CHAPTER 14

Networking

This chapter covers the following A+ exam topics:

- Networking Fundamentals
- Network Cabling and Connectors
- Troubleshooting Network Connectivity
- Installing and Configuring a SOHO Network

You can find a master list of A+ exam topics in the "Introduction."

This chapter covers CompTIA A+ 220-701 objectives 4.1, 4.2, and 4.3 and CompTIA A+ 220-702 objectives 3.1, and 3.2.

Virtually every business has one or more computer networks, and it seems that nowadays just about every home has a network as well. But what is a computer network? The simple answer: A computer network is two or more computers that communicate. For the more in-depth answer, read on!

We use networks so that computers can share files, access databases, collaborate on projects, connect to the Internet, and send email. Important considerations in networking include the technologies used, devices, protocols, cabling; plus the installation, configuration, and troubleshooting of networks. Other things to think about are how the network is organized, what types of communications are necessary, in what way devices share information, how the network is secured, and what is the effect of the network on the budget. As you can see, so much is dependent on a well-designed, quick and efficient, and cost-effective network, making this an important chapter for the exam. Let's begin by discussing the building blocks of networks: networking fundamentals.

Networking Fundamentals

To network your computer, you first need a network adapter. Networking expansion cards for desktop computers include PCI, and PCIe, whereas laptops use PC Cards, ExpressCards, and Mini-PCI.

USB network adapters are also available that enable a computer to connect to the network via a USB port. It is sometimes referred to as a network interface card (NIC). Adapters integrated into the motherboard of the PC or laptop are common. This adapter is either equipped with an RJ45 jack that enables for a wired connection to the network or has a wireless antenna built-in for connectivity to wireless networks. Some computers have both types of adapters. When the adapter is physically installed, drivers for the network adapter are installed much like any other drivers. This enables the operating system to communicate with the network adapter and transmit data over the network.

After a driver is installed, a communications protocol is needed. In most cases the protocol is installed automatically. The most commonly used protocol is Transmission Control Protocol/Internet Protocol (TCP/IP). TCP/IP is actually a suite that includes many protocols, some of which you have probably heard of, for example, HTTP, or FTP. The version of TCP/IP that the exams focus on is TCP/IPv4, more simply known as IPv4. Unless stated otherwise in this chapter, when I use the term IP or TCP/IP, I refer to IPv4. Let's show how to configure IP settings now.

Configuring IPv4

Configuring IP works the same way in most versions of Windows. First we navigate to the Internet Protocol (TCP/IP) Properties window, which we refer to as the IP Properties window.

- **In Windows XP:** Navigate to Start > Control Panel > Network and Internet Connections. Select the Control Panel icon Network Connections. Then right-click the Local Area Connection icon and select Properties. Finally, highlight Internet Protocol and click the Properties button.
- **In Windows Vista:** Navigate to Start > Control Panel > Network and Internet > Network and Sharing Center. Select the Manage My Network Connections link. Then right-click the Local Area Connection icon and select Properties. Finally, highlight Internet Protocol Version 4 and click the Properties button.

ExamAlert

Memorize how to navigate to the IP Properties window for the exam!

Note

These are the default paths. You can shorten these considerably. For example, in Windows XP if you added the My Network Places option in the Start Menu, just right-click that and select properties. In Windows Vista, if you have the Network option in the Start menu, right-click that and select properties. There are other ways to save time, for example using a shortcut or utilizing a network connection link in your System Tray. Use the fastest method available!

The first item to be configured is the IP address. The IP address is the unique assigned number of your computer on the network. IP addresses consist of four octets. Each octet's value can be between 0 and 255. Each number is separated by a dot. For example: 192.168.0.100. The binary equivalent of 0–255 would be 00000000 through 11111111. For example, 192 is equal to 11000000 in binary. Because each octet contains 8 bits, and there are four octets, the IP address collectively is a 32-bit number but is normally expressed in dotted-decimal notation.

There are two main types of addresses: dynamic and static. Dynamically assigned addresses are more common for a client computer; this is when the computer seeks out a DHCP server so that it can get its IP information automatically. In Figure 14.1, you note a radio button that says Obtain an IP Address Automatically. If you select this, the rest of the information becomes grayed out, and the computer attempts to get that IP information from a host such as a D-Link router or DHCP server. This is common; in fact it's the default configuration for Windows. Static addresses are when we configure the IP information manually. Figure 14.1 shows an example of statically configured IP settings in the Local Area Connection properties window. In the figure we configured the computer to use the address 192.168.0.100, but the IP address differs from machine to machine depending on several factors. Remember that the address should be unique for each computer on the network.

Exam*Alert*

Know the difference between static and dynamic IP addresses.

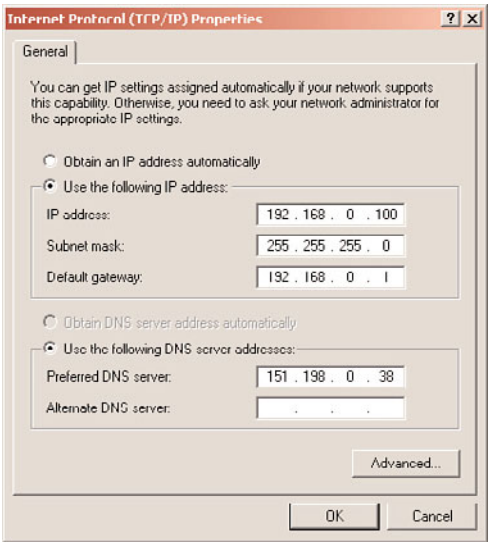


FIGURE 14.1 **IP Properties window with an example IP configuration**

There is another possibility when it comes to IP addresses, and that is when the computer self-assigns an address. This is known as *automatic private IP addressing (APIPA)* and happens when a computer cannot contact a DHCP server to obtain an IP address. If APIPA self-assigns an address, it will be on the 169.254.0.0 network.

IP addresses are divided into two sections: the network portion, which is the number of the network the computer is on, and the host portion, which is the individual number of the computer. The subnet mask defines which portion of the IP address is the network number and which portion is the individual host number. In this case the subnet mask is 255.255.255.0. The 255s indicate the network portion of the IP address. So, 192.168.0 is the network this computer is a member of. The zeros (in this case there is only one of them) indicate the host number, so 100 is the individual number of this computer. Quite often the subnet mask will be configured automatically by Windows after you type in the IP address.

The gateway address is the IP address of the host that enables access to the Internet or to other networks. The IP address of the gateway should always be on the same network as the computer(s) connecting to it. In Figure 14.1 we know it is because the first three octets are 192.168.0. If a computer is not configured with a gateway address, it cannot connect to the Internet.

ExamAlert

To use the gateway, computers must be on the same network number as the gateway device.

The DNS server address is the IP address of the host that takes care of domain name translation to IP.

When you use your browser to connect to a website, you might type something like www.davidlprowse.com. What you need to remember, however, is that computers actually communicate by IP address, not by name. So the DNS server takes care of translating the name davidlprowse.com to its corresponding IP address and forwarding that information back to your computer. When your computer knows the IP address of the website, it can go ahead and start a session with the website and transmit and receive files. Notice in Figure 14.1 that the DNS server address is on a completely different network than our computer. This is typical, in this case the DNS server is run by the Internet service provider (ISP) who provides me with my cable Internet connection. However, DNS servers can also be run internally by a company; this happens more often with larger companies. That brings us to how the different network numbers are categorized.

IPv4 Classes

When working with classful IP addresses, the first number in the IP address dictates what class the address is part of. For example, suppose you use 192.168.0.100. In that case, the first number is 192, which means that the IP address is part of a Class C network.

Table 14.1 shows the various classes and their associated IP address ranges. Table 14.2 shows the IP classes and their associated default subnet masks, which as we mentioned, identify which portion of the IP address is the network portion and which is the host portion.

Take a look at Table 14.1 and try to get a feel for the different IP Classes available. You realize that this classification system was created to appease different organizations of different sizes. If you have a small network at home, it is simplest and most common to use Class C.

TABLE 14.1 **IP Classifications**

IP Class	Range	Number of Networks	Number of Hosts Per Network	Total Hosts Worldwide	Who Uses It?
A	1–126	126	16,777,214	2,113,928,964	Large Corps, ISPs
B	128–191	16384	65534	1,073,709,056	Corps, Universities, ISPs
C	192–223	2,097,152	254	532,676,608	Small companies and organizations
D	224–239	—	—	—	Multi-Cast testing
E	240–255	—	—	—	Future Use

You probably noticed that the number 127 was skipped. That is because this network number is reserved for loopback testing. Technically, it is part of the Class A range, but it cannot be configured as an IP address within the IP Properties window.

You might have also noticed that here are only 254 possible hosts per network in Class C instead of 256. This is because you can never use the first or the last address in the range; the first is actually the network number and the last is the broadcast address!

The total hosts, for all classes combined, is 3,720,314,628. That's just under four billion—and we are getting close to that number of used IP addresses today. Some analysts guess that we will run out of IPv4 addresses by 2012, and this is one of the reasons for IPv6.

ExamAlert

You need to memorize the IP ranges of IPv4 for the Network+ exam. Most important are the Class A, B, and C ranges.

TABLE 14.2 **IP Class Ranges and their equivalent Binary values and Default Subnet Masks**

IP Class	Binary Equivalent	Default Subnet Masks
A: 1-126	00000001-01111110	255.0.0.0 Net.node.node.node
B: 128-191	10000000-10111111	255.255.0.0 Net.net.node.node
C: 192-223	11000000-11011111	255.255.255.0 Net.net.net.node

TABLE 14.2 **Continued**

IP Class	Binary Equivalent	Default Subnet Masks
D: 224-239	11100000-11101111	255.255.255.255 Net.net.net.net
E: 240-255	11110000-11111111	—

Notice in Table 14.2 how the number 255 in a subnet mask coincides with the name *net*. Also, notice the 0 coincides with the name *node*. Net is the network portion of the IP address, whereas node is the host or computer portion of the address.

ExamAlert

Memorize the default subnet masks for Class A, B, and C.

It is also important to know the difference between private and public addresses. A private address is one that is not displayed directly to the Internet and is normally behind a firewall. Typically, these are addresses that a SOHO router would assign automatically to clients. A list of reserved private IP ranges is shown in Table 14.3. Public addresses are addresses that are displayed directly to the Internet; they are addresses that anyone could possibly connect to around the world. Most addresses, besides the private ones listed in Table 14.3, are considered public addresses.

TABLE 14.3 **Private IP Ranges (as Assigned by the IANA)**

IP Class	Assigned Range
Class A	10.0.0.0–10.255.255.255
Class B	172.16.0.0–172.31.255.255
Class C	192.168.0.0–192.168.255.255

ExamAlert

Memorize the private IP ranges for Class A, B, and C.

Analyzing and Configuring the Network Adapter

When analyzing the network adapter, we can use several status indicators, some are hardware-based and some are software-oriented.

The first type of indicators are physical; they show up as LED lights on the network adapter itself. Different network adapters have different LED lights, but typically you have a connectivity LED and an activity LED. The connectivity LED tells you if you have a good connection to a router or switch by displaying a solid color. Usually, solid yellow means connectivity at 10Mbps; solid green means connectivity at 100Mbps. (Green is sometimes used for 1000Mbps as well.) However, if the connectivity LED is blinking, then you know there is an intermittent connection that should be troubleshot. The activity LED blinks when data is passing through the network adapter; the color of this LED doesn't make a difference unless it is the only LED available on the network adapter.

The second type of indicators are logical and show up in the operating system. These normally manifest themselves in the System Tray and can be put there by Windows or by the manufacturer of the network adapter, depending on whether you let Windows install the card or if you used the additional software that came with the network adapter. Figure 14.2 displays a Local Area Connection Status icon used by Windows; it appears as two monitors diagonally, one on top of the other.

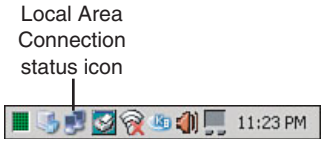


FIGURE 14.2 **Local Area Connection Status icon**

If you were to right-click the status icon and select Status, you would see the status of the adapter, as shown in Figure 14.3

From the default General tab, we can see what our "speed" is, how long we have been connected, and how many bytes have been sent and received. Also, if we click on the Properties button, it brings us to the Local Area Connection properties window—a nice shortcut! If we click on the Support tab, we see our IP configuration and can have Windows attempt to repair the adapter if there were an issue.

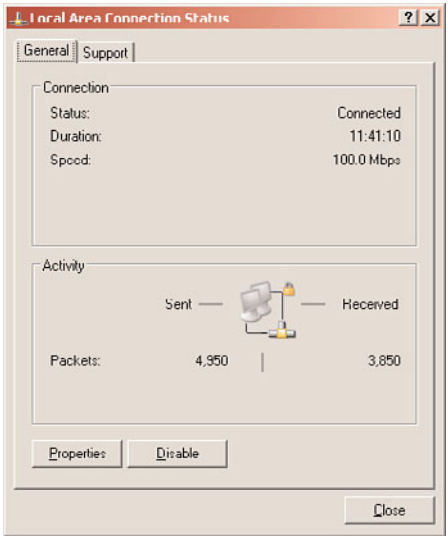


FIGURE 14.3 **Local Area Connection Status window**

How well your network adapter operates depends on a few different factors including bandwidth, latency, and what duplex setting it is configured for.

In computer networking, bandwidth refers to the maximum data throughput of the connection and is measured in bits per second (bps). In Figure 14.3 we saw that our speed was 100Mbps; this would also be known as bandwidth. To get this speed, every link in the networking chain must operate at 100Mbps including the network adapter, cables, and central connecting devices such as SOHO router, switch, or hub. If any one of those links runs at less than 100Mbps, the entire connection would be brought down to 10Mbps.

Latency is the time it takes for sent data packets to be received by a remote computer. An easy way to show this would be to *ping* another computer, for example open the CLI and type **`ping davidlprowse.com`**, the ensuing replies should show a time= amount, probably around 100ms. This tells us that the ping packet took a round-trip time of 100 milliseconds to get from your computer to the destination and back.

There are two duplex settings that a network adapter can be set for: half-duplex and full-duplex. Half-duplex means that your network adapter can send or receive data but not at the same time; full-duplex means that the adapter can do both simultaneously thus doubling the maximum data throughput. This can be configured by navigating to the Device Manager and then going to the properties of the network adapter. Finally, access the Advanced tab and

the Speed & Duplex setting (or like name). This is normally set to auto-negotiation, but you can modify the speed or duplexing settings to take full advantage of your network. Of course, this depends on the type of device your network adapter connects to and how that device is configured.

The most common type of network that a network adapter connects to is Ethernet. Ethernet is a family of network technologies for LANs defined by the IEEE 802.3 standards. The most common of these follow:

- **802.3u:** Specifies 100Mbps data transfer rates. The most common protocol is 100BASE-TX that indicates 100Mbps, a baseband connection (meaning that every computer on the network shares the network frequency used), and that the cable used is twisted pair.
- **802.3ab:** Specifies 1000Mbps data transfer over copper cable.
- **802.3z:** Specifies 1000Mbps data transfer over fiber optic cable.

Network Devices

There are several types of network devices that you will run into in the field. Some are designed to offer connectivity to other computers; others are designed to offer connectivity to other networks. Let's discuss a few of these now:

- **Hub:** A hub is a central connecting device that enables computers to physically connect to each other. It regenerates and passes on the electrical signals initiated by computers. It is used in Ethernet networks only. Other network technologies have a different name for this device. A hub is actually a simple device; it connects multiple computers together and amplifies and passes on the electrical signal. Internally, the hub actually has only one trunk circuit that all the ports connect to. All bandwidth, for example 10Mbps or 100Mbps within the hub, is shared among all computers connected to the hub. Hubs are also known as multiport repeaters.
- **Repeater:** Repeaters enable a network administrator to extend the electrical signal beyond the standard 100 meters if a cable run needs to go farther than that. Generally, they have two ports, one for an incoming cable and one for an outgoing cable. When an electrical signal has traveled 100 meters on a standard network cable (twisted pair), it attenuates or loses power to the point at which it cannot be understood at the receiving end.

- **Switch:** Ethernet Switching was developed in 1996 and quickly took hold as the preferred method of networking. A switch, like a hub, is a central connecting device that all computers connect to, and like a hub it regenerates the signal, but that's where the similarity ends. A switch takes the signal and sends it to the correct computer instead of broadcasting it out to every port. This can effectively make every port an individual entity, and it increases data throughput exponentially. Switches employ a matrix of copper wiring instead of the standard trunk circuit and intelligence to pass information to the correct port. This means that each computer has its own bandwidth, for example 10Mbps or 100Mbps.
- **Router:** A router is used to connect two or more networks together to form an internetwork. They are used in LANs and WANs and on the Internet. This device routes data from one location to another, usually by way of IP address and IP network numbers. Routers are intelligent and even have their own text-based OS known as an IOS (Internetwork Operating System).
- **Wireless Access Point (WAP):** A WAP enables data communications over the air if your computer is equipped with a wireless networking adapter. They transmit their data over radio waves either on the 2.4GHz or 5GHz frequencies. This brings mobility to a new level. Some WAPs also have a router built in, such as the D-Link Router we use in this chapter. This enables wireless computers to not only communicate with each other but to access the Internet as well! Many of these devices also come equipped with a firewall. At this point they are referred to as multifunction network devices, SOHO routers, or simply routers.
- **Proxies:** A proxy server is a computer or device that is between the network client computers and the Internet. Proxies cache information for the clients to increase performance and to conserve Internet connection bandwidth. The most common type is the HTTP proxy. This stores website information requested by a client so that subsequent clients can get that same information much quicker without having to connect to the actual website. A proxy server will usually be on the same network as the client computer. The client computer can be configured to utilize the proxy server by opening Internet Explorer, clicking Tools, Internet Options, selecting the Connections tab, and clicking the LAN settings button. From here the user needs to type in the IP address of the proxy server.

Types of Networks

There are several network types that you need to be cognizant of for the exam including

- Local area network (LAN)
- Wide area network (WAN)
- Workgroup
- Domain
- Virtual private network (VPN)

A local area network (or LAN) is a group of computers in a small geographic area, for example in one room, a house, or in one building. If you have more than one computer in your home that share an Internet connection, they would be considered a LAN.

A wide area network (or WAN) is usually two or more LANs connected together. This covers a larger geographic area and requires the services of a telecommunications provider or ISP.

Workgroups and domains are more logical groupings of computers. A workgroup (sometimes also referred to as peer-to-peer) is usually a small group of computers, often ten or less, which share the same network name. No one computer controls the network, and all systems are considered equal. A domain builds on this by having one or more computers that are in control of the network, enabling for more computers, and centralized administration. Domains also get a name and are sometimes also referred to as client/server networks. Figure 14.4 shows the Computer Name Changes window accessible from the System Properties window, in which we can change the name of the workgroup that we are a member of, join new workgroups, or join domains.

Virtual private networks (VPNs) were developed so that telecommuters, salespeople, and others could connect to the office from a remote location. If set up properly, the remote logon connection is seamless and appears as if you are actually at the LAN in the office. You log on just as you would if you were at your desk at headquarters. VPNs give the user access to all the resources that they get when logging on locally. VPNs are superior to older dial-up connections because they take advantage of the more powerful infrastructure of the Internet and faster connections such as cable, DSL, and so on. A VPN connection can be identified by an additional network connection in the System Tray, as an additional network connection when using the ipconfig command, or as a popup window that comes up during the logon process, for example the kind used by Cisco VPN software.

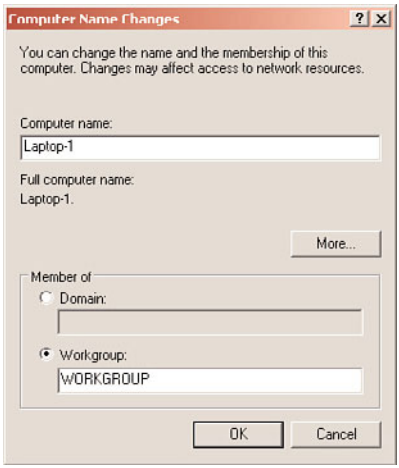


FIGURE 14.4 **Windows XP Computer Name Changes window**

Common TCP/IP Protocols and Their Ports

For two computers to communicate, they must both use the same protocol.

For an application to send or receive data, it must use a particular protocol designed for that application and open up a port on the network adapter to make a connection to another computer. For example, let's say you want to visit www.google.com. You would open up a browser and type in **`http://www.google.com`**. The protocol used is HTTP, short for Hypertext Transfer Protocol. That is the protocol that makes the connection to the web server: google.com. The HTTP protocol selects an unused port on your computer (known as an outbound port) to send and receive data to and from google.com. On the other end, google.com's web server has a specific port open at all times ready to accept sessions. In most cases the web server's port is 80, which corresponds to the HTTP protocol. This is known as an inbound port. Figure 14.5 shows this.

The local computer on the bottom-left part of Figure 14.5 has been given the IP address 172.30.250.3, a Class B private address. It uses port 3266 to go out to the Internet and start a session with google.com. For security purposes this is a dynamically assigned port and will be different every time you connect to another web server, but it will normally be somewhere in the thousands. The session is accepted by google.com's web server, using the public IP address 66.102.1.100, inbound port 80. Conversely, if you want to run your own web server at home and sell widgets and such, that web server would need to have

port 80 open to the public at all times. If it were ever closed, you would lose sales! People's computers that connected to your web server would use dynamically assigned ports.

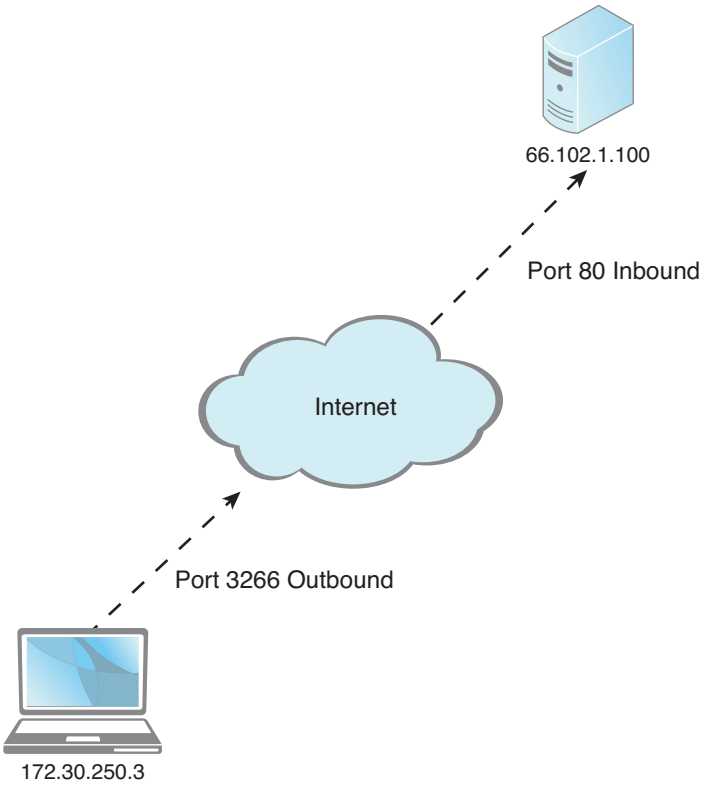


FIGURE 14.5 **HTTP in action**

There are 65536 ports in total, numbered between 0 and 65535, and almost as many protocols! Don't worry; you need to know only a few for the exam, which are listed in Table 14.4.

TABLE 14.4 **Common Protocols and Their Ports**

Protocol	Port Used
FTP	21
SSH	22
TELNET	23
SMTP	25
HTTP	80

TABLE 14.4 **Continued**

Protocol	Port Used
POP3	110
HTTPS	443

ExamAlert

Know these seven common protocols and their corresponding ports for the exam!

The ports mentioned in Table 14.4 are the inbound ports used by the computer that runs the service:

- **FTP:** the File Transfer Protocol allows computers to transfer files back and forth. When you connect to a FTP server, that FTP server will have port 21 open. Some type of FTP client software is necessary to connect to the FTP server, this could be done in the command-line within the FTP shell, or by using a GUI-based application like FileZilla.
- **SSH:** Secure Shell, enables data to be exchanged between computers on a secured channel. This protocol offers a more secure replacement to FTP and TELNET. The Secure Shell server housing the data you want to access would have port 22 open.
- **TELNET:** Short for **Tel**ecommunication **net**work provides remote access to other hosts within the CLI. It uses port 23 but is an insecure and somewhat deprecated protocol. However, because some companies still use it to access routers and other hosts, you might see a question about it on the exam.
- **SMTP:** Simple Mail Transfer Protocol sends email. When you send email from home, it goes to an SMTP server (which has inbound port 25 open) at your ISP and is then sent off to its destination. A good way to remember this is by using the mnemonic device *Send Mail To People*.
- **HTTP:** Hypertext Transfer Protocol transfers web pages and other web-based material from a web server to your web browser. It is normally done in a compressed format but not in a secured format. Web servers have port 80 open by default.
- **POP3:** Post Office Protocol Version 3 is used by email clients to retrieve incoming email from a mail server. The POP3 mail server uses port 110.

- **HTTPS:** Hypertext Transfer Protocol Secure sends and receives information like HTTP but includes the Transport Layer Security protocol (successor of the Secure Sockers Layer [SSL] protocol) to encrypt the information, most commonly when making purchases/payments online or when logging in to a confidential website. The HTTPS server has port 443 open.

Cram Quiz

Answer these questions. The answers follow the last question. If you cannot answer these questions correctly, consider reading this section again until you can.

1. Which protocol uses port 22?
   - ❍ **A.** FTP
   - ❍ **B.** TELNET
   - ❍ **C.** SSH
   - ❍ **D.** HTTP

2. Which of these addresses needs to be configured to enable a computer access to the Internet or to other networks?
   - ❍ **A.** Subnet mask
   - ❍ **B.** Gateway address
   - ❍ **C.** DNS address
   - ❍ **D.** MAC address

3. Which LED blinks when data is passed through the network adapter?
   - ❍ **A.** Activity
   - ❍ **B.** Connectivity
   - ❍ **C.** Full-duplex
   - ❍ **D.** Amber

4. The Computer Name Changes window enables you to add your computer to these two types of networks. (Select two.)
   - ❍ **A.** Domains
   - ❍ **B.** VPNs
   - ❍ **C.** LANs
   - ❍ **D.** Workgroups

5. The IP address 128.0.0.1 would be part of what IPv4 class?
   - ❍ **A.** Class A
   - ❍ **B.** Class B
   - ❍ **C.** Class C
   - ❍ **D.** Class D

Cram Quiz Answers

1. **C.** SSH uses port 22, FTP uses port 21, TELNET uses port 23, and HTTP uses port 80.
2. **B.** The gateway address must be configured to enable a computer access to the Internet through the gateway device. By default, the subnet mask defines the IP address's network and host portions. The DNS server takes care of name resolution, and the MAC address is the address that is burned into the network adapter; it is configured at the manufacturer.
3. **A.** The activity LED blinks when data is passed through the network adapter. The connectivity LED should remain solid.
4. **A** and **D.** This window enables you to set whether the computer connects to a workgroup or domain.
5. **B.** The IP address 128.0.0.1 is part of the Class B range that encompasses 128-191.

Network Cabling and Connectors

The most common type of cable used in today's networks is twisted pair. It is referred to as twisted pair because the copper wires inside of the cable are twisted together into pairs throughout the entire length of the cable. Regularly, admins use UTP cable, short for unshielded twisted pair. Today, the most frequently used twisted pair types are Category 5, 5e, and 6. Table 14.5 shows the various categories of twisted pair and the data transfer rates they can support.

TABLE 14.5 **UTP Categories and Speeds**

Category UTP	Maximum Data Transfer Rate
Category 3	10 Mbps
Category 5	100 Mbps
Category 5e	Rated for 100 Mbps and gigabit networks
Category 6	Rated for 100 Mbps and gigabit networks

> **Note**
>
> Depending on the manufacturer of Category 5e and Category 6, and the type of Category 6, maximum data throughput amounts vary.

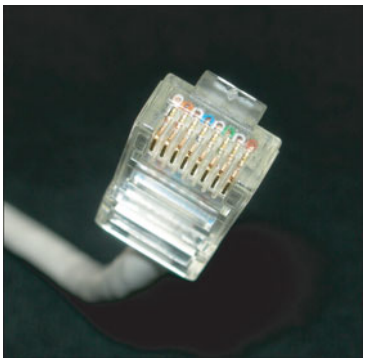
Network data transfer rates (also known as speed or bandwidth) are normally measured in bits because networks normally transfer data serially, or one bit at a time. 100Mbps is 100 megabits per second. 1Gbps is equal to 1 gigabit per second (known as a gigabit network).

Most wiring standards are based on the original BOGB standard, which specifies that wire pair colors go in this order: blue, orange, green, brown. The 568A and B standards are based on this. Generally speaking, the most common standard you see is the 568B standard. Any physical cabling equipment used in the network must comply with this standard. This includes cables, patch panels, jacks, and even connectors! The connector used with twisted pair networks is known colloquially as the RJ45 (more specifically the 8P8C connector). RJ45 plugs connect to each end of the cable, and these connect to RJ45 sockets within network adapters and on hubs/switches.

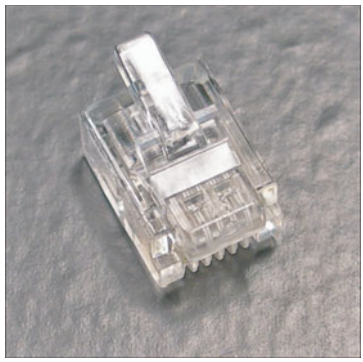
ExamAlert

If a computer cannot connect to the network, check the cables first. Make sure the RJ45 plug has a solid connection.

As you can see in Figure 14.6, RJ45 plugs look a lot like the plugs that connect your telephone (known as RJ11). However, the RJ45 plug is larger and contains eight wires whereas the RJ11 plug can hold only a maximum of six.



RJ45



RJ11

FIGURE 14.6 **RJ45 and RJ11 plugs**

You can use several tools to test the various categories of twisted pair cable. They include

- **Patch testers:** These are designed to test patch cables. Both RJ45 ends are connected to the patch tester to test each individual wire (pin). Pressing a button illuminates eight LED lights that correspond to the eight pins in the cable. In a standard straight-through patch cable, both ends should be wired in the same order. Straight-through patch cables connect computers directly to hubs or switches and are the more common type of patch cable. Another type of cable, the crossover cable connects computers directly to each other; these require a different wiring scheme on one end of the cable, essentially 568B on one end, and 568A on the other. The problem with a patch tester is that you need both ends of the cable in one location, so it cannot test longer cable runs.
- **Continuity testers:** These test those longer cable runs. They check for continuity on each pin to make sure that each end is wired properly. These testers usually consist of a handheld device that connects to one

end of a network connection that indicates test results, and terminators that connect to the other end of the cable, which send the signal back to the tester. Some continuity testers can also act as testing devices for phone lines and more.

- **Time-domain reflectometers (TDR):** These measuring instruments can locate faults in a cable or discontinuities in a connector. They transmit a short pulse across the cable. If the cable is installed properly, no signal will be reflected back to the TDR, but if there are any impedance discontinuities, an error signal will be reflected back and displayed on the TDR.

UTP has a few disadvantages; it can be run only 100 meters before signal attenuation, it's outer jacket is made of plastic, and it has no shielding, making it susceptible to electromagnetic interference (EMI) and susceptible to unauthorized network access in the form of wire tapping.

Because the UTP cable jacket is made of PVCs (plastics) and can be harmful to humans if they catch on fire, most municipalities require that plenum-rated cable be installed in any area that cannot be reached by a sprinkler system. A plenum is an enclosed space used for airflow. For example, if cables are run above a drop ceiling, building code requires that they are plenum-rated: This means that the cable has a special Teflon coating or is a special low-smoke variant of twisted pair, reducing the amount of PVCs that are released into the air in the case of fire.

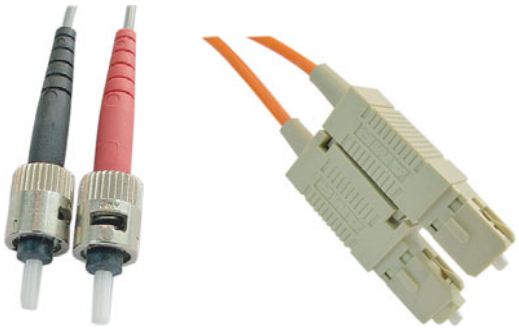
ExamAlert

To meet fire code, use plenum-rated cable above drop ceilings and anywhere else necessary!

Because UTP is susceptible to EMI, a variant was developed known as STP or shielded twisted pair. This includes metal shielding over each pair of wires, reducing external EMI and the possibility of unauthorized network access. A couple of disadvantages of STP include higher cost of product and installation, and the fact that the shielding needs to be grounded to work effectively.

When dealing with EMI, a better option is to use fiber optic cable. Because fiber optic cables transmit data by way of light instead of electricity, they can send signals much further than copper wires, and EMI doesn't even play into the equation. Due to this, fiber optic cable is the most secure type of cable.

You might encounter single mode and multimode fiber; for the most part single-mode fiber is used over longer distances, but both types are capable of supporting 1000Mbps and 10Gbps networks, and can be run farther than twisted pair cable. A couple types of connectors used with fiber include ST and SC, as shown in Figure 14.7. Some of the newer types of connectors include LC and MTP.



ST SC

FIGURE 14.7 **ST and SC connectors**

Coaxial cable is another way to transfer data over a network. This cable has a single conductor surrounded by insulating material, which is then surrounded by a copper screen, and finally an outer plastic sheath. Some networking technologies still use coaxial cable; for example, cable Internet connections use coaxial cable (known as quad shield coaxial cable) with RG-6 connectors (previously RG-59). But older coaxial cabled LANs that used RG-58 connectors are a thing of the past, and it is extremely unlikely that you will see a LAN using coaxial cable.

Cram Quiz

Answer these questions. The answers follow the last question. If you cannot answer these questions correctly, consider reading this section again until you can.

1. Which of the following would be suitable for 100Mbps networks? (Select all that apply.)
   - ❍ **A.** Category 3
   - ❍ **B.** Category 5
   - ❍ **C.** Category 5e
   - ❍ **D.** Category 6

2. Which type of cable would you use if you were concerned about EMI?
   - ❍ **A.** Plenum-rated
   - ❍ **B.** UTP
   - ❍ **C.** STP
   - ❍ **D.** Coaxial

Exam Cram Answers

1. **B**, **C**, and **D.** The only cable listed that is not suitable would be category 3; it is only suitable for 10Mbps networks.
2. **C.** STP or shielded twisted pair is the only cable listed here that can reduce electromagnetic interference.

Troubleshooting Network Connectivity

Okay, now that we've shown some of the basics of networking, let's get into a little bit of network troubleshooting. To troubleshoot client connectivity properly, we need to know a little bit more about command-line interface (CLI) tools and some of the applications available to us. Let's begin with CLI tools.

Command-Line Interface Tools

There are many command-line tools that we can use in Windows to help us troubleshoot situations; in this section we delve into six of them. To open the command-line interface (known as the Command Prompt in Windows), do one of the following:

- Click Start > All Programs > Accessories > Command Prompt.
- Open the Run prompt (by pressing Windows +R) and type **cmd**.
- (Vista only) Click Start and type Command Prompt within the search field; then double-click the Command Prompt shortcut from the list that appears.

Ipconfig

Internet protocol configuration or ipconfig displays current TCP/IP network configuration values. This is one of the first tools you should use when troubleshooting network connectivity. If you type **ipconfig** you get results similar to the following:

```
Windows IP Configuration
Ethernet adapter Local Area Connection:
        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.0.100
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.0.1
```

Ipconfig combined with the /all switch shows more information including the DNS server address and MAC address, which is the hexadecimal address that is burned into the ROM of the network adapter.

ExamAlert

To view additional IP configuration information such as DNS servers and MAC addresses, use the **`ipconfig/all`** command.

This command can offer a lot of information about a problem. For example, if a person cannot connect to any Internet resources, it could be because the gateway address is improperly configured. Remember that the gateway address must be on the same network number as the IP address of the client computer. If a user can't connect to any websites, but they can download email, it could be that the DNS server address is incorrectly configured. Ipconfig also tells you whether the client computer's IP address is obtained from a DHCP server, or assigned via APIPA, and whether it is a private or public address.

Note

Linux operating systems use a similar command called **`ifconfig`**. However, in Linux computers you can also modify the IP address with this command.

Ping

Ping tests whether another host is available over the network. It's the easy way to see if another host is "alive." Let's say your gateway's IP address was 192.168.0.1. To ping that computer you would type **`ping 192.168.0.1`**, as an example and hopefully get the following output:

```
Pinging 192.168.0.1: with 32 bytes of data:
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64
Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Notice the replies indicate that the host is alive.

Any other message would indicate a problem, for example the Request Timed Out or Destination Host Unreachable messages would require further troubleshooting. Keep in mind that if it's the local computer that is configured incorrectly, you might not be able to ping anything! Also watch for the

amount of time the ping took to reply back. A longer latency time could indicate network congestion.

You can also use ping to test whether a computer has TCP/IP installed properly, even if it isn't wired to the network! To do this use the **`ping 127.0.0.1`** command. This IP address is known as the loopback address, is used for testing, and is available on every host. It differs from the IP addresses we talked about previously (for example 192.168.0.100) in that it works internally. This command essentially enables you to ping yourself, meaning you can test the local computer's network connection without a valid IP configuration and without a physical connection to the network. Replies are simulated within local computer; they prove if the network adapter and TCP/IP have been installed properly. However, it does not prove if TCP/IP has been *configured* properly.

Tracert

Tracert, short for traceroute, builds on ping in that it send packets to destinations beyond the local computer's network. It pings each router along the way between you and the final destination. An example of tracert output follows:

```
Tracing route to davidlprowse.com [216.97.236.245]
over a maximum of 30 hops:
  1     6 ms     5 ms     5 ms  bdl1.eas-ubr16.atw-
eas.pa.cable.rcn.net [10.21.80.1]
  2    10 ms     9 ms     9 ms  vl4.aggr1.phdl.pa.rcn.net
[208.59.252.1]
  3    10 ms     9 ms    18 ms  ge3-0.core2.phdl.pa.rcn.net
[207.172.15.35]
  4    11 ms    13 ms    12 ms  pos6-0.core3.nyw.ny.rcn.net
[207.172.19.11]
  5   133 ms   203 ms   133 ms  ge6-1.core4.nyw.ny.rcn.net
[207.172.19.114]
  6    13 ms    11 ms    12 ms  tge2-1.border1.nyw.ny.rcn.net
[207.172.19.109]
  7    11 ms    11 ms    11 ms  207.172.9.74
  8    12 ms    11 ms    14 ms  te2-4.ccr01.jfk02.atlas.cogentco.com
[154.54.6.49]
  9    12 ms    11 ms    11 ms  te9-1.ccr04.jfk02.atlas.cogentco.com
[154.54.25.137]
 10    17 ms    18 ms    25 ms  te3-1.ccr02.dca01.atlas.cogentco.com
[66.28.4.82]
 11    59 ms    60 ms    60 ms  te7-3.ccr02.iah01.atlas.cogentco.com
[66.28.4.90]
 12    55 ms    53 ms    54 ms  te3-1.ccr01.sat01.atlas.cogentco.com
[154.54.27.114]
 13    80 ms    80 ms    81 ms  te4-1.ccr01.elp01.atlas.cogentco.com
[154.54.27.141]
```

```
 14   211 ms   225 ms   208 ms  te4-1.ccr01.phx02.atlas.cogentco.com
 [154.54.27.78]
 15   155 ms   237 ms   243 ms  te3-1.ccr01.san01.atlas.cogentco.com
 [154.54.27.109]
 16    82 ms    82 ms    82 ms  vl3806.na21.b006590-
 1.san01.atlas.cogentco.com [66.28.67.74]
 17    82 ms    82 ms    82 ms  38.112.242.138
 18    86 ms    86 ms    86 ms  unused-240-180-214.ixpres.com
 [216.240.180.214]
 19    98 ms    96 ms    97 ms  lwdc.dbo2.gi9-4.host1.23680.
 americanis.net [38.96.20.2]
 20    97 ms    96 ms    96 ms  zosma.lunarpages.com [216.97.236.245]
 Trace complete.
```

Note that there are three pings per line item measured in milliseconds (ms). Also note that every line item contains a router name and IP address. It starts by sailing through the various routers in our ISP, RCN.net. It ends at a server named zosma.lunarpages.com that hosts www.davidlprowse.com (as of the writing of this book). If you saw any asterisks in the place of the millisecond amounts, you might question whether the router is functioning properly. If the tracert stops altogether before saying Trace Complete, you would want to check your network documentation to find out which router it stopped at, and/or make sure that the router is troubleshot by the appropriate personnel.

Netstat

Moving on to another concept, netstat shows the network statistics for the local computer. The default command displays sessions to remote computers. In the following example, I connected to www.google.com and ran the netstat command. Output follows:

```
Active Connections
  Proto  Local Address          Foreign Address        State
  TCP    laptop-musicxpc:1395   8.15.228.165:http      ESTABLISHED
  TCP    laptop-musicxpc:1396   he-in-f101.google.com:http
ESTABLISHED
```

This output shows that there are two established TCP sessions (they're actually both to the same website) to google.com. In the local address column we see our computer called laptop-musicxpc and the outbound ports it uses to access the website, 1395 and 1396. In the foreign address column, we see an IP address and the protocol used (http) and in the second session, a hostname followed by the protocol (again http). The protocol used by google.com corresponds to port 80. This command can tell us a lot about our sessions. For example, if a session times out, or if it closes completely; this shows up in the State column. To see this information numerically, try using the –n switch

after the netstat command. Netstat has a lot of other options; to view these type **netstat /?**.

Nslookup

Nslookup queries DNS servers to discover DNS details including the IP address of hosts. For example, if I want to find the IP address of davidlprowse.com, I would type **nslookup davidlprowse.com**. The resulting output should look something like this:

```
Non-authoritative answer:
Name:    davidlprowse.com
Address:  216.97.236.245
```

So from the output, we now know the IP address that corresponds to the domain name davidlprowse.com. Nslookup means name server lookup and can aid in finding DNS servers and DNS records in a domain as well. If the command nslookup is typed by itself, it brings the user into the nslookup shell. From here several commands can be utilized; to find out more about these type **?**. To exit the nslookup shell type **exit**, press Ctrl+C, or press Ctrl+Break.

Net

The **net** command is actually a collection of commands. In Chapter 13, "Printers," we used the **net stop** command to stop the print spooler. In networking you might use the **net view** command to see what computers are currently available on the network or the **net send** command to send messages to other users via the command line. For the exam you should know the types of **net** commands that enable you to view or create mapped network drives. To view any currently mapped network drives, simply type **net use**. To create a mapped network drive, use the following syntax:

```
net use x: \\computername\sharename
```

X: is the drive letter, in this case X is a variable; you can use whatever drive letter you want if it's available. Computername is the name of the remote host you want to connect to, and sharename is the share that was created on that remote host.

There is a network share on another computer on my network called C$. The following syntax shows the command to connect to it and the resulting output:

```
net use f: \\laptop-musicxpc\c$
The command completed successfully.
```

In this example, we used F: as our drive letter; the computer we connected to is called laptop-musicxpc and the share is C$ (the default hidden share). For more information on the net command, type **`net /?`**. For more information on the **`net use`** command type **`net use /?`**.

Troubleshooting with Applications

We can use applications to help us troubleshoot client connectivity as well. In this section, we focus on a mail application and the Windows Firewall.

Sometimes users complain that they can't access their email. This can be because they connect to POP3 and SMTP mail servers and their email configuration is incorrect. Figure 14.8 shows the E-mail Accounts window of Outlook.

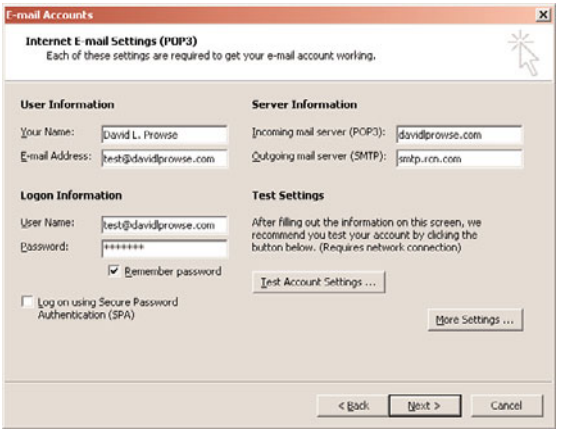


FIGURE 14.8 **Outlook E-mail Accounts window**

This can be accessed in Outlook by going to Tools > E-mail Accounts, selecting View or change existing email accounts, and selecting the appropriate one to modify. Outlook Express works in much the same way, but the navigation might be slightly different. Notice the incoming mail server (POP3) and the Outgoing mail server (SMTP). If these server names are not exact, the client cannot access her mail. Or let's say that the SMTP server is configured properly but the POP3 server is not. Then the user could send messages but not receive them. The same goes for IMAP4 servers (Internet Message Access Protocol 4); be sure that the server name is configured correctly. IMAP4 is another protocol used for incoming mail, less common than POP3, but it

enables a user to store mail folders on the email server and access those folders from other computers. Of course the username and password need to be exact as well, but improperly configured mail servers are a common reason why email fails!

The Windows Firewall is meant to protect client computers from malicious attacks and intrusions, but sometimes it can be the culprit when it comes to certain applications failing. When you turn on the firewall, the default setting is to shield all inbound ports (effectively closing them). This means that certain applications that need to communicate with a remote host might not work properly. Or if the client computer wanted to host some services such as FTP or a web server, the firewall would block them. That's where exceptions come in. You can still use the firewall, but you can specify applications that are exceptions to the rule. You can also do this by port number, so for example, if I want to run an FTP server, I can add port 21 as an exception. Figure 14.9 shows an example of exceptions.

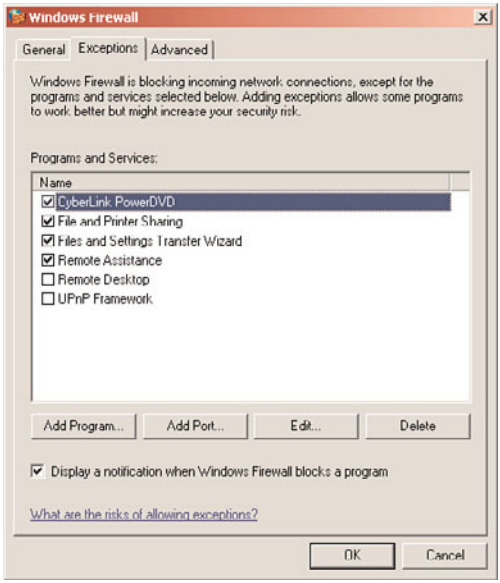


FIGURE 14.9 **Windows Firewall exceptions**

In this example, we have four applications that are not blocked from incoming connections. This way, these applications can communicate with the Internet and the Internet can communicate with them, but we aren't sacrificing the entire security of the system. All other incoming connections will be blocked. You can find more information on firewalls in Chapter 15, "Security."

Cram Quiz

Answer these questions. The answers follow the last question. If you cannot answer these questions correctly, consider reading this section again until you can.

1. Which command tests whether another computer is alive on the local area network?

   - ❍ **A. AGP**
   - ❍ **B. Nslookup**
   - ❍ **C. Netstat**
   - ❍ **D. Ping**

2. Which would be the best command to test for a router that is in another state?

   - ❍ **A. Ipconfig**
   - ❍ **B. Tracert**
   - ❍ **C. Nbtstat**
   - ❍ **D. SSH**

3. Which command would display the following output?

```
Active Connections
  Proto  Local Address          Foreign Address        State
  TCP    laptop-musicxpc:1395   8.15.228.165:http      ESTABLISHED
```

   - ❍ **A. Ping**
   - ❍ **B. Ipconfig**
   - ❍ **C. Nbtstat**
   - ❍ **D. Netstat**

4. Which would be the best command to use if you needed to know the DNS server address that was configured on a computer?

   - ❍ **A. Ipconfig**
   - ❍ **B. Ping**
   - ❍ **C. Ipconfig/all**
   - ❍ **D. Netstat -n**

5. A user can receive mail, but they can't send it. Which of the following servers is most likely configured incorrectly?

   - ❍ **A.** SMTP
   - ❍ **B.** POP3
   - ❍ **C.** FTP
   - ❍ **D.** HTTP

Cram Quiz Answers

1. **D.** Ping tests whether another host on the network is available.
2. **B.** Tracert can attempt to connect to hosts that are outside of the local area network such as a router in another state. The **`tracert`** command will test each router along the way between the local computer and the destination computer.
3. **D.** **`Netstat`** shows sessions like the ones displayed here.
4. **C.** **`Ipconfig /all`** shows DNS server addresses; remember that the default ipconfig will not; it will show only the configured IP address, subnet mask, and gateway address.
5. **A.** The client computer uses the SMTP server to send mail; if they can't send, check the SMTP settings. The POP3 server retrieves mail. FTP servers transfer files, and HTTP servers are used for World Wide Web pages.

Installing and Configuring a SOHO Network

Small office home office (SOHO) networks are extremely common. As such, you should know how to install and configure them for the A+ exam. In this chapter, we cover wireless technologies and multifunction network devices. But first, we need to decide which type of Internet connection to use. This depends on what is available to us, but they include dial-up and broadband options such as Digital subscriber line (DSL), cable, satellite, and Integrated Services Digital Network (ISDN) and cellular.

Internet and Wireless Connectivity Options

There are a lot of different options for connecting to the Internet including the venerable dial-up, DSL, cable Internet, and more. The type of Internet connection dictates download speeds to the clients on a SOHO network. Next, a decision should be made about whether to connect client computers to the network in a wired fashion or as wireless. Another factor in the decision-making process will be whether any Bluetooth-enabled devices need to access the network.

Dial-Up

Strange as it might seem, dial-up Internet is still used by millions, and in some areas of the United States, it is the only Internet connectivity available. Dial-up connections are inexpensive but at the cost of slow data throughput and dropped connections. To connect to a dial-up service, a user needs four things: a working phone line, an account with an ISP, a modem to dial-up to the ISP's networks. and some type of software to control the dial-up connection, for example dial-up networking. The modem serves to modulate and demodulate signals that travel between the computer and the phone line. It sends and receives data in a serial fashion, meaning one bit at a time. It is now possible to purchase devices that enable multiple computers to share the dial-up modem. The modem can be an internal adapter card or an external device that connects to a serial port. The difference is that the internal card incorporates a universal asynchronous receiver transmitter (UART) that converts the serial information coming in from the phone line into parallel data to be sent to the processor. The external modem relies on the UART that is built into the serial port of the computer. Dial-up utilizes the plain old telephone service/public switched telephone network (POTS/PSTN).

DSL

Digital subscriber line (DSL) builds on dial-up by providing full digital data transmissions over phone lines but at high speeds. DSL modems connect to the phone line and to the PC's network adapter or to a SOHO router enabling sharing among multiple computers. One of the benefits of DSL is that you can talk on the phone line and transmit data at the same time. There are several derivatives of DSL, but for the exam you need only know of two:

- **ADSL (Asymmetrical Digital Subscriber Line):** ADSL can run on your home telephone line so that you can talk on the phone and access the Internet at the same time. Users are generally limited to approximately 500Kbps upload and 1Mbps download speed, although there can be lags and spikes in these numbers. Upload speed is always slower than download speed. It is usually not as fast as cable Internet.
- **SDSL (Symmetrical Digital Subscriber Line):** SDSL is installed (usually to companies) as a separate line and is more expensive. SDSL data transfer rates can be purchased at 384K, 768K, 1.1M, and 1.5M. The upload and download speed are the same, or symmetrical unlike ADSL.

Cable Internet

Broadband cable, used for cable Internet and cable TV, offers higher speeds than DSL and can usually get up to an average of 5Mbps to 7Mbps, although the serial connection has the theoretical capability to go to 18Mbps. One website, DSLreports.com, commonly shows people connecting with cable at 10Mbps. Like most Internet connectivity options, cable Internet is shared by the customer base. The more users that are on the Internet, the slower it becomes for everyone.

Satellite

Satellite connectivity uses a parabolic antenna (satellite dish) to connect via line of sight to a satellite; it is used in places in which standard landline Internet access is not available. The satellite is in geosynchronous orbit, at 22,000 miles (35,406 Km) above the Earth. The "dish" connects to coax cable that runs to a switching/channeling device for your computers. Today's satellite connections offer speeds close to traditional broadband access. One of the issues with satellite is electrical and natural interference. Another problem is latency. Due to the distance (44,000 miles total) of the data transfer, there can be a delay of .5 seconds to 5 seconds.

ISDN

Integrated Services Digital Network (ISDN) is a digital technology developed to combat the limitations of PSTN. Users can send data, talk on the phone, fax, all from one line. It is broken down into two types of services:

- **BRI: Basic Rate ISDN:** 128Kbps. Two equal B channels at 64Kbps each for data and one 16Kbps D channel for timing.
- **PRI: Primary Rate ISDN:** 1.536Mbps, runs on a T-1 circuit; 23 equal 64Kbps B channels for data and one *64*Kbps D channel for timing.

Many companies still use ISDN for video conferencing or as a fault tolerant secondary Internet access connection. Data commuters use this if DSL or cable is not available.

Cellular

Cellular has become more popular of late as a means to access the Internet from mobile devices. The term *cellular* has grown to encompass several different technologies such as GSM, CDMA, GPRS, EDGE, and more. Although its not necessary to know these technologies for the exam, you might want to know 3G and 4G because they are all the rage right now.

3G (short for third-generation telecommunications) has been in use for several years. Many new phones and PDAs are equipped to connect to 3G networks. The main purpose is to enable these mobile devices to send data at higher speeds. However, these speeds vary depending on the vendor, the country you are in, and whether you move while you send data. For stationary transmissions, possible data rates range from 2Mbps to 14Mbps; for moving transmissions, data rates fall below 1Mbps. Of course, network congestion also has a hand in 3G data rates. Manufacturers suggest that a user can expect 384Kbps while stationary or walking and less than that in a moving car. There are millions of 3G users; 3G devices are available for laptops in the form of PC Cards and embedded within PDAs. 3G is made out to be the best thing since sliced bread by ISPs and telecommunications companies, but it is questionable whether it has really lived up to expectations.

4G (short for fourth generation), currently in development, is expected to completely replace current networks and create a much faster, more secure IP solution. This is where the real increases in data rates are expected; from 100Mbps in a moving vehicle to 1Gbps when stationary. One of the goals is to have a data rate of 100Mbps between any two points in the world at any time. 4G devices will be available for laptops, PDAs, and cell phones the same way that 3G devices are currently available.

802.11 Wireless

Up until now, we have been talking about Internet connectivity. Now I'd like to move over to wireless options for the LAN. The 802.11x series of protocols defines the various speeds, frequencies, and protocols used to transmit data over radiowaves in small geographic areas using unlicensed spectrums.

There are four different 802.11 derivatives you need to know for the exam: 802.11a, 802.11b, 802.11g, and 802.11n. Table 14.6 shows these technologies and the characteristics that differentiate them.

TABLE 14.6 **802.11x Standards**

802.11 Version	Maximum Data Rate	Frequency	Modulation Protocol Used
802.11a	54Mbps	5 GHz	OFDM
802.11b	11Mbps	2.4GHz	DSSS
802.11g	54Mbps	2.4GHz	OFDM
802.11n	600Mbps 300Mbps is typical	5 and/or 2.4GHz	OFDM

ExamAlert

Know the data rates and frequency used for each of the 802.11 versions!

Note

OFDM is orthogonal frequency-division multiplexing, a common modulation method. DSSS is direct-sequence spread spectrum, a less-used modulation technique.

The key with wireless is to make sure that your access point (AP) and wireless network adapters are compatible.

Bluetooth

This is a short-range radio technology aimed at simplifying communications and synchronization among network devices. Bluetooth is divided into three classes. Class I has a maximum transmission range of 100 meters, Class II (the most common) has a range of 10 meters, and Class III is short range and hardly used at 1 meter. An example of Bluetooth technologies would be the common Motorola Bluetooth wireless headsets. These and other Bluetooth

devices need to be *paired* either with your cellular phone or your PC to transmit data. Bluetooth data transfer rates are broken down into two versions, as shown in Table 14.7.

TABLE 14.7 **Bluetooth Versions**

Version	Maximum Data Rate
Version 1	721Kbps
Version 2	2.1Mbps

> **Note**
>
> Version 3 was just adopted in early 2009, offering higher data rates, low energy, and more security but is not covered in the 2009 A+ exams.

Setting Up a SOHO Router and Wireless Network Adapters

Okay! Now that we have gotten Internet connectivity and wireless out of the way, let's talk about the setup and configuration of our SOHO router. These devices have been called a plethora of different names, from the nice-router, switch, firewall, access point, and multifunction network device to the not so nice, which we can't mention here! Let's put it this way, you will troubleshoot SOHO routers, but much of the troubleshooting will be due to user error. Each manufacturer has their own interface, and some manufacturers are not the best with technical support or in the writing of their manual. In this section, I refer to a D-Link DIR655 that has served me well and is one of the easier devices to understand.

Most SOHO routers are set up to be plug-and–and-play, meaning that computers can be plugged in and they can communicate with each other and access the Internet. But a word of caution, you don't want to use the default settings that the manufacturer gives you; they are quite insecure. So the first thing we want to do is to log in to the router so that we can make some changes. To do this open a browser window and type the IP address of the router. For our D-Link DIR655, the default address is 192.168.0.1, the login is admin, and no password. A web-based emulator of this router is available at http://support.dlink.com/Emulators/dir655/index.html. If for some reason this link does not work, or is changed simply go to www.dlink.com, search for DIR-655, and when at the product page click Support, select your country, and click Emulator.

The first thing we want to do is to update the firmware so that we have the latest options and security available. This can be done in the Tools\Firmware section. Always make sure the router's firmware is updated before proceeding to configure it.

Next we access the Manual Internet Connection Setup button toward the bottom of the default screen. From here we see that the router is set up by default to obtain its WAN IP address automatically from the ISP, but in some cases you need to use a static IP address, or perhaps configure a secure connection to the Internet with Point to Point Tunneling Protocol (PPTP) or Layer 2 Tunneling Protocol (L2TP). Figure 14.10 shows these options.

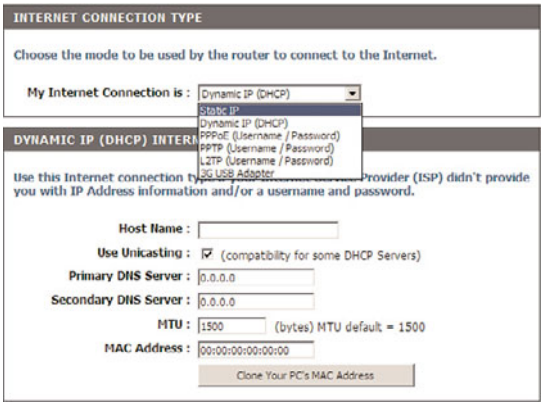


FIGURE 14.10 **D-Link Internet connection options**

If we selected any of the other options, we would have to input the correct information including IP address, username, and so forth. This information should be provided to you by the ISP you connect to.

Next we take a look at the network settings by clicking on the link called Network Settings on the left side. As shown in Figure 14.11, this is where we can change the LAN IP address and subnet mask of the router and enable or disable the DHCP server.

Now we take a look at the wireless settings; to do this, click on the Wireless Settings link on the left and then select the Manual Wireless Network setup at the bottom of the screen. That displays a window like the one shown in Figure 14.12.

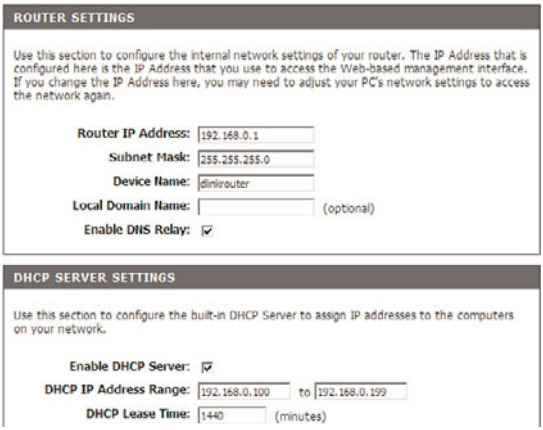


FIGURE 14.11 **D-Link network settings**

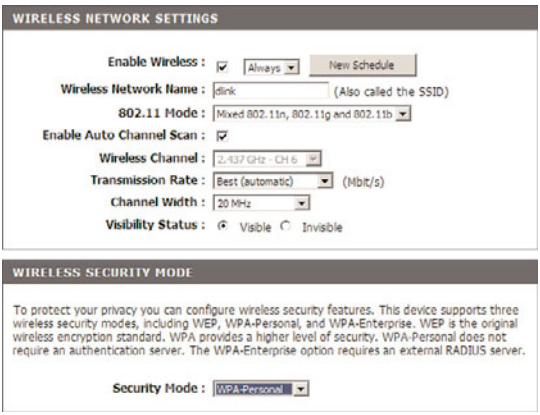


FIGURE 14.12 **D-Link wireless network settings**

From here, we can enable or disable the wireless radio and select the 802.11 technology of our choice. We can also modify the SSID (or Service Set Identifier) that is listed in the figure as Wireless Network Name and enable or disable SSID broadcasts, which is listed in the figure as Visibility Status. It's a good idea to modify the SSID. Think about it; thousands of people are using D-Link routers that all default to the same SSID! And finally, we can modify our encryptions settings for wireless. WPA2 utilizing AES is the most secure encryption that this router offers. Table 14.8 shows the characteristics of the various encryption methods.

TABLE 14.8 **Wireless Encryption Methods**

Wireless Encryption Protocol (Key Size)	Description	Encryption Level
WEP	Wired Equivalent Privacy	64-bit
WPA2	Wi-Fi Protected Access	256-bit
TKIP	Temporal Key Integrity Protocol	128-bit
AES	Advanced Encryption Standard	128-bit, 192-bit, and 256-bit

Note

WEP also has 128-bit and 256-bit versions, but these versions are not commonly found in wireless network hardware.

More SOHO Router Security

To offer a secure device, D-Link incorporated two types of firewalls into its DIR-655 device and most of its other products. The first is a network address translation (NAT) firewall that hides an entire network of IP addresses (the internal IP addresses), for example 192.168.0.100, behind a single publicly displayed IP address. The second is a stateful packet inspection (SPI) firewall, which monitors packets according to each session that they belong to. Many devices offer these technologies today to protect the consumer's computers on the LAN.

Beyond this, SOHO routers offer MAC filtering technology. We mentioned that the MAC address is the unique address that is applied to the network adapter by the manufacturer. You can create a list of the MAC addresses on your network and insert that into the SOHO router. This way, only computers that have MAC addresses on the list can send any data through the router. On the D-Link DIR655, this applies to wireless *and* wired connections, but on some devices it is only wireless connections. An example of a MAC address would be **`00-1e-68-55-ba-01`**; be prepared to see the numbers separated by colons instead of hyphens as well.

It is also recommended to change the administrator username (if possible) and password. Remember that a strong password is one that is at least 8 alphanumeric characters, with at least one capital and one special character. The best passwords incorporate all these ideas but are 14 characters or more. Finally, back up the settings to your computer in the case that you need to reset the device in the future.

Some More SOHO Tidbits

Most people are wireless crazy nowadays but don't forget that these SOHO routers normally come with four wired LAN ports. Some people love wired connections, and this D-Link device is considered 10/100/1000BASE-T. That means that it can auto-negotiate connections at 10bps, 100Mbps, and 1000Mbps (1Gbps). The BASE applies to any speed, and it is short for base-band, meaning every computer on the network shares the same channel or frequency. The T is short for twisted pair. By default unshielded twisted pair cables can send data 100 meters before the electronic signal attenuates to such a point where it is useless.

Exam Alert

UTP cables can send data 100 meters maximum (328 feet).

These devices can usually do another two things concerning ports:

- **Port forwarding:** This forwards an external network port to an internal IP address and port. This enables you to have a web server, FTP server, and other servers, but you need to have only one port open on the WAN side of the router. It can be any port you like; of course, you would need to tell people which port they need to connect to if it is not a standard one.

  The D-Link device we have been using takes this to a new level by enabling what it calls Virtual Servers, making the process a lot more user-friendly. So, for example, you might have an FTP server running internally on your LAN; its IP address and port might be 192.168.0.100:21 (notice how the colon separates the IP address from the port), but you would have users on the Internet connect to your router's WAN address, for example 65.43.18.1 and any port you want. The router takes care of the rest, and the forwarding won't be noticed by the typical user.

- **Port triggering:** This enables you to specify outgoing ports that your computer uses for special applications, and their corresponding inbound ports will be opened automatically when the sessions are established. This is helpful for things like bit torrents.

Finally, we need to place our SOHO router. It is important to keep the device away from any electrical sources such as outlets, UPS, microwaves, and so on and any large amounts of metal to avoid interference.

The basement is probably not the best place for a router due to the thick walls, copper pipes, and most likely your main electrical panel. The antennas should be either at a 90-degree angle from each other or pointing toward where the computers are. The more centralized the router is, the better the wireless access your computers will get.

Wireless Network Adapters

Wireless network adapters require additional configuration compared to wired network adapters. This includes scanning for wireless networks, possibly typing the SSID of the wireless access point, specifying a channel, selecting the type of wireless encryption protocol to correspond with what is used by the wireless access point, and entering the security passphrase for that wireless encryption type that has been configured on the router.

Cram Quiz

Answer these questions. The answers follow the last question. If you cannot answer these questions correctly, consider reading this section again until you can.

1. Which of the following is the fastest wireless protocol?

- ❍ **A.** 802.11b
- ❍ **B.** 802.11g
- ❍ **C.** 802.11n
- ❍ **D.** 802.11x

2. What is the maximum data rate of Bluetooth Version 2?

- ❍ **A.** 721Kbps
- ❍ **B.** 100Mbps
- ❍ **C.** 2.1Gbps
- ❍ **D.** 2.1Mbps

3. Which of these is a valid MAC address?

- ❍ **A.** 00:3e:2b:1d:11:ff
- ❍ **B.** 192.168.0.100
- ❍ **C.** 00:3g:2b:1d:11:fe
- ❍ **D.** 2001:0000:0000:01

4. Which of these hides an entire network of IP addresses?
   - ❍ **A.** SPI
   - ❍ **B.** NAT
   - ❍ **C.** SSH
   - ❍ **D.** FTP

5. Which of the following use the 2.4-GHz frequency range? (Select all that apply.)
   - ❍ **A.** 802.11b
   - ❍ **B.** 802.11a
   - ❍ **C.** 802.11g
   - ❍ **D.** 802.11n

Cram Quiz Answers

1. **C.** 802.11n has a theoretical maximum data rate of 600Mbps; however, 300Mbps is the norm.
2. **D.** Version 2 has a maximum data rate of 2.1Mbps, Version 1 maxes out at 721Kbps.
3. **A.** Answer A is the valid MAC address. B is an IP address, C is not valid because the letter G is not part of the hexadecimal numbering system, and D appears to be a truncated IPv6 address.
4. **B.** Network Address Translation hides an entire network of IP Addresses. SPI or Stateful Packet Inspection is the other type of firewall that today's SOHO routers incorporate.
5. **A**, **C**, and **D.** The only protocol that does not use the 2.4GHz frequency is 802.11a.

Additional Reading and Resources

Prowse, David L. *CompTIA Network+ Video Mentor*, First edition. Que. 2009.

Harwood, Mike. *CompTIA ExamPrep Network+ N10-004*

Additional A+ resources: http://www.davidlprowse.com/aplus