

## **Chapter 2**

### **Network Devices**

#### **At a Glance**

#### **Instructor's Manual Table of Contents**

- Overview
- Objectives
- Teaching Tips
- Quick Quizzes
- Class Discussion Topics
- Additional Projects
- Additional Resources
- Key Terms

## Lecture Notes

### Overview

Many devices help control and extend the usable size of a growing network. These devices have a wide variety of functions and are added to networks to allow a greater number of computers to exist on the network; to extend the usable distance of the network; to segment, or localize, traffic on the network; to subdivide the network so problems are easier to isolate; and to join existing networks together. In this chapter, you will learn about the different devices that can be used to accomplish these objectives. The devices include repeaters, hubs, bridges, switches, routers, brouters, wireless access points, and gateways. In addition, you will learn about Ethernet, which is the most prolific network technology in use on LANs today. This chapter will explain a variety of Ethernet operations including CSMA/CD, Fast Ethernet, Gigabit Ethernet, and half- and full-duplex communications.

### Chapter Objectives

- Explain the uses, advantages, and disadvantages of repeaters, hubs, wireless access points, bridges, switches, and routers
- Define the standards associated with wireless media
- Explain basic wireless connection parameters, security, and troubleshooting
- Define network segmentation
- Explain network segmentation using bridges, switches, routers, brouters, and gateways
- Explain Ethernet operations
- Define Fast Ethernet and Gigabit Ethernet

### Teaching Tips

#### Repeaters

1. Mention that the number of nodes on a network and the length of cable used influence the quality of communication on the network.
2. Define attenuation as the degradation of signal clarity. Repeaters work against attenuation by repeating signals that they receive on a network, typically cleaning and regenerating the digital transmission in the process. Use Figure 2-1 to illustrate your explanation.

<b>Teaching Tip</b>	Learn more about repeaters at: <a href="http://en.wikipedia.org/wiki/Repeater">http://en.wikipedia.org/wiki/Repeater</a> .
-------------------------	--

3. Note that on analog networks, devices that boost the signal are called amplifiers. These devices do not have the same signal regeneration capabilities as repeaters because they must maintain the shape of the received signal.

4. Mention that repeaters work in the Physical layer (layer 1).
5. Mention that on optical networks, signal amplification is handled by optical repeaters.
6. Explain that some repeaters can be used to connect two physically different types of cabling. Use Figure 2-2 to illustrate your explanation.

## Hubs

1. Define a hub as a generic connection device used to tie several networking cables together to create a link between different stations on a network.
2. Explain that active hubs amplify or repeat signals that pass through them. A passive hub merely connects cables on a network and provides no signal regeneration.

<b>Teaching Tip</b>	Refer your students to <a href="http://compnetworking.about.com/cs/internetworking/g/bldef_hub.htm">http://compnetworking.about.com/cs/internetworking/g/bldef_hub.htm</a> for additional information about network hubs.
---------------------	---

3. Explain that topology refers to the physical layout of network cable and devices. Use Figure 2-3 to illustrate your explanation.

## Advantages and Disadvantages of Repeaters and Hubs

1. Describe the following advantages of using repeaters and hubs in your network:
  - a. Repeaters and hubs can extend a network's total distance.
  - b. Repeaters and hubs do not seriously affect network performance.
  - c. Certain repeaters can connect networks using different physical media.
2. Describe the following disadvantages of using repeaters and hubs in your network:
  - a. Repeaters and hubs cannot connect different network architectures, such as Token Ring and Ethernet.
  - b. Repeaters and hubs do not reduce network traffic.
  - c. Repeaters and hubs do not segment the network.
3. Explain that repeaters and hubs do not reformat data structures, so they cannot connect networks that require different types of frames. Also, they do not reduce network traffic because they repeat everything they receive.
4. Mention that repeaters do not segment a network. Frames that are broadcast on a given segment may collide. Devices that "see" the traffic of other devices are said to be on the same collision domain.

## Wireless Access Points

1. Explain that wireless access points provide cell-based areas where wireless clients such as laptops and PDAs can connect to the network by associating with the access point. Use Figure 2-4 to illustrate your explanation.
2. Explain that wireless access points operate at the Physical and Data Link layers of the OSI model. In most respects, a wireless access point functions exactly like a hub.

<b>Teaching Tip</b>	Each access point and wireless client must contain a radio transceiver that matches the wireless technology on the network or there can be no communications between them.
---------------------	--

## Wireless Standards and Organizations

1. Use Table 2-1 to describe various wireless standards and organizations.

## Wireless Network Components

1. Explain that wireless clients can connect and communicate directly with each other in ad hoc mode. In this mode, there is no access point, which is not typical.
2. Explain that commonly, wireless clients attach wirelessly to an access point in infrastructure mode. As previously stated, this mode involves the access point wired back into a switch.
3. Mention that if a single access point is available in infrastructure mode, then the mode is said to be a Basic Service Set (BSS).
4. Explain that more typically, WLANs involve multiple access points connected to various switches in the network. This allows users to roam around the building and remain connected to the WLAN as well as the LAN and WAN. This type of infrastructure mode is known as an Extended Service Set (ESS).

## Wireless Connectivity

1. Mention that access points typically broadcast their network name, also known as the Service Set Identifier (SSID).
2. Explain that when wireless clients are powered on, they begin scanning the airspace for available access points. They detect the broadcasted SSID of the various access points in the area and attempt to associate with the one that has the highest signal level and the lowest error rate. If the system is open, the client is accepted by the access point and begins communications.

3. Explain that when the SSID is not broadcasted, wireless clients must already be configured with the correct SSID. The client will send out a probe request with the configured SSID, and the access point with that SSID configured will allow the client to associate.

**Teaching  
Tip**

Sometimes, access points are configured not to broadcast their SSID. This is a safety feature, although a very weak one.

**Wireless Security Measures**

1. Mention that while security is always necessary in WLANs due to the broadcast nature of the medium, these devices are not designed to handle the most complex and highest levels of security.
2. Explain that the most important reason to implement security on your WLAN at home is so that others in your neighborhood do not use your bandwidth for free.
3. Explain that workspace situations call for security that not only requires the client device to authenticate, but that also prompts the device user to enter a username and password.
4. Mention that the 802.1x is used at the physical layer to block ports, and the Extensible Authentication Protocol (EAP) is used at layer 2 to transfer the authentication frames.
5. Use Table 2-2 to explain the 802.11 Security options.

**Wireless Troubleshooting**

1. Describe the following steps for adding a WLAN to your LAN:
  - a. Make sure your wired LAN is working.
  - b. Complete a wireless site survey to determine access point placement.
  - c. Install the access point(s) with no security.
  - d. Attempt to associate to the access point with a laptop.
  - e. Configure security on both the access point and the client.
  - f. Verify connectivity at all layers.
2. Explain that as the number of users on the WLAN increases, each user's individual bandwidth will decrease.
3. Describe the following problems that are particular to 802.11 networks:
  - a. Interference may occur from too much overlap of one access point's cell range onto another.
  - b. User devices must be using an 802.11 standard that is compatible with the access point standards.
  - c. Access point antennas may not be securely connected and in optimal position.
  - d. Potential sources of interference should be monitored.

## Advantages and Disadvantages of Wireless Access Points

1. Describe the following advantages of using 802.11 on your network:
  - a. Wireless devices provide the ability to work anywhere within range of your access points.
  - b. Wireless extends the range of your network without running additional wires except the ones from the access points to the switch.
2. Describe the following disadvantages of using 802.11 on your network:
  - a. Wireless introduces serious security concerns into the network environment.
  - b. 802.11 provides much less bandwidth than wired devices.
  - c. Many situations exist where 802.11 will not function well due to serious interference from various sources.

## Network Segmentation

1. Define segmentation as the breaking down of a single heavily populated network segment into smaller segments, or collision domains, populated by fewer nodes. Use Figure 2-5 to illustrate your explanation.
2. Define segment as a part of a network that is divided logically or physically from the rest of the network.
3. Explain that network problems occur when network administrators place too many nodes on the same network segment. This situation causes the number of collisions to increase.

## Quick Quiz 1

1. \_\_\_\_ usually refers to the physical layout of network cable and devices.  
Answer: Topology
2. Devices that “see” the traffic of other devices are said to be on the same \_\_\_\_ as those devices.  
Answer: collision domain
3. \_\_\_\_ provide cell-based areas where wireless clients such as laptops and PDAs can connect to the network by associating with the access point.  
Answer: Wireless access points
4. A(n) \_\_\_\_ is a part of a network that is divided logically or physically from the rest of the network.  
Answer: segment

## Bridges

1. Explain that bridges operate at the Data Link layer of the OSI model. They filter traffic between network segments by examining the destination MAC address. Based on the destination MAC address, the bridge either forwards or discards the frame. Use Figure 2-6 to illustrate your explanation.
2. Mention that bridges reduce network traffic by keeping local traffic on the local segment.
3. Define a broadcast frame as a frame destined for all computers on the network.

### *Teaching Tip*

The bridge functions like a repeater in that it listens to incoming frames and repeats them on other segments. The only real difference is that it actually reads the MAC address and chooses whether to repeat or discard a frame.

## Transparent Bridges

1. Explain that transparent bridges are also called learning bridges because they build a table of MAC addresses as they receive frames. This means that they “learn” which addresses are on which segments.
2. Explain that a transparent bridge uses the source MAC addresses to determine which addresses are on which segments. By determining a frame’s origin, the bridge knows where to send frames in the future.
3. Mention that Ethernet networks mainly use transparent bridges.

## Source-Routing Bridges

1. Explain that source-routing bridges rely on the source of the frame transmission to provide the routing information. The source computer determines the best path by sending out explorer frames.
2. Mention that the source includes the routing information returned by its explorer frames in the frame sent across the network. The bridge uses this information to build its table.

## Translation Bridges

1. Explain that translation bridges can connect networks with different architectures, such as Ethernet and Token Ring. These bridges appear as transparent bridges to an Ethernet host and as source-routing bridges to a Token Ring host.

## Advantages and Disadvantages of Bridges

1. Describe the following advantages of using bridges:
  - a. Bridges can extend a network by acting as a repeater.

- b. Bridges can reduce network traffic on a segment by subdividing network communications.
  - c. Bridges increase the available bandwidth to individual nodes because fewer nodes share a collision domain.
  - d. Bridges reduce collisions.
  - e. Some bridges connect networks using different media types and architectures.
2. Describe the following disadvantages of using bridges:
  - a. Because bridges do more than repeaters by viewing MAC addresses, the extra processing makes them slower than repeaters and hubs.
  - b. Bridges forward broadcast frames indiscriminately, so they do not filter broadcast traffic.
  - c. Bridges are more expensive than repeaters and hubs.
3. Explain that a broadcast storm occurs when two or more stations engage in the transmission of excessive broadcast traffic.

<b>Teaching Tip</b>	While some broadcasting is normal on networks, excessive broadcasting due to errors or malfunctioning NICs can seriously erode network performance and even bring a network to a halt.
---------------------	--

## Switches

1. Explain that switches operate at the Data Link layer of the OSI model and increase network performance by reducing the number of frames transmitted to the rest of the network.
2. Explain that a switch opens a virtual circuit between the source and the destination. This prevents communications between just two computers from being broadcast to every computer on the network or segment. This is called microsegmentation. Use Figure 2-7 to illustrate your explanation.
3. Mention that when two machines have a virtual circuit, they do not have to share the bandwidth with any other computers. Multiple virtual circuits can be in use at the same time, each with its own full bandwidth. This is called “switched bandwidth.”
4. Mention that when machines must share a wire and compete for available bandwidth with other machines, they experience contention.

<b>Teaching Tip</b>	Switches filter based on MAC addresses and build tables in memory just like bridges, but the switching table will have a mapping of switch port number to MAC address instead of bridge segment number to MAC address.
---------------------	--



## Advantages and Disadvantages of Switches

1. Describe the following advantages of using switches:
  - a. Switches increase available network bandwidth.
  - b. Switches reduce the workload on individual computers.
  - c. Switches increase network performance.
  - d. Networks that include switches experience fewer frame collisions because switches create collision domains for each connection (a process called microsegmentation).
  - e. Switches connect directly to workstations.
2. Describe the following disadvantages of using switches:
  - a. Switches are significantly more expensive than bridges.
  - b. Network connectivity problems can be difficult to trace through a switch.
  - c. Broadcast traffic may be troublesome.

## Routers

1. Explain that routers operate at the Network layer of the OSI model and provide filtering and network traffic control on LANs and WANs. They can connect multiple segments and multiple networks.
2. Define internetworks as networks connected by multiple routers.
3. Mention that routers are similar to switches and bridges in that they segment a network and filter traffic. Routers use the logical address.

## Physical vs. Logical Addresses

1. Explain that the MAC address is found at the Data Link layer of the OSI model and used by bridges and switches to make forwarding decisions within a network or subnetwork.
2. Explain that the IP address is the logical address when TCP/IP is used on an internetwork. Routers use the IP address to route packets to the correct network segment. Use Figure 2-8 to illustrate your explanation.

## Advantages and Disadvantages of Routers

1. Describe the following advantages of using routers:
  - a. Routers can connect different network architectures, such as Ethernet and Token Ring.
  - b. Routers can choose the best path across an internetwork using dynamic routing techniques.
  - c. Routers reduce network traffic by creating collision domains.
  - d. Routers reduce network traffic by creating broadcast domains.

2. Describe the following disadvantages of using routers:
  - a. Routers work only with routable network protocols; most but not all protocols are routable.
  - b. Routers are more expensive than other devices.
  - c. Dynamic router communications (inter-router communication) cause additional network overhead, which results in less bandwidth for user data.
  - d. Routers are slower than other devices because they must analyze a data transmission from the Physical through the Network layer.
3. Use Figure 2-9 to show how to use a router to connect a network to the Internet.

## **Brouters**

1. Define a brouter as a hybrid device that functions as both a bridge for nonroutable protocols and a router for routable protocols. It provides the best attributes of both a bridge and a router.
2. Mention that a brouter operates at both the Data Link and Network layers and can replace separate bridges and routers.

## **Gateways**

1. Explain that a gateway is usually a combination of hardware and software that translates between different protocol suites.
2. Explain that packets must be rebuilt not just at the lower levels but at the very upper levels so that the actual data content can be converted into a format the destination can process.
3. Mention that gateways have the most negative effect on network performance. Gateways create the most latency.

## **Ethernet Operations**

1. Define Ethernet as a network access method (or media access method) originated by the University of Hawaii, later adopted by Xerox Corporation, and standardized as IEEE 802.3 in the early 1980s.
2. Mention that today, Ethernet is the most commonly implemented media access method in new LANs.

## **CSMA/CD**

1. Explain that Carrier Sense Multiple Access with Collision Detection (CSMA/CD) is used by Ethernet to prevent data packets from colliding on the network. It allows any station connected to a network to transmit anytime there is not already a transmission on the wire.
2. Mention that after each transmitted signal, each station must wait a minimum of 9.6 microseconds before transmitting another frame. This is called the interframe gap (IFG), or interpacket gap (IPG).
3. Explain that two stations could listen to the wire simultaneously and not sense a carrier signal. In such a case, both stations might begin to transmit their data simultaneously. A collision would occur on the network wire.
4. The first station to detect the collision transmits a 32-bit jam signal that tells all other stations not to transmit for a brief period. The two stations that generated the collision enter a backoff period.
5. Define a collision domain as the physical area in which a frame collision might occur. Routers, switches, bridges, and gateways do segment networks and thus create separate collision domains.

## **Fast Ethernet**

1. Explain that Fast Ethernet (100BaseT) uses the same network access method (CSMA/CD) as common 10BaseT Ethernet, but provides 10 times the data transmission rate.
2. Mention that when you upgrade from 10BaseT to Fast Ethernet, all the network cards, hubs, and other connectivity devices that are now expected to operate at 100 Mbps must be upgraded.
3. Mention that Fast Ethernet is defined under the IEEE 802.3u standard.

## **Gigabit Ethernet**

1. Explain that Gigabit Ethernet (1000BaseX) is the next iteration of Ethernet, increasing the speed to 1000 Mbps. It is defined in the IEEE 802.3z standard.
2. Mention that Gigabit Ethernet can work in half-duplex mode through hubs, but this is not typical. Almost all applications of the standard are full-duplexed through switches.
3. Mention that 10 Gigabit Ethernet (10GBaseX, 10GbE or 10GigE) is the fastest of the Ethernet standards.

**Half- and Full-Duplex Communications**

1. Explain that in half-duplex communications, devices can send and receive signals, but not at the same time. In full-duplex communications, devices can send and receive signals simultaneously.
2. Mention that most Ethernet networks can use equipment that supports half- and full-duplex communications. Full-duplex communications use one set of wires to send and a separate set to receive.
3. Describe the following benefits of using full-duplex:
  - a. Time is not wasted retransmitting frames, because there are no collisions.
  - b. The full bandwidth is available in both directions because the send and receive functions are separate.
  - c. Stations do not have to wait until other stations complete their transmissions.

**Quick Quiz 2**

1. Networks connected by multiple routers are called \_\_\_\_ because they create a larger network of interconnected, smaller networks.  
Answer: internetworks
2. A(n) \_\_\_\_ functions as both a bridge for nonroutable protocols and a router for routable protocols.  
Answer: brouter
3. Fast Ethernet is defined under the IEEE \_\_\_\_ standard.  
Answer: 802.3u
4. In \_\_\_\_ communications, devices can send and receive signals, but not at the same time.  
Answer: half-duplex

**Class Discussion Topics**

1. What are the benefits of implementing a WLAN?
2. What are the advantages and disadvantages of using hybrid devices such as routers?

**Additional Projects**

1. Ask your students to read more about Wired Equivalent Privacy (WEP) and write a report describing its major weakness and how Wi-Fi Protected Access (WAP) and WAP2 solve it.

2. CSMA/CA is used in 802.11 based wireless LANs. Ask your students to read more about CSMA/CA and write a report explaining its most important characteristics. They should include the main differences between CSMA/CA and CSMA/CD used with Ethernet.

## **Additional Resources**

1. Network hub  
[http://en.wikipedia.org/wiki/Network\\_hub](http://en.wikipedia.org/wiki/Network_hub)
2. Wireless access point  
[http://en.wikipedia.org/wiki/Wireless\\_access\\_point](http://en.wikipedia.org/wiki/Wireless_access_point)
3. SSID - Service Set Identifier  
[http://compnetworking.about.com/cs/wireless/g/bldef\\_ssid.htm](http://compnetworking.about.com/cs/wireless/g/bldef_ssid.htm)
4. What is 802.1x?  
<http://www.networkworld.com/research/2002/0506whatisit.html>
5. Network bridge  
[http://en.wikipedia.org/wiki/Network\\_bridge](http://en.wikipedia.org/wiki/Network_bridge)
6. Network switch  
[http://compnetworking.about.com/od/hardwarenetworkgear/g/bldef\\_switch.htm](http://compnetworking.about.com/od/hardwarenetworkgear/g/bldef_switch.htm)

## **Key Terms**

- **100BaseFX** A Fast Ethernet implementation over multimode fiber-optic cabling. The maximum segment length is 412 meters.
- **100BaseT4** A 100-Mbps Fast Ethernet implementation that uses four pairs of either Category 3, 4, or 5 UTP cable. The maximum segment length is 100 meters.
- **100BaseTX** A Fast Ethernet implementation that uses two pairs of either Category 5 unshielded twisted-pair (UTP) or shielded twisted-pair (STP). 100Base-TX operates at 100 Mbps with a maximum segment distance of 100 meters.
- **1000BaseCX** An IEEE 802.3z Gigabit Ethernet implementation that uses balanced copper cabling to achieve 1000 Mbps.
- **1000BaseLX** An IEEE 802.3z Gigabit Ethernet implementation that uses single-mode fiber to achieve 1000 Mbps.
- **1000BaseSX** An IEEE 802.3z Gigabit Ethernet implementation that uses multimode fiber to achieve 1000 Mbps.
- **1000BaseT** An IEEE 802.3ab Gigabit Ethernet implementation that uses all four pairs of Category 5 or better UTP cable to achieve 1000 Mbps.
- **active hub** A device that connects multiple nodes and/or networks, is connected to external power, and repeats and regenerates signals on a network.
- **ad hoc mode** A wireless mode where client devices connect directly to each other without an access point.

- **amplifier** A device used to boost analog signals on a broadband network.
- **analog** A method of signal transmission on broadband networks.
- **attenuation** The natural degradation of a transmitted signal over distance.
- **backoff period** A random time interval used after a collision has been detected on an Ethernet network. Use of a backoff period minimizes the likelihood of another collision.
- **bandwidth** The available capacity of the network. The greater the network bandwidth, the greater the speed in data transfer.
- **Basic Service Set (BSS)** A wireless network with only one access point connected to a switch.
- **bridge** A device that operates at the Data Link layer, used to filter traffic between network segments by evaluating the MAC address of packets that are sent to it.
- **broadcast** A frame meant for the entire network.
- **broadcast domain** A group of network devices that will receive LAN broadcast traffic from each other.
- **broadcast storm** Excessive broadcast messages to every host on the network, launched by multiple computers; usually triggered by some error condition on the network.
- **brouter** A device that functions as a bridge for nonroutable protocols and a router for routable protocols. The brouter operates at both the Data Link and Network layers.
- **Carrier Sense Multiple Access with Collision Detection (CSMA/CD)** An access method specified by the IEEE Ethernet 802.3 standard. In this method, a node will listen to see if the line is clear and then, if the line is clear, send data. Two nodes may still send at the same time and cause a collision, in which case the two nodes will then perform the backoff algorithm.
- **carrier signal** A transmitted electromagnetic pulse or wave on the network wire that indicates a transmission is in progress.
- **collision domain** In Ethernet networking, a single segment on a network. Any station on the same physical segment or separated by a repeater is in the same collision domain. Bridges, routers, and switches (depending on how they are configured) can separate collision domains.
- **contention** The condition that occurs when computers on a network must share the available capacity of the network wire with other computers.
- **Ethernet** *See* **Carrier Sense Multiple Access with Collision Detection (CSMA/CD)**.
- **Fast Ethernet** Defined in IEEE 802.3u, and includes any of the following 100-Mbps Ethernet LAN technologies: 100Base-T4, 100Base-TX, 100Base-FX.
- **Extended Service Set (ESS)** A wireless network with multiple access points connected to switches. The access points are typically configured with the same network name (SSID) to facilitate roaming.
- **Extensible Authentication Protocol (EAP)** Works with 802.1x to carry the authentication information between the user, the access point, and the security server.
- **full-duplex** A connection that allows communication in two directions at once; common telephone connections are typically full-duplex because people can talk and listen at the same time.
- **gateway** A combination of hardware and software that translates between different protocols on a network.
- **Gigabit Ethernet** Includes IEEE 802.3z and IEEE 802.3ab, which allow for speeds up to 1000 Mbps.
- **10 Gigabit Ethernet (10GbE or 10 Gige)** A standard ten times faster than gigabit Ethernet that is always implemented as full duplex.

- **half-duplex** A connection that allows communication in two directions, but not simultaneously; the circuit can be used for sending or receiving bits in only one direction at a time.
- **hub** An active or passive device that connects network segments. Passive hubs are connection points; active hubs repeat and regenerate signals.
- **IEEE 802.1x** The IEEE standard that defines port switching designed to shut down a switch port to all frames unless they are authentication frames.
- **IEEE 802.11** The IEEE standard that defines wireless networking in the unlicensed frequency bands 2.4 GHz and 5 GHz.
- **IEEE 802.11i** The most robust wireless security standard in use today. It is based on Wi-Fi Protected Access version 2 (WPA2) which uses AES encryption, dynamic keys, and user authentication via 802.1x and EAP.
- **IEEE 802.3ab** The IEEE standard that defines the Gigabit Ethernet implementation 1000BaseT.
- **IEEE 802.3u** The IEEE standard that defines Fast Ethernet implementations, including 100Base-T4, 100Base-TX, and 100Base-FX.
- **IEEE 802.3z** The IEEE standard that defines Gigabit Ethernet implementations including 1000BaseCX, 1000BaseLX, and 1000BaseSX.
- **infrastructure mode** A wireless mode in which the access point is wired back into a switch so that the client has access to the LAN and WAN, not just the WLAN.
- **interframe gap (IFG)** The time required between the transmission of data frames on the network: 9.6 microseconds.
- **interpacket gap (IPG)** *See interframe gap.*
- **internetwork** A large network comprised of smaller interconnected networks.
- **IP address** A 32-bit binary address used on TCP/IP networks; consists of a host portion and a network portion.
- **jam signal** A 32-bit signal that is sent by the first station to detect a collision on an Ethernet network; ensures that all other stations are aware of the collision.
- **latency** A delay on a network caused by a variety of factors, including the addition of devices.
- **media access method** *See network access method.*
- **microsegmentation** The type of segmentation that occurs through the use of virtual circuits between switches and nodes. Each connection enjoys the total bandwidth. Bandwidth is not shared as it is through hubs.
- **network access method** The process by which network interface cards and devices communicate data on a network; an example is CSMA/CD. Also known as **media access method**.
- **node** A connection point or junction on the network. A node can be a terminal or computer connected to the network.
- **optical repeater** A network device that uses LEDs or diode lasers to amplify optical signals.
- **passive hub** A device that connects network segments but does not perform signal regeneration.
- **port** A connection point, usually for network cable, on a device such as a hub, bridge, switch, or router.
- **repeater** A device that repeats and cleans signals on the network and extends the usable distance of the network.

- **router** A device that connects multiple segments, subdivides a network, filters broadcast traffic, and maintains a routing table. A router uses the logical address to move data packets from point to point.
- **segment (noun)** A section of a network that has been subdivided by routers, switches, or bridges.
- **segment (verb)** To subdivide a network with a networking device, such as a bridge, switch, or router.
- **segmentation** The process of breaking a network into smaller broadcast or collision domains.
- **Service Set Identifier (SSID)** The network name configured on both the access point and the client so that they can communicate.
- **subnetwork** A portion of the network created by manipulating a network address and breaking it down into smaller parts.
- **switch** A device used between nodes on a network or between networks to create virtual circuits between two points. A switch increases bandwidth by isolating traffic between two points.
- **Token Ring** A networking method developed by IBM that organizes the network into a physical or logical ring. The token is a logical device, and because stations may only broadcast on the network when they have the token, traffic does not collide.
- **topology** The physical layout of network components. The topology can take the form of a ring, star, or bus.
- **virtual circuit** A private connection between two points created by a switch that allows the two points to use the entire available bandwidth between them without contention.
- **WEP (Wired Equivalent Privacy)** The initial wireless security standard that uses the RC4 algorithm with static key. This is now considered weak encryption.
- **WPA (Wi-Fi Protected Access)** The improvement to WEP. It provides better encryption with the TKIP algorithm and dynamic keys.
- **WPA2 (Wi-Fi Protected Access version 2)** The upgrade to WPA that provides the more robust AES algorithm for encryption as well as dynamic keys. Both WPA and WPA2 can be configured to use 802.1x/EAP.
- **wireless access point** A network device that contains a radio transceiver, which allows wireless clients to connect to a WLAN.
- **wireless local area network (WLAN)** A local area network consisting either entirely of wireless clients or a traditional LAN that contains wireless access points.