EXAM CRAM

The Smart Way to Study™

Exam N10-004

CompTIA® Network+

Third Edition

Mike Harwood

CompTIA® Network+ Exam Cram, Third Edition

ISBN-13: 978-0-7897-3796-0
ISBN-10: 0-7897-3796-5

Library of Congress Cataloging-in-Publication Data:
Harwood, Mike.
CompTIA Network+ exam cram / Mike Harwood. -- 3rd ed.
p. cm.
ISBN 978-0-7897-3796-0 (pbk. w/cd)
1. Computer networks--Examinations--Study guides. 2. Telecommunications engineers--Certification. 3. Electronic data processing personnel--Certification. I. Title.
TK5105.5.H372 2009
004.6--dc22

2009004266

Printed in the United States of America
First Printing: March 2009
13 12 11 10 09 4 3 2 1

Trademarks

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Pearson cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Warning and Disclaimer

Every effort has been made to make this book as complete and accurate as possible, but no warranty or fitness is implied. The information provided is on an "as is" basis. The author and the publisher shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the CD or programs accompanying it.

Bulk Sales

Que Publishing offers excellent discounts on this book when ordered in quantity for bulk purchases or special sales. For more information, please contact:

U.S. Corporate and Government Sales
1-800-382-3419
corpsales@pearsontechgroup.com

For sales outside of the U.S., please contact:

International Sales
+1-317-581-3793
international@pearsontechgroup.com

Publisher
Paul Boger

Acquisitions Editor
Betsy Brown

Senior Development Editor
Christopher Cleveland

Managing Editor
Patrick Kanouse

Project Editor
Mandie Frank

Copy Editor
Gayle Johnson

Indexer
Ken Johnson

Proofreader
Molly Proue

Technical Editors
Chris Crayton, Pawan Bhardwaj

Publishing Coordinator
Vanessa Evans

Multimedia Developer
Dan Scherf

Designer
Gary Adair

Compositor
Mark Shirar

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).

- Mailing address, which identifies the address to which you want your certificate mailed.
- Exam number and title.
- Email address for contact purposes. This often is the fastest and most effective means of contacting you. Many clients require it for registration.
- Credit-card information so that you can pay online. Vouchers can be redeemed by calling the respective testing center.

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!

7

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.

- 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.

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

dB 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 7.1 Comparing Omnidirectional and Directional Antennas

Characteristic	Omnidirectional	Directional	Advantage/Disadvantage
Wireless area coverage	General coverage area	Focused coverage area.	Omnidirectional allows 360-degree coverage, giving it a wide coverage area. Directional provides a targeted path for signals to travel.
Wireless transmission range	Limited	Long point-to-point range.	Omnidirectional antennas provide a 360-degree coverage pattern and, as a result, far less range. Directional antennas focus the wireless transmission; this focus allows for greater range.
Wireless coverage shaping	Restricted	The directional wireless range can be increased and decreased.	Omnidirectional antennas are limited to their circular pattern range. Directional antennas can be adjusted to define a specific pattern, wider or more focused.

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.

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.

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.

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

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 7.2 RF Channels for 802.11b/g

Channel	Frequency Band
1	2412MHz
2	2417MHz
3	2422MHz
4	2427MHz

Table 7.2 RF Channels for 802.11b/g *Continued*

Channel	Frequency Band
5	2432MHz
6	2437MHz
7	2442MHz
8	2447MHz
9	2452MHz
10	2457MHz
11	2462MHz

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

Channel	Frequency
36	5180MHz
40	5200MHz
44	5220MHz
48	5240MHz
52	5260MHz
56	5280MHz
60	5300MHz
64	5320MHz

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.

EXAM ALERT

Data rate or throughput Data rate refers to the theoretical maximum of a wireless standard, such as 54Mbps. Throughput refers to the actual speeds achieved after all implementation and interference factors.

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 7.4 Wireless Obstacles Found Indoors

Obstruction	Obstacle Severity	Sample Use
Wood/wood paneling	Low	Inside a wall or hollow door
Drywall	Low	Inside walls
Furniture	Low	Couches or office partitions
Clear glass	Low	Windows
Tinted glass	Medium	Windows
People	Medium	High-volume traffic areas that have considerable pedestrian traffic
Ceramic tile	Medium	Walls

Table 7.4 Wireless Obstacles Found Indoors *Continued*

Obstruction	Obstacle Severity	Sample Use
Concrete blocks	Medium/high	Outer wall construction
Mirrors	High	Mirror or reflective glass
Metals	High	Metal office partitions, doors, metal office furniture
Water	High	Aquariums, rain, fountains

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.

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.

EXAM ALERT

The Network+ exam will have questions on the characteristics of the wireless standards. Remember, 802.11 wireless standards use 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.

EXAM ALERT

Wireless standards Be prepared to answer questions on the specific characteristics of wireless standards on the Network+ exam.

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 7.5 802.11 Wireless Standards

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

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 7.6 Comparison of IEEE 802.11 Standards

IEEE Standard	RF Used	Spread Spectrum	Data Rate (in Mbps)
802.11	2.4GHz	DSSS	1 or 2
802.11	2.4GHz	FHSS	1 or 2
802.11a	5GHz	OFDM	54
802.11b	2.4GHz	DSSS	11
802.11g	2.4Ghz	DSSS	54
802.11n	2.4/5GHz	OFDM	600 (theoretical)

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.

EXAM ALERT

Wireless terms When a single AP is connected to the wired network and to a set of wireless stations, it is called a *Basic Service Set (BSS)*. An *Extended Service Set (ESS)* describes the use of multiple BSSs that form a single subnetwork. Ad hoc mode is sometimes called an *Independent Basic Service Set (IBSS)*.

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*.

EXAM ALERT

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.

CAUTION

Default settings Wireless devices ship with default SSIDs, security settings, channels, passwords, and usernames. To protect yourself, it is strongly recommended that you change these default settings. Today, many Internet sites list the default settings used by manufacturers with their wireless devices. This information is used by people who want to gain unauthorized access to your wireless devices.

Configuring the Wireless Connection

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.

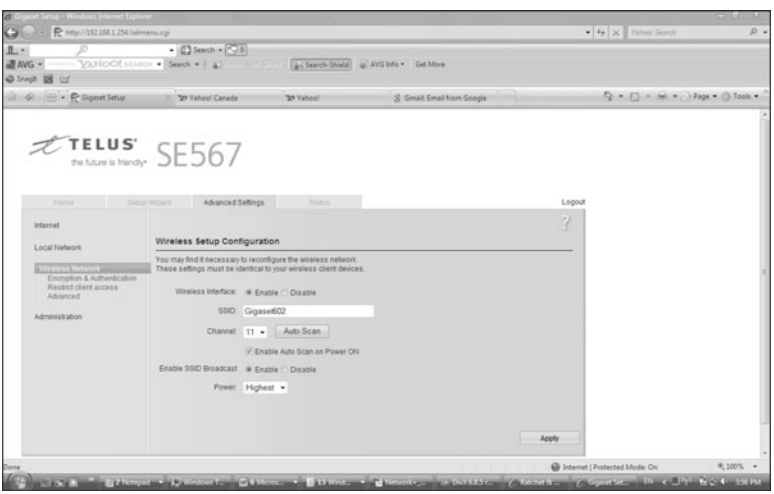

FIGURE 7.1 Wireless configuration information.

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.

TIP

Troubleshooting scenario and solution Suppose users connecting to a wireless access point are experiencing random problems such as lost connections, poor speed, and network errors. Check to see whether the wireless devices are operating within the accepted range of the wireless access point. Also find out whether any environmental considerations have not been fully taken into account, such as construction materials and heavy machinery, which can interfere with the signal's quality.

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.

NOTE

Bluetooth For implementation purposes, Bluetooth provides solutions for three primary areas: cable replacement, ad hoc networking, and data and access points.

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

Characteristic	Description
Specification	Bluetooth
Topology	Ad hoc
Spread spectrum	FHSS
Medium	2.4GHz RF
Speed	720Kbps
Range	10 meters in optimal conditions

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."

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?

Mike Harwood. *Network+ Exam Prep*, 3rd Edition. Que Publishing, 2009.

Douglas Comer. *Computer Networks and Internets*, 5th Edition. Prentice Hall, 2008.

"TechEncyclopedia," www.techencyclopedia.com.

Updated technology information, http://www.wikipedia.org/.

Index

NUMBERS

A

B

C

D

E

F

G

H

I

J - K - L

M

N

O

P

Q - R

S

T

U

V

W

X - Y - Z