Chapter 1

Wireless Networks and Topologies

THE CCNA WIRELESS EXAM TOPICS COVERED IN THIS CHAPTER ARE:

✓ Describe WLAN fundamentals
  ▪ Describe networking technologies used in wireless (SSID → WLAN_ID → Interface → VLAN, 802.1Q trunking)
  ▪ Describe wireless topologies (IBSS, BSS, ESS, Point-to-Point, Point-to-Multipoint, basic Mesh, bridging)
Sipping coffee at a café or hanging out in an airport until they finally fix the plane you’re waiting to board no longer requires reading papers and magazines to avoid mind-numbing boredom. Now, you can just connect to the local wireless network and catch up on your email, blog, do a little gaming—maybe even get some work done! It’s come to the point that many of us wouldn’t even think of checking into a hotel that doesn’t offer this important amenity. So clearly, those of us already in or wishing to enter the IT field better have our chops down regarding wireless network components and their associated installation factors, right? (Answer: a resounding YES!)

With that established, we’ve come to a great starting point: if you want to understand the basic wireless LANs (WLANs) most commonly used today, just think 10BaseT Ethernet with hubs—except the wireless devices we connect to are called access points (APs). This means that our WLANs run half-duplex communication—everyone is sharing the same bandwidth, and only one device is communicating at a time per channel.

This isn’t necessarily bad; it’s just not good enough. Because so many people rely on wireless networks today, it’s critical that they evolve faster than greased lightning to keep up with our rapidly escalating needs. The good news is that this is actually happening—and it even works securely!

In this chapter, I am going talk about the various types of wireless networks, and then discuss the minimum devices needed to create a simple wireless network. I’ll then show you some basic wireless topologies, and finish with a review on switching and VLANs. Why am I going to talk about switching and VLANs? Because if you think about it for a minute, you come to the important realization that APs have to connect to something. If not, how else would all those hosts hanging around in a wireless network area be able to connect to your wired resources, or to the Internet? This is why you absolutely must have a basic understanding of switching.

To find dynamic updates to this chapter, please see www.lammle.com.

Wireless Networks

Wireless networks come in many forms, cover various distances, and provide a range of low to high bandwidth depending on the type installed. The typical wireless network today is an extension of an Ethernet LAN, and wireless hosts use Media Access Control (MAC)
addresses, IP addresses, and so forth, just like any host would on a wired LAN. Figure 1.1 shows how the simple, typical wireless LAN looks today.

**Figure 1.1** Wireless LANs are an extension of our existing LANs.

But wireless networks are more than just run-of-the-mill LANs because—you guessed it—they’re wireless. And as I mentioned, they cover a range of distances from short-range personal area networks, all the way to wide area networks (WANs) that really go the distance. Figure 1.2 illustrates how different types of wireless networks look and the related distances they’ll provide coverage for in today’s world.

**Figure 1.2** Today’s Wireless Networks

Okay, now that you’ve got the picture, we’ll explore each of these networks in more detail.

**Wireless Personal Area Network (WPAN)**

A wireless personal area network (PAN) works in a very small area and connects devices like mice, keyboards, PDAs, headsets, and cell phones to our computers. This conveniently eliminates the cabling clutter of the past. If you’re thinking Bluetooth, you’ve hit it, because it’s by far the most popular type of PAN around! I’ll discuss everything you need to
know about this standard in Chapter 3, “Wireless Regulation Bodies, Standards, and Certifications.”

PANs are low power, they cover short distances, and they’re pretty small. The distance you’ll get out of one of these is about 30 feet max, but most devices on a PAN have a short reach, making them popular for small and/or home offices. Bigger isn’t always better—you don’t want your PAN’s devices stretching out so far that they interfere with your other wireless networks, or someone else’s, and make a mess. Plus you’ve got the usual security concerns to manage. So, basically PANs are the perfect solution for small devices that you want to connect to your PC.

The standard use for PANs is unlicensed, meaning that the users involved don’t have to pay to use the type of devices in the network. As you can imagine, this attribute promotes the development of devices that can use PAN frequencies.

**Wireless LAN (WLAN)**

Wireless LANs (WLANs) were created to have longer distance and higher bandwidth than PANs and are the most popular type of wireless networks in use today.

The first WLAN had a data rate up to 2Mbps, could go about 200–300 feet depending on the area, and was called simply 802.11. The typical rates in use today are higher and are 11Mbps and 54Mbps; these are called IEEE 802.11b and 802.11g/a, respectively. You’ll learn more about these IEEE standards in Chapter 3.

The idea of a WLAN is to have many users connect to the network at the same time, but this can cause interference and collisions as users are competing for the same bandwidth.

Like PANs, WLANs use an unlicensed frequency band, which means you do not have to pay for the frequency band in order to transmit. This fact encourages development of devices for use in this type of network, and we’ve seen an explosion of new development in the WLAN area.

**Wireless Metro Area Network (WMAN)**

Wireless metro area networks (WMANs) are essentially a network that covers a fairly large geographic area like a city or small suburb. They’re becoming increasingly common as more and more products are introduced into the WLAN arena and their price tags continue to drop.

You can think of WMANs as low-budget, bridging networks—something I talk about more in a bit. They offer a frugal alternative to the much more costly T1 or T3 point-to-point leased lines, but there’s a catch: to get your discount long-distance wireless network to work, you’ve got to have a line of sight between each hub or building.

If you can get fiber connections in your metropolitan area, they’re what you want because they’ll provide you with an ultra-solid backbone for your network. This is why more and more fiber networks are being installed these days. But if your ISP doesn’t offer the fiber option, or you lack the cash to pony up for it, a WMAN is a perfectly fine, economical alternative design to cover a campus or some other large area as long as you’ve got that vital line of sight factor in check!
Wireless Wide Area Network (WWAN)

So far, it’s seriously rare to come across a wireless wide area network (WWAN) that can provide you with WLAN speeds, but there sure is a lot of chatter about them. A good example of a WWAN would be the latest cellular networks that can transmit data at a pretty good clip. Even so, they’re still not speedy enough to replace our ubiquitous WLANs. But WWANs can certainly cover plenty of area!

Some people—especially those in TV commercials—claim to adore their infallible, turbo-charged cellular networks. These terminally happy, ceaselessly smiling people are usually watching high-speed video on their shiny new smart phones, but I don’t know anyone who lives outside the TV (including me) who actually gets that kind of speed. And that “coverage anywhere” thing—sorry! Off the set and into reality, dead zones and frozen phones are things we must all deal with for now.

Hopefully we’ll see more efficiency and growth in WWANs soon. But to be real, because WWANs are used to provide connectivity over a really large geographic area, it follows that implementing one will separate your cell service provider from a large quantity of cash. Therefore, as more and more people want this type of service and are willing to pay for it, cellular companies will gain the resources to expand and improve upon these exciting networks.

Here are another couple of positives in favor of WWAN growth and development: they meet a lot of business requirements, and technology is growing in a direction that the need for this type of long-distance wireless network is only getting stronger. So it’s a fairly good bet that development will continue to grow in this industry. Connectivity between a WLAN and a WWAN will be critical to many things in our future—for instance, when we have more IPv6 networks, the “pass-off” between these two types of networks may be seamless.

Basic Wireless Devices

Though it might not seem this way to you right now, simple wireless networks (WLANs) are less complex than their wired cousins because they require fewer components. To make a basic wireless network work properly, all you need are two main devices: a wireless AP and a wireless network interface card (NIC). This also makes it a lot easier to install a wireless network, because basically, you just need an understanding of these two components in order to do so.

Wireless Access Points

You’ll find a central component like a hub or switch in the vast majority of wired networks that’s there to connect hosts together and allow them to communicate with each other. It’s the same thing regarding wireless networks; they also have a component that connects
all wireless devices together, only that device is known as a wireless *access point* (AP). Wireless APs have at least one antenna. Usually there’s two for better reception (referred to as diversity), and a port to connect them to a wired network. Figure 1.3 gives you an example of a Cisco wireless AP. It happens to be one of my personal favorites—an 871W that I use in my home office.

**FIGURE 1.3** A wireless access point

APs have the following characteristics:

- APs function as a central junction point for the wireless stations much like a switch or hub does within a wired network. Due to the half-duplex nature of wireless networking, the hub comparison is more accurate, even though hubs are rarely found in the wired world anymore.
- APs have at least one antenna—most likely two.
- APs function as a bridge to the wired network, giving the wireless station access to the wired network and/or the Internet.
- SoHo APs come in two flavors—the stand-alone AP and the wireless router. They can and usually do include functions like network address translation (NAT) and Dynamic Host Configuration Protocol (DHCP).
Even though it’s not a perfect analogy, you can compare an AP to a hub because it doesn’t create collision domains for each port like a switch does, but APs are definitely smarter than hubs. An AP is a portal device that can either direct network traffic to the wired backbone or back out into the wireless realm. If you look at Figure 1.1 again, you can see that the connection back to the wired network is called the distribution system (DS), and it also maintains MAC address information within the 802.11 frames. What’s more, these frames are capable of holding as many as four MAC addresses, but this would only be the case when a wireless DS is in use—something I’ll discuss in detail in Chapter 4, “Introduction to Wireless Security.” For now, just know that this capability allows the AP to track where everything is going.

An AP also maintains an association table and you can view that from the web-based software that’s used to manage the AP. So what’s an association table? It’s essentially a list of all workstations currently connected to or associated with the AP that are listed by their MAC addresses. Another cool AP feature is that wireless routers can function as NAT routers, and they can perform DHCP addressing for workstations as well.

In the all-important Cisco world, there are two types of APs: autonomous and lightweight. An autonomous AP is one that is configured, managed, and maintained in isolation with regard to all the other APs that exist in the network. A lightweight AP gets its configuration from a central device called a wireless controller. In this scenario, the APs are functioning as antennas and all information is sent back to the wireless LAN controller (WLC). There are a bunch of advantages to this, like the capacity for centralized management and more seamless roaming. You’ll learn all about using WLC and lightweight APs throughout this book.

You can think of an AP as a bridge between the wireless clients and the wired network. Additionally, you can use an AP as a wireless bridge (depending on the settings) to bridge two wired network segments together.

In addition to the stand-alone AP, there’s another type of AP that includes a built-in router (the type shown in Figure 1.3), which you can use to connect both wired and wireless clients to the Internet. These devices are usually employed as NAT routers.

**Wireless Network Interface Card (NIC)**

Every host you want to connect to a wireless network needs a wireless network interface card (NIC) to do so. Basically, a wireless NIC does the same job as a traditional NIC, only instead of having a socket/port to plug a cable into, the wireless NIC has a radio antenna. Figure 1.4 shows an example of a wireless NIC.
The wireless card shown in Figure 1.4 is used in a desktop computer, and most late model laptops have wireless cards plugged into or built into the motherboard.

These days, it’s pretty rare to use an external wireless client card because all laptops come with them built in, and desktops can be ordered with them too. But it’s good to know that you can still buy the client card shown in Figure 1.4. Typically, you would use cards like the ones shown in the figure for areas of poor reception, or for use with a network analyzer because they can have better range—depending on the antenna you use.

Wireless Antennas

Wireless antennas work with both transmitters and receivers. There are two broad classes of antennas on the market today: *omni-directional* (or point-to-multipoint) and *directional*
Wireless Topologies

Now that I’ve discussed the very basics of wireless devices used in today’s simple networks, I want to describe the different types of networks you’ll run across or design and implement as your wireless networks grow.

These include the following:

- IBSS
- BSS
- ESS
- Workgroup bridges
- Repeater APs
- Bridging (point-to-point and point-to-multipoint)
- Mesh

Let’s take a look at these networks in detail.

Independent Basic Service Set (Ad Hoc)

This is the easiest way to install wireless 802.11 devices. In this mode, the wireless NICs (or other devices) can communicate directly without the need for an AP. A good example of this is two laptops with wireless NICs installed. If both cards were set up to operate in ad hoc mode, they could connect and transfer files as long as the other network settings, like protocols, were set up to enable this as well. We’ll also call this an independent basic service set (IBSS), which is created as soon as two wireless devices communicate.
To create an ad hoc network, all you need is two or more wireless-capable devices. Once you’ve placed them within a range of 20–40 meters of each other, they’ll “see” each other and be able to connect—assuming they share some basic configuration parameters. One computer may be able to share the Internet connection with the rest of them in your group. Figure 1.5 shows an example of an ad hoc wireless network. Notice that there’s no access point!

**FIGURE 1.5** A wireless network in ad hoc mode

An ad hoc network, also referred to as peer to peer, doesn’t scale well and I wouldn’t recommend it due to collision and organization issues in today’s corporate networks. With the low cost of APs, you don’t need this kind of network anymore, except for maybe in your home, but maybe not even there.

Additionally, ad hoc networks are a fairly insecure method, and care should be taken to have the AdHoc setting turned off prior to connecting to your wired network.

**Basic Service Set (BSS)**

A basic service set (BSS) is the area, or cell, defined by the wireless signal served by the AP. It can also be called a basic service area (BSA) and the two terms, BSS and BSA, can be interchangeable. Even so, BSS is the most common term that’s used to define the cell area. Figure 1.6 shows an AP providing a BSS for hosts in the area and the basic service area (cell) that’s covered by the AP.
The AP is not connected to a wired network in this example, but the AP provides management of wireless frames so the hosts can communicate. Unlike the ad hoc network, this network will scale better and more hosts can communicate in this network because the AP manages all network connections.

**Infrastructure Basic Service Set**

In infrastructure mode, wireless NICs only communicate with an access point instead of directly with each other as they do when they’re in ad hoc mode. All communication between hosts, as well as any wired portion of the network, must go through the access point. An important fact to remember is that in this mode, wireless clients appear to the rest of the network as though they were standard, wired hosts.

Figure 1.6 shows a typical infrastructure mode wireless network. Pay special attention to the access point and the fact that it’s also connected to the wired network. This connection from the access point to the wired network is called the *distribution system (DS)* and this is how the APs communicate to each other about hosts in the BSA. Basic standalone APs do not communicate with each other via the wireless network, only through the DS.
When you configure a client to operate in wireless infrastructure mode, you need to understand what is called the SSID. The service set identifier (SSID) refers to the unique 32-character identifier that represents a particular wireless network and defines the BSS. (By the way, a lot of people use the terms SSID and BSS interchangeably, so don’t let that confuse you!) All devices involved in a particular wireless network may be configured with the same SSID. Sometimes access points may even have multiple SSIDs. Let’s talk about that in a little more detail.

**Service Set ID**

SSID is a basic name that defines the BSA transmitted from the AP. A good example of this is “Linksys.” You’ve probably seen that name pop up on our host when looking for a wireless network. This is the name the AP transmits out to identify which WLAN the client station can associate with. The SSID can be up to 32 characters long. It normally consists of human-readable ASCII characters, but the standard doesn’t require this. The SSID is defined as a sequence of 1–32 octets, each of which may take any value.

The SSID is configured on the AP and can be either broadcasted to the outside world or hidden. If the SSID is broadcasted, when wireless stations use their client software to scan for wireless networks the network will appear in a list identified by its SSID. But if it’s hidden, it either won’t appear in the list at all or it will show up as an “unknown network” depending on the client’s operating system.

Either way, a hidden SSID will require that the client station be configured with a wireless profile, including the SSID, in order to connect. This requirement is above and beyond any other normal authentication steps or security essentials.

The AP associates a MAC address to this SSID. It can be the MAC address for the radio interface itself (called the basic service set identifier [BSSID]), or it can be derived from the MAC address of the radio interface if multiple SSIDs are used (sometimes called a virtual MAC address). In the latter case, you would call it a multiple basic service set identifier (MBSSID), as shown in Figure 1.7.

There are two things you really want to make note of in this figure: first, there’s a “Contractor BSSID” and a “Sales BSSID”; second, each of these SSID names is associated with a separate virtual MAC address, which was assigned by the AP.

These SSIDs are virtual, and implementing things this way won’t improve your wireless network or AP performance—you just have more hosts sharing the same half-duplex radio. By doing this, you’re not breaking up collision domains or broadcast domains by creating more SSIDs on your AP. The reason for creating multiple SSIDs on your AP is so that you can set different levels of security for each client that’s connecting to your AP(s).

**Extended Service Set**

A good thing to know is that if you set all your access points to the same SSID, mobile wireless clients can roam around freely within the same network. This is the most common wireless network design you’ll find in today’s corporate settings.
Doing this creates something called an extended service set (ESS), which provides more coverage than a single access point and allows users to roam from one AP to another without having their host disconnected from the network. This design creates the ability to move more or less seamlessly from one AP to another. Figure 1.8 shows two APs configured with the same SSIDs in an office, thereby creating the ESS network.

**Figure 1.7** A network with MBSSIDs configured on an AP

**Figure 1.8** Extended service set (ESS)
For users to be able to roam throughout the wireless network—from AP to AP without losing their connection to the network—all APs must overlap by at least 10 percent of their signal or more to their neighbor’s cells. To make this happen, be sure the channels (frequency) on each AP are set differently. No worries—we’ll go over this important detail in greater depth later, in Chapter 3.

**Workgroup Bridge**

If you have a bunch of hosts that need to connect to the wireless network but they don’t have wireless cards or wireless capability, it’s time to go with implementing a wireless workgroup bridge (WGB). A WGB is used in a typical network where it’s just not feasible to install an Ethernet or fiber run. Usually, this is because it’s just not in the budget, or because you’re dealing with a particular environment, like a historic building where cable runs are forbidden. Figure 1.9 shows an example of such a network.

![Basic WGB wireless network](image)

Cisco supports two types of WGBs: autonomous, which is the type shown in Figure 1.9 (sometimes called aWGB), and the universal WGB (uWGB). The aWGB will establish a single wireless connection for multiple Ethernet clients to an AP and appear as a nonstandard client on the AP (This is a proprietary solution provided by Cisco.). Good to know is that the uWBG is a nonproprietary version that supports an Ethernet client by enabling it to connect through an uWGB to an AP from another vendor and still appear as a single, normal client to the AP.
You need to remember the two types of WGBs and the definitions included here.

**Repeaters**

If you need to extend the coverage of an AP, you can either increase the gain of a directional antenna or add another AP in the area. If neither of those options solves your problem, try adding a repeater AP to the network and extending the range without having to pull an Ethernet cable for the new AP.

Figure 1.10 gives you a picture of what this network design looks like.

![Figure 1.10](image-url) An AP repeater network

A wireless repeater AP isn’t connected to the wired backbone. It uses its antenna to receive the signal from an AP that’s directly connected to the network, and repeats the signal for clients located too far away from it.

To make this work, you need appropriate overlap between APs, as shown in Figure 1.10. Another way to get this to happen is to place a repeater AP with two radios in use, with one receiving and the other one transmitting. This works somewhat like a dual half-duplex repeater.

But there is a rather nasty downside to this design—for every repeater installed you lose about half of your throughput, so the hosts off Repeater 2, shown in Figure 1.10, would only get about 5.5Mbps throughput at best when running in an 11Mbps wireless network.
Since no one likes less bandwidth, a repeater network should only be used for low-bandwidth devices, like a barcode reader in a warehouse.

**Bridging**

Bridges are used to connect two or more wired LANs, usually located within separate buildings, to create one big LAN. Bridges operate at the MAC address layer (Data Link layer), which means they have no routing capabilities. So you’ve got to put a router in place if you want to be able to do any IP subnetting within your network. Basically, you would use bridges to enlarge the broadcast domains on your network. Armed with a firm understanding of how bridging works, you can definitely improve your network’s capacity.

To build wireless networks correctly, it’s important to have a working knowledge of root and nonroot bridges (sometimes referred to as parent and child bridges). Some bridges allow clients to connect directly to them, but others don’t, so make sure you understand exactly your business requirements before just randomly buying a wireless bridge. Figure 1.11 shows the typical bridge scenarios used in today’s networks.

**FIGURE 1.11  Typical bridge scenarios**

A point-to-point wireless network is a popular design that’s often used outdoors to connect two buildings or LANs together.

A point-to-multipoint design works well in a campus environment where you have a main building with a collection of ancillary buildings that you want to be able to connect
back to the main one, as well as to each other, through it. Wireless bridges are commonly used to make these connections, and they just happen to be pricier than a traditional AP. The thing you want to remember about point-to-multipoint wireless networks is that each remote building won’t be able to communicate directly with each other. To do that, they must first connect to the central, main point (main building) and then to one of the other ones (multipoint buildings).

Okay—now let’s get back to that root/nonroot issue I brought up a minute ago. I’ve got to tell you more about this because it becomes important to understand, especially when you’re designing outdoor networks!

So look back to Figure 1.11 and find the terms root and nonroot. This figure shows a traditional point-to-point and point-to-multipoint network when one bridge, the root, accepts communications only from nonroot devices.

Root devices are connected to the wired network, which allows nonroot devices, like clients, to access the wired resources through the root device. Here are some important guidelines to help you design your wireless networks:

- Nonroot devices can only communicate to root devices. Nonroot devices include non-root bridges, workgroup bridges, repeater access points, and wireless clients.
- Root devices cannot communicate to other root devices. Examples of devices that can be roots are APs and bridges.
- Nonroot devices cannot communicate to other nonroot devices.

But wait, there’s one exception to that last bullet point. If you have a nonroot bridge set up as a repeater AP with two radios, the device must be configured as a nonroot device. It will then repeat and extend the distance of your outdoor, bridged network, as shown in Figure 1.12.

**Figure 1.12** A repeater AP bridge configured as a nonroot bridge

Figure 1.12 demonstrates that a nonroot bridge will communicate to another nonroot bridge only if one of the nonroot bridges has a root bridge in its uplink.

**Mesh Networks**

As more vendors migrate to a mesh hierarchical design, and as larger networks are built using lightweight access points that are managed by a controller, you can see that we need a standardized protocol that governs how lightweight access points communicate with
WLAN systems. This is exactly the role filled by one of the Internet Engineering Task Force’s (IETF’s) latest draft specifications, Lightweight Access Point Protocol (LWAPP).

Mesh networking infrastructure is decentralized and comparably inexpensive for all the nice amenities it provides because each host only needs to transmit as far as the next host. Hosts act as repeaters to transmit data from nearby hosts to peers that are too far away for a manageable cabled connection. The result is a network that can span a large area, especially over rough or difficult terrain.

Remember that mesh is a network topology in which devices are connected with many redundant connections between host nodes, and we can use this topology to our advantage in large wireless installations. Figure 1.13 shows a large meshed environment using Cisco outdoor managed APs to “umbrella” an outdoor area with wireless connectivity.

**FIGURE 1.13** Typical large mesh outdoor environment

Oh, and did I mention that mesh networks also happen to be extremely reliable? Because each host can potentially be connected to several other hosts, if one of them drops out of the network because of hardware failure or something, its neighbors simply find another route. So you get extra capacity and fault tolerance automatically just by adding more hosts!

Wireless mesh connections between AP hosts are formed with a radio, providing many possible paths from a single host to other hosts. Paths through the mesh network can change in response to traffic loads, radio conditions, or traffic prioritization.

At this time, mesh networks just aren’t a good solution for home use or small companies on a budget. As the saying goes, “If you have to ask...” As with most things in life, the more bells and whistles, the more it costs, and mesh networks are certainly no exception.
Switching

Yes, I know this book is a wireless book, but just trust me on this one—it’s very important for you to understand some vital switching terms and configurations. Can you guess why? Well, if you thought of something along the lines of “Because all those wireless devices such as access points must connect into something, and that something is a Cisco switch,” you nailed it!

Having these switching basics down will come in super handy when we get to managed wireless networks later in this book. That’s when you’ll find out about controllers, how they need to be configured so that they’ll connect to a switch, and vice versa. So as you can see, a basic knowledge of switches, related terminology, and how to configure them will be helpful to you.

Please see my CCNA: Cisco Certified Network Associate Study Guide: Exam 640-802 (Sybex, 2007) for a complete discussion and configuration examples on switching.

As shown in Figure 1.14, Layer 2 switched networks are typically designed as flat networks. Every broadcast packet transmitted is seen by every device on the network, regardless of whether or not the device needs to receive that data.

By default, routers only permit broadcasts to circulate within the originating network segment, but switches forward broadcasts to all segments. The reason for this is also the reason this type of network is called a flat network. The name means that it’s only one broadcast domain, not that its actual design is physically flat.

In Figure 1.14, you can see Host A sending out a broadcast, and all ports on all switches forwarding the broadcast—except for the port that originally received it.

**Figure 1.14** Flat network structure
Now look at Figure 1.15, which pictures a switched network. It shows Host A sending a frame with Host D as its destination, and as you can see, that frame is only forwarded out the port where Host D is located. This is a huge improvement over the old hub networks, unless having only one collision domain by default is what you want.

**Figure 1.15** The benefit of a switched network

![Figure 1.15](image)

You already know that the main benefit gained by having a Layer 2 switched network is that it allows you to create individual collision domain segments for each device plugged into each port on the switch. This scenario frees us from the original Ethernet distance constraints, so now larger networks can be built. But with each new advance, we often encounter new issues—the larger the number of users and devices, the more broadcasts and packets each switch must handle.

And here’s another big advantage—security! This one’s a real problem because within the typical Layer 2 switched internetwork, all users can see all devices by default. Worse, you can’t stop devices from broadcasting or users from trying to respond to broadcasts. Your security options are dismally limited to placing passwords on the servers and other critical devices.

But they’re not if you create a virtual LAN (VLAN). You can solve many of the problems associated with Layer 2 switching with VLANs—as you’ll soon see.

Here are some ways that VLANs simplify network management:

- Network additions, moves, and changes are achieved by configuring a port into the appropriate VLAN.
- A group of users who require high security can be put into their own VLAN so that no users outside their specific VLAN can communicate with them.
- As a logical grouping of users by function instead of a physical one, VLANs are by nature independent of their physical or geographic locations.
- VLANs can help strengthen network security.
- VLANs increase the number of broadcast domains while decreasing their size.

Next, I’m going to cover some cool switching features and show you how switches provide better network services than hubs can within a network. You’ll also learn how to configure switches with VLAN and trunk links.
VLAN Memberships

VLANs are most often created by an administrator who then assigns switch ports to each of them afterward. This kind of VLAN is called a static VLAN. If the administrator wants to do a little more work up front and assign all the host devices’ hardware addresses into a database, the switches can be configured to assign VLANs dynamically whenever a given host is plugged into a switch. This variety is predictably called a dynamic VLAN. Let’s check out the static type first.

Static VLANs

Static VLANs aren’t just the most common way to create VLANs; they’re also the most secure. This is because the switch port that you assign a VLAN association to will always maintain that particular association until you manually change the port assignment.

This type of VLAN configuration also happens to be kind of the “easy button” version because it’s relatively painless to set up and monitor. Dynamic VLANs can make certain things easier too.

Basically, static VLANs work well in a network where the movement of users is tightly controlled. Plus, even though it can be helpful to use network management software to configure the ports, it’s not required.

This is how it works—you configure each switch port with a VLAN membership based on the specific VLAN that the host needs to be a member of. (Remember, the device’s physical location doesn’t matter.) The broadcast domain the hosts will become a member of is an administrative choice. Don’t forget that each host must also have the correct IP address information configured or things won’t work so well.

It is also important to remember that if you plug a host into a switch, you’ve got to verify the VLAN membership of the precise port you’re plugging into. If the membership doesn’t match the specific host, it won’t be able to access or provide the network services it’s intended to. For instance, a host machine that you want to act as a workgroup server won’t be able to function in that capacity.

Dynamic VLANs

A dynamic VLAN determines a node’s VLAN assignment automatically. Using intelligent management software, you can base VLAN assignments on hardware (MAC) addresses, protocols, or even applications when you create dynamic VLANs.

Choosing between static or dynamic VLANs for your network comes down to your personal preferences and needs. For example, let’s say you’ve got all MAC addresses entered into a centralized VLAN management application. If a host is then attached to an unassigned switch port, the VLAN management database can look up the host’s hardware address and assign and configure the switch port to match the right VLAN. This is very cool—it makes management and configuration easier because if a user moves, the switch will simply assign them to the correct VLAN automatically. But as usual, there’s a catch...
Just know that there’s a lot more up-front work you have to do when initially setting up that database!

Cisco administrators can use the VLAN Management Policy Server (VMPS) service to set up a database of MAC addresses that can then be used for the dynamic addressing of VLANs. A VMPS database essentially maps MAC addresses to VLANs.

A dynamic-access port can belong to one VLAN, (VLAN ID 1 to 4094), which is dynamically assigned by the VMPS. You can have dynamic-access ports and trunk ports on the same switch, but you’ve got to connect the dynamic-access port to an end station or hub and not to another switch.

Types of Switch Ports

Okay—so we all know that switch ports are Layer 2–only interfaces associated with a physical port. Switch ports can belong to one or more VLANs, and they can be an access port or a trunk port. You can manually configure a given port as an access port or trunk port, or you can just let the Dynamic Trunking Protocol (DTP) operate on a per-port basis to set the switch port mode by negotiating with the port on the other end of the link.

As frames are switched throughout the network, switches must be able to keep track of all the different types, as well as understand what to do with them depending on their hardware addresses. And remember, frames are handled differently according to the type of link they are traversing. Figure 1.16 depicts the difference between an access link and a trunk link.

Let’s talk about the various types of switch ports—starting with access ports.

**FIGURE 1.16** Access and trunk links in a switched network
Access Ports

An access port belongs to one specific VLAN and only carries its traffic that’s received and sent in native formats with no VLAN tagging at all. Another thing to remember is that all traffic that arrives on an access port is assumed to belong to the VLAN that’s assigned to that port, and if an access port happens to receive, say, an IEEE 802.1Q tagged packet, it will be promptly dropped. Because tagged traffic can only be processed on trunk ports, the source address of the dumped packet will remain a mystery.

This type of link is known as the native VLAN of the port, and a device attached to an access link is unaware of a VLAN membership. The device just assumes that it’s part of a broadcast domain, but it doesn’t have an understanding of the physical network.

Switches remove any VLAN information from the frame before it’s forwarded out to an access link device. Access link devices can’t communicate with devices outside their VLAN unless the packet is routed. And you have to be decisive—you have to designate a switch port as an access port or a trunk port. Remember, if you choose the access port option, that port can almost always be assigned to a single VLAN only.

Voice Access Ports

Here’s what I meant when I said, “almost always”… although an access port can only be assigned to one VLAN, most late-model switches will allow you to add a second VLAN to the access port to be designated as your voice VLAN. This is technically considered to be a different type of link, but it’s still just an access port that can be configured for both data and voice VLANs. It is pretty cool, though, because it allows you to connect a phone and PC device to one switch port, and yet still have each device in a separate VLAN.

Trunk Ports

Trunks can carry multiple VLANs and got their name because of the telephone system trunks that can carry multiple telephone conversations.

A trunk link is a 100 or 1000Mbps point-to-point link between two switches, between a switch and router, or between a switch and server. These carry the traffic of multiple VLANs—from 1 to 4094 at a time—but it’s only up to 1005 unless you’re using extended VLANs.

A very nice feature of trunking is that it allows you to make a single port out of multiple VLANs at the same time. This can be a major advantage because it makes it possible for you to set things up in a way that a server can be in two broadcast domains simultaneously. This means that your users won’t have to cross a Layer 3 device (a router) to log in and access it. Another benefit to trunking is when you’re connecting switches. Trunk links can carry some or all VLAN information across the link, but if the links between your switches aren’t trunked, only VLAN 1 information will be switched across the link by default.

All VLANs send information on a trunked link unless cleared manually by an administrator, and I’ll show you how to clear individual VLANs from a trunk in the configuration section later in this chapter.

Okay—next up is frame tagging and the VLAN identification methods used with it.
Frame Tagging

So you know that you can create your VLANs to span more than one connected switch. This flexible, power-packed capability is probably the main advantage to implementing VLANs.

But it can get kind of complicated—even for a switch—so there needs to be a way for each one to keep track of all the users and frames as they travel the switch fabric and VLANs. (Remember, a switch fabric is basically a group of switches sharing the same VLAN information.) This is where frame tagging comes in. This frame identification method uniquely assigns a user-defined ID to each frame. Sometimes people refer to it as a “VLAN ID” or “color.”

And here’s how it works: each switch that the frame reaches must first identify the VLAN ID from the frame tag, and then it finds out what to do with the frame by looking at the information in the filter table. If the frame reaches a switch that has another trunked link, the frame will be forwarded out the trunk-link port.

Once the frame reaches an exit (determined by the forward/filter table) to an access link matching the frame’s VLAN ID, the switch removes the VLAN identifier. This is so the destination device can receive the frames without having to understand their VLAN identification.

A trunk port will support simultaneous tagged and untagged traffic and is assigned a default port VLAN ID (PVID). All untagged traffic travels on the port default PVID (also called the native VLAN), which is by default VLAN 1.

All untagged traffic and tagged traffic with a NULL (unassigned) VLAN ID is assumed to belong to the port default PVID—VLAN 1 by default. A packet with a VLAN ID equal to the outgoing port default PVID will be sent untagged and will only be allowed to communicate to hosts or devices in VLAN 1. All other VLAN traffic has to be sent with a VLAN tag in order to communicate in another particular VLAN.

VLAN Trunking Protocols

So VLAN identification is what switches use to keep track of all those frames as they’re traversing a switch fabric. It’s how switches identify which frames belong to which VLANs, and there’s more than one trunking method, as you’ll see in this section.

Inter-Switch Link (ISL)

*Inter-switch link (ISL)* is a way of explicitly tagging VLAN information onto an Ethernet frame. This tagging information allows VLANs to be multiplexed over a trunk link through an external encapsulation method (ISL) and allows the switch to identify the VLAN membership of a frame over the trunked link.

By running ISL, you can interconnect multiple switches and still maintain VLAN information as traffic travels between switches on trunk links. ISL functions at Layer 2 by encapsulating a data frame with a new header and cyclic redundancy check (CRC).
Of note, this is proprietary to Cisco switches, and it’s used for Fast Ethernet and Gigabit Ethernet links only. ISL routing can be used on a switch port, router interfaces, and server interface cards to trunk a server.

There are some important differences between ISL and 802.1q: ISL does not support untagged packets on the trunk links, all frames will be encapsulated. Another limitation of ISL is that only 1024 VLANs can ever be carried across the link. These limitations are some of the main reasons ISL isn’t being used as much anymore.

**IEEE 802.1Q**

Created by the IEEE as a standard method of frame tagging, 802.1Q inserts a field into the frame to identify the VLAN. If you’re trunking between a Cisco switched link and a different brand of switch, you have to use 802.1Q for the trunk to work.

It works like this: you must designate each 802.1Q port to be associated with a specific VLAN ID. The ports that populate the same trunk create a group that’s known as a native VLAN, and each port gets tagged with an identification number that reflects its native VLAN (the default is VLAN 1).

---

The basic purpose of ISL and 802.1Q frame-tagging methods is to provide inter-switch VLAN communication. Also, remember that any ISL or 802.1Q frame tagging is removed if a frame is forwarded out an access link—tagging is used across trunk links only.

---

**Configuring VLANs**

Configuring VLANs is pretty easy. Figuring out which users you want in each VLAN is not. It’s super time-consuming, but once you’ve decided on the number of VLANs you want to create and establish the users you want to belong to each one, it’s time to bring your first VLAN into existence.

To configure VLANs on a Cisco Catalyst switch, you use the global `config vlan` command. In the following example, I’m going to demonstrate how to configure VLANs on the S1 switch by creating three VLANs for three different departments (VLAN 1 is the native and administrative VLAN):

```
S1#config t
S1(config)#vlan ?
   WORD  ISL VLAN IDs 1–4094
   internal  internal VLAN
S1(config)#vlan 2
S1(config-vlan)#name Sales
```
S1(config-vlan)#vlan 3
S1(config-vlan)#name Marketing
S1(config-vlan)#vlan 4
S1(config-vlan)#name Accounting
S1(config-vlan)#^Z
S1#

From this output, you can see that you can create VLAN from 2–4094, but as I mentioned, this is only mostly true. VLANs can only be created up to the limit of 1001, and you can't use, change, rename, or delete VLANs 1 and 1002 through 1005 because they are reserved. Any VLAN numbers above that are called extended VLANs and won't be saved in the database unless your switch is set to VTP Transparent mode. You won't see these VLAN numbers used too often in production. Here's a demonstration of setting my S1 switch to VLAN 4000 when my switch is set to VTP Server mode (the default VTP mode):

S1#config t
S1(config)#vlan 4000
S1(config-vlan)#^Z
% Failed to create VLANs 4000
Extended VLAN(s) not allowed in current VTP mode.
%Failed to commit extended VLAN(s) changes.

Find more information on switching and VTP in my CCNA Study Guide.

After you create the VLANs that you want, you can use the show vlan command to see them. But notice that by default, all ports on the switch are in VLAN 1. To change the VLAN associated with a port, you need to go to each interface and tell it which VLAN to be a part of.

S1#sh vlan

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Name</th>
<th>Status</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>default</td>
<td>active</td>
<td>Fa0/3, Fa0/4, Fa0/5, Fa0/6</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Fa0/7, Fa0/8, Gi0/1</td>
</tr>
<tr>
<td>2</td>
<td>Sales</td>
<td>active</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Marketing</td>
<td>active</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Accounting</td>
<td>active</td>
<td></td>
</tr>
</tbody>
</table>

Remember that a created VLAN is unused until it is assigned to a switch port or ports, and that all ports are always assigned in VLAN 1 unless set otherwise.
You can’t change, delete, or rename VLAN 1, because it’s the default VLAN and you just can’t change that—period. It’s the native VLAN of all switches by default, and Cisco recommends that you use this as your administrative VLAN. Native VLAN basically means that any packets that aren’t specifically assigned to a different VLAN will be sent down the native VLAN. The frames sent down the trunk are therefore “untagged.”

In the previous S1 output, you can see that ports Fa0/3–8 and the Gi0/1 uplink are all in VLAN 1, but where are ports 1 and 2? Any port that’s designated as a trunk port will not show up in the show vlan output. Use the `show interface trunk` command instead if you want to check out all your trunked ports.

Okay—now that we can see the VLANs that have been created, we can assign switch ports to specific ones. Each port can be part of only one VLAN.

### Assigning Switch Ports to VLANs

You configure a port to belong to a VLAN by assigning a membership mode that specifies the kind of traffic that port will carry, as well as the number of VLANs that it can belong to. You configure each port on a switch to be in a specific VLAN (access port) by using the `interface` command `switchport`. You can also configure a bunch of ports at the same time with the `interface range` command.

Don’t forget that you can configure either static memberships or dynamic memberships on a port. I’m going to configure interface Fa0/3 to VLAN 3. Check it out:

```
S1#config t
S1(config)#int fa0/3
S1(config-if)#switchport ?
    access        Set access mode characteristics of the interface
    backup        Set backup for the interface
    block         Disable forwarding of unknown uni/multi cast addresses
    host          Set port host
    mode          Set trunking mode of the interface
    nonegotiate   Device will not engage in negotiation protocol on this interface
    port-security Security related command
    priority      Set appliance 802.1p priority
    protected     Configure an interface to be a protected port
    trunk         Set trunking characteristics of the interface
    voice         Voice appliance attributes
```

Looking at this output, you can see some commands that I’ve already shown you, but I’m also going to cover the `access`, `mode`, `nonegotiate`, `trunk`, and `voice` commands in this
section. Let’s start with setting an access port on S1’s that’s probably the most widely used type of port on production switches that has VLANs configured:

S1(config-if)#switchport mode ?
  access   Set trunking mode to ACCESS unconditionally
  dynamic Set trunking mode to dynamically negotiate access or
trunk mode
  trunk    Set trunking mode to TRUNK unconditionally

S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 3

By starting with the switchport mode access command, you’re essentially telling the switch that this is a Layer 2 port. Then you can move on and assign a VLAN to the port with the switchport access command. Remember, you can choose boatloads of ports to configure at the same time if you use the interface range command. The dynamic and trunk commands are used for trunk ports exclusively.

That’s it. Well, sort of. If you plugged devices into each VLAN port, they can only talk to other devices in the same VLAN. We want to enable inter-VLAN communication by using a router or a Layer 3 switch—something that’s just not necessary to cover in this book. But let’s take a look at how to create trunk ports...

### Configuring Trunk Ports

Good to know is that some Cisco switches only run the IEEE 802.1Q encapsulation method. To configure trunking on a Fast Ethernet port, you use the interface command trunk [parameter]. It’s a tad different on a switch that can run both ISL and the 802.1Q switch, and I’ll show you that in a minute.

This switch output shows the trunk configuration on interface Fa0/8 as set to trunk on:

S1#config t
S1(config)#int fa0/8
S1(config-if)#switchport mode trunk

This list describes the options available to you when configuring a switch interface:

- **switchport mode access** This option puts the interface (access port) into permanent nontrunking mode and negotiates to convert the link into a nontrunk link. The interface becomes a nontrunk interface regardless of whether the neighboring interface is a trunk interface, and this port would become a dedicated Layer 2 port.

- **switchport mode dynamic auto** This option allows the interface to convert the link to a trunk link. The interface becomes a trunk interface if the neighboring interface is set to trunk or desirable mode. This is now the default switchport mode for all Ethernet interfaces on all new Cisco switches.
**switchport mode dynamic desirable**  This option makes the interface actively attempt to convert the link to a trunk link. The interface becomes a trunk interface if the neighboring interface is set to trunk, desirable, or auto mode. I used to see this as the default on some older switches but not anymore. The default is dynamic auto now.

**switchport mode trunk**  This option puts the interface into permanent trunking mode and negotiates to convert the neighboring link into a trunk link. The interface becomes a trunk interface even if the neighboring interface isn’t one.

**switchport nonegotiate**  This option prevents the interface from generating DTP frames. You can use this command only when the interface switchport mode is access or trunk. You must manually configure the neighboring interface as a trunk interface to establish a trunk link.

---

**NOTE**

Dynamic Trunking Protocol (DTP) is used for negotiating trunking on a link between two devices, as well as the encapsulation type of either 802.1Q or ISL. I use this nonegotiate command when I want dedicated trunk ports and want no questions asked!

To disable trunking on an interface, use the `switchport mode access` command, which sets the port back to a dedicated Layer 2 switch port.

**Trunking with Switches That Support ISL and 802.1Q**

For this type of 3750 switch, you have the `encapsulation` command available—a feature that the 2960 switch doesn’t offer:

```
Core(config-if)#switchport trunk encapsulation ?
   dot1q   Interface uses only 802.1Q trunking encapsulation when trunking
   isl     Interface uses only ISL trunking encapsulation when trunking
   negotiate Device will negotiate trunking encapsulation with peer on
                interface
Core(config-if)#switchport trunk encapsulation dot1q
Core(config-if)#switchport mode trunk
```

As you can see, you can add either the IEEE 802.1Q (dot1q) encapsulation or the ISL encapsulation to this switch. After you set the encapsulation, you’ve still got to set the interface mode to trunk. Honestly, it’s pretty rare that you’d continue to use the ISL encapsulation method because Cisco is moving away from ISL.

**Defining the Allowed VLANs on a Trunk**

As I said, trunk ports send and receive information from all VLANs by default, and if a frame is untagged, it will be sent straight to the management VLAN. By the way, this includes any extended range VLANs as well.
But I haven’t told you that you can remove VLANs from the allowed list. Doing so can prevent traffic from certain VLANs from traversing a trunked link. Here’s how to make that happen:

```
S1#config t
S1(config)#int f0/1
S1(config-if)#switchport trunk allowed vlan ?
    WORD VLAN IDs of the allowed VLANs when this port is in trunking mode
    add add VLANs to the current list
    all all VLANs
    except all VLANs except the following
    none no VLANs
    remove remove VLANs from the current list
S1(config-if)#switchport trunk allowed vlan remove ?
    WORD VLAN IDs of disallowed VLANs when this port is in trunking mode
S1(config-if)#switchport trunk allowed vlan remove 4
```

The above command stopped the trunk link configured on S1 port F0/1 to drop all traffic sent and received for VLAN 4. You can try to remove VLAN 1 on a trunk link, but it will still send and receive management like CDP, PAgP, LACP, DTP, and VTP, so what’s the point? Well, doing this can be a great way to mess with other people’s heads since they would then be unable to telnet or ping to another switch in the VLAN 1 management VLAN. So if you’re feeling a bit mischievous...

To remove a range of VLANs, just use the hyphen:

```
S1(config-if)#switchport trunk allowed vlan remove 4-8
```

If by chance someone has removed some VLANs from a trunk link and you want to set the trunk back to default, just use this command:

```
S1(config-if)#switchport trunk allowed vlan all
```

Or this one, which accomplishes the same thing:

```
S1(config-if)#no switchport trunk allowed vlan
```

Now is a great time to show you how to configure pruning for VLANs before we start routing between VLANs.

**Changing or Modifying the Trunk Native VLAN**

Believe it or not, you can change the trunk port native VLAN from VLAN 1, and some people do this for security reasons, so pay attention. To change the native VLAN, use the following command:

```
S1#config t
S1(config)#int f0/1
```
S1(config-if)#switchport trunk ?
   allowed Set allowed VLAN characteristics when interface is in trunking mode
   native Set trunking native characteristics when interface is in trunking mode
   pruning Set pruning VLAN characteristics when interface is in trunking mode
S1(config-if)#switchport trunk native ?
   vlan Set native VLAN when interface is in trunking mode
S1(config-if)#switchport trunk native vlan ?
   <1-4094> VLAN ID of the native VLAN when this port is in trunking mode
S1(config-if)#switchport trunk native vlan 40
S1(config-if)#^Z

Sweet—we successfully changed our native VLAN on our trunk link to 40! And now, by using the show running-config command, we'll get to see the configuration under the trunk link:

```
interface FastEthernet0/1
   switchport trunk native vlan 40
   switchport trunk allowed vlan 1-3,9-4094
   switchport trunk pruning vlan 3,4
```

Sounds, looks, and seems simple, right? Uh huh, in a perfect world... You really didn't think that it was this easy, did you? Of course not! So here's the rub: if all switches do not have the same native VLAN configured on the trunk links, you will start to receive this error:

19:23:29: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/1 (40), with Core FastEthernet0/7(1)
19:24:29: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/1 (40), with Core FastEthernet0/7(1)

Actually, this is a good, noncryptic error, so either you go to the other end of your trunk link(s) and change the native VLAN, or set the native VLAN back to the default. Here's how you'd do that:

```
S1(config-if)#no switchport trunk native vlan
```

Now, everything is coming up roses and our trunk link is using the default VLAN 1 as the native VLAN. Just remember that all switches must use the same native VLAN or you'll experience some serious grief!
Summary

This chapter was a great way to begin your journey through the wonderful world of wireless networking. You got a lot of information on wireless technologies in this chapter, plus some critical terms and basics to ensure that you’re well prepared for things to come.

I started off by telling you about various wireless technologies and then described the differences between a PAN, WLAN, WMAN, and WWAN. After talking about the basic wireless networks you’ll run into today, I described in detail the various wireless topologies like BSS, IBSS, ESS, and SSID.

You learned about antennas, repeaters, and some really important fundamentals regarding bridging. You then gained the crucial information on switches and how they work that you’ll need for the rest of this book.

I wrapped up this chapter by delving into the necessary basics of switching and VLANs, as well as how access links, trunk links, and native VLANs all work within switched networks.

Exam Essentials

Remember what an IBSS is. An IBSS is actually two things: an independent basic service set and an infrastructure basic service set. An independent BSS is an ad hoc or peer-to-peer network, and an infrastructure is a wireless network with an AP managing traffic between wireless clients.

Know what an aWBG is. The autonomous workgroup bridge (aWGB) will establish a single wireless connection for multiple Ethernet clients to an upstream AP to appear as a nonstandard client.

Know what a uWGB is. The universal workgroup bridge (uWGB) is used to support one Ethernet client connected through a WGB to an AP from another vendor to appear as a single normal client.

Understand when you would use a repeater. A repeater is an AP that extends the cell of the root AP. The repeater AP must be set in the same frequency (channel) and must overlap by 50 percent.

Understand how to trunk and change the native VLAN on a switch port. When configuring controllers, you must be able to configure a switch with access and trunk ports, set the encapsulation, and change the native VLAN. An example would look something like this:

```
Interface f0/1
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk native vlan 50
```
Written Lab

1. True/False: A uWGB is used to connect a single Ethernet client through a WGB to a root AP from a non-Cisco device.

2. True/False: A aWGB is used to connect a single Ethernet client through a WGB to a root AP from a non-Cisco device.

3. If you have multiple APs connected in the same distribution system and they use the same SSID, what is this type of network called?

4. What is an ad hoc wireless network called?

5. True/False: Root bridges can communicate to other root devices.

6. What type of wireless network only goes 10m?

7. What is an MBSSID?

8. SSIDs can have how many characters configured?

9. True/False: The distribution system (DS) is used to trunk between switches so that MBSSIDs can be used.

10. The native VLAN on switches is VLAN 10 by default and cannot be changed.
Chapter 1 • Wireless Networks and Topologies

Review Questions

1. Which of the following is true regarding aWGBs?
   A. The aWGB will establish a single wireless connection for multiple Ethernet clients to an upstream AP to appear as a nonstandard client.
   B. The aWGB is used to support one Ethernet client connected through a WGB to an AP from another vendor to appear as a single normal client.
   C. The aWGB is used to support a single wireless connection connected through a WGB to an AP from another vendor to appear as a single normal client.
   D. The aWGB is used to support one Ethernet client connected through a WGB to an AP from another vendor to appear as a single normal client.

2. Which of the following is true regarding uWGBs?
   A. The uWGB will establish a single wireless connection for multiple Ethernet clients to an upstream AP to appear as a nonstandard client.
   B. The uWGB is used to support one Ethernet client connected through a WGB to an AP from another vendor to appear as a single normal client.
   C. The aWGB is used to support a single wireless connection connected through a WGB to an AP from another vendor to appear as a single normal client.
   D. The aWGB is used to support one Ethernet client connected through a WGB to an AP from another vendor to appear as a single normal client.

3. Which best describes an ad hoc network?
   A. Basic service set
   B. Extended service set
   C. Independent basic service set
   D. Mesh network
   E. WiMAX network

4. How long can an SSID name be?
   A. 10 characters
   B. 32 characters
   C. 64 characters
   D. 128 characters

5. If you have a small wireless network that connects devices such as your PDA and wireless headset to your PC, what is this network called?
   A. WPAN
   B. WLAN
   C. WMAN
   D. WWAN
6. If you have a wireless network that connects buildings for very long distances and covers a large geographic area, what is this network called?
   A. WPAN
   B. WLAN
   C. WMAN
   D. WWAN

7. If you have a wireless network that connects users in your office together at high speeds, what is this network called?
   A. WPAN
   B. WLAN
   C. WMAN
   D. WWAN

8. If you have a wireless network that connects buildings in your campus area that are line of sight, what is this network called?
   A. WPAN
   B. WLAN
   C. WMAN
   D. WWAN

9. Which of the following is true of independent basic service sets (IBSSs)?
   A. They only provide high-speed wireless across a campus environment.
   B. They only provide high-speed wireless in a small area, are limited in scope, and are not scalable.
   C. They can only send wireless signals about 10m.
   D. You must have multiple APs in order to make this function.

10. What of the following is true of a basic service set (BSS)?
    A. They only provide high-speed wireless across a campus environment.
    B. They only provide high-speed wireless in a small area, are limited in scope, and are not scalable.
    C. They can only send wireless signals about 10m.
    D. They can use multiple APs to extend the WLAN.

11. The wired section of the network that is reachable through the AP is called what?
    A. IBSS
    B. Distribution system (DS)
    C. Ad hoc
    D. ESS
12. If you have an extended service set (ESS), how much do the cells need to overlap in order for users not to lose their connection when roaming from one AP to another?
   A. 5–7 percent
   B. 10–15 percent
   C. 20–25 percent
   D. 35–50 percent

13. If you have a repeater network with two APs, how much do the cells need to overlap in order for users not to lose their connection when on the repeating AP?
   A. 5 percent
   B. 10 percent
   C. 25 percent
   D. 50 percent

14. In order to create an ESS, what must you do to each AP?
   A. If you have two or more APs, they must be set to the same frequency channel.
   B. If you have more than one AP, they must be in separate VLANs.
   C. If you have two or more APs, they must have the same SSID name.
   D. One of the APs in the ESS must be in repeater mode.

15. If you have an ESS network, how does the client understand that it is communicating to different APs when it roams?
   A. It doesn't since the SSID is the same on all APs.
   B. The AP assigns a derived MAC address for each SSID on the AP.
   C. The MAC address of the hosts is stored in a MAC address table on the AP.
   D. The trunk link connected to the AP uses frame tagging to identify each frame.

16. If you have an AP with multiple SSID configured, what is this called?
   A. BSS
   B. ESS
   C. BSSID
   D. MBSSID

17. Which of the following networks have the best redundancy for wireless networks?
   A. IBSS
   C. MBSISS
   C. MESH
   D. ESS
18. Which of the following is true regarding bridged networks?
   A. Root bridges can only communicate to other root bridges.
   B. Nonroot bridges can only communicate to root bridges.
   C. Root bridges can only communicate to APs.
   D. Nonroot bridges can only communicate to nonroot bridges.

19. What are the two types of links on a switch? (Choose two.)
   A. Full-duplex
   B. Half-duplex
   C. Access
   D. Trunk

20. Which command will change the native VLAN on a switch to VLAN 50?
   A. `switch(config-if)#switchport trunk native vlan 50`
   B. `switch(config-if)#switchport native vlan 40`
   C. `switch(config)#switchport trunk native vlan 50`
   D. `switch(config-if)#switchport access native vlan 50`
Answers to Review Questions

1. A. This can be a tricky question. You need to pay attention if the question is asking about universal or autonomous WGBs. This question is about universal, which is nonproprietary and appears to a Cisco AP as a nonstandard client.

2. B. You need to pay attention if the question is asking about universal or autonomous WGBs. This question is about autonomous, which is proprietary and appears to a Cisco AP as a single normal client.

3. C. The ad hoc network, or peer to peer, is also called an independent basic service set (IBSS).

4. B. The service set identifier (SSID) is used to define the basic service area (BSA) and can be up to 32 characters long. You can have multiple SSIDs configured on an AP.

5. A. Wireless personal area networks are used to connect your devices in a small office area. The maximum distance for a WPAN is about 10m (30 feet) and the most common type of WPAN is Bluetooth.

6. D. Wireless wide area networks are typically cellular networks that cover a large geographic area but do not have the speeds of a WLAN.

7. B. Wireless local area networks are the most common type of wireless networks in use in our homes and offices today. They provide high speeds and can cover as much area as you need depending on how many APs you install.

8. C. Wireless metropolitan area networks are used in a campus environment to connect buildings together using bridges. In this type of network, all connections must be line of sight.

9. B. Independent basic service sets, or ad hoc networks, are typically not used in today’s networks because they are no longer needed, but you can use them. Take two PCs with wireless capability and they can communicate, just like taking a crossover cable between two hosts with Ethernet.

10. D. Basic service sets, or WLANs, are the most popular LANs and can be very easy to set up. Just buy an AP and connect to your ISP and they typically just work. However, the commercial-grade APs, such as Cisco’s, do not work out of the box. You must configure at least the SSID on them to make them work.

11. B. The wired section of the network that is reachable through the AP is called distribution system (DS). If you want to have an extended service set (ESS), all APs must be set to the same SSID and connect to the same DS.

12. B. The cells must overlap by at least 10 percent; 15 percent would be better, but the minimum must be at least 10 percent.

13. D. The cells in a repeater number must overlap by at least 50 percent.
14. C. To create an ESS, you must set the SSID the same on all APs. Also, the APs must all connect to the same distribution system (DS).

15. B. The APs all associate clients using a MAC address that they derive from the AP’s MAC address. The clients, when handed off to another AP, see that they are communicating to another AP based on the new AP address they are receiving from the new AP they connected to.

16. D. An AP can have more than one SSID configured. If you have an AP with more than one SSID configured, this is called a multiple basic service set identifier, and it is a MAC address that the AP basically just makes up.

17. C. Bridges networks have a downside: if the central point gets disconnected, the whole network may go down. A mesh network has fully redundancy. If one AP drops out of the network, the neighbor APs simply find another route.

18. B. Nonroot devices, such as bridges, APs in nonroot mode, clients, and WGBs, can only communicate to root devices.

19. C, D. Switch ports are basically configured to be access links, which means they are a member of only one VLAN, or trunk links, which pass information about all, or many, VLANs.

20. A. To change the native VLAN on a switch trunk link, from the switch interface configured as a trunk, use the command `switchport trunk native vlan vlan#` (in this example, `vlan 50`).
Answers to Written Lab

1. False
2. True
3. Extended Service Set (ESS)
4. Independent basic service set (IBSS)
5. False
6. Personal area networks (PANs)
7. A multiple basic service set identifier is an AP configured with multiple SSIDs.
8. 32
9. False
10. False