Configuring and Troubleshooting TCP/IP

On a TCP/IP network, each device (computer, router, or other device with a connection to the network) is referred to as a host. Each TCP/IP host is identified by a logical **IP address** that identifies a computer's location on the network in much the same way as a street address identifies a house on a street. Microsoft's implementation of TCP/IP enables a TCP/IP host to use a static Internet Protocol (IP) address or to obtain an IP address automatically from a **Dynamic Host Configuration Protocol** (DHCP) server.

For simple network configurations based on local area networks (LANs), Windows XP also supports automatic assignment of IP addresses. Windows XP Professional includes many tools that you can use to troubleshoot TCP/IP and test connectivity.

After this lesson, you will be able to
■ Explain the use of IP addresses.
■ Configure TCP/IP to use a static IP address.
■ Configure TCP/IP to obtain an IP address automatically.
■ Explain the use of Automatic Private IP Addressing.
■ Specify an alternate TCP/IP configuration for a computer running Windows XP Professional.
■ Use TCP/IP tools to troubleshoot a connection.

Estimated lesson time: 60 minutes

What Is an IP Address?

Every interface on a TCP/IP network is given a unique IP address that identifies it on that network. IP handles this addressing, defining how the addresses are constructed and how packets are routed using those addresses.

An IP address consists of a set of four numbers, each of which can range from 0 to 255. Each of these numbers is separated from the others by a decimal point, so a typical IP address in decimal form might look something like 192.168.1.102. The reason that each number ranges only up to 255 is that each number is actually based on a binary octet, or an eight-digit binary number. The IP address 192.168.1.102 represented in binary form is 11000000 10101000 00000001 01100110. Computers work with the binary format, but it is much easier for people to work with the decimal representation.

An IP address consists of two distinct portions:

■ The **network ID** is a portion of the IP address starting from the left that identifies the network segment on which a host is located. Using the example 192.168.1.102, the portion 192.168.1 might be the network ID. When representing a network ID, it is customary to fill in the missing octets with zeroes. So, the proper network ID would be 192.168.1.0.

■ The **host ID** is the portion of the IP address that identifies a particular host on a network segment. The host ID for each host must be unique within the network ID. Continuing the example of the IP address 192.168.1.102 (where 192.168.1.0 is the network ID), the host ID is 102.

Two computers with different network IDs can have the same host ID. However, the combination of the network ID and the host ID must be unique to all computers in communication with each other.

Hosts depend on a second number called a **subnet mask** to help determine which portion of an IP address is the network ID and which portion is the host ID. The subnet mask defines where the network ID stops and the host ID starts. It is easier to see why this works if you step away from the decimal representation for a moment and look at the numbers in their binary format.

Figure 13-1 depicts a single IP address shown in both decimal and binary format. A subnet mask is also shown in both formats. In binary format, a subnet mask always represents a string of unbroken ones followed by a string of unbroken zeroes. The position of the change from ones to zeroes indicates the division of network ID and host ID in an IP address.

	Decimal	Binary
IP Address	135.109.15.42	10000111 01101101 00001111 00101010
Subnet Mask	255.255.0.0	11111111 11111111 00000000 00000000
Network ID	135.109.0.0	10000111 01101101 00000000 00000000
Host ID	0.0.15.42	00000000 00000000 00001111 00101010

Figure 13-1 The subnet mask separates the host ID and the network ID.

Classful IP Addressing

IP addresses are organized into classes that help define the size of the network being addressed, a system referred to as classful IP addressing. Five different classes of IP addresses define different-sized networks that are capable of holding varying numbers of hosts.

Classful IP addressing is based on the structure of the IP address and provides a systematic way to differentiate network IDs from host IDs. As you learned earlier, there are four numerical segments of an IP address, ranging from 0 to 255. Here, those segments are represented as w.x.y.z. Based on the value of the first octet (w), IP addresses are categorized into the five address classes listed in Table 13-1.

Table 13-1 IP Address Classes

Class	Network ID	Range of First Octet	Number of Available Network Segments	Number of Available Hosts	Subnet Mask
A	w.0.0.0	1–126	126	16,777,214	255.0.0.0
B	w.x.0.0	128–191	16,384	65,534	255.255.0.0
C	w.x.y.0	192–223	2,097,152	254	255.255.255.0
D	N/A	224–239	N/A	N/A	N/A
E	N/A	240–255	N/A	N/A	N/A

Classes A, B, and C are available for registration by public organizations. Actually, most of these addresses were snapped up long ago by major companies and Internet service providers (ISPs), so the actual assignment of an IP address to your organization will likely come from your chosen ISP. Classes D and E are reserved for special use. The address class determines the subnet mask used, and therefore determines the division between the network ID and the host ID. For class A, the network ID is the first octet in the IP address (for example, the 98 in the address 98.162.102.53 is the network ID). For class B, it is the first two octets; and for class C, it is the first three octets. The remaining octets not used by the network ID identify the host ID.

Classless Interdomain Routing (CIDR)

In the classful method of IP addressing, the number of networks and hosts available for a specific address class is predetermined by the default subnet mask for the class. As a result, an organization that is allocated a network ID has a single fixed network ID and a specific number of hosts. With the single network ID, the organization can have only one network connecting its allocated number of hosts. If the number of hosts is large, the network cannot perform efficiently. To solve this problem, the concept of classless interdomain routing (CIDR) was introduced.

CIDR allows a single classful network ID to be divided into smaller network IDs. The idea is that you take the default subnet mask used for the class to which your IP address range belongs, and then borrow some of the bits used for the host ID to use as an extension to the network ID, creating a custom subnet mask.

A custom subnet mask is not restricted by the same rules used in the classful method. Remember that a subnet mask consists of a set of four numbers, similar to an IP address. Consider the default subnet mask for a class B network (255.255.0.0), which in binary format would be the following:

11111111 11111111 00000000 00000000

This mask specifies that the first 16 bits of an IP address are to be used for the network ID and the second 16 bits are to be used for the host ID. To create a custom subnet mask, you

would just extend the mask into the host ID portion. However, you must extend this by adding ones from left to right. Remember that a subnet mask must be an unbroken string of ones followed by an unbroken string of zeroes. For example, a custom subnet mask might look like this:

11111111 11111111 11111000 00000000

The value 11111000 in decimal format would be 248, making this IP address 255.255.248.0. Table 13-2 shows the possible values for an octet in a custom subnet mask.

Table 13-2 Custom Subnet Mask Values

Binary Value	Decimal Value
10000000	128
11000000	192
11100000	224
11110000	240
11111000	248
11111100	252
11111110	254

In the classful method, each of the four numbers in a subnet mask can be only the maximum value 255 or the minimum value 0. The four numbers are then arranged as contiguous octets of 255, followed by contiguous octets of 0. For example, 255.255.0.0 is a valid subnet mask, whereas 255.0.255.0 is not. The 255 octets identify the network ID, and the 0 octets identify the host ID. For example, the subnet mask 255.255.0.0 identifies the network ID as the first two numbers in the IP address.

When subnetting an existing network ID to create additional subnets, you can use any of the preceding subnet masks with any IP address or network ID. So the IP address 184.12.102.20 could have the subnet mask 255.255.255.0 and network ID 184.12.102.0, as opposed to the default subnet mask 255.255.0.0 with the network ID 184.12.0.0. This allows an organization to subnet an existing class B network ID of 184.12.0.0 into smaller subnets to match the actual configuration of their network.

Private Addressing

Every network interface that is connected directly to the Internet must have an IP address registered with the Internet Assigned Numbers Authority (IANA), which prevents IP address conflicts between devices. If you are configuring a private network that is not connected to the Internet or one that exists behind a firewall or proxy server, you can configure devices on your network with private addresses and have only the public address configured on the interface that is visible to the Internet.

Each address class has a range of private addresses available for general use:

- Class A: 10.0.0.0 through 10.255.255.255
- Class B: 172.16.0.0 through 172.31.255.255
- Class C: 192.168.0.0 through 192.168.255.255

You can choose whichever range you like to use for your network and implement custom subnets as you see fit. None of these addresses is ever officially assigned to a publicly accessible Internet host.

How to Configure TCP/IP to Use a Static IP Address

By default, client computers running Windows 95 and later are configured to obtain TCP/IP configuration information automatically. Automatic TCP/IP information is provided on a network using a DHCP server. When a client computer starts, it sends a broadcast message to the network looking for a DHCP server that can provide IP addressing information. Typically, most computers on a network should be configured to obtain IP addresses automatically because automatic addressing eliminates most of the errors and administrative overhead associated with assigning static IP addresses to clients. However, even in a DHCP-enabled environment, you should assign a static IP address to selected network computers. For example, the computer running the DHCP Service cannot be a DHCP client, so it must have a static IP address. If the DHCP Service is not available, you can also configure TCP/IP to use a static IP address. For each network adapter card that uses TCP/IP in a computer, you can configure an IP address, subnet mask, and default gateway, as shown in Figure 13-2.
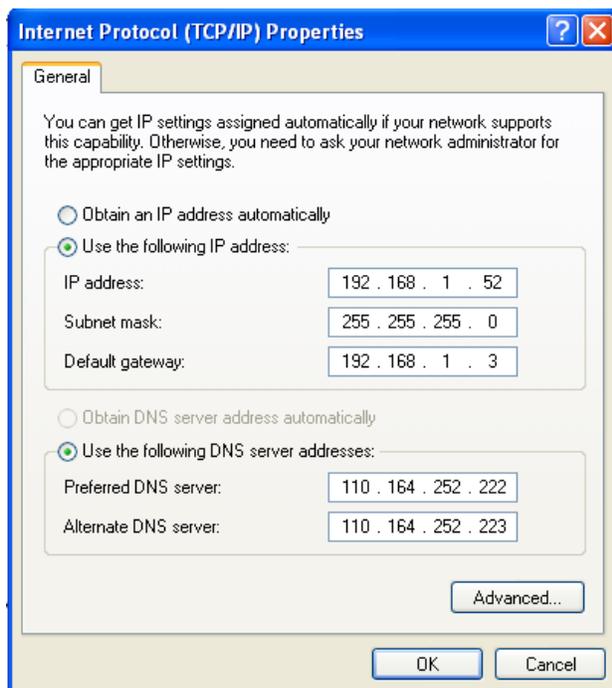
Figure 13-2 Configuring a static TCP/IP address in Windows XP Professional

Table 13-3 Options for Configuring a Static TCP/IP Address

Option	Description
IP address	A logical 32-bit address that identifies a TCP/IP host. Each network adapter card in a computer running TCP/IP requires a unique IP address.
Subnet mask	Subnets divide a large network into multiple physical networks connected with routers. A subnet mask blocks out part of the IP address so that TCP/IP can distinguish the network ID from the host ID. When TCP/IP hosts try to communicate, the subnet mask determines whether the destination host is on a local or remote network. To communicate on a local network, computers must have the same subnet mask.
Default gateway	The router (also known as a gateway) on the local network. The router isresponsible for forwarding traffic to and from remote networks.

To configure TCP/IP to use a static IP address, complete the following steps:
1. Click Start, and then click Control Panel.
2. In the Control Panel window, click Network And Internet Connections.
3. In the Network And Internet Connections window, click Network Connections, double-click Local Area Connection, and then click Properties.
4. In the Local Area Connection Properties dialog box, click Internet Protocol (TCP/IP), verify that the check box to its left is selected, and then click Properties.
5. In the Internet Protocol (TCP/IP) Properties dialog box, in the General tab, click Use The Following IP Address, type the TCP/IP configuration parameters, and then click OK.
6. Click OK to close the Local Area Connection Properties dialog box, and then close the Network And Dial-Up Connections window.

How to Configure TCP/IP to Obtain an IP Address Automatically

If a server running the DHCP Service is available on the network, it can automatically assign TCP/IP configuration information to the DHCP client, as shown in Figure 13-3.
You can then configure any clients running Windows 95 and later to obtain TCP/IP configuration information automatically from the DHCP Service. This can simplify administration and ensure correct configuration information.
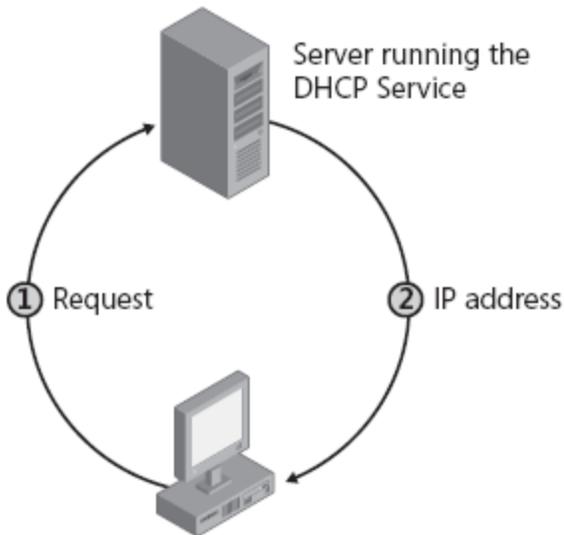
Figure 13-3 A server running the DHCP Service assigns TCP/IP addresses.

You can use the DHCP Service to provide clients with TCP/IP configuration information automatically. However, you must configure a computer as a DHCP client before it can interact with the DHCP Service.

To configure a computer running Windows XP Professional to obtain an IP address automatically, complete the following steps:

1. Click Start, and then click Control Panel.
2. In the Control Panel window, click Network And Internet Connections.
3. In the Network And Internet Connections window, click Network Connections, double-click Local Area Connection, and then click Properties.
4. In the Local Area Connection Properties dialog box, click Internet Protocol (TCP/IP), verify that the check box to its left is selected, and then click Properties.
5. In the Internet Protocol (TCP/IP) Properties dialog box, in the General tab, click Obtain An IP Address Automatically.
6. Click OK to close the Local Area Connection Properties dialog box, and then close the Network And Dial-Up Connections window.

What Is Automatic Private IP Addressing?

The Windows XP Professional implementation of TCP/IP supports automatic assignment of IP addresses for simple LAN-based network configurations. This addressing mechanism is an extension of dynamic IP address assignment for LAN adapters, enabling configuration of IP addresses without using static IP address assignment or using a DHCP server. **Automatic Private IP Addressing** (APIPA) is enabled by default in Windows XP Professional so that home users and small business users can create a functioning, single-subnet, TCP/IP-based network without having to configure the TCP/IP protocol manually or set up a DHCP server.

Note The IANA has reserved 169.254.0.0 through 169.254.255.255 for APIPA. As a result, APIPA provides an address that is guaranteed not to conflict with routable addresses.

APIPA assigns an IP address and subnet mask only, and configures no additional parameters. This service is very useful in smaller, single-network environments in which there is no need for connectivity to other networks. APIPA provides a very simple way to configure TCP/IP; the network administrator does not need any knowledge of the necessary configuration parameters. However, if connectivity to other networks is required, or if the client requires name-resolution services, APIPA is not sufficient.
APIPA does not provide a default gateway or name server address to the client.

The process for the APIPA feature, shown in Figure 13-4, is explained in the following steps:
1. Windows XP Professional TCP/IP attempts to find a DHCP server on the attached network to obtain a dynamically assigned IP address.
2. In the absence of a DHCP server during startup (for example, if the server is down for maintenance or repairs), the client cannot obtain an IP address.
3. APIPA generates an IP address in the form of 169.254.*x.y* (where *x.y* is the client's randomly generated unique identifier) and a subnet mask of 255.255.0.0.

Server running the
DHCP Service is unavailable

② No IP address returned

① Request

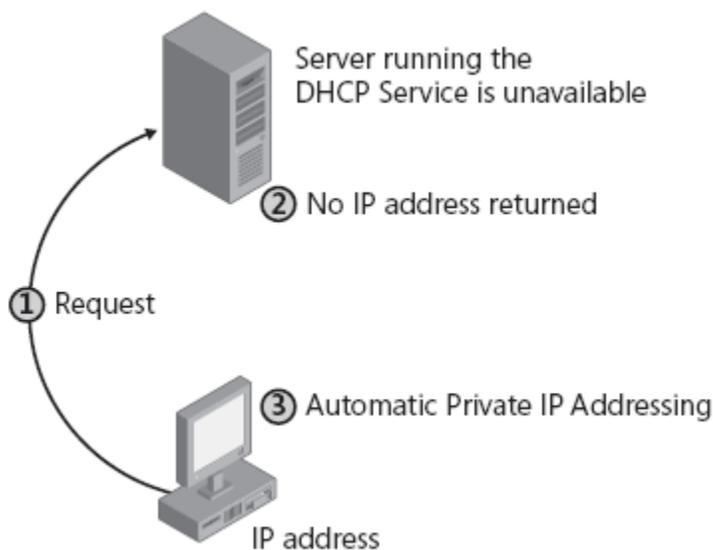③ Automatic Private IP Addressing

IP address

Figure 13-4 APIPA assigns IP addresses automatically.

After the computer generates the address, it broadcasts to this address, and then assigns the address to itself if no other computer responds. The computer continues to use this address until it detects and receives configuration information from a DHCP server. This allows two

computers to be plugged into a LAN hub to restart without any IP address configuration and to use TCP/IP for local network access.

If the computer is a DHCP client that has previously obtained a lease from a DHCP server and the lease has not expired at boot time, the sequence of events is slightly different. The client tries to renew its lease with the DHCP server. If the client cannot locate a DHCP server during the renewal attempt, it attempts to ping the default gateway listed in the lease.

If pinging the default gateway succeeds, the DHCP client assumes that it is still on the same network in which it obtained its current lease, so it continues to use the lease. By default, the client attempts to renew its lease when 50 percent of its assigned lease time has expired. If pinging the default gateway fails, the client assumes that it has been moved to a network that has no DHCP services currently available and it autoconfigures itself, as previously described. After being automatically configured, the client continues to try to locate a DHCP server every five minutes.

APIPA can assign a TCP/IP address to DHCP clients automatically. However, APIPA does not generate all the information that typically is provided by DHCP, such as the address of a default gateway. Consequently, computers enabled with APIPA can communicate only with computers on the same subnet that also have addresses of the form 169.254.$x.y$.

By default, the APIPA feature is enabled. However, you can disable it by specifying an alternate configuration to use if a DHCP server cannot be located (see Figure 13-5), as discussed in the next section.
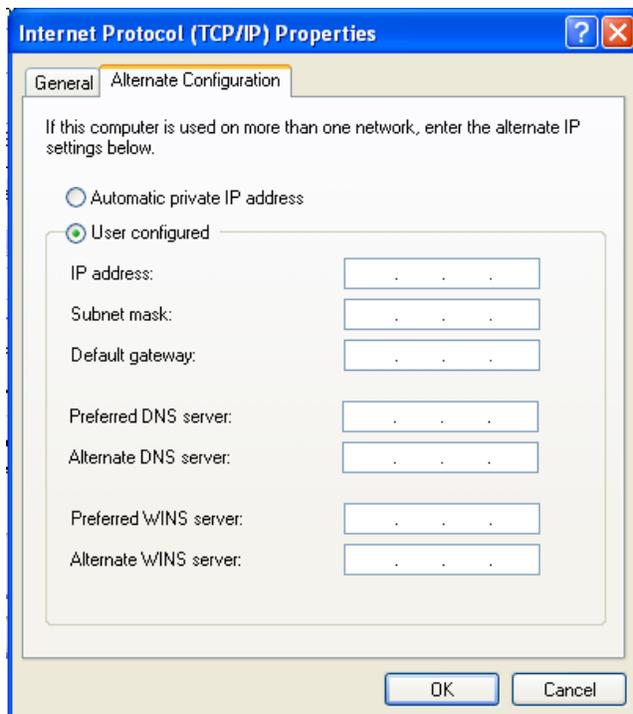

Figure 13-5 Specify an alternate TCP/IP configuration.

How to Specify an Alternate Configuration for TCP/IP

A feature in Windows XP Professional named Auto-Configuration For Multiple Networks Connectivity provides easy access to network devices and the Internet. It also allows a mobile computer user to seamlessly operate both office and home networks without having to manually reconfigure TCP/IP settings. You specify an alternate configuration for TCP/IP if a DHCP server is not found. The alternate configuration is useful when a computer is used on multiple networks, one of which does not have a DHCP server and does not use an automatic private IP addressing configuration.

To configure Auto-Configuration For Multiple Networks Connectivity, use these steps:
1. Click Start and then click Control Panel.
2. In the Control Panel window, click Network And Internet Connections.
3. In the Network And Internet Connections window, click Network Connections, and then click Local Area Connection.
4. Click Change Settings Of This Connection.
 Windows XP Professional displays the Local Area Connection Properties dialog box.
5. Click Internet Protocol (TCP/IP), and then click Properties.
 Windows XP Professional displays the Internet Protocol (TCP/IP) Properties dialog box with the General tab active.
6. Click Alternate Configuration.
7. Specify the alternate TCP/IP configuration (refer to Figure 13-5).

How to Use TCP/IP Tools to Troubleshoot a Connection

Windows XP provides a number of TCP/IP tools for troubleshooting network connectivity problems. You should be familiar with the following tools:
■ Ping
■ Ipconfig
■ Net View
■ Tracert
■ Pathping

Using Ping

When the problem appears to be with TCP/IP, start the troubleshooting process with the **Ping** command, which allows you to check fo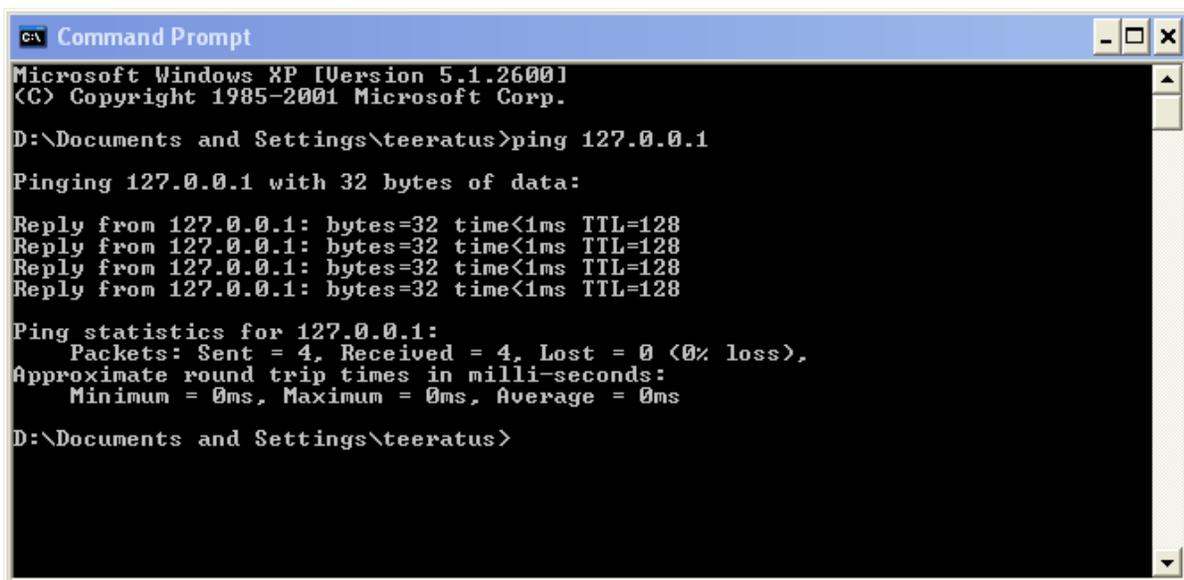r connectivity between devices on a network. When you use the Ping command, you ping from the inside out. You want to find out where the communication and connection fail. For example, you ping the loopback address first, then a local computer on the same network, then a DNS or DHCP server on the local subnet if one exists, then the default gateway, then a remote computer on another network, and

finally a resource on the Internet. You should be able to find out where the breakdown occurs by compiling the results of these checks.

Note When using the Ping command, you can use either the computer name or the computer's IP address.

Pinging the Loopback Address The **loopback address** (127.0.0.1) is the first thing you should check when a TCP/IP problem appears. If this check fails, the TCP/IP configuration for the local machine is not correct. To ping the loopback address, follow these steps:

1. From the Start menu, point to All Programs, point to Accessories, and select Command Prompt.
2. Type **ping 127.0.0.1**. A successful ping to a loopback address is shown in Figure 13-6.

Figure 13-6 Ping the loopback address to verify that TCP/IP is configured correctly.

Figure 13-6 Ping the loopback address to verify that TCP/IP is configured correctly.

If pinging the loopback address fails, check the configuration of TCP/IP by following these steps:
1. Open the Network Connections window, right-click the configured connection, and choose Properties.
2. Select Internet Protocol (TCP/IP), and click Properties to view the configuration. If a static address is configured and a DHCP server is available, select Obtain An IP Address Automatically. If Obtain An IP Address Automatically is selected but a static IP address is necessary, select Use The Following IP Address; then enter the address, subnet mask, and gateway to use. If the configuration is correct, you might have to reset TCP/IP.
3. Click OK in the Properties dialog box and OK in the connection's Properties dialog

box. Reboot the computer if prompted.

Pinging Other Resources To ping any other computer on the network, simply replace the loopback address with the TCP/IP address of the resource on the network. Ping a local computer on the same subnet first, and then ping the gateway address. If you can ping the loopback address (a local computer on the same subnet), but the Ping command to the gateway fails, you probably found the problem. In this case, check the configuration on the local computer for the gateway address and verify that the gateway (or router) is operational.

If the ping to the gateway address is successful, continue to ping outward until you find the problem. For instance, ping a computer on a remote subnet and verify that the DNS server is operational.

Using Ipconfig

You can use the **Ipconfig** command-line utility to view current TCP/IP configuration information for a computer. To use Ipconfig, open the command prompt window and type **Ipconfig** to view basic TCP/IP parameters, **Ipconfig /all** to view the complete TCP/IP configuration (as shown in Figure 13-7), or **Ipconfig /?** to view additional options.
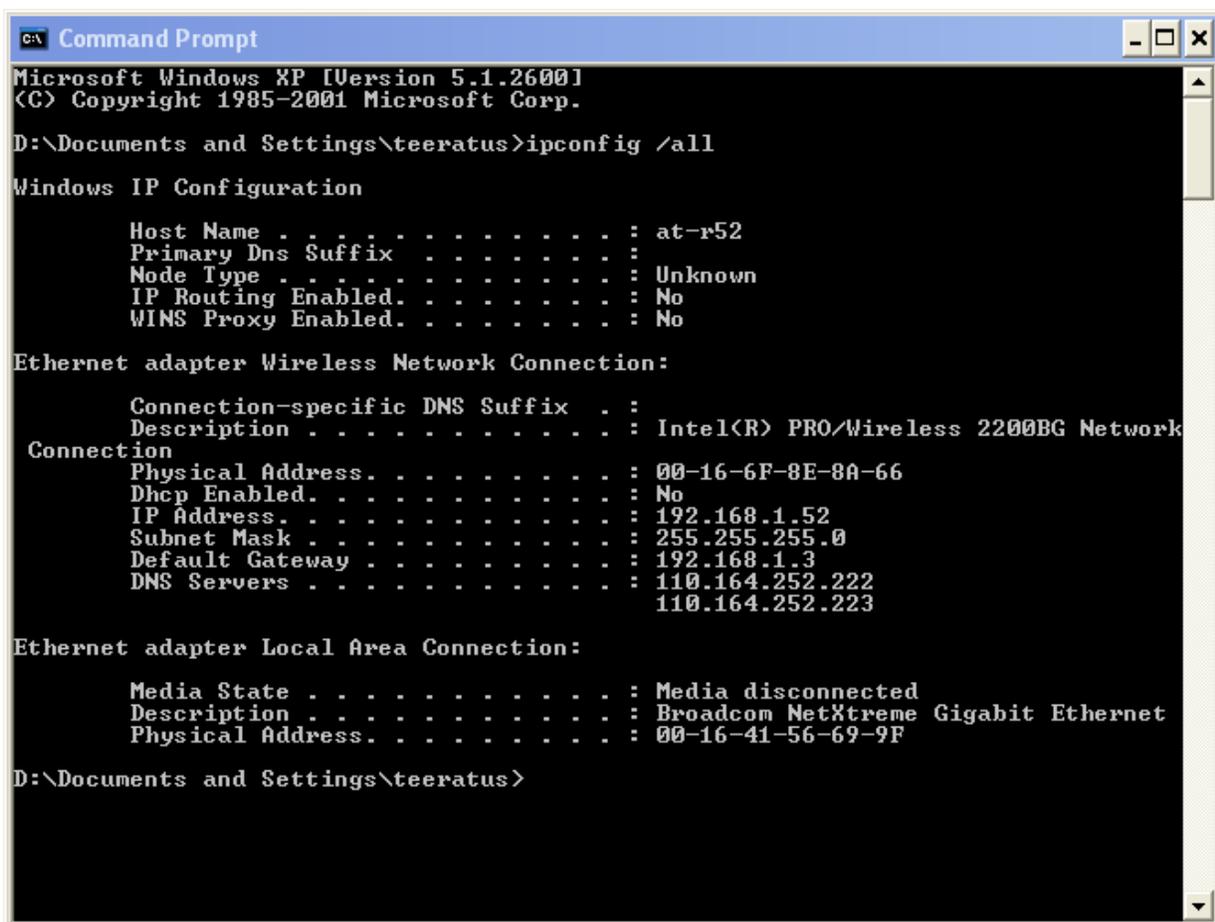
```
Command Prompt                                                    - □ ×
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

D:\Documents and Settings\teeratus>ipconfig /all

Windows IP Configuration

        Host Name . . . . . . . . . . . . : at-r52
        Primary Dns Suffix  . . . . . . . :
        Node Type . . . . . . . . . . . . : Unknown
        IP Routing Enabled. . . . . . . . : No
        WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Wireless Network Connection:

        Connection-specific DNS Suffix  . :
        Description . . . . . . . . . . . : Intel(R) PRO/Wireless 2200BG Network
 Connection
        Physical Address. . . . . . . . . : 00-16-6F-8E-8A-66
        Dhcp Enabled. . . . . . . . . . . : No
        IP Address. . . . . . . . . . . . : 192.168.1.52
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.1.3
        DNS Servers . . . . . . . . . . . : 110.164.252.222
                                            110.164.252.223

Ethernet adapter Local Area Connection:

        Media State . . . . . . . . . . . : Media disconnected
        Description . . . . . . . . . . . : Broadcom NetXtreme Gigabit Ethernet
        Physical Address. . . . . . . . . : 00-16-41-56-69-9F

D:\Documents and Settings\teeratus>
```

Figure 13-7 Use the Ipconfig /all command to display a complete TCP/IP configuration.

Additional Ipconfig options include the following:

/release Releases DHCP-supplied configuration information

/renew Renews DHCP-supplied configuration information

/flushdns Purges the local DNS cache (the area of memory that stores recently resolved names so that the client does not have to contact the DNS server each time)

/registerdns Renews DHCP-supplied configuration information and registers the DNS name to IP address information with DNS

/displaydns Displays the contents of the local DNS cache

/setclassid Provides for the configuration of DHCP user classes, which can control the way IP addresses are assigned

Using Net View

The Net View command is another command that you can use to test TCP/IP connections. To use the command, log on with the proper credentials that are required to view shares on a remote or local computer, open a command prompt, and type **net view ***ComputerName* or **net view ***IP Address*. The resulting report lists the file and print shares on the computer. If there are no file or print shares on the computer, you see the message There Are No Entries In The List.

If the Net View command fails, check the following:

■ The computer name in the System Properties dialog box

■ The gateway or router address in the TCP/IP Properties dialog box

■ The gateway or router status

■ The remote computer is running the File And Printer Sharing For Microsoft Networks Service (this service can be added in the TCP/IP Properties dialog box)

```
Command Prompt                                                    - □ ×
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

D:\Documents and Settings\teeratus>net view
Server Name            Remark

-----------------------------------------------------------------
\\AT-R52                     Server from XP on AT-R52
The command completed successfully.


D:\Documents and Settings\teeratus>net view \\at-r52
Shared resources at \\at-r52

Server from XP on AT-R52

Share name   Type    Used as   Comment

-----------------------------------------------------------------
ecacc_net    Disk    Z:
pgm          Disk
Printer2     Print             Microsoft XPS Document Writer
SharedDocs   Disk
The command completed successfully.


D:\Documents and Settings\teeratus>
```

Using Tracert

When a route breaks down on the way from the destination computer to its target computer, communication fails. The **Tracert** command-line utility can help you figure out exactly where along the route the breakdown happened. Sometimes the connection breaks down at the gateway on the local network and sometimes at a router on an external network.
To use Tracert, at the command prompt type **tracert** followed by the IP address of the remote computer. The resulting report shows where the packets were lost. You can use this information to uncover the source of the problem.

Using Pathping

The Ping command is used to test communication between one computer and another; Tracert is used to follow a particular route from one computer to another. The **Pathping** command is a combination of both Ping and Tracert, displaying information about packet loss at every router between the host computer and the remote one. The Pathping command provides information about data loss between the source and the destination, allowing you to determine which particular router or subnet might be having network problems. To use the Pathping command, at the command prompt, type **pathping** followed by the target name or IP address.

The TCP/IP Protocol Suite

The TCP/IP suite of protocols provides a set of standards for how operating systems and applications communicate and how networks are interconnected. The TCP/IP suite of protocols maps to a four-layer conceptual model known as the Department of Defense (DoD) model. The four layers are as follows:

■ **Network access layer** The network access layer is responsible for placing data on the network medium and receiving data off the network medium.
This layer contains physical devices such as network cables and network adapters.

■ **Internet layer** The Internet layer is responsible for addressing, packaging, and routing the data that is handed down to it from the transport layer. There are four core protocols in this layer: IP, Address Resolution Protocol (ARP), Internet Control Message Protocol (ICMP), and Internet Group Management Protocol (IGMP).

■ **Transport layer** The transport layer protocols provide communication sessions between computers. The desired method of data delivery determines the transport protocol. The two transport layer protocols are TCP and User Datagram Protocol (UDP).

■ **Application layer** At the top of the model is the application layer, in which applications gain access to the network. There are many standard TCP/IP tools and services in the application layer, such as File Transfer Protocol (FTP), Telnet, Simple Network Management Protocol (SNMP), DNS, and so on.

Practice: Configuring and Troubleshooting TCP/IP

Exercise 1: Verify a Computer's TCP/IP Configuration

In this exercise, you will use two TCP/IP tools, Ipconfig and Ping, to verify your computer'sconfiguration.

1. Click Start, point to All Programs, point to Accessories, and then click Command Prompt.
2. At the command prompt, type **ipconfig /all**, and then press ENTER.
The Windows XP Professional IP Configuration tool displays the TCP/IP configuration of the physical and logical adapters configured on your computer.
3. Use the information displayed to complete as much of the following table as possible.
Host name…………………………………………………………………
Primary DNS suffix……………………………………………………….
Connection-specific DNS suffix description………………………………...
Physical address………………………………………………………….
DHCP enabled……………………………………………………………..
Autoconfiguration enabled…………………………………………………
Autoconfiguration IP address………………………………………………
Subnet mask……………………………………………………………….
Default gateway……………………………………………………………

Exercise 2: Configure TCP/IP to Use a Static IP Address

1. Click Start, and then click Control Panel.

2. In the Control Panel window, click Network And Internet Connections.

3. In the Network And Internet Connections window, click Network Connections, and then click Local Area Connection.

4. Under Network Tasks, click Change Settings Of This Connection (you can also right-click the connection and then click Properties).

The Local Area Connection Properties dialog box appears, displaying the network adapter in use and the network components used in this connection.

5. Click Internet Protocol (TCP/IP), and then verify that the check box to the left of the entry is selected.

6. Click Properties.

The Internet Protocol (TCP/IP) Properties dialog box appears.

7. Click Use The Following IP Address.

8. In the IP Address text box, type **198.168.1.201**; in the Subnet Mask text box, type **255.255.255.0**.

9. Click OK to return to the Local Area Connection Properties dialog box.

10. Click Close to close the Local Area Connection Properties dialog box and return to the Network Connections window.

11. Minimize the Network Connections window.

12. Restore the command prompt.

13. At the command prompt, type **ipconfig /all** and then press Enter.

The Windows XP Professional IP Configuration tool displays the physical and logical adapters configured on your computer.

14. Record the current TCP/IP configuration settings for your local area connection in the following table.

IP address……………………………………………………………..
Subnet mask……………………………………………………………

15. To verify that the IP address is working and configured for your adapter, type**ping 127.0.0.1**, and then press ENTER. Record the result:

…………………………………………………
…………………………………………………
…………………………………………………
…………………………………………………

16. If you have a computer that you are using to test connectivity, type **ping** *ip_address* (where *ip_address* is the IP address of the computer you are using to test connectivity), and then press ENTER. Minimize the command prompt.

Exercise 3: Configure TCP/IP to Automatically Obtain an IP Address

In this exercise, you will configure TCP/IP to automatically obtain an IP address, and then test the configuration to verify that the DHCP Service has provided the appropriate IP addressing information. Be sure to perform the first part of this exercise even if you have no DHCP server because these settings are also used in Exercise 4.

1. Restore the Network Connections window, right-click Local Area Connection, and then click Properties.
The Local Area Connection Properties dialog box appears.
2. Click Internet Protocol (TCP/IP) and verify that the check box to the left of the entry is selected.
3. Click Properties.
The Internet Protocol (TCP/IP) Properties dialog box appears.
4. Click Obtain An IP Address Automatically, and then click Obtain DNS Server Address Automatically.
5. Click OK to close the Internet Protocol (TCP/IP) Properties dialog box.
6. Click Close to close the Local Area Connection Properties dialog box.
7. Minimize the Network Connections window.
8. Restore the command prompt, type **ipconfig /release**, and then press ENTER.
9. At the command prompt, type **ipconfig /renew**, and then press ENTER.
10. At the command prompt, type **ipconfig**, and then press ENTER.
11. Record the current TCP/IP configuration settings for your local area connection in the following table.
IP address…………………………………………………………………..
Subnet mask…………………………………………………………………..
Default gateway…………………………………………………………………..

Exercise 4: Obtaining an IP Address Using APIPA

In this exercise, if you have a server running the DHCP Service, you need to disable it on that server so that a DHCP server is not available to provide an IP address for your computer (you can also disconnect the networking cable from your computer). Without a DHCP server available to provide an IP address, the Windows XP Professional APIPA feature provides unique IP addresses for your computer.

1. At the command prompt, type **ipconfig /release**, and then press ENTER.
2. At the command prompt, type **ipconfig /renew**, and then press ENTER.
There is a pause while Windows XP Professional attempts to locate a DHCP server on the network.
3. Which message appears, and what does it indicate?
…………………………………………………………………………………………………

4. Click OK to close the dialog box.
5. At the command prompt, type **ipconfig**, and then press ENTER.
6. Record the current TCP/IP settings for your local area connection
IP address……………………………………………
Subnet mask……………………………………………
Default gateway…………………………………………….

7. Is this the same IP address assigned to your computer in Exercise 3? Why or why not?
……………………………………………………………………………………………………
………………………….

Exercise 5: Obtain an IP Address by Using DHCP

Before you begin this exercise, you will need to enable the DHCP Service running on the computer that is acting as a DHCP server (or reconnect your network cable if you disconnected it in Exercise 4). In this exercise, your computer obtains IP addressing information from the DHCP server.

1. At the command prompt, type **ipconfig /release,** and then press ENTER.
2. At the command prompt, type **ipconfig /renew**, and then press ENTER.
After a short wait, a message box indicates that a new IP address was assigned.
3. Click OK to close the message box.
4. At the command prompt, type **ipconfig /all**, and then press ENTER.
Verify that the DHCP server has assigned an IP address to your computer.
5. Close the command prompt.

Lesson Review

The following questions are intended to reinforce key information presented in thislesson. If you are unable to answer a question, review the lesson materials and try the question again.

1. Why would you assign a computer a static IP address?

....

....

....

2. Which of the following statements correctly describe IP addresses? (Choose all thatapply.)
a. IP addresses are logical 64-bit addresses that identify a TCP/IP host.
b. Each network adapter card in a computer running TCP/IP requires a uniqueIP address.
c. 192.168.0.108 is an example of a class C IP address.
d. The host ID in an IP address is always the last two octets in the address.

3. What is the purpose of a subnet mask?

....

....

....

4. By default, client computers running Windows XP Professional, Windows 95, or Windows 98 obtain TCP/IP configuration information automatically from the DHCP Service: True or false?

....

....

5. Your computer running Windows XP Professional was configured manually for TCP/IP. You can connect to any host on your own subnet, but you cannot connect to or even ping any host on a remote subnet. What is the likely cause of the problem and how would you fix it?

....

....

6. Your computer's Computer Name is Pro1, and you ping Pro1. The local address for Pro1 is returned as 169.254.128.71. What does this tell you?

....

....