ADVANCED ETHERNET SWITCH OPERATION

Now that we have discussed basic Ethernet switch operation involved in frame forwarding, we will begin looking at additional aspects of Ethernet switch operation that are important in larger Ethernet networks.

The Rapid Spanning Tree Protocol (RSTP)

SINGLE POINTS OF FAILURE We have just seen that having only a single possible path between any two hosts allows rapid frame forwarding and, therefore, low switch cost. Unfortunately, having only a single possible path between any two computers also makes Ethernet vulnerable to **single points of failure**, in which the failure of a single component (a switch or a trunk line between switches) can cause widespread disruption.

Having only a single possible path between end hosts in a switched Ethernet network reduces cost, but it creates single points of failure, meaning that a single failure can cause widespread disruption.

To understand this, suppose that Switch 2 in Figure 5-24 fails. Then the hosts connected to Switch 1 will not be able to communicate with hosts connected to Switch 2 or Switch 3. For a second example, suppose that the trunk line between Switch 1 and Switch 2 fails. In this case, too, the network also will be broken into two parts.

Although the two parts of the network might continue to function independently after a failure, many firms put most or all of their servers in a centralized server room. In such firms, clients on the other side of the broken network would lose most of their ability to continue working. For example, in the figure, Client A1-44-D5-1F-AA-4C, which connects to Switch 1, cannot reach Server E5-BB-47-21-D3-56, which connects

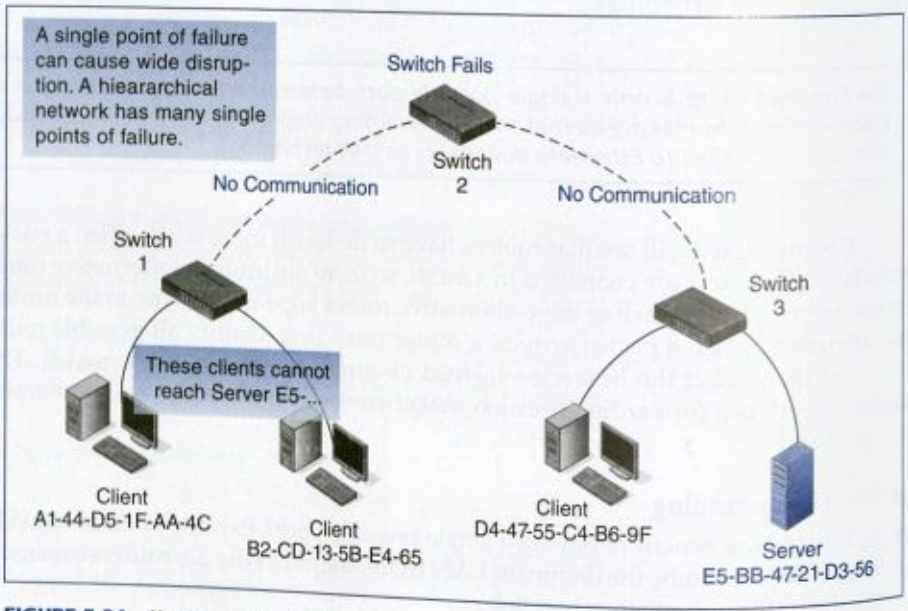

FIGURE 5-24 Single Points of Failure

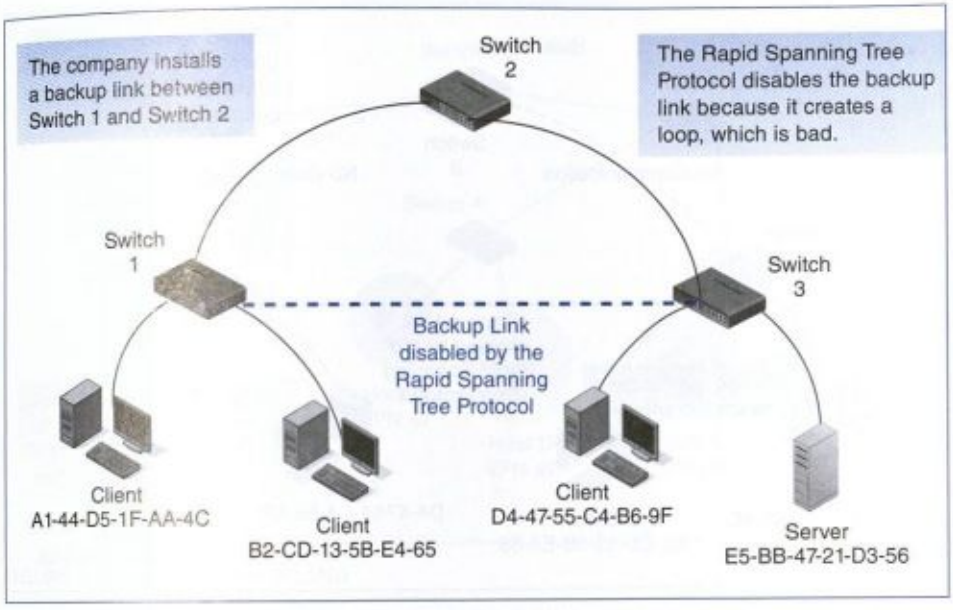

FIGURE 5-25 Backup Link and the Rapid Spanning Tree Protocol (RSTP)

to Switch 3. External connections also tend to be confined to a single network point for security reasons. Computers on the wrong side of the divide after a breakdown would lose external access.

THE RAPID SPANNING TREE PROTOCOL (RSTP) The traditional way to deal with single points of failure is to install backup links. This installs **redundancy**, which means that there is more than one way to connect a pair of switches or a pair of hosts. Redundancy increases **reliability**, which is the probability that connections will be made.

In Figure 5-25, the company has installed a transmission link between Switch 1 and Switch 3. As the figure shows, this creates a loop among the three switches. Loops create serious problems in Ethernet. Fortunately, there is a standard to detect and break loops in Ethernet networks. This is the **Rapid Spanning Tree Protocol (RSTP)**, 802.1w.[7] In the figure, RSTP has deactivated the backup link.

What happens if there is a failure? Switches will exchange messages via RSTP. As Figure 5-26 shows, they will agree to disable the links between Switch 2 and the other two switches. They will also agree to reactivate the backup link. Now, the two clients on the left can reach Server E1-... on the right.

Although RSTP was created to detect and break loops, using it to reactivate backup links is rather tricky. When a loop occurs, the switches hold a backup election to pick a root (top level) switch. They then create a hierarchy beneath it. To ensure that the restored hierarchy is the one the company wants to have, the networking staff must "rig the election." It does this by setting certain parameters on each switch. This is easy if there is a single backup link. If there are many backup links, this is very difficult.

[7]There was an earlier standard, the Spanning Tree Protocol (802.1D), which is now deprecated because of its slow operation.

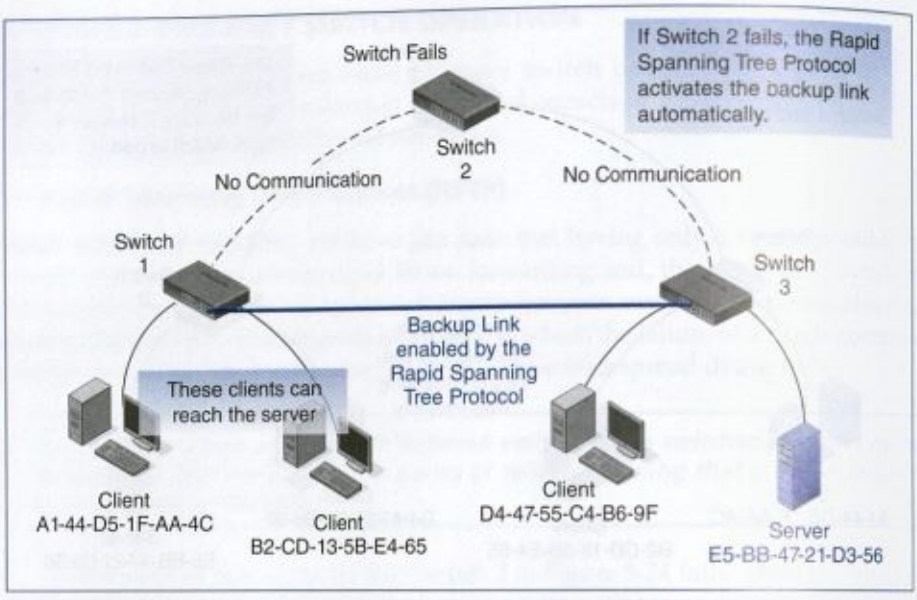

FIGURE 5-26 Reactivating a Backup Link in Ethernet with the Rapid Spanning Tree Protocol

Test Your Understanding

19. a) What is a single point of failure? b) Why is having a single possible path between any two hosts in an Ethernet network dangerous? c) What is the traditional way to address this problem? How does it bring redundancy? How does it improve reliability? d) What standard allows backup links for redundancy in Ethernet networks? e) Is it easy or difficult to create backup links effectively with RSTP?

Virtual LANs and Ethernet Switches

VLANS In a normal Ethernet network, any client can send frames to any server, and any server can reach any client. However, many Ethernet switches can now create virtual LANs. As Figure 5-27 shows, virtual LANs (VLANs) are groups of clients and servers that are allowed to communicate with each other but not with clients or servers on other VLANs.[8] In the figure, clients and servers in VLAN 3 (indicated by blue rectangles) cannot communicate with clients and servers on VLAN 47 (indicated by ellipses).

Virtual LANs (VLANs) are groups of clients and servers that are allowed to communicate with each other but not with clients or servers on other VLANs.

CONGESTION REDUCTION VLANs are used for two main reasons. First, some servers tend to **broadcast** frames to all clients. (One reason for the server to do this is to advertise its availability to its clients every 30 seconds or so.) In a large network, this broadcasting can create a great deal of congestion. With VLANs, however, the server will not flood the entire network with traffic; the frames will go only to the clients on the server's VLAN.

[8] What if a client on one VLAN needs to communicate with a server on another VLAN? The client must reach the server through a router. Routers connect different VLANs just as they connect different physical LANs.

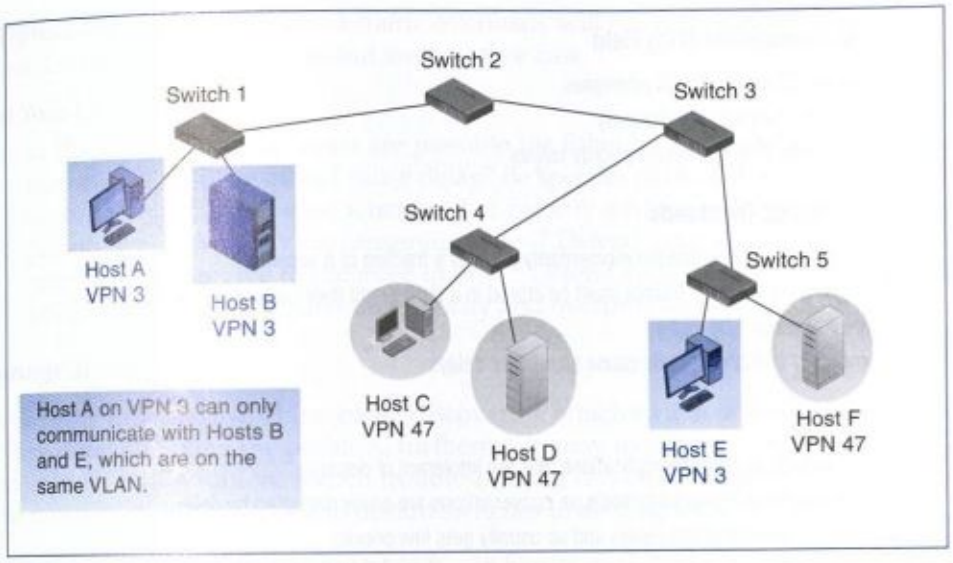

FIGURE 5-27 Virtual LANs (VLANs)

SECURITY A second reason for using VLANs is security. If clients on one VLAN cannot reach servers on other VLANs, they cannot attack these servers. In addition, if a client becomes infected with a virus, it can only pass the virus on to other clients and servers on its own VLAN.

THE 802.1Q VLAN STANDARDS To address VLAN standardization, the 802.3 Working Group extended the Ethernet frame through the **802.1Q** standard. This standard adds two optional tag fields after the address fields, as shown in Figure 5-20.

802.1Q is the standard for frame tagging.

The first tag field is the **Tag Protocol ID** field, which simply indicates that this is a tagged frame. The second tag field is the **Tag Control Information** field. This field contains a 12-bit VLAN ID that the sender sets to 0 if the firm does not use VLANs. If the firm does use VLANs, the frame is given a VLAN number. With the exclusion of 0 values, there are $2^{12} - 1$ (4,095) possible VLANs. This is sufficient for almost all corporate LANs.

Tagging is used for more than VLANs. The TCI field also has three priority bits. This gives up to eight (2^3) priority levels. Frame tagging is necessary to do priority-based switching in Ethernet.

Test Your Understanding

20. a) What is a VLAN? b) What two benefits do VLANs bring? c) How do VLANs bring security? d) When VLANs or priority is used, what two fields does the 802.1Q standard add to Ethernet frames? e) When VLANs are used, what does the Tag Protocol ID field tell a receiving switch or NIC? f) What information does the tag control information field tell the switch or receiver? g) In Figure 5-27, what server or servers can Host A communicate with? h) In Figure 5-27, what server or servers can Host C communicate with?

Tag Control Information (TCI) Field

There are 12 bits for VLAN addresses
There are 3 bits for frame priority
This permits $2^3 = 8$ different priority values

Momentary Traffic Overloads

Switches may be overloaded momentarily (usually a fraction of a second)
During this time, some frames must be stored in a buffer until they can be processed
Some frames will be lost
Momentary traffic overloads cause significant delays

Priority Levels

Higher priority is given to applications that are intolerant of displays
Voice must have high priority because conversations are easily disrupted by delays
E-mail can tolerate slight delays and so usually gets low priority

Overprovisioning

An alternative to using priority is to install much more switch processing speed than needed
Momentary traffic overloads will be extremely rare
Overprovisioning is more expensive, but priority requires more labor

FIGURE 5-28 Priority and Overprovisioning (Study Figure)

Priority

We have just seen that 12 of the bits in the Tag Control Information field are used for VLANs. Another three bits are used to allow switches to give priority to certain types of traffic. This gives 8 (2^3) possible priority levels. If two frames arrive at a switch at the same time, the frame with the higher **priority** number in the Tag Control Information field will be sent out first.

If the switch has enough capacity to handle all the traffic, priority is not important. However, if the switch is overloaded, it will not have enough capacity to handle all traffic. Each switch has a certain amount of storage called the buffer. During traffic overloads, the frames that cannot be processed will be held in the buffer until they can be processed. Typically, traffic overloads last only fractions of a second, so frames in the buffers are delayed but not lost. However, if the overload lasts too long, the buffer will overflow, and frames will be lost. If applications are using TCP, the lost packet will be retransmitted, but this will add considerable delay. It will also to the congestion.

Frames are given priority levels based on their **delay intolerance**. Voice traffic is intensely intolerant of delay. If there is even slight delay, it will be impossible for the two people to carry on a conversation. Consequently, voice traffic is given very high priority. In contrast, it rarely matters if e-mail is delayed by a few seconds. Consequently, e-mail is usually given low priority.

Priority must be managed, and this increases labor cost. Many firms simply buy much faster Ethernet switches than they will normally need. This is called

overprovisioning. It ensures that traffic overloads will be so rare that they can be ignored. This raises hardware cost but lowers labor cost.

Test Your Understanding

21. a) How many priority levels are possible for Ethernet switches? b) Why does a momentary traffic overload cause delay? Be specific. c) How does priority reduce delay? d) What determines what level of priority a frame will be given? e) What priority would you give to streaming video? Defend your decision. f) What priority would you give to database queries? Defend your decision. g) What is the trade-off between implementing priority and overprovisioning?

Manageability

If there is an Ethernet switch problem, discovering which switch is malfunctioning can be very difficult. Fixing the problem, furthermore, may require traveling to the switch to change its configuration. Switch troubleshooting can be very expensive, especially if the network staff must travel to distant switches to do diagnostics or configuration.

MANAGED SWITCHES AND THE MANAGER As Figure 5-29 shows, a company can mitigate these problems by using **managed switches**. As the name suggests, these switches have sufficient intelligence to be managed from a central computer called the **manager**. In most cases, management communication uses the Simple Network Management Protocol (SNMP) that we introduced in Chapter 4.

POLLING AND PROBLEM DIAGNOSIS Every few seconds, the SNMP **manager** polls each managed switch. In the poll, it asks each switch for a certain set of configuration parameters. The manager places all of this information in a **management information base (MIB)**.

If a problem occurs, the manager can discover quickly which switches are not responding and so can narrow down the source of the problem. In many cases, the configuration data collected from the switches can pinpoint the cause of a problem. Polling uses the **Get** command, which asks for information about the switch.

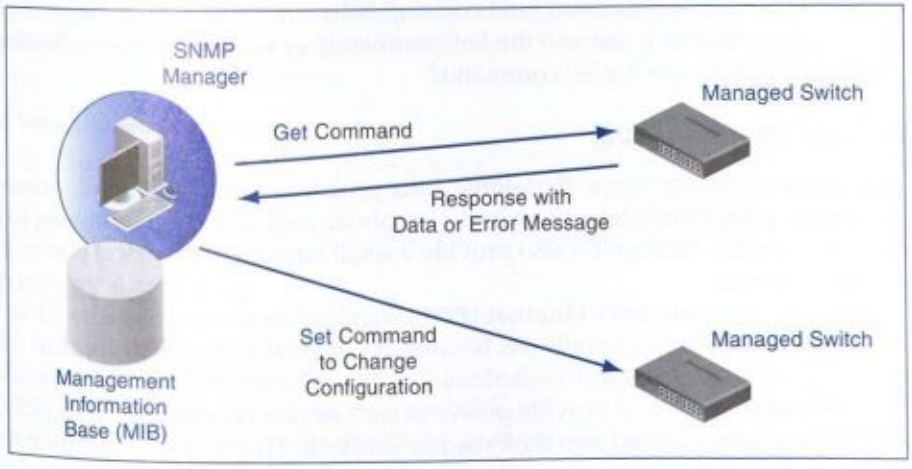

FIGURE 5-29 Managed Switches and the Manager

FIXING SWITCHES REMOTELY In some cases, the network administrator can use the manager to fix switch problems remotely by sending **Set** commands to the switch. The set command tells the switch to change one of its settings. For example, a Set command might tell the switch to turn off a certain port or to test a port that is suspected of malfunctioning. For instance, the manager can command the switch to do a self-test diagnostic. To give another example, the manager can tell the switch to turn off a port suspected of causing problems.

PERFORMANCE SUMMARY DATA At the broadest level, software can search through the SNMP manager's data and can present the status data to the network administrator in summarized form, giving the administrator a good indication of how well the network is functioning and of whether changes will be needed to cope with expected traffic growth.

THE COST SAVINGS OF MANAGEABILITY Managed switches are much more expensive to buy than nonmanaged switches. However, central management slashes network management labor, which is considerable. This labor cost reduction usually far offsets the higher switch purchase costs. The main benefit of network management, then, is to reduce overall costs.

Managed switches are more expensive than nonmanaged switches, but they reduce management labor in large networks enough to more than offset managed switch purchase costs. Managed switches reduce overall costs.

SECURITY A company's security level has a major impact on whether the Set command is used. Set is inherently dangerous because if an attacker can use it, he or she can disable switches and do other damage. In contrast, while Get can help an attacker find information needed for an attack, it is inherently less dangerous than Set because it only supplies information. Unless a company has very strong security, it must disable the Set command on all of its managed switches. This means that it must forgo the cost savings of remote reconfiguration.

Test Your Understanding

22. a) What are managed switches? b) What benefits do they bring? c) Do managed switches increase or decrease total costs? d) Why does a company's security level determine whether it can use the Set command? e) What are the implications of not being able to use the Set command?

Power over Ethernet (POE)

The telephone company wires that come into your home bring a small amount of power. You can plug a basic telephone into a telephone wall jack without having to plug it into a power outlet. USB cables also provide a small amount of electrical power to the devices they connect.

Similarly, the **power over Ethernet (POE)** standard can bring power to RJ-45 wall jacks. POE is important to corporations because it can greatly simplify electrical wiring for installing voice over IP (VoIP) telephones, wireless access points, and surveillance cameras. Instead of having to provide power to each device via electrical wall jacks, the device can simply be plugged into the Ethernet wall jack. This may not seem like much, but given all of the low-power devices in networks today, the total cost savings of using the existing physical Ethernet plant to power many devices is considerable.

Power over Ethernet (POE)

Switches can supply power to devices connected by UTP
(Wired telephone systems and USB ports already do this)
This may be much less expensive than supplying power separately

Latest POE Standard

Provides up to 25 Watts to attached devices
Sufficient for most wireless access points
Sufficient for VoIP phones
Sufficient for surveillance cameras
Sufficient for tablets
Not sufficient for desktop or notebook PCs

The Future

Nonstandard products now supply 60 Watts of power
May become a future standard
Still will not be enough for desktop or notebook PCs

POE switches

New switches can be purchased with POE
Companies can also add POE equipment to an existing non-POE switch

FIGURE 5-30 Power over Ethernet (POE) (Study Figure)

The POE standard currently is limited to 25 Watts of power.[9] Some nonstandard powered switches already raise this to 60 Watts, and these higher power levels may appear in future versions of the POE standard. However, both POE and nonstandard POE are only sufficient for low-power devices. POE does not provide enough power for desktop PCs or even laptop computers.

Companies that wish to supply power through their RJ-45 wall jacks will have to install either new switches compatible with the POE standard or modification kits that can add POE to existing switches.

Test Your Understanding

23. a) What is POE? b) Why is POE attractive to corporations? c) What maximum standard power does the POE standard specify? d) For what types of devices is POE sufficient? e) Is POE sufficient for desktop computers and most notebook computers?

ETHERNET SECURITY

Until recently, few organizations worried about the security of their wired Ethernet networks, presumably because only someone within the site could get access to the network, and security should be strong within the site. Unfortunately, experience has shown that attackers can easily get into sites, especially if a site has public areas. Once

[9] Technically, the standard that specifies 25 Watts is POE Plus. The original standard was simply POE.

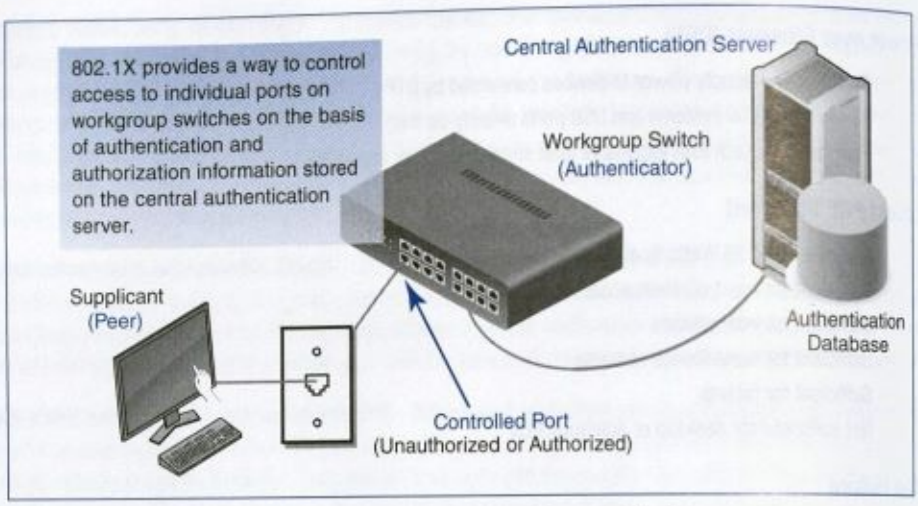

FIGURE 5-31 802.1X Port-Based Access Control on an Ethernet Switch

into the site network, the attacker does not have to worry about the border firewall. He or she is *inside* the border firewall.

Port-Based Access Control (802.1X)

To thwart the ability of attackers to simply plug into the internal network, companies can implement **802.1X**, which is a standard for **Port-Based Access Control** on the workgroup switches that give users access to the network. Quite simply, a switch port will not allow the computer attached to the port to send traffic other than authentication traffic until the computer has authenticated itself.

Figure 5-31 illustrates 802.1X. The workgroup switch is called the **authenticator**. It gets this name because the workgroup switch provides authentication service to the supplicant computer. The 802.1X standard normally also uses a central **authentication server** to do the actual supplicant credentials checking.

When the supplicant host transmits its authentication credentials (password, etc.), the authenticator passes these credentials on to the authentication server. The authentication server checks these credentials against its authentication database. If the authentication server authenticates the credentials, it sends back a confirmation to the workgroup switch. The workgroup switch then allows the supplicant PC to send frames to other devices in the network.

Using a central authentication server provides four benefits.

- ***Switch Cost.*** First, having the central authentication server check credentials instead of having the switch doing this minimizes the processing power needed in the workgroup switch. Given the large number of workgroup switches, this can produce a major cost saving.
- ***Consistency.*** Second, having all credentials on the authentication server gives consistency in authentication. An attacker cannot succeed by trying many different workgroup switches until he or she finds one that is misconfigured and gives the attacker access.

- *Reduced Management Cost.* Third, management cost is reduced because credentials only need to be changed on the central authentication server when user authentication information is changed when a user joins the firm, leaves the firm, or needs other credential changes.
- *Rapid Changes.* Fourth, the credentials of individuals who are fired or suspended can be invalidated in seconds, on all workgroup switches.

Security Standards Come from the 802.1 Working Group

Note from its name that the 802.1X standard was created by the *802.1* Working Group, not by the *802.3* Working Group that creates Ethernet standards. The 802.1 Working Group produces standards that cut across all 802 network technologies. This includes security standards.

Test Your Understanding

24. a) What threat does 802.1X address? b) How does the standard address the threat? c) In 802.1X, what device is the authenticator? d) What are the benefits of using a central authentication server instead of having the individual authenticators do all authentication work?

802.3ba: 40 Gbps and 100 Gbps Ethernet

This chapter talked briefly about 40 Gbps and 100 Gbps Ethernet, which were standardized in 2010 as 802.3ba. In this box, we will look at 802.3ba in a little more detail.

For most organizations, 10 Gbps is adequate for their current LAN requirements. However, a few firms are pushing the limits of this technology. Internet service providers (ISPs), which carry the Internet's backbone traffic, are already being squeezed by 10 Gbps speeds. So are some other industry sectors, such as financial services. Most firms, however, are more interested in 802.3ba as a way to reduce costs, especially where link aggregation is being used on trunk links that require multiple 10GBASE-x connections.

The speed of 100 Gbps is a normal expectation based on earlier Ethernet developments, which grew by a factor of 10 with each new standard. The speed of 40 Gbps is used primarily in wide area networking, which we will look at in Chapter 10.

At the data link layer, the IEEE was able to keep everything the same as in earlier standards. This includes the MAC layer frame structure and minimum and maximum frame sizes. At the physical layer, however, the situation is very different.

The 802.3ba standard uses the concept of *lanes*. The **virtual lane** is the entire 100 Gbp or 40 Gbps transmission path. It is called a virtual lane because the physical situation is more complex. Ports on different devices may be connected by multiple optical fiber transmission lines, each being called a **media lane**. In other words, the 100 Gbps virtual lane can consist of several slower media lanes.

For LANs, the most important 100 Gbps standard in the short run is likely to be 100GBASE-SR10. The 100G indicates that the speed is 100 Gbps. The S indicates that short-wavelength light is used (850 nm). The R denotes how the bits are packaged in terms of data and control bits. (We will not look at this issue). Finally, the 10 indicates that there are 10 media lanes.

In practice, 100GBASE-SR10 connects ports on different devices with 24 optical fibers! Ten are used for transmission *in each direction*, with each fiber carrying data at 10 Gbps. In addition, there are an extra two fibers for transmission in each direction. These are called **dark fibers** in the

(continued)

sense that they normally are not used. However, if one of the used fibers goes bad, the sender will turn on one of the two dark fibers going in that direction.

This seems rather unwieldy, but when 24 fibers are packed into a single cord, the resulting cord is still quite thin. In addition, there is only a single connector at each end of the fiber cable. It simply snaps in place like a traditional connector. Of course, the connector is a bit larger than traditional connectors, but it is only about twice as wide. The 24 fibers, being so thin, can be packed closely together in the connector as well as in the cord.

An obvious question is, "Hey, isn't this just trunking in disguise?" The answer is, "Sort of." Both use multiple physical connections for a single logical connection. However, traditional trunking is somewhat costly to manage, and ten 10 Gbps ports are expensive. By requiring only a single port at each end and by automatically handling the virtual lane's multiple media lanes, 100GBASE-SR10 is attractive economically. 100GBASE-SR10 should also reduce power requirements. This will save money both directly in each device and indirectly by lowering air conditional costs for equipment rooms.

It is important to recognize that the physical layer standards that have already been defined should be viewed as "Generation 1" devices. Over time, new options will appear. For example, if each media lane's speed can be increased to 25 Gbps instead of 10 Gbps, only four media lanes would be recovered, so only 10 fibers would be needed, including a dark fiber in each direction. In addition, 100GBASE-SR10 is currently limited to 100 to 125 meters, even over very good optical fiber. Maximum distance is likely to grow in the future.

Test Your Understanding

25. a) What is likely to be the main standard for 100 gigabit per second Ethernet? b) At what speed does 100GBASE-SR10 operate? c) What is the speed of the 100GBASE-SR10 virtual lane? d) What is the speed of an individual 100GBASE-SR10 media lane? e) How many optical fibers does 100GBASE-SR10 require? f) How many connectors does 100GBASE-SR10 require at each device? g) Why is 100GBASE-SR10 better than simply trunking ten 10GBASE-SX connectors on each device? (Explain your answer.) h) How are 100 Gbps standards likely to change for LANs as technology matures?

CONCLUSION

Synopsis

In this chapter, we looked at Ethernet switched wired LANs. In contrast to wide area networks (WANs), LANs are inexpensive per bit transmitted, so organizations can afford to provide extremely high-speed LAN service. There once were several switched wired LAN technologies, but Ethernet, which is standardized by the IEEE 802 Committee's 802.3 Working Group, is the only significant switched wired LAN technology.

All LANs are governed by physical and data link layer standards. We began by looking at physical layer standards—specifically at binary and digital signaling, which give resistance to transmission error. Ethernet uses two major transmission media. Four-pair unshielded twisted pair (4-pair UTP) dominates transmission between hosts and the workgroup switches they connect to. Optical fiber, which can span longer distances, is used primarily to link switches to other switches. LANs use inexpensive multimode fiber, which can span distances up to about 500 meters, which is sufficient for LANs. Carriers use more expensive single-mode fiber. Normally, a single UTP or optical fiber link connects a pair of switches. However, with link aggregation (also called bonding), a pair of switches can be connected by two or more UTP or fiber links. Ethernet has many physical layer standards for both UTP and optical fiber. Standards set both transmission

speed and maximum distance. They allow network designer to select media standards for specific media runs within the customer premises. For UTP, quality levels are indicated by category numbers. Today, Category 5e, 6, and 6A wiring are dominant.

We looked in some depth at Ethernet's frame organization. The Ethernet frame has many fields. The first helps synchronize the receiver's clock with the sender's clock. The source and destination MAC addresses are 48 bits long and are expressed for human consumption in hexadecimal notation. The final field is used for error checking. Ethernet does error detection but merely discards incorrect frames. There is no error correction, so Ethernet is an unreliable protocol. The data field has two subfields. The first is the logical link control (LLC) subheader, which specifies the type of packet contained in the data field. The second is the packet itself—usually an IP packet, although other types of packets can be carried. The length field specifies the length of the overall data field. There are two optional tag fields used for priority and virtual LAN operations.

We looked at how Ethernet switches forward frames. Ethernet networks must be organized as a hierarchy, in which there are no loops among the switches. Consequently, there is only a single path between any two hosts. This makes Ethernet switching tables very simple, so Ethernet switches are both fast and inexpensive.

Although basic Ethernet switch forwarding is simple, large Ethernet networks add complications to this basic operation. In a hierarchical LAN, a single point of failure, such as a transmission link or switch, can isolate client hosts from server hosts. Backup links would solve this problem but would create loops that would destroy the strict hierarchy. The Rapid Spanning Tree Protocol allows backup links to be installed but to be activated only if there is a break in the hierarchy.

In a basic Ethernet network, any host can reach any other host. However, advanced Ethernet switches can subdivide the physical LAN into multiple virtual LANs (VLANs) whose hosts can talk to one another but cannot talk to hosts on other VLANs. This provides a measure of security.

Another capability is priority. Different frames can be given different priority levels. If a switch is overloaded, high-priority frames will be sent first. Priority is important for applications that are intolerant of latency (delay). It will allow the frames of these applications to be sent on with minimal delay.

An important capability is switch manageability. Manageable switches can be controlled by a central network manager. This allows the manager to get information from the switches. It also allows the manager to change the configuration of switches. Although managed switches are substantially more expensive than basic switches, they reduce management costs more than enough to offset these purchase costs. Only recent versions of the Simple Network Management Protocol have good security, and even this security can be overcome by lazy network administrators.

When you use a wired telephone at home and the power fails, you can still make and receive calls. This is because the telephone network provides enough power to operate the phone. In an analogous way, the power over Ethernet (POE) standard provides a certain amount of electrical power to each switch port. This allows simple devices such as access points to receive power from the switch instead of requiring a separate power connection, which might be expensive to install.

Ethernet security has not been seen as a major issue in most firms. However, we reviewed the 802.1X standard that requires a host to authenticate itself to a switch port before it is allowed to use the network. This prevents attackers from walking into a firm and simply plugging into any Ethernet wall jack. In 802.1X, the host is called a peer,

the switch is the authenticator, and there is a back-end authenticator server that keeps authentication credentials. Having a central authentication server that keeps authentication data and makes authentication decisions reduces the work that must be done by the switch. This minimizes switch cost. Centralizing authentication data and decisions on the authentication server also brings consistency to authentication, reduces management labor, and allows the status of individual users to be changed instantly. Note that this security standard comes from the 802.1 Working Group, not the 802.3 Working Group.

The box at the end of this chapter provided more information on the Ethernet 802.3ba standard for 40 Gbps and 100 Gbps Ethernet. There was an important distinction between the 100 Gbps virtual lane between two devices and the multiple slower media lanes over which the signals are carried. The 802.3ba standard essentially does very elegant and simpler trunking between two devices.

END-OF-CHAPTER QUESTIONS

Thought Questions

1. With power over Ethernet, what is the potential danger to users in having powered switch ports? How do you think this danger might be avoided?
2. When would the optional Tag fields in the Ethernet frame be added?
3. The Length field is 22. a) How long is the combined data field and PAD? b) How long is the PAD?

Design Questions

1. Design an Ethernet network to connect a single client PC to a single server. The two devices are 410 feet apart. They need to communicate at 800 Mbps. Your design will specify the locations of switches and the transmission line between the switches.
2. Add to your design in the previous question. Add another client next to the first client. This client will also communicate with the server and will also need 800 Mbps in transmission speed. Again, your design will specify the the locations of switches and the transmission line between the switches.

Troubleshooting Question

1. You are connecting two switches in a large Ethernet switch with 32 switches. You are using 4-pair UTP. Suddenly, transmissions cannot travel over the network. What do you think might have happened? If you cannot come up with a good solution, reread the synopsis and see which points might apply.

Perspective Questions

1. What was the most surprising thing you learned in this chapter?
2. What was the most difficult part of this chapter for you?

5a HANDS-ON: CUTTING AND CONNECTORIZING UTP[1]

INTRODUCTION

Chapter 5 discussed UTP wirsing in general. This chapter discusses how to cut and connectorize (add connectors to) solid UTP wiring.

SOLID AND STRANDED WIRING

Solid-Wire UTP versus Stranded-Wire UTP

The TIA/EIA-568 standard requires that long runs to wall jacks use **solid-wire UTP**, in which each of the eight wires really is a single solid wire.

However, patch cords running from the wall outlet to a NIC usually are **stranded-wire UTP**, in which each of the eight "wires" really is a bundle of thinner wire strands. So stranded-wire UTP has eight bundles of wires, each bundle in its own insulation and acting like a single wire.

Relative Advantages

Solid wire is needed in long cords because it has lower attenuation than stranded wire. In contrast, stranded-wire UTP cords are more flexible than solid-wire cords, making them ideal for patch cords—especially the one running to the desktop—because they can be bent more and still function. They are more durable than solid-wire UTP cords.

Adding Connectors

It is relatively easy to add RJ-45 connectors to solid-wire UTP cords. However, it is very difficult to add RJ-45 connectors to stranded-wire cords. Stranded-wire patch cords should be purchased from the factory precut to desired lengths and preconnectorized.

In addition, when purchasing equipment to connectorize solid-wire UTP, it is important to purchase crimpers designed for solid wire.

CUTTING THE CORD

Solid-wire UTP normally comes in a box or spool containing 50 meters or more of wire. The first step is to cut a length of UTP cord that matches your need. It is good to be a little generous with the length. This way, bad connectorization can be fixed

[1]This material is based on the author's lab projects and on the lab project of Professor Harry Reif of James Madison University.

Solid-Wire UTP

- Each of the eight wires is a solid wire
- Low attenuation over long distances
- Easy to connectorize
- Inflexible and stiff—not good for runs to the desktop

Stranded-Wire UTP

- Each of the eight "wires" is itself several thin strands of wire within an insulation tube
- Flexible and durable—good for runs to the desktop
- Impossible to connectorize in the field (bought as patch cords)
- Higher attenuation than solid-wire UTP—Used only in short runs
  - From wall jack to desktop
  - Within a telecommunications closet (see Chapter 3)

FIGURE 5a-1 Solid-Wire and Stranded-Wire UTP (Study Figure)

by cutting off the connector and adding a new connector to the shortened cord. Also, UTP cords should never be subjected to pulls (strain), and adding a little extra length creates some slack.

STRIPPING THE CORD

Now the cord must be stripped at each end using a **stripping tool** such as the one shown in Figure 5a-2. The installer rotates the stripper once around the cord, scoring (cutting into) the cord jacket (but not cutting through it). The installer then pulls off the scored end of the cord, exposing about 5 cm (about 2 in.) of the wire pairs.

It is critical not to score the cord too deeply, or the insulation around the individual wires may be cut. This creates short circuits. A really deep cut also will nick the wire, perhaps causing it to snap immediately or later.

WORKING WITH THE EXPOSED PAIRS

Pair Colors

The four pairs each have a color: orange, green, blue, or brown. One wire of the pair usually is a completely solid color. The other usually is white with stripes of the pair's color. For instance, the orange pair has an orange wire and a white wire with orange stripes.

Untwisting the Pairs

The wires of each pair are twisted around each other several times per inch. These must be untwisted after the end of the cord is stripped.

Ordering the Pairs

The wires now must be placed in their correct order, left to right. Figure 5a-3 shows the location of Pin 1 on the RJ-45 connector and on a wall jack or NIC.

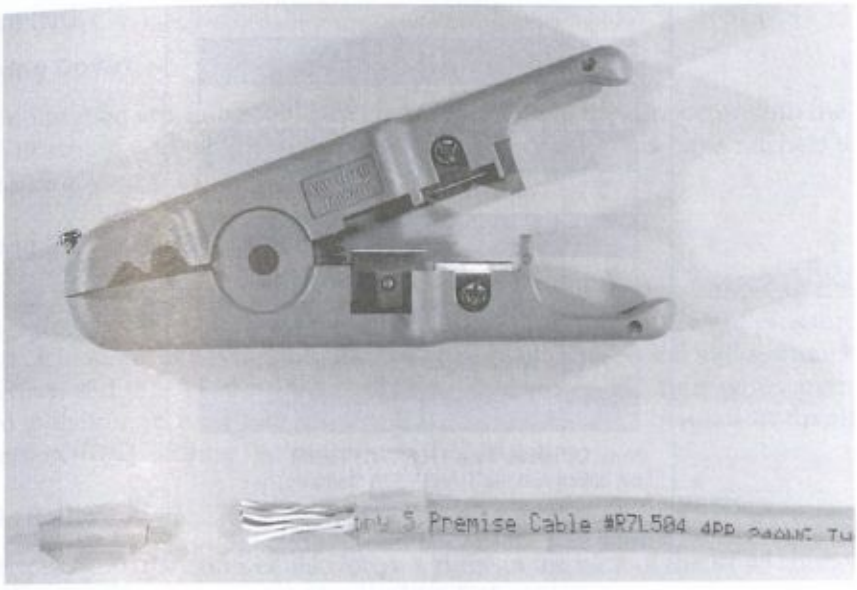

FIGURE 5a-2 Stripping Tool

Source: Courtesy of Raymond R. Panko

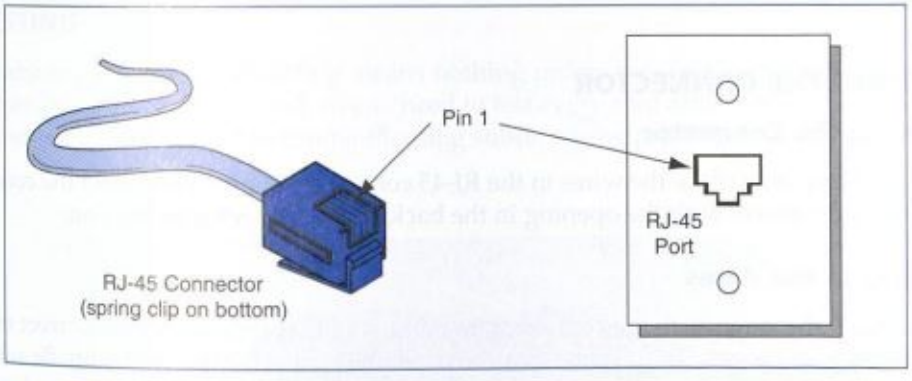

FIGURE 5a-3 Location of Pin 1 on an RJ-45 Connector and Wall Jack or NIC

Which color wire goes into which connector slot? The two standardized patterns are shown in Figure 5a-4. The T568B pattern is much more common in the United States.

The connectors at both ends of the cord use the same pattern. If the white-orange wire goes into Pin 1 of the connector on one end of the cord, it also goes into Pin 1 of the connector at the other end.

Cutting the Wires

The length of the exposed wires must be limited to 1.25 cm (0.5 in.) or slightly less. After the wires have been arranged in the correct order, a cutter should cut across the wires to make them this length. The cut should be made straight across, so that all

Pin*	T568A	T568B
1	White-Green	White-Orange
2	Green	Orange
3	White-Orange	White-Green
4	Blue	Blue
5	White-Blue	White-Blue
6	Orange	Green
7	White-Brown	White-Brown
8	Brown	Brown

Note: Do not confuse T568A and T568B pin colors with the TIA/EIA-568 Standard.

FIGURE 5a-4 T568A and T568B Pin Colors

wires are of equal length. Otherwise, they will not all reach the end of the connector when they are inserted into it. Wires that do not reach the end will not make electrical contact.

ADDING THE CONNECTOR

Holding the Connector

The next step is to place the wires in the RJ-45 connector. In one hand, hold the connector, clip side down, with the opening in the back of the connector facing you.

Sliding in the Wires

Now, slide the wires into the connector, making sure that they are in the correct order (white-orange on your left). There are grooves in the connector that will help. Be sure to push the wires all the way to the end or proper electrical contact will not be made with the pins at the end.

Before you crimp the connector, look down at the top of the connector, holding the tip away from you. The first wire on your left should be mostly white. So should every second wire. If they are not, you have inserted your wires incorrectly.[2]

Some Jacket Inside the Connector

If you have shortened your wires properly, there will be a little bit of jacket inside the RJ-45 connector.

[2]Thanks to Jason Okumura, who suggested this way of checking the wires.

CRIMPING

Pressing Down

Get a really good **crimping tool** (see Figure 5a-5). Place the connector with the wires in it into the crimp and push down firmly. Good crimping tools have ratchets to reduce the chance of your pushing down too tightly.

Making Electrical Contact

The front of the connector has eight pins running from the top almost to the bottom (spring clip side). When you **crimp** the connector, you force these eight pins through the insulation around each wire and into the wire itself. This seems like a crude electrical connection, and it is. However, it normally works very well. Your wires are now connected to the connector's pins. By the way, this is called an **insulation displacement connection** (IDC) because it cuts through the insulation.

Strain Relief

When you crimp, the crimper also forces a ridge in the back of the RJ-45 connector into the jacket of the cord. This provides **strain relief**, meaning that if someone pulls on the cord (a bad idea), he or she will be pulling only to the point where the jacket has the ridge forced into it. There will be no strain where the wires connect to the pins.

TESTING

Purchasing the best UTP cabling means nothing unless you install it properly. Wiring errors are common in the field, so you need to test every cord after you install it. Testing is inexpensive compared to troubleshooting subtle wiring problems later.

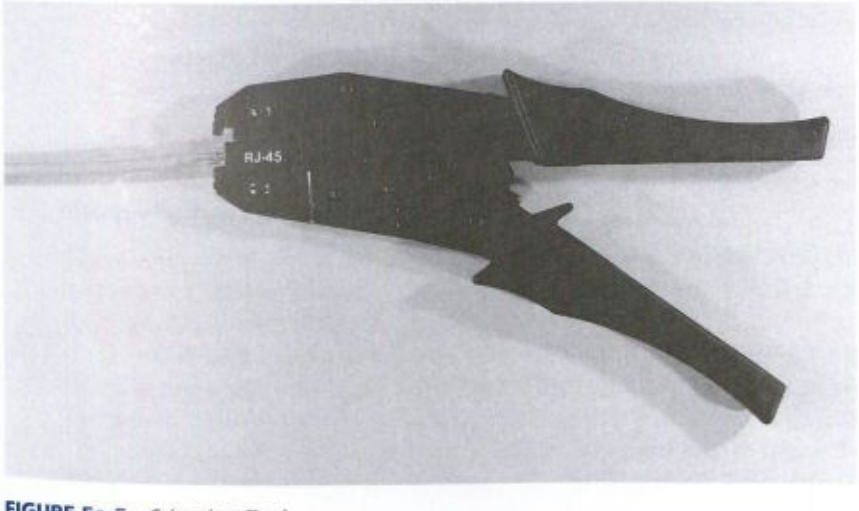

FIGURE 5a-5 Crimping Tool

Source: Courtesy of Raymond R. Panko

Testing with Continuity Testers

The simplest testers are **continuity testers**, which merely test whether the wires are arranged in correct order within the two RJ-45 connectors and are making good electrical contact with the connector. They cost only about $100.

Testing for Signal Quality

Better testers cost $500–$2,000 but are worth the extra money. In addition to testing for continuity problems, they send **test signals** through the cord to determine whether the cord meets TIA/EIA-568 signal-quality requirements. Many include **time domain reflectometry (TDR)**, which sends a signal and listens for echoes in order to measure the length of the UTP cord or to find if and where breaks exist in the cord.

Test Your Understanding

1. a) Explain the technical difference between solid-wire UTP and stranded-wire UTP. b) In what way is solid-wire UTP better? c) In what way is stranded-wire UTP better? d) Where would you use each? e) Which should only be connectorized at the factory?
2. If you have a wire run of 50 meters, should you cut the cord to 50 meters? Explain.
3. Why do you score the jacket of the cord with the stripping tool instead of cutting all the way through the jacket?
4. a) What are the colors of the four pairs? b) If you are following T568B, which wire goes into Pin 3? c) At the other end of the cord, would the same wire go into Pin 3?
5. After you arrange the wires in their correct order and cut them across, how much of the wires should be exposed from the jacket?
6. a) Describe RJ-45's insulation displacement approach. b) Describe its strain relief approach.
7. a) Should you test every cord in the field after installation? b) For what do inexpensive testers test? c) For what do expensive testers test?

5b HANDS-ON: ETHERNET SWITCHING

LEARNING OBJECTIVES

By the end of this chapter, you should be able to:

- Set up a small Ethernet switched network.
- Observe what happens if you create a loop among Ethernet switches.

THE EXERCISE

This is a class exercise rather than an individual exercise. It is rather quick (taking 15 to 20 minutes), but it takes an investment in resources.

What You Will Need

- A number of Ethernet switches. In general, it is good to have one switch for every two to four students, with the low ratio being much better. These can be very cheap switches.
- Enough UTP cords to connect the switches to each other and to the wall jack that bring the campus network into the classroom. Each will need to be 3–6 meters in length, depending on the layout of the classroom. Each student group should have sufficient room to work.
- Each Ethernet switch is powered. You may need to have some power cables so that all of the teams have power for their switches.
- Two notebooks to plug into the network.

Creating the Network

The students should create a network like the one in Figure 5b-1. There should be a top-level switch at the front of the classroom. It should plug into the wall jack that connects the classroom to the campus network.

Below the top-level switch, other switches should be arranged in a hierarchy. I find it is useful to have a simple hierarchy with two columns of switches as shown in the figure. It is important to keep a strict hierarchy among the switches.

After the switches are set up, attach PCs to switches at the end of each column. See if the PCs can connect to the Internet via the classroom wall jack. They should be able to do so.

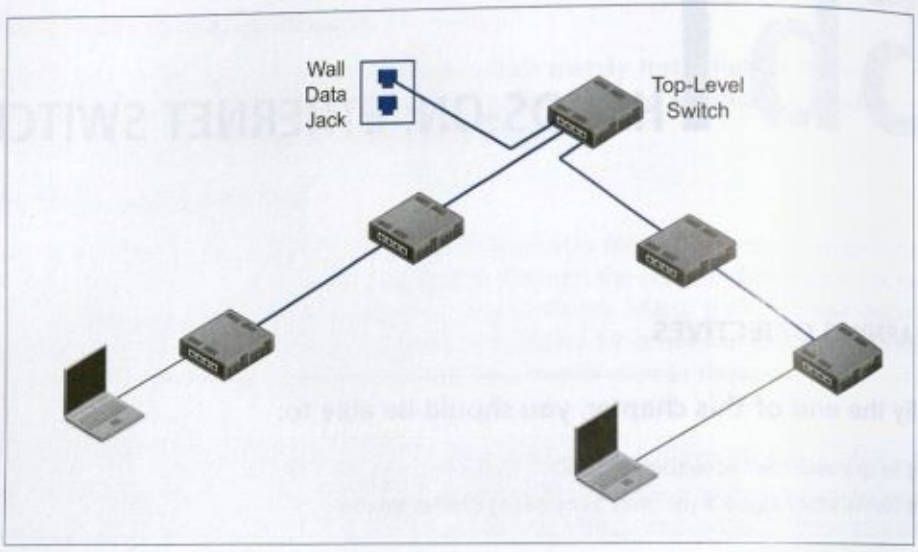

FIGURE 5b-1 The Network

At the end of this exercise, you can see how straightforward it is to set up a hierarchical Ethernet network. The switches are easy to power up, and RJ-45 connectors simply go "snap."

Creating a Loop

Now that the network is working, it is time to create a loop. Loops are not allowed in Ethernet, and you are about to see why. Connect two switches so that a loop is created, as Figure 5b-2 illustrates. Now see if the PCs can still access the Internet. They should not be able to do so.

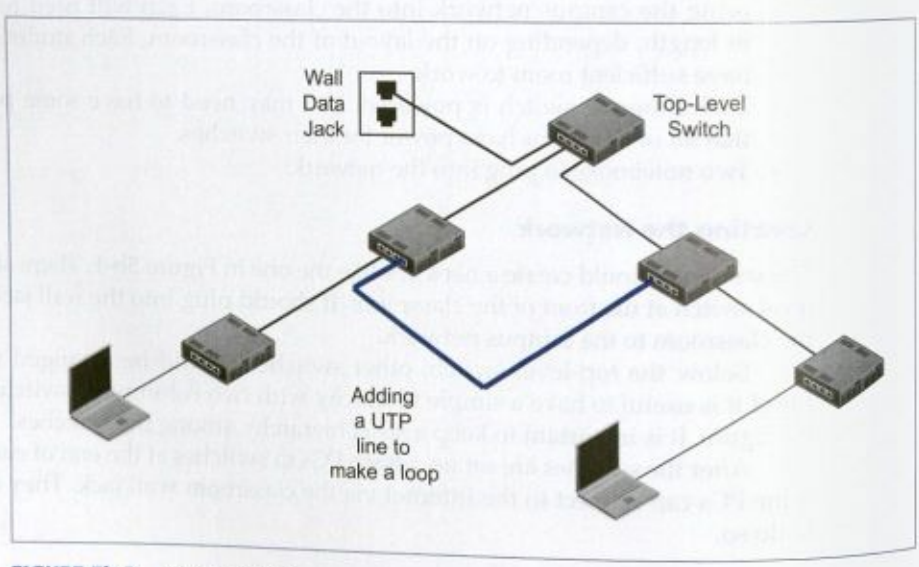

FIGURE 5b-2 Adding a Loop

6 WIRELESS LANs I

LEARNING OBJECTIVES

By the end of this chapter, you should be able to:

- Explain radio signal propagation: frequencies, antennas, and wireless propagation problems.
- Describe wireless LAN technologies.
- Explain radio bands, bandwidth, and channels.
- Distinguish between normal and spread spectrum transmission.
- Describe 802.11 WLAN operation with access points and a switched Ethernet distribution system to link the access points.
- Compare and contrast the 802.11g, 802.11n, 802.11ac, and 802.11ad transmission standards. Discuss emerging trends in 802.11 operation, including channels with much wider bandwidth, MIMO, beamforming, and multiuser MIMO.
- Briefly discuss emerging trends in 802.11 standards. Discuss the key points of Wi-Fi Direct and wireless mesh networking.

CHRISTOPHER LOREK

Two years ago, Christopher Lorek bought his wife a new notebook computer. Claire was pleased with her new computer, but she didn't want to run a new unshielded twisted pair (UTP) line to it from their access router. She wanted mobility. So Christopher bought a new access router with a built-in access point. The new wireless router was inexpensive. It operated in the 2.4 GHz radio band, and it followed the 802.11g standard. Christopher also bought a wireless printer for them to use. It also operated in the 2.4 GHz band using the 802.11g standard.

Although Claire liked the mobility, she found Internet access painfully slow. Christopher downloaded an application to Claire's computer to identify nearby wireless access routers. When he used it, he found that there were only three available channels, and at least one of his neighbors had an access point operating on each channel. The problem, then, appeared to be interference.

Christopher decided to get a router that would operate in the uncrowded 5 GHz band. He was pleased to find that routers that operated in the 5 GHz band also used the 802.11n standard, which is several times faster than 802.11g. The store had two 5 GHz routers. One only operated in the 2.4 GHz band. The other operated in both the 2.4 GHz and 5 GHz bands simultaneously. The one that operated simultaneously in the two bands was more expensive.

Test Your Understanding

1. a) Which terms in this case were unfamiliar to you? b) What do you think Christopher should do? Justify your conclusion.

INTRODUCTION

In Chapter 5, we looked at wired switched networks. Technologies for those networks, for instance, Ethernet, require both physical and data link layer standards. Consequently, they are OSI standards. In this chapter and in Chapter 7, we will look at wireless LAN management and security. Like wired LANs, wireless networks are also single networks, which require physical and data link layer standards. So they too are OSI standards.

Although many people think of wireless transmission as something new and underdeveloped, businesses were already spending more on wireless LANs than wired LANs in 2008. Wireless transmission is the growth sector in networking today and will be for some time to come.

Test Your Understanding

2. a) At what layers do wireless networks operate? b) Are wireless network standards OSI standards or TCP/IP standards? Explain.

BASIC 802.11 WIRELESS LAN (WLAN) OPERATION

Having discussed wireless transmission briefly, we will look at wireless networking's widest application today, wireless local area networks. A **wireless local area network (WLAN)**, like any type of LAN, operates on the customer premises.

Wireless LANs (WLANs) use radio for physical layer transmission on the customer premises.

Wireless LAN Technology

The dominant WLAN technology today

Standardized by the 802.11 Working Group

Wireless Computers Connect to Access Points (Figure 6-2 and Figure 6-3)

Supplement Wired LANs

Access points connect to the corporate LAN

So that wireless hosts can reach servers on the Ethernet LAN

So that wireless hosts can reach Internet access routers on the Ethernet LAN

Large 802.11 WLANs

Organizations can provide coverage throughout a building or a university campus

By the judicious installation of many access points

FIGURE 6-1 802.11 Wireless LAN (WLAN) Standards (Study Figure)

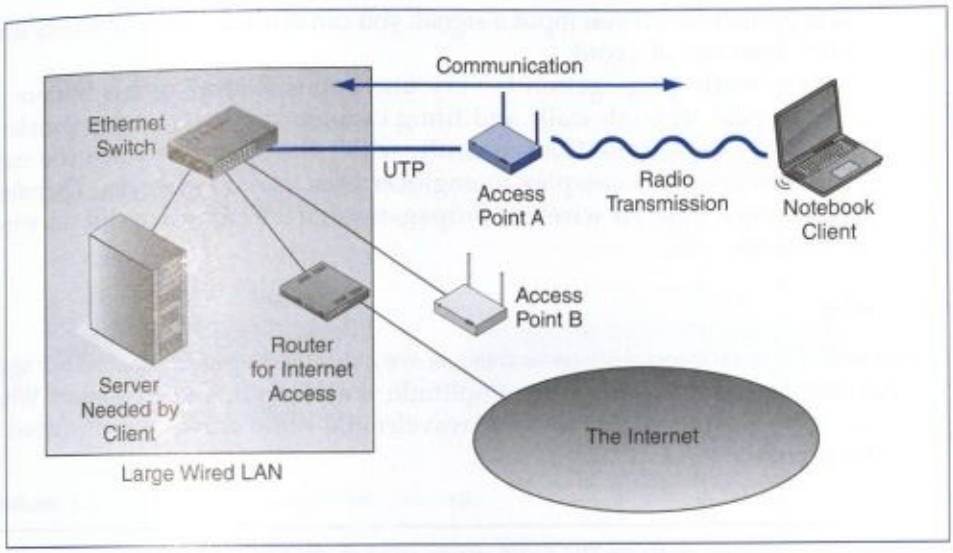

FIGURE 6-2 802.11 Wireless LAN (WLAN) Operation

The most important WLAN standards today are the **802.11** standards, which are created by the IEEE **802.11 Working Group**. Recall that Ethernet standards are created by a different working group, the 802.3 Working Group.

Rather than being a competitor for wired Ethernet LANs, **802.11 WLANs** today primarily *supplement* wired LANs, but do not replace them. Figure 6-2 shows that mobile users typically connect by radio to devices called **wireless access points**, or, simply, **access points**. These access points link the mobile user to the firm's wired Ethernet LAN.

Why is there normally a connection to the firm's main wired LAN? Quite simply, the servers that mobile host devices need, as well as the firm's Internet access router, usually are on the wired LAN. Wireless hosts need the wired LAN to reach the resources they need. A single 802.11 wireless access point can serve multiple hosts up to 30 to 100 meters away.

In a home, you are likely to have a single access point. Businesses need far larger coverage areas. By placing wireless access points judiciously throughout a building, a company can construct a large 802.11 WLAN "cloud" that can serve mobile users anywhere in the building. We will spend most of this chapter looking at the technology of 802.11 WLANs.

Test Your Understanding

3. a) What 802 working group creates 802.11 standards? b) Why do wireless clients need access to the wired Ethernet LAN? c) How can firms provide WLAN coverage throughout a large building?

RADIO SIGNAL PROPAGATION

Chapter 5 discussed propagation effects in wired transmission media (UTP and optical fiber). Generally speaking, these effects can be well controlled by respecting cord distance limits and taking other installation precautions. This is possible because wired

propagation is predictable. If you input a signal, you can estimate fairly precisely what it will be at the other end of a cord.

In contrast, radio propagation is very unreliable. Radio signals bounce off obstacles, fail to pass through walls and filing cabinets, and have other problems we will look at in this section. Consequently, wireless networks, which use radio to deliver signals, are more complex to engineer than wired networks. Therefore, we will spend more time on wireless propagation effects than we did on wired propagation effects.

Frequencies

Wireless radio signals propagate as waves, as we saw in Chapter 5. Figure 6-3 again notes that waves are characterized by amplitude, wavelength, and frequency. While optical fiber waves are given in terms of wavelength, radio waves are described in terms of **frequency**.

Frequency is used to describe the radio waves used in WLANs.

In waves, frequency is the number of complete cycles per second. One cycle per second is one **hertz (Hz)**. Metric designations are used to describe frequencies. In the metric system, frequencies increase by a factor of 1,000, rather than 1,024. The most common radio frequencies for wireless data transmission are about 500 **megahertz (MHz)** to 10 **gigahertz (GHz)**.

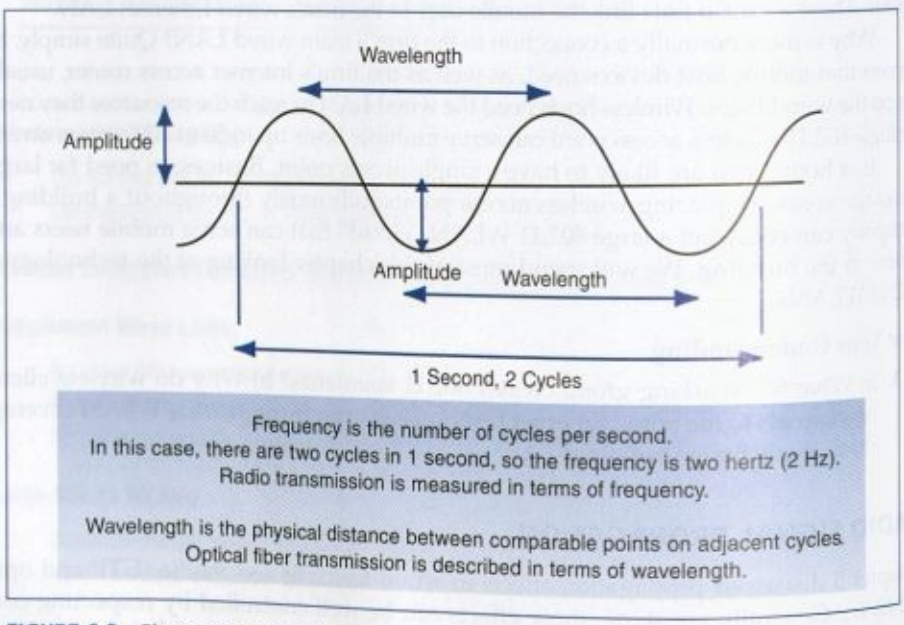

FIGURE 6-3 Electromagnetic Wave

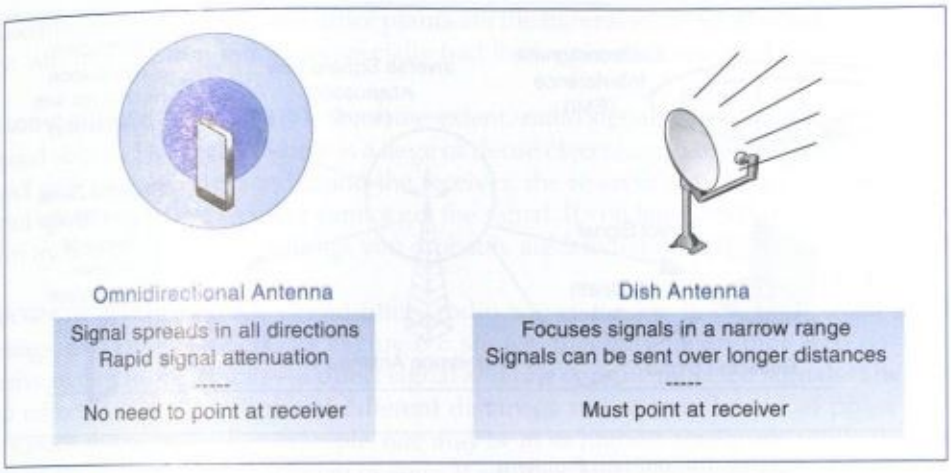

FIGURE 6-4 Omnidirectional and Dish Antennas

Test Your Understanding

4. a) Is wireless radio transmission usually expressed in terms of wavelength or frequency? b) What is a hertz? c) Convert 3.4 MHz to a number without a metric prefix. d) At what range of frequencies do most wireless systems operate?

Antennas

Radio transmission requires an antenna. Figure 6-4 shows that there are two types of radio antennas: omnidirectional antennas and dish antennas.

- **Omnidirectional antennas** transmit signals equally strongly in all directions and receive incoming signals equally well from all directions. Consequently, the antenna does not need to point in the direction of the receiver. However, because the signal spreads in all three dimensions, only a small fraction of the energy transmitted by an omnidirectional antenna reaches the receiver. Omnidirectional antennas are best for short distances, such as those found in a wireless LAN (WLAN) or a cellular metropolitan area network.
- **Dish antennas**, in contrast, point in a particular direction, which allows them to focus stronger outgoing signals in that direction for the same power and to receive weaker incoming signals from that direction. (A dish antenna is like the reflector in a flashlight.) Dish antennas are good for longer distances because of their focusing ability, but users need to know the direction of the other antenna. Also, omnidirectional antennas are easier to use. (Imagine if you had to carry a dish with you whenever you carried your cellular phone. You would not even know where to point the dish!)

Test Your Understanding

5. a) Distinguish between omnidirectional and dish antennas in terms of operation. b) Under what circumstances would you use an omnidirectional antenna? c) Under what circumstances would you use a dish antenna? d) What type of antenna normally is used in WLANs? Why?

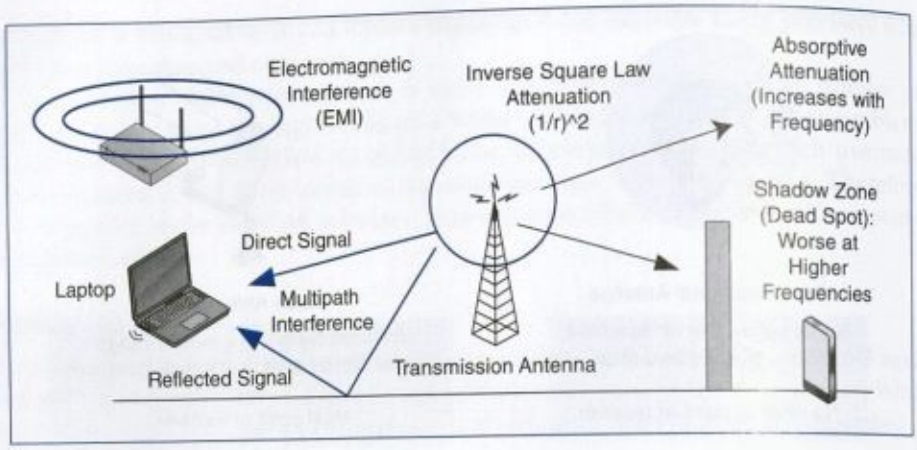

FIGURE 6-5 Wireless Transmission Problems

Wireless Propagation Problems

We have already noted that, although wireless communication gives mobility, wireless transmission is not very predictable, and there often are serious propagation problems. Figure 6-5 illustrates five common wireless propagation problems.

INVERSE SQUARE LAW ATTENUATION Compared with signals sent through wires and optical fiber, radio signals attenuate very rapidly. When a signal spreads out from any kind of antenna, its strength is spread over the area of a sphere. (In omnidirectional antennas, power is spread equally over the sphere, while in dish antennas, power is concentrated primarily in one direction on the sphere.)

The area of a sphere is proportional to the square of its radius, so signal strength in any direction weakens by an **inverse square law** ($1/r^2$), as Equation 5-1 illustrates. Here, S_1 is the signal strength at distance r_1, and S_2 is the signal strength at a farther distance r_2.

$$S_2 = S_1 * (r_1/r_2)^2 \qquad \textbf{(Equation 5-1)}$$

To give an example, if you triple the distance ($r_1/r_2 = 1/3$), the signal strength (S_2) falls to only one-ninth ($1/3^2$) of its original strength (S_1). With radio propagation, you have to be relatively close to your communication partner unless the signal strength is very high, an omnidirectional antenna is used, or both.

To give a specific example, at 10 meters, the signal strength is 20 milliwatts (mW). How strong will the signal be at 20 meters?

- The distance doubles (so r_1/r_2 is 1/2).
- So we multiply the signal strength at 10 meters by 1/4 (1/2 squared)
- Twenty mW multiplied by 1/4 is 5 mW.
- So the strength of the signal at 10 meters will be 5 mW.

ABSORPTIVE ATTENUATION As a radio signal travels, it is partially absorbed by the air molecules, plants, and other things it passes through. This **absorptive attenuation** is

especially bad in moist air, and office plants are the natural enemies of wireless transmission. Absorptive attenuation is especially bad for longer-distance outdoor propagation.

SHADOW ZONES (DEAD SPOTS) To some extent, radio signals can go through and bend around objects. However, if there is a large or dense object (e.g., a brick wall), blocking the direct path between the sender and the receiver, the receiver may be in a **shadow zone (dead spot)**, where the receiver cannot get the signal. If you have a cellular telephone and often try to use it within buildings, you probably are familiar with this problem.

MULTIPATH INTERFERENCE In addition, radio waves tend to bounce off walls, floors, ceilings, and other objects. As Figure 6-6 shows, this may mean that a receiver will receive two or more signals—a direct signal and one or more reflected signals. The direct and reflected signals will travel different distances and so may be out of phase when they reach the receiver. For example, one may be at its highest amplitude while the other is at its lowest, giving an average of zero. If so, they will completely cancel out if their amplitudes are the same.

This **multipath interference** may cause the signal to range from strong to nonexistent within a few centimeters (inches). If the difference in time between the direct and reflected signal is large, some reflected signals may even interfere with the next direct signal. Multipath interference is the most serious propagation problem at WLAN frequencies.

Multipath interference is the most serious propagation problem at WLAN frequencies.

ELECTROMAGNETIC INTERFERENCE (EMI) A final common propagation problem in wireless communication is **electromagnetic interference (EMI)**. Other devices produce EMI at frequencies used in wireless data communications. Among these

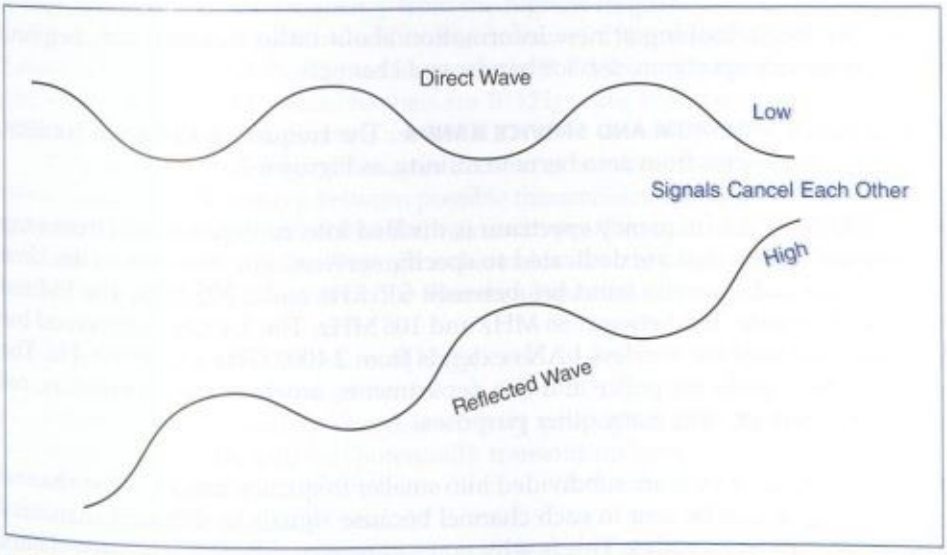

FIGURE 6-6 Multipath Interference

devices are cordless telephones, microwaves, and especially devices in other nearby wireless networks.

FREQUENCY-DEPENDENT PROPAGATION PROBLEMS To complicate matters, two wireless propagation problems are affected by frequency.

- First, higher-frequency waves suffer more rapidly from absorptive attenuation than lower-frequency waves because they are absorbed more rapidly by moisture in the air, leafy vegetation, and other water-bearing obstacles. Consequently, as we will see in this chapter, WLAN signals around 5 GHz attenuate more rapidly than signals around 2.4 GHz.
- Second, shadow zone problems grow worse with frequency. As frequency increases, radio waves become less able to go through and bend around objects.

Test Your Understanding

6. a) Which offers more reliable transmission characteristics—UTP or radio transmission? b) Which attenuates more rapidly with distance—signals sent through wired media or radio signals? c) If the signal strength from an omnidirectional radio source is 8 mW at 30 meters, how strong will it be at 120 meters, ignoring absorptive attenuation? Show your work. d) How are shadow zones (dead spots) created? e) Why is multipath interference very sensitive to location? f) What is the most serious propagation problem in WLANs? g) List some sources of EMI. h) What propagation problems become worse as frequency increases?

RADIO BANDS, BANDWIDTH, AND SPREAD SPECTRUM TRANSMISSION

Radio Bands

Now we can begin looking at new information about radio transmission, beginning with the frequency spectrum, service bands, and channels.

THE FREQUENCY SPECTRUM AND SERVICE BANDS The **frequency spectrum** consists of all possible frequencies from zero hertz to infinity, as Figure 6-7.

SERVICE BANDS The frequency spectrum is divided into contiguous spectrum ranges called **service bands** that are dedicated to specific services. For instance, in the United States, the AM radio service band lies between 535 kHz and 1,705 kHz. The FM radio service band, in turn, lies between 88 MHz and 108 MHz. The 2.4 GHz unlicensed band that we will see later for wireless LANs extends from 2.4000 GHz to 2.4835 GHz. There are also service bands for police and fire departments, amateur radio operators, communication satellites, and many other purposes.

CHANNELS Service bands are subdivided into smaller frequency ranges called **channels**. A different signal can be sent in each channel because signals in different channels do not interfere with one another. This is why you can receive different television channels successfully.

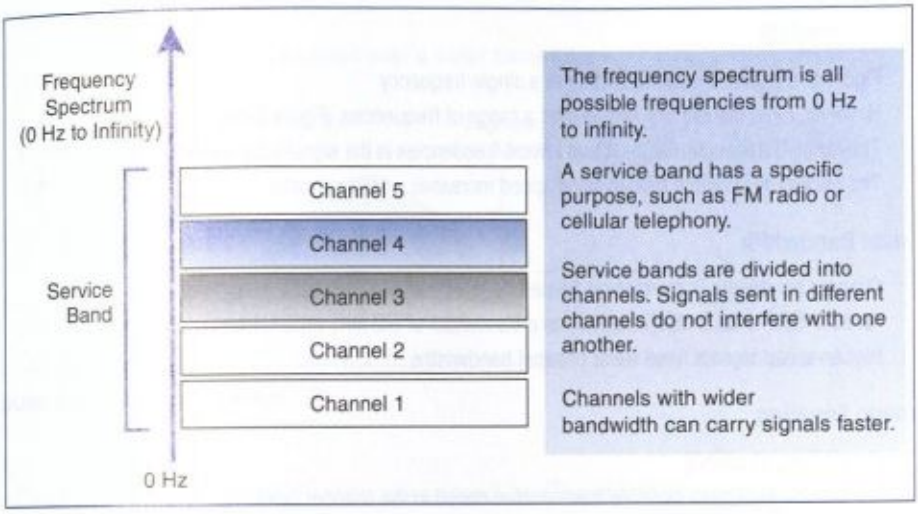

FIGURE 6-7 The Frequency Distribution, Service Bands, and Channels

Test Your Understanding

7. a) Distinguish among the frequency spectrum, service bands, and channels. b) In radio, how can you send multiple signals without the signals interfering with one another?

Signal and Channel Bandwidth

Figure 6-3 showed wave operating at a single frequency. In contrast, Figure 6-9 shows that signals do not operate at a single frequency. Rather, signals spread over a range of frequencies. This range is called the signal's **bandwidth**. Signal bandwidth is measured by subtracting the lowest frequency from the highest frequency.

A channel also has a bandwidth. For instance, if the lowest frequency of an FM channel is 89.0 MHz and the highest frequency is 89.2 MHz, then the **channel bandwidth** is 0.2 MHz (200 kHz). AM radio channels are 10 kHz wide, FM channels have bandwidths of 200 kHz, and television channels are 6 MHz wide.

Why are there such large differences in channel bandwidth across service bands? The answer lies in the relationship between possible transmission speed in a channel and channel bandwidth. Shannon found that the maximum possible transmission speed (C) in bits per second when sending data through a channel is directly proportional to the channel's bandwidth (B) in hertz, as shown in the **Shannon Equation** (Equation 5-2).[1]

$$C = B[\text{Log}_2(1 + S/N)] \qquad \textbf{(Equation 5–2)}$$

The maximum possible speed is directly proportional to bandwidth, so if you double the bandwidth, you can potentially transmit up to twice as fast. However, C is

[1] Claude Shannon, "A Mathematical Theory of Communication," *Bell System Technical Journal*, (July 1938), pp. 379–423, and (October 28, 1938), pp. 623–56.

Signal Bandwidth

Figure 6-4 shows a wave operating at a single frequency
However, most signals are spread over a range of frequencies (Figure 6-10)
The range between the highest and lowest frequencies is the signal's bandwidth
The maximum possible transmission speed increases with bandwidth

Channel Bandwidth

Channel bandwidth is the highest frequency in a channel minus the lowest frequency
An 88.0 MHz to 88.2 MHz channel has a bandwidth of 0.2 MHz (200 kHz)
Higher-speed signals need wider channel bandwidths

Shannon Equation

$C = B\ [\text{Log}_2\ (1+S/N)]$

C = Maximum possible transmission speed in the channel (bps)
B = Bandwidth (Hz)
S/N = Signal-to-noise ratio measured as the power ratio, not as decibels

Note that doubling the bandwidth doubles the maximum possible transmission speed
Multiplying the bandwidth by X multiplies the maximum possible speed by X
Wide bandwidth is the key to fast transmission
Increasing S/N helps slightly, but usually cannot be done to any significant extent

Broadband and Narrowband Channels

Broadband means wide channel bandwidth and therefore high speed
Narrowband means narrow channel bandwidth and therefore low speed
Traditionally, narrowband is below 200 kbps; broadband is above 200 kbps

The Golden Zone

Most organizational radio technologies operate in the golden zone in the 500 MHz to 10 GHz range
Golden zone frequencies are high enough for there to be large total bandwidth
At higher frequencies, there is more available bandwidth
Golden zone frequencies are low enough to allow fairly good propagation characteristics
At lower frequencies, signals propagate better
Growing demand creates intense competition for frequencies in the Golden Zone

FIGURE 6-8 Channel Bandwidth and Transmission Speed (Study Figure)

the *maximum possible speed* for a given bandwidth and signal-to-noise ratio. *Real transmission throughput* will always be less.

To transmit at a given speed, you need a channel wide enough to handle that speed. For example, video signals produce many more bits per second than audio signals, so television uses much wider channels than AM radio (6 MHz versus 10 kHz in AM radio transmission).

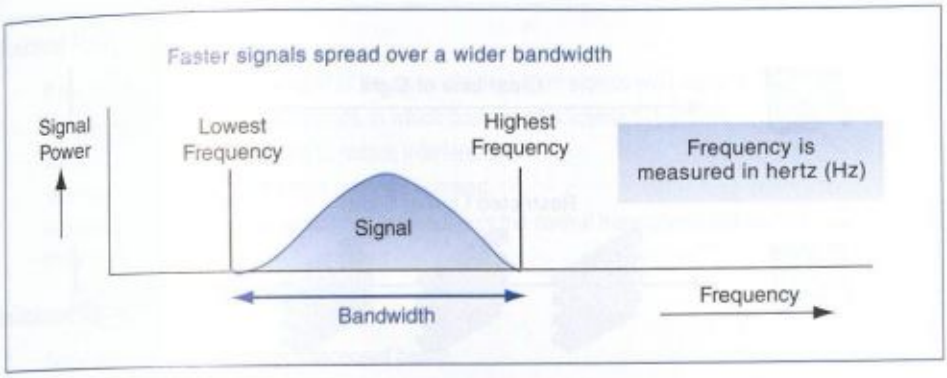

FIGURE 6-9 Signal Bandwidth

The signal-to-noise (S/N) ratio discussed in Chapter 5 is also important, but it is difficult to modify in practice. Radio signal strengths tend to be limited by law, and reducing noise is very difficult without going to super-cooled senders and receivers.

Channels with large bandwidths are called **broadband** channels. They can carry data very quickly. In contrast, channels with small bandwidths, called **narrowband** channels, can carry data only slowly. Although the terms *broadband* and *narrowband* technically refer only to the width of a channel, broadband has come to mean "fast," while narrowband has come to mean "slow."

Transmission systems that are very fast are usually called broadband systems even when they do not use channels.

Test Your Understanding

8. a) Does a signal usually travel at a single frequency, or does it spread over a range of frequencies? b) What is channel bandwidth? c) If the lowest frequency in a channel is 1.22 MHz and the highest frequency is 1.25 MHz, what is the channel bandwidth? (Use proper metric notation.) d) Why is large channel bandwidth desirable? e) What do we call a system whose channels have large bandwidth? f) What other types of system do we call *broadband*?
9. a) Write the Shannon Equation. List what each letter is in the equation. b) What information does C give you? c) What happens to the maximum possible propagation speed in a channel if the bandwidth is tripled while the signal-to-noise ratio remains the same? d) Given their relative bandwidths, about how many times as much data is sent per second in television than in AM radio? (The information to answer this question is in the text.) e) Telephone channels have a bandwidth of about 3.1 kHz. Do the following in Excel. Cut and paste your analyses into your homework. f) If a telephone channel's signal-to-noise ratio is 1,000 (the signal strength is 1,000 times larger than the noise strength), how fast can a telephone channel carry data? (Check figure: Telephone modems operate at about 30 kbps, so your answer should be roughly this speed.)

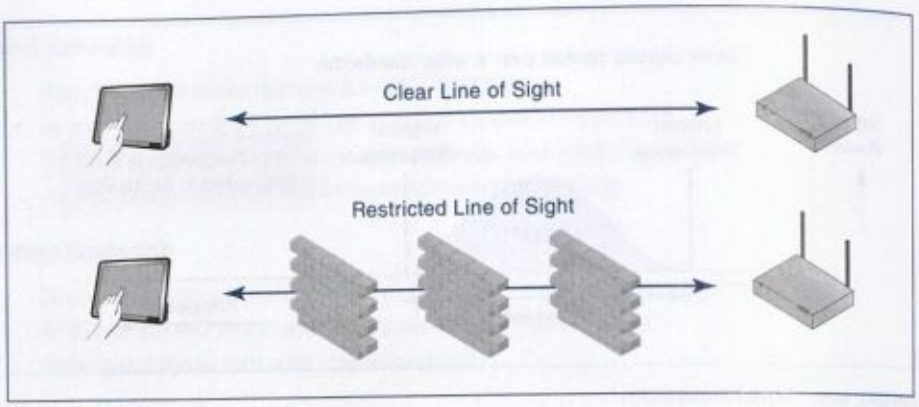

FIGURE 6-10 Line of Sight

The Golden Zone

Commercial mobile services operate in the high-megahertz to low-gigahertz range (approximately 500 MHz to 10 GHz). This is the **golden zone**. At lower frequencies, the spectrum is limited and has been almost entirely assigned. At higher frequencies, radio waves attenuate very rapidly with distance because of absorptive attenuation and cannot flow through or around objects as they do at lower frequencies. Consequently, at frequencies above about 10 GHz, the sender and receiver typically must have a **clear line of sight** (unobstructed direct path) between them. (See Figure 6-10.) Even at the high end of the golden zone, absorption and shadow zone propagation problems are large. The golden zone is limited, and demand for channels and service bands in the golden zone is increasing rapidly. Consequently, there is strong competition for bandwidth in the golden zone.

The golden zone for commercial mobile services is 500 MHz to 10 GHz.

Test Your Understanding

10. a) What is the golden zone in commercial mobile radio transmission? b) Why is the golden zone important? c) What is a clear line-of-sight limitation?

Licensed and Unlicensed Radio Bands

If two radio hosts transmit at the same frequency, their signals will interfere with each other. In the terminology of Chapter 5, this is electromagnetic interference. To prevent such chaos, governments regulate how radio transmission is used. The International Telecommunications Union, which is a branch of the United Nations, creates worldwide rules that define service bands and specify how individual radio service bands are to be used. Individual countries enforce these rules but are given discretion over how to implement controls.

LICENSED RADIO BANDS In licensed radio bands, stations must have a government license to operate. They also need a license change if they move their antennas.

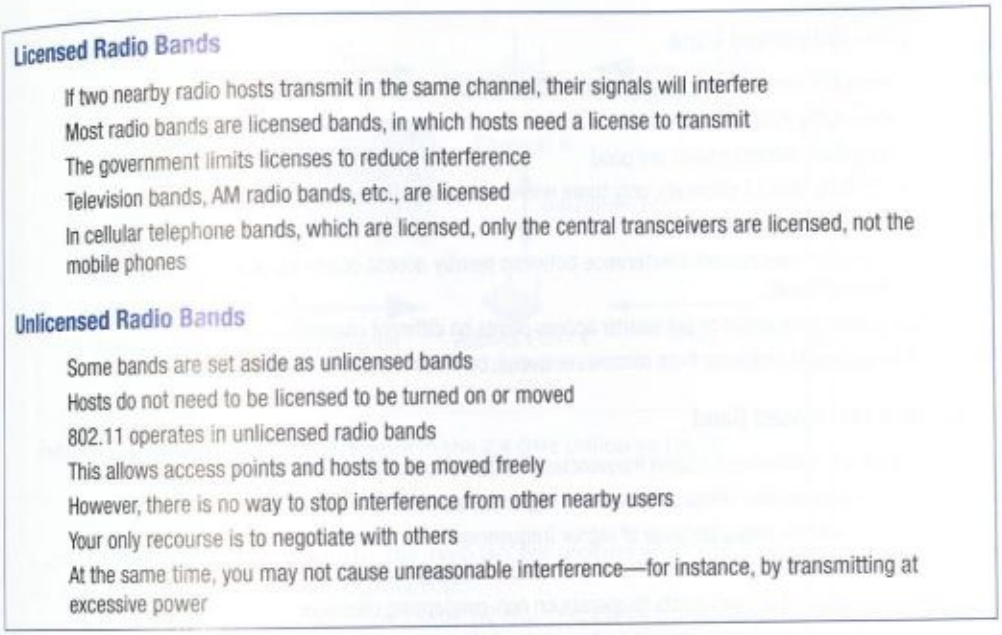

FIGURE 6-11 Licensed and Unlicensed Radio Bands (Study Figure)

Commercial television bands are licensed bands, as are AM and FM radio bands. Government agencies control who may have licenses. By doing so, the government limits interference to an acceptable level. In some licensed bands, the rules allow mobile hosts to move about while only central antennas are regulated. This is the case for mobile telephones.

UNLICENSED RADIO BANDS However, for companies that have wireless access points and mobile computers, even the requirement to license central antennas (in this case, access points) is an impossible burden. Consequently, the government has created a few **unlicensed radio bands**. In these bands, any wireless host can be turned on or moved around without the need for any government approval.

The problem with unlicensed radio bands is that users of unlicensed radio bands must tolerate interference from others. If your neighbor sets up a wireless LAN next door to yours, you have no recourse but to negotiate with him or her over such matters as which channels each of you will use. At the same time, the law prevents you from creating unreasonable interference—for instance, by using illegally high transmission power.

Test Your Understanding

11. a) Do WLANs today use licensed or unlicensed bands? b) What is the advantage of using unlicensed bands? c) What is the disadvantage?

The 2.4 GHz and 5 GHz Unlicensed Bands

It would be impossible for a company to have licenses for all of its access points and wireless hosts, so 802.11 operates in unlicensed radio bands. More specifically, WLANs today use two unlicensed bands. One is the 2.4 GHz band. The other is the 5 GHz band.

The 2.4 GHz Unlicensed Band

Defined the same in almost all countries (2.400 GHz to 2.485 GHz)
Commonality reduces radio costs
Propagation characteristics are good
For 20 MHz 802.11 channels, only three non-overlapping channels are possible
Channels 1, 6, and 11
This creates co-channel interference between nearby access points transmitting in the same 20 MHz channel
Difficult or impossible to put nearby access points on different channels (Figure 6-14)
Also, potential problems from microwave ovens, cordless telephones, etc.

The 5 GHz Unlicensed Band

Radios are expensive because frequencies in different countries are different
Shorter propagation distance because of higher frequencies
Deader shadow zones because of higher frequencies
More bandwidth, so between 11 and 24 non-overlapping channels
Allows different access points to operate on non-overlapping channels
Some access points can operate on two channels to provide faster service

FIGURE 6-12 The 2.4 GHz and 5 GHz Unlicensed Bands (Study Figure)

THE 2.4 GHZ UNLICENSED BAND The **2.4 GHz unlicensed band** is the same in most countries in the world, stretching from 2.40 GHz to 2.4835 GHz. This commonality allows companies to sell generic 2.4 GHz radios, driving down the price of radios. In addition, radio propagation is better in the 2.4 GHz unlicensed band than in the higher-frequency 5 GHz band.

Unfortunately, the 2.4 GHz band is very limited. It has only 83.5 MHz of bandwidth. Traditionally, each 802.11 channel was 20 MHz wide, although 40 MHz bandwidth channels were introduced in 802.11n. Furthermore, due to the way channels are allocated, there are only three possible non-overlapping 20 MHz 802.11 channels, which are centered at Channels 1, 6, and 11.[2] If nearby access points operate in the same channel, their signals will interfere with each other unless the access points are far apart. This interference is called **co-channel interference**. If an 802.11n station finds itself in a crowded area, it will drop back to 20 MHz to reduce the interference it causes.

If you have only three access points that can all hear each other, there is no problem with having only three channels. You simply run each on a different channel, and there will be no co-channel interference. However, when you have multiple access points that can all hear each other, Figure 6-13 shows that there is no way to avoid having some co-channel interference. You can minimize co-channel interference somewhat

[2] Channel numbers were defined for the 2.4 GHz band when channels were narrower. A 20 MHz 802.11 channel overlaps several defined channels. Channels 1, 6, and 11 operate in the 2,402 MHz to 2,422 MHz, 2,427 MHz to 2,447 MHz, and 2,452 MHz to 2,472 MHz frequency ranges, respectively. Note that there are 5 MHz unused "guard bands" between the channels to prevent inter-channel interference.

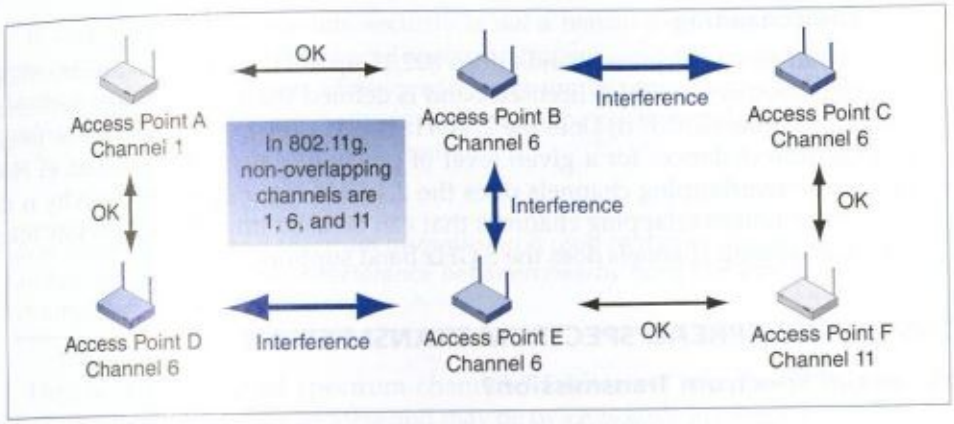

FIGURE 6-13 Co-channel Interference in the 2.4 GHz Unlicensed Band

by giving the shared channel to the two access points that are farthest apart, but this will only reduce interference somewhat.

In addition, the frequencies used in the 2.4 GHz band overlap the frequencies used in microwave ovens, cordless telephones, and Bluetooth equipment. This results in occasional interference that is difficult to diagnose.

THE 5 GHZ UNLICENSED BAND The 802.11 standard can also operate in the **5 GHz unlicensed band**. There have been two problems with this band. The first is the cost of radios. In the 2.4 GHz band, high sales have allowed manufacturers to ride the learning curve down to lower costs. In addition, while the 2.4 GHz band is standardized throughout most of the world, different countries use different parts of the 5 GHz band. This also makes 5 GHz radios more expensive due to the need to use only those channels permitted within a given country.

Second, because of the 5 GHz band's higher frequencies, signals do not travel as far, and shadow zones are darker. This means that access points have to be placed closer together. It also means that siting access points to avoid dead spots is more difficult.

The big advantage of the 5 GHz band is that it is much wider than the 2.4 GHz band. In contrast to the 2.4 GHz band's mere three channels, the 5 GHz band provides between 11 and 24 non-overlapping 20 MHz channels, depending on the frequencies allocated to unlicensed operation in a country.

Having many channels eliminates the co-channel interference problem because it is easy to assign noninterfering channels to access points even in multi-floor buildings (which introduce interference in three dimensions).

In addition, in the sparsely used 5 GHz service bands, some access points can operate simultaneously on two different channels. This doubles the amount of bandwidth available to devices.

The disadvantage of operating in the 5 GHz band is higher radio cost because 5 GHz radios are inherently more expensive and because fewer of them are being produced, raising the cost per unit. However, this cost difference is rather small, and 5 GHz access points and clients are now available on retail shelves at only a modest premium.

Test Your Understanding

12. a) In what two unlicensed bands does 802.11 operate? b) How wide are 802.11 channels usually? c) Which licensed band is defined the same way in most countries around the world? d) Does the 2.4 GHz band or the 5 GHz band allow longer propagation distances for a given level of power? Justify your answer. e) How many non-overlapping channels does the 2.4 GHz band support? f) Why is the number of non-overlapping channels that can be used important? g) How many non-overlapping channels does the 5 GHz band support?

NORMAL AND SPREAD SPECTRUM TRANSMISSION

Why Spread Spectrum Transmission?

At the frequencies used by WLANs, there are numerous and severe propagation problems. In these unlicensed bands, regulators mandate the use of a form of transmission called spread spectrum transmission. Spread spectrum transmission is transmission that uses far wider channels than transmission speed requires.

Spread spectrum transmission is transmission that uses far wider channels than transmission speed requires.

Regulators mandate the use of spread spectrum transmission primarily to minimize propagation problems—especially multipath interference. (If the direct and reflected signals cancel out at some frequencies within the range, they will be double at other frequencies.)

Spread Spectrum Transmission

You are required by law to use spread spectrum transmission in unlicensed bands
Spread spectrum transmission reduces propagation problems
    Especially multipath interference
Spread spectrum transmission is NOT used for security in WLANs

Normal Transmission versus Spread Spectrum Transmission (See Figure 6-16)

Normal transmission uses only the channel bandwidth required by your signaling speed
Spread spectrum transmission uses channels much wider than signaling speed requires

Orthogonal Frequency Division Multiplexing (See Figure 6-17)

OFDM is the dominant spread spectrum transmission method today
It is difficult to transmit in a very wide channel
So the sender divides the channel into multiple subchannels called subcarriers
Part of the frame is sent in each subcarrier
The frame is sent redundantly, so if some subcarriers are lost, the frame is still likely to get through
It is much easier to transmit in many smaller-bandwidth subcarriers

FIGURE 6-14 Spread Spectrum Transmission (Study Figure)

In commercial transmission, security is *not* a reason for doing spread spectrum transmission. The military uses spread spectrum transmission for security, but it does so by keeping certain parameters of its spread spectrum transmission secret. Commercial spread spectrum transmission methods must make these parameters publicly known in order for two parties to communicate easily.

In wireless LANs, spread spectrum transmission is used to reduce propagation problems and to reduce co-channel interference between nearby hosts transmitting in the same channel, not to provide security.

How wide are spread spectrum channels? Earlier, we saw that 802.11 channel bandwidth was traditionally 20 MHz and may be twice as wide for the 802.11n standard.

Test Your Understanding

13. a) In unlicensed bands, what type of transmission method is required by regulators?
b) What is the benefit of spread spectrum transmission for business communication?
c) Is spread spectrum transmission done for security reasons in commercial WLANs?

Spread Spectrum Transmission Methods

NORMAL VERSUS SPREAD SPECTRUM TRANSMISSION As noted earlier in our discussion of the Shannon Equation, if you need to transmit at a given speed, you must have a channel whose bandwidth is sufficiently wide.

To allow as many channels as possible, channel bandwidths in *normal radio transmission* are limited to the speed requirements of the user's signal, as Figure 6-15 illustrates. For a service that operates at 10 kbps, regulators would permit only enough channel bandwidth to handle this speed.

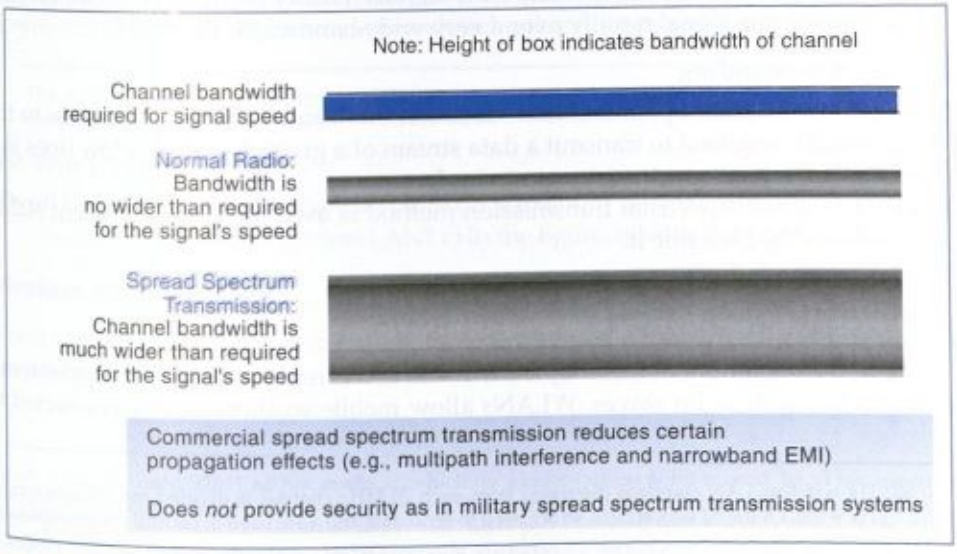

FIGURE 6-15 Normal Radio Transmission and Spread Spectrum Transmission

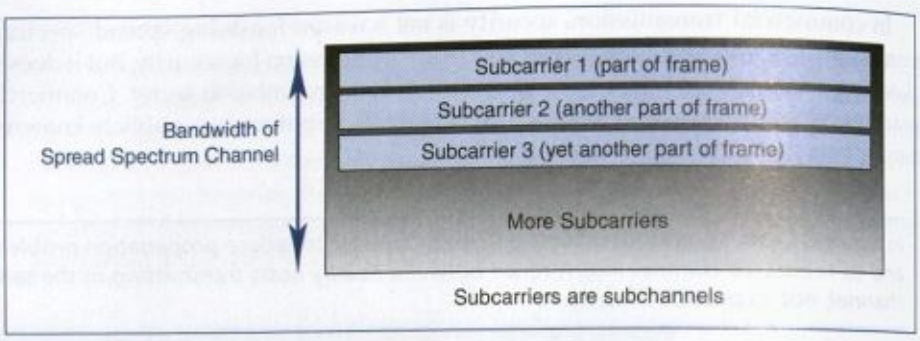

FIGURE 6-16 Orthogonal Frequency Division Multiplexing

In contrast to normal radio transmission, which uses channels just wide enough for transmission speed requirements, **spread spectrum transmission** takes the original signal, called a **baseband signal**, and spreads the signal energy over a much broader channel than is required.

ORTHOGONAL FREQUENCY DIVISION MULTIPLEXING (OFDM) There are several spread spectrum transmission methods. The 801.11 Working Group's most recent standards, 802.11g and 802.11n, use **orthogonal frequency division multiplexing (OFDM)**, which Figure 6-16 illustrates.

In OFDM, each broadband channel is divided into many smaller subchannels called **subcarriers**. Parts of each frame are transmitted in each subcarrier.[3] OFDM sends data redundantly across the subcarriers, so if there is impairment in one or even a few subcarriers, all of the data usually will still get through.

OFDM is complex and therefore expensive. However, sending data over a single very large channel reliably is difficult. In contrast, OFDM can be used at very high speeds because it is easier to send many slow signals reliably in many small subcarriers than it is to send one signal rapidly over a very wide-bandwidth channel.[4]

Test Your Understanding

14. a) In normal radio operation, how does channel bandwidth usually relate to the bandwidth required to transmit a data stream of a given speed? b) How does this change in spread spectrum transmission?
15. a) What spread spectrum transmission method is used for the most recent 802.11 standards? b) Describe it.

802.11 WLAN OPERATION

As noted at the beginning of this chapter, wireless LANs replace signals in copper wires or optical fiber with radio waves. WLANs allow mobile workers to stay connected to

[3] In the 802.11g wireless LAN standard discussed later, each 20 MHz channel is divided into 52 subcarriers, each 312.5 kHz wide. Of the 52 subcarriers, 48 are used to send data and 4 are used to control the transmission.

[4] The ADSL services discussed in Chapter 10 generally also use OFDM, although in ADSL service, OFDM is called discrete multitone (DMT) service.

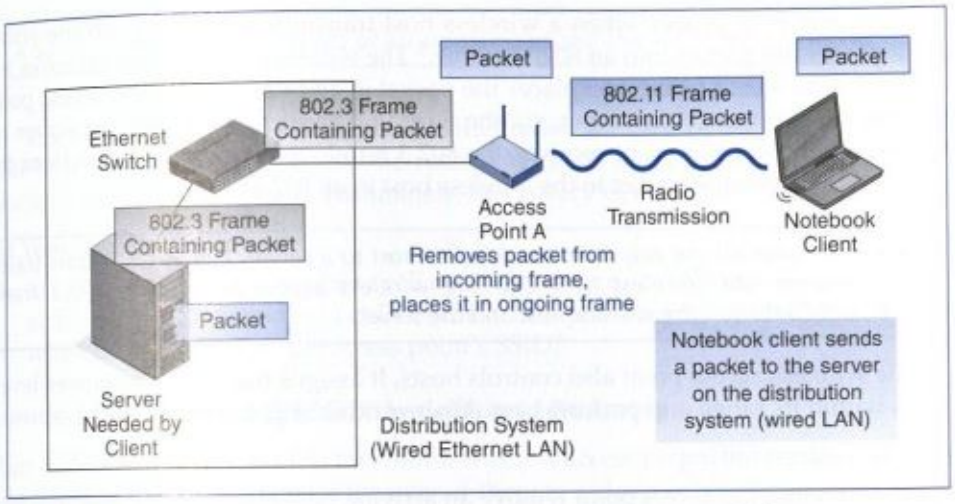

FIGURE 6-17 Typical 802.11 Wireless LAN Operation with Wireless Access Points

the network as they move through a building. In some cases, wireless LANs are less expensive to install than wired LANs, but this certainly is not always the case.

Extending the Wired LAN

As noted at the start of the chapter, and as Figure 6-17 shows, an 802.11 wireless LAN typically is used to connect a small number of mobile devices to a large wired LAN—typically, an Ethernet LAN—because the servers and Internet access routers that mobile hosts need to use usually are on the wired LAN.[5]

In 802.11 terminology, the network to which access points connect is called a **distribution system (DS)**. This typically is an Ethernet network, as we have just discussed. However, it is possible to use any network technology to connect the access points.

The network to which access points connect is called a distribution system (DS).

Test Your Understanding

16. a) List the elements in a typical 802.11 LAN today. b) Why is a wired LAN usually still needed if you have a wireless LAN? c) In the figure, what is the distribution system?

Wireless Access Points

When a wireless host wishes to send a frame to a server, it transmits the frame to a wireless access point.

[5] There is a rarely used 802.11 **ad hoc mode**, in which no wireless access point is used. In ad hoc mode, computers communicate directly with other computers. (In contrast, when an access point is used, this is called 802.11 infrastructure mode.) In addition, 802.11 can create point-to-point transmission over longer distances than 802.11 normally supports. This approach, which normally is used to connect nearby buildings, uses dish antennas and higher power levels authorized for this purpose.

As Figure 6-17 shows, when a wireless host transmits to a server on the wired LAN, it places the packet into an 802.11 frame.[6] The wireless access point removes the packet from the 802.11 frame and places the packet in an 802.3 frame. The access point sends this 802.3 frame to the server, via the wired Ethernet LAN. When the server replies, the wireless access point receives the 802.3 frame, removes the packet from the frame, and forwards the packet to the wireless host in an 802.11 frame.[7]

The packet goes all the way from the wireless host to a server. The 802.11 frame travels only between the wireless host and the wireless access point. The 802.3 frame travels only between the wireless host and the server.

The wireless access point also controls hosts. It assigns transmission power levels to hosts within its range and performs a number of other supervisory chores.

Test Your Understanding

17. a) Why must the access point remove an arriving packet from the frame in which the packet arrives and place the packet in a different frame when it sends the packet back out? b) Besides moving packets between wireless clients and the Ethernet network, what other control functions do access points have?

Basic Service Sets (BSSs)

We need to introduce a bit of jargon at this point. First, a **basic service set (BSS)** consists of an access point and the set of hosts it serves. In Figure 6-18, there are two BSSs.

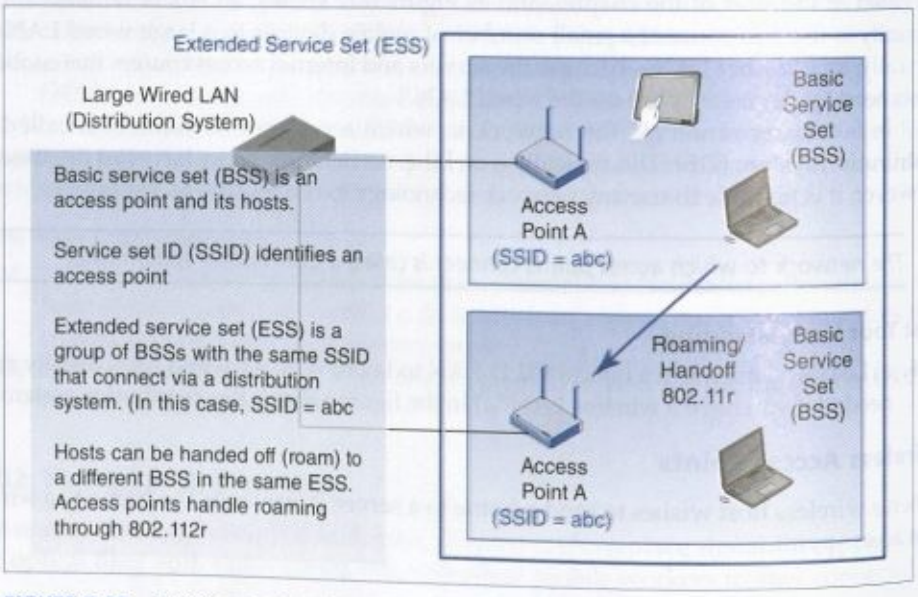

FIGURE 6-18 Basic Service Sets, Extended Service Set, and Roaming

[6] Note that 802.11 frames are much more complex than 802.3 Ethernet frames. Much of this complexity is needed to counter wireless propagation problems.

[7] This sounds like what a router does. However, a router can connect any two single networks. Access points are limited to connecting 802.3 and 802.11 networks.

A basic service set (BSS) consists of an access point and the set of hosts it serves

The access point in a BSS has an identifier called the **service set identifier (SSID)**. (Note that the term *basic* is not in the name.) Wireless hosts must know the SSID to associate with the access point. Fortunately, this is very easy to do.

Test Your Understanding

18. a) What is a BSS? (Do not just spell out the acronym.) b) What is an SSID? (Do not just spell out the acronym.) c) Does the access point have an SSID? d) Why must wireless devices know the access point's SSID?

Extended Service Sets (ESSS), Handoff, and Roaming

When a mobile host travels too far from a wireless access point, the signal will be too weak to reach the access point. However, if there is a closer access point, the host can be **handed off** to that access point for service. In WLANs, the ability to use handoffs is also called **roaming**.[8]

Roaming requires that both access points belong to the same extended service set. An **extended service set (ESS)** is a group of BSSs that are 1) connected to the same distribution system (network) and 2) have the same SSID.

An extended service set (ESS) is a group of BSSs that are 1) connected to the same distribution system (network) and 2) have the same SSID.

Figure 6-17 shows a wireless client communicating with an internal server. This is the service as users see it. However, access points also need to contact one another via the distribution system. For example, in roaming, they have to exchange information between themselves in order to hand off the client. To do so, they communicate via the **802.11r** standard, which is nicely named because it deals with roaming.

Access points also need to contact one another via the distribution system.

An organization with a single distribution system, like an Ethernet network, may have several different extended service sets. Each ESS will have its own SSID. It is even possible for an access point to be a member of multiple ESSs.

Test Your Understanding

19. a) What is a handoff in 802.11? b) What is the relationship between handoffs and roaming in WLANs? c) What is an ESS? (Do not just spell out the abbreviations.) d) What feature do all access points in an ESS share? e) How can access points communicate with each other? f) What is the purpose of the 802.11r standard?

[8] In cellular telephony, which we will see in Chapter 7, the terms *handoff* and *roaming* mean different things.

Sharing a Single Channel

As Figure 6-19 shows, the access point and all of the wireless hosts it serves transmit and receive in a single channel. When a host or the access point transmits, all other devices must wait. (If two devices transmit in the same channel at the same time, their signals will interfere with each other.) As the number of hosts served by an access point increases, individual throughput falls because of this waiting. The box "Controlling 802.11 Transmission" discusses how **media access control (MAC)** methods govern when hosts and access points may transmit so that collisions can be avoided.

Media access control (MAC) methods govern when hosts and access points may transmit so that collisions can be avoided.

The access point and all of the wireless hosts it serves transmit and receive in a single channel. When a host or the access point transmits, all other devices must wait.

Test Your Understanding

20. All wireless hosts and the access point that serves them transmit on the same channel. Why does this cause throughput to fall as the number of wireless hosts increases? Explain why.

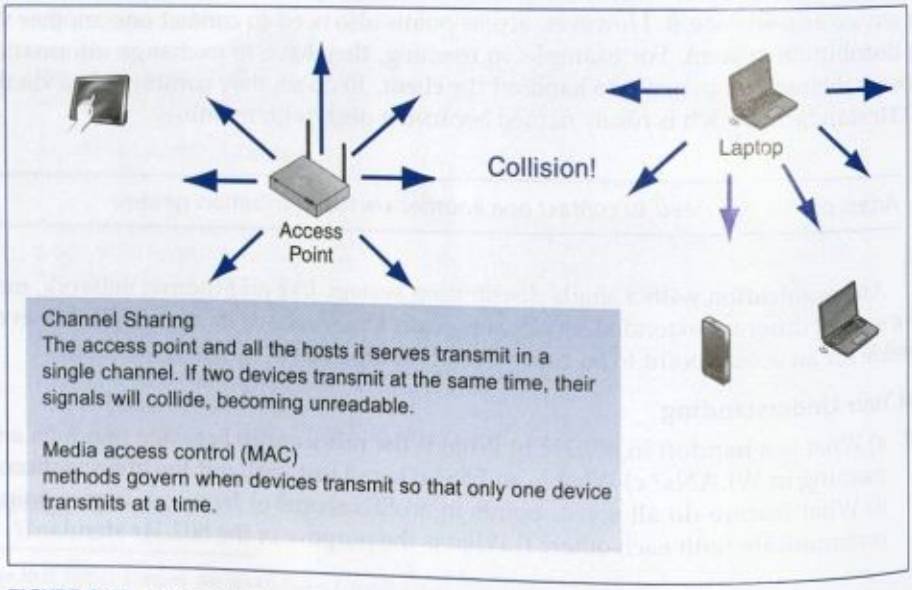

FIGURE 6-19 Hosts and Access Points Transmit on a Single Channel

Controlling 802.11 Transmission

Media Access Control

As noted in the body of the text, the access point and the hosts it serves all transmit in the same channel. If two 802.11 devices (hosts or wireless access points) transmit at the same time, their signals will be jumbled together and will be unreadable. This is called a **collision**.

The 802.11 standard has two mechanisms for **media access control (MAC)**—ensuring that hosts and the access point do not transmit simultaneously. The first, CSMA/CA+ACK, is mandatory. Access points and wireless hosts *must* support it. The second, RTS/CTS, is optional.[9]

Test Your Understanding

21. a) What is a collision? b) Why is it bad? c) What is the purpose of media access control? d) Does media access control limit the actions of wireless hosts, the access point, or both?

CSMA/CA+ACK Media Access Control

CSMA/CA

To reduce the number of collisions, wireless access points and wireless hosts use **carrier sense multiple access with collision avoidance (CSMA/CA)**. Note the focus on collision *avoidance*. Figure 6-20 illustrates CSMA/CA.

CSMA requires that a host refrain from transmitting if it hears traffic. This is a very simple rule. Carrier sensing means listening for traffic. Multiple access means that this is a way of controlling how multiple hosts can access the network to transmit.

CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance)

Sender listens for traffic

Carrier is the signal; sensing is listening

1. If there is traffic, waits
2. If there is no traffic:

2a. If there has been no traffic for less than the critical time value, waits a random amount of time, then returns to Step 1.

2b. If there has been no traffic for more than the critical value for time, sends without waiting

This avoids collision that would result if hosts could transmit as soon as one host finishes transmitting.

ACK (Acknowledgment)

Receiver immediately sends back an acknowledgment

If sender does not receive the acknowledgment, retransmits using CSMA

CSMA/CA plus ACK is a reliable protocol

FIGURE 6-20 CSMA/CA+ACK in 802.11 Wireless LANs

(continued)

[9] Actually, if you have even a single host with older 802.11b equipment connected to an access point, RTS/CTS becomes mandatory. However, 802.11b wireless hosts are almost never encountered anymore.

CSMA requires not transmitting if a device hears traffic. Collision avoidance (CA) is a set of two rules that determine what a host or the access point does if it does *not* hear traffic.

- If the host does not hear traffic, it considers the last time it heard traffic. If the time since the last transmission exceeds a critical value, the host may transmit immediately.
- However, if the time is less than the critical value, the host sets a random timer and waits. If there still is no traffic after the random wait, the host may send.

If the last two points seem odd, note that the goal is to avoid collisions as much as possible. Two hosts are most likely to transmit at the same time if they both have been waiting for another host to finish transmitting. Without the random delay, both will transmit at the same time, causing a collision.

ACK

More specifically, 802.11 uses **CSMA/CA+ACK**. Collisions and other types of signal loss are still possible with CSMA/CA. When a wireless access point receives a frame from a host, or when a host receives a frame from an access point, the receiver *immediately* sends an acknowledgment frame, an **ACK**. A frame that is not acknowledged is retransmitted. Note that there is no wait when transmitting an ACK. This ensures that ACKs get through while other hosts are waiting.

Note also that retransmission makes CSMA/CA+ACK a reliable protocol. We saw in Chapter 2 that very few protocols are reliable because reliability usually costs more than it brings in benefits. The low error rates in wired media simply do not justify implementing reliability in Ethernet and other wired LAN protocols. However, wireless transmission has many errors, so a reliable protocol is required for reasonably good operation.[10]

Thanks to CSMA/CA+ACK, 802.11 is a reliable protocol.

Inefficient Operation

CSMA/CA+ACK works well, but it is inefficient. Waiting before transmission wastes valuable time. Sending ACKs also is time consuming. Overall, an 802.11 LAN can only deliver throughput (actual speed) of about half the rated speed of its standard—that is, the speed published in the standard.

This throughput, furthermore, is aggregate throughput shared by the wireless access point and all of the hosts sharing the channel. Individual host throughput will be substantially lower.

Test Your Understanding

22. a) Describe CSMA/CA+ACK. Do not go into detail about how long a host must wait to transmit if there is no traffic. b) Is CSMA/CA+ACK transmission reliable or unreliable? Explain. c) Why is CSMA/CA+ACK inefficient?

Request to Send/Clear to Send (RTS/CTS)

Although CSMA/CA+ACK is mandatory, there is another control mechanism called **request to send/clear to send (RTS/CTS)**. Figure 6-21 illustrates RTS/CTS. As noted earlier, the RTS/CTS protocol is optional except in one rare case. Avoiding RTS/CTS whenever possible is wise because RTS/CTS is much less efficient, and therefore slower, than CSMA/CA+ACK.

[10] In addition, 802.11 uses forward error correction. It adds many redundant (extra) bits to each frame. If there is a small error, the receiver can use these redundant bits to fix the frame. If the receiver can make the repair, it does so and then sends back an ACK. This process makes wireless NICs more expensive than Ethernet NICs, but wireless transmission errors are so common that it makes economic sense to correct errors at the receiver in order to minimize retransmissions.

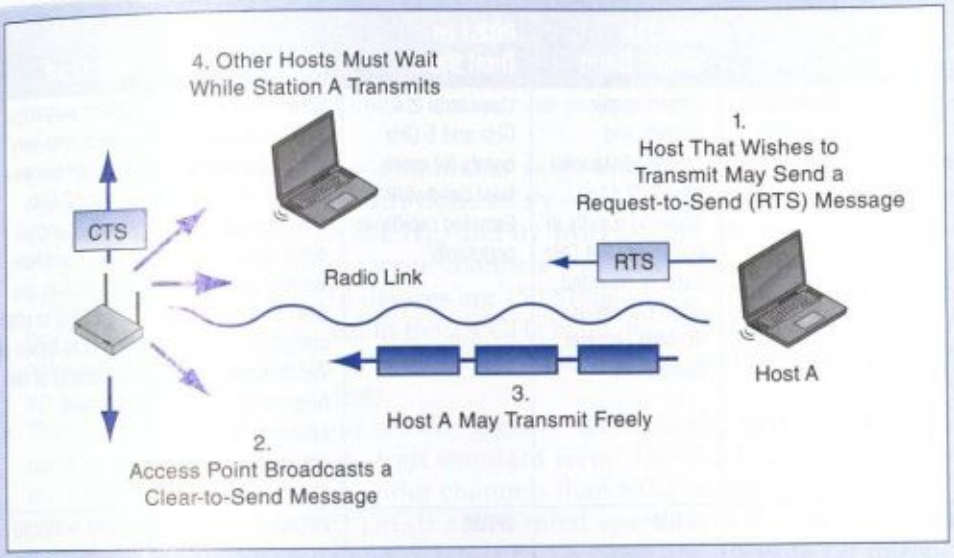

FIGURE 6-21 Request to Send/Clear to Send

When a host wishes to send and is able to send because of CSMA/CA, the host may send a **request-to-send (RTS)** message to the wireless access point. This message asks the access point for permission to send messages.

If the access point responds by broadcasting a **clear-to-send (CTS)** message, then other hosts must wait. The host sending the RTS may then transmit, ignoring CSMA/CA.

Although RTS/CTS is widely used, keep in mind that it is only an option, while CSMA/CA is mandatory. Also, tests have shown that RTS/CTS reduces throughput when it is used.

RTS/CTS makes sense primarily when two wireless clients can both hear the access point but cannot hear each other. If CSMA/CD+ACK is used, the two stations may transmit at the same time.

Test Your Understanding

23. a) Describe RTS/CTS. b) Is CSMA/CA+ACK required or optional? c) Is RTS/CTS required or optional? d) Which is more efficient, RTS/CTS or CSMA/CA+ACK? e) When does RTS/CTS make sense to use?

802.11 TRANSMISSION STANDARDS

The 802.11 Working Group has created several WLAN transmission standards since 1997. We will look at the most important of these standards today.

Characteristics of 802.11g, 802.11n, 802.11ac, and 802.11ad

Figure 6-22 compares the 802.11g and 802.11n standards that dominate usage today and the 802.11ac and 802.11ad standards that are just entering the market.

Characteristic	802.11g	802.11n Single Band	802.11n Dual Band	802.11ac	802.11ad
Status	Obsolete but widely used	Offers longer speeds and greater distances than 802.11g Growing rapidly in popularity 2.4 GHz band is crowded; often cannot use 40 MHz channel bandwidth	Uses both 2.4 GHz and 5 GHz bands for more total bandwidth Growing rapidly in popularity	Offers much higher speed in the 5 GHz band through wider channels and other technical innovations. Standard is not complete, but vendors are beginning to offer products based on late drafts of the standard.	Offers very high speed over very short distances in the 60 GHz band. Standard is not complete, but vendors are beginning to offer products based on late drafts of the standard.
Spread Spectrum Method	OFDM	OFDM	OFDM	OFDM	OFDM or Single Channel for lower speed
Unlicensed Band(s)	2.4 GHz	2.4 GHz	2.4 GHz and 5 GHz	5 GHz	60 GHz
Channel Bandwidth	20 MHz	40 MHz, but will drop back to 20 MHz if there is interference on the two selected channels	40 MHz, but will drop back to 20 MHz if there is interference on the two selected channels	80 MHz or 160 MHz	2.1 GHz
Number of Non-Overlapping Channels (varies by country)	3	3 in 2.4 GHz band	3 in 2.4 GHz band; 12 in the United States in 5 GHz band The 5 GHz band is still relatively uncrowded.	6 at 80 MHz channel bandwidth and 3 at 160 MHz bandwidth in the United States	3 in the United States, 4 in Europe
MIMO?	No	Yes	Yes	Yes	Yes
Maximum Number of Spatial Streams			4	8	
Multiuser MIMO/ Beamforming?	No	Yes but no single standard	Yes but no single standard	Yes, and only one standard	
Rated Speed	54 Mbps	100 Mbps to 600 Mbps; 300 Mbps common.	100 Mbps to 600 Mbps; 300 Mbps common.	433 Mbps to 6.9 Gbps; 867 Mbps and 1.3 Gbps common.	7 Gbps
Typical Maximum Distance for Rated Speed	30 m (100')	70 m (230')	70 m at 2.4 GHz 50 m at 5 GHz		

FIGURE 6-22 Main 802.11 Standards

- The 802.11g standard is obsolete, but it offers a good rated speed of 54 Mbps up to about 30 meters (100 feet). Even if only a single user is accessing an access point, he or she will only get throughput of about half of that rated speed. The standard has a large installed base of clients and access points that need to continue to be supported.
- The 802.11n standard now dominates sales and will soon dominate the installed base if it has not already done so. By offering wider channels and other technical innovations than 802.11g, and by working in both the 2.4 GHz and 5 GHz bands, 802.11n offers more channels and faster channels than 802.11g. The rated speeds of 802.11n devices are 150 Mbps to 600 Mbps, with 300 Mbps being a common rated speed. In the 2.4 GHz band, the maximum speed is available up to 70 meters (230 feet). In the 5 GHz band, the maximum speed is available up to about 50 meters (160 feet).
- The 802.11ac standard is one of two "gigabit" technologies that are just beginning to reach the market in draft standard form. The 802.11ac standard uses the 5 GHz band along with wider channels than 802.11n and even more technical innovations than 802.11n. It offers rated speeds of 433 Mbps to nearly 7 Gbps, and rated speeds of 433 Mbps to 1.3 Gbps are likely to be common initially.
- The 802.11ad standard is a radical break from earlier standards. Instead of using the 2.4 GHz and 5 GHz bands, it operates in the 60 MHz band. Its rated speed is an enormous 7 Gbps, but absorptive attenuation is so high in the 60 GHz band that distance will be limited to about 10 meters. This will make it ideal for streaming high-definition video, even if multiple HDTV channels are required.

Although gigabit speeds may seem like overkill, it makes new applications possible. In consumer applications, it will make the streaming of multiple simultaneous television signals possible. About a third of all U.S. houses have four or more televisions today, and HD is becoming the norm. For business, data backup and synchronization will become feasible to do wirelessly.

Test Your Understanding

24. a) Of the four 802.11 transmission standards summarized in this section, which are full standards, and which are only draft standards? b) What is the maximum rated speed for each standard? c) Compare maximum speeds for 802.11g and 802.11n and the maximum distances at which each standard can provide these speeds. d) Which can bring gigabit speeds to clients? e) What business application will gigabit transmission speed make feasible to do wirelessly?

Spread Spectrum Method

Figure 6-22 shows that all four standards use OFDM as their main spread spectrum method. The 802.11ad standard has an alternative single-carrier mode, in which the subcarriers of OFDM are not used. The signal is spread across the entire channel. This is simple enough to be implemented on hand-held devices, at the cost of substantially lower speed.

Test Your Understanding

25. What spread spectrum method do all four standards use as their main method?

Bands and Channel Bandwidth

Earlier in this chapter, we saw that transmission speed is highly dependent upon channel bandwidth. Other things being equal, doubling channel bandwidth doubles transmission speed. However, service bands have limited total bandwidth, so wider channels means fewer channels.

802.11G CHANNEL BANDWIDTH The 802.11g standard operates only in the crowded 2.4 GHz band. With channel bandwidth of 20 MHz, only three 802.11g channels are possible.

802.11N CHANNEL BANDWIDTH The 802.11n standard operates in both the 2.4 GHz band and the less-crowded and wider 5 GHz band. It also doubles 802.11g bandwidth to 80 MHz. This alone roughly doubles speed. However, early 802.11n products were single-band 802.11n products that operated only in the 2.4 GHz band. In this band, there are already many 802.11g stations operating on 20 MHz channels. To be a good neighbor, when there are stations operating on the three possible channels, 802.11n products will drop back to a 20 MHz channel bandwidth, losing their channel bandwidth advantage. Dual-band 802.11n products operate in both the 2.4 GHz band and the 5 GHz band. In the higher band, 40 MHz channels are widely available. In other words, 802.11n reaches its full expression only in the 5 GHz band.

802.11AC CHANNEL BANDWIDTH The emerging 802.11ac standard has even wider channels. Support for 80 MHz channels is mandatory, and support for 160 MHz channels is likely to gain quick support. Doubling and quadrupling channel bandwidth compared to 802.11n means roughly a doubling and quadrupling of transmission speeds, other things being equal. Of course, having wider channels means having fewer channels. In the United States, available spectrum capacity in the 5 GHz band can handle twelve 802.11n channels, but it can support only six 80 MHz channels or three 160 MHz channels.

802.11AD CHANNEL BANDWIDTH The emerging 802.11ad standard, as just noted, uses the 60 GHz band, which has a total bandwidth of about 7 GHz to 9 GHz. (In contrast, the 5 GHz band has less than 1 GHz of bandwidth.) However, 802.11ad channels are an enormous 2.1 GHz wide. In the United States, there are only three non-overlapping 802.11ad channels, while Europe can support four with its wider 60 GHz band spectrum capacity. Fortunately, because 60 GHz signals do not travel far, mutual channel interference should not be a major problem.

Test Your Understanding

26. a) Why is wider channel bandwidth good? What is the downside of wider channel bandwidth? b) What frequency band or bands do 802.11g, 802.11n single band, 802.11n dual band, 802.11ac, and 802.11 ad use? c) For each, compare channel bandwidth and the number of possible channels. d) What are the benefits and problems of transmission in the 60 GHz band?

MIMO

Increasing bandwidth is the easiest way to boost transmission speed, but there are other less brute force way to increase speed without increasing bandwidth. Figure 6-23 notes

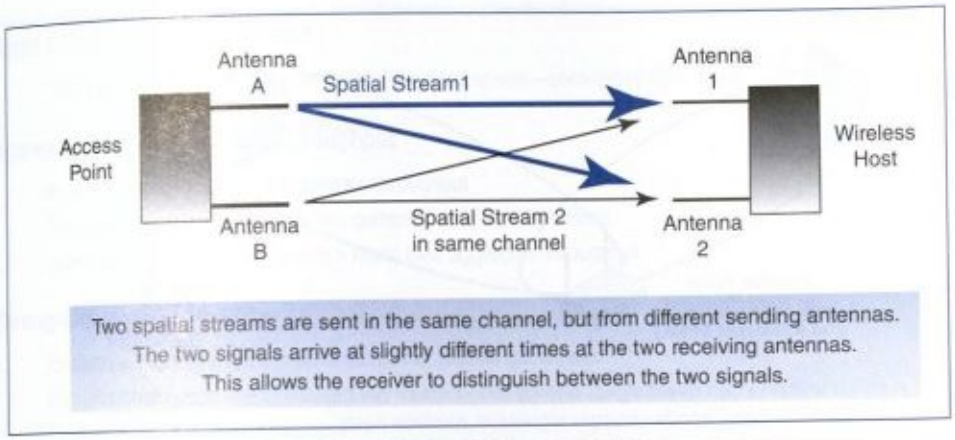

FIGURE 6-23 Multiple Input/Multiple Output (MIMO) Transmission

that standards beyond 802.11g use a technique called **multiple input/multiple output (MIMO)** to achieve speeds far more than increasing bandwidth alone can provide.

The key to higher throughput in MIMO is that the host or access point sends two or more **spatial streams** (radio signals) in the same channel between two or more different antennas on access points and wireless hosts.

In the figure, there are two spatial streams. Transmitting in the same channel, they should interfere with each other. However, the two spatial streams sent by different antennas will arrive at the two receiving antennas at slightly different times. Using detection and separation methods based on differences in arrival times for the two spatial streams, the receiver can separate the two spatial streams in the same channel and so can read them individually.

Even with only spatial streams and two antennas each on the sender and receiver, MIMO can substantially increase throughput. Using more spatial streams and more antennas can increase throughput even more. The MIMO standard will permit two, three, or four antennas on each device and up to four data streams.

With two spatial streams, rated speed in 802.11n with 40 MHz channels is 300 Mbps. Three spatial streams raise the rated speed to 450 Mbps, and four raise it to 600 Mbps. The 802.11n standard requires access points to support four spatial streams, although wireless hosts are only required to support two spatial streams. Typical speeds in 802.11n products today have rated speeds of 150 Mbps to 300 Mbps.

The 802.11ac standard, in addition to doubling or quadrupling channel bandwidth compared to 802.11n, doubles the number of possible spatial streams to eight. The standard offers many possible combinations of bandwidth (80 MHz or 160 MHz) and number of spatial streams (1 to 8). This creates a large number of possible rated speeds, beginning at 433 MHz and extending to 6.93 GHz. Of these, 433 Mbps, 867 Mbps, and 1.3 Gbps are likely to be offered the most when products appear.

Another benefit of MIMO, beyond greater transmission speed, is greater transmission distance. The reasons for this are rather technical, but it is the end result that is important. Greater propagation distances may permit fewer access points to be installed, and this will lower equipment and installation cost.

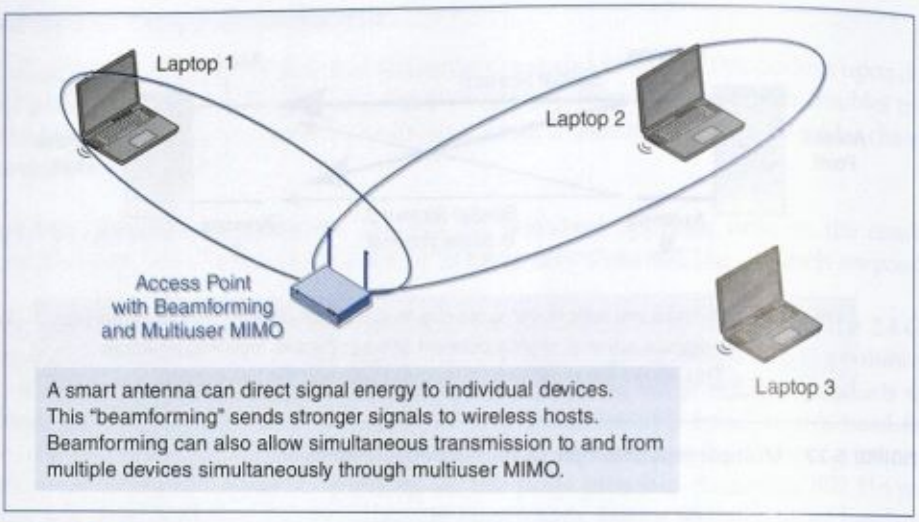

FIGURE 6-24 Beamforming (Multiuser MIMO or Smart Antennas)

Test Your Understanding

27. a) How does MIMO work? b) What is the main benefit of MIMO? What is its other benefit? c) Compare the range of rated speeds possible 802.11g with 40 MHz channels and 802.11ac.

Beamforming and Multiuser MIMO

Another technology to increase propagation and speed is beamforming. By having multiple antennas and changing the phase of waves coming from different antennas, an access point can focus signals toward individual hosts instead of broadcasting them, as Figure 6-24 indicates. This is called **beamforming**. It gives more effective power and therefore a stronger signal to each wireless host. This permits greater propagation distance. Devices that do beamforming are said to have **smart antennas**.

Beamforming can also bring **multiuser MIMO**, which is the possibility of simultaneous transmission in a single channel by multiple devices that are using a single access point.

The 802.11n standard specified multiuser MIMO, but it did not specify a single multiuser MIMO technology. This led to a great deal of market confusion, and multiuser MIMO did not become popular with 802.11n. With 802.11ac, the Technical Group 802.11ac avoided market confusion by specifying a single multiuser MIMO technique. Beamforming is likely to be common in 802.11ac products.

Test Your Understanding

28. a) What is beamforming? b) What two benefits can it bring? c) Distinguish between MIMO and multiuser MIMO. D) What is another name for beamforming?

Speed, Throughput, and Distance

So far, we have been talking about rated speeds. But what throughput—actual speed—can individuals expect to see? The general answer is complicated, but the single most important word is *less*. Individual users will always receive less than rated speeds, often much less.

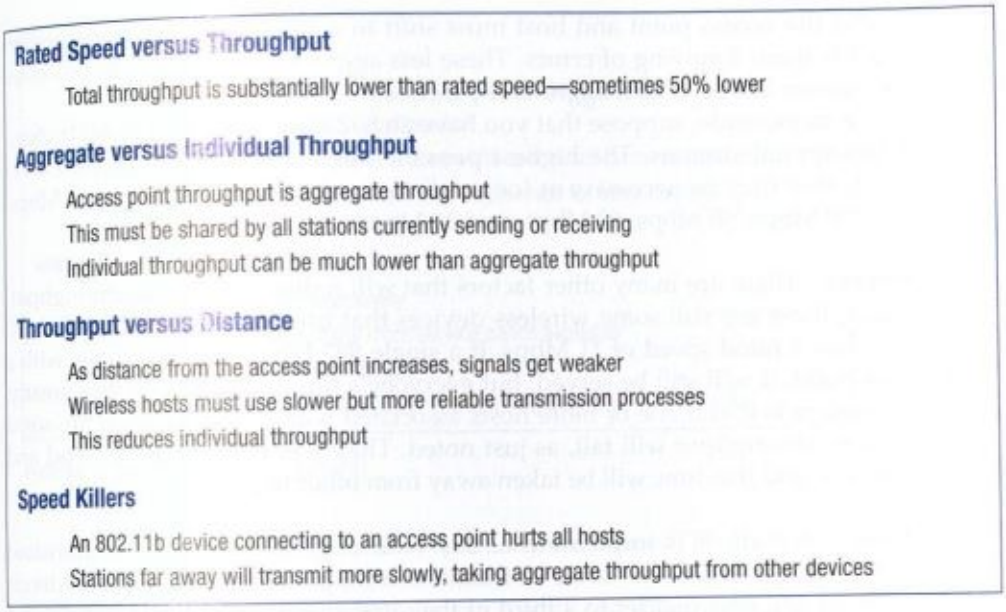

FIGURE 6-25 Speed, Throughput, and Distance (Study Figure)

RATED SPEED VERSUS THROUGHPUT Rated speed is the number of bits that the host or access point will transmit per second. As noted earlier, stations often have to wait to transmit, even if no other station is transmitting. In addition, wireless frames contain many extra bits to improve transmission reliability, even beyond the normal overhead of frame headers. For 802.11g, the highest actual throughput is about half the rated transmission speed. For standards beyond 802.11g, actual throughput is somewhat closer to rated speeds, but throughput of about two-thirds of the rated speed is about the highest possible throughput.

AGGREGATE THROUGHPUT VERSUS INDIVIDUAL THROUGHPUT In addition, access point throughput is *aggregate* throughput, which is shared by all users of an access point. Suppose that the aggregate throughput is 100 Mbps per second and there are 10 users of an access point. If all 10 transmit or receive simultaneously, then *individual* throughput would be about 10 Mbps (actually somewhat less because of time lost in turn-taking). Of course, it would be rare for all stations to transmit simultaneously. However, even if three are sending and receiving simultaneously, the individual throughput they experience would be about 30 Mbps.

What percentage of time do hosts transmit or receive? It depends entirely on what they are doing. Web downloads occur about every 30 seconds and take only a second or two to download on a fast host. However, streaming video creates an almost continuous data stream, consuming a good deal of the aggregate throughput.

THROUGHPUT VERSUS DISTANCE Another consideration is that speed is highest when a user is very near an access point. As the user moves away, speed falls. The problem is that at maximum transmission speed, there must be almost perfect propagation characteristics. As a user moves away from an access point, signal strength falls, errors

increase, and the access point and host must shift to a less aggressive transmission process that is more forgiving of errors. These less aggressive transmission processes are always slower than the most aggressive processes.

To give an example, suppose that you have an 802.11n host with a 40 MHz channel and two spatial streams. The highest possible rated speed is 300 Mbps. Lower rated speeds that may be necessary at longer distances include 270 Mbps, 240 Mbps, 180 Mbps, 120 Mbps, 90 Mbps, 60 Mbps, and 30 Mbps.

SPEED KILLERS There are many other factors that will reduce individual throughput. For example, there are still some wireless devices that use the old 802.11b standard, which only has a rated speed of 11 Mbps. If a single 802.11b device associates with a later access point, it will still be served, but everyone's throughput will suffer greatly. Another problem is that if one or more hosts associated with an access point are some distance away, throughput will fall, as just noted. They will take longer to send and receive packets, and this time will be taken away from other users.

IN GENERAL Overall, it is impossible to say with any certainty what individual throughput a user will receive. A rule of thumb that frequently works is that individual throughput will be a quarter to a third of the rated speed if the access point is not overloaded.

Test Your Understanding

29. a) Distinguish between rated speed, aggregate throughput, and individual throughput. b) What factors influence individual throughput, given a certain level of aggregate throughput? c) Why does transmission speed drop as a computer moves farther from an access point? d) How does the presence of a distant station harm all users of an access point?

Backward Compatibility

When new access points and wireless clients are created, they must be able to work with older equipment. For instance, an 802.11n client must be able to work with an older 802.11g access point. In the same way, an 802.11n access point must be able to work with an older 802.11g access point. Of course, when an 802.11n device works with an 802.11g device, the transmission can take place only at 802.11g speeds. The 802.11n device must drop back to 802.11g operation. This is called **backward compatibility**. Newer devices usually contain multiple radios so that they can work with newer and older devices.

Test Your Understanding

30. a) What is backward compatibility? b) Why do you think it is important? c) When a device designed to use a newer standard must work with a device that only uses an older standard, what standard do they use to communicate?

On the Horizon

Wireless standards are evolving in dog years. Although 802.11ac and 802.11ad are obvious things to consider for the future, there are other issues as well.

In the United States, UHF television channels were required to give up analog operation and relinquish their channels. The Federal Communications Commission

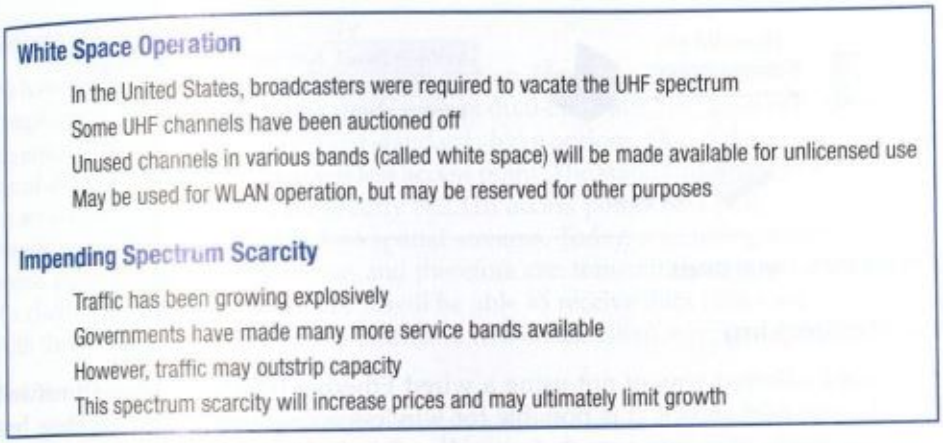

FIGURE 6-26 Trends (Study Figure)

sold some of these channels at auction, but many are unused. The FCC is now considering how equipment can use empty channels (known as **white space**) on an opportunistic basis. This can provide more spectrum capacity for WLAN operation, cellular and similar service, or both. Regulatory agencies around the world are now considering how to allocate white space.

In general, governments have recently made many new blocks of frequency spectrum available to satisfy exploding demands for WLAN operation, cellular telephony, and other wireless data transmission technology. However, demand for spectrum capacity is growing very rapidly, and unless more efficient wireless transmission methods emerge very rapidly, spectrum capacity will place limits on demand growth. Well before that occurs, spectrum scarcity will increase transmission prices.

Test Your Understanding

31. a) What is white space, and why is using it attractive? b) Why may spectrum scarcity be a problem? d) If spectrum scarcity becomes a problem, how will that affect users?

ADVANCED OPERATION

We have been discussing 802.11 WLANs that connect to the corporate wired LAN for backbone transmission. However, two developments will implement 802.11 transmission in different ways.

Wi-Fi Direct

If two 802.11 devices are physically near each other, why go through a wired LAN or even an access point? Figure 6-27 shows that **Wi-Fi Direct**, which is being built into emerging transmission standards, permits direct transmission between two 802.11 devices without using an access point. Although this is a desirable use of 802.11 transmission, two nearby devices can also connect directly through Bluetooth and Near Field Communication (NFC), which we will see in Chapter 7.

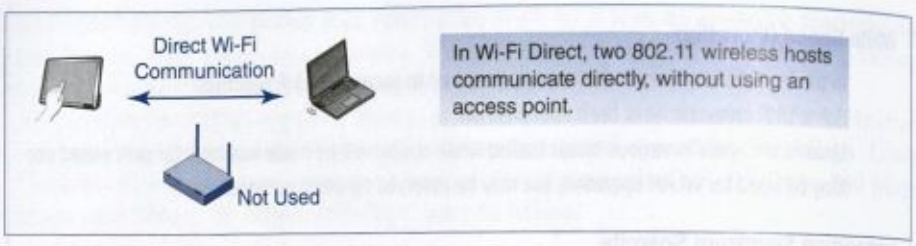

FIGURE 6-27 Wi-Fi Direct

Mesh Networking

A more sophisticated way of not using a wired Ethernet backbone is mesh networking. As Figure 6-28 shows, it is possible for wireless access points and wireless hosts to organize themselves into a mesh, forwarding frames from one to another until they reach the wireless destination host.

The **802.11s** standard for mesh networks exists. However, there are many other subsidiary standards that need to be developed before mesh networking's issues can be resolved sufficiently to be useful in corporations. Standards must address three main issues.

- First, meshes must be self-organizing. If hosts and access points enter and leave the mesh frequently, the amount of processing power consumed in maintaining the routing tables on the access points and wireless hosts must not be substantial.
- Second, it will be difficult to avoid overloading access points near the geographical center of the mesh. (Think of sitting in the middle seat at a table during a Christmas dinner and constantly having to pass food back and forth.) If mesh networking works but does not work well, it will have little value.
- Third, an even bigger issue is security. With no central control, security will have to exist between pairs of devices, many of which will have just entered the mesh and are not well known. This is a recipe for security nightmares.

Test Your Understanding

32. a) How does Wi-Fi Direct differ from the traditional way in which two wireless hosts communicate? b) Can a large Wi-Fi network operate without an Ethernet switched backbone? c) What technology allows this? d) What is the current 802.11 standard for this technology? e) What devices forward frames in a mesh network? f) What three issues must be overcome to make mesh networking acceptable to corporations?

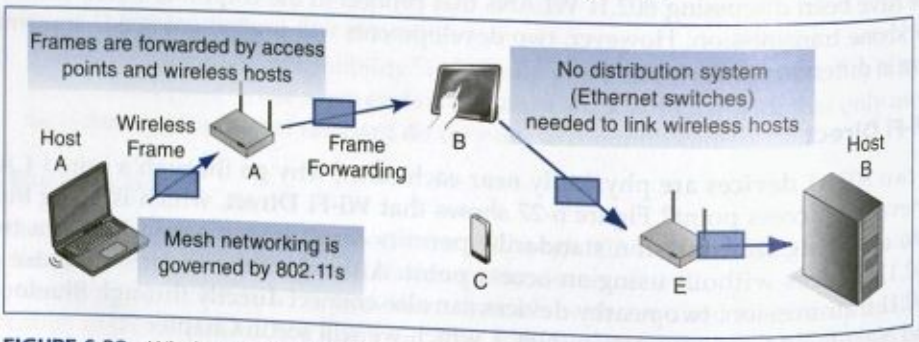

FIGURE 6-28 Wireless Mesh Networking

Standards and Compatibility

We have looked at many standards in this section. However, just because two products are compliant with a particular standard, such as dual-band 802.11n, does not mean that they are equal. This is true because most standards have options. One, for example, is the number of antennas on an 802.11n wireless access point. The standard calls up to four antennas on an access point. In fact, most early 802.11n access points had only two antennas and therefore could only transmit two spatial streams. Today, a growing number of 802.11n access points have three antennas and therefore can transmit three spatial streams. Even if a client has only two antennas, it will be able to receive data faster and more reliably. With three antennas on the access point and two on the client, a typical speed gain in 67%.

Test Your Understanding

33. a) Why can two products that comply with the same standard have different performance? b) What is the advantage of having three antennas rather than two on an access point?

CONCLUSION

Synopsis

Chapter 5 looked at Ethernet switched local area networks. This chapter and Chapter 7 look at wireless LANs (WLANs). All single networks, whether switched or wireless, operate at Layers 1 and 2. OSI standards dominate at those layers, so we can expect all wireless network standards to be OSI standards.

This chapter spends a long time on physical layer propagation. This detail is needed because wireless propagation effects are complex. We can predict what will happen as a signal travels down copper wire or optical fiber, but predicting how strong a radio signal will be where a user is located is far more difficult. We looked at five wireless propagation problems: absorptive attenuation, inverse square law attenuation (yes, there are two types of attenuation), interference, shadow zones, and multipath interference. Multipath interference occurs when the destination device receives multiple signals, with some coming directly from the radio source and some bouncing off walls, ceilings, and other objects. The direct and reflected signals may interfere with each other, making the direct signal unreadable. Multipath interference is the biggest propagation problem in wireless LANs. Absorptive attenuation and shadow zones become worse at higher frequencies.

We looked at two types of antennas—omnidirectional antennas and dish antennas. Wireless LANs use omnidirectional antennas because users would not know where to point a dish antenna and certainly do not want to carry a dish around. Fixed users may use dishes pointing at a distant radio source to have stronger transmission and reception.

We looked at basic radio concepts, including the frequency spectrum that consists of all frequencies from 0 Hz to infinity. (Radio propagation is described by frequency, which is measured in hertz.) Service bands are contiguous chunks of the frequency spectrum that are reserved for particular purposes, such as FM radio, television, or police communication. Service bands are divided into channels. Signals are sent in a single channel, and signals in different channels do not interfere with each other. Most commercial wireless services and corporate WLANs operate in the golden zone, which lies between 500 MHz and 10 GHz. In this golden zone, there is good spectrum capacity plus good propagation characteristics.

Radio signals do not propagate at a single frequency. They spread over a range of frequencies, and the spread increases as signal speed increases. Consequently, to carry fast signals, channels must have wide bandwidth. According to the Shannon Equation, doubling bandwidth should double possible signal speed.

Most radio bands are licensed, meaning that you need a government license to operate and a new license every time you move an antenna. Obviously, that would not work with wireless LAN. Consequently, wireless LANs operate in unlicensed bands. In an unlicensed band, you can set up your network the way you wish. However, you must tolerate interference from nearby WLANs built by others.

Most WLAN technology operates in the 2.4 GHz band, in which radio prices are low and reception is good. However, there are only three non-overlapping channels in this band, so nearby access points often interfere with one another. Some WLAN equipment operates in the 5 GHz unlicensed band, in which there are one or two dozen channels, depending on the country. The 5 GHz band is uncrowded, and the gap between 2.4 GHz prices and 5 GHz prices is narrowing. Consequently, use of the 5 GHz band is beginning to grow rapidly.

In the 2.4 GHz and 5 GHz bands, propagation effects tend to be worse at certain frequencies. This is especially true of multipath interference. Consequently, the government requires the use of spread spectrum transmission, in which the signal is spread far more than it needs to be for its speed. By sending a signal over a much wider range of frequencies, frequency-specific problems tend to be washed out. The two dominant WLAN standards, 802.11g and 802.11n, both use orthogonal frequency division multiplexing (OFDM), in which the channel is broken into much smaller channels called subcarriers. The frame is transmitted redundantly within the subcarriers. WLAN spread spectrum techniques, unlike military spread spectrum techniques, do not provide security.

In 802.11 WLAN operation, access points normally attach to the firm's main wired Ethernet LAN so that wireless clients can access servers and Internet access routers on the wired LAN. When a wireless host transmits, it sends its packet in an 802.11 frame. The access point removes the packet from the 802.11 frame, puts it in an 802.3 frame, and sends the frame to the server or Internet access router. The packet travels all the way; the 802.11 frame does not. We saw that when users move between access points, they can be transferred automatically to the new access point. This is called handoff or roaming. We defined the terms *basic service set*, *service set ID*, and *extended service set*. A BSS is an access point and the wireless stations it serves. The SSID is the name of a radio on an access point. In an ESS, all access points have the same SSID. Among other things, this permits roaming, which is also called being handed off.

The access point and the stations it serves all transmit in a single channel. Media access control is needed to ensure that they take turns transmitting so that their signals do not interfere. Wireless hosts that want to transmit often have to wait their turns. This reduces individual throughput. A box described the two main media access control protocols. CSMA/CA+ACK is mandatory on access points. Request to send/clear to send is optional but sometimes useful.

WLAN products on the market follow one of two 802.11 standards and two 802.11 draft standards. The 802.11g standard allows equipment to be less expensive but has lower speed and distance. The 802.11n standard is much more advanced. Products using 802.11n have higher speeds and longer propagation distances. The 802.11n standard now dominates in terms of sales, although there will be a large installed base of 802.11g products for several years to come. All 802.11n products are backward-compatible with 802.11g, so there is no problem mixing products from

the two standards together, although they will all operate with 802.11g performance. Two draft standards are also being used in new equipment sold by vendors. These are 802.11ac and 802.11ad. Both can give gigabit transmission speeds, allowing such tasks as backup and data synchronization to be done in a reasonable amount of time.

Figure 6-22 compares these four 802.11 transmission standards. One consistent theme for newer versions is the use of ever-wider channel bandwidths, which bring ever-higher rated speeds. The 802.11g standard uses 20 MHz-wide channels. The 802.11n standard doubles this, except when there is interference from 802.1g devices in the 2.4 GHz band. The 802.11ac standard beings 80 MHz and 160 MHz channels, and 802.11g brings enormous 2.1 GHz channels. While 802.11g uses the crowded and limited 2.4 GHz band, 802.11n and 802.11ac can take advantage of the wider 5 GHz band's far greater total bandwidth. The 802.11ad standard moves to the ultrawide 60 GHz band, but absorptive attenuation is very high in this band, so 802.11ad signals are limited to about 10 meters.

Another way to boost speed is MIMO, which uses multiple antennas on the sender and receiver. The signals sent by different antennas are called spatial streams. The sender can transmit multiple spatial streams in the same channel, and the receiver will be able to read them. Roughly speaking, transmission speed approximately increases in proportion to the number of spatial streams. The 802.11g standard does not use MIMO. The 802.11n standard uses MIMO and can support up to four spatial streams. The 802.11ac standard can support up to eight.

The 802.11n, 802.11ac, and 802.11ad standards can also use beamforming, which uses smart antennas to direct signals to and from individual devices instead of broadcasting signals omnidirectionally. Beamforming increases distance by focusing more of the sender's power on the receiver. A particularly sophisticated type of beamforming is multiuser MIMO, which allows multiple stations to transmit simultaneously. The access point can use their different spatial streams to separate their signals. If one station is sending, other stations do not have to wait to send. The 802.11n standard did not specify a single beamforming standard, and market confusion has largely left beamforming out of 802.11n technology. The 802.11ac standard specifies a single beamforming standard, and beamforming is likely to be common in 802.11ac products.

It is easy to talk about rated speeds, but actual throughput is more difficult to discuss. Throughput is always slower than rated speed, and this is aggregate throughput shared by all devices transmitting simultaneously. Consequently, individual throughput is always lower. In addition, as a station moves farther from the access point, it must use slower transmission processes, further reducing individual throughput. In addition if a single older 802.11b host connects to an access point, everyone's throughput will suffer, and a single station far from the access point may transmit so slowly that it will take a substantial amount of the total aggregate throughput.

On the horizon, access points may be able to use unused spectrum in bands designated for other purposes. This could help alleviate a likely shortage of total spectrum capacity.

We looked briefly at two 802.11 approaches that do not use a switched Ethernet backbone to connect access points. Wi-Fi Direct allows two 802.11 hosts to communicate directly, without even using an access point. Mesh networks, in turn, use access points and client hosts to forward 802.11 frames wirelessly between two wireless hosts. This forwarding process may require several hops among wireless devices.

In Chapter 7, we will continue to look at 802.11 wireless LANs, focusing on security and management. We will then look at other local wireless technologies, including Bluetooth.

END-OF-CHAPTER QUESTIONS

Thought Questions

1. Reread the Christopher Lorek case. Are any terms still unfamiliar to you? Would you give the same advice? Why or why not?
2. The first letter part in this question was previously asked as a test your understanding question. Telephone channels have a bandwidth of about 3.1 kHz. Do the following in Excel. Cut and paste your analyses into your homework. a) If a telephone channel's signal-to-noise ratio is 1,000 (the signal strength is 1,000 times larger than the noise strength), how fast can a telephone channel carry data? (Check figure: Telephone modems operate at about 30 kbps, so your answer should be roughly this speed.) b) How fast could a telephone channel carry data if the SNR were increased massively, from 1,000 to 10,000? (This would not be realistic in practice.) c) With an SNR of 1,000, how fast could a telephone channel carry data if the bandwidth were increased to 4 kHz? Show your work or no credit. d) What did you learn from these three analyses?
3. A building has four sides that are each 100 meters long. The building is 100 meters tall. Draw a picture. a) If access points have a service radius of 25 meters, how many access points would you need? b) If access points have a range of 33 meters, how many access points would you need. c) What did you learn from your answers?
4. The following matters were not addressed specifically in the text. However, if you understand the concepts of Layer 1 and Layer 2 standards, in each case, give your answer and explain your reasoning. a) Is multipath interference a Layer 1 or Layer 2 concern? b) Is media access control a Layer 1 or Layer 2 concern? c) Is MIMO a Layer 1 or Layer 2 concern? d) Are wireless propagation problems Layer 1 or Layer 2 concerns?

Design Question

1. Consider a one-story building that is a square. It will have an access point in each corner and one in the center of the square. *All access points can hear one another.* a) Assign access point channels to the five access points if you are using 802.11g. Try not to have any access points that can hear each other use the same channel. Available channels are 1, 6, and 11. b) Were you able to eliminate interference between access points? c) Repeat the first two parts of the question, this time using 802.11a. Available channels are 36, 40, 44, 48, 53, 56, 60, 64, 149, 153, 157, and 161, but many NICs and access points only support channels below 100.

Troubleshooting Question

1. When you set up an 802.11g wireless access point in your small business, your aggregate throughput is only about 6 Mbps. a) List at least two possible reasons for this low throughput. b) Describe how you would test each. c) Describe what you would do if each proved to be the problem.

Perspective Questions

1. What was the most surprising thing you learned in this chapter?
2. What was the most difficult part of this chapter for you?

6a USING XIRRUS WI-FI INSPECTOR

LEARNING OBJECTIVES

By the end of this chapter you should be able to:

- Use Xirrus Wi-Fi Inspector with some facility.
- Interpret output from Wi-Fi Inspector in specific situations.
- Do a site survey.

INTRODUCTION

Wi-Fi analysis programs listen to nearby access points (and sometimes wireless hosts) to determine such things as how strong their signals are, what types of security they use, what their SSIDs and BSSIDs are, and sometimes the directions of the individual access points.

There are many Wi-Fi analysis programs for mobile devices. Many have "stumbler" in their names in homage to one of the first examples, NetStumbler. This chapter looks at *Wi-Fi Inspector* from Xirrus, which runs on Microsoft Windows and which is available as a free download from Xirrus. A comparable Windows Widget that always remains on the desktop is also available from Xirrus.

THE FOUR WINDOWS

Figure 6a-1 shows the ribbon menu and four tiled windows that appear when you bring up Wi-Fi Inspector. This view shows all information in a single Window. This is the default. It is also what you see if you click on Show All in the Layout ribbon.

The Radar Window (Read the Fine Print)

The most obvious window is the radar window, which shows all access points in the vicinity. The access points are spread out across the two-dimensional picture.

RELATIVE DIRECTION (MEANINGLESS) It appears that the radar window shows the relative directions of the access points, much as an air traffic radar display shows the directions of nearby aircraft. Actually, it does not. The access points are merely spread out

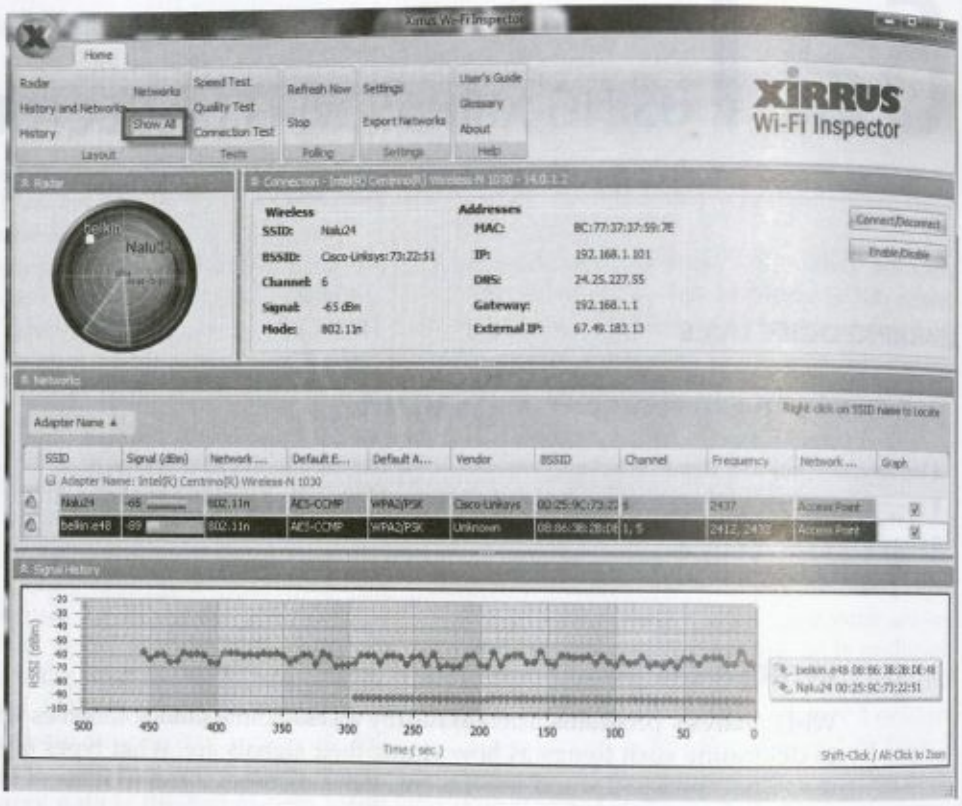

FIGURE 6a-1 Four Windows in Wi-Fi Inspector

Source: © 2012 Xirrus, Inc.

for readability. Direction is meaningless. In this sense, the radar window is misleading. However, it looks cool.

DISTANCE FROM THE CENTER (SIGNAL STRENGTH) What does distance from the center mean? It looks like it means physical distance, as it would on a physical radar screen. Rather, it means *signal strength*. Access points that are shown closest to the center are the *strongest*, and access points that are the farthest from the center are the *weakest*.

MEASURING SIGNAL STRENGTH Signal strength gives the RSSI (relative signal strength indicator) for the access point. Smaller negative numbers are better. For example, –60 dBm is a very strong signal, while –87 dBm is a very weak signal. In Figure 6a-1, Nalu24 has a signal strength of –65, which is quite good. Belkin has a signal strength of –89, which is terrible.

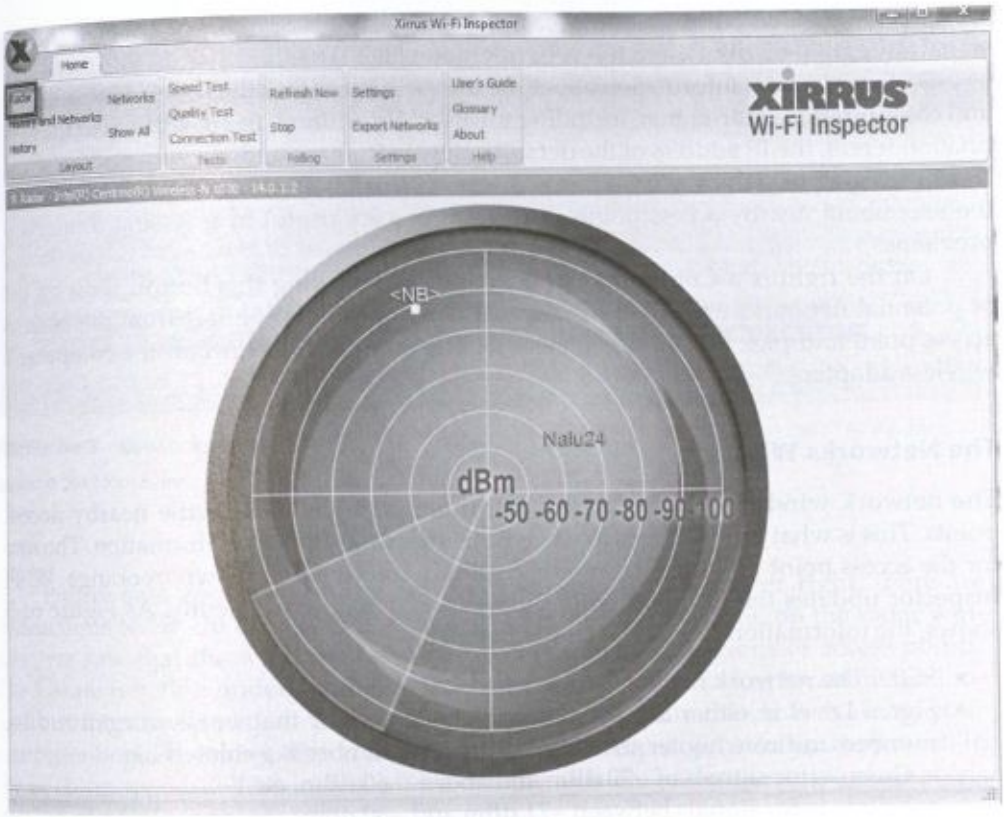

FIGURE 6a-2 Expanded Radar Window

Source: © 2012 Xirrus, Inc.

For signal strength, smaller negative numbers are better. (It's a double negative.)

EXPANDING THE RADAR WINDOW The radar window in its normal small form can display only four access points. Under the Layout section of the menu, selecting Radar in the Layout Group will maximize the radar window. This allows up to 10 access point names to be seen. By the way, "network" and "SSID" are synonyms.

Figure 6a-2 shows the expanded radar window. There are only two nearby access points, so there is no need for a large radar window. However, it certainly is easier to read the relative indicated signal strength.

Connection Window

The connection window (in the upper right in Figure 6a-1) shows information about the access point to which the computer running Wi-Fi Inspector is currently connected (Nalu24). It shows the SSID (the network name, in this case, Nalu24),the BSSID (the

access point's MAC address, in this case Cisco-Linksys:73:22:51[1]), the channel (6), the signal strength (–65 dBm), and the network mode (802.11n).

In the middle is information about the user's PC. It shows the user's MAC address and configuration information, including the user's IP address, the IP address of the destination server, the IP address of the default gateway (router), and the network's external IP address given to it by the ISP. (This is a home network.) This information does not tell the user about nearby access points, but it can be very useful in assessing connection problems.

On the right is a Connect/Disconnect button. Clicking this button shows a list of potential networks and allows the user's computer to disconnect from the current access point and pick another to connect to. The user can also turn off the computer's wireless adapter.

The Networks Window

The network window shows detailed information about each of the nearby access points. This is what the user goes to when he or she wants detailed information. The row for the access point to which the user is currently connected is shown in orange. Wi-Fi Inspector updates the information in the network window frequently. As Figure 6a-3 shows, the information in this window is detailed.

- SSID. The network name.
- Signal Level in either dBm or percentage. Remember that smaller negative dBm numbers indicate higher strength. Next to the number is a colored bar.
  - Green is for signals of –70 dBm and above (–60 dBm, etc.).
  - Yellow is for signals between –71 dBm and –80 dBm
  - Orange is for signals between –81 dBm and –90 dBm.
  - Red is for –91 dBm and below.
- Network Mode. 802.11g, 802.11n, etc.
- Default Encryption. None, WEP, TKIP (in WPA), or AES (802.11i).
- Default Authentication. Open (none), WPA/PSK, WPA2/PSK, WPA/802.1X, or WPA2/802.1X.
- Vendor. The name of the device manufacturer.
- BSSID. The access point's MAC address.
- Channel. The channel number.
- Frequency. The center frequency of the channel.
- Network Type. Access point or ad hoc (no access point).
- Graph. This is a checkbox that tells Wi-Fi Inspector to graph the signal level over time (checked) or not to do so (unchecked). In the figure, both are checked, so both will be graphed.

In the figure, the access points are listed in terms of declining signal strength. However, the networks table can be sorted by any column heading. The user merely clicks on the column heading.

[1] The first two octets in a MAC address identify the company making the network adapter in the access point. Wi-Fi Inspector converts this information into a humanly readable name.

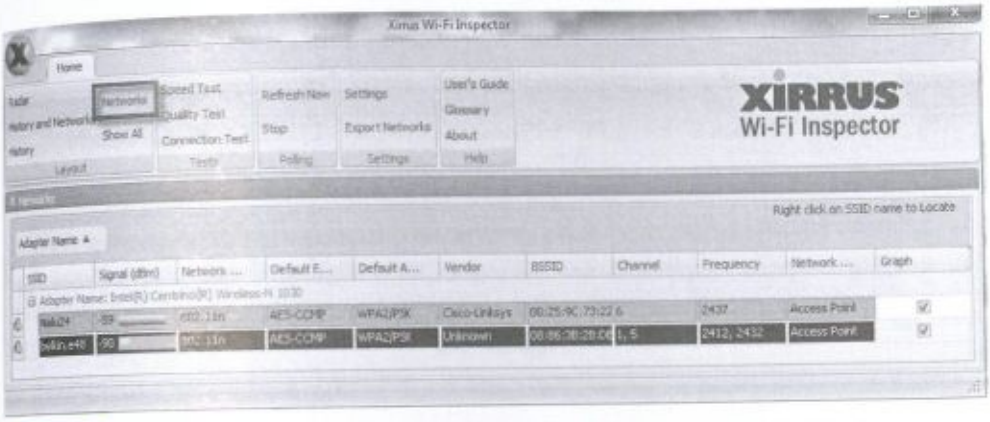

FIGURE 6a-3 Networks Window

Source: © 2012 Xirrus, Inc.

Figure 6a-4 zooms in on the networks window. In the upper right, there are instructions to "Right click on SSID name to Locate." In the section on the radar window, we saw that the window does not give the physical locations of access points. The Locate function under networks addresses this lack of physical location in a limited but interesting way. If you right click on an SSID name such as Nalu24, your computer begins beeping. If you are far away, it will beep slowly. As you approach it, the beeping speed will be increased. Essentially, you are using the network analysis version of a Geiger counter.

Signal History

In the network window, we saw that the user can check or uncheck whether graphing should be done. The Signal History window shows these graphs. The graphs in Figure 6a-5 show that the signal strength for Nalu24 is uniformly excellent, while the signal strength for Belkin is uniformly poor. Major fluctuations would indicate serious problems.

FIGURE 6a-4 Locating an Access Point

Source: © 2012 Xirrus, Inc.

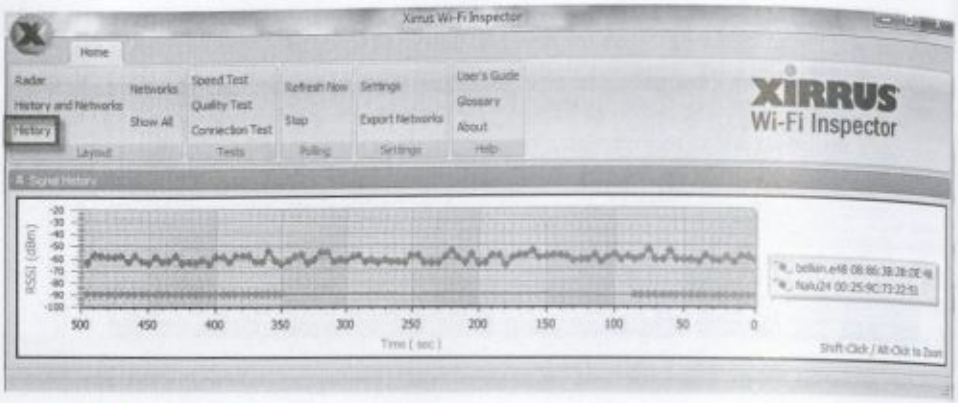

FIGURE 6a-5 Signal History

Source: © 2012 Xirrus, Inc.

Other Groups on the Ribbon

The Layout group on the ribbon is the most-used feature of the Xirrus Wi-Fi Inspector.

HELP GROUP The Help group provides a user's guide to explain the program's detailed functionality. There is also a helpful glossary of terms.

SETTINGS GROUP The Settings group allows the user to adjust many settings, for example, expressing RSSI in percentage terms instead of in terms of dBm.

TESTS GROUP The windows in Wi-Fi Inspector provide information visually. The Tests group allows the user to conduct more detailed tests. These tests are good for troubleshooting.

TESTS

As just noted, the Tests group actively tests the quality of your service. The tests group performs three important tests.

Connection Test

The connection test shows how well you are connected to the outside world and to critical internal devices. Figure 6a-6 shows the results of a connection test. It shows that Wi-Fi Inspector uses ping to test latency to your DNS server, default gateway (router), and a host on the Internet (Internet Reachable). It also does a DNS lookup, in this case for www.google.com.

The test shows that the user has low latency for the default router and an Internet host. It also shows that the DNS lookup was successful. In color, these are show in green, with the word *Pass*. However, there is relatively high latency to the user's DNS server (152 ms). This is indicated by a yellow bar with the text *Warning: high latency*. However, the latency is not very high. This connection looks good.

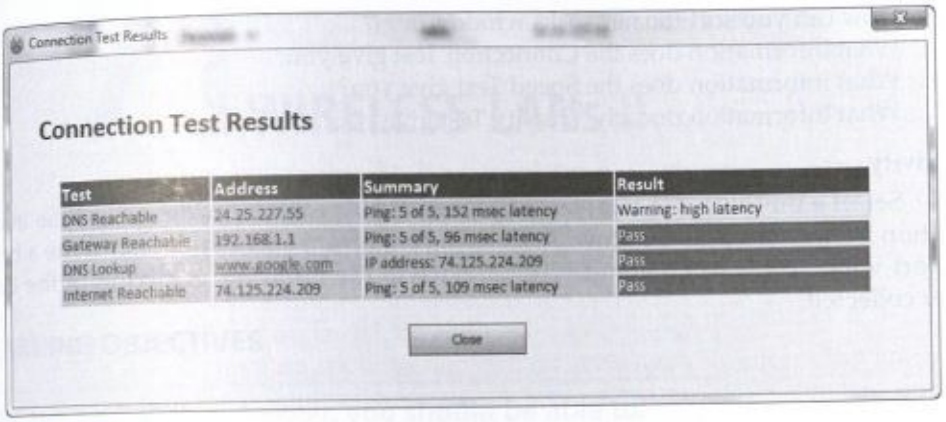

FIGURE 6a-6 Connection Test

Source: © 2012 Xirrus, Inc.

Speed Test

The speed test takes the user to speedtest.net.

Quality Test

The quality test takes you to pingtest.net. When the author ran this test, it gave the user's quality level a B. However, the box on the left notes that the connection should be fine for anything but gaming.

- The ping (latency) averaged 84 ms, which is a little high for games. The server is less than 50 miles away. Connecting to a more distant server would increase latency.
- Jitter, which is variation in latency from packet to packet is 24 ms. This can affect voice and video, for which jitter can result in jittery voice or video.
- There was zero packet loss. The connection appears to be reliable.
- There is a MOS score of 4.33. This is a traditional subjective indicator of voice call quality. A MOS score of 5 indicates toll-call quality on the telephone system. A MOS of 4.33 is quite good.

One caveat is that pingtest.net is a bit "grabby." It tries to sell you its tools and is slightly aggressive. In addition, the site uses Java, which you may have to download. You may also have to give a firewall exception to this Java program.

ACTIVITIES

Questions

1. Why is the radar window's image of a radar scope misleading?
2. How would you locate an access point despite the limitations of the radar window? This will take one to four paragraphs.
3. There is a value of –44 dBm for signal strength. How good is this?

4. How can you sort the networks window?
5. What information does the Connection Test give you?
6. What information does the Speed Test give you?
7. What information does the Quality Test give you?

Activity

Select a building. Go to at least 10 locations. At each location, record the information in the networks window. Also, do a connection and speed test. Write a brief report what you learned about Wi-Fi service in the building, referring to the data you collected.

7 WIRELESS LANs II

LEARNING OBJECTIVES

By the end of this chapter, you should be able to:

- Explain 802.11 WLAN security.
- Explain 802.11 wireless LAN management.
- Describe other local wireless technologies, including Bluetooth, ultrawideband (UWB) transmission, Zigbee, RFIDs, and software-defined radio.

INTRODUCTION

In Chapter 6, we focused on how 802.11 wireless LANs operate. This chapter continues to look at wireless networks. We will look at 802.11 security and management. We will then turn to other local wireless technologies, including Bluetooth.

Like switched networks, wireless networks are single networks. They are defined by standards at the physical and data link layers. Therefore, they are OSI standards, even if they are created by other organizations, such as the IEEE.

TJX

TJX Companies, Inc. (TJX), is a group of over 2,500 retail stores operating in the United States, Canada, England, Ireland, and several other countries. These companies do business under such names as TJ Maxx and Marshalls. In its literature, TJX describes itself as "the leading off-price retailer of apparel and home fashions in the U.S. and worldwide." With this mission statement, there is strong pressure to minimize costs.

On December 18, 2006, TJX detected "suspicious software" on its computer systems. On December 21, consultants confirmed that an intrusion had actually occurred. The next day, the company informed law enforcement authorities in the United States and Canada. Five days later, the security consultants determined that customer data had been stolen.

The consultants initially determined that the intrusion software had been working for seven months when it was discovered. A few weeks later, the consultants discovered that the company had also been breached several times in 2005. All told, the consultants estimated that 45.7 million customer records had been stolen. This was by far the largest number of personal customer records stolen from any company.