2.5.1

Network Sniffing - TCP Handshaking

(Ethereal)

Laboratory Overview

Objective

Students will learn to use the Ethereal protocol analyzer to capture packets on a computer with an Internet connection. Initial TCP packets that are produced when a browser is used to view an Internet site will be observed. Observation will also be made of TCP packets when an attempt to connect fails.

Information for Laboratory

A. Students will start capturing packets using Ethereal.
B. A connection to an Internet site via a web browser will be made.
C. Students will stop the capturing of packets, and observe details gathered by Ethereal including a TCP handshake.
D. Students will attempt to telnet into a computer on the same network segment while capturing more packets using Ethereal.
E. Students can then observe an attempted TCP handshake that failed to make a connection.

Student Preparation

The student will have completed requisite reading. The student will require paper for notes and should be prepared to discuss the exercises upon completion. Ethereal and WinPcap must be installed for this lab.

Estimated Completion Time

30 Minutes

TCP Handshake

All network protocols send and receive control packets to enable communication between the source and the destination nodes. The two transport protocols within the TCP/IP suite are TCP and UDP. Both TCP and UDP keep track of different communications through the use of 16 bit ports, many of which are well-known. The use of UDP is connectionless, and thus does not require acknowledgements from recipients.

By its very nature, TCP (Transport Control Protocol) is connection-oriented. That is, it requires acknowledgement from the recipient. A TCP connection initiates by the three-way TCP handshake. Suppose node (A) attempts to connect to node (B) via TCP. TCP's three-way handshake between these two nodes will proceed as follows:

1.) A SYN packet is sent from node (A) to node (B)
2.) A SYN/ACK packet is sent from node (B) to node (A), acknowledging the receipt of a SYN packet.
3.) An ACK packet is sent from node (A) to node (B), completing the connection.

Each step places relevant ports in certain states. Under normal circumstances, a SYN packet is sent from a specific port on (A) to a specific port on (B) that is in a LISTEN state.

System B responds by going into the SYN_RECV state (pending completion of the connection). System B then sends back a SYN/ACK packet to System A, acknowledging that it received System A's SYN packet successfully.

If all goes well, (A) will return an ACK packet to (B) and the connection will move to the ESTABLISHED state on both (A) and (B).

Many common applications use TCP. Some of the more common applications include Internet browsing (using HTTP, port 80), Telnet (port 23), FTP (port 21), and SNMP (port 25). Every time these applications are used they are initiated by a TCP three-way handshake.

Network Monitoring

Network monitors, protocol analyzers, and “sniffers” are all a class of tools used by network administrators to gather information about their network for a wide variety of protocols. It cannot be overstated how important such tools are for proper network management as well as for detecting possible security breaches.

Network monitors may either be a software program running on a computer, or it can be a separate stand alone device. Like many network devices, cost and capabilities vary widely. They range from free software to platforms costing thousands of dollars.

Using Ethereal to Capture a TCP Handshake

Ethereal is an open source network monitor/ protocol analyzer. Being open source, the tool is free and runs on multiple platforms, including Unix, Linux, and Windows. It has a robust feature set that continues to be developed by a large number of contributors. It supports over 500 types of protocols which may be analyzed in very fine detail.

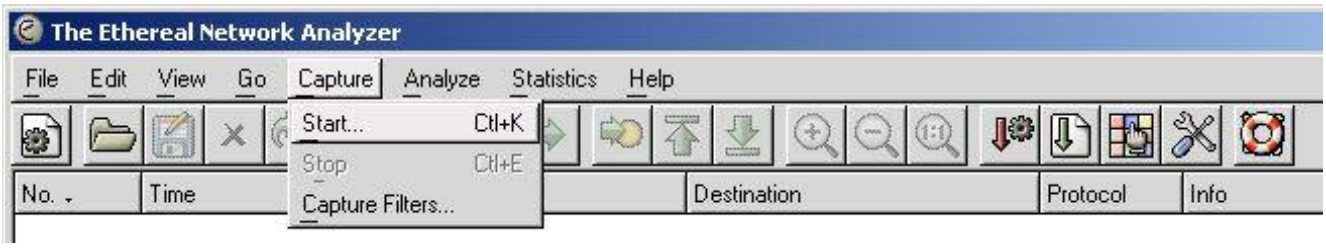
The use of Ethereal involves the initiation of a “capture”, which is simply the retention of protocol utilization information that the tool has detected. This information may be retained in a

capture file which can be saved for later reference. Ethereal is also compatible with numerous capture file formats that are compatible with other network monitors.

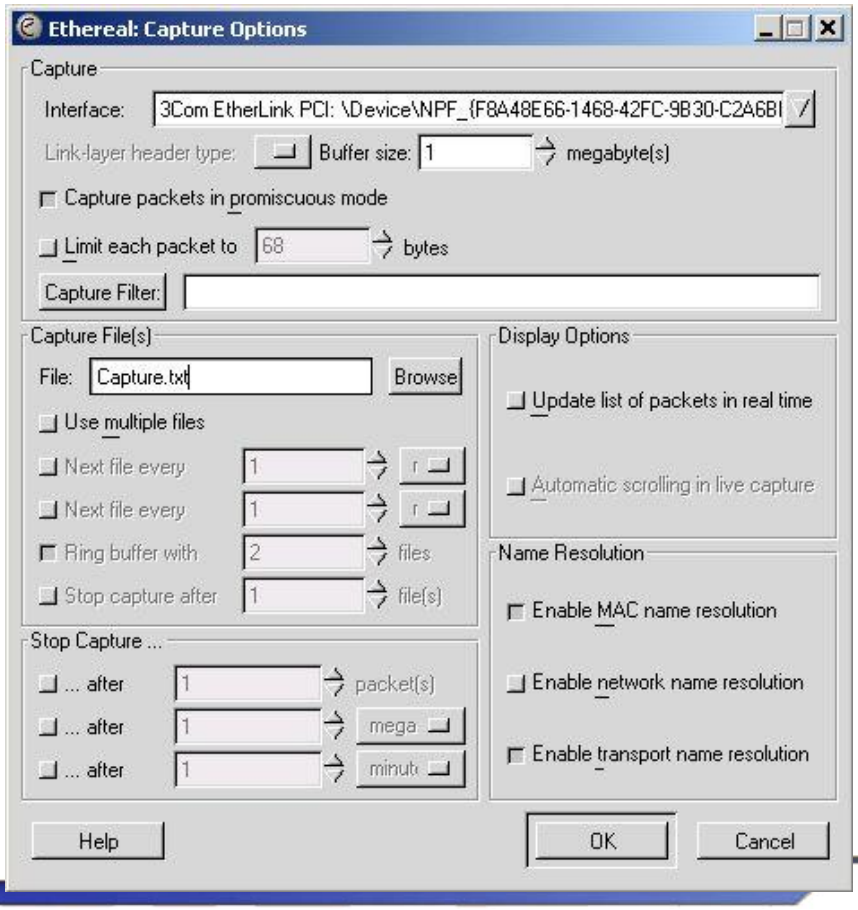
Step 1:

Start Ethereal which usually places an icon on the desktop. If Ethereal is not installed, see the Appendix for information regarding installation files.

Begin capturing packets by clicking on **Capture** on the menu bar, then clicking on Start. Note the keyboard shortcut CTRL-K will also start capturing packets.

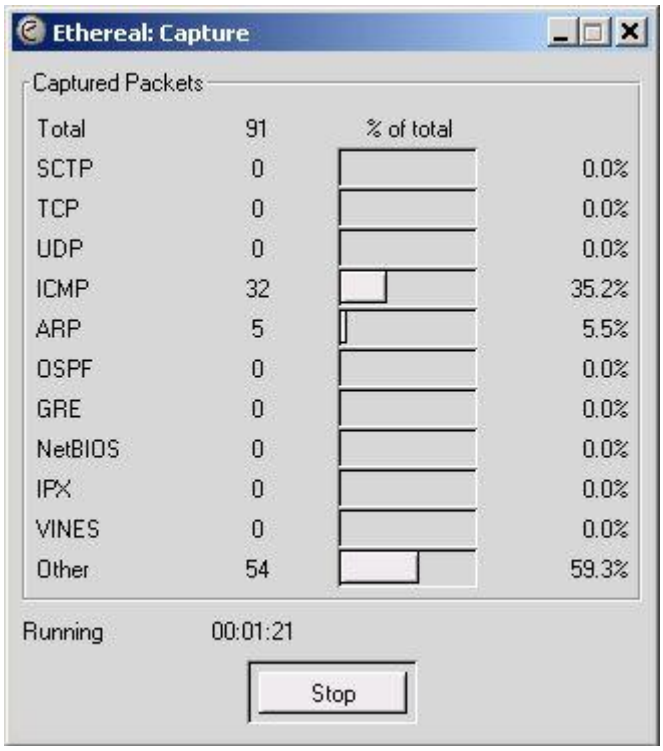


You should see the capture options dialog box similar to the following:


Ethereal: Capture Options
Capture
Interface:
3Com EtherLink PCI: \Device\NPF_{F8A48E66-1468-42FC-9B30-C2A6BI
Link-layer header type:
Buffer size:
1
megabyte(s)
Capture packets in promiscuous mode
Limit each packet to
68
bytes
Capture Filter:
Capture File(s)
File:
Capture.txt
Browse
Use multiple files
Next file every
1
Next file every
1
Ring buffer with
2
files
Stop capture after
1
file(s)
Display Options
Update list of packets in real time
Automatic scrolling in live capture
Name Resolution
Enable MAC name resolution
Enable network name resolution
Enable transport name resolution
Stop Capture ...
... after
1
packet(s)
... after
1
... after
1
Help
OK
Cancel

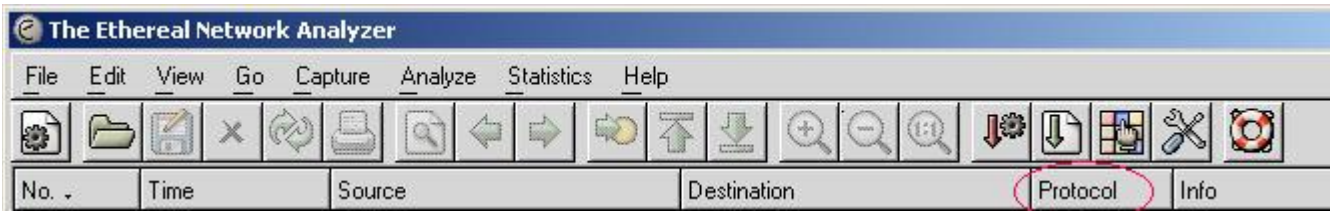
You may specify the name of a capture file for retention and later viewing. Be sure the interface is selected properly, but otherwise except the defaults.

You should now see the capture dialog box like the following:

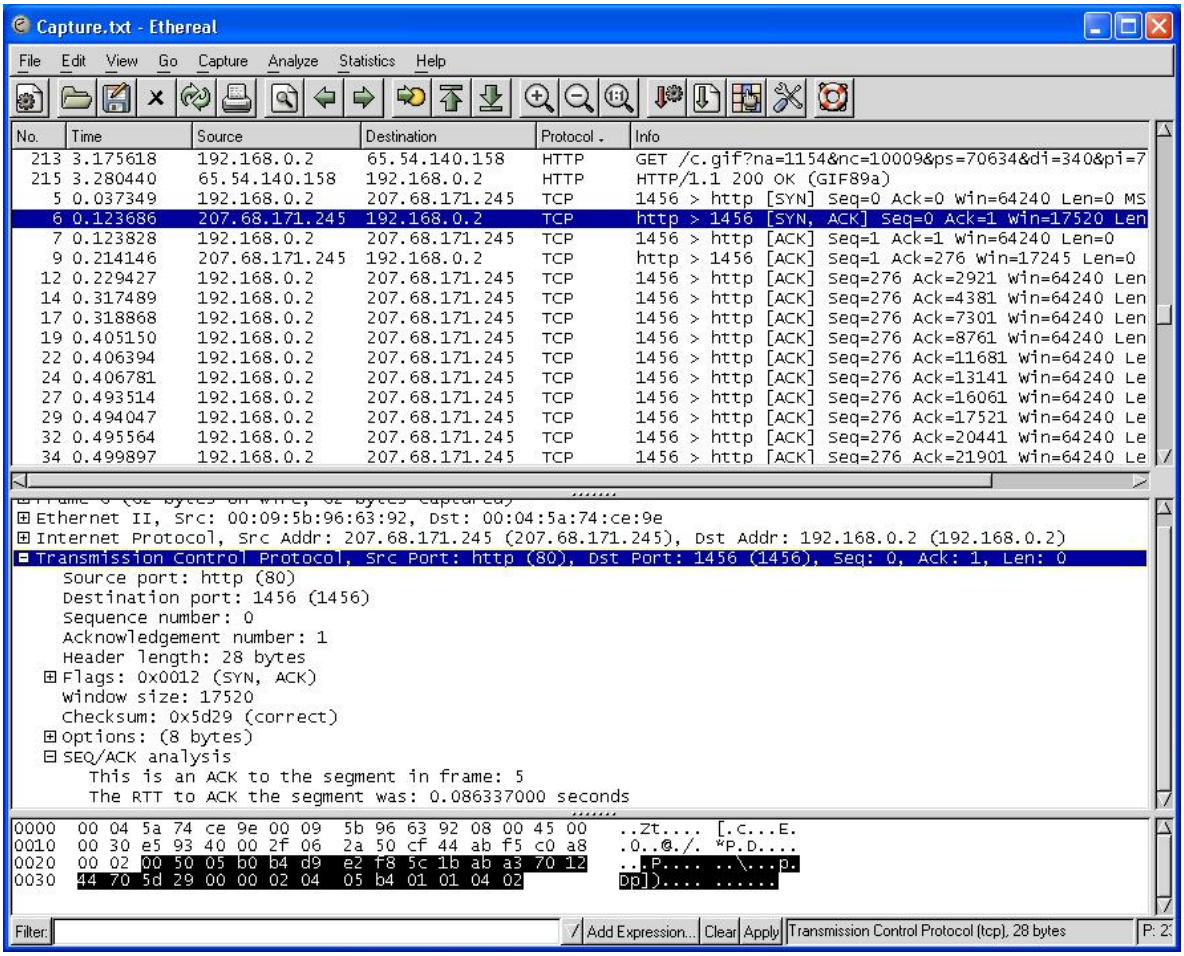


Step 2:

Visit a web site on the Internet, such as www.msn.com. Once the site is observed in the browser, leave the browser open, but stop the Ethereal capture via the capture dialog box shown above. After the capture has been stopped, Ethereal should be populated with data based on network information acquired during the capture period. Click on the protocol field shown below to sort the display by protocol type, and scroll down to TCP.



You should now see something similar to the following graphic:



Step 3:

Observe the top, middle, and bottom displays within Ethereal, each showing greater detail in succession. With proper sorting, the first three lines of the top display should correspond to the TCP three-way handshake. Note the [SYN], [SYN, ACK], and [ACK] in the figure.

The top portion of the display shows a summary of a particular packet. The middle display lists more detailed information sorted by layers of the OSI model beginning with the physical layer. Be sure to expand the middle display information by clicking on the +, and note the port numbers.

The lowest display area is the greatest detail showing the actual bit stream in hex.

Step 4:

Bring up a command window and ping the web site you visited in step 2. For www.msn.com, the command would be,

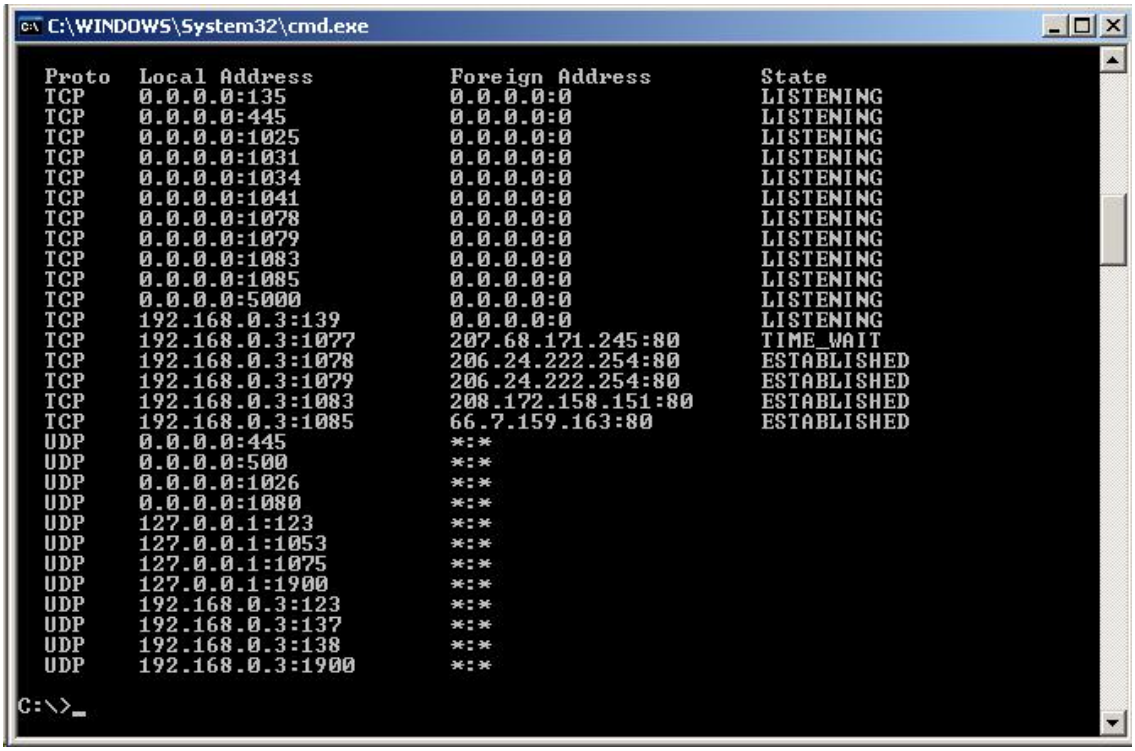
C:\>ping www.msn.com

The ping will probably fail, but the command output should show the actual IP address via DNS lookup. Here the web site corresponds to an address of 207.68.171.245, which is indicated in the Ethereal display.

The following command is also useful for disclosing summary information and states of open ports on the local host:

C:\>netstat –na

You should see something like,



Once again, note the ports following the colons. If a session with your web site is not evident, try refreshing your browser, and repeat the command.

Step 5:

To observe a failure to complete a three-way handshake, attempt may be made to telnet into another computer host on the local network segment. Though nearly all computer workstations support telnet for remote connection to other devices, they do not usually support telnet requests from other nodes.

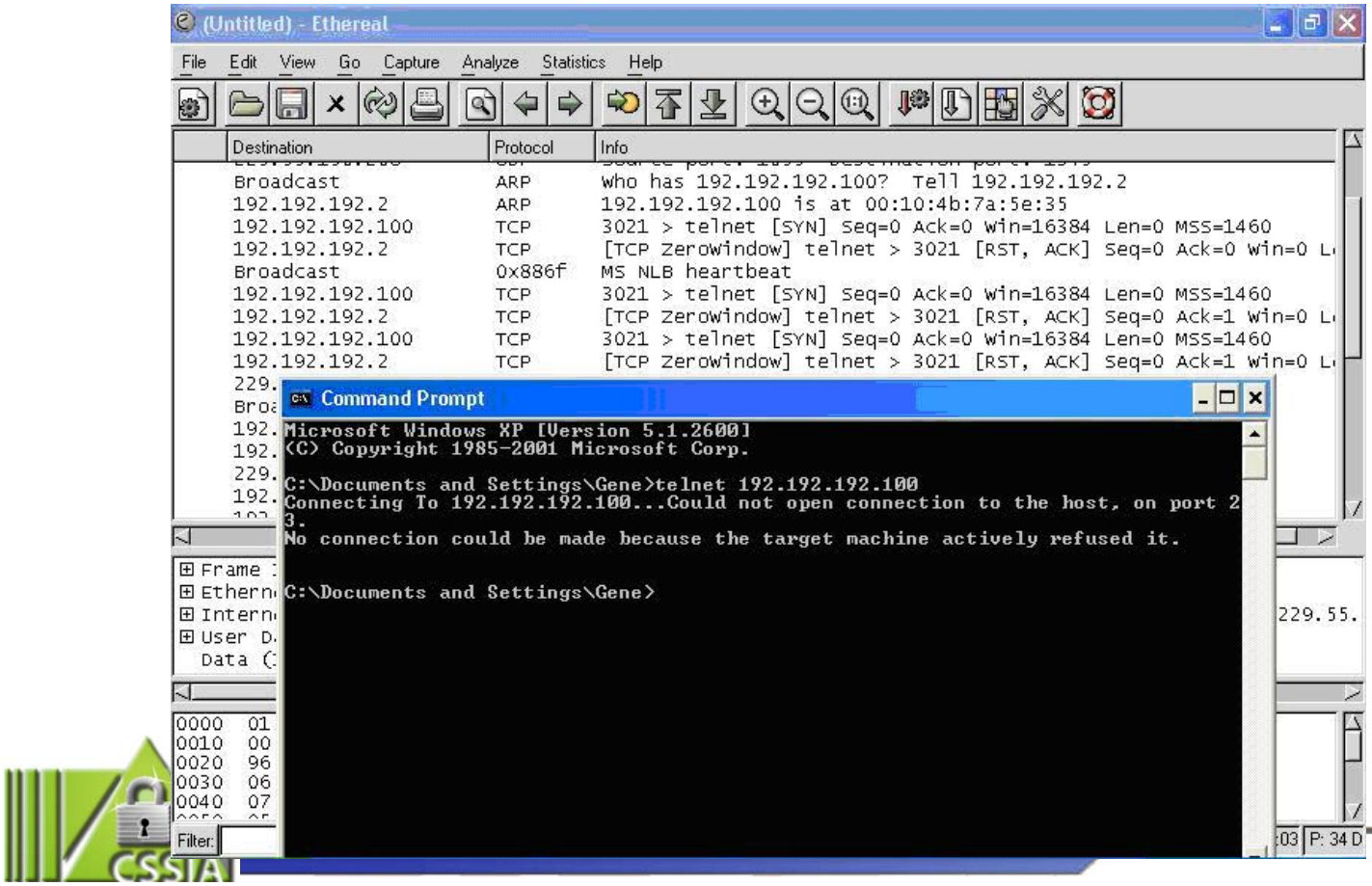
Verify connectivity with another host on the network segment via the ping command.

C:\>ping <IP address of host>

Once connectivity is verified, start another Ethereal capture as in step 1, and attempt to telnet into another host.

C:\>telnet <IP address of host>

After the failure to connect is indicated within the command window, stop the Ethereal capture. You should observe something similar to the next graphic. The sequence of TCP packets can be observed within Ethereal. Note that the [SYN] packet is not followed by a [SYN ACK] response, but rather a [RST ACK]. Telnet makes one more attempt to connect by sending another [SYN] packet, and after the same response, the failure message displays in the command window.


(Untitled) - Ethereal
File Edit View Go Capture Analyze Statistics Help
Destination Protocol Info
Broadcast ARP Who has 192.192.192.100? Tell 192.192.192.2
192.192.192.2 ARP 192.192.192.100 is at 00:10:4b:7a:5e:35
192.192.192.100 TCP 3021 > telnet [SYN] Seq=0 Ack=0 Win=16384 Len=0 MSS=1460
192.192.192.2 TCP [TCP ZeroWindow] telnet > 3021 [RST, ACK] Seq=0 Ack=0 Win=0
Broadcast 0x886f MS NLB heartbeat
192.192.192.100 TCP 3021 > telnet [SYN] Seq=0 Ack=0 Win=16384 Len=0 MSS=1460
192.192.192.2 TCP [TCP ZeroWindow] telnet > 3021 [RST, ACK] Seq=0 Ack=1 Win=0
192.192.192.100 TCP 3021 > telnet [SYN] Seq=0 Ack=0 Win=16384 Len=0 MSS=1460
192.192.192.2 TCP [TCP ZeroWindow] telnet > 3021 [RST, ACK] Seq=0 Ack=1 Win=0
Command Prompt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\Gene>telnet 192.192.192.100
Connecting To 192.192.192.100...Could not open connection to the host, on port 23.
No connection could be made because the target machine actively refused it.
C:\Documents and Settings\Gene>
Frame
Ethern
Intern
User D
Data
229.55.
0000 01
0010 00
0020 96
0030 06
0040 07
Filter:
P: 34 D

Analysis

1) What features of Ethereal are particularly useful for network administration and cyber security?

2) What happens if your computer attempts to telnet to an inactive IP address on your network segment? Does your computer send out a TCP [SYN] packet?

3) Explore what happens when you ping your localhost address 127.0.0.1.

4) Explore what happens when you ping your local IP address. What is the difference between this and pinging the localhost address?

Summary Discussion

A classroom discussion should follow the lab. Review the lab questions and your analyses as a group. Share your experiences and knowledge with the class.

If You Want To Learn More

Consult the **Help** feature of Ethereal, which is a series of text files. Be sure to view the **Well Known** tab which contains valuable information for networking novices.

Explore the web site of Ethereal, www.ethereal.com, to obtain more information about this tool.

Appendix:

This lab was developed using Ethereal 0.10.8, which can be obtained from:

www.ethereal.com

-or-

http://www.download.com

and WinPcap (Windows Packet Capturing software), which can be obtained from:

http://winpcap.polito.it/

-or-

www.ethereal.com

-or-

http://www.download.com

Note that Ethereal, in particular WinPcap, may have difficulty starting a capture from a wireless network adaptor.

The OS environment for this lab was Windows XP Professional, Version 2002, Service Pack 2 (8/04).