configure TCP/IP to use a static IP address and DNS information. To do this, obtain an IP address from the person who maintains the database of IP addresses that your organization can use. If using DHCP, all DHCP servers also need to be updated to exclude your static IP address.

To set up a system with a static IP address, follow these steps:

1. Select the Internet Protocol (TCP/IP) component in the Local Area Connection Properties dialog box, and click Properties.

2. Select the Use The Following IP Address option, enter the address you obtain in the IP Address text box, and then press Tab to automatically fill in the default subnet mask. Most likely, you’ll be able to use the default subnet mask, but if your network is using a specific subnet mask, you need to find the proper mask and enter it in the Subnet Mask text box.

3. Enter the IP address for your default gateway or router in the Default Gateway text box. The default gateway forwards, or routes, any traffic
destined for hosts outside your local subnet, possibly to another portion of your wide area network (WAN) or to the Internet.

4. Choose the Use The Following DNS Server Addresses option to specify the IP addresses for your DNS servers. Enter the primary and secondary DNS server addresses in the text boxes provided.

**Note** The DNS service is critical for resolving host names such as http://www.microsoft.com into IP addresses that your computer can access. Without the DNS service, users could access resources only by typing in their IP addresses directly or by broadcasting their NetBIOS names (which only works on local subnets and consumes lots of network bandwidth).

**Setting Advanced TCP/IP Options**

If you aren’t using a DHCP server to configure your server’s IP address and associated settings and you need to enter other settings besides just your server’s IP address and DNS servers, select Advanced in the TCP/IP Properties dialog box. This opens the Advanced TCP/IP Settings dialog box, shown in Figure 6-8, which you use to specify additional settings, including WINS servers, NetBIOS over TCP/IP, and optional TCP/IP parameters. Chapter 13 contains more information about configuring TCP/IP.

**Figure 6-8.** The IP Settings tab of the Advanced TCP/IP Settings dialog box.

**Configuring IP Settings** The Advanced TCP/IP Settings dialog box contains four tabs, the first of which is the IP Settings tab. You use this tab to add the IP address
and subnet mask for your network connection and the gateways your server should use. To change the options on this tab, follow these steps:

1. Use the Add, Edit, and Remove buttons in the IP Addresses box to modify your IP address and subnet mask settings.
2. To add a default gateway or router, click Add and enter the IP address for the router.
3. Now add the interface metric for the connection. The interface metric assigns a relative cost to using a particular router to access a particular IP address. Assign lower interface metrics with routers connecting to fast networks, such as another section of a local network; assign higher numbers to slower connections, such as an Integrated Services Digital Network (ISDN) or a slow digital subscriber line (DSL) connection to the Internet.

**Configuring DNS Settings**

Click the DNS tab to access the advanced DNS settings for your network connection, as shown in Figure 6-9. Then use the following procedure to configure your DNS settings:

1. Use the Add, Edit, and Remove buttons in the DNS Addresses box to add or modify the DNS servers you want to use for this connection. Use the up and down arrows next to the box to change the order in which your server queries the DNS servers.
2. Select the appropriate options for unqualified names:
   - **Append Primary And Connection Specific DNS Suffixes**  Limits the resolution for unqualified names to the domain suffixes and connection-specific suffixes. If your primary DNS suffix is eng.scribes.com and you type `ping srv4` at a command prompt, DNS looks for `srv4.eng.scribes.com`. If you also specify a connection-specific name (under DNS Suffix For This Connection), such as dev.scribes.com, DNS queries `srv4.eng.scribes.com` and `srv4.dev.scribes.com`.
   - **Append Parent Suffixes Of The Primary DNS Suffix**  Includes parent suffixes up to the second-level domain in the resolution of unqualified names. So if the primary DNS suffix is eng.uk.corp.scribes.com and you type `ping srv4` at a command prompt, DNS queries for the following:
     - `srv4.eng.uk.corp.scribes.com`
     - `srv4.uk.corp.scribes.com`
     - `srv4.corp.scribes.com`
     - `srv4.scribes.com`
Append These DNS Suffixes (In Order)  Specifies the only domain suffixes to be appended to unqualified domain names during the name resolution process. If you specify domain suffixes here, the primary and connection-specific suffixes are not used.

Figure 6-9. The DNS tab of the Advanced TCP/IP Settings dialog box.

3. To override the parent DNS domain name specified for your computer in the Network Identification tab of the System Properties Control Panel tool, type the DNS domain name you want to use in the DNS Suffix For This Connection text box.

4. To prevent the full DNS name of your server's IP address from being registered with the DNS server, clear the Register This Connection’s Addresses In DNS check box.

5. To register the IP addresses of your network connections in DNS based on the domain name of the connections as well as by the fully qualified domain name (FQDN) for your server, select the Register This Connection’s DNS Suffix In DNS Registration check box. The domain name of the connection is entered in the DNS Suffix For This Connection text box or assigned by the DHCP server.

Configuring WINS Settings  To configure the WINS settings for your computer, click the WINS tab in the Advanced TCP/IP Settings dialog box (Figure 6-10). If WINS servers are operating on your network, you should add their addresses here. Doing so gives you the best results when communicating with hosts that are running Microsoft operating systems earlier than Windows 2000. As with the other tabs in the Advanced TCP/IP Settings dialog box, use the Add, Edit, and Remove
buttons to modify your WINS server list. For a more thorough discussion of when to use WINS servers on your network, see Chapter 14.

Figure 6-10. The WINS tab of the Advanced TCP/IP Settings dialog box.

To enable the use of an Lmhosts file for resolving NetBIOS names to IP addresses, select the Enable LMHOSTS Lookup check box, and click Import LMHOSTS to import an Lmhosts file. We recommend using Lmhosts files only when absolutely necessary because trying to keep them up-to-date can be tricky—the minuscule reduction of network traffic that Lmhosts files offer isn’t worth it.

Tip When you configure a WINS server, use the Ipconfig command at a command prompt to obtain your current IP address, and then enter that address in the WINS Addresses field. Don’t enter any other WINS server in this field; you don’t want your WINS server registering its NetBIOS name with another WINS server if WINS hasn’t started in time to respond at bootup.

In all likelihood, you’ll need to communicate with clients that are running Microsoft operating systems earlier than Windows 2000, so make sure the Enable NetBIOS Over TCP/IP option is selected. Disable this only if you communicate exclusively with other computers running Windows 2000 or computers that rely solely on DNS for name resolution services (for example, UNIX). Also, note that any applications that use NetBIOS won’t work if you disable NetBIOS Over TCP/IP.
Configuring TCP/IP Options  If you need to configure any TCP/IP options, click the Options tab in the Advanced TCP/IP Settings dialog box. Select an option you want to configure, and then click Properties. For more information about TCP/IP properties and secure TCP/IP connections, see Chapter 13.

Configuring NWLink IPX/SPX

The NWLink IPX/SPX protocol was designed as an easy-to-use-and-configure, routable protocol that is compatible with NetWare’s IPX/SPX protocol. As such, it used to be a popular protocol in many companies and can still be useful in maintaining interoperability with older network environments. For detailed information about interoperating with NetWare, see Chapter 21.

Fortunately, configuring the NWLink IPX/SPX protocol is easy. Just follow these steps:

1. Install the protocol in the Local Area Connection Properties dialog box, which can be accessed by right-clicking the Local Area Connection icon in the Network and Dial-Up Connections folder and then selecting Properties.

2. Select the protocol and click Properties.

3. To advertise the services running on your server (such as File and Print Services For NetWare or IPX routing) to native NetWare clients, enter a unique eight-digit hexadecimal number in the Internal Network Number text box (Figure 6-11) to identify your server.

4. In most cases, you can also let Windows 2000 handle your frame type detection by selecting the Auto Frame Type Detection option. Windows 2000 then detects the proper frame type by sending out a Routing Information Protocol (RIP) request for all frame types and then waiting for a response. The frame type for which Windows 2000 received a response then becomes the default. If responses are received for multiple frame types, Windows 2000 sets the default frame types for which the responses were received in this order: Ethernet 802.2, Ethernet 802.3, Ethernet II, Sub-Network Access Protocol (SNAP).

5. If you want to specify the frame type manually or add multiple frame types, select the Manual Frame Type Detection option, select Add, and then choose a frame type and enter the network number for that frame type.


### Configuring Storage

Microsoft recommends that you partition and format only the system partition during Windows installation, and that you exclusively use the NTFS file system (no FAT), and we back them up on this recommendation. The Disk Management snap-in is a much more elegant and efficient way of partitioning and formatting disks and volumes than is Windows Setup, and we recommend that you do as many of your disk management chores as possible after Setup completes.

The chores that you will likely need to perform include partitioning and formatting the rest of the computer’s hard disk(s), as well as possibly setting up software-based redundant arrays of independent disks (RAIDs), stripe sets, or mirror sets. In the interest of reducing redundancy (in this book), we refer you to Chapter 17, where these tasks (and others) are covered in detail.

### Using the Windows 2000 Configure Your Server Tool

The Windows 2000 Configure Your Server tool provides a central location that you can use to install and manage most of the important server tools, such as Microsoft Active Directory, DHCP, DNS, and WINS. However, given the sometimes bewildering number of administrative tools and Microsoft Management Console (MMC) snap-ins available, having an organized and central location...
from which to access all of these tools is crucial. You don’t actually use the Con- 
figure Your Server tool to perform many actions, but it serves as an interface for 
launching the various MMC snap-ins that you use to accomplish your tasks.

The Windows 2000 Configure Your Server tool appears when you first boot your 
server after completing Setup. If it doesn’t appear, set up any additional devices 
and prepare any additional drives you need for your server programs and data, 
and then launch the Windows 2000 Configure Your Server tool from the Admin-
istrative Tools folder on the Programs menu.

In the Configure Your Server tool, use the topics on the left to choose the services 
you want to configure, and click the hyperlinks and buttons to set up and con- 
figure these services. The Configure Your Server tool launches any necessary 
wizards to walk you through installing the services you select.

Choosing Whether to Set Up a Domain Controller

The first screen in the Windows 2000 Configure Your Server tool asks whether 
your server is the only one on your network (Figure 6-12). When you create a new 
network and this is the first server on the network, choose the This Is The Only 
Server In My Network option. (See the “Configuring the First Server on Your 
Network” section later in this chapter for more information.) This selection sets 
up your server as a domain controller and installs Active Directory, DHCP, and 
DNS on your server. Otherwise, choose the One Or More Servers Are Already 
Running In My Network option. Choosing this option allows you to pick exactly 
which services you want to install on your system. After choosing an option, click 
Next to continue.

Figure 6-12. The first screen of the Configure Your Server tool.
You should be extremely careful about adding a domain controller to an existing Windows NT 4 network. Before you can add any Windows 2000 domain controllers to an existing Windows NT 4 domain, you must upgrade the primary domain controller (PDC) to Windows 2000. This upgrade is required because Windows NT domains are single-master networks where the PDC contains the master records for the domain. Windows 2000 servers use full, multimaster replication, and each domain controller acts as a master repository for domain information. If you add a Windows 2000 server or upgrade any machine other than the PDC on an existing Windows NT domain, you'll create a new Windows 2000 domain that looks like the existing domain but is not the same domain. The Windows 2000 domain controller that will work as the PDC for the network won’t have the same security identifier (SID) as the PDC of the Windows NT 4 domain you were trying to upgrade. The result is a “network” that doesn’t work. Therefore, you must upgrade the PDC on a Windows NT domain to Windows 2000 before attempting to install any other iterations of Windows 2000 Server as domain controllers (member servers can be added at any point).

**Tip**  When upgrading a PDC to Windows 2000, be sure the server’s hardware is capable of handling the upgrade. If there’s any doubt about whether your existing PDC can function with the additional load, you can do a little juggling by promoting a backup domain controller (BDC) that you’re sure of to be the PDC. Then upgrade the new PDC to Windows 2000. See Chapter 7 for more information on upgrading servers.

### Configuring the First Server on Your Network

If you’re creating a new network or domain and you’re setting up the first server in the domain, the Windows 2000 Configure Your Server tool can guide you through the configuration process. Just follow these steps:

1. In the first window of the Windows 2000 Configure Your Server tool, choose the This Is The Only Server In My Network option, and click Next (as discussed in the previous section). Choosing this option helps you configure your server as a domain controller running Active Directory, DHCP, and DNS.
2. Click the Show More Details link to view information about how your server’s TCP/IP services will be configured, and then click Back.
3. Click Next, and then enter the domain name you want to use in the first text box, as shown in Figure 6-13.
Part II  Installation and Initial Configuration

Figure 6-13. Entering your domain name using the Configure Your Server tool.

4. To use an Internet-registered domain name (such as scribes.com) as the root for your fully qualified domain name, enter the Internet domain name in the second text box. Or, to specify that your domain is a local domain that isn’t a part of an Internet-registered domain, type local in the second text box.

5. Verify that the Active Directory and downlevel domain names are correct in the preview boxes at the bottom of the window, and then click Next.

6. Click Next again. Active Directory, DHCP, and DNS are installed in Unattended mode and Windows restarts. Once logged on, Windows displays the Windows 2000 Configure Your Server tool again. (See Chapter 11 for help with any Active Directory installation questions you are asked, or see the sections on installing DHCP and DNS in Chapter 14 for help with DHCP and DNS questions.)

7. Configure your server to use the static IP address specified in the Windows 2000 Configure Your Server tool. To do this, right-click the Local Area Connection icon in the Network and Dial-Up Connections folder, and choose Properties from the shortcut menu. Select Internet Protocol (TCP/IP), and click Properties. Then enter the proper IP address and subnet mask, and verify that the DNS server addresses include your server’s IP address.

8. Open DHCP Manager and expand the DHCP server.

9. Select the DHCP server and choose All Tasks-Authorize from the Action menu.
10. Reboot your computer, and then use the Windows 2000 Configure Your Server tool to add any other services you need.

Real World Special Facts About Windows 2000 Domain Controllers
Although it’s true that all Windows 2000 domain controllers are equal, some are more equal than others. The first Windows 2000 domain controller is automatically assigned the role of Global Catalog server. At least one Global Catalog server is needed on every domain. The Global Catalog is a database that contains a full replica of all directory objects in its host domain plus a partial replica of all directory objects in every domain in the forest. The Global Catalog’s role is to enable the finding of directory information and to provide universal group membership information during logon. After additional controllers are installed, you can reassign the role of Global Catalog server or designate more than one machine as a Global Catalog server. This process is described in Chapter 11.

The first domain controller is also assigned the operations master roles. A single controller must perform each of these roles because they are functions that can’t be executed in different places at the same time. (For example, a single controller must handle the creation of security identifiers to ensure that each identifier is unique.) Under most circumstances, you won’t have to change the location for any of the operations master roles, but you should be familiar with each of the roles and what happens in the case of failure. See Chapter 12 for information on operations master roles.

Performance and Memory Tuning
Although the Windows 2000 Server family of operating systems is self-tuning, there are a few settings that you might want to modify to maximize the performance of a server. To adjust the way Windows 2000 Server optimizes its memory, page file, and visual settings, use the following procedure:

1. Double-click the System icon in the Control Panel.
2. Click the Advanced tab and then click Performance Options.
3. In the Optimize Performance For section, choose the Background Services option.
4. Click Change in the Virtual Memory section to open the Virtual Memory dialog box, shown in Figure 6-14.
5. Select the drive for which you want to adjust virtual memory settings.

6. Enter the Initial Size and Maximum Size for the page file and then click Set. Use the following guidelines for optimizing page file sizes:

   - Create a page file on the system (most likely C:\) partition with the initial size and maximum size set to the amount of installed physical RAM. This allows the system to create a memory dump in the event of a system crash.

   - In addition to the page file on the system partition, allocate space for the page file on the fastest drive or drives in the system. Placing it on multiple physical drives improves performance, unless the drives are slow or heavily used (avoid these). Placing page files on multiple partitions on the same drive doesn’t improve performance.

   - Place the page file on the fastest drive available. You might want to avoid software or hardware-based RAID volumes, as the data redundancy might reduce performance. Instead pick a simple volume, stripe set, or mirrored volume.

   - Create a page file in its own logical partition or in a partition before any data is written to it. This minimizes page file fragmentation. Alternatively, defragment the partition before creating the page file to ensure that the page file is allocated a contiguous area on the hard drive.
If there is plenty of disk space available, set the initial size and maximum size to the same value. This reduces page file fragmentation because additional hard disk space doesn’t have to be allocated for the page file at a later time.

Use the Page File Bytes counter in Performance Monitor to determine how much virtual memory is consumed under the heaviest usage conditions, and then use this amount to set the initial size, and possibly the maximum size (after increasing the number to anticipate increased future demands).

Tip Microsoft recommends that virtual memory be equal to 1.5 times the amount of physical RAM installed in the server. Web servers don’t usually require much virtual memory, so half the physical RAM size would be sufficient, but we like to err on the too big side, say three-fourths as a minimum. Database and other application servers often need lots of virtual memory, so consider setting the virtual memory setting to twice the amount of physical RAM installed.

7. Click OK when finished, and then restart the computer.
8. Click Start, select Settings, and then choose Network And Dial-Up Connections.
9. Right-click the internal network connection and choose Properties from the shortcut menu.
10. Select File And Printer Sharing For Microsoft Networks and then click Properties.
11. Select the memory optimization method that the server should use, as described here and shown in Figure 6-15:
   - **Minimize Memory Used** The best setting for servers that service only a limited number of clients (say 10 or so) or have a limited amount of RAM (less than 160 MB). This setting uses the least amount of RAM for caching.
   - **Balance** Uses somewhat more RAM for caching, improving file sharing speed while still leaving lots of RAM available for applications. This setting is a good choice for domain controllers.
   - **Maximize Data Throughput For File Sharing** This is the default setting and is appropriate for servers that mainly act as file servers. It allocates the largest amount of RAM for the system cache, maximizing file sharing performance but reducing the amount of available RAM for other programs.
Maximize Data Throughput For Network Applications  Allocates a small amount of RAM for the system cache, making as much RAM available for server-based applications as possible while still ensuring good connectivity for clients. This setting is appropriate for servers that run network applications such as Microsoft SQL Server or Microsoft Exchange Server.

12. Click OK when finished.

![File and Printer Sharing for Microsoft Networks Properties](image)

**Figure 6-15. Optimizing memory usage for File and Printer Sharing.**

---

**Updating Windows**

It’s important to update Windows 2000 with the latest service pack and any security updates and hot fixes that are appropriate for the server and your network (this is a key point—applying every hot fix that comes out of Redmond could actually decrease your stability). We recommend that you stay on top of the service packs, and deploy only hot fixes and security updates that fix problems you’re currently experiencing.

To update Windows, follow these guidelines:

- Install the latest service pack. (You don’t have to go out and grab it right away. In general, though, it’s a good idea not to fall more than one service pack behind.) You can download the latest service packs
from Windows Update, or Microsoft Corporate Windows Update (http://corporate.windowsupdate.microsoft.com), among other locations.

- Install any security hot fixes that are important for your server and network. Web servers will need to install many (if not most) of the security updates to stay secure; internal file servers will infrequently need hot fixes. We recommend that you evaluate and test any hot fix before deploying it.
- Install a newer version of Microsoft Internet Explorer if Web browsing will be done locally on the server. The version of Internet Explorer that ships with Windows 2000 has a number of security holes and should be updated.

---

**Securing Windows**

Entire books could be (and have been) written about securing Windows 2000 Server, and rightly so; it’s an important topic (and one that we devote considerable space to, including Chapters 18 and 19). We won’t launch a big security discussion here, but some security precautions are necessary before considering your server “online.” Here’s what Microsoft recommends (for a detailed explanation of these suggestions, see http://www.microsoft.com/technet/security/tools/w2ksvrcl.asp, or refer to the appropriate sections of this book):

- Eliminate FAT (make sure all hard disk partitions are using NTFS).
- Rename the administrator account and create a strong password for it (and use a different password for each server).
- Set appropriate password policies and account lockout policies for your network.
- Disable unnecessary services, especially Internet Information Services. If not doing file or printer sharing, disable the Server service.
- Don’t install unnecessary applications such as e-mail, Microsoft Office, or utilities.
- Disable unnecessary accounts.
- Check folder permissions.
- Disable the Guest account.
• Protect the registry from anonymous access.
• Apply appropriate registry access control lists (ACLs).
• Restrict access to the Local System Authority (LSA).
• Remove unnecessary file shares.
• Install antivirus software and the latest virus definition files.
• Install the latest service pack.
• Install security hot fixes as appropriate for your network.
Summary

If you put in the planning time recommended in the first part of this book, it’s probably paying off around now. Although the configuration of various services and protocols is relatively complex, primarily because of the interdependencies among them, you should have a good idea of which services and protocols will best suit the needs of your network in a Windows 2000 environment. In the next chapter, we address the general topic of upgrading existing systems to Windows 2000 and tying them into the network.