HANDS-ON ACTIVITY 4A

Capturing Packets on Your Network

In this chapter, we discussed several data link layer protocols, such as SDLC and Ethernet. The objective of this Activity is for you to see the data link layer frames in action on your network.

Wireshark is one of the many tools that permit users to examine the frames in their network. It is called a packet sniffer because it enables you to see inside the frames and packets that your computer sends, as well as the frames and packets sent by other users on your LAN. In other words, you can eavesdrop on the other users on your LAN to see what Web sites they visit and even the email they send. We don't recommend using it for this reason, but it is important that you understand that someone else could be using Ethereal to sniff your packets to see and record what you are doing on the Internet.

1. Use your browser to connect to www.wireshark.org and download and install the Wireshark software.
2. When you start Wireshark you will see a screen like that in Figure 4.14, minus the two smaller windows on top.
   a. Click Capture
   b. Click Interfaces
   c. Click the Capture button beside your Wire-shark connection (wireless LAN or traditional LAN).
3. Wireshark will capture all packets moving through your LAN. To make sure you have something to see, open your Web browser and visit one or two Web sites. After you have captured packets for 30–60 seconds, return to Wireshark and click Stop.
4. Figure 4.15 shows the packets captured on my home network. The top window in Wireshark displays the complete list of packets in chronological order. Each packet is numbered; I've scrolled the window, so the first packet shown is packet 11. Wireshark lists the time, the source IP address, the destination IP address, the protocol, and some additional information about each packet. The IP addresses will be explained in more detail in the next chapter.

   For the moment, look at packet number 16, the second HTTP packet from the top. I've clicked on this packet, so the middle window shows the inside of the packet. The first line in this second window says the frame (or packet if you prefer) is 1091 bytes long. It contains an Ethernet II packet, an Internet Protocol (IP) packet, a Transmission Control Protocol (TCP) Packet, and a Hypertext Transfer Protocol (HTTP) packet. Remember in Chapter 1 that Figure 1.4 described how each packet was placed inside another packet as the message moved through the layers and was transmitted.

   Click on the plus sign (+) in front of the HTTP packet to expand it. Wireshark shows the contents of the HTTP packet. By reading the data inside the HTTP packet, you can see that this packet was an HTTP request to my.yahoo.com that contained a cookie. If you look closely, you'll see that the sending computer was a Tablet PC—that's some of the optional information my Web browser (Internet Explorer) included in the HTTP header.