

Connecting and Troubleshooting a Network

Previous chapters in this network section covered the basics of networking. In this chapter, the pieces are tied together, showing you common components for a small office home office (SOHO) network. It also includes some basic tools you can use for troubleshooting.

Exam 220-801 objectives in this chapter:

- 2.3 Explain properties and characteristics of TCP/IP.
 - Client-side DNS
- 2.10 Given a scenario, use appropriate networking tools.
 - Toner probe
 - Cable tester
 - Loopback plug

Exam 220-802 objectives in this chapter:

- 1.3 Given a scenario, use appropriate command line tools.
 - Networking
 - PING
 - TRACERT
 - NETSTAT
 - IPCONFIG
 - NET
 - NSLOOKUP
 - NBTSTAT
- 1.6 Setup and configure Windows networking on a client/desktop.
 - Establish networking connections
 - VPN

- Dialups
- Wireless
- Wired
- WWAN (Cellular)
- HomeGroup, file/print sharing
- Network shares/mapping drives
- 2.6 Given a scenario, secure a SOHO wired network.
 - Change default usernames and passwords
 - Enable MAC filtering
 - Assign static IP addresses
 - Disabling ports
 - Physical security
- 4.2 Given a scenario, troubleshoot common problems related to motherboards, RAM, CPU and power with appropriate tools.
 - Tools
 - Loopback plugs
- 4.5 Given a scenario, troubleshoot wired and wireless networks with appropriate tools.
 - Common symptoms
 - No connectivity
 - APIPA address
 - Limited connectivity
 - Local connectivity
 - IP conflict
 - Tools
 - Cable tester
 - Loopback plug
 - Toner probes
 - PING
 - IPCONFIG
 - TRACERT
 - NETSTAT
 - NBTSTAT
 - NET

REAL WORLD THE COMMAND PROMPT IS VALUABLE

While teaching an advanced Microsoft course on Server 2008 recently, I discovered that one of the students was having some problems. It turned out that he simply wasn't familiar with basic troubleshooting tools such as ping and ipconfig. Because of this, he couldn't troubleshoot the most basic networking problems.

We stayed late and worked together, and I was able to help him learn some of these tools. Just before he left, he mentioned that he always thought that the command prompt wasn't needed if a Windows interface is available. His thought was, "Why use the command prompt if you can point and click?" With that mindset, he simply skipped over the command prompt topics and found himself struggling later.

It's easy to think that these command prompt tools are archaic and simply not needed. I strongly suggest that you don't let yourself fall into that trap. There's a reason why CompTIA put these topics in the objectives. They're needed by technicians on the job.

Install and Configure a SOHO Network

Previous chapters have given you the information you need to install and configure a small office/home office (SOHO) network. For clarity, this section puts everything together. These are the steps you'd commonly take to install and configure a SOHO network today. You can also use these same steps to configure a network in your home.

The primary reasons to create a network are to share resources and to provide access to the Internet. With this in mind, you'll need different devices, cables, and protocols.

Figure 24-1 shows a typical SOHO network. Refer to this figure as you read through the following sections.

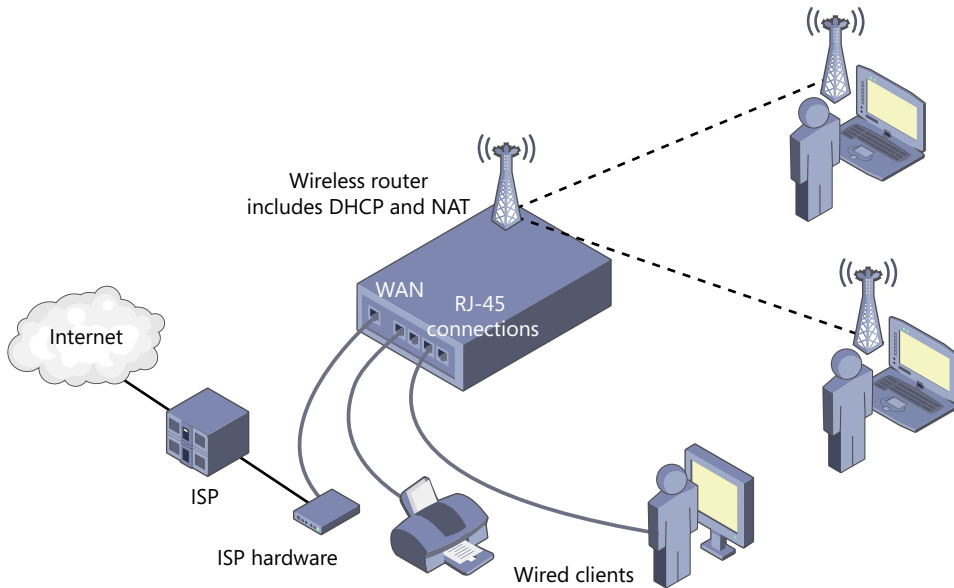


FIGURE 24-1 Components in a SOHO network.

Devices

A network that has Internet access requires the following hardware devices:

- **Internet access hardware.** This is typically provided by the Internet Service Provider (ISP). For example, you might have a broadband connection, and the ISP will lease or sell you a broadband modem. It could also be via a fiber connection, ISDN, DSL, or even through a satellite.
- **Wireless router.** The ISP connection plugs into the WAN connection of the wireless router, and the router provides connectivity for all internal clients. The wireless router has multiple components.
 - **Wireless access point (WAP).** The WAP provides access to wireless clients using Radio Frequency (RF) signals.
 - **Switch functionality.** Internal systems can communicate with each other through the switch capability of the wireless router.
 - **Wireless capability.** It's common to have a wireless router to provide connectivity for wireless clients. This isn't a requirement, but it does provide greater flexibility.

NOTE SWITCH FUNCTIONALITY AND WIRED ROUTERS

If you use a wired router instead of a wireless router, you will need to ensure that it also has built-in switch functionality. As an alternative, you can purchase an additional switch or hub to provide connectivity for multiple clients.

- **Network interface cards (NICs).** Each wired client needs a NIC. Common NICs have RJ-45 connectors for twisted-pair cable. A printer is shown as a wired client, but you can have a wireless printer instead.
- **Wireless adapters.** Wireless clients need to have wireless adapters that can communicate with the WAP. These are commonly built into laptops. It's also possible to purchase wireless adapter cards for desktop computers, or USB adapters that can plug into any open USB port.

Cables

Wired clients need to be connected with cables. Chapter 19, "Exploring Cables and Connectivity," covers a wide range of cables and connectivity, but a SOHO will typically use twisted-pair cable. Unshielded twisted-pair (UTP) cable with RJ-45 connectors is the most commonly used cable in SOHOs.

Three important points with the twisted-pair cable are as follows:

- If the devices support speeds of 1 Gbps or greater, you'll need to use at least CAT 5e cable.
- If the environment has an excessive amount of interference, you might need to use shielded twisted-pair (STP) cable.
- If the cables run through a plenum, you'll need to ensure that you're using plenum-safe cable.



EXAM TIP

CAT 5e or CAT 6 cable is required for Gigabit Ethernet. Plenum-safe cable is fire resistant and doesn't emit toxic fumes if it burns.

The wired clients connect to the wireless by router using straight-through cable. The connection from the WAN port of the wireless router to the ISP hardware often uses a crossover cable. If a device has an MDI/MDIX button, you can select MDIX instead of using a crossover cable.

MDI/MDIX is short for medium dependent interface (MDI)/medium dependent interface crossover (MDIX). Selecting MDIX mimics a crossover cable. Additionally, many newer devices will automatically sense the need for a crossover cable and automatically select MDIX for this connection.

Protocols

The Internet uses the Transmission Control Protocol/Internet Protocol (TCP/IP) suite, so all internal devices need to support TCP/IP.

Additionally, the wireless router will typically have the following protocols running:

- **Dynamic Host Configuration Protocol (DHCP).** DHCP provides internal clients with TCP/IP configuration. This includes an IP address, subnet mask, default gateway, and address of a Domain Name System (DNS) server.
- **Network Address Translation (NAT).** NAT translates public and private IP addresses. This allows internal clients to have private addresses but share the public IP address provided by the ISP.
- **Wireless protocols.** Wireless clients need to be running compatible wireless protocols. IEEE 802.11n is the fastest and is compatible with 802.11g. Therefore, you can have an 802.11n wireless router and a mixture of 802.11g and 802.11n wireless clients.

The wireless router usually acts as a DHCP client and a DHCP server. The WAN port connected to the ISP is configured as a DHCP client, and it receives TCP/IP configuration from the ISP. This includes a public IP address and the address of a DNS server on the Internet.

As a DHCP server, the wireless router provides internal clients with private IP addresses. It will also provide these internal clients with the address of the DNS server provided by the ISP.

VoIP

While it's not a requirement, many SOHOs also have basic Voice over Internet Protocol (VoIP) applications. These applications allow users to use the network connection for voice communications and multimedia sessions.

For example, users can subscribe to a service that allows them to use the Internet connection to make long-distance phone calls. In other cases, applications support video teleconferencing. Users can have meetings and conferences using the Internet connection.

Securing a SOHO Wired Network

In addition to making sure everything works, security is also an important consideration. The following key steps can be used to secure a SOHO wired network:

1. **Change default user names and passwords.** If computers or network devices have default user names and passwords, these should be changed. This is stressed in Chapter 23, "Exploring Wireless Networking," in the context of wireless networks, and the same steps should be followed with a wired network.
2. **Enable MAC filtering.** You can restrict which computers can access a network based on their MAC address. Chapter 23 shows how to do this on a wireless router, and the same concepts apply to a wired network.

- 3. Assign static IP addresses.** You can statically assign IP addresses instead of using Dynamic Host Configuration Protocol (DHCP) to dynamically assign them. This makes it more difficult for unauthorized systems to access your network but requires more effort. Chapter 21, “Comparing IPv4 and IPv6,” shows how to assign static IP addresses to Windows-based systems.
- 4. Disable ports.** You should enable only the firewall ports needed by the SOHO. By disabling unneeded ports, you ensure that unauthorized traffic over these ports is blocked. Chapter 20, “Understanding Protocols,” introduces the concepts of ports, and chapter 22, “Network Security Devices,” discusses ports in the context of firewalls.
- 5. Ensure physical security.** Physical security includes any security that you can touch. Ideally, computing devices such as servers and routers should be protected in a locked closet. Similarly, portable disk drives and other media with valuable data should be locked up when not in use.



Quick Check

1. What do most wireless routers include to provide systems with IP addresses?
2. What type of cable is used for a SOHO with Gigabit Ethernet?

Quick Check Answers

1. DHCP.
2. CAT 5e or CAT 6.

Establish Networking Connections

One of the great strengths of computers today is the ability to connect to a network and share resources. Many of the methods have been described in general terms within the Networking chapters. This section provides a review and includes some steps you'd take to connect to specific types of networks.

Wired

When connecting a client or desktop system to a wired network, you need to ensure that the system is physically connected and configured with the proper TCP/IP settings. Most internal networks use twisted-pair cable, so you'd connect the cable from the computer's NIC to a hub, router, or switch in the network.

The two ways of configuring TCP/IP are statically or dynamically. Chapter 21 includes details about both methods. If the wired network is using DHCP, simply configure the computer to get the settings dynamically. If the network is not using DHCP, assign the settings manually with an available IP address used within the network.

Wireless

The primary difference between connecting to a wireless network or a wired network is that the wireless network doesn't use cables. You need to ensure that a wireless access point (WAP) is functioning within the network and configure the client to connect to it.

Chapter 23 covers the wireless requirements. As a reminder, you'll need the following information:

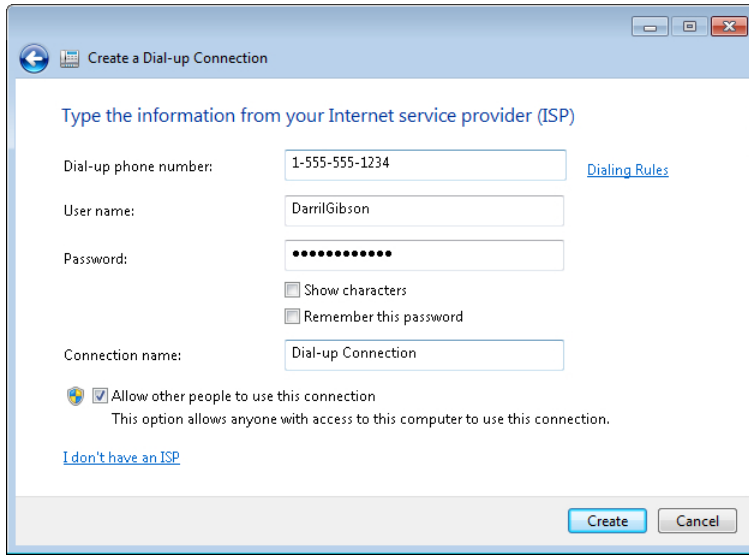
- The wireless standard (802.11a, b, g, or n) supported by the WAP
- The Service Set Identifier (SSID), which is the name of the wireless network
- The security method used by the WAP, such as Wi-Fi Protected Access version 1 (WPA) or 2 (WPA2)
- The passphrase or shared secret used by the security method

You configure TCP/IP on the wireless NIC just as you'd configure it on the wired NIC. It is more common to use DHCP, but you can statically assign them if desired.

Dial-Up Connections

A dial-up connection requires a modem, a connection to a phone line, and an Internet Service Provider (ISP) that supports a dial-up connection. You can use the following steps to create a dial-up connection on a Windows 7 computer:

1. Click Start and select Control Panel.
2. Select Network And Sharing Center.
3. Select Set Up A New Connection Or Network.
4. Select Set Up A Dial-Up Connection and click Next. The system will try to detect a modem in your system. If it isn't detected, you can still complete the steps. Click Set Up A Connection Anyway.
5. Enter the information required by your ISP. This includes the phone number used to connect to the ISP, your user name, and a password. You can rename the connection or leave it as Dial-up Connection.
6. Select the Allow Other People To Use This Connection check box or leave it unchecked. If the box is left unchecked, only the account used to create the connection will be able to use it. Your display will look similar to the following graphic.



7. Click Create and click Close.

At this point, you can click Connect To A Network from the Network And Sharing Center and select this dial-up connection.

WWAN (Cellular)

The steps that you'd use to connect to a cellular network are dependent on the cellular provider. For example, I have a wireless air card that I purchased from Verizon Wireless with a cellular contract. They have an application called VZAccess Manager that I use with this modem.

MORE INFO CHAPTER 18, "INTRODUCING NETWORKING COMPONENTS"

Chapter 18 included a section on cellular phone connections with a picture of a wireless air card. These are sometimes called USB dongles.

Figure 24-2 shows the VZAccess Manager in action. When I want to connect, I plug the card into my system, start the application, and click Connect. This application also gives an indication of the connection type (4G LTE) and the signal strength using bars.

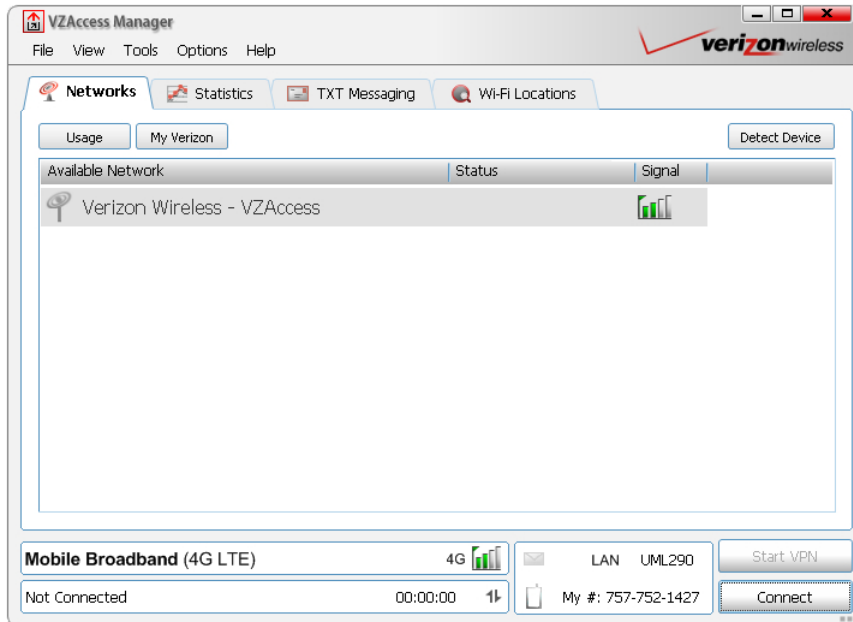


FIGURE 24-2 Connecting to cellular service.

VPN

A virtual private network (VPN) allows a user to connect to a private network over a public network. In most cases, the public network is the Internet. After a user is connected to the Internet, the user can connect to the private network.



For example, consider Figure 24-3. The user connects to the ISP using *Point-to-Point Protocol (PPP)*, and the ISP provides access to the Internet. After connecting to the Internet, a VPN connection creates a tunnel to the VPN server or to a firewall that forwards traffic to the VPN server. Users connected to the VPN server have access to any internal resources that they could normally access. For example, they can check their mail or access files.

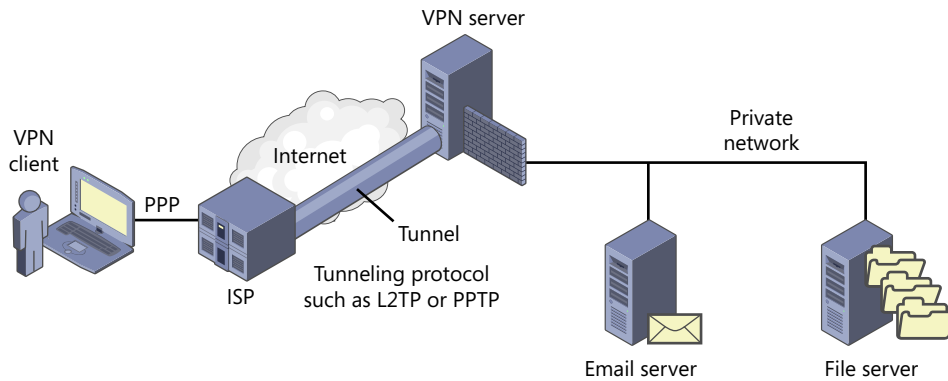


FIGURE 24-3 Connecting to a VPN server.



Several types of VPN tunneling protocols are in use. Two common ones are Layer Two Tunneling Protocol (L2TP) and *Point to Point Tunneling Protocol (PPTP)*. One of the challenges when sending data over a public network is that data can be intercepted, so most VPNs are encrypted. For example, L2TP uses *Internet Protocol security (IPsec)* to encrypt the data in the tunnel.

You can use the following steps to create a VPN connection on a Windows 7–based computer:

1. Click Start and select Control Panel.
2. Select Network And Sharing Center.
3. Select Set Up A New Connection Or Network.
4. Select Connect To A Workplace and click Next.
5. Select Use My Internet Connection (VPN). If your organization is hosting a remote access server with a modem, you can select Dial Directly. However, this direct dial connection is not considered a VPN.
6. Enter the IP address of the VPN server. You can get this from the company that is hosting the VPN. Click Next.
7. Enter a user name, password, and domain name (if required) that are authorized to connect to the VPN server. Click Connect.
8. The computer will try to connect to the VPN server by using all of the available tunneling protocols. When it finds a tunneling protocol that is accepted by the VPN server, it will use it.

Homegroups and Network Places

One of the reasons to create a network is to share network resources. Accessing these shared resources depends on the operating system version.

- **My Network Places.** In Windows XP, users can access resources via My Network Places.
- **Network.** Network replaced My Network Places in Windows Vista and Windows 7. The functionality is similar, although it looks a little different.
- **Homegroup.** Homegroups were introduced in Windows 7. This provides a simpler method of sharing and accessing resources on small networks, such as those used in SOHOs.



EXAM TIP

Homegroups are supported only on Windows 7–based computers. You can create a homegroup on a SOHO network that includes Windows XP and Windows Vista computers, but only Windows 7 computers will be able to join it.

Accessing My Network Places and Network

You can access My Network Places on Windows XP with the following steps:

1. Click Start and select My Computer.
2. In the left pane under Other Places, select My Network Places.
 - A. If the left pane is not showing, click the Tools drop-down menu and select Folder Options.
 - B. On the General tab, select Show Common Tasks In Folders in the Tasks section. Click OK.
3. Click View Workgroup Computers.

This will show you all devices on your network, and you can double-click any of these devices. You'll be able to see any shared folders that you have permissions to access.

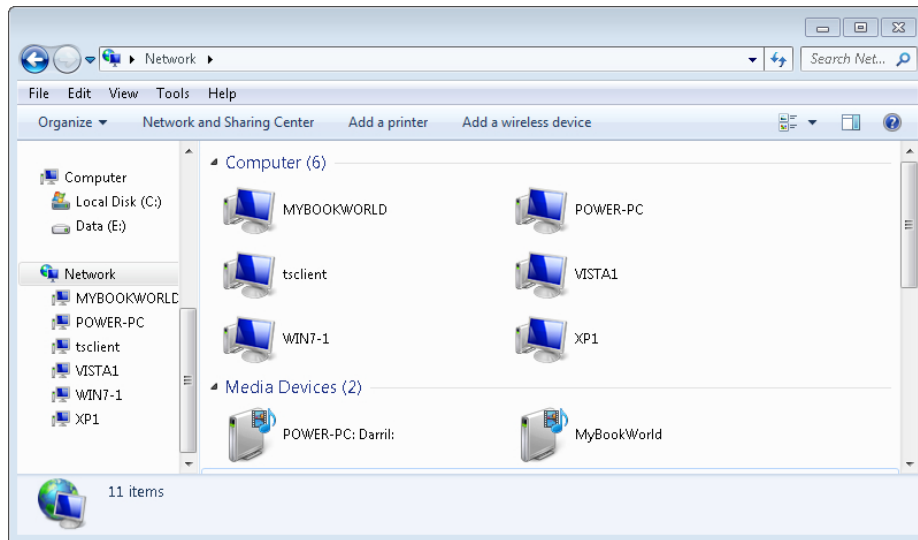
With Windows Vista and Windows 7, you don't use the term My Network Places, but you can access network locations on these systems with the following steps:

1. Click Start and select Computer.
2. Select Network.

NOTE DYNAMIC MENU

When you select Network, the choices on the menu ribbon change to give you additional options. They include the Network And Sharing Center, Add A Printer, and Add A Wireless Device selections.

3. The following graphic shows what you'll see on a Windows 7 computer. If you double-click any of these, you'll see a listing of resources shared by that system.



Understanding Homegroups

Windows 7 introduced *homegroups* as a simpler way to share resources in a network. Users can share any of their libraries with other users in the network.

MORE INFO CHAPTER 13, "USING WINDOWS OPERATING SYSTEMS"

Chapter 13 covers libraries in more depth. As a reminder, users can group common files into a library even if the files are stored in different locations.

The following three primary steps are related to using homegroups.

1. Create a homegroup on one Windows 7 computer in the network. This user also decides which libraries to share.
2. Other users running Windows 7–based systems join the homegroup. Users decide which libraries to share from their computer.
3. All users can now access resources shared on other systems.

The following sections describe the process of creating, joining, and using homegroups. You might also want to check out the videos on the following Microsoft sites:

- <http://windows.microsoft.com/en-us/windows7/Access-files-and-printers-on-other-homegroup-computers>
- <http://windows.microsoft.com/en-US/windows7/Join-a-homegroup>
- <http://windows.microsoft.com/en-US/windows7/help/videos/sharing-files-with-homegroup>

Additionally, Microsoft has created a comprehensive start-to-finish page on homegroups that you can check out if you want to dig a little deeper:

- <http://windows.microsoft.com/en-US/windows7/help/homegroup-from-start-to-finish>



EXAM TIP

HomeGroup is available in all editions of Windows 7. However, if you're running Windows 7 Starter or Home Basic edition, you cannot create a homegroup, but these systems can join a homegroup created on another Windows 7 system.

Creating a Homegroup

You can use the following steps to create a homegroup on a Windows 7–based computer.

1. Click Start, Control Panel. If necessary, change the view to Large Icons and select Homegroup.
2. On the Homegroup page, click the Create A Homegroup button.
3. Select the corresponding check box for the items that you want to share. You can share pictures, documents, music, and videos that are stored on your system. Selecting any of these check boxes will share your library in that category. You can also share printers configured on your computer. Click Next.
4. Windows 7 will create the homegroup and display a password. You can share this password with other users so that they can join the homegroup.
5. Click Finish.
6. The Change Homegroup Settings page appears. You can use this to change what is shared, view the password, change the password, and leave the homegroup.

NOTE SHARING FOLDERS

In addition to your libraries, you can share folders within the homegroup. Use Windows Explorer to browse to the folder you want to share. Right-click the folder and select Share With. Select Homegroup (Read) to give other users read access. Select Homegroup (Read/Write) to give other users the ability to read and write to the folder.

Joining a Homegroup

If another user has created a homegroup in your network, you can join it, share your libraries, and access other users' shared files.

1. Click Start, Control Panel. If necessary, change the view to Large Icons and select Homegroup.
2. Windows 7 will check the network for the existence of a homegroup. If one exists, it will display homegroup information and prompt you to join it.
3. Click Join Now to join the homegroup.
4. Select the corresponding check box for the items that you want to share from your computer on the homegroup. You can share pictures, documents, music, printers, and videos that are stored on your system. Click Next.
5. Enter the password of the homegroup and click Next.
6. A page will appear indicating that you have joined the homegroup. Click Finish.

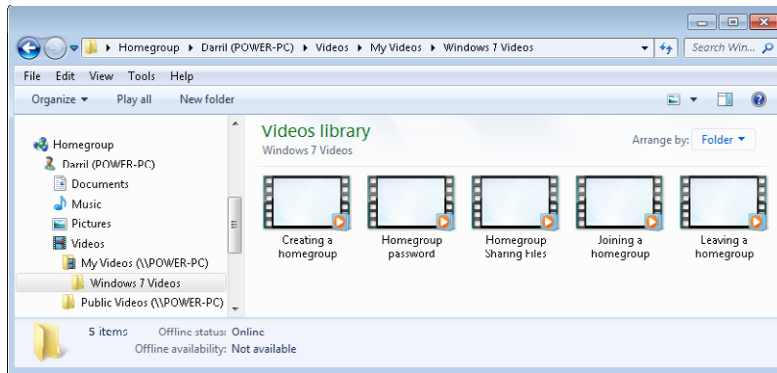
NOTE TROUBLESHOOTING HOMEGROUPS

Occasionally, homegroups develop problems, stopping other users from joining. The homegroup troubleshooter can sometimes correct the problems. If this doesn't work, another fix that often works is to leave the homegroup on each of the systems and then re-create it.

Viewing Homegroup Resources

After you've created and joined a homegroup, any user that has joined the homegroup can access resources on other homegroup systems. You can use the following steps on any computer in the homegroup:

1. Click Start and select Computer.
2. Select Homegroup in the left pane. Your display will resemble the following graphic. The graphic shows one other computer (Power-PC) in the workgroup hosted by a user named Darril. Darril is sharing the Documents, Music, Pictures, and Videos libraries from his system, and the Windows 7 Videos folder is opened. Any other user in the workgroup can copy or view these videos or any other shared files.



EXAM TIP

Windows 7–based systems support up to 20 concurrent connections. That is, a Windows 7–based computer can share files in a homegroup, and up to 20 other users at a time can connect to this system to access the files. In contrast, Windows XP Professional supports up to 10 concurrent connections.

Mapping Drives



When you share a folder on a computer, it can be accessed by other users as long as they know the *Universal Naming Convention (UNC)* path. A UNC path is in the format of `\\ComputerName\ShareName`. For example, if your computer was named `Success` and you shared a folder named `Notes`, other users could connect to it by using the UNC path of `\\success\notes`. UNC paths are not case-sensitive.

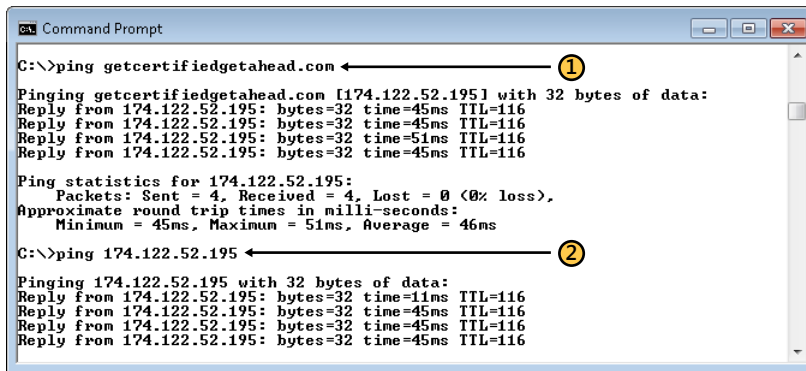
Users can enter the UNC path from the command prompt, the Run line, or the Search Programs And Files text box in Windows 7.

While the UNC path will connect users to the share, it's often confusing to users. Instead of requiring users to remember the UNC path, you can map a drive letter to the path. The drive will appear in Windows Explorer and can be accessed with a simple drive letter.

Mapped drives can be created from Windows Explorer in any Windows-based system. The following steps show how to map a drive on Windows 7.

1. Click Start and select Computer. This starts Windows Explorer.
2. Select Map Network Drive from the Tools drop-down menu. If the menu bar isn't showing, you can click Organize, Layout, Menu Bar to display it. Alternatively, you can click Map Network Drive on the menu along the top.
3. You can change the drive letter or leave it as is. Enter the UNC path in the Folder text box in the format of `\\ComputerName\ShareName`.

4. Select Reconnect At Logon to ensure that the mapped drive appears each time the user logs on. Your display will look similar to the following graphic.



```
Command Prompt
C:\>ping getcertifiedgetahead.com
Pinging getcertifiedgetahead.com [174.122.52.195] with 32 bytes of data:
Reply from 174.122.52.195: bytes=32 time=45ms TTL=116
Reply from 174.122.52.195: bytes=32 time=45ms TTL=116
Reply from 174.122.52.195: bytes=32 time=51ms TTL=116
Reply from 174.122.52.195: bytes=32 time=45ms TTL=116

Ping statistics for 174.122.52.195:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 45ms, Maximum = 51ms, Average = 46ms

C:\>ping 174.122.52.195
Pinging 174.122.52.195 with 32 bytes of data:
Reply from 174.122.52.195: bytes=32 time=11ms TTL=116
Reply from 174.122.52.195: bytes=32 time=45ms TTL=116
Reply from 174.122.52.195: bytes=32 time=45ms TTL=116
Reply from 174.122.52.195: bytes=32 time=45ms TTL=116
```

5. Click Finish.

The graphic also shows how a mapped drive appears in Windows Explorer after it has been created. This network includes a server named archive used for file sharing. It includes folders named public and APlusNotes. Public is mapped to the Z drive, and the previous steps will map the APlusNotes folder to the Y drive.



Quick Check

1. What is used in Windows 7 to allow users to easily share data in a SOHO?
2. What is the maximum number of concurrent connections allowed in Windows 7?

Quick Check Answers

1. Homegroups.
2. 20.

Command Prompt Tools

You can often troubleshoot connectivity issues from the command prompt and quickly identify a network problem. As with any tool, the key is to know which tool to use for which problem. This section provides an overview of common command prompt tools you can use, along with information about how to use them.

As a quick reminder, you can start the command prompt on a Windows 7 system by clicking Start, typing **command** in the Search Programs And Files text box, and selecting command prompt.

MORE INFO CHAPTER 14, “USING THE COMMAND PROMPT”

The command prompt is covered in Chapter 14. It shows how to start and use the command prompt, including how to start it with administrative privileges when needed. If you get an error indicating that the command requires elevation, it means that you must run it from a command prompt with administrative privileges.

The following sections describe these tools in more depth. As a short introduction, the following is a summary of the important tools:

- **Ping.** Checks connectivity with a device on a network and identifies response times.
- **Ipconfig.** Displays TCP/IP configuration assigned to network interface cards.
- **Tracert.** Checks connectivity with a device and shows routers in the path.
- **Nslookup.** Verifies that DNS can resolve a host name to an IP address. It can verify that a record exists in DNS.
- **Netstat.** Shows network statistics, including a list of inbound and outbound connections for a system.
- **Nbtstat.** Shows statistics for NetBIOS.
- **Arp.** Shows MAC address to IP address mappings.
- **Net Use.** Used to map drives to remote shares.

The command prompt is easier to learn through experience. That is, don't just read about it—do it. I strongly encourage you to type each of the commands covered in this section to see the results. You will probably make some typos. That's natural and actually helpful. If everything works perfectly the first time, you probably won't remember it as easily.

NOTE COMMAND-LINE REFERENCE

This chapter covers some command prompt commands and basic usage. If you want to dig deeper, check out Microsoft's Command-line Reference, which covers all the commands you have available, at <http://technet.microsoft.com/library/cc754340>.

Ping



Ping is an invaluable tool for checking connectivity between two devices. For example, if you're having trouble connecting to another computer, you can use ping to verify that you have network connectivity.

The basic syntax is as follows:

```
Ping target
```

The target can be either the IP address or the name of a destination computer. For example, if the IP address of your default gateway is 192.168.1.1, you can use the following command to check connectivity:

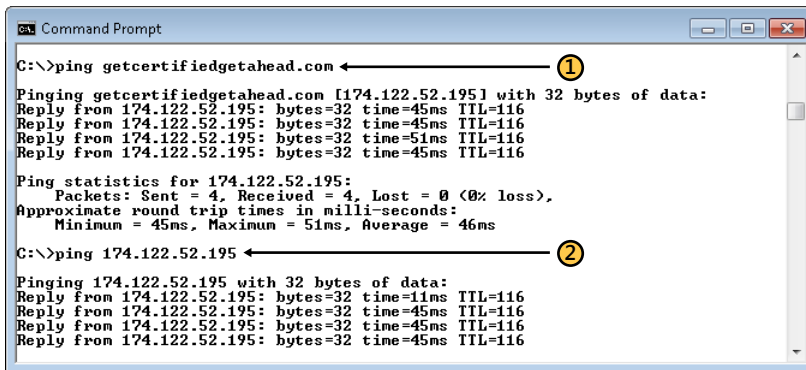
```
Ping 192.168.1.1
```

If you instead want to check connectivity with a server named mail1 in your network, you can use the following command:

```
Ping mail1
```

Ping will resolve the name of the server (mail1) to an IP address. It usually does so by querying DNS.

Figure 24-4 shows an example of the ping utility in action. The first command (ping getcertifiedgetahead.com) pings the website by the name, and the second command (ping 174.122.52.195) pings the website by using the website's IP address. Both commands sent four pings to the server and successfully received four replies, indicating that the site is reachable.



```
Command Prompt
C:\>ping getcertifiedgetahead.com
Pinging getcertifiedgetahead.com [174.122.52.195] with 32 bytes of data:
Reply from 174.122.52.195: bytes=32 time=45ms TTL=116
Reply from 174.122.52.195: bytes=32 time=45ms TTL=116
Reply from 174.122.52.195: bytes=32 time=51ms TTL=116
Reply from 174.122.52.195: bytes=32 time=45ms TTL=116

Ping statistics for 174.122.52.195:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 45ms, Maximum = 51ms, Average = 46ms

C:\>ping 174.122.52.195
Pinging 174.122.52.195 with 32 bytes of data:
Reply from 174.122.52.195: bytes=32 time=11ms TTL=116
Reply from 174.122.52.195: bytes=32 time=45ms TTL=116
Reply from 174.122.52.195: bytes=32 time=45ms TTL=116
Reply from 174.122.52.195: bytes=32 time=45ms TTL=116
```

FIGURE 24-4 Using ping.

Notice that the first example resolves the name to an IP address. The first line after the command (Pinging getcertifiedgetahead.com [174.122.52.195]) shows that it identified the address of the site as 174.122.52.195. This also verifies that it was able to query DNS to get the IP address of the web server.

You can also see in the figure that ping shows the approximate roundtrip time. This gives you an indication of the response time of the remote computer. These times are shown in milliseconds, and for reference, 1,000 msec equals one sec.

MORE INFO CHAPTER 21, “COMPARING IPV4 AND IPV6”

Chapter 21 briefly introduces ping in the context of TCP/IP. It shows how you can use the ping command with the loopback address (as ping 127.0.0.1) to check the TCP/IP stack. You can also ping the name localhost (as ping localhost), because systems automatically resolve the name localhost to the loopback address.

If ping cannot reach a computer, you'll see a "Request timed out" error listed four times instead of four Reply From messages. This does not necessarily mean that the other computer is not operational. Many firewalls block ping requests, so a system can be operating but be configured so that it does not respond to pings.

Windows-based systems send four ping packets out and expect to receive four packets back. In contrast, Linux systems will constantly ping a system until you press Ctrl+C to stop the command.

You can use the `-t` switch on Windows systems so that the ping command has the same functionality as it does on Linux systems. For example, if you think a problem might be related to a loose connection in a cable, you might want to wiggle the cable around to see whether your symptoms change. You can use the following command and then watch the display as you manipulate the cable:

```
ping 192.168.1.1 -t
```



EXAM TIP

Ping is used to check connectivity with other network devices. If you ping the name, your system must be able to resolve the name to an IP address, and DNS is commonly used to resolve names to IP addresses. You can use the `-t` switch on Microsoft systems to cause ping to continuously repeat until you press Ctrl+C keys.

Table 24-1 shows common switches used with the ping command. The help for ping shows switches listed with a dash (-). However, you can use any of the switches with a dash or a forward slash. This is the same for many other command prompt commands.

TABLE 24-1 Common Ping Switches and Examples

Switch and Example	Usage
-? ping -?	View help on the ping command.
-t ping 192.168.1.1 -t	Continue sending until stopped. You can stop the ping by pressing Ctrl+C.
-l nn ping 192.168.1.1 -l 16	Modify the buffer size with a lowercase <i>L</i> and a number. The example changes the buffer size to 16 bytes.
-4 ping server1 -4	Force ping to use IPv4. It will first resolve the name to an IPv4 address and then ping it with the IPv4 address.
-6 ping server1 -6	Force ping to use IPv6. This resolves the name to an IPv6 address and then pings the IPv6 address.

Ping and Sonar

The late Mike Muus wrote the original ping program and named it after the sound that sonar makes. Sonar sends a sound wave to another object, and when the sound wave hits the object, it returns. Based on how long it takes for the wave to return, it's possible to identify the distance between the two objects. Similarly, the ping program can measure the time it takes for a packet to travel to and from a remote system.

Submarines use sonar all the time. In war time, they send these sound waves to locate enemies, and enemies can also locate submarines using sonar. If you've watched any submarine movies, such as *Hunt for Red October*, you've probably heard the "ping" sound when a sound wave hits the hull of the submarine.

Ipconfig



Ipconfig (short for IP configuration) is an easy tool you can use to view the TCP/IP configuration on a system. *Ipconfig* is both simple and complex. When you use it without any switches, it gives you a quick indication of the configuration. However, you can also use *ipconfig* with switches to do much more.

As a simple example, the following code shows what you'll see if you enter *ipconfig* on a Windows 7-based system:

```
C:\>ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection:
    Connection-specific DNS Suffix  . :
    IPv4 Address. . . . . : 169.254.8.51
    Subnet Mask . . . . . : 255.255.0.0
    Default Gateway . . . . . :
```

This computer is unable to communicate on the network. Do you know why?

Chapter 21 introduces IP addressing, including Automatic Private IP Addressing (APIPA). As a reminder, an APIPA address always starts with 169.254. Additionally, APIPA addresses are assigned to DHCP clients when they do not receive a response from a DHCP server.

You don't necessarily know why you can't reach DHCP. However, this is the problem you'd need to pursue.

On the other hand, if *ipconfig* shows a valid IP address and the default gateway, you could then use the ping command. You could do any of the following:

- Ping the default gateway to determine connectivity
- Ping the IP address of the NIC to verify that it can respond
- Ping the loopback address to verify the TCP/IP stack



EXAM TIP

When troubleshooting connectivity issues, ping and ipconfig are two of the most commonly used tools. You can often identify a problem by first checking the TCP/IP configuration with ipconfig and then checking connectivity with ping.

Table 24-2 shows some of the common switches used with the ipconfig command, along with sample usage.

TABLE 24-2 Common Ipconfig Switches and Examples

Switch and Example	Usage
-? ipconfig /?	View help on the ipconfig command. This provides a listing of all switches available.
/all ipconfig /all	View full TCP/IP configuration information. This identifies the host name, the media access control (MAC) address, the address of a DNS server, the address of a DHCP server address (if it is a DHCP client), and more.
/release ipconfig /release	Release the IPv4 address. Use this on DHCP clients to remove all DHCP assigned information.
/renew ipconfig /renew	Renew the IPv4 address. Use this on DHCP clients to renew all DHCP assigned information.
/release6 ipconfig /release6	Release the IPv6 address. Use this on DHCP clients to remove all IPv6 assigned settings.
/renew6 ipconfig /renew6	Renew the IPv6 address. Use this on DHCP clients to renew IPv6 DHCP assigned settings.



EXAM TIP

If a client can't reach DHCP, DHCP clients assign themselves an APIPA address. After repairing the problem, you can use ipconfig /renew to get a new IP address from DHCP. If you want to get a new IP address from DHCP, use ipconfig /release and then ipconfig /renew.

Many Unix-based systems also support ifconfig in addition to ipconfig. The ifconfig command has more capabilities than ipconfig, and technicians use it to configure the network interface card.

Client-Side DNS and Ipconfig

Chapter 20 discusses client-side DNS. As a reminder, the hosts file (located in the C:\Windows\System32\drivers\etc folder by default) includes name-to-IP address mappings used by a computer. If a host name is in this file, the computer will always use that IP address instead of querying DNS.

Some viruses have modified the hosts file, causing problems for computers. For example, some viruses have modified them by giving a bogus IP address for Microsoft's Windows Update website. When a user attempts to update the operating system, the system goes to the bogus IP address instead of the Windows Update site. The result is that the system cannot be updated.

You can detect problems like this by using the following two additional ipconfig switches:

```
ipconfig /displaydns
```

```
ipconfig /flushdns
```

The first command (/displaydns) displays the contents of the host cache (sometimes called the DNS cache). These cached entries come from the hosts file and from recent responses from DNS.

You can remove all the cached entries from DNS responses with the /flushdns switch. However, this command does not remove entries from the hosts file. If you flush the cache and then immediately display the cache, you'll see entries that originate from the hosts file.

Tracert



Tracert is another tool you can use to check connectivity between two devices. However, *tracert* goes a step further. It will trace the path or route (think of it as trace route) showing all the routers between the two devices. The basic command is:

```
tracert target
```

Similar to the ping command, the target can be either the IP address or the name of a destination computer. Therefore, if a file server named File1 has an IP address of 192.168.15.19, you can use either of the following commands:

```
tracert 192.168.15.19
```

```
tracert file1
```

For example, consider Figure 24-5, which shows a network with multiple routers. Imagine that Gail is unable to reach the file server. Gail can ping the default gateway (on Router 1), and this succeeds, but she finds that she cannot ping the file server. Where is the problem?

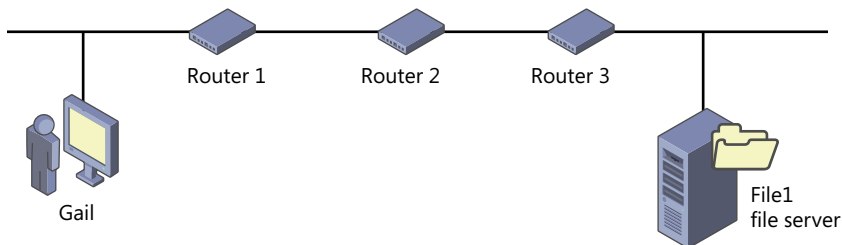


FIGURE 24-5 Network with multiple routers.



EXAM TIP

Tracert checks connectivity just as ping does but is much more useful if you have multiple routers in the network. If a faulty router is in the path, ping fails without any indication of why. Tracert helps the technician identify the router that is likely the problem.

Tracert will trace the path through each of the routers and identify where the path stops. In this context, the routers are often referred to as hops, and tracert can evaluate the hops.

You can also use tracert to trace the path to a site over the Internet. For example, if you want to identify all the routers between you and a site named Getcertifiedgetahead.com, you could use the following command:

```
tracert getcertifiedgetahead.com
```

You probably aren't going to be troubleshooting Internet problems very soon. However, if you were, tracert might be one of the tools you'd use to identify Internet router problems. Table 24-2 lists some switches and examples.

TABLE 24-2 Common Tracert Switches and Examples

Switch and Example	Usage
-d Tracert darrilgibson.com -d	Do not resolve addresses to host names. Only IP addresses are listed.
-4 Tracert darrilgibson.com -4	Use only IPv4 in the trace.
-6 Tracert darrilgibson.com -6	Use only IPv6 in the trace.



Quick Check

1. Name two commands you can use to check connectivity between two systems.
2. List the two commands used to get a new IP address from a DHCP server.

Quick Check Answers

1. Ping and tracert.
2. Ipconfig /release and ipconfig /renew.

Nslookup



Nslookup (short for name server lookup) is often used to troubleshoot name resolution problems with DNS. It queries DNS and can verify that records exist in DNS to resolve host names to IP addresses. It can help you determine whether a system can map a host name to an IP address by querying DNS.

MORE INFO CHAPTER 20, “UNDERSTANDING PROTOCOLS”

Chapter 20 covers name resolution and name resolution protocols in more depth. In short, DNS is used to resolve host names to IP addresses. Host names are used on the Internet and in many internal networks.

Nslookup is a *shell* command, which means that if you type just **nslookup** and press Enter, you'll start the shell and see a prompt of ">". You'll then be able to enter nslookup commands from the shell. However, you can also enter nslookup commands directly from the command prompt. The basic command is as follows:

```
nslookup hostname
```

For example, suppose you have problems reaching the Getcertifiedgetahead.com site. You might want to determine whether DNS can resolve the name to an IP address. You can use the following command:

```
nslookup getcertifiedgetahead.com
```

When I run this command on my system, I get the following result:

```
Server:  cdns1.cox.net
Address:  68.105.28.11
Non-authoritative answer:
Name:     getcertifiedgetahead.com
Address:  174.122.52.195
```

The DNS server providing the response is identified in the first two lines as cdns1.cox.net, along with its IP address (68.105.28.11). The last two lines show that the DNS server can resolve the site to the IP address of 174.122.52.195.

NOTE NON-AUTHORITATIVE ANSWERS

A non-authoritative answer indicates that the DNS server doesn't host the record to map the computer to an IP address. However, it can query other DNS servers to get the answer. If the DNS server hosts the record, it will not include the line "Non-authoritative answer" in the response.

Netstat



Netstat (short for network statistics) is a useful command you can use to view inbound and outbound TCP/IP connections. It allows you to quickly view network activity and identify what is generating the activity. Table 24-3 shows some common switches used with netstat.

TABLE 24-3 Common Netstat Switches and Examples

Switch and Example	Usage
-? netstat -?	View help on netstat.
-a netstat -a	Show all connections and ports. This is very useful for viewing Internet connections.
-b netstat -b	List the application associated with each connection. You can combine this with the -a switch (netstat -b -a).
-s netstat -s	Show statistics for protocols. This will list statistics for TCP, UDP, and IP statistics for both IPv4 and IPv6.

NOTE USING NETSTAT TO DETECT CONNECTIONS

Netstat can sometimes identify activity caused by virus infections. For example, if a system was joined to a botnet after a virus infection, netstat will show connections to Internet systems with public IP addresses even if web browser sessions aren't active.

For a quick exercise to see netstat in action, try the following steps:

1. Close all applications that have Internet access.
2. Open a command prompt, run the following command to list all of the current connections, and write the information into a file named Connections.txt:

```
Netstat -a > connections.txt
```
3. Enter the following command to open up the text file you just created in Notepad:

```
notepad connections.txt
```
4. Open Internet Explorer, and visit an Internet website.
5. With Internet Explorer still open, run the following command at the command prompt:

```
Netstat -a
```
6. If you compare the output with the connections.txt file, you can see the connections your system created when you visited the website. Many websites create multiple connections.

Nbtstat



Nbtstat is a command-line tool used to troubleshoot Network Basic Input/Output System (NetBIOS) name resolution. NetBIOS names are primarily resolved to an IP address by a WINS server and used only on internal networks. Nbtstat is one of the few commands that use case-sensitive switches. That is, nbtstat -r is different from nbtstat -R.

When a Windows Internet Name System (WINS) client is turned on, it contacts the WINS server and registers its name and IP address. Other clients can then query the WINS server with the name, and the WINS server responds with the IP address. Clients can also use broadcasts to resolve NetBIOS names.

MORE INFO CHAPTER 20, “UNDERSTANDING PROTOCOLS”

Chapter 20 covers name resolution and name resolution protocols in more depth. In brief, WINS is used to resolve NetBIOS names. NetBIOS names are used only on internal networks, and some internal networks use only host names. In contrast, host names are resolved by DNS and used on the Internet and in internal networks.

Nbtstat is short for NetBIOS over TCP/IP statistics. Table 24-4 shows some common switches used with nbtstat, with some examples.

TABLE 24-4 Common Nbtstat Switches and Examples

Switch and Example	Usage
-c nbtstat -c	Lists known system names and their IP addresses. These are placed in cache after being resolved to an IP.
-r nbtstat -r	Lists all the names resolved by broadcast and via WINS.
-R nbtstat -R	Purges and reloads the remote cache name table from the lmhosts file (if it exists).
-RR nbtstat -RR	Release/Refresh. This first releases the name registration with WINS and then refreshes the name registration. This is useful if WINS has the incorrect IP address registered for the client.

Arp



Arp is a command-line tool you can use to show MAC and IP address mapping. Before seeing what it does, it helps to understand some background information.

As discussed in Chapter 21, NICs have MAC addresses assigned to them. The MAC address is sometimes called a physical address. A MAC address is 48 bits long and is shown as six hexadecimal pairs, like this: 68-7f-74-ae-8b-de.

Additionally, NICs have IP addresses assigned. In many situations, TCP/IP has an IP address of another system but it needs to know the MAC address. The Address Resolution Protocol (ARP) is used to identify the MAC address from the IP address. Each time a system needs to know the MAC address of another system, it broadcasts the IP address, essentially asking, “Who has this IP address?”

The system with the IP address responds with its MAC address. The first system then stores the results in a short-term memory cache called the ARP cache, which brings us to the `arp` command. You can view the contents of the ARP cache with the `arp -a` command as follows:

```
C:\>arp -a
Interface: 192.168.1.111 --- 0xa
  Internet Address      Physical Address      Type
  192.168.1.1          68-7f-74-ae-8b-de    dynamic
  192.168.1.107        00-90-a9-82-4b-5f    dynamic
. . .
```

This first shows the IP address of the NIC listed as Interface. If your system has more than one interface, it will list the mappings for each. For brevity, I've shortened the output, but as you can see, the command lists the Internet address (the IP address), the physical address (the MAC address), and the type of storage.

If the result is from an ARP query, it is listed as dynamic and stays in cache for just a few minutes. If the mapping was added manually or by the operating system, it is listed as static.

Resolving Names, IPs, and MACs

You might have noticed that TCP/IP uses several resolution processes. You and I use words and names, but computers use numbers. Moreover, computers use different types of numbers in networking. Overall, here's the process:

- Computers have names. People commonly use names to identify the computers.
- DNS resolves computer names (host names) to IP addresses. You can use the `nslookup` name command to verify that DNS can resolve a name to an IP address. In some cases, WINS is used to resolve NetBIOS names to IP addresses.
- NICs are assigned IP and MAC addresses. MAC (or physical) addresses are often burned into the card, but IP addresses are changed frequently.
- ARP resolves IP addresses to MAC addresses. You can use the `arp -a` command to show the addresses that ARP has resolved and is currently storing in cache.

Net



The `net` command has multiple uses. One of the common uses related to networking is the `net use` command. It allows you to map a drive to a shared folder on a remote system. The basic syntax is as follows:

```
net use driveLetter UNCPath
```

In the "Mapping Drives" section earlier in this chapter, you saw how you could map a drive to a UNC path with Windows Explorer. The `net` command does the same thing, but from the

command prompt. For example, imagine that your network includes a server named DC1 and that this server is sharing a folder named Data. The UNC path is \\dc1\data.

One way you could connect to this share from a Windows 7–based system is by entering \\dc1\data in the Search Programs And Files text box. However, you can also map the share to a drive so that it is accessible in Windows Explorer. You’d do so with the following command:

```
net use p: \\dc1\data
```

This command maps the P drive letter to the share. When viewed in Windows Explorer, it would resemble Figure 24-4.

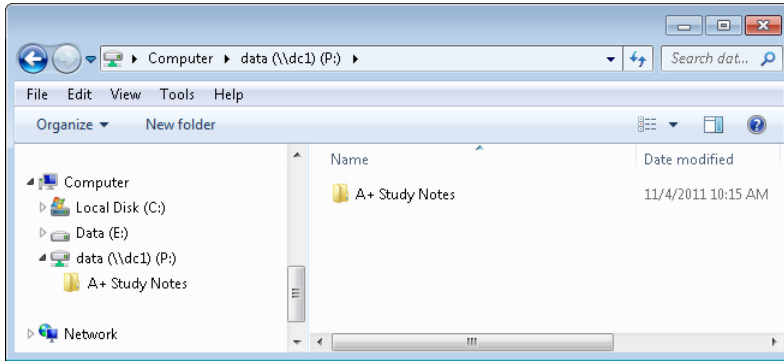


FIGURE 24-6 Viewing a mapped drive in Windows Explorer in Windows 7.

When a share is mapped this way, users can access the data just as if it were a folder on their system. If you want to delete the mapping, you can use the following command:

```
Net use p: /delete
```

This doesn’t delete the share on the server. It deletes only the mapping so that is no longer visible in Windows Explorer.

Table 24-5 shows some other common net commands you might find useful.

TABLE 24-5 Common Net Commands

Command	Usage
Net use	Shows mapped drives.
Net view	Shows a list of remote shares known to the system. These are often listed in the Network area of Windows Explorer.
Net share	Lists all files shared on the local system.
Net statistics workstation	Shows basic statistics on data sent and received.
Net statistics server	Shows connections for a system sharing folders, including how many files have been accessed in the current session.



Quick Check

1. What command can you use to view open connections on a system?
2. What command shows you a listing of MAC addresses matched to IP addresses?

Quick Check Answers

1. Netstat -a.
2. Arp -a.

Hardware Tools

Many of the easy troubleshooting steps are from the command prompt. However, you might need to use one of the hardware tools described in this section to help when troubleshooting network problems.

Cable Tester



Cable testers are handy tools used to ensure that cables are wired correctly and that there aren't any breaks in the cable. Most cable testers allow you to plug in both ends of the cable to verify that each of the wires within the cable is connected.

Some cable testers have LED displays that show a picture of the connection. For example, if you plug a crossover cable into both connectors, it will show you a display with the wires crossed over. Plug in a straight-through cable, and it shows the wires going to the same pins on both connectors. If you plug in a faulty cable, it will show the wires that are broken or not connected.

Loop Back Plugs



A *loop back plug* is a small plug that you can plug into a jack that loops output signals back into the device. For example, an RJ-45 loop back plug is just a connector that loops signals from output pins to input pins. It simulates plugging the NIC into a network.

After plugging in the loop back plug, you can ping the IP address of the computer. This will verify the NIC is functional.

Toner Probe

Sometimes you'll need to trace a cable from one room to another. For example, imagine that you have 50 identical white wires going from room 101 to room 405. You've located wire 22 in room 101. You now need to locate wire 22 in room 405. How can you do it?

In some cases, you can manually trace a cable or wire by using the hand-over-hand method. This can be tedious, and it isn't always feasible, especially if you have to trace a cable between floors. A better option is a toner probe.



Toner probes have two elements. One creates a tone and has alligator clips that you can use to connect it to a wire. When you connect it and turn on the tone, the signal travels down the wire. The second element usually has a speaker and a probe that you can use to touch a cable or wire. In this example, you'd connect the tone to the wire in room 101. You'd then go to room 405 and connect the speaker probe to each of the wires until you heard the tone. When you hear the tone, you've found the wire.



Quick Check

1. What tool can you use to verify that a cable is not wired incorrectly?
2. After plugging in a loop back plug, what can you ping to verify that the NIC is working?

Quick Check Answers

1. Cable tester.
2. The IP address assigned to the NIC.

Troubleshooting Network Problems

This section provides a short summary of actions you can take to resolve some common networking problems. The goal in this section is to put the networking topics into context for common on-the-job networking problems.

Cannot Communicate on the Network

The most common symptom is that a system cannot communicate at all. Use the following quick checks to narrow down the problem:

1. Use **ipconfig** to determine the system configuration.
 - A. If the IP address is an APIPA address (starting with 169.254), it indicates that it's a DHCP client but that it can't reach a DHCP server.
 - B. If it isn't an APIPA address, note the IP address and subnet mask.
2. Verify that the IP address and subnet mask are correct for the network. Chapter 21 describes how to determine the network ID.
 - A. If the information was manually assigned, it might have been entered incorrectly. Use **ipconfig /all**. If it does not show a DHCP server in the listing, it indicates that the information was manually assigned.

- B.** If possible, use **ipconfig** on a system that is working and compare the configuration. Enter an IP address and subnet mask using the correct network ID if necessary.
- 3.** Ping the loopback address (127.0.0.1). If this fails, it indicates a problem with the TCP/IP stack within the operating system. A reboot might resolve the problem.
- 4.** Ping the IP of the NIC. This will verify that the NIC is functional. You might also choose to use a loopback plug and ping the NIC to eliminate any issues on the network as possible causes.

Cannot Get out of Network

In some cases, a system can access resources on the network but not any resources on other networks. For example, a user might be able to print to a network printer but can't access the Internet.

In this case, check the default gateway with the following steps:

- 1.** Use **ipconfig** to determine the IP address of the default gateway.
 - A.** Verify that an IP address for the default gateway is assigned. If not, correct the IP configuration for the NIC.
 - B.** Verify that the default gateway is on the same network as the computer. Both share the same subnet mask and need to have the same network ID.
- 2.** Ping the default gateway.
 - A.** If successful, the problem is probably with the router or somewhere after the router.
 - B.** If pings to the default gateway are not successful, the problem might be with the cabling between the switch and the router.
- 3.** Verify that a valid IP address is assigned for the DNS server. You can check this with **ipconfig /all**. Without a valid DNS address, the system won't be able to access systems beyond the default gateway by using host names. You will be able to ping remote systems with IP addresses, but pings to remote systems using their host names will fail. For example, the following will fail:

```
ping getcertifiedgetahead.com
```

But this will succeed:

```
ping 174.122.52.195
```


Remember the Lights

Networking devices have LEDs that provide a quick indication of connectivity and activity. This includes network interface cards, switches, and routers. If you're troubleshooting a problem, a quick look at the lights can help you identify problems.

These indicators are discussed in Chapter 18, "Introducing Networking Components," and Chapter 19, "Exploring Cables and Connectivity." To summarize, possible indicators include the following:

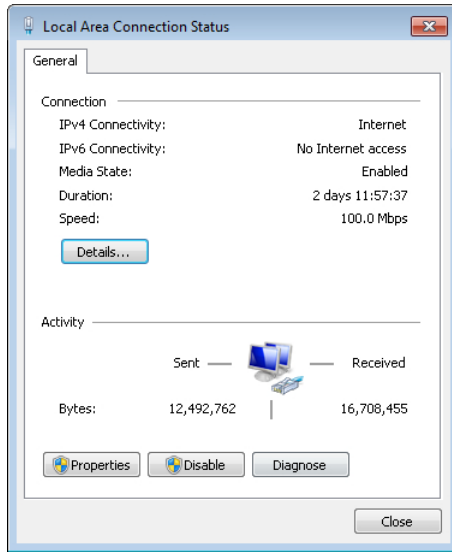
- **No light.** Indicates no connection, either because the cable is faulty or because one of the devices is faulty.
- **Steady activity light.** The activity light should be blinking, so if it is steady, there is no network activity. Resetting the device might help. For example, if all the lights on a switch are steady green, power cycling the switch might clear the problem.
- **Different colored light (duplex mode).** Many devices show one color (such as green) when the device is running in full-duplex mode and another color (such as amber) when the device is running in half-duplex mode.
- **Different colored light (speed).** Many devices show one color for one speed and another color for a different speed.

If you see different-colored lights for any connection, verify that both devices support the faster mode and speed. You should also verify that autosense is enabled. If autosense is not enabled or not a feature of the device, you might need to manually configure the faster mode or speed.

Use Windows Network Diagnostics

Another tool that is sometimes useful is the Windows Network Diagnostics included with Windows 7. For example, if you're having problems with connectivity, you might be able to just click a couple of buttons and let Windows resolve the problem. You can start Windows Network Diagnostics for a NIC with the following steps:

1. Click Start, Control Panel. If necessary, switch to Large Icons view.
2. Select Network And Sharing Center from the Control Panel list.
3. Select the connection in the View Your Active Networks section. This is commonly named Local Area Connection.
4. Your display will resemble the following graphic. Click the Diagnose button. Windows will run through a series of diagnostics and attempt to resolve the problem.



Common Symptoms

The previous section described methods used to troubleshoot network problems. In summary, the following list shows common symptoms and the likely causes:

- **No connectivity.** This indicates a problem with the NIC or the connection. Check the link lights, cables, and connections.
- **APIPA address.** An address starting with 169.254 is a clear indication that the system is a DHCP client but that it was not able to reach DHCP.
- **Local connectivity.** This indicates that the client can communicate with systems on the same local subnet but not on any other subnets. Ensure that the default gateway is configured correctly and that the router is functioning.
- **Limited connectivity.** This indicates that the client can connect to some devices or networks but not to all of them. If the client can't connect to only a specific device, such as a server in the network, check that device. Routers are used to provide connectivity to other networks, so if you can't reach another network, check the routers in the path.
- **IP conflict.** If two devices on the same network have the same IP address, it results in an IP address conflict. If a Windows-based system detects that it has the same IP address as another system, it assigns itself an IP address of 0.0.0.0, allowing the first device that has the duplicated address to function. Additionally, you'll see error messages on Windows-based systems, indicating that there is a conflict. The solution is to identify the devices and change one of the IP addresses.

Chapter Summary

- A SOHO network with Internet access includes hardware to connect to the ISP, a router (commonly a wireless router), and NICs on internal systems.
- Common networks use twisted-pair cabling. Gigabit Ethernet networks require at least CAT 5e twisted-pair.
- TCP/IP is required for a network connected to the Internet. Additionally, internal networks commonly use DHCP to assign IP addresses, and NAT to translate public and private IPs.
- Windows XP uses My Network Places to access many network resources.
- Windows 7 uses homegroups to share and access resources on other Windows 7–based systems. Homegroups are supported on all Windows 7–based systems but cannot be created on Windows 7 Starter or Home Basic editions.
- A mapped drive assigns a drive letter to a shared folder on another system.
- Ping is used to check connectivity with systems and identify response times. Pinging the loopback address (127.0.0.1) verifies the TCP/IP stack.
- Ipconfig is used to view IP configuration information. The /release switch can be used to release an IP address assigned by DHCP, and the /renew switch requests a new IP address from DHCP.
- Tracert traces the path through all routers between two systems. It checks connectivity with each of these routers.
- Nslookup verifies that host names can be resolved by a DNS server.
- Netstat shows network statistics and can also identify which application is using specific network connections.
- Nbtstat helps troubleshoot NetBIOS name resolution issues.
- Arp shows MAC address to IP address mappings.
- Net use can map drive letters to UNC paths.
- Hardware tools include cable testers, loop back plugs, and toner probes. A cable tester can verify that a cable is wired correctly. A loop back plug can be used when troubleshooting NICs. Toner probes help you locate both ends of a wire using a tone and a speaker.

Chapter Review

Use the following questions to test your knowledge of the information in this chapter. The answers to these questions, and the explanations of why each answer choice is correct or incorrect, are located in the “Answers” section at the end of this chapter.

1. What should be enabled on a wireless router to ensure that all internal users are assigned IP addresses?
 - A. DNS
 - B. DHCP
 - C. NAT
 - D. VoIP

2. You are managing a network with 15 Windows 7 Home Basic and Windows 7 Professional–based systems. You are trying to create a homegroup on a Windows 7 Home Basic–based system, but it is not working. Why not?
 - A. Homegroups cannot be created on networks with more than 10 systems.
 - B. Homegroups can be created only on Windows XP systems.
 - C. You cannot create homegroups on networks that include Windows 7 Home Basic.
 - D. You cannot create a homegroup on a Windows 7 Home Basic–based system.

3. Which of the following commands can you use to check connectivity with a remote system? (Choose all that apply.)
 - A. Ping
 - B. Tracert
 - C. Ipconfig
 - D. Net use

4. You’re troubleshooting a computer, and you want to verify that the computer can connect to another system on the network. Which of the following would you use?
 - A. Ping 127.0.0.1.
 - B. Ping loopback.
 - C. Ping the address of the default gateway.
 - D. Ping the address of the subnet mask.

5. You suspect that DHCP has assigned a user's system an IP address that is used by another system on the network. Which of the following commands can you use to force the system to get a new IP address from DHCP?
- A. Ping dhcp -4
 - B. DHCP /force
 - C. Ipconfig /release and ipconfig /renew
 - D. Ipconfig /force
6. A user is unable to connect to a remote server in a large network with several routers. What tool can you use to list all the routers between the user's system and the server?
- A. Tracert
 - B. Ping
 - C. Arp
 - D. Net Trace
7. Which of the following commands will show the following result?
- ```
192.168.1.1 68-7f-74-ae-8b-de dynamic
```
- A. Ping DC1
  - B. Ipconfig /all
  - C. Arp -a
  - D. Netstat -a
8. Which of the following commands can map a drive to a share on a remote computer?
- A. Netstat
  - B. Net use
  - C. Nslookup
  - D. Arp
9. You have connected a computer with a switch. However, you don't have any connectivity and the LED lights are not lit on either the NIC or the switch. You've verified that the switch and the computer are functioning. What tool would you use as the next step?
- A. Nslookup
  - B. Tracert
  - C. Homegroup
  - D. Cable tester

# Answers

---

1. **Correct Answer:** B
  - A. **Incorrect:** DNS helps systems resolve names to IP addresses but does not assign IP addresses.
  - B. **Correct:** DHCP provides internal users with IP addresses and other TCP/IP configuration information.
  - C. **Incorrect:** NAT translates public and private IP addresses, but it does not assign IP addresses.
  - D. **Incorrect:** Some applications use VoIP to transmit voice over an IP network, but VoIP does not assign IPs.
2. **Correct Answer:** D
  - A. **Incorrect:** There are no limitations to how many systems are on a network using homegroups. However, Windows 7–based systems do not support more than 20 concurrent connections.
  - B. **Incorrect:** Windows XP–based systems do not support home groups.
  - C. **Incorrect:** Windows 7 Home Basic–based systems can join a homegroup, but they cannot create homegroups.
  - D. **Correct:** Homegroups cannot be created on Windows 7 Home Basic–based systems.
3. **Correct Answer:** A, B
  - A. **Correct:** Ping will check connectivity with a remote system.
  - B. **Correct:** Tracert will check connectivity with a remote system and also list all routers in the path.
  - C. **Incorrect:** Ipconfig shows the TCP/IP configuration of a system.
  - D. **Incorrect:** Net use can map drive letters to shares on remote systems.
4. **Correct Answer:** C
  - A. **Incorrect:** Pinging the loopback IP address (127.0.0.1) verifies that the TCP/IP stack is installed but does not verify network connectivity.
  - B. **Incorrect:** Pinging the loopback name is the same as pinging the loopback IP address.
  - C. **Correct:** Pinging the address of the default gateway will verify network connectivity with another system. In this case, it verifies connectivity with the router.
  - D. **Incorrect:** It is not possible to ping the subnet mask.

- 5. Correct Answer: C**
- A. Incorrect:** This command will try to ping a host named dhcp using IPv4. However, ping does not request a new IP.
  - B. Incorrect:** There is no such command as DHCP /force.
  - C. Correct:** The ipconfig /release command releases a DHCP assigned IP address, and the ipconfig /renew command requests a new IP address.
  - D. Incorrect:** Ipconfig does not have a /force switch.
- 6. Correct Answer: A**
- A. Correct:** The tracert command will trace the route between two systems and list all routers in the path.
  - B. Incorrect:** Ping can check connectivity, but you've already verified that you cannot connect to the remote server, so this will fail without giving any extra help.
  - C. Incorrect:** Arp lists MAC-to-IP address mappings.
  - D. Incorrect:** Net Trace includes many commands but not a Net Trace command.
- 7. Correct Answer: C**
- A. Incorrect:** The ping command checks connectivity with systems and shows the result of these attempts.
  - B. Incorrect:** The ipconfig /all command shows all of the TCP/IP configuration information of a system.
  - C. Correct:** The arp -a command shows IP address to MAC address mappings.
  - D. Incorrect:** The netstat -a command displays a listing of inbound and outbound connections.
- 8. Correct Answer: B**
- A. Incorrect:** Netstat shows network statistics, including inbound and outbound connections.
  - B. Correct:** The net use command can be used to map a drive to a share. After it is mapped, the share is viewable in Windows Explorer with the mapped drive letter.
  - C. Incorrect:** Nslookup can verify whether a DNS server can resolve a host name to an IP address.
  - D. Incorrect:** The Arp -a command shows information about MAC address and IP address mappings.

**9. Correct Answer: D**

- A. Incorrect:** Nslookup verifies that DNS can resolve a host name but would not work if you don't have connectivity.
- B. Incorrect:** Tracert lists routers in the path between two systems but would not work without connectivity.
- C. Incorrect:** Homegroups are used to share files between Windows 7–based systems but wouldn't work without connectivity.
- D. Correct:** If you've verified that the switch and computer are functioning correctly, the next step is to verify that the cable between the two is functioning, and a cable tester does that.