ONE

Introduction to TCP/IP

In this chapter we will look at the terminology of TCP/IP, its history and perspectives. We will speak about installation of TCP/IP on a Windows 2000 computer and briefly cover major TCP/IP utilities that are used to test the installation. We will also discuss Microsoft Network Monitor, which helps you diagnose and troubleshoot many TCP/IP related problems.

TCP/IP Basics

TCP/IP stands for Transmission Control Protocol/Internet Protocol and it's an industry-standard suite of protocols designed for wide area networks (WANs). Since the Internet is an example of a WAN, we can say that TCP/IP is the protocol suite for the Internet also. The most common mistake is to think that TCP/IP is one protocol or two (TCP and IP). As we will see, the TCP/IP abbreviation implies several protocols. Among them are some that you might already have heard about: HTTP (Hypertext Transfer Protocol) which is used to navigate World Wide Web, FTP (File Transfer Protocol) protocol that provides reliable file transfer over the Internet, and SMTP (Simple Mail Transfer Protocol) which supports email communications. Some of the protocols that are included in the TCP/IP suite are quite exotic, for example ICMP, SNMP, and TFTP.

Although many of the ideas associated with TCP/IP are quite new, the technology itself has been with us for a relatively long time.

Table 1.1 presents some of the major milestones in TCP/IP technology.

TABLE 1.1 *TCP/IP History*

Year	Event
1969	The Department of Defense Advanced Research Projects Agency (ARPA) creates an experimental network called ARPANET. This network provides a test-bed for emerging network technologies. ARPANET originally connected four universities and enabled scientists to share information and resources across long distances. ARPANET continued to expand, connecting many more sites throughout the 1970s and 1980s.
1972	The National Center for Supercomputing Applications (NCSA) develops the *telnet* application for remote login, making it easier to connect to a remote computer.
1973	FTP (File Transfer Protocol) is introduced, standardizing the transfer of files between networked computers.
1974	The Transmission Control Protocol (TCP) specified in detail. Later revised in RFC 793.
1981	The IP standard specified and published in RFC 791.
1982	Transmission Control Protocol (TCP) and Internet Protocol (IP) established as the TCP/IP Protocol Suite.
1983	The TCP/IP suite of networking protocols, or rules, becomes the only set of protocols used on the ARPANET. This decision sets a standard for other networks, and generates the use of the term "Internet" as the network of networks which either use the TCP/IP protocols or are able to interact with TCP/IP networks. To keep military and nonmilitary network sites separate, the ARPANET splits into two networks: ARPANET and MILNET.
1984	Domain Name System (DNS) elaborated and introduced.
1985-86	The National Science Foundation (NSF) connects the nation's six supercomputing centers. This network is called the NSFNET, or NSFNET backbone.
1990	The ARPANET is dissolved.
1993	The European Laboratory for Particle Physics in Switzerland (CERN) releases the World Wide Web (WWW), developed by Tim Berners-Lee. The WWW uses Hypertext Transfer Protocol (HTTP) and hypertext links, changing the way information can be organized, presented, and accessed on the Internet.

Standards and How They Appear

As you can see, TCP/IP has a rich history. Today, TCP/IP is often associated with the Internet. Its architecture and design are closely bound with Internet advances and growth. Since, however, there is no organization that owns the Internet, you might ask how this whole system is controlled. There are organizations that are responsible for setting up standards and controlling the advance of the TCP/IP technologies. Some examples are The Internet Society and The Internet Architecture Board.

INTERNET SOCIETY (ISOC)

The **I**nternet **SOC**iety (http://www.isoc.org/) is a professional membership society with more than 150 organizational and 6,000 individual members in over 100 countries. It provides leadership in addressing issues that confront the future of the Internet, and is the organization home for the groups responsible for Internet infrastructure standards, including the Internet Engineering Task Force (IETF) and the Internet Architecture Board (IAB). ISOC's members are bound by a common stake in maintaining the viability and global scaling of the Internet. They comprise the companies, government agencies, and foundations that have created the Internet and its technologies as well as innovative entrepreneurial organizations contributing to maintain that dynamic. The Society is governed by its board of trustees elected by its membership around the world.

INTERNET ARCHITECTURE BOARD

The IAB is a technical advisory group of ISOC. Some issues discussed during IAB meetings are:

- The future of Internet addressing
- Architectural principles of the Internet
- Management of top level domains in the Domain Name System
- International character sets
- Charging for addresses

The IAB governs the Internet Engineering Task Force (IETF) (http://www.ietf.cnri.reston.va.us/), Internet Assigned Number Authority (IANA) (http://www.iana.org/), and Internet Research Task Force (IRTF) (http://www.irtf.org/).

REQUESTS FOR COMMENTS

You may wonder how the groups' decisions are documented. Requests for Comments (RFCs) are a series of notes, started in 1969, about the Internet (originally the ARPANET). The notes discuss many aspects of computing and computer communication focusing on networking protocols, procedures, pro-

grams, and concepts, but also include meeting notes, opinion, and sometimes humor. TCP/IP standards are always published as RFCs.

Warning Although TCP/IP standards are always published as RFCs, not all RFCs specify standards. Some of them have *Limited use* or even *Not recommended* status.

When a document is published, it is assigned an RFC number. The original RFC number is never updated, but when changes are required, a new RFC is issued with a new number. Therefore, when you are looking for information in RFCs, be sure that you have the most recent one.

Note You can find the text of the RFCs at www.cis.ohio-state.edu/htbin/rfc. You can also find links to RFC sites as well as a wealth of Internet information at www.internic.net.

Advantages of TCP/IP

As TCP/IP has become the industry standard protocol suite, many software vendors have included TCP/IP support in their products. Let's take a closer look at the Microsoft implementation of TCP/IP. Because of its myriad advantages, TCP/IP is the default protocol for Windows 2000. This text will explore the advantages that drove Microsoft to select TCP/IP for that role.

Modern networks are large and complex. They are connected with routers and need reliable protocols to communicate. Implementing TCP/IP in a corporate network gives you a standard, routable environment. Since TCP/IP offers robust, scalable architecture, you can easily expand your network. This is why most of today's large networks rely on TCP/IP.

Imagine a large enterprise network with hundreds of computers, many of which work under different operating systems such as Microsoft Windows NT, Windows 2000, UNIX, and Novell NetWare. The typical problem is to connect all these computers so users can seamlessly exchange information. Obviously, this situation requires common protocols as well as connectivity utilities and tools to access and transfer data. Since TCP/IP is supported by all modern operating systems, it has become the logical choice when connecting dissimilar systems. In addition to a common network protocol, however, compatible applications are needed on both ends. Microsoft TCP/IP includes useful utilities that provide access to foreign hosts for data transfer, monitoring, and remote control. For example: FTP, tracert, and telnet.

Remember, also, that the Internet is based on TCP/IP. The TCP/IP protocol running on a Windows 2000 computer allows it to gain Internet access (assuming, of course, it has physical connectivity to the Internet).

Finally, Microsoft TCP/IP offers the Windows Sockets Interface, which can be used for developing client/server applications that can run on Windows Sockets-compliant stacks from other vendors. By using Sockets, TCP/IP provides a robust, scalable, cross-platform client/server framework.

To summarize:

- TCP/IP is an industry-standard suite of networking protocols.
- TCP/IP is a routable transport for Windows 2000 networks.
- TCP/IP provides the ability to share information with non-Microsoft network TCP/IP-based hosts.
- TCP/IP provides the ability to log on to remote TCP/IP-based hosts from a Windows 2000 computer.
- TCP/IP adheres to Internet-community standards, providing access to thousands of networks worldwide.

TCP/IP Utilities and Services

We have already seen that the Microsoft implementation of TCP/IP provides a way to access foreign hosts, tune the TCP/IP configuration, and troubleshoot connectivity problems. This is achieved through a number of tools and utilities. Knowing how to use the utilities often helps you to solve network-related problems. To get started, we'll identify the purpose of the most important Microsoft TCP/IP utilities (we will cover them in greater detail later in the book).

Microsoft TCP/IP utilities can be logically divided into groups based on their purpose: data transfer utilities, remote execution utilities, printing utilities, and diagnostic utilities.

DATA TRANSFER UTILITIES

These tools allow you to transfer data between two computers. The computers can be located anywhere as long as there is a TCP/IP connection between them.

TABLE 1.2 *TCP/IP Data Transfer Utilities*

Utility	Function
File Transfer Protocol (FTP)	Provides bidirectional file transfers between two TCP/IP hosts. One host is acting as an FTP server, while another is acting as a client.
Trivial File Transfer Protocol (TFTP)	Provides bidirectional file transfers between two TCP/IP hosts where one is running TFTP server software.
Remote Copy Protocol (RCP)	This connectivity command copies files between a Windows 2000 computer and a system running **rshd**, the remote shell server. The **rshd** server is available on UNIX computers, but not on Windows 2000, so the Windows 2000 computer can only participate as the system from which the commands are issued.

REMOTE EXECUTION UTILITIES

These utilities provide the ability to launch applications and processes on remote hosts.

TABLE 1.3 *TCP/IP Remote Execution Utilities*

Utility	Function
Telnet	Provides terminal emulation to a TCP/IP host running Telnet server software. When you connect, your computer acts as if your keyboard were attached to the remote computer. This means that you can run programs on a computer on the other side of the world, just as if you were sitting in front of it.
Remote Shell (RSH)	Runs commands on remote computers running the RSH service. Runs commands on a UNIX host.
Remote Execution (REXEC)	This connectivity command runs commands on remote hosts running the **REXEC** service. **REXEC** authenticates the user name on the remote host by using a password, before executing the specified command.

PRINTING UTILITIES

TCP/IP printing utilities provide a way to submit, receive, and manage print jobs in a TCP/IP environment. TCP/IP printing utilities allow, in particular, Microsoft-based clients to submit print jobs for printers connected to UNIX computers.

TABLE 1.4 *TCP/IP Printing Utilities*

Utility	Function
Line Printer Remote (LPR)	LPR lets a client application on one computer send a document to a print spooler service on another computer. The client application is usually named LPR and the service (or daemon) is usually named LPD.
Line Printer Queue (LPQ)	This diagnostic utility is used to obtain the status of a print queue on a host running the LPD server.
Line Printer Daemon (LPD)	A line printer daemon (LPD) service on the print server receives documents from line printer remote (LPR) utilities running on client systems. With LPD installed, a Windows 2000 Server can receive print jobs from UNIX-based computers.

DIAGNOSTIC UTILITIES

In addition to the data transfer utilities we've already discussed, Windows 2000 provides tools for diagnosing TCP/IP related problems. Table 1.5 describes the major diagnostics utilities that are included in the Microsoft TCP/IP implementation.

TABLE 1.5 *TCP/IP Diagnostic Utilities*

Utility	Function
Finger	Displays information about a user on a specified system running the Finger service.
Address Resolution Protocol (ARP)	Displays and modifies the cache of locally resolved IP addresses to Media Access Control (MAC) addresses.
NBTSTAT	Displays protocol statistics and current TCP/IP connections using NetBIOS over TCP/IP. This utility is also used to determine the registered NetBIOS name and to view the local name cache.
Packet InterNet Groper (PING)	Verifies the availability of the remote host by sending the echo request and analyzing replies.
TRACERT	Traces the route for packets from local hosts to the specified remote host.
IPCONFIG	Displays current TCP/IP configuration including IP address(es) and DNS and WINS addresses.
HOSTNAME	Returns the local computer's host name. You can use it in logon scripts for identification.
NSLOOKUP	Displays information from DNS name servers about a particular host or domain. You can also use this utility to check the availability of the domain name.
NETSTAT	Displays protocol statistics and current TCP/IP network connections.
ROUTE	Views and modifies the local routing table.

Installing Microsoft TCP/IP on Windows 2000

Now that you're sold on TCP/IP, let's see how TCP/IP can be installed on your computer. Before we proceed, we need to decide on parameters.

TABLE 1.6 *TCP/IP Parameters*

Parameter	Description
IP address	An IP address is a logical 32-bit address that is used for the unique identification of a TCP/IP host. For your convenience the 32-bit value is divided into 4 octets, 8 bits in each, and written in the decimal form. An example of an IP address is **137.200.0.10**. Each computer running TCP/IP must have a unique IP address.
Subnet mask	A subnet mask is used to determine the network ID. When TCP/IP hosts communicate the subnet mask is used to determine whether the destination host is located on a local or remote network. An example of a subnet mask is **255.255.0.0**. Each computer running TCP/IP must have a subnet mask.
Default gateway	If your network consists of two or more segments connected by routers the default gateway address must be provided in order to access the other segment(s). TCP/IP packets, destined for remote networks, are sent to the default gateway if there is no route configured on the local host. Although this parameter is optional, communication will be limited to the local network segment if the default gateway address is omitted.

Automatic Configuration

If your network supports a *dynamic* TCP/IP configuration, an automatic TCP/IP configuration takes place when Windows 2000 is installed. A dynamic configuration, based on the Dynamic Host Configuration Protocol (DHCP), is usually used if another computer on your network is installed as a DHCP server. The DHCP server can provide the IP address, subnet mask, default gateway (IP router), DNS domain name, DNS server, and WINS server configuration information.

The Windows 2000 *Media Sense* feature permits the network interface card to detect when it is physically moved from one network segment to another (assuming the card supports this feature). The computer uses Media Sense to effect a reconfiguration of dynamic network parameters without rebooting.

It is possible to configure TCP/IP for automatic addressing after Windows 2000 is installed. You must be logged on as an administrator or a member of the administrators' group in order to complete this procedure:

1. From the **Start** menu open **Settings** and launch **Network** and **Dial-up Connections**.
2. Right-click the network connection that you want to configure, and then click **Properties** (see Figure 1-1).

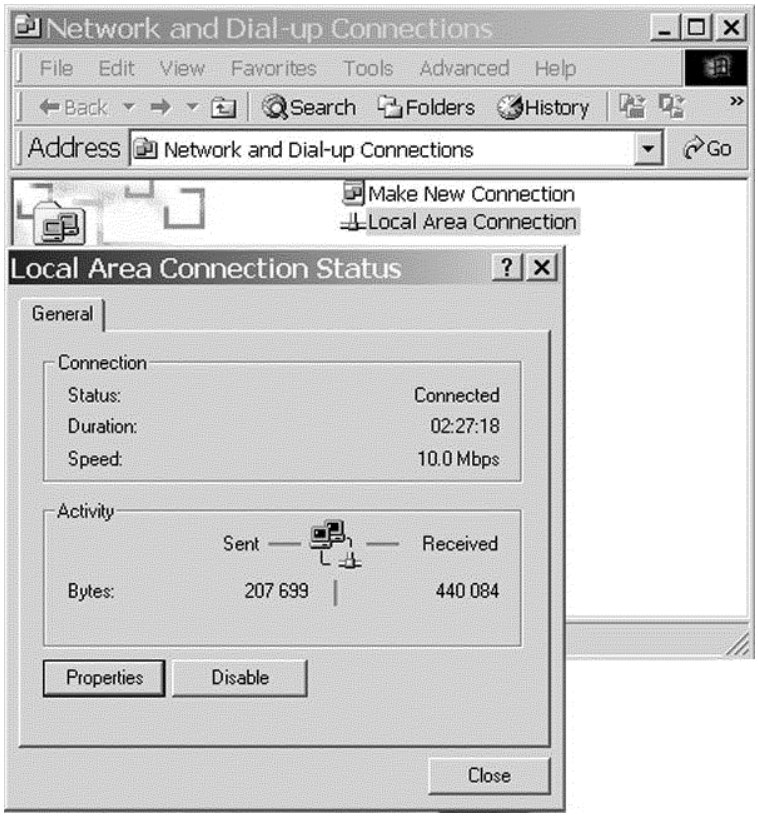

FIGURE 1–1 *Configuring TCP/IP for automatic addressing (Steps 1 and 2)*

3. On the **General** tab (for a local area connection) or the **Networking** tab (all other connections), click **Internet Protocol (TCP/IP)**, and then click **Properties**.
4. Click **Obtain an IP address automatically**, and then click **OK** (see Figure 1-2).

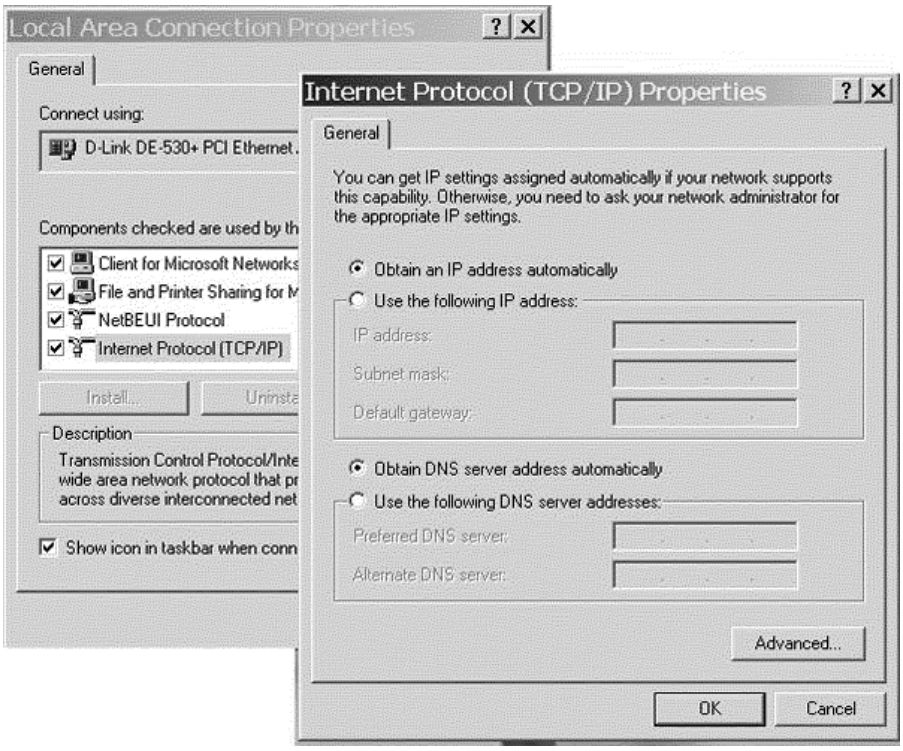

FIGURE 1–2 *Configuring TCP/IP for automatic addressing (Steps 3 and 4)*

Manually Configuring TCP/IP

You also have the opportunity to install TCP/IP after Windows 2000 is operational. To set up TCP/IP manually you need to define the IP address and subnet mask. Be sure to keep track of the assigned parameters.

Important IP addresses and subnet masks cannot be assigned arbitrarily. The process of assigning TCP/IP parameters requires planning and following certain rules. For now, we may assume we've already calculated these parameters. We will learn all about them in the following chapters.

Once you have decided on an IP address and subnet mask, you are ready to install TCP/IP. You must be logged on as an administrator or a member of the administrators' group in order to complete this procedure.

1. From the **Start** menu point to **Settings**, and then click **Network and Dial-up Connections**.

Tip You can quickly launch the Network and Dial-up Connections dialog box by right-clicking the My Network Places icon on the desktop and choosing Properties.

2. Right-click the network connection for which you want to install and enable TCP/IP, and then click **Properties**.
3. On the **General** tab (for a local area connection) or the **Networking** tab (all other connections), if **Internet Protocol (TCP/IP)** is not in the list of installed components, then do the following (see Figure 1-3):
   a. Click **Install**.
   b. Click **Protocol**, and then click **Add**.
   c. In the **Select Network Protocol** dialog box, click **Internet Protocol (TCP/IP)**, and then click **OK**.

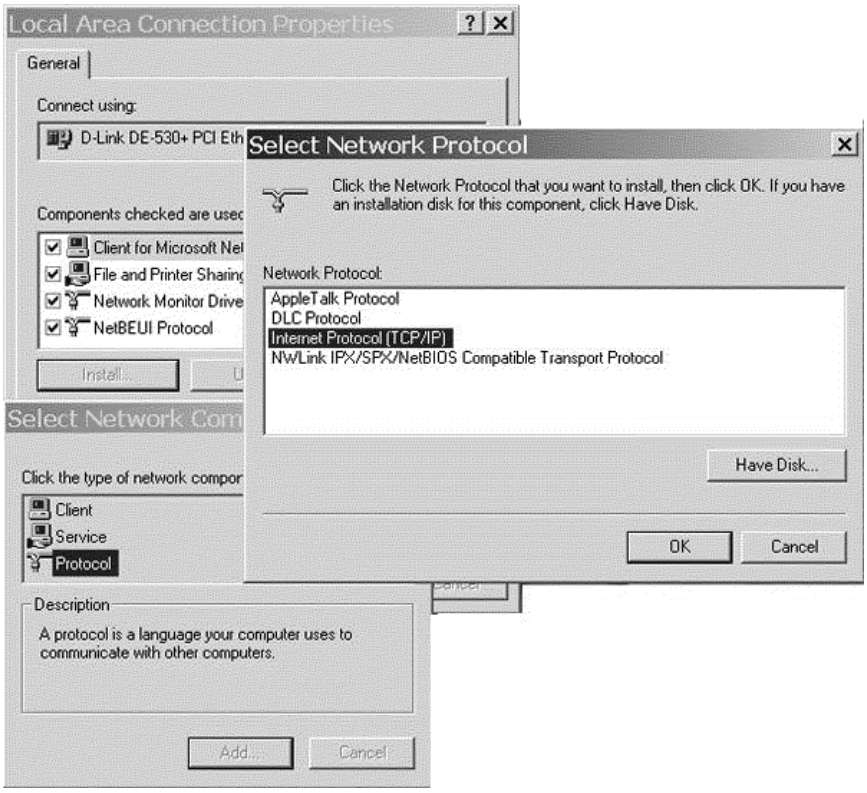

FIGURE 1–3 *Manually installing TCP-IP on Windows 2000*

4. Verify that the **Internet Protocol (TCP/IP)** check box is selected, and then click **OK**.
5. Launch the **Internet Protocol (TCP/IP) Properties** dialog box (see Figure 1-4.) Type your IP address, subnet mask, default gateway address, and DNS server in the corresponding boxes. (At this point we assume you already have an IP address, DNS server, subnet mask, and default gateway assigned. We will learn how to calculate them ourselves a bit later in the text.)
6. Click **OK**.
7. After the computer recalculates the network bindings the **Network** Dialog Box will appear, prompting you to restart the computer. Click **Yes** and wait until the computer restarts.

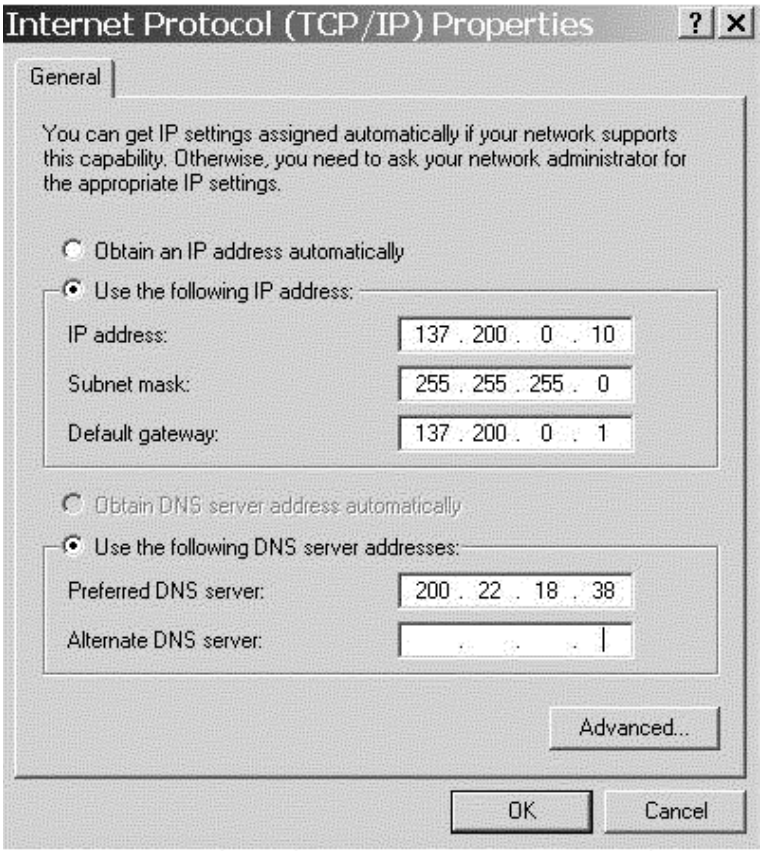

FIGURE 1–4 *Internet protocol TCP/IP properties*

After the computer restarts, it will have your TCP/IP settings.

Changing TCP/IP Parameters

In some cases you need to change existing TCP/IP parameters—for example when you move the computer to another building. In order to change the TCP/IP parameters for the existing installation perform the following steps:

1. From the **Start** menu open **Settings** and launch **Network** and **Dial-up Connections**.
2. Right-click the network connection that you want to configure, and then click **Properties**.
3. Choose the **Internet Protocol** (TCP/IP) and click **Properties**.
4. The TCP/IP properties dialog box appears.
5. Make the appropriate changes to the IP address, subnet mask, DNS server, and default gateway boxes.
6. Click **OK**.

Testing the TCP/IP Configuration

After you have successfully installed TCP/IP on Windows 2000, it's a good idea to verify you have set the TCP/IP parameters properly. You can perform the following steps as the basic troubleshooting tool.

USING THE IPCONFIG UTILITY

To verify the TCP/IP configuration parameters, including the IP address, subnet mask, and default gateway, use the IPCONFIG utility. This utility is provided as a part of the Microsoft TCP/IP installation. IPCONFIG is useful in determining whether your parameters have been initialized or what values these parameters received.

IPCONFIG is a command line utility, and the simplest way to use it is to type the following at the command prompt:

```
ipconfig
```

If the TCP/IP configuration is initialized, the assigned IP address, subnet mask, and default gateway (if configured) appear. For example:

```
C:\WINDOWS>ipconfig
Windows 2000 IP Configuration
Ethernet adapter Elnk31:
 IP Address. . . . . . . . . . : 137.200.0.10
 Subnet Mask . . . . . . . . . : 255.255.255.0
 Default Gateway . . . . . . . : 137.200.0.1
```

USING THE PING UTILITY

While the IPCONFIG utility is used to test the configuration parameters on a local computer, the PING utility will test connectivity with other computers.

PING is a diagnostic tool that can report basic TCP/IP problems such as connection failures or router problems. For example, you can use the PING utility to verify that contact can be established between the client and server.

The work of the PING utility is based on the Internet Control Message Protocol (ICMP). PING sends ICMP echo packets to the host and listens for echo reply packets. PING waits up to one second for each packet sent and prints the number of packets transmitted and received. Each packet is validated against the transmitted message.

PING is a command line utility. Its syntax is:

`ping` *`IP_address,`* `where` *`IP_address`* `is the IP address of the destination host.`

The successful PING returns a sequence of replies as follows:

```
C:\WINDOWS>ping 137.200.0.1
Pinging 137.200.0.1 with 32 bytes of data:
Reply from 137.200.0.1: bytes=32 time<10ms TTL=128
Reply from 137.200.0.1: bytes=32 time<10ms TTL=128
Reply from 137.200.0.1: bytes=32 time<10ms TTL=128
Reply from 137.200.0.1: bytes=32 time<10ms TTL=128
```

If communication problems exist, for example the destination node is powered down, the PING output may look like this:

```
C:\WINDOWS>ping 137.200.0.2
Pinging 137.200.0.2 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

This listing may indicate a problem with a router:

```
C:\WINDOWS>ping 137.200.3.1
Pinging 137.200.3.1 with 32 bytes of data:
Destination host unreachable.
Destination host unreachable.
Destination host unreachable.
Destination host unreachable.
```

Some specific IP addresses are reserved for special purposes. For example the IP address 127.0.0.1 is the loopback address. You can use **ping 127.0.0.1** to check if TCP/IP is loaded correctly on your computer.

As you may have noticed, by default the PING command sends four 32-byte packets and waits for four replies. The following syntax will cause PING to continuously send packets until interrupted with a CTRL-C:

`ping -t` *`IP_address`*

TCP/IP Testing Sequence

Using the PING and IPCONFIG utilities you can perform basic testing and troubleshooting tasks.

To verify a computer's configuration and check router connections perform the following steps:

1. Use the IPCONFIG for the verification of the TCP/IP initialization. At the command prompt type:

   ```
   ipconfig
   ```

2. Ping the loopback address, to verify that TCP/IP is installed and bound to the network adapter. Type:

   ```
   ping 127.0.0.1
   ```

3. Ping the IP address of your own host, to verify that TCP/IP was added correctly. Type:

   ```
   ping your_IP_address
   ```

   If the previous steps fail, you most likely have an IP addressing problem.

4. Ping the IP address of your default gateway, to ensure that it is operational. Additionally, a successful ping to the default gateway indicates that you can connect to hosts in your local subnet. Type:

   ```
   ping default_gateway_IP_address
   ```

5. Finally, ping the IP address of the remote host to verify that you can connect through a router. Type:

   ```
   ping remote_host_IP_address
   ```

   If this step fails, you may have an incorrect subnet mask, or an incorrect default gateway. It can also indicate the failure of a WAN link or malfunctioning router.

Important If you go directly to Step 5 and can successfully ping the remote host, it guarantees all previous steps would have been successful.

Microsoft Network Monitor

Sometimes network problems become too complex to solve by means of simple diagnostic tools such as IPCONFIG and PING. In this case Microsoft Network Monitor, the tool which can capture network traffic, may be helpful. Network Monitor is able to capture and display frames (also called packets) in order to detect and troubleshoot problems on a local area network (LAN).

Network Monitor is particularly useful in diagnosing hardware and software problems when two or more computers cannot communicate. If the problem is too complex, you can capture network activity and send the capture file to a support organization or network analyst for assistance.

Microsoft Network Monitor configures the network card to capture all incoming and outgoing frames. You can define capture filters and capture triggers to capture only specific data. For security reasons the version of Microsoft Network Monitor that is shipped with Windows 2000 is limited to capturing only data originating from or destined to the computer running network monitor, as well as broadcast and multicast messages. Microsoft Systems Management Server (SMS) includes a version of Network Monitor that can also capture frames sent to or from any computer on the network, edit and transmit frames on the network, and capture frames remotely. The SMS version achieves this by setting the network adapter card to the so-called promiscuous mode.

Note You can use the SMS version of Network Monitor to capture frames remotely from Network Agents installed on Windows 2000 computers, Windows NT Workstations, and Windows 95 computers.

Installing Microsoft Network Monitor

You must be logged on with Administrator or Power User privileges to install Microsoft Network Monitor in Windows 2000.

To install Network Monitor (see Figure 1-5), follow these steps.

1. Click **Start**, point to **Settings**, and then click **Control Panel**.
2. Double-click **Add/Remove Programs**.
3. Click **Add/Remove Windows Components**.
4. Click **Management and Monitoring Tools**, and then click **Details**.
5. Select the **Network Monitor Tools** check box and click **OK**.
6. Select **Network Monitor Tools** and click **OK**.
7. You may be asked to provide the path to the Windows 2000 Setup files. Type the full path to the Windows 2000 distribution point and click **Continue**.

Now you can use Microsoft Network Monitor.

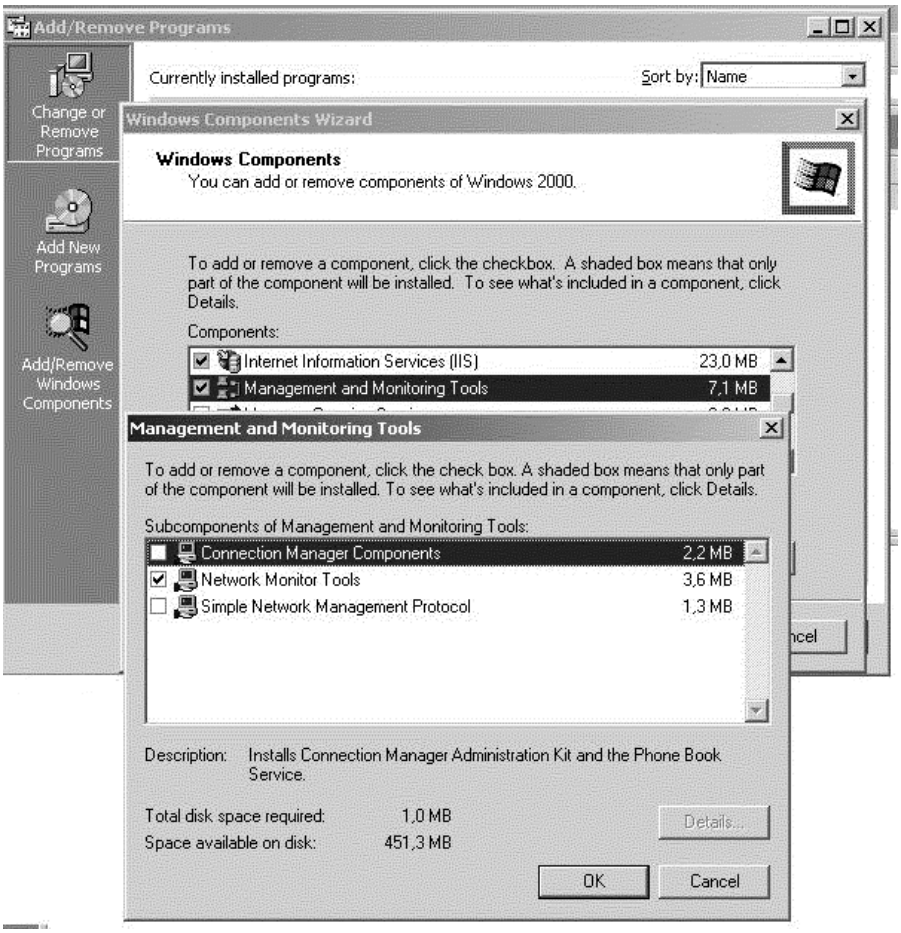

FIGURE 1–5 *Installing Microsoft Network Monitor on Windows 2000*

Using Microsoft Network Monitor to Capture and View Data

When the Microsoft Network Monitor is installed you can access it in the Administrative Tools (Common) folder in the Start menu. Figure 1-6 illustrates the layout of the Microsoft Network Monitor Window.

The typical procedure for using Network Monitor is:

1. Start capturing
2. Generate network traffic to capture
3. Stop capturing
4. View captured data

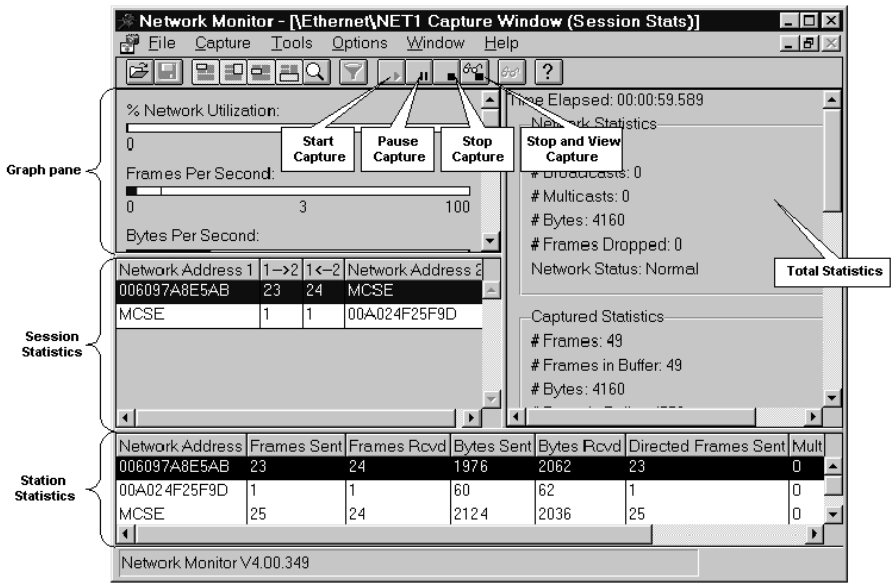

FIGURE 1–6 *Microsoft Network Monitor window*

STARTING A CAPTURE

To start capturing network traffic, use the **Start Capture** button on the toolbar (you can also use the **Start** command from the **Capture** menu or press **F10**). Captured frames are stored in the capture buffer. When the buffer overflows, new frames replace the oldest ones. You can control the buffer size with the **Buffer Settings** option in the **Capture** menu. When you are capturing, the information panes display capture statistics. The meaning of the panes is described in the Table 1.7.

TABLE 1.7 *Microsoft Network Monitor Panes Capture View*

Pane	Displays
Graph	A graphical representation of the activity currently taking place on the network, including network utilization and broadcast level.
Session Statistics	Statistics about individual sessions currently taking place on the network.
Station Statistics	Statistics about the sessions in which the computer running Network Monitor participates. They include bytes and frames sent and received.
Total Statistics	Summary statistics about network activity detected since the capture began.

GENERATING NETWORK TRAFFIC

To generate network traffic you wish to analyze, use a network-based application such as Microsoft Internet Explorer or the PING command.

STOPPING AND VIEWING THE CAPTURED DATA

To stop the capture, use the **Stop Capture** button (see Figure 1-6), the **Stop** command from the **Capture** menu, or **F11**.

To view the captured data, use the **Stop and View** command from the **Capture** menu if you are currently capturing or the **View** command from the **Capture** menu if the capture has been stopped.

When opening a capture window, a **Frame Viewer** window appears (see Figure 1-7). The Frame Viewer window shows each captured frame. It contains a frame number, the time the frame was received, source and destination addresses, protocols contained in the frame, and other information. To get more detailed information about the particular frame, double-click the frame.

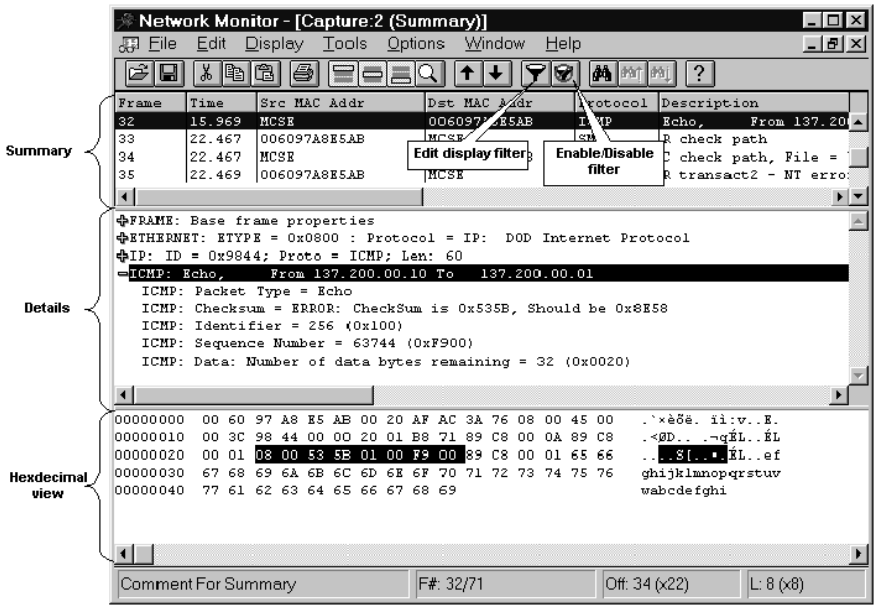

FIGURE 1–7 *Microsoft Network Monitor capture view*

The Frame Viewer window includes the panes shown in Table 1.8.

TABLE 1.8 *Microsoft Network Monitor Panes Frame View*

Panes	Displays
Detail	The frame's contents, including the protocols used to send it.
Hex	A hexadecimal and ASCII representation of the captured data.
Summary	General information about captured frames in the order in which they were captured.

You can save the capture to hard disk for later analysis. To do this, choose **Save As** from the **File** menu.

As we use Microsoft Network Monitor in the labs following this chapter, you will become familiar with its more advanced features.

Summary

In this chapter we discussed the basics of TCP/IP. You learned that TCP/IP is not just one or two protocols, but a set of protocols that have different purposes and properties. We covered the main advantages of using Microsoft TCP/IP such as its industry standard routable environment, its compatibility with modern operating systems, its connectivity with dissimilar systems, and its ability to provide access to the Internet. You also learned how to install Microsoft TCP/IP on Windows 2000. Finally, we looked at a number of network analysis tools and procedures to include IPCONFIG, PING, and Microsoft Network Monitor, the tool that can be used to capture network traffic and analyze network-related problems.

Test Yourself

1. Which protocol provides bidirectional file transfers between TCP/IP hosts?
   - **A.** FTP
   - **B.** ARP
   - **C.** IP
   - **D.** PPTP

2. Which application allows your keyboard to act as if it were attached to a remote computer?
   A. Ping
   B. Telnet
   C. LPR
   D. FTP
3. What does the Ping utility do?
4. What is Microsoft Network Monitor used for?