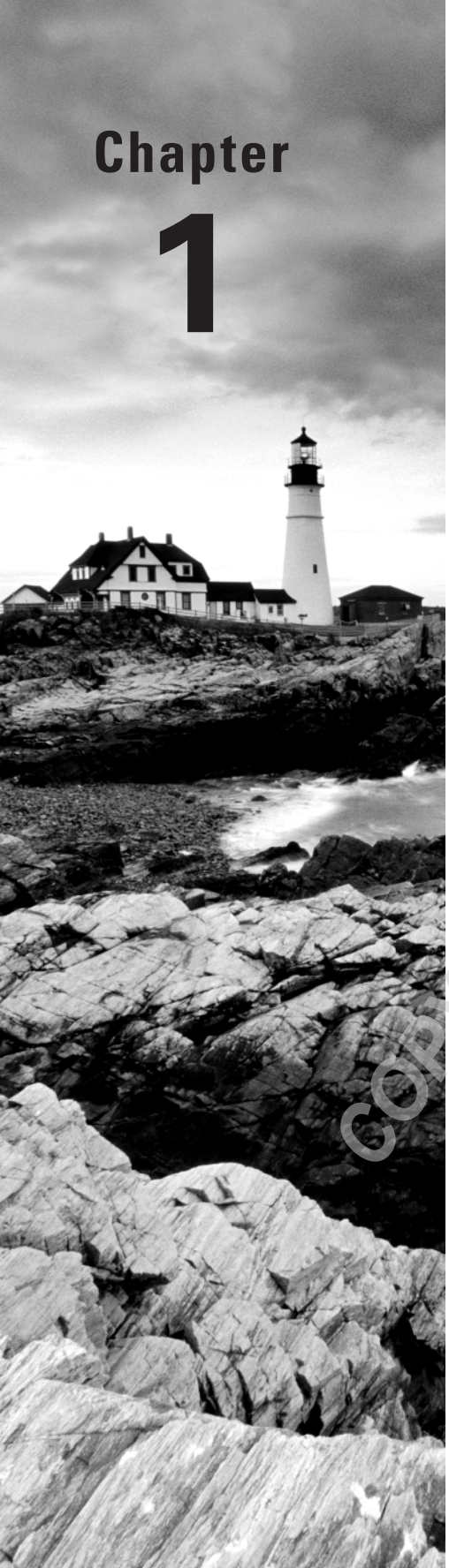


Chapter 1

Introduction to Networks

THE FOLLOWING COMPTIA NETWORK+ EXAM OBJECTIVES ARE COVERED IN THIS CHAPTER:

- ✓ **2.3 Identify common physical network topologies**
  - Star
  - Mesh
  - Bus
  - Ring
  - Point to point
  - Point to multipoint
  - Hybrid
- ✓ **2.7 Explain common logical network topologies and their characteristics**
  - Peer to peer
  - Client/server
  - VPN
  - VLAN

COPYRIGHTED MATERIAL

You'd have to work pretty hard these days to find someone who would argue that our computers have become invaluable to us personally and professionally. Our society has become highly dependent on these resources and on sharing them with each other. The ability to communicate with those we need to—whether they're in the same building or in some far-away land—completely hinges on our capacity to create and maintain solid, dependable networks.

And those vitally important networks come in all shapes and sizes—ranging from small and simple, to humongous and super complicated. But whatever their flavor, they all need to be maintained properly; and in order to do that well, you've got to understand networking basics. The various types of devices and technologies that are used to create networks, as well as how they work together, is what this book is about, and I'll go through this critical information one step at a time with you. Understanding all of this will not only equip you with a rock-solid base to build on as you grow in your IT knowledge and career, but will also arm you with what you'll need to ace the Network+ certification exam!

There are two other topics under Objective 2.7—virtual private networks (VPNs) and virtual local area networks (VLANSs)—that I'll only be introducing to you in this chapter. So make a little note to yourself that I'm going to cover VPNs thoroughly later on in Chapter 13, "Authentication and Access Control," and I'll tell you all about VLANs in Chapter 11, "Switching and Virtual LANs."

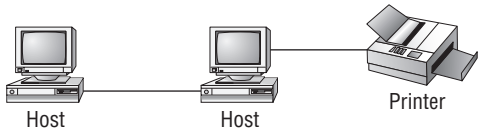
To find up-to-the-minute updates for this chapter, please see `www.lammle.com` or `www.sybex.com/go/comptianetwork+studyguide`.

First Things First: What's a Network?

The dictionary defines the word *network* as "a group or system of interconnected people or things." Similarly, in the computer world, the term *network* means two or more connected computers that can share resources like data and applications, office machines, an Internet connection, or some combination of these, as shown in Figure 1.1.

Okay—Figure 1.1 shows a really basic network made up of only two host computers connected together; they share resources like files and even a printer hooked up to one of the hosts. These two hosts "talk" to each other using a computer language called *binary code*, which consists of lots of 1s and 0s in a specific order that describes exactly what they want to "say."

FIGURE 1.1 A basic network



Next, I'm going to tell you about local area networks (LANs), how they work, and even how we can connect LANs together. Then, later in this chapter, I'll describe how to connect remote LANs together through something known as a wide area network (WAN).

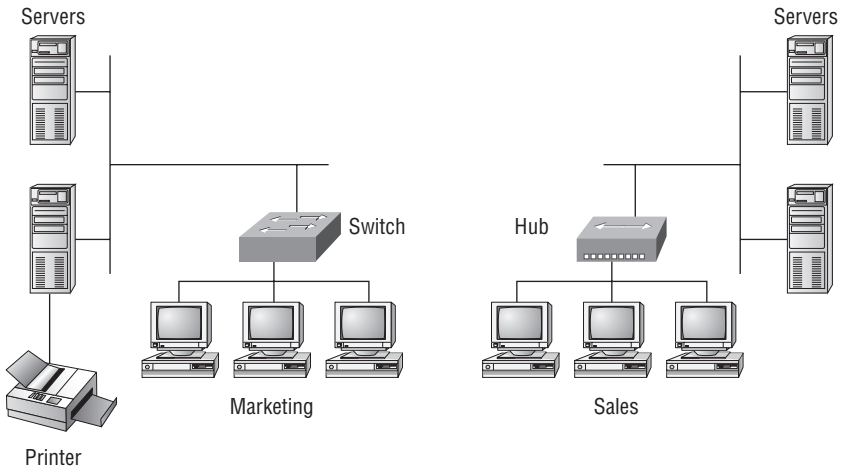
The Local Area Network (LAN)

Just as the name implies, a *local area network (LAN)* is usually restricted to spanning a particular geographic location like an office building, a single department within a corporate office, or even a home office.

Back in the day, you couldn't put more than 30 workstations on a LAN, and you had to cope with strict limitations on how far those machines could actually be from each other. Because of technological advances, all that's changed now, and we're not nearly as restricted in regard to both a LAN's size and the distance a LAN can span. Even so, it's still best to split a big LAN into smaller logical zones known as *workgroups* to make administration easier.

In a typical business environment, it's a good idea to arrange your LAN's workgroups along department divisions; for instance, you would create a workgroup for Accounting, another one for Sales, and maybe another for Marketing—you get the idea. Figure 1.2, which shows two separate LANS, each as its own workgroup.

FIGURE 1.2 A small LAN Two separate LANs (workgroups)



First, don't stress about the devices labeled *hub* and *switch*—these are just connectivity devices that allow hosts to physically connect to resources on a LAN. Trust me; I'll describe them to you in much more detail later in Chapter 5, "Networking Devices."

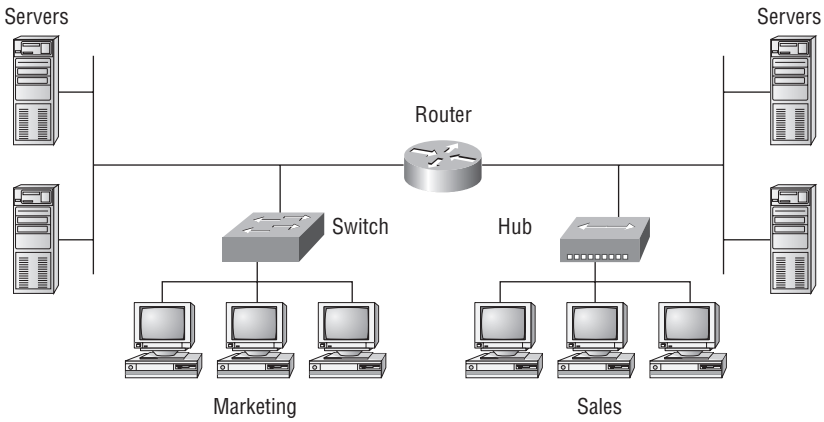
Anyway, back to the figure… Notice that there's a Marketing workgroup and a Sales workgroup. These are LANs in their most basic form. Any device that connects to the Marketing LAN can access the resources of the Marketing LAN—in this case, the servers and printer. If you want to access resources from the Sales LAN, then you must connect directly to the Sales LAN.

There are two problems with this:

1. You must be physically connected to each LAN to get the resources from that specific workgroup's LAN.
2. You can't get from one LAN to the other LAN and use its server data and printing resources remotely.

This is a typical network issue that's easily resolved by using a cool device called a router to connect the two LANs together, as shown in Figure 1.3.

FIGURE 1.3 A router connects LANs together.



Nice—problem solved! Even though you can use routers for more than just connecting LANs together, the router shown in Figure 1.3 is a great solution because the host computers from the Sales LAN can get to the resources (server data and printers) of the Marketing LAN, and vice versa.

Now, you might be thinking that we really don't need the router—that we could just physically connect the two workgroups together with a type of cable that would allow the Marketing and Sales workgroups to hook up somehow. True—we could do that, but if we did, then we would have only one big, cumbersome workgroup instead of separate workgroups for Marketing and Sales. And that kind of arrangement isn't practical for today's networks.

This is because with smaller, individual, yet connected groups, the users on each LAN enjoy much faster response times when accessing resources; and administrative tasks are a

lot easier, too. Larger workgroups run more slowly because in them, a legion of hosts are all trying to get to the same resources simultaneously. So the router shown in Figure 1.3, which separates the workgroups while still allowing access between them, is a really great solution after all.

Like I said—don't worry about the network connectivity devices I've mentioned so far in this chapter, like hubs, switches, and routers. I promise to cover them all in detail in Chapter 5. At this stage, I really want you to focus on understanding the concepts that I'm presenting. For now, all you need to know is that hubs and switches are devices that connect other devices together, and routers connect networks together.

So now, let me define those other terms I've used so far: workstations, servers, and hosts.

Common Network Components

There are a lot of different machines, devices, and media that make up our networks. Right now, I'm going to tell you about three of the most common:

- Workstations
- Servers
- Hosts

Workstations

Workstations are often seriously powerful computers that run more than one central processing unit (CPU) and whose resources are available to other users on the network to access when needed. Don't confuse workstations with client machines, which can be workstations but aren't always. A *client machine* is any device on the network that can ask for access to resources from a workstation—for instance, a printer.

The terms *workstation* and *host* are used interchangeably because computers have become more and more powerful and the terms have become somewhat fuzzy. The term *host* is used to describe pretty much anything that takes an IP address.

Servers

Servers are also powerful computers. They get their name because they truly are "at the service" of the network and run specialized software for the network's maintenance and control known as the *network operating system*.

In a good design that optimizes the network's performance, servers are highly specialized and are there to handle one important labor-intensive job. This is not to say that a single server can't do many jobs; but more often than not, you'll get better performance if you dedicate a server to a single task. Here's a list of common dedicated servers:

File server Stores and dispenses files.

Mail server The network's post office, which handles email functions.

Print server Manages all printers on the network.

Web server Manages web-based activities by running Hypertext Transfer Protocol (HTTP) for storing web content and accessing web pages.

Fax server The "memo maker" that sends and receives paperless faxes over the network.

Application server Manages network applications.

Telephony server Handles the call center and call routing and can be thought of as a sophisticated network answering machine.

Remote-access server Provides remote users with access to the network through modems, an IP connection, or wirelessly.

Proxy server Handles tasks in the place of other machines on the network.

See how the name of each kind of server indicates what it actually does—how it serves the network? This is an excellent way to remember them.

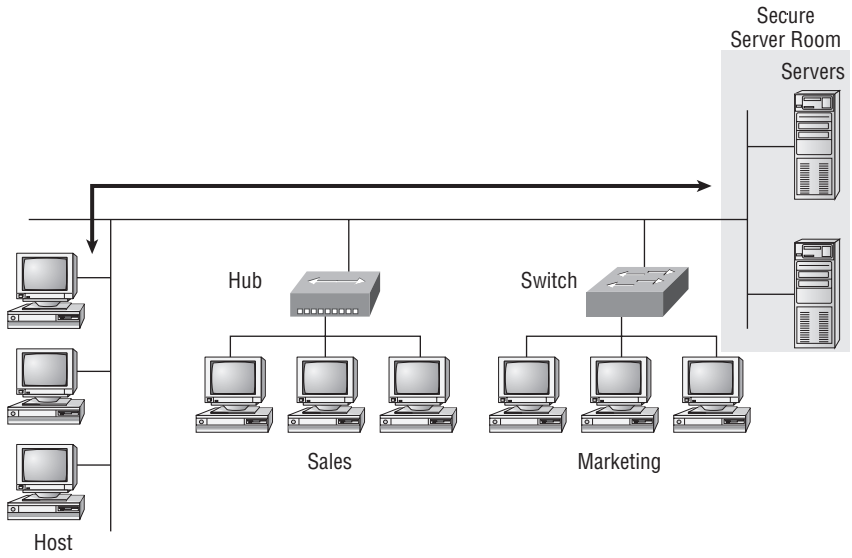
Okay, like I said, servers are usually dedicated to doing one specific important thing within the network. But not always—sometimes they have more than one job. But whether servers are designated for one job or are network multitaskers, they all maintain the network's data integrity by backing up the network's software and hardware. And no matter what, they all serve a number of client machines.

Back in Figure 1.2, I showed you an example of two really simple LAN networks. I want to make sure you know that servers must have considerably superior hard-drive space—a lot more than a simple workstation's capacity—because they serve many client machines and provide any resources they require. Because they're so important, you should always put your servers in a very secure area. My company's servers are in a locked server room because not only are they really pricey workhorses, but they also store huge amounts of important and sensitive company data; so, they need to be kept safe from any unauthorized access.

In Figure 1.4, you can see a network populated with both workstations and servers. You also see that the hosts can access the servers across the network—pretty much the general idea of having a network.

You probably noticed that there are more workstations here than servers, right? Think of why that is… If you answered that it's because one server can provide resources to what can sometimes be a huge number of individual users at the same time, but workstations don't, you've got it!

FIGURE 1.4 A network populated with servers and workstations



Hosts

It can be kind of confusing because when people refer to hosts, they really can be referring to almost any type of networking devices—including workstations and servers. But if you dig a bit deeper, you'll find that usually this term comes up when people are talking about resources and jobs that have to do with Transmission Control Protocol/Internet Protocol (TCP/IP). The scope of possible machines and devices is so broad because, in TCP/IP-speak, a *host* means any network device with an IP address. Yes, you'll hear IT professionals throw this term around pretty loosely; but for the Network+ exam, stick to the definition being network devices, including workstations and servers, with IP addresses.

Here's a bit of background: The name *host* harkens back to the Jurassic period of networking when those dinosaurs known as *mainframes* were the only intelligent devices to roam the network. These were called *hosts* whether they had TCP/IP functionality or not. In that bygone age, everything else in the network-scape was referred to as *dumb terminals*, because only mainframes—hosts—were given IP addresses. Another fossilized term from way back then is the use of *gateways* when talking about any Layer 3 machines like routers. We still use these terms today, but they've evolved a bit to refer to the many intelligent devices populating our present-day networks, each of which has an IP address. This is exactly the reason why you hear *host* used so broadly.

Now, let's dive a tad deeper into the workgroup subject I started when I described a basic LAN to you in the beginning of this chapter.

Virtual LANs (VLANs)

It's time to stop using the word *workgroups* when referring to the hosts and resources on a LAN and start using the words *virtual LANs (VLANs)*, which are pretty much the same thing with a new name.

A VLAN is really no different than a LAN or LAN workgroup, except that it's not physically built to look anything like the individual LANs shown in Figure 1.2. Instead, it's built *logically*. They both work exactly the same way—the hosts, server, and printers are configured exactly the same—and it's even possible that the router will be configured the same way, too.

So where does the word *virtual* fit in here, and how is this different than the earlier definition of a workgroup? Well, back in Figure 1.2, your network resources were all physically connected together locally. You had to physically walk to the Sales department to get to its resources like servers. The router in Figure 1.3 fixed this problem because it made it so that you could be physically on the Marketing LAN and get to the Sales servers via the router. I've got to tell you—doing this is not a solution I'd recommend. "What!? But Todd, you just said that's why we put the router in Figure 1.3—so one LAN can talk to the other one!"

Yes, true, we want to make our workgroups (VLANs) small, and the router helped us accomplish this. But in today's networks, we don't want to send data through a router unless we absolutely have to. We want resources like servers and printers local to the hosts—meaning right there on the same LAN. This isn't always possible in a network designed as shown in Figures 1.2 and 1.3 because people move around so much in today's possibly worldwide networks. So it's VLANs to the rescue!

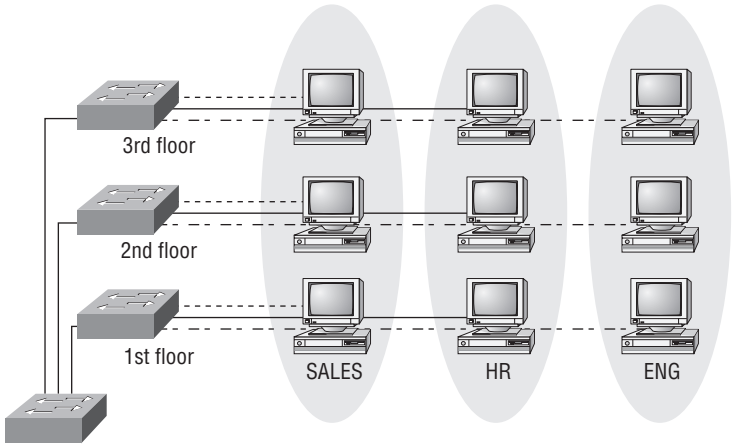
Okay, because this can get confusing fast, so let me clarify what I've said so far: In a LAN, your host is connected to a network, which is the workgroup where it resides—for example, in Sales. In a VLAN, your host still resides in a network (or VLAN), but where you're physically connected within your network is no longer relevant. You can be hanging out on the same floor where the Marketing workgroup people work, but you can still access the Sales resources as if you were physically on the Sales LAN without going through a router to get there. This makes network access to the resources you need faster for you; plus, it can provide some nice security benefits because, by default, your host cannot communicate outside the VLAN. So even though you're connected to the Marketing floor, you can still only communicate on the Sales VLAN.

How does this work? It comes down to the particular port you're plugged into (physically connected to). That port is configured for the LAN workgroup you're a member of—if that's the Sales VLAN, you're a Sales local to the Sales servers, even if you're not actually in the Sales department. This type of network is illustrated Figure 1.5, which shows three VLANs.

This type of port configuration is called a *VLAN membership*, and it's got to be configured by an administrator on a network device called a *switch*. VLANs are seriously important in today's networks, and like I said, I'll cover them thoroughly in Chapter 11. For now, remember that VLANs are the new workgroups, and they define the same thing: a group of users sharing network resources. The difference is that VLANs allow you to be anywhere on the physical network and still be local to the specific network resources you need—sweet!

VLANs help isolate network traffic

FIGURE 1.5 A sample VLAN network



Wide Area Network (WAN)

There are legions of people who, if asked to define a *wide area network (WAN)*, couldn't do it. Yet most of them use the Big Dog of all WANs—the Internet—every day! With that in mind, you can imagine that WAN networks are what we use to span large geographic areas and truly go the distance. Like the Internet, WANs usually employ both routers and public links, so that's generally the criteria used to define them.

WANs are so important that I have dedicated an entire chapter to them: Chapter 16, "Wide Area Networks."

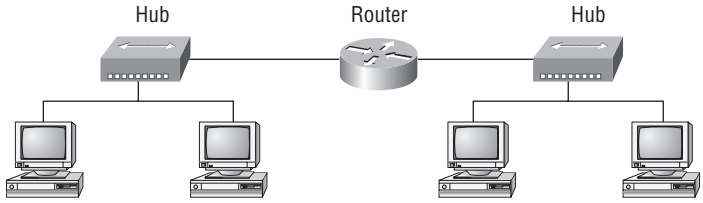
Here's a list of some of the important ways that WANs are different from LANs:

- They usually need a router port or ports.
- They span larger geographic areas and/or can link disparate locations.
- They're usually slower.
- We can choose when and how long we connect to a WAN. A LAN is all or nothing—our workstation is either connected permanently to it or not at all, although most of us have dedicated WAN links now.
- WANs can utilize either private or public data transport media like phone lines.

We get the word *Internet* from the term *internetwork*. An internetwork is a type of WAN that connects of a bunch of networks, or *intranets*. In an internetwork, hosts still use hardware addresses to communicate between each host on the LAN. However, in an internetwork, hosts use logical addresses (IP addresses) to communicate with hosts on a different LAN (other side of the router).

And *routers* are the devices that make this possible. Each connection into a router is a different logical network (broadcast domain). Figure 1.6 demonstrates how a router is employed to create an internetwork and enable our LANs (or VLANs) to access WAN resources.

FIGURE 1.6 An internetwork



The Internet is a prime example of what's known as a *distributed WAN*—an internetwork that's made up of a lot of interconnected computers located in a lot of different places. There's another kind of WAN, referred to as *centralized*, that's composed of a main, centrally located computer or location that remote computers and devices can connect to. A good example is remote offices that connect to a main corporate office.

Okay, so now we have our LANs from corporate headquarters connecting with a WAN to our remote offices. This is all good, but what if we want the hosts at the remote site to be able to access secure servers at the corporate office? Well, if you like to live dangerously, you could just open your corporate network up to the Internet so the whole world could easily get in there to your secure servers. But because that's a really bad idea, you can use *virtual private networks (VPNs)* instead.

Virtual Private Networks (VPNs)

No worries—VPNs aren't really that hard to understand. A VPN fits somewhere between a LAN and WAN and many times may seem just like a WAN link because your computer, on one LAN, connects to a different, remote LAN, and uses its resources remotely. The key difference with VPNs is a big one—security! So the definition of connecting a LAN (or VLAN) to a WAN may sound the same, but a VPN is much more.

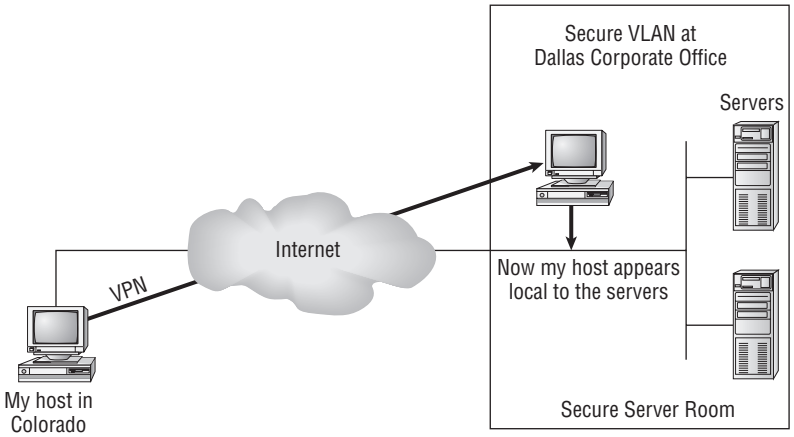
Here's the difference: A typical WAN connects two or more remote LANs together using someone else's network like, say, your Internet service provider (ISP), using a router. Your local host and router see these networks as remote networks and not as local networks or local resources. This would be a WAN in its most general definition. A VPN actually makes your local host part of the remote network by using the WAN link that connects you to the remote LAN. The VPN will make your host appear as though it's actually local on the remote network! This means that we now have access to the remote LANs resources, and that access is very secure.

This may sound a lot like the VLAN definition I just used, and really, the concept is the same: "Take my host and make it appear local to the remote resources." Just remember that for networks that are physically local, using VLANs is a good solution; but for networks that are physically remote—those that span a WAN—we'd opt for using VPNs instead.

For a simple VPN example, let's use my home office in Boulder, Colorado. Here, I have my personal host, but I want it to appear as if it's on a LAN in my corporate office in Dallas, Texas, so I can get to my remote servers. VPN is the solution I use for this because I need the security it provides.

Figure 1.7 shows this example of my host using a VPN connection from Boulder to Dallas, which allows me to access the remote network services and servers as if my host is right there on the same VLAN as my servers.

FIGURE 1.7 Example of using a VPN network



Why is this so important? If you answered, "because my servers in Dallas are secure, and only the hosts on the same VLAN are allowed to connect to them and use the resources of these servers," you nailed it! A VPN allows me to connect to these resources by locally attaching to the VLAN through a VPN across the WAN. The other option is to open up my network and servers to everyone on the Internet or another WAN service, in which case my security goes "poof!" So you can see that it's a very good thing I have a VPN.

Network Architecture: Peer-to-Peer or Client/Server?

So, we've developed networking as a way to share resources and information, and how that's achieved directly maps to the particular architecture of the network operating system software. There are two main network types you need to know about: peer-to-peer and client/server. And by the way, it's really tough to tell the difference just by looking at a diagram or even by checking out live video of the network humming along, but the difference between peer-to-peer and client/server architectures are major. They're not just physical; they're logical differences. You'll see what I mean in a bit.

Peer-to-Peer Networks

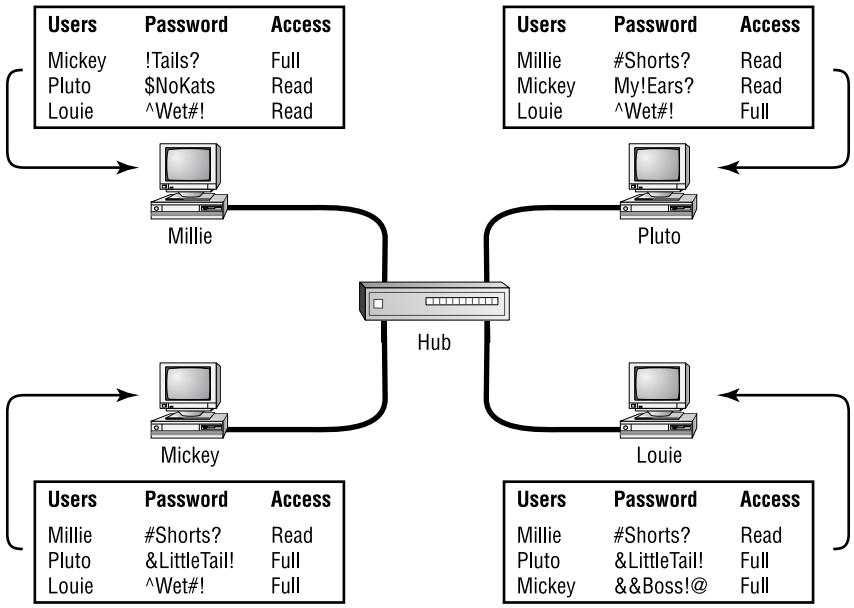
Computers connected together in *peer-to-peer networks* do not have any central, or special authority—they're all *peers,* meaning that when it comes to authority, they're all equals. This

means it's up to the computer that has the resource being requested to perform a security check for access rights to its resources.

It also means that the computers existing in a peer-to-peer network can be client machines that access resources and server machines that provide them to other computers. This works really well if there's not a huge number of users on the network, each user handles backing things up locally, and your network doesn't require a lot of security.

If your network is running Windows, Mac, or Unix in a local LAN workgroup, you have a peer-to-peer network. Figure 1.8 gives you a snapshot of a typical peer-to-peer network. Peer-to-peer networks present some challenges. For example, backing up company data becomes an iffy proposition.

FIGURE 1.8 A peer-to-peer network



Since it should be clear by now that peer-to-peer networks are all sunshine,—backing up all that super-important data is not only vital, it can be really challenging. What if you forget where you put a badly needed file (haven't we all done that)? And then there's that security issue to tangle with. Because security is not centrally governed, each and every user has to remember and maintain a list of users and passwords on each and every machine. Worse, some of those all-important passwords for the same users change on different machines—even for accessing different resources. Yikes!

Client/Server Networks

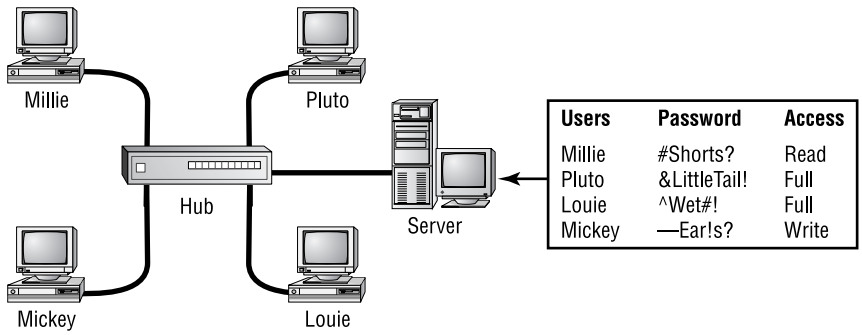
Client/server networks are pretty much the polar opposite of peer-to-peer networks because in them, a single server is specified that uses a network operating system for managing the whole network. So a client machine's request for a resource goes to the main server, which

responds by handling security and directing the client to the resource it wants, instead of the request going directly to the machine with the desired resource.

This arrangement definitely has its benefits. First, because the network is much better organized and doesn't depend on users remembering where needed resources are, it's a whole lot easier to find the files you need because everything is stored in one spot on that special server. Your security also gets a lot tighter because all usernames and passwords are on that server (which, by the way, isn't ever used as a workstation). You even gain scalability—client/server networks can have legions of workstations on them. And even with all those demands, their performance is actually optimized.

Check out Figure 1.9. Looking at it, you see a client/server network with a server that has a database of access rights, user accounts, and passwords.

FIGURE 1.9 A client/server network



Many of today's networks are a healthy (we hope) combination of the peer-to-peer and client/server architectures with carefully specified servers that permit the simultaneous sharing of resources from devices running workstation operating systems. Even though the supporting machines can't handle as many inbound connections at a time, they still run the server service reasonably well. If this type of mixed environment is designed well, most networks benefit greatly by having the capacity to take advantage of the positive aspects of both worlds.

Physical Network Topologies

Just as a topographical map shows the shape of the terrain, the *physical topology* of a network is also a type of map. It defines the specific characteristics of a network, such as where all the workstations and other devices are located, and the precise arrangement of all the physical media like cables. On the other hand, *logical topologies*, which were covered in the previous section, delineate exactly how data moves through the network. And though these two topologies are usually a lot alike, a particular network can have physical and logical topologies that are very different. But basically, what you want to remember is that a network's physical topology essentially gives you the lay of the land, and the logical topology shows how data navigates through that layout.

Here is a list of the various topologies you're most likely to run in to these days:

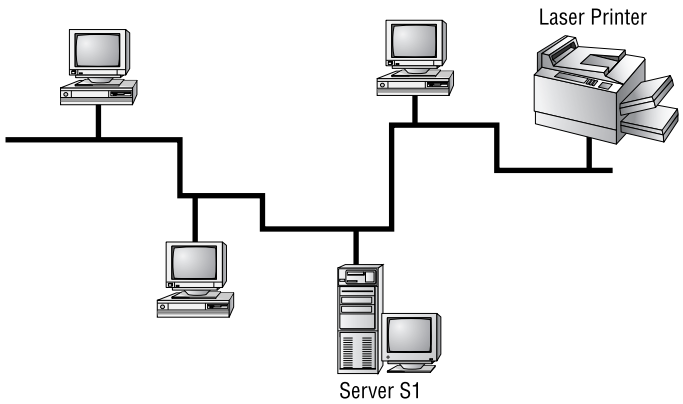
- Bus
- Star
- Ring
- Mesh
- Point-to-point
- Point-to-multipoint
- Hybrid

Bus Topology

This type of topology is the most basic one of the bunch, and it really does sort of resemble a bus. (Well, okay—actually, it looks more like a bus that's been in a pretty nasty wreck!) Anyway, the *bus topology* consists of two distinct and terminated ends, with each of its computers connecting to one unbroken cable running its entire length. Back in the day, we used to attach computers to that main cable with wire taps, but this didn't work all that well so we began using drop cables in their place (unless you're dealing with 10Base-2 Ethernet, in which case you would slip a "T" into the main cable anywhere you wanted to connect a device to it, instead of using drop cables).

Figure 1.10 depicts what a typical bus network's physical topology looks like.

FIGURE 1.10 A typical bus network's physical topology



Even though all the computers on this kind of network see all the data flowing through the cable, only the one computer that the data is specifically addressed to actually gets it. Some of the benefits in favor of using a bus topology are that it's easy to install and it's not very expensive, in part because it doesn't require as much cable as the other types of physical topologies. But it also has some drawbacks: For instance, it's hard to troubleshoot,

change, or move, and it really doesn't offer much in the way of fault tolerance because everything is connected to that single cable.

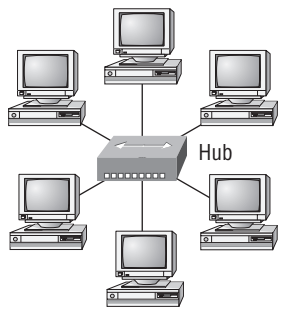
By the way, *fault tolerance* is the capability of a computer or a network system to respond to a condition automatically, often resolving it, which reduces the impact on the system. If fault-tolerance measures have been implemented correctly on a network, it's highly unlikely that any of that network's users will know that a problem even existed.

Star Topology

A *star topology's computers are* connected to a central point with their own individual cables or wireless connections. You'll often find that central spot inhabited by a device like a hub, a switch, or an access point.

Star topology offers a lot of advantages over bus topology, making it more widely used even though it obviously requires more physical media. One of its best features is that because each computer or network segment is connected to the central device individually, if the cable fails, it brings down only that particular machine or network segment. That's truly a great benefit because it makes the network much more fault tolerant as well as a lot easier to troubleshoot. Another great thing about a star topology is that it's a lot more scalable—all you have to do if you want to add to it is run a new cable and connect to the machine at the core of the star. In Figure 1.11, you'll find a great example of a typical star topology.

FIGURE 1.11 Typical star topology with a hub



Okay, although it is called *star* topology, it really looks a lot more like the imaginary pictures people draw of the sun. (Yes, the sun is a star—but it definitely doesn't look like how we usually depict it, does it?) You could also get away with saying it looks like a bike wheel with spokes connecting to the hub in the middle of the wheel and extending outward to connect to the rim. And just like that bike wheel, it's the hub device at the center of a star-topology network that can give you the most grief if something goes wrong with it. If that hub in the middle of it all happens to fail, down comes the whole network, so it's a very good thing hubs don't fail often!

Just as it is with pretty much everything, a star topology has its pros and cons. But the good news far outweighs the bad, which is why people are choosing to go with a star topology more and more. Here's a list of benefits gained by opting for a star topology:

- New stations can be added easily and quickly.
- A single cable failure won't bring down the entire network.
- It is relatively easy to troubleshoot.

The disadvantages of a star topology include the following:

- The total installation cost can be higher because of the larger number of cables (but prices are constantly becoming more competitive).
- It has a single point of failure (the hub or other central device).

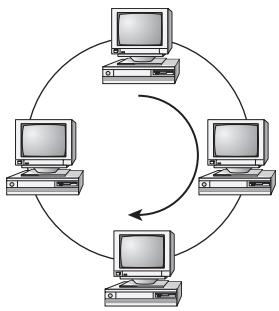
There are two more sophisticated implementations of star topology. The first is called *point-to-point link*, where you have not only the device in the center of the spoke acting as a hub, but also the one on the other end. This is still a star-wired topology, but as I'm sure you can imagine, it gives you a huge amount of scalability!

Another refined version is the wireless flavor; but to understand this version well, you've really got to have a solid grasp of the capabilities and features of all the devices populating the wireless star topology. No worries, though—I'll be covering wireless access points later on in Chapter 12, "Wireless Networking." For now, it's good enough for you to know that access points are pretty much just wireless hubs or switches that behave like their wired counterparts. Basically, they set up by point-to-point connections to endpoints and other wireless access points.

Ring Topology

In this type of topology, you'll find that each computer is directly connected to other computers within the same network. Looking at Figure 1.12, you can see that the network's data flows from computer to computer back to the source, with the network's primary cable forming a ring. The problem is, the *ring topology* has a lot in common with the bus topology because if you want to add to the network, you have no choice but to break the cable ring—something that is probably going to bring down the entire network.

FIGURE 1.12 A typical ring topology



This is one big reason why this topology isn't all that popular—you just won't run into it a lot as I did in the 1980s and early 1990s. A few more reasons include the fact that it's pricey because you need several cables to connect each computer; it's really hard to reconfigure; and as you've probably guessed, it's not fault tolerant.

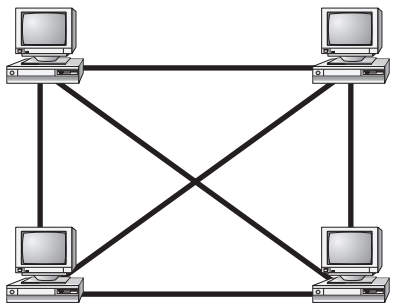
However, with all that being said, if you work at an ISP, you may find a physical ring topology in use for a technology called SONET or possibly some other WAN technology. You just won't find any LANs in physical rings anymore.

Mesh Topology

In this type of topology, you'll find that there's a path from every machine to every other one in the network. That's a lot of connections—in fact, the *mesh topology* wins the prize for "most physical connections per device"! You won't find it used in LANs very often, if ever, these days, but you will find a modified version of it known as *hybrid mesh* used in a restrained manner on WANs including the Internet.

Often, hybrid mesh topology networks will have quite a few connections between certain places to create redundancy (backup). And other types of topologies can sometimes be found in the mix too, which is also why it's dubbed *hybrid*. At any rate, it isn't a full-on full mesh topology if there isn't a connection between all devices in the network. But it's still respectably complicated—Figure 1.13 shows just how much only four connections can complicate things.

FIGURE 1.13 A typical mesh topology



As shown in the figure, things just get more and more complex as both the wiring and the connections multiply. For each n locations or hosts, you end up with $n(n–1)/2$ connections. This means that in a network consisting of only four computers, you have 4(4–1)/2, or 6 connections. And if that little network grows to, say, a population of 10 computers, you'll have a whopping 45 connections to cope with—yikes! That's a huge amount of overhead, so only small networks can really use this topology and manage it well. On the bright side, you get a very respectable level of fault tolerance. But it is nice that we don't use these in corporate LANs any longer, because they were very complicated to manage.

A Full Mesh physical topology has the absolute least likelihood of having a collision.

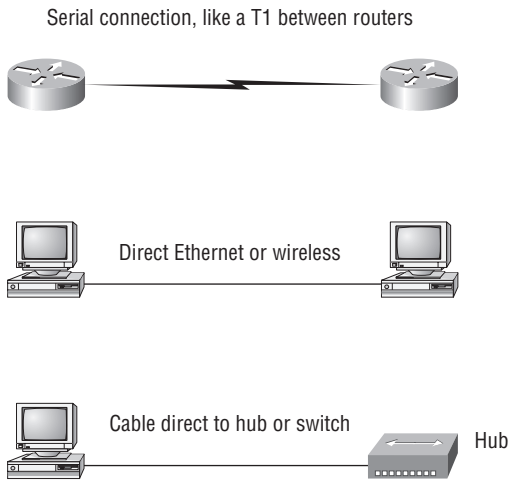
This is the reason you will usually find the hybrid version in today's WANs. In fact, the mesh topology is actually pretty rare these days. It's mainly used because of the robust fault tolerance it offers—because you've got a multitude of connections, if one goes on the blink, computers and other network devices can simply switch to one of the many redundant connections that are up and running. But as you can imagine, all that cabling in the mesh topology requires makes it really costly. Plus, you can make your network management much less insane by using what's known as a *partial mesh topology* solution instead, so why not go that way? You may lose a little fault tolerance; but if you go the partial-mesh route, you still get to use the same technology between all the network's devices. Just remember that with partial mesh, not all devices will be interconnected, so it's very important to choose wisely the ones that are.

Point-to-Point Topology

As its name implies, in a *point-to-point* topology you have a direct connection between two routers, giving you one communication path. The routers in a point-to-point topology can either be linked by a serial cable, making it a physical network, or be far apart and only connected by a circuit within a frame relay network, making it a logical network.

Figure 1.14 gives you a prime specimen of a T1, or WAN point-to-point connection.

FIGURE 1.14 Three point-to-point connections



What you see here is a lightning bolt and a couple of round things with a bunch of arrows projecting from them, right? Well, the two round things radiating arrows represent our network's two routers, and that lightning bolt represents a WAN link. (These symbols are industry standard and I'll be using them throughout this book, so it would a good idea to get used to them.)

Part two of the diagram shows two computers connected by a cable—a point-to-point link. By the way, this should remind you of something we just went over… remember our talk about peer-to-peer networks? Good! I hope you also happen to remember that a big

drawback related to peer-to-peer network sharing is that it is not very scalable. With this in mind, you probably won't be all that surprised that even if both machines have a wireless point-to-point connection, the network won't be very scalable.

You'll usually find point-to-point networks within many of today's WANs; and as you can see in part three of Figure 1.14, a link from a computer to a hub or switch is also a valid point-to-point connection. A common version of this setup consists of a direct wireless link between two wireless bridges that's used to connect computers in two different buildings together.

Point-to-Multipoint Topology

Again as the name suggests, a *point-to-multipoint* topology consists of a succession of connections between an interface on one router to multiple destination routers—one point of connection to multiple points of connection. Each of the routers and every one of their interfaces involved in the point-to-multipoint connection are part of the same network.

Figure 1.15 shows a WAN to best demonstrate a point-to-multipoint network that depicts a single corporate router connecting to multiple branches.

FIGURE 1.15 A point-to-multipoint network, Example 1

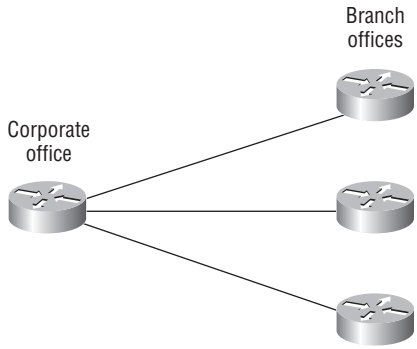
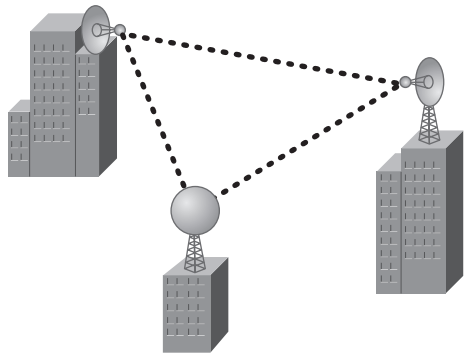


Figure 1.16 shows another prime example of a point-to-multipoint network: a college or corporate campus.

FIGURE 1.16 A point-to-multipoint network, Example 2

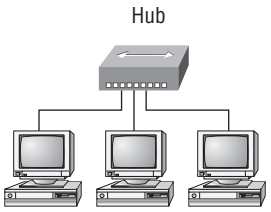


Hybrid Topology

I know I talked about hybrid network topology back in the section about mesh topology, but I didn't give you a picture of it in the form of a figure. I also want to point out that *hybrid topology* means just that—a combination of two or more types of physical or logical network topologies working together within the same network.

Figure 1.17 depicts a simple hybrid network topology. Here you see a LAN switch or hub in a star topology configuration that connects to its hosts via bus topology:

FIGURE 1.17: A Simple Hybrid Network



Physical Star, Logical Bus

Real World Scenario

They're just cables, right?

Wrong! Regardless of the type of network you build, you need to start thinking about quality at the bottom and work up.

Think of it as if you were at an electronics store buying the cables for your sweet new home-theater system. You've already spent a bunch of time and money getting the right components to meet your needs. In fact, you've probably parted with a respectable chunk of change, so why would you stop there and connect all these great devices together with the cable equivalent of twine? No, you're smarter than that. You know that picking out the exact cables that will maximize the sound and picture quality of your specific components can also protect them.

It's the same thing when you're faced with selecting the physical media for a certain network (such as your new client-server network)—you just don't want to cut corners here. Because it's the backbone of the network, you absolutely don't want to be faced with having to dig up everything that's already been installed after the fact. Doing this costs a lot more than taking the time to wisely choose the right cables and spending the money it takes to get them in the first place. The network downtime alone can cost a company a bundle (pun intended). Another reason for choosing the network's physical media correctly is that it's going to be there for a good 5 to 10 years. This means two things: It better be solid quality, and it better be scalable, because that network is going to grow and change over the years.

Topology Selection, Backbones, and Segments

Okay—now that you're familiar with many different types of network topologies, you're ready for some tips on selecting the right one for your particular network. You also need to know about backbones and segments—the very last part of this chapter.

Selecting the Right Topology

As you now know, not only do you have a buffet of network topologies to choose from, but each one also has pros and cons to implementing it. But it really comes down to that well-known adage, "ask the right questions." First, how much cash do you have? And how much fault tolerance do you really need? Also, is this network likely to grow like a weed—is it probably going to need to be quickly and easily reconfigured often? In other words, how scalable does your network need to be?

For instance, if your challenge is to design a nice, cost-effective solution that only involves a few computers in a room, getting a wireless access point and some wireless network cards is definitely your best way to go because you won't need to pony up for a bunch of cabling and it's super simple to set up. Alternately, if you're faced with coming up with a solid design for a growing company's already-large network, you're probably good to go using a wired star topology because it will nicely allow for future changes. Remember, a star topology really shines when it comes to making additions to the network, moving things around, and making any kind of changes happen quickly, efficiently, and cost effectively.

If, say, you're hired to design a network for an ISP that needs to be up and running 99.9% of the time with no more than eight hours a year allowed downtime, well, you need Godzilla-strength fault tolerance. Do you remember which topology gives that up the best? (Hint—Internet.) Your primo solution is to go with either a hybrid or a partial-mesh topology. Remember that partial mesh leaves you with a subset of $n(n–1)/2$ connections to maintain—a number that could very well blow a big hole in your maintenance budget!

Here's a list of things to keep in mind when you're faced with coming up with the right topology for the right network:

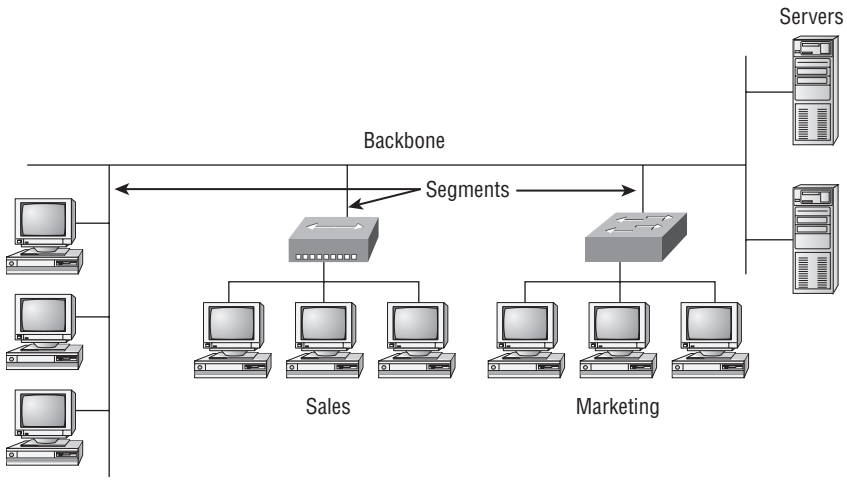
- Cost
- Ease of installation
- Ease of maintenance
- Fault-tolerance requirement

The Network Backbone

Today's networks can get pretty complicated, so we've got have a standard way of communicating with each other intelligibly about exactly which part of the network we're referring to. This is the reason we divide networks into different parts called *backbones* and *segments*.

Figure 1.18 illustrates a network and shows which part is the backbone and which parts are segments.

FIGURE 1.18 Backbone and segments on a network



You can see that the network backbone is actually kind of like our own. It's what all the networks segments and servers connect to and what gives the network its structure. As you can imagine, being such an important nerve center, the backbone must use some kind of seriously fast, robust technology—often that's Gigabit Ethernet. And to optimize network performance (that is, speed and efficiency), it follows that you would want to connect all of the network's servers and segments directly to the network's backbone.

Network Segments

When we refer to a segment, we can mean any small section of the network that may be connected to, but isn't actually a piece of, the backbone. The network's workstations connect to its servers, which in turn connect to the network backbone; you can see this by taking another look at Figure 1.18, which displays three segments.

Summary

This chapter created a solid foundation for you to build your networking knowledge on as you go through this book.

In it, you learned what, exactly, a network is, and you got an introduction to some of the components involved in building one: routers, switches, and hubs, as well as the jobs they do in a network.

You also learned that having the components required to build a network isn't all you need—understanding the various types of network connection methods like peer-to-peer and client/server is also vital.

Also covered were key networking technologies like VLANs and VPNs—the latter being the secure way to connect remote networks.

Further, you learned about the various types of logical and physical network topologies and the features and drawbacks of each. We wrapped up the chapter with a short discussion about network backbones and segments, and equipped you with the right questions to ask yourself to ensure that you come up with the right network topology for your networking needs.

Exam Essentials

Know your network topologies. Know the names and descriptions of the topologies. Be aware of the difference between physical networks—what humans see—and logical networks—what the equipment "sees."

Know the advantages and disadvantages of the topologies. It is important to know what each topology brings to the table. Knowing the various characteristics of each topology comes in handy during troubleshooting.

Understand the term *virtual private network*. You need to understand why and how to use a VPN between two sites.

Written Labs

Provide the answers to the following questions:

1. What are the three primary LAN topologies?
2. What common WAN topology often results in multiple connections to a single site, leading to a high degree of fault tolerance?
3. What is the term for a device that shares its resources with other network devices?
4. What network model draws a clear distinction between devices that share their resources and devices that do not?
5. Which network topology or connection type can be implemented with only two endpoints?
6. What device is an example of an Ethernet technology implemented as a star topology?
7. What does VPN stand for?
8. What does VLAN stand for?
9. Will a computer that shares no resources most likely be connected to the backbone or to a segment?
10. Which LAN topology is characterized by all devices being daisy-chained together with the devices at each end being connected to only one other device?

(The answers to the Written Lab can be found following the answers to the Review Questions for this chapter.)

Review Questions

1. You need a network that provides centralized authentication for your users. Which of the following logical topologies should you use?
   - **A.** VLANs
   - **B.** Peer-to-peer
   - **C.** Client/Server
   - **D.** Mesh
2. You need a topology that is scalable to use in your network. Which of the following will you install?
   - **A.** Bus
   - **B.** Ring
   - **C.** Star
   - **D.** Mesh
3. Which of the following physical topolgies has the least likelihood of having a collision?
   - **A.** Bus
   - **B.** Start
   - **C.** Ring
   - **D.** Mesh
4. In a physical-star topology, what happens when a workstation loses its physical connection to another device?
   - **A.** The ring is broken, so no devices can communicate.
   - **B.** Only that workstation loses its ability to communicate.
   - **C.** That workstation and the device it's connected to lose communication with the rest of the network.
   - **D.** No devices can communicate because there are now two unterminated network segments.
5. You want to remotely log into an office computer using remote desktop in a secure manner. Which of the following should you use?
   - **A.** VPN
   - **B.** Tagged packets
   - **C.** VLANs
   - **D.** Telnet
   - **E.** SSH

6. What is a logical grouping of network users and resources connected to administratively defined ports on a switch?
   - **A.** Host
   - **B.** Hub
   - **C.** VLAN
   - **D.** VTP

7. Which of the following is a concern when using peer-to-peer networks?
   - **A.** Where to place the server
   - **B.** Whose computer is least busy and can act as the server
   - **C.** The security associated with such a network
   - **D.** Having enough peers to support creating such a network

8. Which of the following is an example of when a point-to-multipoint network is called for?
   - **A.** When a centralized office needs to communicate with many branch offices
   - **B.** When a full mesh of WAN links is in place
   - **C.** When multiple offices are daisy-chained to one another in a line
   - **D.** When there are only two nodes in the network to be connected

9. Which of the following is an example of a LAN?
   - **A.** Ten buildings interconnected by Ethernet connections over fiber-optic cabling
   - **B.** Ten routers interconnected by frame-relay circuits
   - **C.** Two routers interconnected with a T1 circuit
   - **D.** A computer connected to another computer so they can share resources

10. Which of the following is a disadvantage of the star topology?
    - **A.** When a port on the central concentrating device fails, the attached end device loses connectivity to the rest of the network.
    - **B.** When the central concentrating device experiences a complete failure, all attached devices lose connectivity to the rest of the network.
    - **C.** In a star topology, a more expensive type of host must be used when compared to the host used when implementing a physical bus.
    - **D.** It is more difficult to add stations and troubleshoot than with other topologies.

11. What is a difference between a LAN and a WAN?
    - **A.** WANs need a special type of router port.
    - **B.** WANs cover larger geographical areas.
    - **C.** WANs can utilize either private or public data transport.
    - **D.** All of the above.

12. What does the acronym VPN stand for?

A. Virtual processor network

B. Virtual passive network

C. Virtual private network

D. Variable-length private network

13. In what type of network are all computers considered equals and do they not share any central authority?

A. Peer-to-peer

B. Client-server

C. Physical topology

D. None of the above

14. What advantage does the client-server architecture have over peer-to-peer?

A. Easier maintenance

B. Greater organization

C. Tighter security

D. All of the above

15. An example of a hybrid network is which of the following?

A. Ethernet

B. Ring topology

C. Bus topology

D. Star topology

16. You have a network with multiple devices and need to have a smaller broadcast domain while working with a tight budget. Which of the following is the best solution?

A. Use static IP addresses

B. Add more hubs

C. Implement more switches

D. Create VLANs

17. Which type of topology has the greatest number of physical connections?

A. Point-to-multipoint

B. Star

C. Point-to-point

D. Mesh

18. What type of topology gives you a direct connection between two routers so that there is one communication path?

A. Point-to-point

B. Star

C. Bus

D. Straight

19. Which network topology is a combination of two or more types of physical or two or more types of logical topologies?

A. Point-to-multipoint

B. Hybrid

C. Bus

D. Star

20. When designing a network and deciding which type of network topology to use, which item(s) should be considered? (Select all that apply.)

A. Cost

B. Ease of installation

C. Ease of maintenance

D. Fault-tolerance requirements

Answers to Review Questions

1. C. A client/server logical topology allows you to have a centralized database of users so that authentication is provided in one place.

2. C. To install a physical topology that provides ease of scalability use a star network. This is a hub or switch device, and this is the most common LAN networks today.

3. D. Only a Mesh physical topology has point-to-point connections to every device, so it has the least likelihood of ever having a collision.

4. B. In a star topology, each workstation connects to a hub, switch, or similar central device, but not to other workstations. The benefit is when connectivity to the central device is lost, the rest of the network lives on.

5. A. To connect to remote office securely, you need to use a Virtual Private Network (VPN).

6. C. VLANs allow you to be anywhere on the physical network and still be local to the network resources you need.

7. C. Security is easy to relax in a peer-to-peer environment. Because of the trouble it takes to standardize authentication, a piecemeal approach involving users' personal preferences develops. There are no dedicated servers in a peer-to-peer network, and such a network can be created with as few as two computers.

8. A. When a central office, such as a headquarters, needs to communicate directly with its branch offices, but the branches do not require direct communication with one another, the point-to-multipoint model is applicable. The other scenarios tend to indicate the use of a point-to-point link between sites.

9. D. LANs generally have a geographic scope of a single building or smaller. They can range from simple (two hosts) to complex (with thousands of hosts).

10. B. The only disadvantage mentioned is the fact that there is a single point of failure in the network. However, this topology makes troubleshooting easier; if the entire network fails, you know where to look first. The central device also ensures that the loss of a single port and the addition of a new device to an available port do not disrupt the network for other stations attached to such a device.

11. D. A typical WAN connects two or more remote LANs together using someone else's network (your ISP's) using a router. Your local host and router see these networks as remote networks and not as local networks or local resources.

12. C. Virtual private networks (VPNs) allow for the creation of private networks across the Internet. A VPN makes your local host part of the remote network by using the WAN link that connects you to the remote LAN.

13. A. In a peer-to-peer network, all computers are considered equals. It is up to the computer that has the resource being requested to perform a security check for access rights to its resources.

14. D. In client-server networks, requests for resources go to a main server that responds by handling security and directing the client to the resource it wants, instead of the request going directly to the machine with the desired resource (as in peer-to-peer).

15. A. The best answer to this question is Ethernet, which uses a star physical topology with a logical bus technology.

16. D. If you have a switch, you can break up a layer-2 switched networks into smaller broadcast domains by creating VLAN's.

17. D. In the mesh topology, there is a path from every machine to every other one in the network. A mesh topology is used mainly because of the robust fault tolerance it offers—if one connection goes on the blink, computers and other network devices can simply switch to one of the many redundant connections that are up and running.

18. A. As its name implies, in a point-to-point topology you have a direct connection between two routers, giving you one communication path. The routers in a point-to-point topology can either be linked by a serial cable, making it a physical network, or be far away and only connected by a circuit within a frame-relay network, making it a logical network.

19. B. A hybrid topology is a combination of two or more types of physical or logical network topologies working together within the same network.

20. A, B, C, D. Each topology has its own set of pros and cons regarding implementation, so asking the right questions and considering cost, ease of installation, maintenance, and fault tolerance are all important factors to be considered.

Answers to Written Labs

1. Bus, ring, and star
2. Mesh
3. Server
4. Client/server
5. Point-to-point
6. Hub
7. Virtual private network
8. Virtual LAN
9. A segment
10. Bus