Introduction

Welcome to the Network+ Exam Cram. This book is designed to prepare you to take—and pass—the CompTIA Network+ exam. The Network+ exam has become the leading introductory-level network certification available today. It is recognized by both employers and industry giants (such as Microsoft and Novell) as providing candidates with a solid foundation of networking concepts, terminology, and skills. The Network+ exam covers a broad range of networking concepts to prepare candidates for the technologies they are likely to work with in today's network environments.

About Network+ Exam Cram

Exam Crams are designed to give you the information you need to know to prepare for the Network+ exam. They cut through the extra information, focusing on the areas you need to get through the exam. With this in mind, the elements within the Exam Cram titles are aimed at providing the exam information you need in the most succinct and accessible manner.

In this light, this book is organized to closely follow the actual CompTIA objectives. As such, it is easy to find the information required for each of the specified CompTIA Network+ objectives. The objective focus design used by this Exam Cram is an important feature because the information you need to know is easily identifiable and accessible. To see what we mean, compare the CompTIA objectives to the book's layout, and you will see that the facts are right where you would expect them to be.

Within the chapters themselves, potential exam hot spots are clearly highlighted with Exam Alerts. They have been carefully placed to let you know that the surrounding discussion is an important area for the exam. To further help you prepare for the exam, a Cram Sheet is included that can be used in the final stages of test preparation. Be sure to pay close attention to the bulleted points on the Cram Sheet, because they pinpoint the technologies and facts you probably will encounter on the test.

Finally, great effort has gone into the end-of-chapter questions and practice tests to ensure that they accurately represent the look and feel of the ones you will see on the real Network+ exam. Be sure, before taking the exam, that you are comfortable with both the format and content of the questions provided in this book.
About the Network+ Exam

The Network+ (2009 Edition) exam is a revised version of the original exam. The new Network+ objectives are aimed toward those who have nine months of experience in network support and administration. CompTIA believes that new Network+ candidates will require more hands-on experience in network administration and troubleshooting, but this should not discourage those who do not. Quite simply, the nature of the questions on the new exam is not dissimilar to the old, and you can get by without actual hands-on experience. Still, a little hands-on experience never hurt anyone and will certainly add to your confidence going into the exam.

You will have a maximum of 90 minutes to answer the 72 questions on the exam. The allotted time is quite generous, so when you are finished, you probably will have time to double-check a few of the answers you were unsure of. By the time the dust settles, you will need a minimum score of 646 to pass the Network+ exam. This is on a scale of 100 to 900.

One of the best things about the Network+ certification is that after you pass the exam, you are certified for life. There is no need to ever recertify. This fact can make the cost of taking the Network+ exam a little easier to swallow. For more information on the specifics of the Network+ exam, refer to CompTIA's main website at http://www.comptia.org/certification/.

Booking and Taking the Network+ Certification Exam

Unfortunately, testing is not free. You're charged $239 for each test you take, whether you pass or fail. In the United States and Canada, tests are administered by Sylvan Prometric or VUE testing services. To book a test with Prometric or to locate a Prometric testing center near you, refer to the website at http://securereg3.prometric.com/ or call 1-888-895-6116. To access the VUE contact information and book an exam, refer to the website at http://www.vue.com or call 1-877-551-7587. When booking an exam, you need to provide the following information:

- Your name as you would like it to appear on your certificate.
- Your Social Security or Social Insurance number.
- Contact phone numbers (to be called in case of a problem).
What to Expect from the Exam

If you haven’t taken a certification test, the process can be a little unnerving. Even if you’ve taken numerous tests, it is not much better. Mastering the inner mental game often can be as much of a battle as knowing the material. Knowing what to expect before heading in can make the process a little more comfortable.

Certification tests are administered on a computer system at a Prometric or VUE authorized testing center. The format of the exams is straightforward: Each question has several possible answers to choose from. In fact, the questions in this book provide a very good example of the types of questions you can expect on the exam. If you are comfortable with them, the test should hold few surprises. Many of the questions vary in length; some of them are longer scenario questions, whereas others are short and to the point. Read the questions carefully; the longer questions often have a key point that will lead you to the correct answer.

Most of the questions on the Network+ exam require you to choose a single correct answer, but a few require multiple answers. When there are multiple correct answers, a message at the bottom of the screen prompts you to “choose all that apply.” Be sure to read these messages.
A Few Exam Day Details

It is recommended that you arrive at the examination room at least 15 minutes early, although a few minutes earlier certainly would not hurt. This will give you time to prepare and will give the test administrator time to answer any questions you might have before the test begins. Many people suggest that you review the most critical information about the test you’re taking just before the test. (*Exam Cram* books provide a reference—the Cram Sheet, located inside the front of this book—that lists the essential information from the book in distilled form.) Arriving a few minutes early will give you some time to compose yourself and mentally review this critical information.

You will be asked to provide two forms of ID, one of which must be a photo ID. Both of the identifications you choose should have a signature. You also might need to sign in when you arrive and sign out when you leave.

Be warned: The rules are very clear about what you can and cannot take into the examination room. Books, laptops, note sheets, and so on are not allowed in the examination room. The test administrator will hold these items, to be returned after you complete the exam. You might receive either a wipe board or a pen and a single piece of paper for making notes during the exam. The test administrator will ensure that no paper is removed from the examination room.

After the Test

Whether you want it or not, as soon as you finish your test, your score is displayed on the computer screen. In addition to the results appearing on the computer screen, a hard copy of the report is printed for you. Like the onscreen report, the hard copy displays the results of your exam and provides a summary of how you did on each section and on each technology. If you were unsuccessful, this summary can help you determine the areas you need to brush up on.

When you pass the Network+ exam, you will have earned the Network+ certification, and your certificate will be mailed to you within a few weeks. Should you not receive your certificate and information packet within five weeks of passing your exam, contact CompTIA at fulfillment@comptia.org, or call 1-630-268-1818 and ask for the fulfillment department.
Last-Minute Exam Tips

Studying for a certification exam really is no different from studying for any other exam, but a few hints and tips can give you the edge on exam day:

- **Read all the material**: CompTIA has been known to include material not expressly specified in the objectives. This book has included additional information not reflected in the objectives in an effort to give you the best possible preparation for the examination.

- **Watch for the Exam Tips and Notes**: The Network+ objectives include a wide range of technologies. Exam Tips and Notes found throughout each chapter are designed to pull out exam-related hot spots. These can be your best friends when preparing for the exam.

- **Use the questions to assess your knowledge**: Don’t just read the chapter content; use the exam questions to find out what you know and what you don’t. If you are struggling, study some more, review, and then assess your knowledge again.

- **Review the exam objectives**: Develop your own questions and examples for each topic listed. If you can develop and answer several questions for each topic, you should not find it difficult to pass the exam.

Good luck!
CHAPTER SEVEN

Wireless Networking

Objectives

1.7 Compare the characteristics of wireless communication standards
   ▶ 802.11 a/b/g/n
   ▶ Speeds
   ▶ Distance
   ▶ Channels
   ▶ Frequency
   ▶ Authentication and encryption
   ▶ WPA
   ▶ WEP
   ▶ RADIUS
   ▶ TKIP

3.4 Implement a basic wireless network
   ▶ Install client
   ▶ Access point placement
   ▶ Install access point
   ▶ Configure appropriate encryption
   ▶ Configure channels and frequencies
   ▶ Set ESSID and beacon
   ▶ Verify installation

What You Need To Know

▶ Review the characteristics of the various network topologies, including their strengths and weaknesses.
▶ Review the characteristics of 802.11 standards, including the information provided in all tables in this chapter.
▶ Identify the components involved in wireless communications.
Chapter 7: Wireless Networking

Review the factors that cause wireless interference.
Review the Notes, Tips, and Exam Alerts in this chapter. Be sure that you understand the information in the Exam Alerts. If you don't understand the topic mentioned in an Exam Alert, reread that information in the chapter, and then reread the Exam Alert.

Introduction

One of the bigger changes in the networking world since the release of the previous Network+ is in wireless networking. Networks of all shapes and sizes incorporate wireless segments into their networks. Home wireless networking has also grown significantly in the last few years.

Wireless networking enables users to connect to a network using radio waves instead of wires. Network users within range of a wireless access point (AP) can move around an office freely without needing to plug into a wired infrastructure. The benefits of wireless networking clearly have led to its growth.

Today, wireless local area networks (WLANs) provide a flexible and secure data communications system that augments an Ethernet LAN or, in some cases, replaces it. Wireless transmissions send and receive data using radio frequency (RF) signals, freeing us from wired solutions.

In a common wireless implementation, a wireless transceiver (transmitter/receiver), known as an access point, connects to the wired network from a fixed location using standard cabling. The wireless access point receives and then transmits data between the wireless LAN and the wired network infrastructure.

Client systems communicate with a wireless access point using wireless LAN adapters. Such adapters are built into or can be added to laptops, PDAs, or desktop computers. Wireless LAN adapters provide the communication point between the client system and the airwaves via an antenna.

This chapter explores the many facets of wireless networking, starting with some of the concepts and technologies that make wireless networking possible.

**NOTE**

Ad hoc and infrastructure This chapter discusses ad hoc and infrastructure wireless network topologies. If you need a refresher on these topologies, they are discussed in Chapter 1, “Introduction to Networking.”
Wireless Access Points

As discussed in Chapter 3, “Networking Components and Devices,” a wireless access point (AP) is both a transmitter and receiver (transceiver) device used for wireless LAN (WLAN) radio signals. An AP typically is a separate network device with a built-in antenna, transmitter, and adapter. APs use the wireless infrastructure network mode to provide a connection point between WLANs and a wired Ethernet LAN. APs also typically have several ports, giving you a way to expand the network to support additional clients.

Depending on the size of the network, one or more APs might be required. Additional APs are used to allow access to more wireless clients and to expand the range of the wireless network. Each AP is limited by a transmission range—the distance a client can be from an AP and still get a usable signal. The actual distance depends on the wireless standard being used and the obstructions and environmental conditions between the client and the AP. Factors affecting wireless transmission ranges are covered later in this chapter.

NOTE

Wireless access points An AP can operate as a bridge, connecting a standard wired network to wireless devices, or as a router, passing data transmissions from one access point to another.

TIP

AP range If you are using a wireless device that loses its connection, you might be too far from the AP.

As mentioned in Chapter 1, an AP can be used in an infrastructure wireless network design. Used in the infrastructure mode, the AP receives transmissions from wireless devices within a specific range and transmits those signals to the network beyond. This network might be a private Ethernet network or the Internet. In infrastructure wireless networking, there might be multiple access points to cover a large area or only a single access point for a small area, such as a single home or small building.
Chapter 7: Wireless Networking

Working with APs

When working with wireless APs, you need to understand many terms and acronyms. This section defines some of the more common wireless acronyms you will see both on the exam and in wireless networking documentation.

**EXAM ALERT**

Several of the acronyms provided in the following list are sure to be on the Network+ exam. Be sure you can identify the function of each before taking the exam.

- **Service Set Identifier (SSID)**—A network name needed to connect to a wireless AP. It is like a workgroup name used with Windows networking. 802.11 wireless networks use the SSID to identify all systems belonging to the same network. Client stations must be configured with the SSID to be authenticated to the AP. The AP might broadcast the SSID, allowing all wireless clients in the area to see the AP’s SSID. For security reasons, APs can be configured not to broadcast the SSID or to cloak it. This means that an administrator needs to give client systems the SSID instead of allowing it to be discovered automatically.

  **TIP**

  One element of wireless security involves configuring the AP not to broadcast the SSID. This configuration is made on the AP.

- **Basic Service Set (BSS)**—Refers to a wireless network that uses a single AP and one or more wireless clients connecting to the AP. Many home offices are an example of a BSS design. The BSS is an example of the infrastructure wireless topology. Wireless topologies and other network topologies are discussed in Chapter 1.

- **Extended Service Set (ESS)**—Refers to two or more connected BSSs that use multiple APs. The ESS is used to create WLANs or larger wireless networks and is a collection of APs and clients. Connecting BSS systems allows clients to roam between areas and maintain the wireless connection without having to reconfigure between BSSs.
Extended Service Set Identifier (ESSID)—Although the terms ESSID and SSID are used interchangeably, there is a difference between the two. SSID is the name used with BSS networks. ESSID is the network name used with an ESS wireless network design. With an ESS, not all APs necessarily use the same name.

Basic Service Set Identifier (BSSID)—The MAC address of the BSS AP. The BSSID is not to be confused with the SSID, which is the name of the wireless network.

Basic Service Area (BSA)—When troubleshooting or designing wireless networks, the BSA is an important consideration. The BSA refers to the AP’s coverage area. The BSA for an AP depends on many factors, including the strength of the AP antenna, interference in the area, and whether an omnidirectional or directional antenna is being used.

Wireless Antennas

A wireless antenna is an integral part of overall wireless communication. Antennas come in many different shapes and sizes, with each one designed for a specific purpose. Selecting the right antenna for a particular network implementation is a critical consideration and one that could ultimately decide how successful a wireless network will be. In addition, using the right antenna can save you money on networking costs, because you need fewer antennas and access points.

Many small home network adapters and access points come with a nonupgradable antenna, but higher-grade wireless devices require you to choose an antenna. Determining which antenna to select takes careful planning and requires an understanding of what range and speed you need for a network. The antenna is designed to help wireless networks do the following:

- Work around obstacles
- Minimize the effects of interference
- Increase signal strength
- Focus the transmission, which can increase signal speed

The following sections explore some of the characteristics of wireless antennas.
Antenna Ratings

When a wireless signal is low and is being affected by heavy interference, it might be possible to upgrade the antenna to create a more solid wireless connection. To determine an antenna's strength, we refer to its gain value. But how do we determine the gain value?

Suppose that a huge wireless tower is emanating circular waves in all directions. If we could see these waves, we would see them forming a sphere around the tower. The signals around the antenna flow equally in all directions, including up and down. An antenna that does this has a 0dBi gain value and is called an isotropic antenna. The isotropic antenna rating provides a base point for measuring actual antenna strength.

NOTE

The dB in dBi stands for decibels, and the i stands for the hypothetical isotropic antenna.

An antenna's gain value represents the difference between the 0dBi isotropic and the antenna's power. For example, a wireless antenna advertised as 15dBi is 15 times stronger than the hypothetical isotropic antenna. The higher the decibel figure, the higher the gain.

When looking at wireless antennas, remember that a higher gain value means stronger send and receive signals. In terms of performance, the rule of thumb is that every 3dB of gain added doubles an antenna's effective power output.

Antenna Coverage

When selecting an antenna for a particular wireless implementation, it is necessary to determine the type of coverage the antenna uses. In a typical configuration, a wireless antenna can be either omnidirectional or directional. Which one you choose depends on the wireless environment.

An omnidirectional antenna is designed to provide a 360-degree dispersed wave pattern. This type of antenna is used when coverage in all directions from the antenna is required. Omnidirectional antennas are advantageous when a broad-based signal is required. For example, if you provide an even signal in all directions, clients can access the antenna and its associated access point from various locations. Because of the dispersed nature of omnidirectional antennas, the signal is weaker overall and therefore accommodates shorter signal distances. Omnidirectional antennas are great in an environment that has a clear line of sight between the senders and receivers. The power is evenly spread to all
points, making omnidirectional antennas well suited for home and small office applications.

**NOTE**

**Directional differences**  Omnidirectional antennas provide wide coverage but weaker signal strength in any one direction than a directional antenna.

Directional antennas are designed to focus the signal in a particular direction. This focused signal allows for greater distances and a stronger signal between two points. The greater distances enabled by directional antennas give you a viable alternative for connecting locations, such as two offices, in a point-to-point configuration.

Directional antennas are also used when you need to tunnel or thread a signal through a series of obstacles. This concentrates the signal power in a specific direction and allows you to use less power for a greater distance than an omnidirectional antenna. Table 7.1 compares omnidirectional and directional wireless antennas.

<table>
<thead>
<tr>
<th>Table 7.1 Comparing Omnidirectional and Directional Antennas</th>
</tr>
</thead>
<tbody>
<tr>
<td>Characteristic</td>
</tr>
<tr>
<td>Wireless area coverage</td>
</tr>
<tr>
<td>Wireless transmission range</td>
</tr>
<tr>
<td>Wireless coverage shaping</td>
</tr>
</tbody>
</table>
Wireless Radio Channels

Radio frequency (RF) channels are an important part of wireless communication. A channel is the band of RF used for the wireless communication. Each IEEE wireless standard specifies the channels that can be used. The 802.11a standard specifies radio frequency ranges between 5.15 and 5.875GHz. In contrast, 802.11b and 802.11g standards operate in the 2.4 to 2.497GHz range. IEEE wireless standards are discussed later in this chapter.

As far as channels are concerned, 802.11a has a wider frequency band, allowing more channels and therefore more data throughput. As a result of the wider band, 802.11a supports up to eight nonoverlapping channels. 802.11b/g standards use the smaller band and support only up to three nonoverlapping channels.

It is recommended that nonoverlapping channels be used for communication. In the U.S., 802.11b/g use 11 channels for data communication, as mentioned; three of these—channels 1, 6, and 11—are nonoverlapping. Most manufacturers set their default channel to one of the nonoverlapping channels to avoid transmission conflicts. With wireless devices you can select which channel your WLAN operates on to avoid interference from other wireless devices that operate in the 2.4GHz frequency range.

When troubleshooting a wireless network, be aware that overlapping channels can disrupt the wireless communications. For example, in many environments, APs are inadvertently placed close together—perhaps two access points in separate offices located next door to each other or between floors. Signal disruption

**NOTE**

Polarization

In the wireless world, polarization refers to the direction in which the antenna radiates wavelengths. This direction can either be vertical, horizontal, or circular. Today, vertical antennas are perhaps the most common. As far as the configuration is concerned, the sending and receiving antennas should be set to the same polarization.

**NOTE**

That hertz! Hertz (Hz) is the standard of measurement for radio frequency. Hertz is used to measure the frequency of vibrations and waves, such as sound waves and electromagnetic waves. One hertz is equal to one cycle per second. Radio frequency is measured in kilohertz (KHz), 1,000 cycles per second; megahertz (MHz), one million cycles per second; or gigahertz (GHz), one billion cycles per second.
results if channel overlap exists between the access points. The solution is to try to move the access point to avoid the overlap problem, or to change channels to one of the other nonoverlapping channels. For example, you could switch from channel 6 to channel 11.

Typically you would change the channel of a wireless device only if it overlapped with another device. If a channel must be changed, it must be changed to another, nonoverlapping channel. Table 7.2 shows the channel ranges for 802.11b/g wireless standards. Table 7.3 shows the channel ranges for 802.11a. 802.11n has the option of using both channels used by 802.11a and b/g.

**EXAM ALERT**

Troubleshooting utilities When troubleshooting a wireless problem in Windows, you can use the `ipconfig` command to see the status of IP configuration. Similarly, the `ifconfig` command can be used in Linux. In addition, Linux users can use the `iwconfig` command to view the state of your wireless network. Using `iwconfig`, you can view such important information as the link quality, AP MAC address, data rate, and encryption keys, which can be helpful in ensuring that the parameters in the network are consistent.

**TIP**

IEEE 802.11b/g wireless systems communicate with each other using radio frequency signals in the band between 2.4GHz and 2.5GHz. Neighboring channels are 5MHz apart. Applying two channels that allow the maximum channel separation decreases the amount of channel crosstalk and provides a noticeable performance increase over networks with minimal channel separation.

Tables 7.2 and 7.3 outline the available wireless channels. When deploying a wireless network, it is recommended that you use channel 1, grow to use channel 6, and add channel 11 when necessary, because these three channels do not overlap.

<table>
<thead>
<tr>
<th>Table 7.2 RF Channels for 802.11b/g</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Channel</strong></td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>2</td>
</tr>
<tr>
<td>3</td>
</tr>
<tr>
<td>4</td>
</tr>
</tbody>
</table>
Table 7.2 RF Channels for 802.11b/g  

<table>
<thead>
<tr>
<th>Channel</th>
<th>Frequency Band</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>2432MHz</td>
</tr>
<tr>
<td>6</td>
<td>2437MHz</td>
</tr>
<tr>
<td>7</td>
<td>2442MHz</td>
</tr>
<tr>
<td>8</td>
<td>2447MHz</td>
</tr>
<tr>
<td>9</td>
<td>2452MHz</td>
</tr>
<tr>
<td>10</td>
<td>2457MHz</td>
</tr>
<tr>
<td>11</td>
<td>2462MHz</td>
</tr>
</tbody>
</table>

NOTE

Why do they overlap? One thing to remember when looking at Table 7.2 is that the RF channels listed (2412 for channel 1, 2417 for 2, and so on) are actually the center frequency that the transceiver within the radio and access point uses. There is only 5MHz separation between the center frequencies, and an 802.11b signal occupies approximately 30MHz of the frequency spectrum. As a result, data signals fall within about 15MHz of each side of the center frequency and overlap with several adjacent channel frequencies. This leaves you with only three channels (channels 1, 6, and 11 for the U.S.) that you can use without causing interference between access points.

Table 7.3 RF Channels for 802.11a

<table>
<thead>
<tr>
<th>Channel</th>
<th>Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>36</td>
<td>5180MHz</td>
</tr>
<tr>
<td>40</td>
<td>5200MHz</td>
</tr>
<tr>
<td>44</td>
<td>5220MHz</td>
</tr>
<tr>
<td>48</td>
<td>5240MHz</td>
</tr>
<tr>
<td>52</td>
<td>5260MHz</td>
</tr>
<tr>
<td>56</td>
<td>5280MHz</td>
</tr>
<tr>
<td>60</td>
<td>5300MHz</td>
</tr>
<tr>
<td>64</td>
<td>5320MHz</td>
</tr>
</tbody>
</table>

Data Rate Versus Throughput

When talking about wireless transmissions, it is important to distinguish between throughput and data rate. From time to time these terms are used interchangeably, but technically speaking, they are different. As shown later in this
chapter, each wireless standard has an associated speed. For instance, 802.11g lists a speed of up to 54Mbps. This represents the speed at which devices using this standard can send and receive data. However, in network data transmissions, many factors prevent the actual speeds from reaching this end-to-end theoretical maximum. For instance, data packets include overhead such as routing information, checksums, and error recovery data. Although this might all be necessary, it can impact overall speed.

The number of clients on the network can also impact the data rate; the more clients, the more collisions. Depending on the network layout, collisions can have a significant impact on end-to-end transmission speeds. Wireless network signals degrade as they pass through obstructions such as walls or doors; the signal speed deteriorates with each obstruction.

All these factors leave us with the actual throughput of wireless data transmissions. Throughput represents the actual speed to expect from wireless transmissions. In practical application, wireless transmissions are approximately one-half or less of the data rate. This means that you could hope for about 20 to 25Mbps for 802.11g. Depending on the wireless setup, the transmission rate could be much less.

**Factors Affecting Wireless Signals**

Because wireless signals travel through the atmosphere, they are susceptible to different types of interference than standard wired networks. Interference weakens wireless signals and therefore is an important consideration when working with wireless networking.

**Interference Types**

Wireless interference is an important consideration when you’re planning a wireless network. Interference is unfortunately inevitable, but the trick is to minimize the levels of interference. Wireless LAN communications typically are based on radio frequency signals that require a clear and unobstructed transmission path.
The following are some factors that cause interference:

- **Physical objects**: Trees, masonry, buildings, and other physical structures are some of the most common sources of interference. The density of the materials used in a building’s construction determines the number of walls the RF signal can pass through and still maintain adequate coverage. Concrete and steel walls are particularly difficult for a signal to pass through. These structures will weaken or at times completely prevent wireless signals.

- **Radio frequency interference**: Wireless technologies such as 802.11b/g use an RF range of 2.4GHz, and so do many other devices, such as cordless phones, microwaves, and so on. Devices that share the channel can cause noise and weaken the signals.

- **Electrical interference**: Electrical interference comes from devices such as computers, refrigerators, fans, lighting fixtures, or any other motorized devices. The impact that electrical interference has on the signal depends on the proximity of the electrical device to the wireless access point. Advances in wireless technologies and in electrical devices have reduced the impact that these types of devices have on wireless transmissions.

- **Environmental factors**: Weather conditions can have a huge impact on wireless signal integrity. Lightning, for example, can cause electrical interference, and fog can weaken signals as they pass through.

Many wireless implementations are found in the office or at home. Even when outside interference such as weather is not a problem, every office has plenty of wireless obstacles. Table 7.4 highlights a few examples to be aware of when implementing a wireless network indoors.

<table>
<thead>
<tr>
<th>Obstruction</th>
<th>Obstacle Severity</th>
<th>Sample Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wood/wood paneling</td>
<td>Low</td>
<td>Inside a wall or hollow door</td>
</tr>
<tr>
<td>Drywall</td>
<td>Low</td>
<td>Inside walls</td>
</tr>
<tr>
<td>Furniture</td>
<td>Low</td>
<td>Couches or office partitions</td>
</tr>
<tr>
<td>Clear glass</td>
<td>Low</td>
<td>Windows</td>
</tr>
<tr>
<td>Tinted glass</td>
<td>Medium</td>
<td>Windows</td>
</tr>
<tr>
<td>People</td>
<td>Medium</td>
<td>High-volume traffic areas that have considerable pedestrian traffic</td>
</tr>
<tr>
<td>Ceramic tile</td>
<td>Medium</td>
<td>Walls</td>
</tr>
</tbody>
</table>
Factors Affecting Wireless Signals

Table 7.4 Wireless Obstacles Found Indoors

<table>
<thead>
<tr>
<th>Obstruction</th>
<th>Obstacle Severity</th>
<th>Sample Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Concrete blocks</td>
<td>Medium/high</td>
<td>Outer wall construction</td>
</tr>
<tr>
<td>Mirrors</td>
<td>High</td>
<td>Mirror or reflective glass</td>
</tr>
<tr>
<td>Metals</td>
<td>High</td>
<td>Metal office partitions, doors, metal office furniture</td>
</tr>
<tr>
<td>Water</td>
<td>High</td>
<td>Aquariums, rain, fountains</td>
</tr>
</tbody>
</table>

Spread-Spectrum Technology

*Spread spectrum* refers to the manner in which data signals travel through a radio frequency. With spread spectrum, data does not travel straight through a single RF band; this type of transmission is known as *narrowband transmission*. Spread spectrum, on the other hand, requires that data signals either alternate between carrier frequencies or constantly change their data pattern. Although the shortest distance between two points is a straight line (narrowband), spread spectrum is designed to trade bandwidth efficiency for reliability, integrity, and security. Spread-spectrum signal strategies use more bandwidth than in the case of narrowband transmission, but the trade-off is a data signal that is clearer and easier to detect. The two types of spread-spectrum radio are *frequency hopping* and *direct sequence*.

Frequency-Hopping Spread-Spectrum (FHSS) Technology

FHSS requires the use of narrowband signals that change frequencies in a predictable pattern. The term *frequency hopping* refers to data signals hopping between narrow channels. For example, consider the 2.4GHz frequency band used by 802.11b/g. This range is divided into 70 narrow channels of 1MHz each. Somewhere between 20 and several hundred milliseconds, the signal hops to a new channel following a predetermined cyclical pattern.

Because data signals using FHSS switch between RF bands, they have a strong resistance to interference and environmental factors. The FHSS signal strategy makes it well suited for installations designed to cover a large geographic area and where using directional antennas to minimize the influence of environmental factors is not possible.

FHSS is not the preferred spread-spectrum technology for today’s wireless standards. However, FHSS is used for some lesser-used standards and for cellular deployments for fixed broadband wireless access (BWA), where the use of DSSS (discussed next) is virtually impossible because of its limitations.
Chapter 7: Wireless Networking

Direct-Sequence Spread-Spectrum (DSSS) Technology
With DSSS transmissions, the signal is spread over a full transmission frequency spectrum. For every bit of data that is sent, a redundant bit pattern is also sent. This 32-bit pattern is called a chip. These redundant bits of data provide both security and delivery assurance. The reason transmissions are so safe and reliable is simply because the system sends so many redundant copies of the data, and only a single copy is required to have complete transmission of the data or information. DSSS can minimize the effects of interference and background noise.

As for a comparison between the two, DSSS has the advantage of providing better security and signal delivery than FHSS, but it is a sensitive technology, affected by many environmental factors.

Orthogonal Frequency Division Multiplexing
Orthogonal Frequency Division Multiplexing (OFDM) is a transmission technique that transfers large amounts of data over 52 separate, evenly spaced frequencies. OFDM splits the radio signal into these separate frequencies and simultaneously transmits them to the receiver. Splitting the signal and transferring over different frequencies reduces the amount of crosstalk interference. OFDM is associated with 802.11a, 802.11g amendments, and 802.11n wireless standards.

Beacon Management Frame
Within wireless networking is a frame type known as the beacon management frame (beacon). Beacons are an important part of the wireless network because it is their job to advertise the presence of the access point so that systems can locate it. Wireless clients automatically detect the beacons and attempt to establish a wireless connection to the access point.

The beacon frame is sent by the access point in an infrastructure network design. Client stations send beacons only if connected in an ad hoc network design. The beacon frame has several parts, all of which the client system uses to learn about the AP before attempting to join the network:

- **Channel information**: Includes which channel the AP uses.
- **Supported data rates**: Includes the data transfer rates identified by the AP configuration.
Service Set Identifier (SSID): This beacon includes the name of the wireless network.

Time stamp: Includes synchronization information. The client system uses the time stamp to synchronize its clock with the AP.

These beacons are transmitted from the AP about every 10 seconds. The beacon frames add overhead to the network. Therefore, some APs let you reduce the number of beacons that are sent. With home networks, constant beacon information is unnecessary.

Passive and Active Scanning
Before a client system can attempt to connect to an access point, it must be able to locate it. The two methods of AP discovery are as follows:

Passive scanning: The client system listens for the beacon frames to discover the AP. After it is detected, the beacon frame provides the information necessary for the system to access the AP.

Active scanning: The client station transmits another type of management frame known as a probe request. The probe request goes out from the client system, looking for a specific SSID or any SSID within its area. After the probe request is sent, all APs in the area with the same SSID reply with another frame, the probe response. The information contained in the probe response is the same information included with the beacon frame. This information enables the client to access the system.

802.11 Wireless Standards
802.11 represents the IEEE designation for wireless networking. Several wireless networking specifications exist under the 802.11 banner. The Network+ objectives focus on 802.11, 802.11a, 802.11b, 802.11g, and 802.11n. All these standards use the Ethernet protocol and the CSMA/CA access method.
The 802.11 wireless standards can differ in terms of speed, transmission ranges, and frequency used, but in terms of actual implementation they are similar. All standards can use either an infrastructure or ad hoc network design, and each can use the same security protocols. Ad hoc and infrastructure wireless topologies were discussed in Chapter 1.

- **IEEE 802.11**: There were actually two variations on the initial 802.11 wireless standard. Both offered 1 or 2Mbps transmission speeds and the same RF of 2.4GHz. The difference between the two was in how data traveled through the RF media. One used FHSS, and the other used DSSS. The original 802.11 standards are far too slow for modern networking needs and are now no longer deployed.

- **IEEE 802.11a**: In terms of speed, the 802.11a standard was far ahead of the original 802.11 standards. 802.11a specified speeds of up to 54Mbps in the 5GHz band, but most commonly, communication takes place at 6Mbps, 12Mbps, or 24Mbps. 802.11a is incompatible with the 802.11b and 802.11g wireless standards.

- **IEEE 802.11b**: The 802.11b standard provides for a maximum transmission speed of 11Mbps. However, devices are designed to be backward-compatible with previous 802.11 standards that provided for speeds of 1, 2, and 5.5Mbps. 802.11b uses a 2.4GHz RF range and is compatible with 802.11g.

- **IEEE 802.11g**: 802.11g is a popular wireless standard today. 802.11g offers wireless transmission over distances of 150 feet and speeds up to 54Mbps compared with the 11Mbps of the 802.11b standard. Like 802.11b, 802.11g operates in the 2.4GHz range and therefore is compatible with it.

- **IEEE 802.11n**: The newest of the wireless standards listed in the Network+ objectives is 802.11n. The goal of the 802.11n standard is to significantly increase throughput in both the 2.4GHz and the 5GHz frequency range. The baseline goal of the standard was to reach speeds of 100Mbps, but given the right conditions, it is estimated that the 802.11n speeds might reach a staggering 600Mbps. In practical operation, 802.11n speeds will be much slower.
802.11 Wireless Standards

The Magic Behind 802.11n

802.11n is poised to bring about the next big change in wireless networking, promising greater distances and staggering speeds. But how is this done? 802.11n takes the best from the 802.11 standards and mixes in some new features to take wireless to the next level. First among these new technologies is multiple input multiple output (MIMO) antenna technology.

MIMO is unquestionably the biggest development for 802.11n and the key to the new speeds. Essentially, MIMO uses multiplexing to increase the range and speed of wireless networking. Multiplexing is a technique that combines multiple signals for transmission over a single line or medium. MIMO enables the transmission of multiple data streams traveling on different antennas in the same channel at the same time. A receiver reconstructs the streams, which have multiple antennas as well. By using multiple paths, MIMO provides a significant capacity gain over conventional single-antenna systems, along with more reliable communication.

In addition to all these improvements, 802.11n allows channel bonding that essentially doubles the data rate again. What is channel bonding? The 802.11b and 802.11g wireless standards use a single channel to send and receive information. With channel bonding, you can use two channels at the same time. As you might guess, the ability to use two channels at once increases performance. It is expected that bonding will help increase wireless transmission rates from the 54Mbps offered with the 802.11g standards to a theoretical maximum of 600Mbps. 802.11n uses the OFDM transmission strategy.

NOTE
Channel surfing In wireless networking a single channel is 20MHz in width. When two channels are bonded, they are a total of 40MHz. 802.11n systems can use either the 20MHz channels or the 40MHz channel.
Summary of 802.11 Wireless Standards

Table 7.5 highlights the characteristics of the various 802.11 wireless standards.

<table>
<thead>
<tr>
<th>IEEE Standard</th>
<th>Frequency/Medium</th>
<th>Speed</th>
<th>Topology</th>
<th>Transmission Range</th>
<th>Access Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.11</td>
<td>2.4GHz RF</td>
<td>1 to 2Mbps</td>
<td>Ad hoc/ infrastructure</td>
<td>20 feet indoors.</td>
<td>CSMA/CA</td>
</tr>
<tr>
<td>802.11a</td>
<td>5GHz</td>
<td>Up to 54Mbps</td>
<td>Ad hoc/ infrastructure</td>
<td>25 to 75 feet indoors; range can be affected by building materials.</td>
<td>CSMA/CA</td>
</tr>
<tr>
<td>802.11b</td>
<td>2.4GHz</td>
<td>Up to 11Mbps</td>
<td>Ad hoc/ infrastructure</td>
<td>Up to 150 feet indoors; range can be affected by building materials.</td>
<td>CSMA/CA</td>
</tr>
<tr>
<td>802.11g</td>
<td>2.4GHz</td>
<td>Up to 54Mbps</td>
<td>Ad hoc/ infrastructure</td>
<td>Up to 150 feet indoors; range can be affected by building materials.</td>
<td>CSMA/CA</td>
</tr>
<tr>
<td>802.11n</td>
<td>2.4GHz/5GHz</td>
<td>Up to 600Mbps</td>
<td>Ad hoc/ infrastructure</td>
<td>175+ feet indoors; range can be affected by building materials.</td>
<td>CSMA/CA</td>
</tr>
</tbody>
</table>

FHSS, DSSS, OFDM, and 802.11 Standards

The original 802.11 standard had two variations, both offering the same speeds but differing in the RF spread spectrum used. One of the 802.11 standards used FHSS. This 802.11 variant used the 2.4GHz radio frequency band and operated at a 1 or 2Mbps data rate. Since this original standard, wireless implementations have favored DSSS.

The second 802.11 variation used DSSS and specified a 2Mbps peak data rate with optional fallback to 1Mbps in very noisy environments. 802.11, 802.11b, and 802.11g use DSSS. This means that the underlying modulation scheme is
similar between each standard, allowing all DSSS systems to coexist with 2, 11, and 54Mbps 802.11 standards. As a comparison, it is like the migration from the older 10Mbps Ethernet networking to the more commonly implemented 100Mbps standard. The speed was different, but the underlying technologies were similar, allowing for an easier upgrade.

Table 7.6 compares wireless standards and the spread spectrum used.

<table>
<thead>
<tr>
<th>IEEE Standard</th>
<th>RF Used</th>
<th>Spread Spectrum</th>
<th>Data Rate (in Mbps)</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.11</td>
<td>2.4GHz</td>
<td>DSSS</td>
<td>1 or 2</td>
</tr>
<tr>
<td>802.11</td>
<td>2.4GHz</td>
<td>FHSS</td>
<td>1 or 2</td>
</tr>
<tr>
<td>802.11a</td>
<td>5GHz</td>
<td>OFDM</td>
<td>54</td>
</tr>
<tr>
<td>802.11b</td>
<td>2.4GHz</td>
<td>DSSS</td>
<td>11</td>
</tr>
<tr>
<td>802.11g</td>
<td>2.4GHz</td>
<td>DSSS</td>
<td>54</td>
</tr>
<tr>
<td>802.11n</td>
<td>2.4/5GHz</td>
<td>OFDM</td>
<td>600 (theoretical)</td>
</tr>
</tbody>
</table>

Securing Wireless Networks

Many different strategies and protocols are used to secure LAN and WAN transmissions. What about network transmissions that travel over the airwaves?

In the last few years, wireless networking has changed the look of modern networks, bringing with it an unparalleled level of mobility and a host of new security concerns.

Wireless LANs (WLANs) require new protocols and standards to handle security for radio communications. As it stands today, wireless communications represent a significant security concern. You should be aware of a few wireless security standards when working with wireless, including Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), and 802.1X.

Wired Equivalent Privacy (WEP)

Wired equivalent privacy (WEP) was the first attempt to keep wireless networks safe. WEP was designed to be easy to configure and implement. Originally it was hoped that WEP would provide the same level of security to wireless networks as was available to wired. For a time it was the best and only option for securing wireless networks.
WEP is an IEEE standard introduced in 1997, designed to secure 802.11 networks. With WEP enabled, each data packet transmitted over the wireless connection would be encrypted. Originally, the data packet was combined with a secret 40-bit number key as it passed through an encryption algorithm known as RC4. The packet was scrambled and sent across the airwaves. On the receiving end, the data packet passed through the RC4 backward, and the host received the data as it was intended. WEP originally used a 40-bit number key, but later it specified 128-bit encryption, making WEP that much more robust.

WEP is a protocol designed to provide security by encrypting data from the sending and receiving devices. In a short period of time, however, it was discovered that WEP encryption was not nearly as secure as hoped. Part of the problem was that when the 802.11 standards were being written, security was not the major concern it is today. As a result, WEP security was easy to crack with freely available hacking tools. From this point, wireless communication was regarded as a potentially insecure transmission medium.

The two types of WEP security are static and dynamic. Dynamic and static WEP differ in that dynamic WEP changes security keys periodically, making it more secure. Static WEP uses the same security key on an ongoing basis. The primary security risks are associated with static WEP, which uses a shared password to protect communications. Security weaknesses discovered in static WEP mean that WLANs protected by it are vulnerable to several types of threats. Freely available hacking tools make breaking into static WEP-protected wireless networks a trivial task. Unsecured WLANs are obviously exposed to these same threats as well; the difference is that less expertise, time, and resources are required to carry out the attacks.

**Wi-Fi Protected Access (WPA)**

Security weaknesses associated with WEP gave administrators a valid reason to be concerned about wireless security. The need for increased wireless security was important for wireless networking to reach its potential and to reassure those who had sensitive data that it was safe to use wireless communications. In response, Wi-Fi Protected Access (WPA) was created. WPA was designed to improve on the security weaknesses of WEP and to be backward-compatible with older devices that used the WEP standard. WPA addressed two main security concerns:

- **Enhanced data encryption**: WPA uses a temporal key integrity protocol (TKIP), which scrambles encryption keys using a hashing algorithm. Then the keys are issued an integrity check to verify that they have not been modified or tampered with during transit.
Authentication: Using Extensible Authentication Protocol (EAP), WEP regulates access to a wireless network based on a computer’s hardware-specific MAC address, which is relatively simple to be sniffed and stolen. EAP is built on a more secure public-key encryption system to ensure that only authorized network users can access the network.

802.1X

802.1X is an IEEE standard specifying port-based network access control. 802.1X was not specifically designed for wireless networks; rather, it provides authenticated access for both wired and wireless networks. Port-based network access control uses the physical characteristics of a switched local area network (LAN) infrastructure to authenticate devices attached to a LAN port and to prevent access to that port in cases where the authentication process fails. The 802.1X framework has three main components:

- **Supplicant**: The system or node requesting access and authentication to a network resource.
- **Authenticator**: A control mechanism that allows or denies traffic that wants to pass through a port.
- **Authentication server**: Validates the credentials of the supplicant that is trying to access the network or resource.

During a port-based network access control interaction, a LAN port adopts one of two roles: authenticator or supplicant. In the role of authenticator, a LAN port enforces authentication before it allows user access to the services that can be accessed through that port. In the role of supplicant, a LAN port requests access to the services that can be accessed through the authenticator’s port. An authentication server, which can be either a separate entity or colocated with the authenticator, checks the supplicant’s credentials on behalf of the authenticator. The authentication server then responds to the authenticator, indicating whether the supplicant is authorized to access the authenticator’s services.

The authenticator’s port-based network access control defines two logical access points to the LAN through one physical LAN port. The first logical access point, the *uncontrolled port*, allows data exchange between the authenticator and other computers on the LAN, regardless of the computer’s authorization state. The second logical access point, the *controlled port*, allows data exchange between an authenticated LAN user and the authenticator.
In a wireless network environment, the supplicant typically is a network host. The authenticator could be the wireless network switch or AP. The role of authentication server would be played by a Remote Authentication Dial-In User Service (RADIUS).

RADIUS is a protocol that allows a single server to become responsible for all remote-access authentication, authorization, and auditing (or accounting) services. RADIUS functions as a client/server system. The remote user dials in to the remote access server, which acts as a RADIUS client, or network access server (NAS), and connects to a RADIUS server. The RADIUS server performs authentication, authorization, and auditing (or accounting) functions and returns the information to the RADIUS client (which is a remote-access server running RADIUS client software). The connection is either established or rejected based on the information received.

**Temporal Key Integrity Protocol**

As mentioned previously, WEP lacked security. Temporal Key Integrity Protocol (TKIP) was designed to address the shortcomings of the WEP security protocol. TKIP is an encryption protocol defined in IEEE 802.11i. TKIP was designed not only to increase security but also to use existing hardware, making it easy to upgrade to TKIP encryption.

TKIP is built on the original WEP security standard but enhances it by “wrapping” additional code at both the end and the beginning of the data packet. This code modifies the code for additional security. Because TKIP is based on WEP, it too uses the RC4 stream encryption method. But unlike WEP, TKIP encrypts each data packet with a stronger encryption key than is available with regular WEP.

TKIP provides increased security for data communications, but it is far from the final solution. TKIP provides strong encryption for home users and nonsensitive data. However, it may not provide the level of security necessary to protect corporate or more sensitive data while in transmission.

**Establishing Communications Between Wireless Devices**

When you work with wireless networks, it is important to have a basic understanding of the communication that occurs between wireless devices. If you’re using an infrastructure wireless network design, the network has two key
parts—the wireless client, also known as the station (STA), and the AP. The AP acts as a bridge between the STA and the wired network.

As with other forms of network communication, before transmissions between devices can occur, the wireless access point and the client must begin to talk to each other. In the wireless world, this is a two-step process involving association and authentication.

The association process occurs when a wireless adapter is turned on. The client adapter immediately begins scanning the wireless frequencies for wireless APs or, if using ad hoc mode, other wireless devices. When the wireless client is configured to operate in infrastructure mode, the user can choose a wireless AP with which to connect. This process may also be automatic, with the AP selection based on the SSID, signal strength, and frame error rate. Finally, the wireless adapter switches to the assigned channel of the selected wireless AP and negotiates the use of a port.

If at any point the signal between the devices drops below an acceptable level, or if the signal becomes unavailable for any reason, the wireless adapter initiates another scan, looking for an AP with stronger signals. When the new AP is located, the wireless adapter selects it and associates with it. This is known as reassociation.

Roaming The 802.11 standards allow a wireless client to roam between multiple APs. An AP transmits a beacon signal every so many milliseconds. It includes a time stamp for client synchronization and an indication of supported data rates. A client system uses the beacon message to identify the strength of the existing connection to an AP. If the connection is too weak, the roaming client attempts to associate itself with a new AP. This allows the client system to roam between distances and APs.
With the association process complete, the authentication process begins. After the devices associate, keyed security measures are applied before communication can take place. On many APs, authentication can be set to either shared key authentication or open authentication. The default setting typically is open authentication. Open authentication enables access with only the SSID and/or the correct WEP key for the AP. The problem with open authentication is that if you don’t have other protection or authentication mechanisms in place, your wireless network is totally open to intruders. When set to shared key mode, the client must meet security requirements before communication with the AP can occur.

After security requirements are met, you have established IP-level communication. This means that wireless standard requirements have been met, and Ethernet networking takes over. There is basically a switch between 802.11 to 802.3 standards. The wireless standards create the physical link to the network, allowing regular networking standards and protocols to use the link. This is how the physical cable is replaced, but to the networking technologies there is no difference between regular cable media and wireless media.

Several components combine to enable wireless communications between devices. Each of these must be configured on both the client and the AP:

- **Service Set Identifier (SSID):** Whether your wireless network is using infrastructure mode or ad hoc mode, an SSID is required. The SSID is a configurable client identification that allows clients to communicate with a particular base station. Only client systems configured with the same SSID as the AP can communicate with it. SSIDs provide a simple password arrangement between base stations and clients in a BSS network. ESSIDs are used for the ESS wireless network.

- **Wireless channel:** RF channels are an important part of wireless communications. A *channel* is the frequency band used for the wireless communication. Each standard specifies the channels that can be used. The 802.11a standard specifies radio frequency ranges between 5.15 and 5.875GHz. In contrast, the 802.11b and 802.11g standards operate in the 2.4 to 2.497GHz ranges. Fourteen channels are defined in the IEEE 802.11b/g channel set, 11 of which are available in North America.

- **Security features:** IEEE 802.11 provides security using two methods, authentication and encryption. Authentication verifies the client system. In infrastructure mode, authentication is established between an AP and each station. Wireless encryption services must be the same on the client and the AP for communication to occur.
Now that we have reviewed key wireless settings, let's take a look at an actual wireless connection configuration.

As shown in Figure 7.1, the settings for this wireless router are clearly laid out. For instance, you can see that the wireless connection uses an SSID password of Gigaset602 and wireless channel 11.

![FIGURE 7.1 Wireless configuration information.]
As shown in Figure 7.1, you can adjust many settings for troubleshooting or security reasons. Here are some of the settings that can be adjusted on a wireless access point:

- **SSID**: Figure 7.1 shows the SSID of Gigaset602. This name is used for anyone who wants to access the Internet through this wireless access point. The SSID is a configurable client identification that allows clients to communicate with a particular base station. In application, only clients configured with the same SSID can communicate with base stations having the same SSID. SSID provides a simple password arrangement between base stations and clients.

  As far as troubleshooting is concerned, if a client cannot access a base station, make sure that both are using the same SSID. Incompatible SSIDs are sometimes found when clients move computers, such as laptops, between different wireless networks. They obtain an SSID from one network. If the system is not rebooted, the old SSID doesn’t allow communication with a different base station.

- **Channel**: The channel in Figure 7.1 is set to use channel 11. To access this network, all systems must use this channel. If needed, you can change the channel using the drop-down menu. The menu lists channels 1 through 11.

- **SSID Broadcast**: In their default configuration, wireless access points typically broadcast the SSID name into the air at regular intervals. This feature is intended to allow clients to easily discover the network and roam between WLANs. The problem with SSID broadcasting is that it makes it a little easier to get around security. SSIDs are not encrypted or protected in any way. Anyone can snoop and get a look at the SSID and attempt to join the network.

  **NOTE**

  There’s no place like roam  For home and small office use, roaming is not really needed. This feature can be disabled for home use to improve the security of your WLAN. As soon as your wireless clients are manually configured with the right SSID, they no longer require these broadcast messages.

- **Authentication**: When configuring authentication security for the AP, you have several options, including WEP-Open, WEP-Shared, and WPA-psk. WEP-Open is the simplest of the authentications methods because it does not perform any type of client verification. It is a very weak form of authentication, because it requires no proof of identity.
WEP-Shared requires that a WEP key be configured on both the client system and the access point. This makes authentication with WEP-Shared mandatory, so it is more secure for wireless transmission. WPA-psk (Wi-Fi Protected Access with Pre-Shared Key) is a stronger form of encryption in which keys are automatically changed and authenticated between devices after a specified period of time, or after a specified number of packets have been transmitted.

- **Wireless Mode**: To access the network, the client must use the same wireless mode as the AP. Today most users configure the network for 802.11g for faster speeds or a combination of 802.11b/g because these wireless standards are compatible.

- **DTIM Period (seconds)**: Wireless transmissions can broadcast to all systems—that is, they can send messages to all clients on the wireless network. Multiple broadcast messages are known as multicast or broadcast traffic. Delivery Traffic Indication Message (DTIM) is a feature used to ensure that when the multicast or broadcast traffic is sent, all systems are awake to hear the message. The DTIM setting specifies how often the DTIM is sent within the beacon frame. For example, if the DTIM setting by default is 1, this means that the DTIM is sent with every beacon. If the DTIM is set to 3, the DTIM is sent every three beacons as a DTIM wake-up call.

- **Maximum Connection Rate**: The transfer rate typically is set to Auto by default. This allows the maximum connection speed. However, it is possible to decrease the speed to increase the distance that the signal travels and boost signal strength due to poor environmental conditions.

- **Network Type**: This is where the network can be set to use the ad hoc or infrastructure network design.

### Access Point Coverage

Like any other network medium, APs have a limited transmission distance. This limitation is an important consideration when you’re deciding where an AP should be placed on the network. When troubleshooting a wireless network, pay close attention to how far the client systems are from the AP.

When faced with a problem in which client systems cannot consistently access the AP, you could try moving the access point to better cover the area, but then you may disrupt access for users in other areas. So what can be done to troubleshoot AP coverage?
Depending on the network environment, the quick solution may be to throw money at the problem and purchase another access point, cabling, and other hardware to expand the transmission area. However, you can try a few things before installing another wireless access point. The following list starts with the least expensive solution and progresses to the most expensive:

- **Increase transmission power**: Some access points have a setting to adjust the transmission power output. By default, most of these settings are set to the maximum output; however, this is worth verifying just in case. Also note that you can decrease the transmission power if you’re trying to reduce the dispersion of radio waves beyond the immediate network. Increasing the power gives clients stronger data signals and greater transmission distances.

- **Relocate the AP**: When wireless client systems suffer from connectivity problems, the solution may be as simple as relocating the AP. You could relocate it across the room, a few feet away, or across the hall. Finding the right location will likely take a little trial and error.

- **Adjust or replace antennas**: If the access point distance is insufficient for some network clients, it might be necessary to replace the default antenna used with both the AP and the client with higher-end antennas. Upgrading an antenna can make a big difference in terms of transmission range. Unfortunately, not all APs have replaceable antennas.

- **Signal amplification**: RF amplifiers add significant distance to wireless signals. An RF amplifier increases the strength and readability of the data transmission. The amplifier improves both the received and transmitted signals, resulting in an increase in wireless network performance.

- **Use a repeater**: Before installing a new AP, you might want to think about a wireless repeater. When set to the same channel as the AP, the repeater takes the transmission and repeats it. So, the AP transmission gets to the repeater, and then the repeater duplicates the signal and passes it on. This is an effective strategy to increase wireless transmission distances.

**EXAM ALERT**

For the Network+ exam, be prepared to answer questions on access point coverage and possible reasons to relocate APs.
Wireless Signal Quality

Because wireless signals travel through the atmosphere, they are subjected to all sorts of environmental and external factors. This includes storms and the number of walls, ceilings, and so on that the signal must pass through. Just how weakened the signal becomes depends on the building material used and the level of RF interference. All these elements decrease the power of the wireless signal.

EXAM ALERT

Signal strength Wireless signals degrade depending on the construction material used. Signals passing through concrete and steel are particularly weakened.

If you are troubleshooting a wireless connection that has a particularly weak signal, you can do a few things to help increase the signal's power:

- **Antenna**: Perhaps the first and most obvious thing to do is to make sure that the antenna on the AP is positioned for best reception. It often takes a little trial and error to get the placement right. Today's wireless access cards commonly ship with diagnostic software that displays signal strength and makes it easy to find the correct position.

- **Device placement**: One factor that can degrade wireless signals is RF interference. Because of this, it is important to try to keep wireless devices away from appliances that output RF noise. This includes microwaves, electrical devices, and certain cordless devices using the same frequency, such as phones.

- **Network location**: Although there may be limited choice, as much as possible it is important to try to reduce the number of obstructions that the signal must pass through. Every obstacle strips a little more power from the signal. The type of material a signal must pass through also can have a significant impact on signal integrity.

- **Boost the signal**: If all else fails, you can purchase devices, such as wireless repeaters, that can amplify the wireless signal. The device takes the signal and amplifies it to make it stronger. This also increases the distance that the client system can be placed from the AP.

To successfully manage wireless signals, you need to know which wireless standard you are using. The standards used today specify range distances, RF ranges, and speeds. It may be that the wireless standard cannot do what you need it to.
Wireless Troubleshooting Checklist

Poor communication between wireless devices has many different potential causes. The following is a review checklist of wireless troubleshooting:

- **Auto transfer rate**: By default, wireless devices are configured to use the strongest, fastest signal. If you’re experiencing connectivity problems between wireless devices, try using the lower transfer rate in a fixed mode to achieve a more stable connection. For example, you can manually choose the wireless transfer rate. Also, instead of using 11Mbps, the highest rate for 802.11b, try 5.5Mbps, 2Mbps, or 1Mbps. The higher the transfer rate, the shorter the connection distance.

- **Router placement**: If signal strength is low, try moving the access point to a new location. Moving it just a few feet can make a difference.

- **Antenna**: The default antenna shipped with wireless devices may not be powerful enough for a particular client system. Better-quality antennas can be purchased for some APs, which will boost the distance the signal can go.

- **Building obstructions**: Wireless RF communications are weakened if they have to travel through obstructions such as metal and concrete.

- **Conflicting devices**: Any device that uses the same frequency range as the wireless device can cause interference. For example, 2.4GHz phones can cause interference with devices using the 802.11g standard.

- **Wireless channels**: If connections are inconsistent, try changing the channel to another, nonoverlapping channel.

- **Protocol issues**: If an IP address is not assigned to the wireless client, an incorrect SSID or incorrect WEP settings can prevent a system from obtaining IP information.
SSID: The SSID number used on the client system must match the one used on the AP. Typically, the default SSID assigned is sufficient, but you might need to change it if you're switching a laptop between different WLANs.

WEP: If WEP is enabled, the encryption type must match what is set in the AP.

Infrared Wireless Networking

Infrared has been around for a long time; perhaps our first experience with it was the TV remote. The commands entered onto the remote control travel over an infrared light wave to the receiver on the TV. Infrared technology has progressed, and today infrared development in networking is managed by the Infrared Data Association (IrDA).

Infrared wireless networking uses infrared beams to send data transmissions between devices. Infrared wireless networking offers higher transmission rates, reaching 10Mbps to 16Mbps.

As expected, infrared light beams cannot penetrate objects; therefore, the signal is disrupted when something blocks the light. Infrared can be either a directed (line-of-sight) or diffuse technology. A directed infrared system provides a limited range of approximately 3 feet and typically is used for personal area networks. Diffused infrared can travel farther and is more difficult to block with a signal object. Diffused infrared wireless LAN systems do not require line of sight, but usable distance is limited to room distances.

Infrared provides a secure, low-cost, convenient cable-replacement technology. It is well suited for many specific applications and environments. Some key infrared points are as follows:

- It provides adequate speeds—up to 16Mbps.
- Infrared devices use less power and therefore don’t drain batteries as much.
- Infrared is a secure medium. Infrared signals typically are a direct-line implementation in a short range and therefore do not travel far outside the immediate connection. This eliminates the problem of eavesdropping or signal tampering.
Infrared is a proven technology. Infrared devices have been available for some time and as such are a proven, nonproprietary technology with an established user and support base.

- It has no radio frequency interference issues or signal conflicts.
- It replaces cables for many devices, such as keyboards, mice, and other peripherals.
- It uses a dispersed mode or a direct line-of-sight transmission.
- Transmissions travel over short distances.

**Bluetooth**

Bluetooth is a wireless standard used for many purposes, including connecting peripheral devices to a system. Bluetooth uses a low-cost, short-range radio link that replaces many of the cords used to connect devices.

Bluetooth is an easily configured technology. When Bluetooth-enabled devices are within 10 or so meters of each other, they can establish a connection. Bluetooth establishes the link using an RF-based link and therefore does not require a direct line-of-sight connection. The Bluetooth Standard defines a short RF link that is capable of voice or data transmission up to a maximum capacity of 720Kbps per channel.

Bluetooth operates at 2.4 to 2.48GHz and uses an FHSS technology. The signal can hop between 79 frequencies at 1MHz intervals to give a high degree of interference immunity.

As an established technology, Bluetooth has many advantages, but the speed of 720Kbps is limiting. The newest version of Bluetooth, Bluetooth 2.0, increases overall speed to a data rate of 3Mbps. This speed may still be significantly slower than 802.11b or 802.11g, but for an easily configured cable replacement technology, it is an attractive option. Table 7.7 highlights the advantages of the Bluetooth standard.
Table 7.7 Bluetooth Characteristics

<table>
<thead>
<tr>
<th>Characteristic</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specification</td>
<td>Bluetooth</td>
</tr>
<tr>
<td>Topology</td>
<td>Ad hoc</td>
</tr>
<tr>
<td>Spread spectrum</td>
<td>FHSS</td>
</tr>
<tr>
<td>Medium</td>
<td>2.4GHz RF</td>
</tr>
<tr>
<td>Speed</td>
<td>720Kbps</td>
</tr>
<tr>
<td>Range</td>
<td>10 meters in optimal conditions</td>
</tr>
</tbody>
</table>

Review and Test Yourself

The following sections provide you with the opportunity to review what you've learned in this chapter and to test yourself.

The Facts

- A wireless access point (AP) is both a transmitter and receiver (transceiver) device used for wireless LAN (WLAN) radio signals.
- A wireless channel is the band of RF used for wireless communication.
- Many different strategies and protocols are used to secure wireless transmissions, including Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), and 802.1X.
- The 802.11 wireless standards can differ in terms of speed, transmission ranges, and frequency used.
- 802.11 wireless standards use the CSMA/CA access method.
Key Terms

- Ad hoc
- AP
- Authentication
- Beaconing
- BSSID
- Channel
- ESS
- ESSID
- Infrastructure
- RADIUS
- SSID
- TKIP
- Topology
- WEP
- WPA
Exam Prep Questions

1. Which of the following wireless protocols operate at 2.4GHz? (Select two.)
   - A. 802.11a
   - B. 802.11b
   - C. 802.11g
   - D. 802.11t

2. Under what circumstance would you change the default channel on an access point?
   - A. When channel overlap occurs between access points
   - B. To release and renew the SSID
   - C. To increase WEP security settings
   - D. To decrease WEP security settings

3. A client on your network has had no problems accessing the wireless network in the past, but recently she moved to a new office. Since the move she has been unable to access the network. Which of the following is most likely the cause of the problem?
   - A. The SSIDs on the client and the AP are different.
   - B. The SSID has been erased.
   - C. The client has incorrect WEP settings.
   - D. The client system has moved too far from the access point.

4. You configure a wireless connection using the Bluetooth standard. At what speed does Bluetooth operate?
   - A. 350Mbps
   - B. 720Kbps
   - C. 200Kbps
   - D. 11Mbps
5. You purchase a new wireless access point that uses no WEP security by default. You change the security settings to use 128-bit encryption. How must the client systems be configured?
   □ A. All client systems must be set to 128-bit encryption.
   □ B. The client system inherits security settings from the AP.
   □ C. WEP does not support 128-bit encryption.
   □ D. The client WEP settings have to be set to autodetect.

6. You are asked to configure the security settings for a new wireless network. You want the setting that offers the greatest level of security. Which of the following would you choose?
   □ A. WEP-Open
   □ B. WEP-Closed
   □ C. WEP-Shared
   □ D. WEP-Unshared

7. Which of the following best describes 802.1X?
   □ A. A port-based access control
   □ B. A wireless standard specifying 11Mbps data transfer
   □ C. A wireless standard specifying 54Mbps data transfer
   □ D. An integrity-based access control

8. You are installing a wireless network solution, and you require a standard that can operate using either 2.4GHz or 5GHz frequencies. Which of the following standards would you choose?
   □ A. 802.11a
   □ B. 802.11b
   □ C. 802.11g
   □ D. 802.11n
9. You are installing a wireless network solution that uses a feature known as MIMO. Which wireless networking standard are you using?

- A. 802.11a
- B. 802.11b
- C. 802.11g
- D. 802.11n

10. In the 802.1X security framework, which of the following best describes the role of the supplicant?

- A. Authenticating usernames and passwords
- B. Encrypting usernames and passwords
- C. The system or node requesting access and authentication to a network resource
- D. A control mechanism that allows or denies traffic that wants to pass through a port

Answers to Exam Prep Questions

1. B, C. Wireless standards specify an RF range on which communications are sent. The 802.11b and 802.11g standards use the 2.4GHz range. 802.11a uses the 5GHz range. 802.11t is not a valid standard. For more information, see the section “802.11 Wireless Standards.”

2. A. Ordinarily the default channel used with a wireless device is adequate; however, you might need to change the channel if overlap occurs with another nearby access point. The channel should be changed to another, nonoverlapping channel. Changing the channel would not impact the WEP security settings. For more information, see the section “Wireless Radio Channels.”

3. D. An AP has a limited distance that it can send data transmissions. When a client system moves out of range, it can’t access the AP. Many strategies exist to increase transmission distances, including RF repeaters, amplifiers, and buying more powerful antennas. The problem is not likely related to the SSID or WEP settings, because the client had access to the network before, and no settings were changed. For more information, see the section “Wireless Troubleshooting Checklist.”

4. B. Bluetooth is a wireless standard commonly used to interconnect peripheral devices to the computer system. Bluetooth operates at 720Kbps. For more information, see the section “Bluetooth.”
Chapter 7: Wireless Networking

5. A. On a wireless connection between an access point and the client, each system must be configured to use the same WEP security settings. In this case, they must both be configured to use 128-bit encryption. For more information, see the section “Wireless Troubleshooting Checklist.”

6. C. Both WEP-Open and WEP-Shared are forms of wireless security. WEP-Open is the simpler of the two authentication methods because it does not perform any type of client verification. It is a very weak form of authentication, because no proof of identity is required. WEP-Shared requires that a WEP key be configured on both the client system and the access point. This makes authentication with WEP-Shared mandatory and therefore more secure for wireless transmission.

7. A. 802.1X is an IEEE standard specifying port-based network access control. Port-based network access control uses the physical characteristics of a switched local area network (LAN) infrastructure to authenticate devices attached to a LAN port and to prevent access to that port in cases where the authentication process fails. For more information, see the section “802.1X.”

8. D. The IEEE standard 802.11n can use either the 2.4GHz or 5GHz radio frequencies. 802.11a uses 5GHz, and 802.11b and 802.11g use 2.4GHz. For more information, see the section “802.11 Wireless Standards.”

9. D. MIMO is used by the 802.11n standard and takes advantage of multiplexing to increase the range and speed of wireless networking. Multiplexing is a technique that combines multiple signals for transmission over a single line or medium. MIMO enables the transmission of multiple data streams traveling on different antennas in the same channel at the same time. A receiver reconstructs the streams, which have multiple antennas. For more information, see the section “The Magic Behind 802.11n.”

10. C. The 802.1X security framework has three main components. The supplicant is the system or node requesting access and authentication to a network resource. The authenticator usually is a switch or AP that acts as a control mechanism, allowing or denying traffic that wants to pass through a port. Finally, the authentication server validates the credentials of the supplicant that is trying to access the network or resource. For more information, see the section “802.1X.”

Need to Know More?


Index

NUMBERS

10BaseFL standard, 82
10BaseT standard, 81
10Gbe Ethernet standards, 86
  10GBaseER/EW standard, 87
  10GBaseLR/LW standard, 87
  10GBaseLX4 standard, 88
  10GBaseSR/SQW standard, 86
  10GBaseT standard, 88
80/20 rule (bridges), 101
100BaseFX standard, 83
100BaseT4 standard, 83
100BaseTX standard, 83
100BaseX standard, 83
568A telecommunications standard, 63-64
568B telecommunications standard, 63-64
802.11 wireless standard, 260-263
  802.11a wireless standard, 252-254, 260-263
  802.11b wireless standard, 252-253, 260-263
  802.11g wireless standard, 252-253, 260-263
  802.11n wireless standard, 260-263
  802.11x wireless standard, 265
  802.1q standard, 21
  802.2 (LLC) standard, 76
  802.3 Ethernet standards
    10BaseFL standard, 82
    10BaseT standard, 81
    Fast Ethernet standards, 82
      100BaseFX standard, 83
      100BaseT4 standard, 83
      100BaseTX standard, 83
      100BaseVG-AnyLAN standard, 84
    comparison chart, 84
    repeaters, 83
  Gigabit Ethernet standards
    10Gbe standards, 86-88
    1000BaseT standard, 85
    1000BaseX standard, 84-85

1000BaseT standard, 85
1000BaseX standard, 84-85

A

AAA (authentication, authorization, accounting). See individual entries
  access control
    access masks, 355
    ACL, 355
    DAC, 354-355
    MAC (mandatory access control), 354
    MAC address filtering, 356-357
    RBAC, 355
    RoBAC, 356
  server room security
    biometric systems, 380-381
    lock and key, 379
    PIN pads, 380
    swipe cards, 380
    TCP/IP filtering, 357
  access masks, 355
  access methods, IEEE standards
    CSMA/CA, 78-79
    CSMA/CD, 77-78
  topologies, 79

accounting, 368

ACL (access control lists), DAC, 355
  action plan implementation (troubleshooting steps/procedures), 448-449
  active hubs, 97
  active scanning, AP discovery, 259
  activity lights (network interfaces), 104
  ad hoc wireless topologies, 32
  adapters, 295
  address classes (IPv4), 180-182
  administrator training, network documentation’s help in, 399
  ADSL (Asymmetric Digital Subscriber Lines), 227
  affected area identification (troubleshooting steps/procedures), 446
  aggregated links, 295
  alarms, smart jacks, 73
  answers (practice exams)
    exam 1, 499-514
    exam 2, 549-552
  antennas
    MIMO technology, 261
antennas

wireless antennas, 249
directional antennas, 251
gain values, 250
isotropic antennas, 250
omnidirectional antennas, 250-251
polarization, 252
wireless networks
amplifying data signal strength, 273
coverage, 250-252
ratings, 250
troubleshooting, 272-274
antivirus software, 388
anycast IPv6 addresses, 190
AP (access points), 31
active scanning, 259
BSS, 267
coverage of, troubleshooting, 271-272
ESS, 267
IBSS, 267
open authentication, 268
repeaters, 272
rogue AP, 388
shared key authentication, 268
WAP, 107-108, 247, 267
active scanning, 259
beacons, 258-259
BSS, 249
BSSID, 249
ESS, 248
ESSID, 249
OSI reference model maps, 140
passive scanning, 259
repeaters, 272
SSID, 248
troubleshooting, 271-272, 456
APIDS (Application Protocol-Based Intrusion Detection System), 362
APIPA (Automatic Private IP Addressing), 194
application layer (OSI reference model), 138-139, 349-350
applications, documenting, 400, 424
ARP (Address Resolution Protocol), 191-192, 317
ping utility, 319
switches list table, 318
association (wireless network communications), 267
asymmetric key cryptography, 372-373
ATM (Asynchronous Transfer Mode), 224
troubleshooting, 47
coaxial cable, 52
coverage, 250-252
troubleshooting, 272-274
troubleshooting, 454
attenuation (data signals), 112
auditing, 368
authentication, 366-368
CHAP, 378
EAP, 265
Kerberos, 371-372
MS-CHAP, 377
MS-CHAP v2, 377
open authentication, 268
PAP, 378
passwords, 369-370
PKI
CA, 373
components of, 373
CRL, 373
digital signatures, 375
e-mail, 375
private key encryption, 374
public key encryption, 374
uses for, 375
ports, 126
PPTP, 359
RADIUS, 376
shared key, 268
SNMPv3, 164
strong passwords, 370
wireless network connections, 267, 270-271
WPA, 265
authenticators (LAN ports), 265
authorization, 367-368
auto transfer rates, troubleshooting wireless networks, 274
back door attacks, 387
backbone cable. See vertical (backbone) cable
backoff periods, 78
backups, 287
  differential backups, 298
  full backups, 297
  incremental backups, 299
  new tapes, 301
  offsite storage, 300-301
  procedures for, 410
  strategy comparison table, 299-300
  tape rotation backups, 300-301
  verifying, 301
bandwidth, 48, 76
  dedicated local bandwidth, 230
  firewalls, managing via, 347
  shapers, 117, 123
  shared bandwidth, 230
baseband transmissions, 46, 80
  baselines (performance), documenting, 407-408
  beacons (wireless networks), 258-259
  BGP (Border Gateway Protocol), 203
  binary command, 145
  biometric security systems, server room security, 380-381
  blackouts, 296
  Bluetooth, 276-277
  BNC (British Naval connectors), 56, 427
  BOOTP, 194
  BPDU (bridge protocol data units), STP and, 125
  BRI (Basic Rate Interface) standard, 217-218
  bridges, 100, 121
  80/20 rule, 101
  bridging loops, 101
  gateways, 103
  IEEE 802.1d Spanning Tree Protocol, 101
  OSI reference model maps, 140
  source route bridges, 101
  STP, 124-125
  translational bridges, 101
  transparent bridges, 101
  troubleshooting, 456
  bridging loops, 101
  broadband Internet access, 226, 232
  broadband transmissions, 46, 80-81
  broadcast IPv4 addresses, 187
  broadcast storms, troubleshooting, 470
brownouts, 297
BSA (Basic Service Areas), 249
BSS (Basic Service Sets), 248, 267
BSSID (Basic Service Set Identifiers), 249
buffering, 137
built-in network interfaces, 106
bus topologies, 28-27
  star bus topologies, 36
  troubleshooting, 467-468
buses, network card compatibility, 104
bott sets, 434

CA (Certificate Authorities), PKI, 373

cable
  coaxial cable, 48, 52-53
  crossover cable, 64-65, 82
  direct cable connections, 70
  fiber-optic cable, 48, 53-55
  horizontal cable, 67
  labeling, 431
  loopback cable, 66
  patch cable, 458
  plenum cable, 56
  punchdown tools, 428
  risers, 452
  rollover cable, 66
  screwdrivers, 427
  straight-through cable, 64
  terminators, 467
  testing, 432, 453
  troubleshooting, 451
  attenuation, 454
  crosstalk, 453-454
  EMI, 454
  FEXT, 454
  identifying characteristics, 452
  identifying where cable is used, 452
  installations, 74
  NEXT, 454
  open impedance mismatches (echoes), 454-455
  testing cable, 453
  trunking, 125
  twisted-pair cable, 48-49
  categories of, 50-51
  hubs, 96-98
cable

ScTP cable, 49
STP cable, 49-50
UTP cable, 49-50
vertical (backbone) cable, 67, 69
wire crimpers, 427
wire snips, 427
wire strippers, 427
wiring installation, 74-75
wiring termination, 74-75
cable Internet access
cable modems, 229-230
security, 232
troubleshooting, 230
cable modems, 229-231
caching, 119-120, 306-307
capturing network statistics, 408
case-sensitivity in passwords, 370
causes, establishing (troubleshooting steps/procedures), 447
cd command, 145
centralized computing network models, 18
certificate templates, PKI, 373
certificates, 376
changes, establishing (troubleshooting steps/procedures), 446
channel surfing (wireless networks), 261
CHAP (Challenge Handshake Authentication Protocol), 378
CIDR (Classless Interdomain Routing), 185
circuit switching, 216-217
circuit-level firewalls, 349-350
Citrix ICA. See ICA
cladding, 54
cleaning backup tape drives, 301
clear text, 363
client/server networks, 16-17
clients
connectivity, troubleshooting
coxial network connections, 458
duplex settings, 461
network card selection, 457
port speeds, 461
TCP/IP configuration, 458-460
twisted-pair network connections, 458
VPN, 19, 358
CNAME (Canonical Name) resource records, 159
coaxial cable, 48, 52-53
coaxial networks, client connectivity, 458
cold recovery sites, 303
cold spares, 302
cold swapping, 302
COM serial port resource assignments (modems), 108
comments
HOSTS files, 155
RFC, 142
component baselines, documenting, 408
configurations (networks)
documenting, 411
monitoring, 414
connection-oriented protocols, 140-141
connectionless protocols, 141
connectors
568A telecommunications standard, 63-64
568B telecommunications standard, 63-64
BNC connectors, 56
F-type connectors, 59
fiber connectors, 59
FireWire (IEEE 1394), 62
RJ-11 connectors, 57
RJ-45 connectors, 58
USB connectors, 62
consultants, network documentation’s help with, 399
content filtering, firewalls and, 346
content switches, 113, 122
contractors, network documentation’s help with, 399
controlled ports, 265
convergence (routers), 203
crimpers (wire), 427
CRL (Certificate Revocation Lists), 373
crossover cable, 64-66, 82, 99
crosstalk, 47
coxial cable, 52
FEXT, 454
NEXT, 454
troubleshooting, 453-454
cryptography, 372-373
CSMA/CA, IEEE standards, 78-79
CSMA/CD, IEEE standards, 77-78  
CSU/DSU (Channel Service Units/Data Service Units), 120-121  
cut-through switching environments, 98  

D  
DAC (discretionary access control), 354-355  
data availability, importance of, 285  
data encryption  
IPSec protocol, 361-362  
L2TP, 360  
presentation layer (OSI reference model), 138  
SNMPv3, 164  
WPA, 264  
data flow control, LLC network standard (802.2), 76  
data link layer, L2TP (Layer 2 Tunneling Protocol), 360  
data rate (data signals), throughput versus, 254-255  
data signals  
amplifying, smart jacks, 73  
attenuation, 47, 112  
rain fade, 237  
repeaters, 112, 121  
wireless antennas, 249  
directional antennas, 251  
gain values, 250  
isotropic antennas, 250  
omnidirectional antennas, 250-251  
polarization, 252  
wireless networks  
amplifying in, 272-274  
antenna coverage, 249-252  
antenna ratings, 250  
beacons, 258-259  
data rate versus throughput, 254-255  
interference, 255-256  
OFDM, 258  
spread spectrum technology, 257-258  
throughput versus data rate, 254-255  
data transmission rates, 48  
data-link layer (OSI reference model), 136, 139  
datagram packet switching, 215  
dB (decibels), isotropic antennas, 250  

DCE (data circuit-terminating equipment), 223  
DDNS (Dynamic Domain Name Systems), 156  
decimal-to-binary value conversion chart (IPv4 addressing), 180  
dedicated local bandwidth, 230  
default gateways, 185-186  
client connectivity, 460  
gateways versus, 104  
TCP/IP routing, 200  
TCP/IP client system configurations, 193  
demarcation points, 72-73  
demarcation extensions, 73  
Destination Host Unreachable error message (ping utility), 313  
DHCP (Dynamic Host Configuration Protocol), 164-166  
dynamic IP addressing, 192  
servers, 111-112, 122  
DHCPACK packets, 166  
DHCPDISCOVER broadcasts, 165  
DHCPFFER packets, 165  
DHCPREQUEST packets, 166  
diagnostic utilities  
ARP, 317-319  
dig, 331-332  
help facility, accessing, 308  
host, 333  
ifconfig, 329-330  
ipconfig, 327-329  
list of, 307-308  
mtr, 333  
nbtstat, switches list table, 326  
netstat  
information headings, 321  
netstat utility, 321  
nstat-a utility, 322-323  
nstat-e utility, 322  
nstat-r utility, 323-324  
nstat-s utility, 324-325  
switches list table, 320  
nnslookup, 330-331  
ping  
ARP, 319  
Destination Host Unreachable error message, 313
diagnostic utilities

- DNS, 317
- Expired TTL error message, 315
- loopback addresses, 316
- Request Timed Out error message, 314-315
- switches list table, 312
- troubleshooting example, 316
- Unknown Host error message, 315
- route, 333
- trace route
  - commands list table, 309-310
  - network congestion, 311-312

dialog modes
- full-duplex, 46, 98
- half-duplex, 46
- simplex, 46

dialup Internet access, 232-234
differential backups, 298
dig diagnostic utility, 331-332
digital signatures, PKI and, 375
dip switches, 105
direct cable connections, 70
directional antenna signal, 251
disaster recovery, 297
  - backups
    - cleaning tape drives, 301
    - labeling tapes, 301
    - new tapes, 301
    - offline storage, 300-301
    - strategy comparison table, 299-300
    - verifying, 301
    - cold-spares, 302
    - cold-swapping, 302
  - differential backups, 298
  - full backups, 297
  - hot-spares, 301
  - hot-swapping, 301
  - incremental backups, 299
  - recovery sites, 302
  - cold sites, 303
  - hot sites, 303-304
  - warm sites, 304
  - tape rotation backups, 300
  - warm-swapping, 302
disk duplexing, 290
disk mirroring, 289
disk striping with parity. See RAID 5 fault tolerance
distance-vector routing, 202-204
distributed computing network models, 18
DNS (Domain Name Systems), 154
  - CNAME resource records, 159
  - entry types, 158
  - implementing, 159
  - MX resource records, 159
  - namespaces, 156, 158
  - NS resource records, 159
  - ping utility, 317
  - servers, 116-117, 123
    - client connectivity, 460
    - TCP/IP client system configurations, 193
  - SOA resource records, 159
documentation
  - baselines (performance), 407-408
  - benefits of, 398
  - key applications, 400
  - network configurations, 411
  - network equipment, 400
  - network procedures, 400
  - network services, 400
  - network topologies, 399, 404-406
  - policies, 409
  - procedures, 410-411
  - regulations, 412
  - server configurations, 400
  - solution documentation (troubleshooting steps/procedures), 450-451
  - wiring schematics, 400-404
domain names, FQDN, 157
DoS (Denial of Service) attacks, 385-386
downtime, levels of, 285
drivers
  - network card installations, 105
  - troubleshooting DSL, 229
DSL (Digital Subscriber Lines), 226
  - ADSL, 227
  - filters, 228
  - HDSL, 227
  - ISDN DSL, 227
  - RADSL, 227
  - SDSL, 227
  - security, 232
Expired TTL (Time to Live) error message (ping utility)

- Destination Host Unreachable error message, 313
- Request Timed Out error message, 314-315
- Unknown Host error message, 315
- Escalation procedures (troubleshooting steps/procedures), 447-448, 469-470
- ESD (electrostatic discharge), network card installations, 105
- ESS (Extended Service Sets), 248, 267
- ESSID (Extended Service Set Identifiers), 249
- Ethernet
  - 10BaseFL standard, 82
  - 10BaseT standard, 81
  - baseband transmissions, 80
  - crossover cable, 65
  - Fast Ethernet standards, 82
  - 10BaseFX standard, 83
  - 10BaseT4 standard, 83
  - 10BaseTX standard, 83
  - 100BaseVG-AnyLAN standard, 84
  - comparison chart, 84
  - Repeaters, 83
  - Gigabit Ethernet standards
    - 10GbE standards, 86-88
    - 1000BaseT standard, 85
    - 1000BaseX standard, 84-85
  - IEEE 802.3 network standards, 76
  - PoE, 123-124
  - Switching loops, 469
  - switches, 98, 101

- Event logs, 422
  - Application logs, 424
  - History logs, 425
  - LM, 426
  - Security logs, 423-424
  - System logs, 425

- Exams (practice)
  - Exam 1
    - Answers, 499-514
    - Questions, 479-498
  - Exam 2
    - Answers, 549-552
    - Questions, 515-532

- Expired TTL (Time to Live) error message (ping utility), 315
F-type connectors, 59
failover configuration, standby servers, 293
failures
   hard disks, 288
   networks, costs of, 285-286
Fast Ethernet standards, 82
   100BaseFX standard, 83
   100BaseT4 standard, 83
   100BaseTX standard, 83
   100BaseVG-AnyLAN standard, 84
   100BaseX standard, 83
   comparison chart, 84
   repeaters, 83
fault detection, 414
fault tolerance, 287
   adapters, 295
   hard disks
      RAID 0, 288
      RAID 1, 289
      RAID 5, 290-291
      RAID 10, 291
      RAID comparison list, 292-293
   servers
      clustering, 294
      standby servers, 292-293
   UPS, 296-297
FDM (Frequency Division Multiplexing), 46, 81
FEXT (far-end crosstalk), troubleshooting, 454
FHSS (Frequency-Hopping Spread Spectrum), wireless networks, 257, 262
fiber connectors, 59
fiber-optic cable, 48, 53-55
filtering
   content via firewalls, 346
   DSL filtering, 228
   MAC filtering, 356-357
   TCP/IP filtering, 357
   URL via firewalls, 347
firewalls, 110, 122
   application layer firewalls, 349-350
   bandwidth management, 347
   circuit-level firewalls, 349-350
   content filtering via, 346
   functions of, 346
host-based firewalls, 350
   NAT, 346-347
network-based firewalls, 350
   packet-filtering firewalls, 348-349
private networks, 345
   session layer firewalls, See circuit-level firewalls
   signature identification via, 346
   stateful firewalls, 347
   stateless firewalls, 347
   URL filtering via, 347
   virus scanning via, 346
FireWire (IEEE 1394), network connectors, 62
flow control (OSI transport layer), 137
foreign address information heading (netstat diagnostic utility), 321
FQDN (fully qualified domain names), 157
fractional T, 219
Fraggle attacks, 386
FragmentFree-switching environments, 99
Frame Relay, 222-223
FTP (File Transfer Protocol), 144, 381
full backups, 297
full-duplex dialog mode, 46, 98

G

gain values (wireless antennas), 250
gateways, 103-104, 121
gateways (default), 185-186
client connectivity, 460
TCP/IP
   client system configurations, 193
   routing, 200
global unicast IPv6 addresses, 190
Gigabit Ethernet standards
   10GbE standards
      10GBaseER/EW standard, 87
      10GBaseLR/LW standard, 87
      10GBaseLX4 standard, 88
      10GBaseSR/SW standard, 86
      10GBaseT standard, 88
   1000BaseT standard, 85
   1000BaseX standard, 84-85
half-duplex dialog mode, 46
hard disks
failures, 288
fault tolerance
RAID 0, 288
RAID 1, 289
RAID 5, 290-291
RAID 10, 291
RAID comparison list, 292-293
HDSL (High Bit Rate Digital Subscriber Lines), 227
heartbeats, 293
help facility (diagnostic utilities), accessing, 308
HIDS (Host-Based Intrusion Detection System), 352
high-density devices, 97
history logs, 425
honeynets (security), 353
honeypots (security), 353
horizontal cable, 67
host diagnostic utility, 333
host-based firewalls, 350
HOSTS files, 155
hot recovery sites, 303-304
hot spares, 301
hot swapping, 301
hotspots, 237
HTTP (Hypertext Transfer Protocol), 147, 381
HTTPS (Hypertext Transfer Protocol Secure), 148, 381
hubs, 28, 96, 121
active hubs, 97
crossover cable, 64-65, 99
direct cable connections, 70
high-density devices, 97
MDI ports, 99
MDI-X ports, 99
OSI reference model maps, 140
passive hubs, 97
straight-through cable, 64
switches versus, 98
troubleshooting, 455
workgroup hubs, 97
hybrid network topologies, 36
Hz (hertz), RF (radio frequency) channels, 252
iANA (Internet Assigned Numbers Authority), IP addresses, 183
IBSS (Independent Basic Service Sets), 267
ICA (Independent Computing Architecture), 366
ICMP (Internet Control Message Protocol), 150, 319, 386
IDC (insulation displacement connectors), 70
IDF (Intermediate Distribution Frame) telecommunications rooms, 71
IDS (intrusion detection systems), 114, 352
IEEE (Institute of Electrical and Electronic Engineers)
100BaseT4 standard, 83
100BaseTX standard, 83
100BaseX standard, 83
802.11 wireless standard, 260-263
802.11a wireless standard, 252-254, 260-263
802.11b wireless standard, 252-253, 260-263
802.11g wireless standard, 252-253, 260-263
802.11n wireless standard, 260-263
802.11x wireless standard, 265
802.1q standard, 21
802.2 (LLC) standard, 76
802.3 Ethernet standards
10BaseFL standard, 82
10BaseT standard, 81
Fast Ethernet standards, 82-84
Gigabit Ethernet standards, 84-88
1000BaseT standard, 85
1000BaseX standard, 84-85
ifconfig diagnostic utility, 253, 329-330
IGMP (Internet Group Management Protocol), 154
IGP (Interior Gateway Protocol), 206
IMAP4 (Internet Message Access Protocol version 4), 148
impedence mismatches (echoes), troubleshooting, 454-455
incremental backups, 299
independent routing, 215
information gathering process (troubleshooting steps/procedures), 445-446
infrared wireless networks, 275
infrastructure hardware, troubleshooting, 455-456
infrastructure wireless topologies, 31
interference (wireless networks), 255-256
crosstalk, 47, 52, 453-454
EML, 47, 52
Internet
broadband access, 226
cable access, 229-230, 232
dialup access, 232-234
DSL access, 226-229, 232
MPLS, 238-239
POTS access, 232-234
PSTN access, 235
satellite access, 235-237
usage policies, 409
wireless access, 237-238
IP addressing, 142, 179
APIPA, 194
BOOTP, 194
client connectivity, 459
dynamic addresses, 192
IANA, 183
IPv4
address classes, 180
classful addresses, 187
decimal-to-binary value conversion chart, 180
default gateways, 185-186, 193
IPv6 addresses versus, 191
multicasting, 187
octets in, 180
private address ranges, 459
private networks, 183-185
public networks, 183
unicast addresses, 187
IPv6, 187
anycast addresses, 190
global unicast addresses, 190
identifying IPv6 addresses, 188-189
IPv4 addresses versus, 191
link-local addresses, 190-191
multicasting, 190
reserved addresses, 190
site-local addresses, 190
stateful configurations, 190
stateless configurations, 190
unicast addresses, 189
NAT, 196
packet-filtering firewalls, 348
scapes, 192
static addresses, 191
subnet masks, 181, 185, 193
subnetting, 182-183
TCP/IP client system configurations, 193
IP Properties dialog, 460
ipconfig diagnostic utility, 327
switches list table, 329
troubleshooting wireless networks, 253
usage examples, 328
ipconfig/all command, 460
IPS (Intrusion prevention systems), 114, 351
IPSec (IP Security) protocol, 361-362
IRQ (Interrupt Requests), network cards, 104-105
IS-IS (Intermediate System-to-Intermediate System) link-state protocol, 205
ISDN (Integrated Services Digital Networks), 217-218
ISDN DSL (Integrated Services Digital Network Digital Subscriber Lines), 227
ISO (International Standardization Organization), OSI reference model development, 134
isotropic antennas, 250
iwconfig command, troubleshooting wireless networks, 253
J - K - L
J-carrier lines, 219-220
jam signals, 78
jumpers, 105
Kerberos authentication, 371-372
L2TP (Layer 2 Tunneling Protocol), 359-360
labeling
backup tapes, 301
cable, 431
LAN (local area networks), 14
  ports, 265
  segmenting, 25
VLAN, 21
  advantages of, 22
  MAC address-based VLAN, 24
  memberships, 23
  port-based VLAN, 23
  protocol-based VLAN, 23
  security, 22
  segmenting, 25
  troubleshooting, 462
latency, satellite Internet access, 237
Layer 3 addresses, 23
  `ls` command, 145
LDAP (Lightweight Directory Access Protocol), 154
  least privilege security principle, 356
  link aggregation, 125, 295
  link lights (network interfaces), 104
  link-local IPv6 addresses, 190-191
  link-state routing, 204-205
  Linux, Telnet and, 149
LLC (Logical Link Control) layer (OSI reference model), 136
  LLC (Logical Link Control) network standard (802.2), 76
LM (log management), 426
  load balancers, 115, 122, 295
  load tests, 421
  load-balancing switches. See content switches
local address information heading (netstat diagnostic utility), 321
lock and key access, server room security, 379
logical topologies (networks), 26, 404-406
loopback cable, 66
loopback feature (smart jacks), 73
loopbacks, ping diagnostic utility, 316
  loops
  routing loops, 204, 469
  switching loops, 469
  `ls` command, 145
LSA (link-state advertisements), 204
MAC (mandatory access control), 354
MAC (Media Access Control) addresses, 195
  ARP, 317-318
  filtering, 356-357
  MAC layer, 136
  NIC, viewing in, 196
  packet-filtering firewalls, 348
VLAN, 24
  advantages of, 22
  MAC address-based VLAN, 24
  membershioes, 23
  port-based VLAN, 23
  protocol-based VLAN, 23
  security, 22
  segmenting, 25
  troubleshooting, 462
macro viruses, 382-384
maintenance (networks), monitoring, 414
malware
  antivirus software, 388-390
  comparison chart, 385
  viruses as, 383
MAN (Metropolitan Area Networks), 15
  man-in-the-middle attacks, 387
maximum connection rates, wireless network connections, 271
maximum password age, 369
MDF (Main Distribution Frame) telecommunications rooms, 71
MDI (Medium Dependant Interface) ports, 99
MDI-X (Medium Dependant Interface-Crossed) ports (hubs), 99
  media (cable) testers, 432
media connectors
  568A telecommunications standard, 63-64
  568B telecommunications standard, 63-64
  BNC connectors, 56
  F-type connectors, 59
  fiber connectors, 59
  FireWire (IEEE 1394), 62
  RJ-11 connectors, 57
  RJ-45 connectors, 58
  RS-232 serial transmission standard, 61
  USB connectors, 62
media converters, 106, 122
media testers, 432-433
memory I/O addresses, network cards, 104-105
mesh topologies

mesh topologies, 30-31
troubleshooting, 468
wireless mesh topologies, 35-36
mget command, 145
MIB (Management Information Bases, 163
MIMO (multiple input multiple output) antenna technology, 261
mirrored stripe sets, RAID 10 fault tolerance, 291
mirroring ports, 126
modems, 108, 122
cable modems, 229-231
COM serial port resource assignments, 108
eight-one-none configuration, 234
mouse device resource conflicts, 110
UART chips, 109
monitoring network performance
application logs, 424
event logs, 422-426
fault detection, 414
history logs, 425
load tests, 421
maintenance, 414
network configurations, 414
packet sniffers, 415
performance tests, 421
port scanners, 417-420
reasons for, 413
security, 414
security logs, 423-424
stress tests, 422
system logs, 425
throughput testers, 415-417
procedures for, 411
mouse devices, modem resource conflicts, 110
MPLS (Multiprotocol Label Switching), 238-239
mput command, 145
MS-CHAP (Microsoft Challenge Handshake Authentication Protocol), 377
MS-CHAP v2 (Microsoft Challenge Handshake Authentication Protocol version 2), 377
MSAU (multistation access units), 28, 97, 465
mtr diagnostic utility, 333
multicasting, 154, 187, 190
multifunction network devices, 115-116, 123
multilayer switches, 113, 122
multimeters, 433
 multimode fiber-optic cable, 55
multiplexing, 80
MX (Mail Exchange) resource records, 159
narrowband transmissions. See spread spectrum technology (wireless networks)
NAT (Network Address Translation), 196
firewalls, 346-347
PAT, 197
SNAT, 198
nbtstat diagnostic utility, 326
NetBIOS (Network Basic Input/Output System), 160
netstat diagnostic utility
information headings, 321
netstat-a utility, 322-323
netstat-e utility, 322
netstat-r utility, 323-324
netstat-s utility, 324-325
switches list table, 320
network cards, 122, 427
adapter teaming, 295
bus compatibility, 104
dip switches, 105
installing, 105-106
IRQ, 104-105
jumpers, 105
MAC addresses, viewing, 196
media compatibility, 104
memory I/O addresses, 104-105
network interfaces, 104-106
OSI reference model maps, 140
selecting, 457
troubleshooting DSL, 228
network connectors
568A telecommunications standard, 63-64
568B telecommunications standard, 63-64
BNC connectors, 56
F-type connectors, 59
fiber connectors, 59
FireWire (IEEE 1394), 62
RJ-11 connectors, 57
RJ-45 connectors, 58
RS-232 serial transmission standard, 61
USB connectors, 62
network interface cards. See network cards
network layer (OSI reference model), 136, 139
network services
documenting, 400
TCP/IP
  DDNS, 156
  DHCP, 164-166
  DNS, 154-159
  RTP, 167
  SIP, 166-167
  SNMP, 161-164
  TLS, 166
networks
  10BaseFL standard, 82
  10BaseT standard, 81
ad hoc wireless topologies, 32
attenuation, 47, 52
bandwidth, 48, 76
bandwidth shapers, 117, 123
baseband transmissions, 46
bridges, 100-101, 121
bus topologies, 26-27, 36, 467-468
cable
  coaxial cable, 48, 52-53
crossover cable, 64-65, 82
  fiber-optic cable, 48, 53-55
  horizontal cable, 67
  loopback cable, 66
  plenum cable, 56
  rollover cable, 66
  straight-through cable, 64
twisted-pair cable, 48-51, 96-98
  vertical (backbone) cable, 67-69
centralized computing models, 18
client/server networks, 16-17
c coaxial networks, 458
configurations
documenting, 411
monitoring, 414
connectivity, selecting network cards, 457
content switches, 113, 122
CSU/DSU, 120-121
data transmission rates, 48
demarcation extensions, 73
demarcation points, 72-73
DHCP servers, 111-112, 122
dialog modes
  full-duplex, 46, 98
  half-duplex, 46
  simplex, 46
distributed computing models, 18
DNS servers, 116-117, 123
documentation
  baselines (performance), 407-408
  benefits of, 398
  key applications, 400
  network configurations, 411
  network equipment, 400
  network procedures, 400
  network services, 400
  network topologies, 399, 404-406
  policies, 409
  procedures, 410-411
  regulations, 412
  server configurations, 400
  wiring schematics, 400-403
Ethernet networks, switches, 98, 101
event logs, 422
  application logs, 424
  history logs, 425
  LM, 426
  security logs, 423-424
  system logs, 423
failures, costs of, 285-286
Fast Ethernet standards, 82-84
firewalls, 110, 122, 350
gateways, 103, 121
Gigabit Ethernet standards, 84-88
hubs, 121
hybrid topologies, 36
IDS, 114
infrastructure wireless topologies, 31
interfaces, 105
  activity lights, 104
  built-in interfaces, 106
networks

link lights, 104
speed lights, 104
interference, 47, 52
IPS, 114
ISDN, 217-218
LAN, 14, 25
load balancers, 115, 122
load tests, 421
logical topologies, 26
MAC addresses, MAC layer (OSI reference model), 136
maintenance, monitoring, 414
MAN, 15
media converters, 106, 122
mesh topologies, 35-36, 468
modems, 122
COM serial port resource assignments, 108
UART chips, 109
monitoring procedures, 411
multifunction devices, 123
multifunction network devices, 115-116
multilayer switches, 113, 122
network cards, 122
bus compatibility, 104
dip switches, 105
installing, 105-106
jumpers, 105
media compatibility, 104
memory I/O addresses, 104-105
network interfaces, 104-106
optimization strategies, QoS, 304-307
packet sniffers, 413
peer-to-peer networks, 16-17
performance monitoring
application logs, 424
event logs, 422-426
fault detection, 414
history logs, 425
load tests, 421
maintenance, 414
network configurations, 414
packet sniffers, 415
performance tests, 421
port scanners, 417-420
reasons for, 413
security, 414
security logs, 423-424
stress tests, 422
system logs, 423
throughput testers, 415-417
performance tests, 421
physical topologies, 26
port scanners, 417-420
private networks
firewalls, 345
IPv4 addressing, 183-185
VPN, 358-360
procedures, documenting, 400
proxy servers, 118-120, 123
public networks, IPv4 addressing, 183
qualification testers, 434
repeaters, 112, 121
ring topologies, 28, 97, 101, 465-466
routers, 102, 121
security
authentication, 369-370
firewalls, 345-350
smart jacks, 73
star bus topologies, 36
star topologies, 28, 36, 464
statistics, capturing, 408
stress tests, 422
switches, 121
throughput, testing, 415-417
token ring networks, 28, 97, 101
troubleshooting steps/procedures, 445
action plan implementation, 448-449
affected area identification, 446
establishing recent changes, 446
result testing, 449
solution documentation, 450
solution results/effects identification, 450
twisted-pair networks, 458
usage policies, 409
VLAN, 21
advantages of, 22
MAC address-based VLAN, 24
memberships, 23
port-based VLAN, 23
protocol-based VLAN, 23
security, 22
OFDM (Orthogonal Frequency Division Multiplexing), wireless networks

- segmenting, 25
- troubleshooting, 462

VPN, 358
- access methods, 20
- advantages/disadvantages of, 21
- connections, 20
- costs of, 20
- L2TP, 359-360
- PPTP, 359-360
- scalability of, 20

WAN, 15, 214
- ATM, 224
- circuit switching, 216-217
- Frame Relay, 222-223
- ISDN, 217
- OCx levels, 221
- packet-switching, 215-222
- PSTN, 235
- SONET, 220
- T-carrier lines, 220
- technology comparison chart, 224-225
- X.25 packet-switching technology, 222
- WAP, 107-108

wireless mesh topologies, 35-36

wireless networks
- 802.11 wireless standard, 260-263
- 802.11a wireless standard, 252-254, 260-263
- 802.11b wireless standard, 252-253, 260-263
- 802.11g wireless standard, 252-253, 260-263
- 802.11n wireless standard, 260-263
- 802.11x wireless standard, 265
- amplifying data signals, 272-274
- antennas, 249-252, 272-274
- auto transfer rates, 274
- beacons, 258-259
- Bluetooth, 276-277
- channel surfing, 261
- connection configuration, 269-271
- data rate versus throughput, 254-255
- DSSS, 258, 262
- establishing communications between devices, 266-271
- FHSS, 257, 262
- infrared, 275
- interference, 255-256
- MIMO technology, 261
- OFDM, 258
- repeaters, 272
- RF amplifiers, 272-273
- RF channels, 252-253
- security, 265
- spread spectrum technology, 257
- SSID, 275
- STA (stations), 267
- throughput versus data rate, 254-255
- TKIP, 266
- troubleshooting, 252-253, 270-275
- WAP, 247-249, 267, 271-272
- WEP, 263-264, 275
- wireless antennas, 249-251
- WPA, 264
- wireless topologies, 31
- PtMP wireless topologies, 34
- PtP wireless topologies, 33
- WPAN, 15

new user procedures, 410
newsgroups, 153
NEXT (near-end crosstalk), 454
NIC (Network Interface Cards). See network cards
NID (Network Interface Devices). See smart jacks
NIDS (Network-Based Intrusion Detection System), 352
NMS (network management systems). SNMP versus, 161
NNTP (Network News Transfer Protocol), 153
NOC (network operations centers). See telecommunication rooms
nodes, defining, 77
NS (Name Server) resource records, 159
nslookup diagnostic utility, 330-331
NTP (Network Time Protocol), 152-153

octets in IPv4 addresses, 180
OCx (Optical Carrier) levels, 221
OFDM (Orthogonal Frequency Division Multiplexing), wireless networks, 258
offsite storage (backups), 300-301
omnidirectional antenna signal, 250
one-way satellite systems, 236
open authentication, 268
open impedance mismatches (echoes), troubleshooting, 454-455
optical cable testers, 433
optimization strategies (networks), QoS (quality of service), 304
caching, 306-307
priority queuing, 305
traffic shaping, 305-306
OSI (Open Systems Interconnect) reference model
application layer, 138-139
bridges, mapping to, 140
data-link layer, 136, 139
hubs, mapping to, 140
ISO, 134
network cards, mapping to, 140
network layer, 136, 139
physical layer, 135, 139
presentation layer, 138-139
routers, mapping to, 140
session layer, 138-139
switches, mapping to, 140
transport layer, 137-139
UDP, 144
WAP, mapping to, 140
OSPF (Open Shortest Path First) link-state protocol, 205
OTDR (optical time-domain reflectometer), 433
overwriting/nonoverwriting viruses, 384
ownership policies, 409
packet sniffers, 415
packet switching, 215-216, 222
packet-filtering firewalls, 348-349
PAD (packet assemblers/disassemblers), 222
PAP (Password Authentication Protocol), 378
passive hubs, 97
passive scanning, AP discovery, 259
passwords
attacks, 386
complexity, 370
dialup Internet access, 234
enforcing history of, 369
expiration of, 369
maximum password age, 369
minimum length of, 369
POTS Internet access, 234
reusing, 369
strength of, 370
strong passwords, 370
weak passwords, 370
PAT (Port Address Translation), 197
patch cable, 458
patch panels, 69
patches, antivirus software, 390
PCMCIA cards, 104-105
peer-to-peer networks, 16-17
performance
baselines, documenting, 407-408
monitoring
event logs, 422-426
fault detection, 414
load tests, 421
maintenance, 414
network configurations, 414
packet snarfers, 415
performance tests, 421
port scanners, 417-420
reasons for, 413
security, 414
stress tests, 422
throughput testers, 415-417
testing, 421
permanent cable. See horizontal cable
personal software policies, 409
phishing attacks, 388
physical bus topologies (networks), 26-27
physical layer (OSI reference model), 135, 139
physical security. See server room security
physical topologies (networks), 26, 404-406
PIDS (Protocol-Based Intrusion Detection System), 352
PIN pads, server room security, 380
ping attacks, 319, 386
ping diagnostic utility
ARP, 319
PKI (Public Key Infrastructures)
  CA, 373
components of, 373
CRL, 373
digital signatures, 375
e-mail, 375
private key encryption, 374
public key encryption, 374
uses for, 375
plenum cable, 56
plugs. See loopback cable
PoE (Power over Ethernet), 123-124
poison reverse strategy, troubleshooting routing loops, 204
polarization (antennas), 252
policies, documenting, 409
polymorphic viruses, 383
POP3 (Post Office Protocol version 3), 148
port-based VLAN (virtual local area networks), 23
ports
  authentication, 126
controlled ports, 265
MDI ports, 99
MDI-X ports (hubs), 99
mirroring, 126
numbers, packet-filtering firewalls, 348
port scanners, 417-420
speed settings, 461
TCP/IP port assignments, 198-199
trunking, 125
UDP port assignments, 198-199
uncontrolled ports, 265
well-known ports, 199
POTS Internet access, 232-234
PPP (Point-to-Point Protocol), 364
RIP (Routing Information Protocol), 203
RIPv2 (Routing Information Protocol version 2), 203
risers, 452
RJ-11 (Registered Jack-11) connectors, 57
RJ-45 (Registered Jack-45) connectors, 58
roaming (wireless network communications), 267, 270
RoBAC (role-based access control), 356
roles, least privilege security principle, 356
rollover cable, 66
rouge AP (access points), 388
route add command, 202
route diagnostic utility, 333
route print command, 200
route selection, OSI network layer, 136
route utility, 334
routers, 102, 121
convergence, 203
gateways, 103
OSI reference model maps, 140
rollover cable, 66
routing loops, troubleshooting, 204
TCP/IP routing
default gateways, 200
distance-vector routing, 202-204
dynamic routing, 202-205
link-state routing, 204-205
routing tables, 200-201
static routing, 201
troubleshooting, 456
updates, 203
wireless networks, troubleshooting placement in, 274
routing loops, 469
routing tables
TCP/IP routing, 200-201
troubleshooting, 469
RRAS (Routing and Remote Access Service). See RAS
RS-232 serial transmission standard, 61
RSH (Remote Shell), 381
RTP (Real-time Transport Protocol), 167

sags, 297
satellite Internet access, 235
latency and, 237
one-way satellite systems, 236
propagation times, 236
rain fade, 237
troubleshooting, 236
two-way satellite systems, 236
scalability
VPN, 20
wireless mesh topologies, 36
schematics (wiring)
documenting, 400-403
troubleshooting, 404
updates, 404
scopes, 164, 192
SCP (Secure Copy Protocol), 153, 382
screwdrivers, 427
ScTP (screened twisted pair) cable, 49
SDH (Synchronous Digital Hierarchy). See SONET
SDSL (Symmetric Digital Subscriber Lines), 227
secret key cryptography, 372
Secure Shell (SSH), 146, 150
security
access control
access masks, 355
ACL, 355
DAC, 354-355
MAC, 354
MAC filtering, 356-357
RBAC, 355
RoBAC, 356
TCP/IP filtering, 357
accounting, 368, 376-377
antivirus software, 388
auditing, 368, 376-377
authentication, 366-368
CHAP, 378
EAP, 378
Kerberos, 371-372
MS-CHAP, 377
MS-CHAP v2, 377
PAP, 378
security

passwords, 369
passwords, strength of, 370
PKI, 373-375
RADIUS, 376-377
remote authentication protocols, 377-378
TACACS+, 376-377
authorization, 367-368, 376-377
back door attacks, 387
broadband Internet access, 232
cable Internet access, 232
cryptography, 372
DoS attacks, 385-386
DSL, 232
eavesdropping attacks, 387
encryption, presentation layer (OSI reference model), 138
firewalls
application layer firewalls, 349-350
bandwidth management, 347
circuit-level firewalls, 349-350
content filtering via, 346
functions of, 346
host-based firewalls, 350
NAT, 346-347
network-based firewalls, 350
packet-filtering firewalls, 348-349
private networks, 345
session layer firewalls. See circuit-level firewalls
signature identification via, 346
stateful firewalls, 347
stateless firewalls, 347
URL filtering via, 347
virus scanning via, 346
Fraggle attacks, 386
honeynets, 353
honeypots, 353
ICMP floods, 386
IDS, 352
IPS, 351
IPSec protocol, 361-362
L2TP, 359-360
least privilege security privilege, 356
logs, 423-424
macro viruses, 382-384
man-in-the-middle attacks, 387
monitoring, 414
password attacks, 386
phishing attacks, 388
physical security. See security, server rooms
ping of death attacks, 386
procedures for, 410
protocol summary table, 381
remote access ICA, 366
remote access RAS, 362
roles, least privilege security principle, 356
rogue AP (access points), 388
spoofing attacks, 387
spyware, 383
SSH (Secure Shell), 146, 150
SYN floods, 386
Trojan horses, 383-384
tunneling, 359-360
viruses, 383-385
macro viruses, 382-384
protection strategies, 389
VLAN, 22
VPN, 358-160
VPN concentrators, 352-353
wireless networks, 268
802.1X, 265
TKIP, 266
WEP, 263-264
WPA, 264
worms, 382, 384
server clustering, 294
server room security, 379-381
servers
configuring, documenting configurations, 400
DHCP servers, 111-112, 122
DNS servers, 116-117, 123
fault tolerance
server clustering, 294
standby servers, 292-293
heartbeats, 293
primary server configurations, 293
proxy servers, 118-120, 123
standby servers, 292-293
VPN, 19, 358
Components of, 161
management systems, 162
MIB, 163
NMS versus, 161
SNMPv3, 164
SOA (Start of Authority) resource records, 159
social engineering attacks, 387
software
personal software policies, 409
procedures for, 411
solution documentation (troubleshooting steps/procedures), 450-451
solution results/effects identification (troubleshooting steps/procedures), 450
SONET (Synchronous Optical Networks), 86, 220
source quenches, 150
source route bridges, 101
speed lights (network interfaces), 104
spikes, 296
split horizon strategy, troubleshooting routing loops, 204
spoofing attacks, 387
spread spectrum technology (wireless networks), 257-258, 262
spyware, 383
SSH (Secure Shell), 146, 150, 381
SSID (Service Set Identifiers), 248
beacons, 259
wireless network communications, 268-270
STA (Spanning Tree Algorithm), 124-125
STA (stations), wireless networks, 267
standby servers, 292-293
star topologies, 28
star bus topologies, 36
troubleshooting, 464
state information heading (netstat diagnostic utility), 321
stateful firewalls, 347
stateful IP configurations, 190
stateless firewalls, 347
stateless IP configurations, 190
static addressing, 191
static routing, 136, 201
statistics (networks), capturing, 468
stealth viruses, 384
storage, backups

storage, backups, 300-301
store-and-forward switching environments, 99
STP (shielded twisted pair) cable, 49-50
STP (Spanning Tree Protocol), 124-125
straight-through cable, 64
stress tests, 422
strippers (wire), 427
strong passwords, 370
structure cable. See horizontal cable
subnet masks
    CIDR, 185
    client connectivity, 459
    IP addresses, 181
    TCP/IP client system configurations, 193
subnetting, 182-183
supplicants (LAN ports), 265
surge protection, smart jacks, 73
surges, 297
SVC (switched virtual circuits), 223
swipe cards, server room security, 380
switch console ports, rollover cable, 66
switches, 28, 101, 121
    content switches, 113, 122
crossover cable, 64-65, 99
cut-through switching environments
    98
direct cable connections, 70
FragmentFree-switching environments, 99
    full-duplex dialog mode, 98
hubs versus, 98
load-balancing switches. See content switches
MDI ports, 99
multilayer switches, 113, 122
OSI reference model maps, 140
PoE, 123-124
port authentication, 126
port mirroring, 126
route utility, 334
store-and-forward switching environments, 99
STP, 124-125
straight-through cable, 64
troubleshooting, 456
trunking, 125
switching loops, 469
symmetric key cryptography, 372
SYN floods, 386
system baselines, documenting, 408
system buses, network card compatibility, 104
system logs, 425
T-carrier lines, 218
    fractional T, 219
T1 lines, 219
T2 lines, 219
T3 lines, 219-220
T4 lines, 219
transmission speed comparison chart, 219-220
tapes (backups)
    labeling, 301
    new tapes, 301
    offsite storage, 300-301
    rotation backups, 300
tape drives, cleaning, 301
tCP/IP (Transmission Control Protocol/Internet Protocol)
    ARP, 151-152
client connectivity, 458-460
client system configurations, 193
cable requirements, 193, 460
cabling, 193
cable types, 193
filtering, 357
FTP, 144
HTTP, 147
HTTPS, 148
ICMP, 150
IGMP, 154
IMAP4, 148
IPSec, 362
IPv4, 142
    address classes, 180
    APIPA, 194
    BOOTP, 194
cable broadcast addresses, 187
CIDR, 185
cable client system configurations, 193
cable decimal-to-binary value conversion chart, 180
cable default gateways, 185-186, 193
cable dynamic addresses, 192
time stamps, beacons, 259
timeouts, 143
TKIP (Temporal Key Integrity Protocol), 264-266
TLS (Transport Layer Security), 166
token ring networks
MSAU, 28, 97, 465
source route bridges, 101
tone generators, 431
toner probes, 430
tools
route utility, 334
wiring
media tester, 432-433
screwdriver, 427
tone generator, 431
Wi-Fi, 434-435
wire crimper, 427
topologies (networks)
ad hoc wireless topologies, 32
bus topologies, 26-27
star bus topologies, 36
troubleshooting, 467-468
documenting, 399, 404-406
IEEE standards, 79
infrastructure wireless topologies, 31
mesh topologies, 30-31
troubleshooting, 468
wireless mesh topologies, 35-36
ring topologies
token ring networks, 28, 97, 101, 465
troubleshooting, 465-466
star topologies
star bus topologies, 36
troubleshooting, 464
wireless topologies
ad hoc topologies, 32
infrastructure topologies, 31
PtMP topologies, 34
PtP topologies, 33
trace route diagnostic utility, 202, 309-312
traffic shaping, 305-306
training, network documentation’s help in, 399
translational bridges, 101
transmission rates (data), 48
transparent bridges, 101
transport layer (OSI reference model), 137-139
trap managers, 182
triggered updates, routers, 203
Trojan horses, 383-384
troubleshooting
ARP diagnostic utility, 317-319
attenuation, 454
bridges, 456
broadcast storms, 470
cable, 451
attenuation, 454
crosstalk, 453-454
EMI, 454
FEXT, 454
identifying characteristics, 452
identifying where cable is used, 452
installations, 74
NEXT, 454
open impedance mismatches (echoes), 454-455
testing cable, 453
cable Internet access, 230
cable Internet access, 230
client connectivity
coaxial network connections, 458
duplex settings, 461
network card selection, 457
port speeds, 461
TCP/IP configuration, 458-460
twisted-pair network connections, 458
crosstalk, 453-454
Destination Host Unreachable error message (ping utility), 313
diagnostic utilities list, 307-308
dialup Internet access, 233-234
dig diagnostic utility, 331-332
DSL, 228-229
echoes (open impedance mismatches), 454-455
EMI, 454
Expired TTL error message (ping utility), 315
FEXT, 454
host diagnostic utility, 333
hubs, 455
ICMP floods, 319
troubleshooting

ifconfig diagnostic utility, 329-330
impedence mismatches (echoes), 454-455
infrastructure hardware, 455-456
ipconfig diagnostic utility, 327-329
mtr diagnostic utility, 333
nbtstat diagnostic utility, 326
netstat diagnostic utility
information headings, 321
   netstat-a utility, 322-323
   netstat-e utility, 322
   netstat-r utility, 323-324
   netstat-s utility, 324-325
   switches list table, 320
network documentation's help in, 398
   NEXT, 454
nslookup diagnostic utility, 330-331
open impedence mismatches (echoes), 454-455
ping attacks, 319
ping diagnostic utility
   ARP, 319
   Destination Host Unreachable error message, 313
   DNS, 317
   Expired TTL error message, 315
   loopback addresses, 316
   Request Timed Out error message, 314-315
   switches list table, 312
   troubleshooting example, 316
   Unknown Host error message, 315
POTS Internet access, 233-234
Proxy ARP, 470
Request Timed Out error message (ping utility), 314-315
route diagnostic utility, 333-334
routers, 456
routing loops, 204, 469
routing tables, 469
satellite Internet access, 236
steps/procedures
   action plan implementation, 448-449
   affected area identification, 446
   escalation procedures, 447-448, 469-470
   establishing probable cause, 447
   establishing recent changes, 446
   information gathering process, 445-446
result testing, 449
solution documentation, 450
solution results/effects identification, 450
switches, 456
switching loops, 469
tools for
   butt sets, 434
   media (cable) testers, 432
   multimeters, 433
   network qualification testers, 434
   optical cable testers, 433
   OTDR, 433
   protocol analyzers, 431
   punchdown tools, 428
   screwdrivers, 427
   TDR, 432-433
   temperature monitors, 429-430
   toner probes, 410
   voltage event recorders, 428
   Wi-Fi detectors, 434-435
   wire crimpers, 427
   wire snips, 427
   wire strippers, 427
topologies
   bus topologies, 467-468
   mesh topologies, 468
   ring topologies, 465-466
   star topologies, 464
trace route diagnostic utility, 309-312
Unknown Host error message (ping utility), 315
VLAN, 462
WAP, 456
wireless networks, 252-253, 270
   antennas, 274
   auto transfer rates, 274
   data signal strength, 273-274
   troubleshooting checklist, 274-275
   troubleshooting router placement, 274
   WAP coverage, 271-272
   WEP, 275
wiring, 451
   attenuation, 454
   crosstalk, 453-454
   EMI, 454
   FEXT, 454
identifying characteristics, 452
identifying use, 453
identifying where cable is used, 452
NEXT, 454
open impedance mismatches (echoes), 454-455
schematics, 404
testing cable, 453
wiring tools
media testers, 432-433
screwdrivers, 427
tone generators, 431
Wi-Fi, 434-435
wire crimpers, 427
trunking, 125
tunneling, 18, 358
L2TP, 359-360
PPTP, 359-360
twisted-pair cable, 48-49
categories of, 50-51
hubs, 96-98
ScTP cable, 49
STP cable, 49-50
UTP cable, 49-50
twisted-pair networks, 458
two-way satellite systems, 236
type 66 punchdown blocks, 71
type 110 punchdown blocks, 71

UART (Universal Asynchronous Receiver/Transmitter) chips, 109
UDP (User Datagram Protocol), 137, 143
OSI model, 144
port assignments, 198-199
uncontrolled ports, 265
unicast IPv4 addresses, 187
unicast IPv6 addresses, 189
UNIX, Telnet and, 149
Unknown Host error message (ping utility), 315
updates
antivirus software, 389-390
routers, 203
wiring schematics, 404
UPS (Uninterruptible Power Supplies), 296-297
uptime, defining, 285-286
URL (Uniform Resource Locators), filtering, 347
USB (Universal Serial Buses), network connectors, 62
user account policies, 409
usernames, POTS (dialup) Internet access, 234
UTP (unshielded twisted pair) cable, 49-50, 427

variant viruses, 383
vertical (backbone) cable, 67-69
VHDSL (Very High Bit Rate Digital Subscriber Lines), 227
violations, reporting, 411
virtual circuits, 223
virtual-circuit packet switching, 215
virtual private networks. See VPN
viruses, 382-383, 385
antivirus software, 388-390
macro viruses, 382-384
protection strategies, 389
scanning, 346, 389-390
VLAN (virtual local area networks), 21
advantages of, 22
MAC address-based VLAN, 24
memberships, 23
port-based VLAN, 23
protocol-based VLAN, 23
security, 22
segmenting, 25
troubleshooting, 462
voltage event recorders, 428
VPN (virtual private networks), 18
access methods, 20
advantages/disadvantages of, 21
clients, 19, 358
connections, 20, 359
costs of, 20
L2TP, 359-360
PPTP, 359-360
protocols, 20, 358
scalability of, 20
servers, 19, 358
VPN concentrators, 352-353
## Wireless Networks

### WAN (Wide Area Networks)
- ATM, 224
- Circuit switching, 216-217
- Frame Relay, 222-223
- ISDN, 217
- OCx levels, 221
- Packet switching, 215-216, 222
- PSTN, 235
- SONET, 220
- Switching methods comparison chart, 216
- T-carrier lines, 218
- T3, 220
- Transmission speed comparison chart, 219-220
- Technology comparison chart, 224-225

### WAP (Wireless Access Points)
- Active scanning, 259
- Beacons, 258-259
- BSA, 249
- BSS, 248
- BSSID, 249
- ESS, 248
- ESSID, 249
- OSI reference model maps, 140
- Passive scanning, 259
- Repeaters, 272
- SSID, 248
- Troubleshooting, 456

### Warm Recovery Sites, 304

### Warm Swapping, 302

### Weak Passwords, 370

### Web-Based Mail, 149

### Well-Known Ports, 199

### WEP (Wired Equivalent Privacy), 263-264, 275

### Wi-Fi Detector, 434-435

### Windowing, 137

### WINS (Windows Internet Name Service), 160

### Wi-Fi Crimpers, 427

### Wi-Fi Snips, 427

### Wi-Fi Strippers, 427

### Wireless Antennas, 249
- Directional antennas, 251
- Gain values, 250
- Isotropic antennas, 250
- Omnidirectional antennas, 250-251
- Polarization, 252

### Wireless Internet Access, 237-238

### Wireless Mesh Topologies, 35-36

### Wireless Networks, 246, 271
- 802.11 wireless standard, 260-263
- 802.11a wireless standard, 252-254, 260-263
- 802.11b wireless standard, 252-253, 260-263
- 802.11g wireless standard, 252-253, 260-263
- 802.11n wireless standard, 260-263
- 802.11x wireless standard, 265
- Antennas
  - Amplifying data signal strength, 273
  - Troubleshooting, 272-274
- Auto transfer rates, troubleshooting, 274
- Beacons, 258-259
- Bluetooth, 276-277
- Channel surfing, 261
- Data rate versus throughput, 254-255
- Data signals, 249
  - Amplifying, 272-274
  - Antenna coverage, 250-252
  - Antenna ratings, 250
  - Troubleshooting, 273-274
- DSSS, 258, 262
- Establishing communications between devices, 266
  - Association, 267
  - Authentication, 267
  - Authentication in, 270
  - Connection configuration, 269-271
  - Default device settings, 269
  - DTIM periods, 271
  - Maximum connection rates, 271
  - Reassociation, 267
  - RF channels, 268-270
  - Roaming, 267, 270
  - Security in, 268
  - SSID, 268-270
  - Wireless mode, 271
- FHSS, 257, 262
- Infrared, 275
- Interference, 255-256
- OFDM, 258
wireless networks

repeaters, 272
RF amplifiers, 272-273
RF channels, 252-254
routers, troubleshooting placement of, 274
security
  802.1X, 265
  TKIP, 266
  WEP, 263-264
  WPA, 264
spread spectrum technology, 257
SSID, troubleshooting, 275
STA, 267
throughput, data rate versus, 254-255
troubleshooting, 252-253, 270, 274-275
WAP, 247, 267
  BSA, 249
  BSS, 248
  BSSID, 249
  ESS, 248
  ESSID, 249
  SSID, 248
troubleshooting coverage of, 271-272
WER, 275
wireless antennas, 249
directional antennas, 251
gain values, 250
isotropic antennas, 250
MIMO technology, 261
omnidirectional antennas, 250-251
polarization, 252
wireless topologies
  ad hoc topologies, 32
  infrastructure topologies, 31
  PtMP topologies, 34
  PtP topologies, 33
wiring
  installations, 74-75
  risers, 452
  schematics
documenting, 400-403
troubleshooting, 404
  updates, 404
  screwdrivers, 427
termination, 74-75
tools for
  media tester, 432-433
  screwdriver, 427
tone generator, 431
Wi-Fi, 434-435
wire crimpers, 427
wire snips, 427
wire strippers, 427
troubleshooting, 451
  attenuation, 454
crosstalk, 453-454
  EMI, 454
  FEXT, 454
  identifying characteristics, 452
  identifying use, 453
  identifying where cable is used, 452
  NEXT, 454
  open impedance mismatches (echoes), 454-455
testing cable, 453
wiring closets.
  See telecommunications rooms
WISP (Wireless Internet Service Providers), 237-238
workgroup hubs, 97
worms, 382, 384
WPA (Wi-Fi Protected Access), 264-265
WPAN (wireless personal area networks), 15

X - Y - Z

X.25 packet-switching technology, 222
xDSL (Digital Subscriber Lines), 226
  ADSL, 227
  filters, 228
  HDSDL, 227
  ISDN DSL, 227
  RADSL, 227
  SDSL, 227
  security, 232
  speed comparison chart, 228
troubleshooting, 228-229
  VHDSL, 227