CHAPTER

14

NETWORKING FUNDAMENTALS

SCOTT M. ROGALA

The world of networking and the world of picture archiving and communications systems (PACS) are two different environments that converge in such a way as to require a very special skill set. This chapter gives you the basics of computer networking and shows you how they apply to a PACS environment.

It is important to appreciate the role the network plays in a PACS implementation. Our goal is not to make you an expert network engineer, but rather to give you enough information so you can navigate the often confusing, cluttered world of computer networking. With the right kind of information you will feel comfortable enough with the terminology to understand what your vendor(s) are providing, on both the PACS and network sides. We also want to impress on you the importance of good network design and implementation; these are integral parts of the PACS system. Failure to create a strong, robust network infrastructure will result in unhappy users, finger-pointing, and loss of confidence in PACS. If the network is designed and implemented correctly, it can contribute immensely to a successful PACS implementation.

We will start with some basic concepts, intended not for the veteran network engineer but for those who have had no exposure to computer networking. Through extensive use of analogies, most of you will grasp the concepts well enough to see how much thought is needed in the design of networks, and why the necessary investment of time and capital must be made to achieve a successful implementation. We hope that by explaining in familiar terms what is considered wizardry and hocus-pocus will help bridge the gap between network engineers and radiologists.

FOR REFERENCE: THE INTERNATIONAL ORGANIZATION FOR STANDARDIZATION MODEL

The International Organization for Standardization (ISO) model (see Figures 14.1 and 14.2) was set down by the ISO as a framework to make it easier to construct computer networks from the application (as one views an image) all the way down to the physical layer (i.e., the wires). It defined how networks should interoperate. Note that the ISO model serves only as a guideline, and no network, to our knowledge, is set up exactly to the ISO definition.

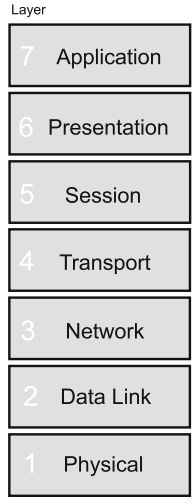


FIGURE 14.1

The ISO model.

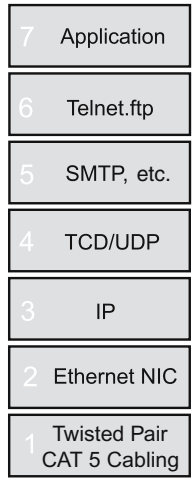


FIGURE 14.2

The ISO model with Ethernet and TCIP/IP.

A SIMPLE NETWORK

Let us start by setting up a very simple network of 2 computers, a server and a client, to illustrate many of the concepts.

In our example, the server machine is an image archive in a small PACS system, and the client machine represents a primary interpretation workstation. For the PACS to work, these 2 computers exchange data with each other, for instance, radiology images. This simple network would look something like Figure 14.3.

What are the components of this architecture? First we will work from the top down, and then we will explain in more detail from the bottom up.

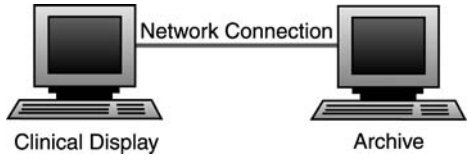


FIGURE 14.3

Two computers connected.

THE ARCHITECTURE AND COMPONENTS AND THE INTERNATIONAL ORGANIZATION FOR STANDARDIZATION MODEL

The archive machine hosts the images the clinical display needs. An application on the archive knows how to answer image requests from clinical displays. In the ISO model this portion of communication happens at the higher levels. The application needs to transfer this information from itself to the clinical display requesting the information. The overall picture would look something like Figure 14.4. Figure 14.4 is an extremely simplified way of looking at the ISO model. It is displayed in this way to emphasize the fundamental components that we will need to understand to effectively make PACS networking decisions.

Each layer is interested only in the exchange of information between the layer directly above and that directly below. (For example, the hardware layer generally does not care how the protocol layers pass information to the application: it is concerned only with passing the information up to the protocol layer.) In this way the application communicates with the protocol stack, which in turn hands the information over to the hardware layer (the network interface card, or NIC). Next, the hardware layer puts the information out onto the network.

Each layer has a different and well-defined task. The application layer knows the data it wants to transmit, and it knows which machine it wants to transmit it to. The protocol stack knows how to find the computer in question (or how to find a device that knows how to locate it). The network layer knows how to transmit the data over the network, and the network knows

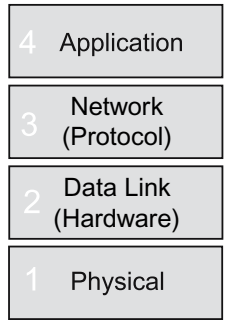


FIGURE 14.4

A simplified ISO model.

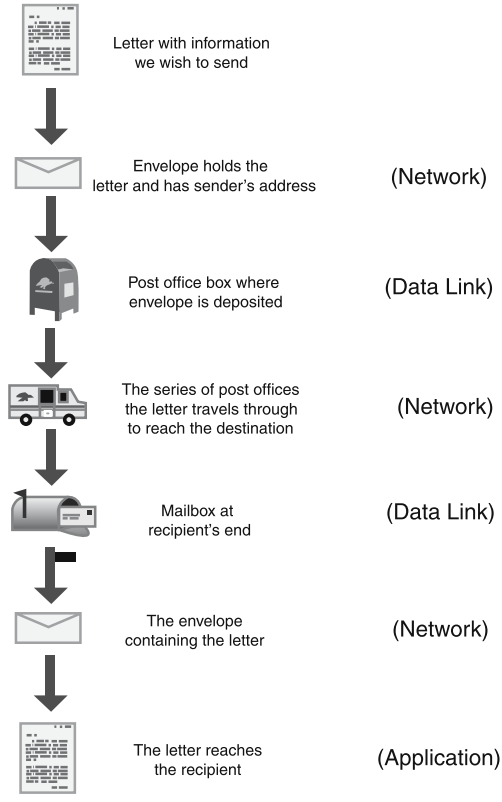


FIGURE 14.5

Postal system analogy.

how to transmit the data to its destination. On the other end, the information works its way back up until it ultimately reaches the application and the image is viewable.

In many ways, this is analogous to the way the U.S. postal system works. In our scenario it would look something like Figure 14.5.

In this example it is easy to see how each layer is independent of the others. It is not important to the envelope what information is contained in it, only that the information fits. The same goes for the post office box, which does not care what size envelope or even small box is put in it, only that it is not a koala or something else that does not belong in post office boxes. Moreover, the post office box could not care less about the contents of the envelope. As we will see later, the post office system uses the address on the envelope to move the envelope throughout the postal system.

Now we will work our way back up through the layers, starting with the physical layer. The physical layer consists of the wires that make up the network. It may also include the NIC in the computers attached to it. In general, the physical layer can be thought of as the "plumbing" or highway of a network. The quality and width of the pipe can determine the speed at which the data can be transmitted, the reliability of the network, and the distance at which the data can be transmitted.

Most of you have probably seen the cable coming out of the wall plate and connecting to your computer's NIC. These cables are commonly known as unshielded twisted pair (UTP) copper cabling, also referred to as Category 5 (CAT5) or Category 3 (CAT3), depending on the exact quality. Networks can also be made up of telephone wires, coax cable (otherwise known as thinnet or 10Base5), and other types of wires. One advance that has changed networks dramatically in recent years has been the use of fiber-optic cabling, which can transmit more data over longer distances than conventional cabling by using light or lasers instead of electrical signals. The relatively high cost of fiber cabling has relegated it generally to the core of networks where bandwidth is needed most. Of late, fiber cabling has become the only type of cabling that can support faster transmission rates, and it is finding its way to the desktop as it becomes more popular and less expensive. Later in this chapter, we will discuss which types of cabling are generally used where.

Let us return to our example in Figure 14.3. Our hypothetical network will use CAT5 cabling between the 2 workstations for now. The workstations could be directly connected or, using a device discussed earlier, we could use a hub, to which both devices can be connected, as shown in Figure 14.6. Just like the hub of a wheel, a hub in networking terms is a device

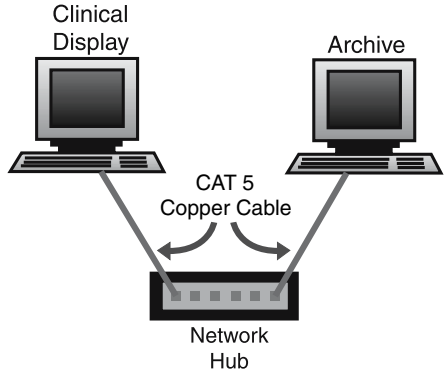


FIGURE 14.6

Two computers connected with a hub.

connecting multiple computers. Hubs can have from as few as 4 to as many as 24 or 48 connections for computers.

One layer higher, the hardware (data link) layer consists of the NIC, as well as the software drivers installed on the computer that allow the computer to communicate with the hardware. The most common types of cards are Ethernet cards, which are designed to communicate on Ethernet networks. There are also ATM cards (asynchronous transfer mode, discussed later), token ring cards, and a variety of others. As with all the other layers, direct communication occurs between cards of the same type (i.e., Ethernet to Ethernet, or ATM to ATM). As we get into more complicated network topologies, we will see that networks can become very diverse, consisting of computers with Ethernet cards, ATM cards, and token ring cards, all communicating via the use of various internetworking devices.

For now, to keep it simple, let us say that both computers have Ethernet cards in them. Both computers also have the appropriate software drivers installed.

As we continue to move up our simplified ISO model, we need to discuss protocols. Loosely defined, protocols are a set of predetermined rules that 2 or more parties follow in communication or other interactions. In computer networks, protocols are the set of rules, or languages, that enable computers to communicate over the underlying network infrastructure. Protocols and how they are used are very much akin to languages in the real world: just as humans speak languages such as English, French, and Swahili, networks use languages such as TCP/IP, IPX, and Appletalk. For 2 computers to communicate, they must be speaking the same language. In our scenario we will say that our 2 computers are speaking TCP/IP with each other, thus using a common language to communicate over an Ethernet network on CAT5 cabling.

Last but not least is the application that uses this language to communicate. In this example, that application is PACS.

COMMUNICATION AND CONVERSATIONS

It is time to delve more deeply into exactly how conversations occur. Once we establish that 2 computers want to exchange data, they must use their shared set of rules (protocols) to do so. Further, these protocols need to communicate over a network. So far we have talked about Ethernet, ATM, and token ring. These are sometimes called network topologies, and they all occur at the data link layer. Certain rules must be followed on these topologies for them to work correctly. We have also identified a few of the more common protocols (or languages), such as TCP/IP and IPX. These

computer communication languages operate at the network layer. Any protocol that is routable is using layer 3, the network layer, to make decisions. Protocols that are not routable are called bridged protocols and are aware of only the data link layer. We discuss this further when we discuss routing and bridging.

To better explain the relationship between a topology, such as Ethernet, and a protocol, such as TCP/IP, we again use the analogy of human communication. When we communicate, we can do so via a wide variety of media: the air (speech), paper (the written word), or hands (sign language). What language we use is completely independent of the medium we use. Similarly, computers can communicate via TCP/IP or IPX and do so over Ethernet or copper wire or token ring or fiber-optic cabling. (Later we discuss devices that do the functional equivalent of taking written English and verbalizing it, or vice versa. You are much less likely to find a network device that does the functional equivalent of translating from English to French, however; such devices are commonly referred to as gateways.)

Since protocols are much like languages, it is useful to use the conversation model to explain how computers communicate. The primary obstacle in using this analogy is that communication for us is second nature; we talk and write without being aware that we are in fact following a set of rules. In the world of computers, where only logic exists and everything is taken literally, conversations are actually very complicated to carry out.

As an example, in human behavior, there are protocols for starting a conversation, such as saying "Hello, how are you?" and responding "Good, and yourself?" These sorts of things occur naturally (assuming everyone is civil!). Similarly, ending a conversation has sets of rules concerning goodbyes, and so on. Even during the conversation, it is important not to interrupt the person speaking, and to acknowledge what the person is saying with a nod. If you do not understand what the person is saying, you ask the person to repeat himself or herself. Very similar things happen on computer networks, as we will explain.

AN EXAMPLE OF A CLASSIC COMPUTER NETWORK—SHARED ETHERNET

To get a better understanding of how computers handle this, let us look at a conversation between our archive computer (server) and our clinical display (client) and postulate how they might communicate. The client knows it wants certain information from the server. Its request makes its way down through the protocol stack using a language that it knows the archive

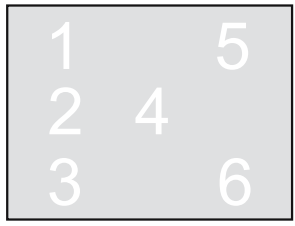
understands. This message makes its way out onto the wire, heading for the destination machine. The destination, in this case the archive, is listening for anybody looking to talk to it, and sees the packet (piece of data) on the network. The 2 machines begin with their "Hello, how are you?" routine and agree to communicate with certain rules.

They agree, for instance, on how much data the 2 will transmit at any given time, what to call their conversation, and a great number of other things. All the while, since there is a single shared network between the 2 devices, only 1 of the 2 computers can be speaking at any given time. If the client and archive attempt to send information at the same time, both of their transmissions are lost, and they need to start their sentences over. When such a situation arises, it is termed a "collision," because the electrical signals effectively collide with one another on the network of shared cabling. In these instances, algorithms in the program determine when it is safe to start trying to repeat the message while decreasing the likelihood of another collision.

When only 2 computers are in the equation, the likelihood of a collision is smaller than you might imagine. However, as more and more computers compete for the same network, the likelihood of 2 or more computers trying to transmit at once increases greatly. At some point, when you are building networks with hundreds of computers on them or networks in which computers are constantly trying to communicate, collisions become the norm rather than the exception, and the network cannot bear the burden of all those sentences in the conversation. The sentences, in network terms, are called packets.

What we are describing is called shared Ethernet, in which all the computers share the same network. Even today it is probably the most popular type of network in the world, although newer technologies are becoming more prevalent. Only 1 computer can be transmitting its electrical impulses onto the network at any given time. We like to use the example of a conference room to make the idea of a shared medium a little easier to understand (see Figure 14.7).

Let us say that our conference room holds 200 people. First, we set up a simple rule: anybody can talk to anybody else, but only 1 person in the entire room can be talking at a time. If somebody tries to talk while somebody else is in midsentence, they both have to stop and start their sentences again. One can see very quickly how, in a room full of people operating under these rules, very little is going to get said, especially if a lot of conversations are in progress. In this example, the conference room is analogous to a network segment, the air is the medium (Ethernet), the people are the computers, and the information they are trying to transmit could be PACS



layer

4 PACS, Baseball
3 English or TCP/IP
2 The People
1 The Air the Sound Travels Over

FIGURE 14.7

The conference room.

knowledge, baseball news, or the latest juicy gossip. Some could be speaking English or French, but only those who understand French are able to communicate with others who understand French. Similarly, on our network, computers could be talking TCP/IP to one another while others are speaking IPX. They all share the same network segment, but they communicate only with those speaking the same language.

ENTER BRIDGING

You can see in this scenario how inefficient such communications can be. The same was true for early networks. The first attempt to tackle the problem of collision was with a concept called bridging. A bridge is a device that connects 2 or more networks together. (As we see later, a bridge understands only the 2 lower layers of our simplified ISO model. Next we talk about a device that understands the lower 3 layers, a router.)

To explain exactly what a bridge does, let us take the conference room and split it in two. We assign each person a unique number, known as his or her MAC address, or media access control address. The MAC address is unique not only in the conference room, but also throughout the world. In computing, the MAC address is derived from the network interface card. It is how each computer (or in our example, each person) is identified.

In Figure 14.8 you see that the conference room is split in two, with people numbered 1, 2, and 3 on the left side and 4, 5, and 6 on the right side. In the middle of the conference room is a dividing wall, which stops all noise unless the bridge, B, allows it through. It is the bridge's job to keep

track of who is where, and to bridge the traffic through the dividing wall as necessary.

For the bridge to do its job effectively, it listens to all network traffic. It does this by listening for broadcasts. In a network, a broadcast is a method a computer uses to locate another computer when it does not know exactly where to find that computer. It is almost like yelling out, "Joe, where are you?" In the case of a simple shared network segment, the client looking for the archive for the first time sends out a broadcast requesting the MAC address of the archive. The archive answers this request, and the conversation between these 2 computers ensues. In the case of our conference room without the dividing wall, these broadcasts are just like any other packet—they can cause a collision.

A bridge sits between 2 network segments (i.e., in the middle of the conference room) and keeps track of who is on which half. Initially the bridge has no idea who is on which side, so it begins to listen to traffic and build a list. When device 1 makes a request to find device 2, the bridge records that 1 is on its left side and that 2 responded from the left side. This is illustrated in Figure 14.9, and the conference room analogy is carried forward in Figure 14.10.

From this point on, any traffic between 1 and 2 is isolated from the right half, effectively creating 2 different collision domains. Devices 1 and 2 can communicate directly with each other without affecting the right side. Similarly, devices 3 and 4 on the right side can function the same way. When the bridge sees device 4 broadcast to locate device 1, the bridge knows that device 1 is on its left side, and will pass the traffic. In performing this sort of task on what once had been 1 large, congested segment, the bridge can greatly decrease the number of collisions, provided that it is properly located (that is, that proper network design and traffic analysis have been performed). We look more closely at those functions as we design our PACS network.

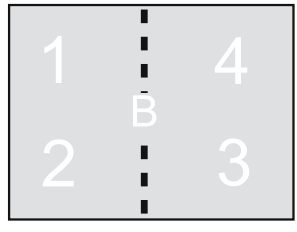


FIGURE 14.8

The conference room split by a bridge.

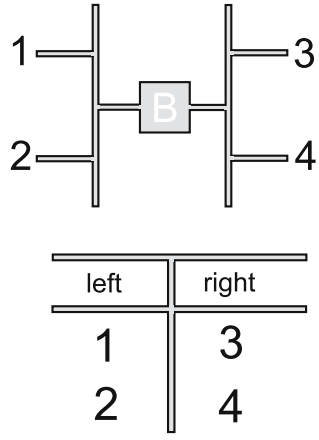


FIGURE 14.9

A segmented network with a bridge and the bridge's table.

ROUTING

Bridging solved some, but not all, of the problems computer networks faced with respect to traffic. Devices still needed to broadcast in order to find their destinations, and in larger networks with many segments bridged together, networks could still collapse under the sheer weight. On networks that comprised hundreds and even thousands of computers, bridging just was not up to the task. Also, although we will not go into detail here, another problem was that bridging did not scale particularly well, meaning that large, complex networks were susceptible to prolonged outages that could be very difficult to troubleshoot.

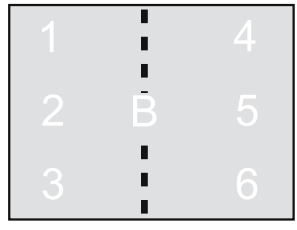


FIGURE 14.10

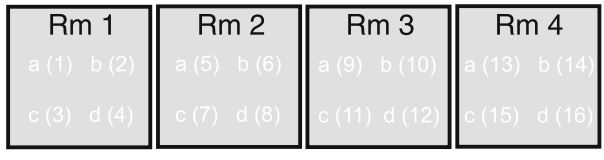
The equivalent conference room.

The challenge facing programmers was to create a more intelligent networking device that could limit broadcasts and more efficiently use the bandwidth. Routing is a technology developed in the mid-1980s to address these problems. Routing made use of protocols that had more intelligence built into them so they could pass traffic more effectively throughout the network. Protocols that came along before routing existed had no concept of layer 3 of the ISO model; they simply made use of the MAC address and used broadcasts to find their destinations. Protocols like that are called bridged protocols, and examples are LAT and Netbeui. When routing was introduced, protocols came along such as TCP/IP and IPX, which sent out information in packets that routers could use to more intelligently handle the traffic. These are commonly referred to as routable protocols. Such protocols could limit broadcasts and make it much easier to find devices on a large network.

Again we will use the conference room example, except this time we will expand our world to include the hallway outside the conference room, and add other conference rooms off this hallway (see Figure 14.11).

In this example, each room has a letter assigned to it: A through D. There are folks in each room and now they can be addressed in two ways. MAC addresses still need to be unique, but the protocol address needs to be unique only within that conference room. Addressing at the routable protocol level would look something like Table 14.1.

The benefit is realized when we have many conference rooms, as in Table 14.1. When device A.a wants to communicate with device D.c, it knows that (1) device D.c is not in the same conference room as itself (otherwise it would have the same room letter) and (2) the hallway knows how to find room D. So device A.a sends its information out into the hallway (the router, sometimes referred to as its "default gateway"), and the router relays the conversation to room D, where device D.c receives the information.



In the user 1. a protocol (network) layer address, the "1" is the data link layer unique address.

FIGURE 14.11

Four conference rooms (A through D) with devices in each.

TABLE 14.1
Conference Rooms and Addresses of Their Devices

Room	Devices' Addresses
A	A.a, A.b, A.c, A.d
B	B.a, B.b, B.c, B.d
C	C.a, C.b, C.c, C.d
D	D.a, D.b, D.c, D.d

Earlier we mentioned that there are devices that can take the spoken word and convert it to written, and the reverse, as well. Both routers and bridges are capable of doing this, and commonly do. For instance, room C could be a room in which all the devices are communicating via the written word, while rooms A, B, and D are communicating via oral speech. The router would know how to verbalize everything coming out of room C and going into the other rooms, and know how to do the reverse for traffic going into room C.

Routing has been tremendously beneficial in large, complicated environments. Although it adds another layer of complexity and requires significantly more engineering to set up, it goes a long way toward simplifying, troubleshooting, and preventing a network from collapsing during heavy traffic. Unfortunately, routing can slow traffic down, because it has to perform some intensive tasks in order to determine exactly where the packet needs to travel. Keeping with our analogy, the time spent using the hallway to get to another conference room slows the conversation. In most cases the slowdown is negligible, but as we discuss in designing PACS networks, it can be detrimental to PACS performance.

A router is slow because it has to examine more of the packet to make routing decisions. Bridges work much more quickly because they have fewer decisions to make. The nature of networks is such that they are never set up as efficiently as possible—the server you need so you get your information inevitably has 2 or 3 routers in the way. In addition, as bandwidth demands increase, segments need to become smaller, which means more routers, which means slower response time to the server. When routing became too slow, another technology was introduced. Enter switching.

SWITCHING

Switching, as simple as it is, revolutionized the networking industry. Many networks were collapsing under the sheer weight of routers, and engineers were unable to break up their segments any more than they already had without creating hopelessly complex architectures. The idea of switching is to step back and look at only as much of the packet as a bridge looks at, the data link layer. This means that a switch is essentially a bridge. To a lot of people this is confusing, so let us look at it this way—a switch is basically a bridge with many, many interfaces, and sometimes each interface has only 1 device connected to it. Switches were developed because it became cost-effective to build bridges with numerous interfaces on them. Switches are essentially bridges that are applied in a different manner than original bridges because they are more powerful. As we begin to look at network design and talk about bandwidth, we will see how the idea of switching (and the fact that it came about as higher-speed networks were being developed), when incorporated with routing, helps make network bottlenecks easier to remove.

Switches are used in a variety of ways. Some switches are used in the core of the network (more on this later), whereas other switches are used to replace hubs. When they replace hubs, they have the same effect as changing the rules in the conference room. Recall our first rule of the conference room: anybody can talk to anybody else, but only 1 person in the room can be talking at a time. If more than 1 person speaks we have a collision. To help alleviate the problem, we first installed a bridge in the conference room; then we added conference rooms with a hallway as the router. But that scheme can be applied only so far. At some point we cannot take everybody out of the conference room, and 50 chatty people are going to have some serious collision problems. It does not seem productive to install 25 bridges in the conference room. But when switching came along, it greatly simplified the situation by doing just that. In effect, switching looked at the rules we established concerning talking and changed 1 rule in the conference room—that which was the most inefficient. Switching allows us to say that anybody can talk to anybody else, as long as each person is talking to only 1 other person. Sometimes when a switch is used to separate everybody from everybody else in the conference room, it is referred to as a switching hub.

But what happens when the users in the conference room do not want to talk to each other, but instead want to talk to somebody in another room, that is, through the router? Then we need to talk about bandwidth.

BANDWIDTH

Bandwidth, simply stated, is the rate at which information can be transmitted in a specific time interval, usually seconds. In computer networks, the rate at which data can be transmitted is measured in bits per second. A bit, or binary digit, is either a 0 or a 1. A bit can be considered the atom of the computer world. Eight bits are called a byte. The reason 8 bits are significant is that eight 1s in binary form (11111111) are equivalent to 255 in decimal form, which is enough to represent all variations in the English alphabet of upper- and lower-case letters, numbers, and other characters.

One million bytes are commonly referred to as 1 megabyte, or 1 MB. This is how most computer users understand file sizes, hard drive sizes, and the like. In the data networking world, however, transmission rates are measured in megabits, not megabytes. One megabit is denoted as 1 Mb to distinguish it from a megabyte. In this way, data transmission rates can be deceiving because a network that can transmit data at 10 Mb per second is really transmitting 1.25 MB per second (one eighth the speed). Why megabytes are used when referring to file sizes and megabits are used when referring to data transfer rates is a mystery. It could have been a marketing ploy by network vendors to make their networks sound faster than they really are.

To most people, megabits mean very little. It is like telling people your car has 282 horsepower when they have not experienced 150, 250, or 300 horsepower. To put megabits into perspective, let us use the example shown in Table 14.2.

Many different types of common networks are available. Along with the shared Ethernet mentioned in our example network, others are listed in Table 14.3 in relative order of performance (though bear in mind that certain

TABLE 14.2
Putting Megabits into Perspective

The typical individual reads at approximately 600 bits/second.
The image transmitted to your television screen represents about 3,000,000 bits/second.
Most modems connect to the Internet at 56,000 bits/second.
The most common type of network in existence today is shared Ethernet, which operates at 10,000,000 bits/second.

TABLE 14.3
Different Types of Networks Available and Their Speeds

4 Mb/s token ring
10 Mb/s Ethernet
16 Mb/s token ring
100 Mb/s Ethernet (also known as Fast Ethernet)
155 Mb/s ATM (also known as OC3)
622 Mb/s ATM (also known as OC12)
1000 Mb/s Ethernet (also known as Gigabit Ethernet)
2488 Mb/s ATM (also known as OC48)

traffic conditions may alter the order somewhat, meaning that mileage may vary).

As data transmission rates increase, so does the quality of the cabling required to support those rates. For instance, there is no standard to transmit anything faster than 100 Mb/s Ethernet on copper cabling. All speeds higher than 100 Mb/s require some type of fiber-optic cabling. The industry continues to work on the standard for Gigabit Ethernet that will support copper, but the distance will likely be very short (25 m).

Note that all network transmission rates are theoretical speeds. To say that 10 Mb/s Ethernet can transmit a 1.25 MB file in 1 second would be fallacious. It is important to make the distinction between theoretical and actual bandwidth and understand why the difference (sometimes called overhead) exists.

Many factors contribute to the difference. To understand overhead, consider how, in shared Ethernet, there is the possibility of a collision. This is one form of overhead. Anytime there is a collision, the data that is being transmitted is discarded and must be retransmitted. In a shared Ethernet segment, this affects the actual bandwidth. Other network types, such as token ring, ATM, and to a lesser extent switched Ethernet, do not share the problems of collisions, but all network types must deal with some form of overhead that prevents them from reaching their theoretical bandwidth.

To understand some of the other factors, we need to examine conversations again, and realize just how little of the conversation in a data network

has to do with the actual data being transmitted. Each half of spoken dialogue is made of sentences. In a network, each of these sentences is called a packet. Packets are the elements composed of bits that carry data between the 2 computers on the network.

Let us look at the example of the letter and the envelope to see how a packet is formed.

In Figure 14.12, the letter represents the data that needs to be sent to the recipient. Realize that this letter is only a small part of what is actually getting sent through the postal system. The letter requires the envelope, the recipient's address, and the return address. All of this contributes to overhead. In some cases, the actual data could comprise as little as 33% of the packet. On top of that, each packet must be checked to make sure it made it to its destination without any errors (from electrical interference, for instance, which may cause a 0 to be interpreted as a 1 or vice versa). There is overhead in doing the checking, as well. As you might imagine, all of this extra information can quickly contribute to overhead on a network, gobbling up bandwidth you thought you had all to yourself. In some protocols, packets also have to be acknowledged by the receiver, or else the sender resends the packet. Imagine the overhead involved in sending a message that simply says, "Yes, I got your letter." There is very little data in that packet compared to the actual bandwidth it consumes.

(Bear in mind that the packet in Figure 14.13 is an example of a packet, and not to be taken too literally. Each packet is actually made up of other information, depending on the exact protocol and data link layer for which it is designed. Our example packet has been simplified dramatically.)

All of this goes a long way toward dragging the actual bandwidth of a network down. Most engineers agree that between collisions and overhead,

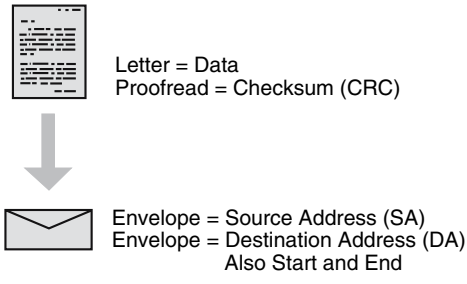


FIGURE 14.12

A letter and envelope with address are like a packet.

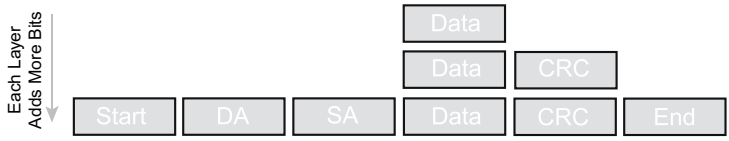


FIGURE 14.13

A simplified packet.

actual bandwidth on a shared Ethernet segment is somewhere between 3 and 4 Mb/s. Any time you try to transmit more than that you will experience the law of diminishing returns in which collisions become the norm rather than the exception, and very little gets transmitted. The same holds true for 100 Mb/s shared Ethernet, which typically maximizes at somewhere between 30 and 40 Mb/s. Switching can go a long way toward bringing the theoretical and actual closer together by eliminating collisions on a segment. For example, on 100 Mb Ethernet segments (known as Fast Ethernet) that have implemented switching, the maximum bandwidths are closer to 75%, or 75 Mb/s. For reasons we discuss later, ATM has different theoretical figures based on a variety of assumptions and other factors.

FACTORS TO CONSIDER IN BUILDING A NETWORK

Up to this point we have discussed all the various working parts of a network. We have discussed hubs, routers, bridges, and switches. We have examined different types of cabling used in building networks, and we have discussed how data actually is transmitted between computers. Given the vast array of protocols, hardware, and topologies at our disposal, how is one supposed to determine exactly how to go about building a network? Our original example network is quite simple: 2 computers, a server and a client connected to a hub using CAT5 cabling to transmit image information. Depending on how important it is to get the information from the archive to the client, we could upgrade them to a faster network speed, such as 100 Mb/s Ethernet. What happens as we start to add workstations? (See Figure 14.14.)

If all the devices are connected to the same hub, they share the same collision domain. Because all the devices are relatively close together (within 300 ft), we continue to use CAT5 cabling. Each device is configured to communicate on the network at 10 Mb/s. In this scenario, each of the clinical

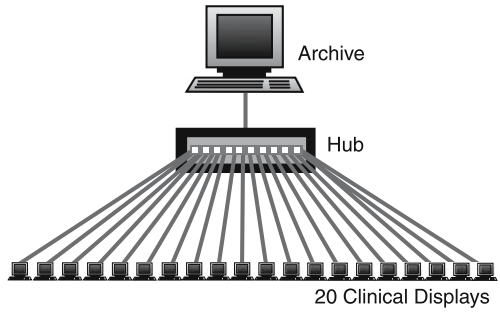


FIGURE 14.14

Adding workstations to our network.

displays is attempting to access information on the archive computer. The clinical display can theoretically access the information at 10 Mb/s, and the fastest the archive can respond with information collectively is 10 Mb/s. Even if we were to implement a switched architecture here, that would only make the situation worse, as the clinical displays currently do not have to compete with one another to send out their packets. They have to compete only for the archive's 10 Mb/s of bandwidth. Here we can see a bottleneck.

Another way to look at bottlenecks is to look at the example of a human conversation. Let us say that with speaking and listening you can process 200 words per minute in a dialogue hypothetically. This means that you can listen at the rate of 200 words per minute or you can speak at the rate of 200 words per minute. Any more than that and you might become confused and request that the other person slow down in speaking, or you have to slow yourself down in speaking. For argument's sake, let us say you are pretty good at multitasking and can actually be having 2 conversations at once; you can be discussing PACS networking with 1 individual and the Red Sox with another. Nevertheless, you can discuss these 2 subjects collectively at a total of 200 words per minute. If 2 more people try to talk to you, those 200 words need to be divided among all 4 parties. At some point you become the bottleneck, as each of the other 4 parties is capable of handling 200 words per minute but you are able to give each party only 50 words apiece. Either they have to get their information from another source, or you have got to find a way to speak and listen more rapidly. Similarly, we will see how we can intelligently upgrade our network in the proper places to get the most for our investment. In our example, we could upgrade the server to "speak" at

100 Mb/s Ethernet, while keeping the clinical displays at 10 Mb/s Ethernet. Upgrading all the clinical displays to 100 Mb/s Ethernet while the archive processes at 100 Mb/s will accomplish little except in an environment where only 1 or 2 clinical displays are requesting information at once, in which case optimum transmission rates can still be realized. If multiple workstations are operating at 100 Mb/s and requesting data from the archive, the archive could again become the bottleneck, at which time we could upgrade it to Gigabit Ethernet or ATM of one type or another.

It is clear there are multiple ways to handle this arms race. In the next example, we begin to integrate the various devices and architectures into a coherent PACS solution.

A REAL-WORLD EXAMPLE

It would be helpful to use a real-world example of how our institutions used to use switching and routing together to increase productivity for several thousand users on a network experiencing high utilization, collisions, and very poor performance. In one case, 1200 users in a particular building were using one 10 Mb/s Ethernet segment sharing the same collision and broadcast domain; that is to say, they were all in the same conference room. Each computer in the room was a client, all accessing servers off their network segment (outside the conference room). Simply installing a bridge would have accomplished little in this case, because all the traffic was attempting to use the same 10 Mb/s router interface. We could not take half the users and put them on a different routed segment, because that would have meant readdressing 600 computers by hand to tell them they were on a different network segment (in a different room). We needed to somehow keep all the users on the same segment, while decreasing the number of collisions. Installing a switch for all these users would help some, as they would still be competing for the same 10 Mb/s interface on the router. We needed to do a combination that allowed faster access out of the conference room (the router interface) and used switching within the room so all 10 Mb/s users would suffer from fewer collisions. New equipment enabled us to install a switch and give the router a 100 Mb/s interface into the room, while allowing all users to communicate on the network at 10 Mb/s in a switched architecture. In doing so, we dramatically decreased the number of collisions and circumvented the bottleneck that would have resulted from upgrading to 100 Mb/s the router's interface onto the segment (see Figures 14.15 and 14.16).

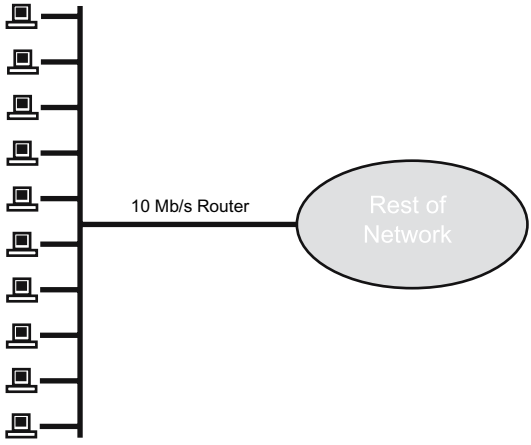


FIGURE 14.15

Network before upgrade.

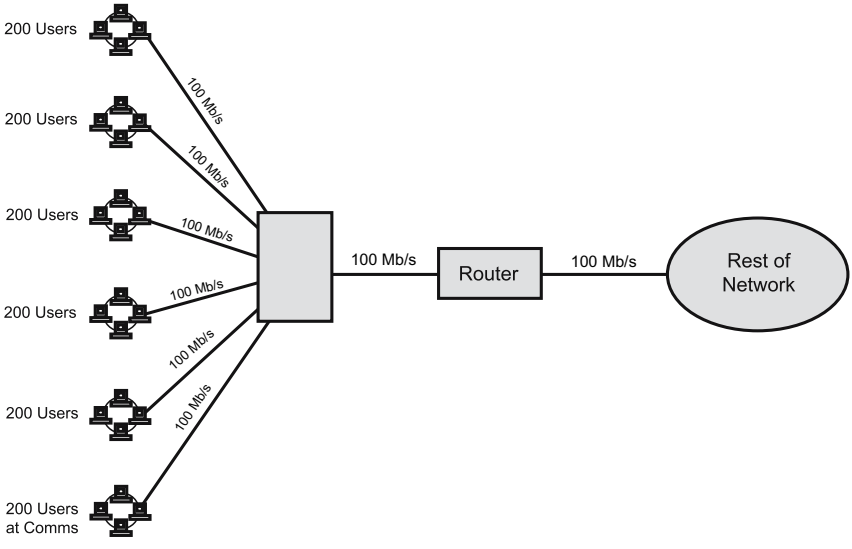


FIGURE 14.16

Network after upgrade.

PACS NETWORKS

As you probably see by now, networks can be incredibly diverse. There are a number of factors to take into consideration when building a network, and we have many tools available to us in the form of routers, switches, Ethernet, ATM, and copper and fiber cabling. How effectively we put this together depends on the amount of knowledge we have of the tools available to us, as well as an intimate understanding of exactly how traffic on the network flows. We also need to take cost into consideration. Among the many important factors, 4 stand out (Table 14.4).

The decision-making process is similar to that used for choosing a car. Potentially, one could purchase a high-performance car for a midrange price, but in the long run there may be reliability issues with it, and maintenance may be expensive. On the other hand, a more reliable car might cost the same amount but lack the performance we might require on the highway. Getting both reliability and performance costs more money.

PACS networks are different from most networks. Typical networks are intended to transmit e-mail, share small files, share printers, and handle other processes. If it takes 2 minutes or 3 minutes to transmit an e-mail, does it really matter? If it takes 10 seconds to open that Word document rather than 8, who is going to notice? On the other hand, PACS networks are transmitting large amounts of data, and that data needs to get where it is going quickly and reliably. PACS networks require both performance, because of the sheer amount of data being transmitted, and reliability, because of the data's clinical nature. The reason PACS is becoming so popular is that only recently have fast, reliable technologies become available to make PACS implementations practical and cost-effective. In the following examples, you will see networks on 3 different scales and learn the rationale behind their design.

TABLE 14.4
Four Important Factors in Building a Network

Performance—How quickly the network can transmit data.
Reliability—How reliable the network is. How easy is it to maintain?
Upgradability—How easy is it to upgrade?
Price—How much does the network cost?

ASYNCHRONOUS TRANSFER MODE

First let us look at few technologies that we will use in building this network. One such technology is ATM, or asynchronous transfer mode. We will explain the differences between ATM and Ethernet by explaining how they were derived.

Ethernet, in its purest form, is a "dumb" medium. It does not know what traffic is passing over it, nor does it need to. It operates under simple rules and principles that govern how traffic will be transported. Your e-mail about the Red Sox has no higher or lower priority than a PACS image or a telephone call. In this sense, Ethernet is said to have no concept of quality of service, or QoS.

ATM, on the other hand, was designed with the intent of allowing the network administrator to classify different types of traffic with different priorities. In this sense, an ATM network offers different levels of QoS depending on the application or workstation.

ATM is able to do this so well in large part because it is a much more predictive architecture. In an Ethernet network, packets can vary in size, reaching a maximum of 1500 bytes. However, some packets can be 300 bytes, some 50 bytes, and some 1500 bytes. Thus, it is very difficult for an Ethernet network to be able to predict traffic patterns. On the other hand, ATM packets are called "cells" and are always 53 bytes in length. Because of the constant size of the cells, ATM is predictive: a packet of streaming video will not get "stuck" behind a 1500-byte e-mail packet in a router while it tries to reach its destination.

ATM is often compared to a telephone network because of the high predictability it ensures. ATM networks can be built so that voice cells will have a high priority and always get through. ATM does this in much the same way the telephone system does. When you pick up the telephone and attempt to make a call, the ATM or telephone network checks to see whether it can complete the call with the parameters you require. In the case of ATM and computer networks, you may request a certain amount of bandwidth. If the ATM network cannot guarantee that amount of bandwidth, the computer and the network can negotiate a lower bandwidth rate, or not start the conversation at all. This is very much like a telephone call, especially a cell phone call, where you occasionally get a "fast busy" because the voice network cannot guarantee enough bandwidth to complete the call.

That said, ATM has had a long, troubled journey toward universal acceptance. It has taken years from its inception to make it to a finished product. Along the way various vendors have released products based

only loosely on not-yet-agreed-upon standards that make vendor interoperability very unlikely. Because of this, when you choose an ATM vendor, understand the high probability of the product's not working with other ATM hardware.

Another consideration in choosing to use ATM in networks is the work a router or switch needs to perform in converting packets into cells and back. This conversion contributes a certain overhead, which is often viewed as detrimental. Strong consideration should be made when mixing ATM with other network types, such as Ethernet. However, those considerations go beyond the scope of this book.

There are other downsides to ATM. The number of ATM installations in most LAN environments is rather small when compared to those of Ethernet. Hence, it can be harder to find engineers who have expertise in the area. What is more, the price per port of ATM is significantly higher than that of Ethernet. Add to this the fact that Gigabit Ethernet is beginning to gain steam and provide high bandwidth at a lower price, so an investment in ATM may not be a good one.

WIDE AREA NETWORKING

All the technologies that we have talked about so far (ATM, Ethernet, token ring) have been designed for local campus settings; that is, for connections on which we can run either fiber or copper cabling. When we leave the campus setting, however, we no longer have the luxury of being able to run our own cable. Whether trying to go across the street, across town, or across the world, we need an external provider to connect sites. Telephone companies (also known as Regional Bell Operating Companies, or RBOCs), such as Bell Atlantic or AT&T, have massive networks designed for handling telephone calls all over the world. They can use these networks to provide data transmission as well.

RBOCs lease "circuits" to companies over which to transmit data. These circuits are generally point-to-point connections between 2 sites. Generally speaking, the circuits they provide offer bandwidth from 56 kilobits (Kb)/s all the way up to 155 Mb/s. Unfortunately, charges are recurring (usually monthly), and the price per megabit is much higher than on the local area network (LAN) for a connection of the same speed. For instance, a standard type of circuit, a T1, operates at 1.554 Mb/s, and can cost several hundred dollars per month. The farther the circuit extends, the more the RBOC charges. Several factors in the industry have kept these costs fairly stable for many years, but technologies to get around these charges are

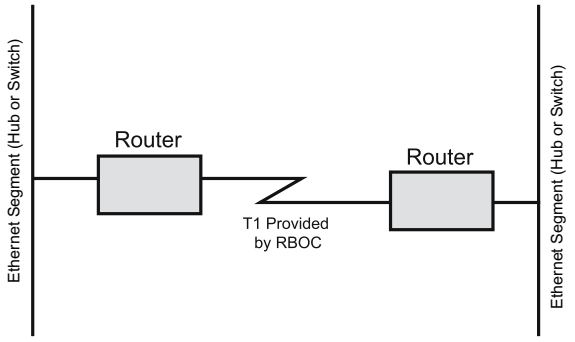


FIGURE 14.17

Illustration of how leased circuits from RBOCs can be integrated into LANs to allow connectivity between 2 LANs.

becoming more popular, and competition is starting to drive down prices (see Figure 14.17). We discuss some of these technologies and the competition factors later in this chapter.

A SIMPLE PACS NETWORK

Figure 14.18 shows a relatively simple PACS network. As you can see, there are 2 modalities, 3 clinical and diagnostic displays, and an archive server. All

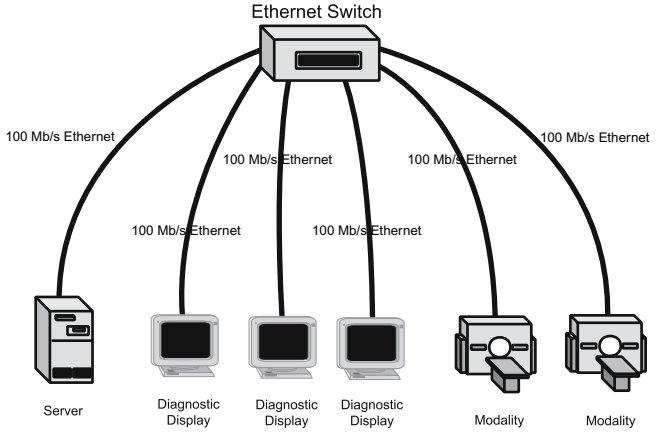


FIGURE 14.18

A simple PACS network.

these devices are connected to a central Ethernet switch, probably using CAT5 cabling. This network assumes that all devices connecting to the central switch are within cable specifications for connecting at speeds of 100 Mb/s.

In this diagram the archive server is connected at 100 Mb/s, as are the diagnostic and clinical displays. The modalities are connected at 100 Mb/s. As most traffic is being sent to the archive server and retrieved from the archive server, we see our first potential bottleneck, but in a network of this size, it is very unlikely that the 100 Mb/s connection will be swamped. In some cases, a 1000 Mb/s (Gigabit Ethernet) connection could be substituted for the 100 Mb/s connection to the server, but the likelihood that it would enhance performance is minimal.

MAKING LIFE MORE COMPLICATED

Now we will complicate our PACS network somewhat. First, we will add some modalities and displays. Let us say that these additions are located at the other end of the building and thus the distance exceeds our maximum cable requirements. We will need to connect them to a second Ethernet switch, and then connect the Ethernet switches together, probably with fiber-optic cabling because the 2 switches are 750 feet apart.

Adding this additional closet (switch) causes us to look at our network in a whole new light. Now we have to consider how much bandwidth we need between the 2 closets (1, in Figure 14.19). This second switch has 3 modalities and 3 display stations and could conceivably saturate 330 Mb/s of bandwidth if all are transmitting at the same time. This is very unlikely, and Fast Ethernet is likely to be enough bandwidth for quite some time.

Still, just as in the simple PACS network, all the traffic is going to the archive. So it is even more conceivable that the connection between the archive and the switch will be the most likely bottleneck. Given the technologies available these days, both links (2 and 3 in Figure 14.19) could be 155 Mb/s ATM, although that is not much of an improvement over 100 Mb/s Ethernet. We also need to consider the cell conversion if the rest of the devices are still Ethernet and if we want to add ATM to an all-Ethernet environment. Another option is 622 Mb/s (OC-12) ATM, which offers significantly better performance than 155 Mb/s ATM. Gigabit Ethernet is yet another option, and would probably come in at the same price point or better than 622 Mb/s ATM. These options offer a perfect example of how you must work with your PACS vendor and network vendor to determine which connection type best fits your situation.

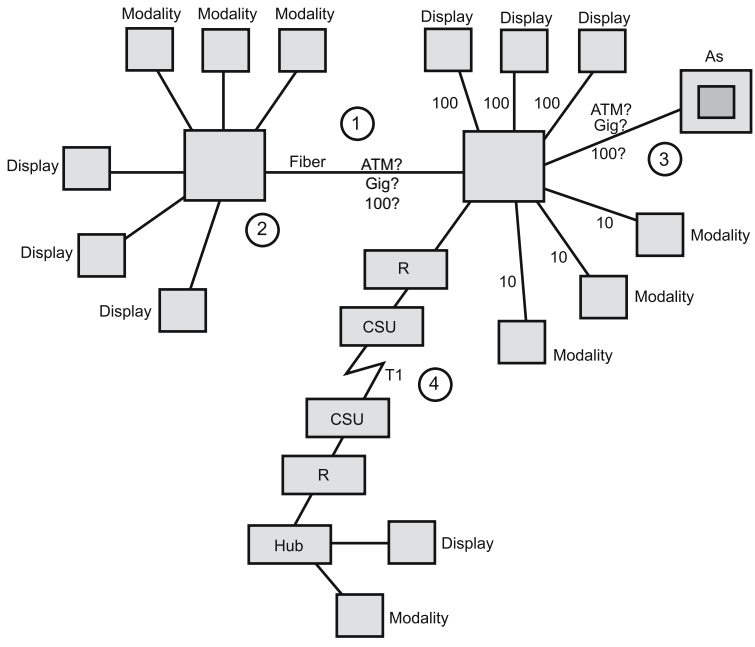


FIGURE 14.19

A more complicated network.

In our network example let us say we decide to add a remote site across town. We have routers on each end (1 at our local site and 1 at the remote site). Our RBOC is providing a T1 (1.554 Mb/s), a relatively slow connection speed for PACS. With the modality at the remote site, images could still be stored on the archive at a reasonable rate, meaning that compressed images could be read at the remote site. If we need to view uncompressed images in a more timely manner we probably need a faster connection type, perhaps multiple T1s or a T3 (which an RBOC offers at 45 Mb/s) (Table 14.5).

COMPLEX PACS NETWORK

Our complex network incorporates a very large number of devices. Including what is shown in Figure 14.20, 50 or so modalities could be spread around our hypothetical hospital, as well as 50 or more displays for reading the images. We will need a fast, robust network to address bandwidth and reliability concerns. Although the scale has changed dramatically, many of

TABLE 14.5
RBOC Circuit Types and Bandwidth

Circuit Type	Speed
Fractional T1	56 Kb/s–1.554 Mb/s
T1	1.554 Mb/s
T3/DS 3	45Mb/s
OC3	155 Mb/s
OC12	622Mb/s

the same technologies are at our disposal. It is a question of how we use them.

We have chosen what is commonly referred to as a "star topology" for this network. In this architecture each switch B in Figure 14.20 connects via

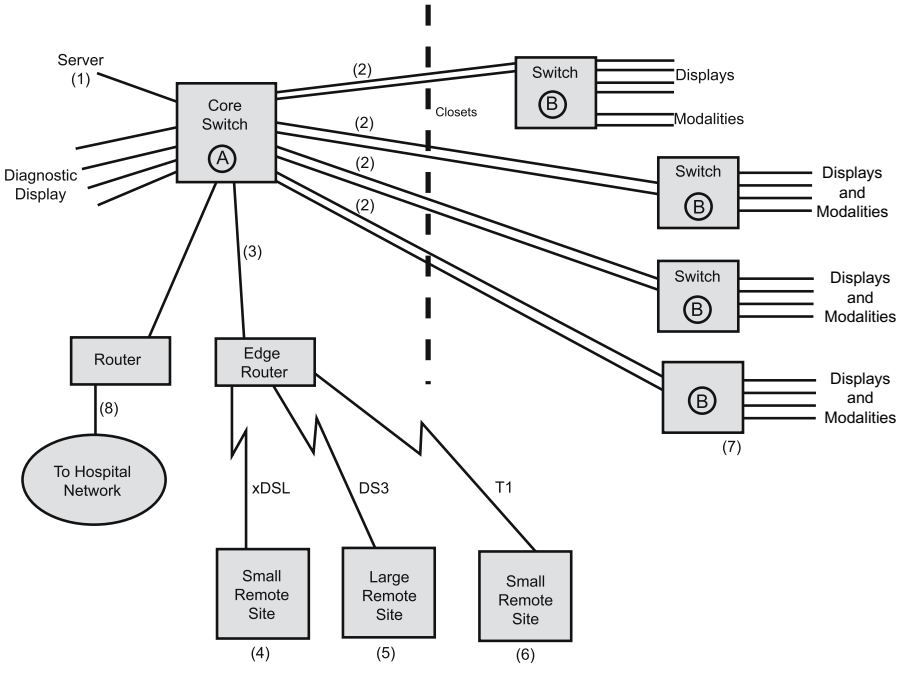


FIGURE 14.20
Complex PACS network.

fiber to the core switch A in Figure 14.20. Modalities and displays can be connected to either the closet switch closest to them or to the core switch, if it is closer. We chose this design in our example because the archive server was centrally located to all of them, thus cutting down on wiring costs.

As for the actual connections between the core switch A and the closet switches B, we have a number of technologies. Again, your PACS vendor may have preferences. In this case, we chose Gigabit Ethernet for the connections (uplinks) between the core and closet switches (2 in Figure 14.20). You may notice that we include 2 fiber-optic uplinks from the closets to the core switch. This allows greater reliability in the event that 1 of the pairs of fiber-optic connections experiences a failure, or if the fiber-optic connection on either the core switch or the closet fails.

Although not illustrated here, an even more resilient design would include 2 core switches A, with the archive server having a connection to both core switches, and each closet switch having a connection to both core switches. This type of connection would create a somewhat more complicated design to troubleshoot in the event of a failure, and it would certainly cost more, but it provides a high level of redundancy (meaning cable failures and hardware failures have less of an impact on the network) and ensures a high degree of availability of the archive server.

You also should notice a connection, 3, in Figure 14.20 to an edge router. This router acts just the same as the router in our previous PACS design, except that multiple sites of varying speed connect to it. In the current example, we are connecting to a remote site (4) using xDSL at 144 Kb/s. This speed is too slow for sending or retrieving compressed images, but fast enough for a remote site that needs only to view compressed images. The site connected with the DS3 (5) acts just like the site in the previous network example (Figure 14.19).

The site with the DS3 connection can communicate back to our main network at 45 Mb/s. This allows ample bandwidth for the large remote site to host a few modalities and display computers, although at a premium in terms of price. If bandwidth becomes an issue over this link we could upgrade to an OC3 connection providing 155 Mb/s, but the cost would be great.

Finally, 8 in Figure 14.20 shows a router that is providing connectivity to the rest of the hospital network, including its clinical systems. Note that this is the only router we are using on the LAN, and that in none of our previous examples did we include a router, as it can slow down performance in moving large images. However, in interfacing with the rest of a hospital network, a router should provide an efficient way of allowing us to move patient information between the 2 networks, as well as allowing cli-

nicians to view compressed images throughout the hospital on lower-priced workstations.

FUTURE TRENDS

The networking industry as a whole experiences changes at an extremely rapid pace. The rate of change is dizzying. There are several changes in the industry that will affect how PACS is implemented in the near future.

GIGABIT ETHERNET

Gigabit Ethernet has gained acceptance. Now Gigabit Ethernet is offered by nearly all vendors at reasonable prices. For the first time on the LAN, the ability for the network to provide inexpensive bandwidth has outpaced the computer's ability to transmit data. This means that since it is difficult for a Sparc workstation to transmit much more than 200 Mb/s, a Gigabit Ethernet connection offers plenty of bandwidth. Before Gigabit Ethernet, only expensive OC-12 ATM could make such a promise, while most workstations could saturate a 100 Mb/s Ethernet pipe. Of course, as computers get faster, their ability to transmit data will also increase. At this point, however, Gigabit Ethernet provides a lot of room for growth. Even so, it is possible for computers to collectively saturate Gigabit Ethernet backbones and connections, so careful network design is still required. Further, there are groups currently working on terabit Ethernet speed solutions.

RESOURCE RESERVATION PROTOCOL

Earlier, when explaining the advantages of ATM, we said that ATM had the ability to distinguish between different traffic types, thus allowing it to efficiently pass video and voice traffic while still moving e-mail along at a reasonable rate. Ethernet vendors, not wanting to be left in the dust, recognized this distinguishing capability as an important feature and have been working toward implementing some of those features into the Ethernet architecture. Called RSVP (resource reservation protocol), this feature will give Ethernet some ATM-like capabilities by allowing it to offer a lesser degree of QoS (almost a poor man's QoS). When combined with the brute force of Gigabit Ethernet, it offers a challenge to the future of the more elegant ATM in the LAN environment.

LAYER 3 SWITCHING

As detailed at length earlier in this chapter, switching occurs at the ISO model layer 2 and routing occurs at layer 3. The lines are becoming blurred, however, as vendors seek to offer the speed and flexibility of switching and the intelligence and efficiency of routing. Vendors are calling this layer 3 switching, although different vendors have widely varying ideas of how to implement it and what it means. In effect, layer 3 switching should combine the best of both worlds to such an extent that the idea of using the corridor in the conference room model will no longer be seen as an impediment to fast, efficient communication between different segments. In a large network, where PACS seeks to peacefully coexist with any number of applications, layer 3 switching offers potentially dramatic benefits by getting large images and studies out to a vast clientele.

VIRTUAL PRIVATE NETWORKS

Virtual private networks, or VPNs, have constituted a major buzzword in the industry. The goal of this technology is to make the Internet a safe medium for the secure transfer of private information, such as clinical data or images. It does this by encrypting the information at the source and decrypting it at the destination. In doing so a private virtual network is set up over the public, unsecure Internet. There is hope that companies can use this technology to decrease costs by using the Internet to exchange information that they normally would be able to share only over private circuits leased from RBOCs, thus saving money. This is also an ideal technology to use for remote access to the corporate network for home users or in virtual office environments. In the near future, as this technology matures and vendors are able to produce scalable solutions, VPNs will make a great impact on how the Internet is used.

LOWER COSTS

Competitiveness among vendors also means lower costs in the networking industry, just as in the computer industry. In the first year that Gigabit Ethernet became available, prices dropped nearly in half. The price of NICs continues to drop, as well as the price of routers and switches. On the WAN front, RBOCs are seeing increasing competition from one another, from cable providers, and from other third-party providers who are seeking to take

advantage of the tremendous hunger for bandwidth on the WAN. The cost and speed of the connection to the home or remote office, often called the "last mile," is quickly reaching attractive price points for many applications, especially PACS. RBOCs will be forced to lower prices of T1s and T3s as new technologies such as cable modems, xDSL, and wireless become more common. Similarly, use of the Internet and technologies such as VPN will also allow for significant price reductions for remote access.