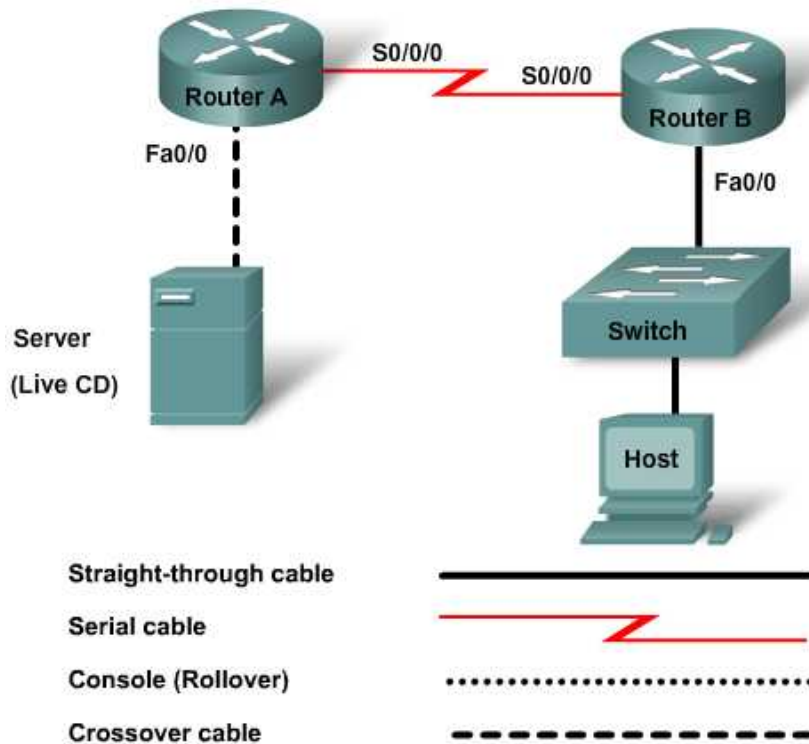


Lab 1.2.2 Capturing and Analyzing Network Traffic



Host Name	IP Address Fa0/0	Subnet Mask	IP Address S0/0/0	Subnet Mask	Default Gateway
RouterA	172.17.0.1	255.255.0.0	192.168.1.1 (DCE)	255.255.255.0	N/A
RouterB	192.168.3.1	255.255.255.0	192.168.1.2	255.255.255.0	N/A
Server	172.17.1.1	255.255.0.0			172.17.0.1
Switch					
Host	192.168.3.2	255.255.255.0			192.168.3.1

Objectives

- Use Wireshark to capture protocol data packets as they cross the networks.
- Use Wireshark to analyze protocol data packets from the captured results.

Background / Preparation

This lab focuses on the basic configuration of the Cisco 1841 or comparable routers using Cisco IOS commands. The information in this lab applies to other routers; however, command syntax may vary. The Cisco Catalyst 2960 switch comes preconfigured and only needs to be assigned basic security information before being connected to a network.

The following resources are required:

- Cisco 2960 switch or other comparable switch
- Two Cisco 1841 or comparable routers with minimum one serial and one fast Ethernet interface
- Two Windows-based PCs, one with a terminal emulation program. Use one PC as the host, and use the other as the server.
- RJ-45-to-DB-9 connector console cable to configure the routers
- Two straight-through Ethernet cables
- One crossover Ethernet cable
- Access to the PC command prompt
- Access to PC network TCP/IP configuration

NOTE: Make sure that all routers and the switch have been erased and have no startup configurations. If you need instructions, refer to the end of this lab. Instructions are provided for both the switch and router.

NOTE: SDM Enabled Routers – If the startup-config file is erased on an SDM enabled router, SDM will no longer come up by default when the router is restarted. It will be necessary to build a basic router configuration using IOS commands. Contact your instructor if necessary.

NOTE: To capture PDUs on the computer on which Wireshark is installed, the network must be set up and a ping between the server and the host should be successful. Wireshark must be running before any data can be captured. Wireshark may be downloaded from www.wireshark.org and installed on the local hosts, or run from the Discovery Server Live CD. For detailed instructions on installation of the Discovery Server Live CD, please refer to the lab manual that is located on Academy Connection in the Tools Section.

NOTE: The Ethernet interface on the server must be active when the server is started. Therefore, the router should be connected to the server and started before booting the server.

Step 1: Connect the routers and configure

- a. Connect the two routers with a serial cable. RouterA will provide the clocking signal between the two routers. Use S0/0/0 on both routers to connect them.
- b. Use RIP as the protocol when configuring both routers. Advertise the appropriate networks on each router.
- c. Connect the Fa0/0 on RouterA with a crossover cable to the server running the Discovery Server Live CD.
- d. RouterB will use a straight-through cable from its Fa0/0 to connect to the switch through the Fa0/1. Configure the routers as shown in the topology diagram above.

Step 2: Connect the host to the switch and configure

Connect the Host to attach to Fast Ethernet switch port Fa0/2. Configure the host as shown in the topology diagram above.

Step 3: Verify connectivity using ping

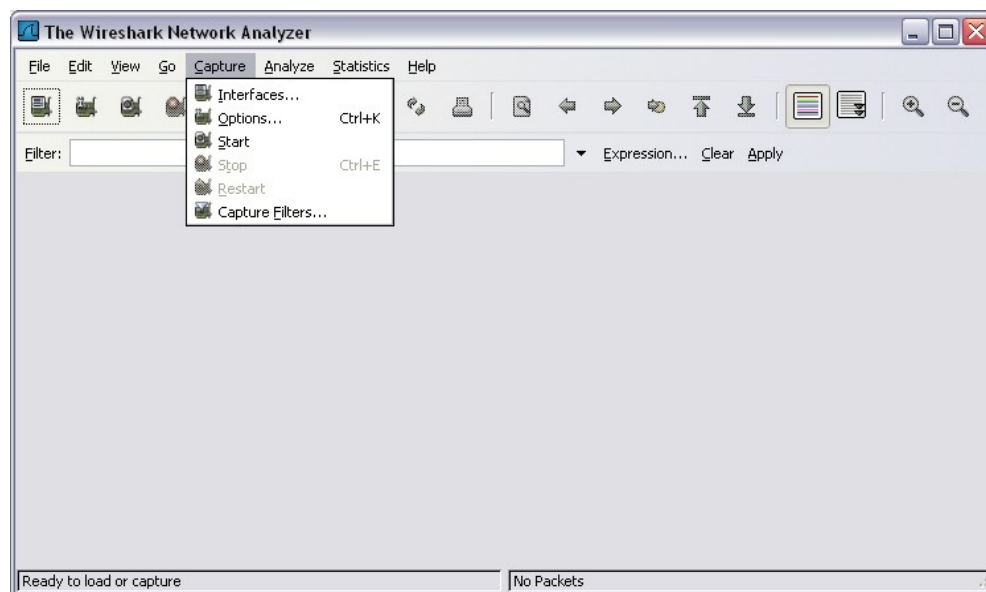
- a. To verify that the network is set up successfully, ping from the host to the server.

- b. If the ping is not successful, verify the connections and configurations again. Check to ensure that all cables are correct and that connections are seated. Check the host, server, and router configurations.
- c. Was the ping successful? _____

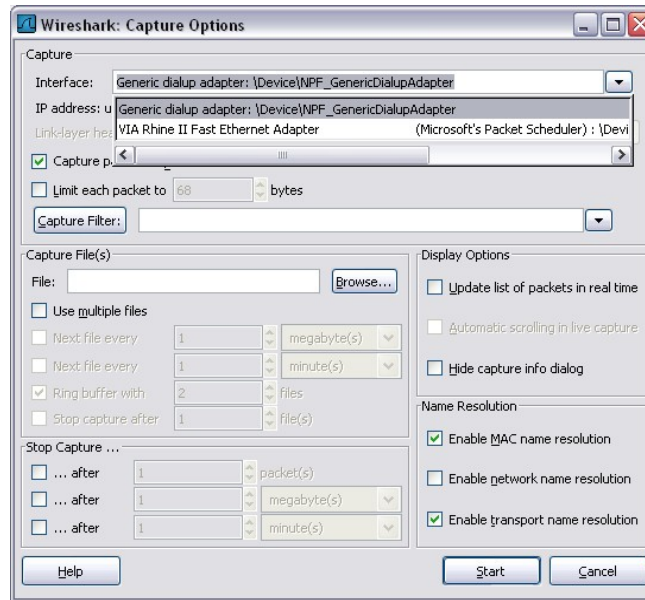
Step 4: Launch Wireshark

NOTE: Wireshark may be downloaded from the Internet at www.wireshark.org and installed on each local host. If this is not possible, Wireshark may be run from the Discovery Live CD. Check with your instructor to determine which procedure to follow.

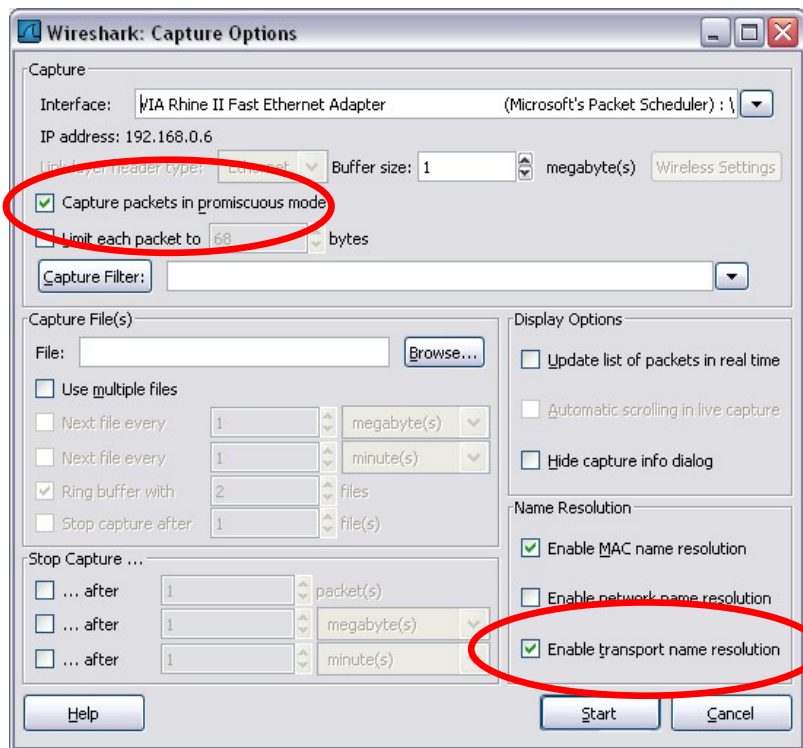
- a. If running Wireshark from the local host, double-click on the icon to begin the application and proceed to step d. If running Wireshark from the Discovery server, proceed to step b.
- b. From the **K Start** menu on the server desktop, choose **Internet> Wireshark Network Analyzer**.
- c. Launch Wireshark if it is not already open. If prompted for a password, enter **discoverit**.
- d. To start data capture, go to the **Capture** menu click **Options**. The **Options** dialog provides a range of settings and filters that determine how much data traffic is captured.



- e. Ensure that Wireshark is set to monitor the correct interface. From the **Interface** drop-down list, select the network adapter in use. For most computers, this will be the connected Ethernet Adapter.



- f. Next, other options can be set. The two options highlighted below are worth examination: Capture packets in promiscuous mode and enable transport name resolution.



- **Setting Wireshark to capture packets in promiscuous mode**

If this feature is *not* checked, only PDUs destined for this computer will be captured.

If this feature is checked, all PDUs destined for this computer *and* all those detected by the computer NIC on the same network segment (i.e., those that "pass by" the NIC but are not destined for the computer) are captured.

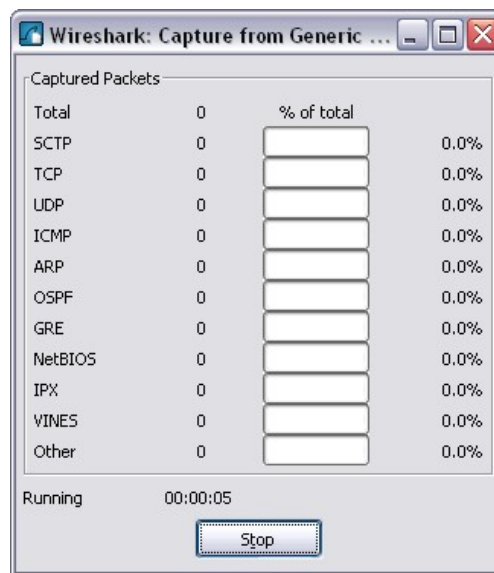
NOTE: As you use different intermediary devices (hubs, switches, routers) to connect end devices on a network, you will experience different Wireshark results.

- **Setting Wireshark for network name resolution**

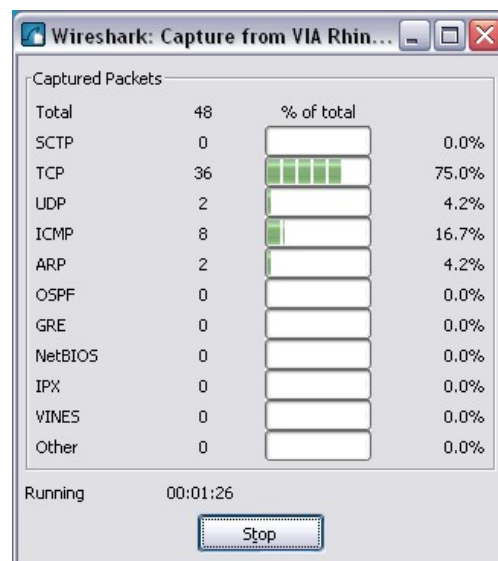
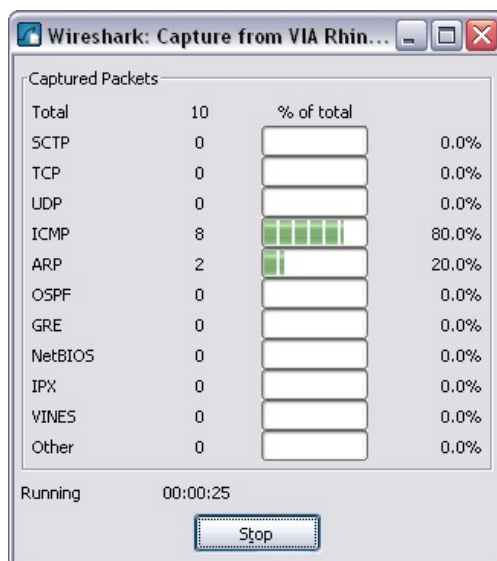
This option allows you to control whether or not Wireshark translates network addresses found in PDUs into names. Although this is a useful feature, the name resolution process may add extra PDUs to your captured data, perhaps distorting the analysis.

There are also a number of other capture filtering and process settings available on this screen.

- Clicking the **Start** button starts the data capture process. A message box displays the progress of this process.
- Create some traffic to be captured. Issue a **ping** and **tracert** from the host and watch for routing updates.

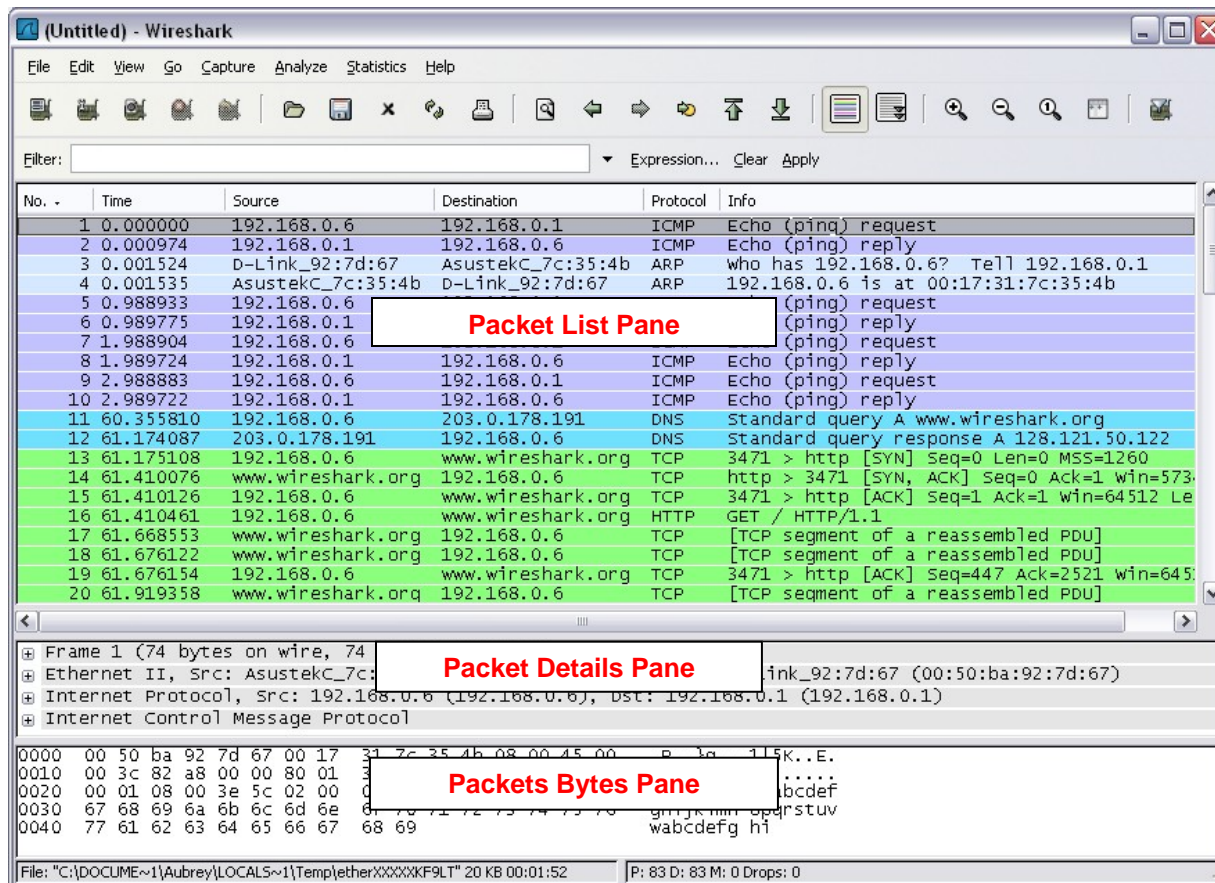


As data PDUs are captured, the types and number are indicated in the message box. The examples show the capture of a ping process and then accessing a web page.



- Clicking the **Stop** button terminates the capture process. The main screen is displayed.

This main display window of Wireshark has three panes.



- The PDU (or Packet) List pane at the top of the diagram displays a summary of each packet captured. By clicking on packets in this pane, you control what is displayed in the other two panes.
- The PDU (or Packet) Details pane in the middle of the diagram displays the packet selected in the Packet List Pane in more detail.
- The PDU (or Packet) Bytes pane at the bottom of the diagram displays the actual data (in hexadecimal form representing the actual binary) from the packet selected in the Packet List pane, and highlights the field selected in the Packet Details pane.

Packet List Pane

Each line in the Packet List pane corresponds to one PDU or packet of the captured data. If you select a line in this pane, additional details are displayed in the Packet Details and Packet Bytes panes. The example above shows the PDUs captured when the ping utility was used and <http://www.Wireshark.org> was accessed. Packet number 1 is selected in this pane.

Packet Details Pane

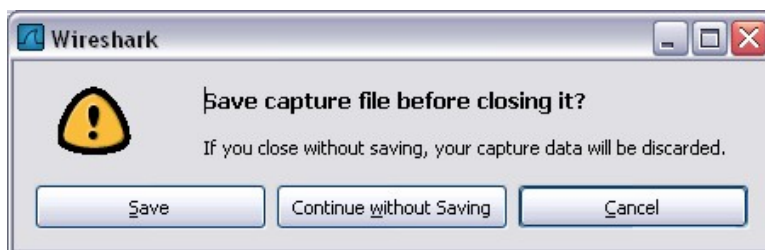
The Packet Details pane shows the current packet (selected in the Packet List pane) in a more detailed form. This pane shows the protocols and protocol fields of the selected packet. The protocols and fields of the packet are displayed using a tree, which can be expanded and collapsed.

Packet Bytes Pane

The Packet Bytes pane shows the data of the current packet (selected in the Packet List pane) in what is known as "hexdump" style. In this lab, this pane will not be examined in detail. However, when a more in-depth analysis is required, this displayed information is useful for examining the binary values and content of PDUs.

The information captured for the data PDUs can be saved in a file. This file can then be opened in Wireshark for future analysis without the need to recapture the same data traffic again. The information displayed when a capture file is opened is the same as the original capture.

When closing a data capture screen or exiting Wireshark, you are prompted to save the captured PDUs.



Clicking **Continue without Saving** closes the file or exits Wireshark without saving the displayed captured data.

Step 5: Ping PDU Capture

- Launch Wireshark.
- Set the Capture Options as described in Step 4 and start the capture process.
- From the command line of the host, ping the IP address of the server on the other end of the lab topology. In this case, ping the Discovery Server Live CD using the command `ping 172.17.1.1`.
- After receiving the successful replies to the ping in the command-line window, stop the packet capture.

Step 6: Examine the Packet List pane

- The Packet List pane on Wireshark should now look similar to this:

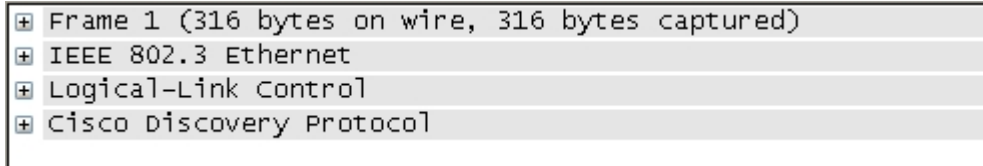
No.	Time	Source	Destination	Protocol	Info
1	0.000000	Cisco_79:f3:80	CDP/VTP/DTP/PAgP/UDLD	CDP	Device ID: ROUTER_A Port ID: FastEthernet0/0
2	4.959859	Cisco_79:f3:80	Cisco_79:f3:80	LOOP	Reply
3	5.555085	192.168.3.2	172.17.1.1	ICMP	Echo (ping) request
4	5.555108	172.17.1.1	192.168.3.2	ICMP	Echo (ping) reply
5	6.557116	192.168.3.2	172.17.1.1	ICMP	Echo (ping) request
6	6.557137	172.17.1.1	192.168.3.2	ICMP	Echo (ping) reply
7	7.557337	192.168.3.2	172.17.1.1	ICMP	Echo (ping) request
8	7.557359	172.17.1.1	192.168.3.2	ICMP	Echo (ping) reply
9	8.557088	192.168.3.2	172.17.1.1	ICMP	Echo (ping) request
10	8.557111	172.17.1.1	192.168.3.2	ICMP	Echo (ping) reply
11	10.557548	Intel_56:98:68	Cisco_79:f3:80	ARP	who has 172.17.0.1? Tell 172.17.1.1
12	10.558224	Cisco_79:f3:80	Intel_56:98:68	ARP	172.17.0.1 is at 00:0d:28:79:f3:80

- Look at the packets listed; we are interested in the packets numbered 3 through 10.
- Locate the equivalent packets on the packet list on your computer. The numbers may be different.
- From the Wireshark Packet List, answer the following questions:
 - What protocol is used by ping? _____
 - What is the full protocol name? _____
 - What are the names of the two ping messages? _____ and _____

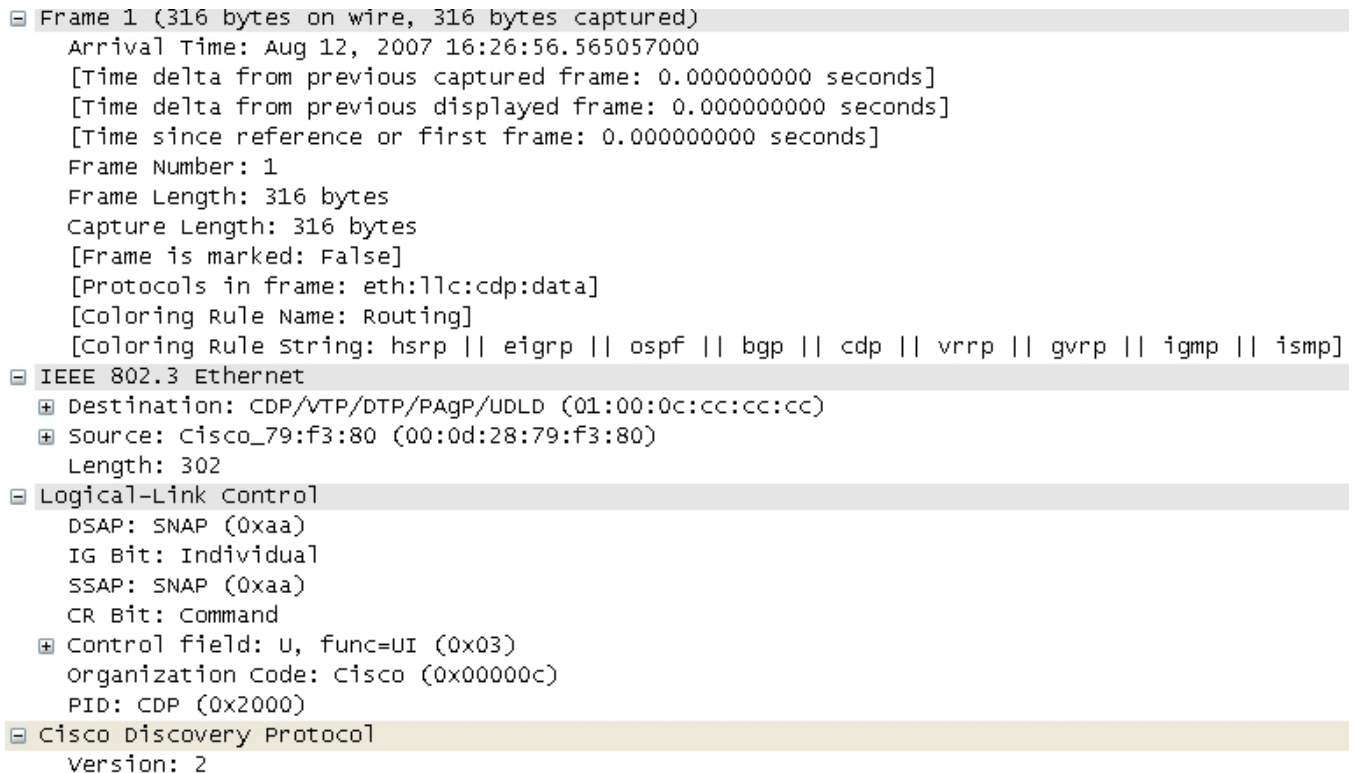
- 4) Are the listed source and destination IP addresses what you expected? _____
- 5) Why?

Step 7: Examine the Packet Details pane

- a. Select (highlight) the first echo request packet on the list with the mouse. The Packet Detail pane will now display something similar to this:



- b. Click each of the four + to expand the information. The packet Detail Pane will now be similar to:



As you can see, the details for each section and protocol can be expanded further.

- c. Spend some time scrolling through this information. At this stage of the course, you may not fully understand the information displayed. Make a note of the information you do recognize.

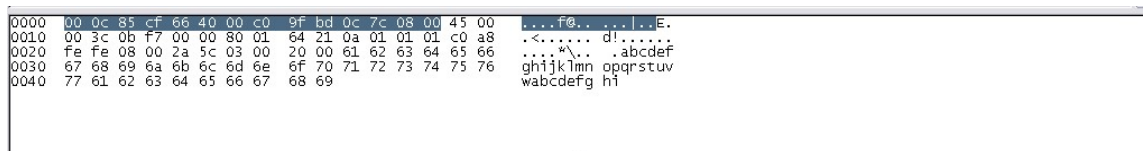
- d. Locate the two different types of Source and Destination.

Why are there two types?

What protocols are in the Ethernet frame?

- e. Select a line in the Packets Detail pane (middle pane). Notice that all or part of the information in the Packet Bytes pane also becomes highlighted.

For example, if the second line (+ Ethernet II) is highlighted in the Details pane, the Bytes pane now highlights the corresponding values.



0000	00 0c 85 cf 66 40 00 c0 9f bd 0c 7c 08 00 45 00	...f@...E.
0010	00 3c 0b f7 00 00 80 01 64 21 0a 01 01 01 c0 a8	.<....d!....
0020	fe fe 08 00 2a 5c 03 00 20 00 61 62 63 64 65 66	...*\...abcdef
0030	67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76	ghijklmn opqrstuv
0040	77 61 62 63 64 65 66 67 68 69	wabcedfg hi

This example shows the particular binary values that represent that information in the PDU. At this point in the course, it is not necessary to understand this information in detail.

- f. Go to the **File** menu and click **Close**.
- g. Click **Continue without Saving** when this message box appears.



Step 8: Perform an FTP PDU Capture

- a. Assuming that Wireshark is still running from the previous steps, start packet capture by clicking the **Start** option on the Wireshark **Capture** menu.
- b. At the command line on your host, enter **ftp 172.17.1.1**. When the connection is established, enter **anonymous** as the user.
- c. When successfully logged in, enter **get /pub/Discovery_1/document_1** and press the **Enter** key. Note that there is a space after **get**. This command will start downloading the file from the ftp server. The output will look similar to:

```
C:\> ftp 172.17.1.1
Connected to 172.17.1.1
220 Welcome to The CCNA-Discovery FTP service.
ftp> get /pub/Discovery_1/document_1
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for pub/Discovery_1/document_1
<73 bytes>.
226 File send OK.
ftp: 73 bytes received in 0.03Seconds 2.35Kbytes/sec.
```

- d. When the file download is complete, enter **quit**.

```
ftp> quit
```

221 Goodbye .

C:\>

- e. Stop the PDU capture in Wireshark.

Step9: Examine the Packet List pane

- a. Increase the size of the Wireshark Packet List pane and scroll through the PDUs listed.
- b. Locate and note those PDUs associated with the file download. These will be the PDUs from the Layer 4 protocol TCP and the Layer 7 protocol FTP.
- c. Identify the three groups of PDUs associated with the file transfer. The first group is associated with the connection phase and logging into the server. List examples of messages exchanged in this phase.
- d. Locate and list examples of messages exchanged in the second phase that is the actual download request and the data transfer.
- e. The third group of PDUs relate to logging out and breaking the connection. List examples of messages exchanged during this process.
- f. Locate recurring TCP exchanges throughout the FTP process. What feature of TCP does this indicate?

Step 10: Examine Packet Details and Packet Byte panes

- a. Select (highlight) a packet on the list associated with the first phase of the FTP process. View the packet details in the Packet Details pane.
 - b. What are the protocols encapsulated in the frame?
-
- c. Highlight the packets containing the username and password. Examine the highlighted portion in the Packet Byte pane. What does this say about the security of this FTP login process?
-
- d. Highlight a packet associated with the second phase. From any pane, locate the packet containing the filename. What is the filename that was downloaded?
-
- e. When finished, close the Wireshark file and continue without saving.

Step 11: Perform an HTTP PDU Capture

- a. Start packet capture. Assuming that Wireshark is still running from the previous steps, start packet capture by clicking the **Start** option on the Wireshark **Capture** menu.
NOTE: Capture Options do not have to be set if continuing from previous steps of this lab.
- b. Launch a web browser on the computer that is running Wireshark.
- c. Enter the IP address of the Discovery Server 172.17.1.1 in the address box. When the webpage has fully downloaded, stop the Wireshark packet capture.

Step 12: Examine the Packet List pane

- a. Increase the size of the Wireshark Packet List pane and scroll through the PDUs listed.
- b. Locate and identify the TCP and HTTP packets associated with the webpage download.
- c. Note the similarity between this message exchange and the FTP exchange.

Step 13: Examine the Packet Details and Bytes panes

- In the Packet List pane, highlight an HTTP packet that has the notation **(text/html)** in the **Info** column.
 - In the Packet Details pane, click the **+** next to **Line-based text data: html**. When this information expands, what is displayed?
-
- Examine the highlighted portion of the Byte pane. This portion shows the HTML data carried by the packet.
 - When finished, close the Wireshark file and continue without saving.

Step 14: Analyze the capture

- Look at the capture below and examine the various protocols being used in this network.

No.	Time	Source	Destination	Protocol	Info
39	75.037581	Cisco_79:f3:80	CDP/VTP/DTP/PagP/UDLD	CDP	Device ID: ROUTER_A Port ID: FastEthernet0/0
40	79.997380	Cisco_79:f3:80	Cisco_79:f3:80	LOOP	Reply
41	82.124081	192.168.3.2	172.17.1.1	FTP	Request: QUIT
42	82.124111	172.17.1.1	192.168.3.2	FTP	Response: 221 Goodbye.
43	82.131646	172.17.1.1	192.168.3.2	TCP	ftp > 1042 [FIN, ACK] Seq=275 Ack=97 win=5840 Len=0
44	82.141466	192.168.3.2	172.17.1.1	TCP	1042 > ftp [FIN, ACK] Seq=97 Ack=275 win=65261 Len=0
45	82.141482	172.17.1.1	192.168.3.2	TCP	ftp > 1042 [ACK] Seq=276 Ack=98 win=5840 Len=0
46	82.148391	192.168.3.2	172.17.1.1	TCP	1042 > ftp [ACK] Seq=98 Ack=276 win=65261 Len=0
47	89.997017	Cisco_79:f3:80	Cisco_79:f3:80	LOOP	Reply
48	99.885642	172.17.0.1	255.255.255.255	RIPv1	Response
49	99.996682	Cisco_79:f3:80	Cisco_79:f3:80	LOOP	Reply
50	109.996337	Cisco_79:f3:80	Cisco_79:f3:80	LOOP	Reply
51	115.806501	192.168.3.2	172.17.1.1	TCP	1047 > http [SYN] Seq=0 Len=0 MSS=1460
52	115.806540	172.17.1.1	192.168.3.2	TCP	http > 1047 [SYN, ACK] Seq=0 Ack=1 win=5840 Len=0
53	115.822708	192.168.3.2	172.17.1.1	TCP	1047 > http [ACK] Seq=1 Ack=1 win=65535 Len=0
54	115.886954	192.168.3.2	172.17.1.1	HTTP	GET / HTTP/1.1
55	115.886977	172.17.1.1	192.168.3.2	TCP	http > 1047 [ACK] Seq=1 Ack=403 win=6432 Len=0
56	115.888244	172.17.1.1	192.168.3.2	HTTP	HTTP/1.1 200 OK (text/html)
57	115.888334	172.17.1.1	192.168.3.2	TCP	http > 1047 [FIN, ACK] Seq=1114 Ack=403 win=6432
58	116.068416	192.168.3.2	172.17.1.1	TCP	1047 > http [FIN, ACK] Seq=403 Ack=1114 win=6442
59	116.068430	172.17.1.1	192.168.3.2	TCP	http > 1047 [ACK] Seq=1115 Ack=404 win=6432 Len=0
60	116.075768	192.168.3.2	172.17.1.1	TCP	1047 > http [ACK] Seq=404 Ack=1115 win=64422 Len=0
61	116.189037	192.168.3.2	172.17.1.1	TCP	1048 > http [SYN] Seq=0 Len=0 MSS=1460
62	116.189048	172.17.1.1	192.168.3.2	TCP	http > 1048 [SYN, ACK] Seq=0 Ack=1 win=5840 Len=0
63	116.205143	192.168.3.2	172.17.1.1	TCP	1048 > http [ACK] Seq=1 Ack=1 win=65535 Len=0
64	116.259606	192.168.3.2	172.17.1.1	HTTP	GET /favicon.ico HTTP/1.1
65	116.259618	172.17.1.1	192.168.3.2	TCP	http > 1048 [ACK] Seq=1 Ack=334 win=6432 Len=0
66	116.260609	172.17.1.1	192.168.3.2	HTTP	HTTP/1.1 404 Not Found (text/html)
67	116.260672	172.17.1.1	192.168.3.2	TCP	http > 1048 [FIN, ACK] Seq=464 Ack=334 win=6432
68	116.348047	192.168.3.2	172.17.1.1	TCP	1048 > http [FIN, ACK] Seq=334 Ack=464 win=65072
69	116.348059	172.17.1.1	192.168.3.2	TCP	http > 1048 [ACK] Seq=465 Ack=335 win=6432 Len=0
70	116.355070	192.168.3.2	172.17.1.1	TCP	1048 > http [ACK] Seq=335 Ack=465 win=65072 Len=0
71	119.995999	Cisco_79:f3:80	Cisco_79:f3:80	LOOP	Reply
72	128.964548	172.17.0.1	255.255.255.255	RIPv1	Response
73	129.995382	Cisco_79:f3:80	Cisco_79:f3:80	LOOP	Reply
74	135.035662	Cisco_79:f3:80	CDP/VTP/DTP/PagP/UDLD	CDP	Device ID: ROUTER_A Port ID: FastEthernet0/0
75	139.995357	Cisco_79:f3:80	Cisco_79:f3:80	LOOP	Reply
76	149.995055	Cisco_79:f3:80	Cisco_79:f3:80	LOOP	Reply

- List the protocols used on the network shown above.
-

c. Examine the capture below.

No.	Time	Source	Destination	Protocol	Info
76	149.995055	Cisco_79:f3:80	Cisco_79:f3:80	LOOP	Reply
77	153.608179	192.168.3.2	172.17.1.1	TCP	1051 > https [SYN] Seq=0 Len=0 MSS=1460
78	153.608206	172.17.1.1	192.168.3.2	TCP	https > 1051 [SYN, ACK] Seq=0 Ack=1 win=5840 Len=0
79	153.624452	192.168.3.2	172.17.1.1	TCP	1051 > https [ACK] Seq=1 Ack=1 win=65535 Len=0
80	153.646527	192.168.3.2	172.17.1.1	SSLv2	Client Hello
81	153.646552	172.17.1.1	192.168.3.2	TCP	https > 1051 [ACK] Seq=1 Ack=106 win=5840 Len=0
82	153.679445	172.17.1.1	192.168.3.2	TLSv1	Server Hello, Certificate, Server Key Exchange, Se
83	153.943418	192.168.3.2	172.17.1.1	TCP	1051 > https [ACK] Seq=106 Ack=1410 win=64126 Len=
84	156.239770	172.17.0.1	255.255.255.255	RIPv1	Response
85	159.994711	Cisco_79:f3:80	Cisco_79:f3:80	LOOP	Reply
86	166.543988	192.168.3.2	172.17.1.1	TLSv1	Client Key Exchange, Change Cipher Spec, Encrypted
87	166.574022	172.17.1.1	192.168.3.2	TLSv1	Change Cipher Spec, Encrypted Handshake Message
88	166.660920	192.168.3.2	172.17.1.1	TLSv1	Application Data
89	166.701160	172.17.1.1	192.168.3.2	TCP	https > 1051 [ACK] Seq=1469 Ack=741 win=7504 Len=0
90	169.994404	Cisco_79:f3:80	Cisco_79:f3:80	LOOP	Reply
91	171.761781	172.17.1.1	192.168.3.2	TLSv1	Application Data, [Unreassembled Packet (Incorrect
92	171.761797	172.17.1.1	192.168.3.2	TLSv1	Ignored Unknown Record
93	171.765143	172.17.1.1	192.168.3.2	TLSv1	Ignored Unknown Record
94	172.197946	192.168.3.2	172.17.1.1	TCP	1051 > https [ACK] Seq=741 Ack=2929 win=65535 Len=
95	172.408969	192.168.3.2	172.17.1.1	TCP	1051 > https [ACK] Seq=741 Ack=5725 win=65535 Len=
96	172.421510	192.168.3.2	172.17.1.1	TLSv1	Encrypted Alert
97	172.421522	172.17.1.1	192.168.3.2	TCP	https > 1051 [ACK] Seq=5725 Ack=778 win=7504 Len=0
98	172.428472	192.168.3.2	172.17.1.1	TCP	1051 > https [RST, ACK] Seq=778 Ack=5725 win=0 Len=
99	172.436417	192.168.3.2	172.17.1.1	TCP	1051 > https [RST] Seq=778 Len=0
100	178.984332	192.168.3.2	172.17.1.1	TCP	1052 > https [SYN] Seq=0 Len=0 MSS=1460
101	178.984356	172.17.1.1	192.168.3.2	TCP	https > 1052 [SYN, ACK] Seq=0 Ack=1 win=5840 Len=0
102	178.992585	192.168.3.2	172.17.1.1	TCP	1053 > https [SYN] Seq=0 Len=0 MSS=1460
103	178.992610	172.17.1.1	192.168.3.2	TCP	https > 1053 [SYN, ACK] Seq=0 Ack=1 win=5840 Len=0
104	179.000452	192.168.3.2	172.17.1.1	TCP	1052 > https [ACK] Seq=1 Ack=1 win=65535 Len=0
105	179.024725	192.168.3.2	172.17.1.1	SSL	Client Hello
106	179.024746	172.17.1.1	192.168.3.2	TCP	https > 1052 [ACK] Seq=1 Ack=121 win=5840 Len=0
107	179.025978	172.17.1.1	192.168.3.2	TLSv1	Server Hello, Change Cipher Spec, Encrypted Handsh
108	179.031660	192.168.3.2	172.17.1.1	TCP	1053 > https [ACK] Seq=1 Ack=1 win=65535 Len=0
109	179.055932	192.168.3.2	172.17.1.1	SSL	Client Hello
110	179.055945	172.17.1.1	192.168.3.2	TCP	https > 1053 [ACK] Seq=1 Ack=121 win=5840 Len=0
111	179.056978	172.17.1.1	192.168.3.2	TLSv1	Server Hello, Change Cipher Spec, Encrypted Handsh
112	179.134371	192.168.3.2	172.17.1.1	TLSv1	Change Cipher Spec, Encrypted Handshake Message, A
113	179.135645	172.17.1.1	192.168.3.2	TLSv1	Application Data, [Unreassembled Packet (Incorrect

d. What two protocols are listed in this capture that were not listed in the previous capture?

e. Compare the first capture in Step 14 with the second capture. What is one noticeable difference between the HTTP and HTTPS protocols?

Step 15: Reflection

How are the OSI and TCP/IP Layer models reflected in the captured network data provided by Wireshark?

Erasing and Reloading the Switch

For the majority of the labs in CCNA Discovery, it is necessary to start with an unconfigured switch. Using a switch with an existing configuration may produce unpredictable results. The following instructions prepare the switch prior to performing the lab so that previous configuration options do not interfere. Instructions are provided for the 2900 and 2950 series switches.

- a. Enter into privileged EXEC mode by typing **enable**. If prompted for a password, enter **class** (if that does not work, ask the instructor).

```
Switch>enable
```

- b. Remove the VLAN database information file.

```
Switch#delete flash:vlan.dat
Delete filename [vlan.dat]?[Enter]
Delete flash:vlan.dat? [confirm] [Enter]
%Error deleting flash:vlan.dat (No such file or directory)
```

- c. Remove the switch startup configuration file from NVRAM.

```
Switch#erase startup-config
Erasing the nvram filesystem will remove all files! Continue? [confirm]
Erase of nvram: complete
```

- d. Check that VLAN information was deleted.
- e. Restart the software using the **reload** command.

- 1) At the privileged EXEC mode, enter the **reload** command:

```
Switch# reload
System configuration has been modified. Save? [yes/no]:
```

- 2) Type **n**, and then press **Enter**.

```
Proceed with reload? [confirm] [Enter]
Reload requested by console.
Would you like to enter the initial configuration dialog? [yes/no]:
```

- 3) Type **n**, and then press **Enter**.

```
Press RETURN to get started! [Enter]
```

Erasing and Reloading the Router

- a. Enter the privileged EXEC mode by typing **enable**.

```
Router>enable
```

- b. In privileged EXEC mode, enter the **erase startup-config** command.

```
Router#erase startup-config
Erasing the nvram filesystem will remove all files! Continue?
[confirm]
```

- c. Press **Enter** to confirm.

```
Erase of nvram: complete
```

- d. In privileged EXEC mode, enter the **reload** command.

```
Router# reload
System configuration has been modified. Save? [yes/no]:
```

- e. Type **n** and then press **Enter**.

- Proceed with reload? [confirm]
- f. Press **Enter** to confirm.
- Reload requested by console.
Would you like to enter the initial configuration dialog? [yes/no]:
- g. Type **n** and then press **Enter**.
- Press RETURN to get started!
- h. Press **Enter**.

SDM Router Basic IOS Configuration to Bring Up SDM

If the startup-config is erased in an SDM router, SDM will no longer come up by default when the router is restarted. It will be necessary to build a basic config as follows. Further details regarding the setup and use of SDM are can be found in the SDM Quick Start Guide:

http://www.cisco.com/en/US/products/sw/secursw/ps5318/products_quick_start09186a0080511c89.html#wp44788

- a. Set the router Fa0/0 IP address.

```
Router(config)#interface Fa0/0  
Router(config-if)#ip address 10.10.10.1 255.255.255.248  
Router(config-if)#no shutdown
```

- b. Enable the router's HTTP/HTTPS server, using the following Cisco IOS commands:

```
Router(config)#ip http server  
Router(config)#ip http secure-server  
Router(config)#ip http authentication local
```

- c. Create a user account with privilege level 15 (enable privileges).

```
Router(config)#username <username> privilege 15 password 0 <password>
```

- d. Configure SSH and Telnet for local login and privilege level 15.

```
Router(config)#line vty 0 4  
Router(config-line)#privilege level 15  
Router(config-line)#login local  
Router(config-line)#transport input telnet  
Router(config-line)#transport input telnet ssh  
Router(config-line)#exit
```