

# Packets and Frames

## 1 Introduction

This lab will explore some standard formats for packets and frames. The Ethernet/802.3 frames and Internet Protocol (IP) packet formats can be studied and examined. The Wireshark program will be utilized again for the task of capturing, and additionally examining the packets and frames. Please read the entire handout before beginning the lab.

## 2 Data Capture

1. Prepare the work area so the Vista Host, Linux Host and the switch are all on VLAN1 and it is active. (Appendix A)
2. Begin the Wireshark program and start it capturing from the Ethernet NIC.
3. Open a Command shell (cmd.exe) on the Vista Host and issue a PING to the switch's IP address.
4. Run the Telnet program in a command window on the Vista Host and open a session to the switch. Try an invalid password in the telnet session first (try the password "testingABC"), then use the correct password and logout afterwards. (Switch should have an address on VLAN1, and not shutdown)
5. Use the SSH program to ssh into the Linux Host. (Login: **misy** Password: **misy**)
6. In the command shell window, use the **tracert** program to trace a packet to the Linux Host.
7. Finally, issue a PING to a non-existent IP address (10.20.30.40) from the command shell.
8. Save the capture file for offline processing and stop the Wireshark program.

## 3 Data Analysis

Restart the Wireshark program and load the capture file using the File -> Open menu. Browse for the capture file, and disable the 3 filters on the Open Capture File window (MAC, network, and transport name resolutions). The frames in the capture file are default sorted by time. You can click on the Protocol column header and sort the captured frames by protocol types.

The screenshot shows the Wireshark interface with a packet capture sorted by protocol. The main pane displays a list of packets with columns for No., Time, Source, Destination, Protocol, and Info. The bottom pane shows the details of the selected packet (Frame 1), including Ethernet II, Logical-Link Control, and Spanning Tree Protocol fields.

No.	Time	Source	Destination	Protocol	Info
53	75.420280	00:0e:d7:79:04:81	01:00:0c:cc:cc:cc	CDP	Device ID: Switch
108	135.419714	00:0e:d7:79:04:81	01:00:0c:cc:cc:cc	CDP	Device ID: Switch
296	195.419150	00:0e:d7:79:04:81	01:00:0c:cc:cc:cc	CDP	Device ID: Switch
224	174.025923	10.101.0.10	255.255.255.255	DNS	Standard query A e
229	177.031095	10.101.0.10	255.255.255.255	DNS	Standard query A e
231	180.035270	10.101.0.10	255.255.255.255	DNS	Standard query A e
17	20.192115	00:0e:d7:79:04:81	01:00:0c:cc:cc:cc	DTP	Dynamic Trunking P
36	50.191835	00:0e:d7:79:04:81	01:00:0c:cc:cc:cc	DTP	Dynamic Trunking P
58	80.192549	00:0e:d7:79:04:81	01:00:0c:cc:cc:cc	DTP	Dynamic Trunking P
80	110.191271	00:0e:d7:79:04:81	01:00:0c:cc:cc:cc	DTP	Dynamic Trunking P
113	140.190991	00:0e:d7:79:04:81	01:00:0c:cc:cc:cc	DTP	Dynamic Trunking P
211	170.190705	00:0e:d7:79:04:81	01:00:0c:cc:cc:cc	DTP	Dynamic Trunking P
328	200.190422	00:0e:d7:79:04:81	01:00:0c:cc:cc:cc	DTP	Dynamic Trunking P
364	230.190141	00:0e:d7:79:04:81	01:00:0c:cc:cc:cc	DTP	Dynamic Trunking P
91	126.812428	10.101.0.3	10.101.0.10	ICMP	Echo (ping) reques
99	131.614582	10.101.0.3	10.101.0.10	ICMP	Echo (ping) reques
101	131.616494	10.101.0.10	10.101.0.3	ICMP	Echo (ping) reply

Frame 1 (60 bytes on wire, 60 bytes captured)

- IEEE 802.3 Ethernet
- Logical-Link Control
- Spanning Tree Protocol

```

0000  01 80 c2 00 00 00 0e d7 79 04 81 00 26 42 42  ..... .y...&BB
0010  03 00 00 00 00 80 01 00 0e d7 79 04 80 00 00  ..... ..y....
0020  00 00 80 01 00 0e d7 79 04 80 80 01 00 00 14 00  ..... y .....
0030  02 00 0f 00 00 00 00 00 00 00 00 00  ..... ..

```

File: "C:\Users\CPEG\AppData\Local\Temp\etherXXXa04044" 34 ... P: 385 D: 385 M: 0 Drops: 0

Figure 1: Frames Sorted by Protocol

You should verify that your capture file contains several frames of each type: ARP, STP, ICMP, Telnet, SSH (TCP port 22) and TCP. You may have other types of frames, but we will concentrate on these for this lab. The middle and bottom panels of the Wireshark window will now be examined. By mouse-clicking on a packet/frame in the top panel, you'll notice the middle and bottom panels change, reflecting data in the selected packet/frame. We'll examine the data presented in both of the bottom panels for each of the protocol types listed above. The middle panel lists standard fields and information about the selected packet, in a hierarchical form. By clicking on the "+" box in front of each of the top level information hierarchies, it will open to further information within those hierarchies. In the example of Figure 2, you can see the ARP packet is recognized as an Ethernet II frame, and within that hierarchy, it decodes the Source and Destination addresses, the protocol type, and the Ethernet trailer.

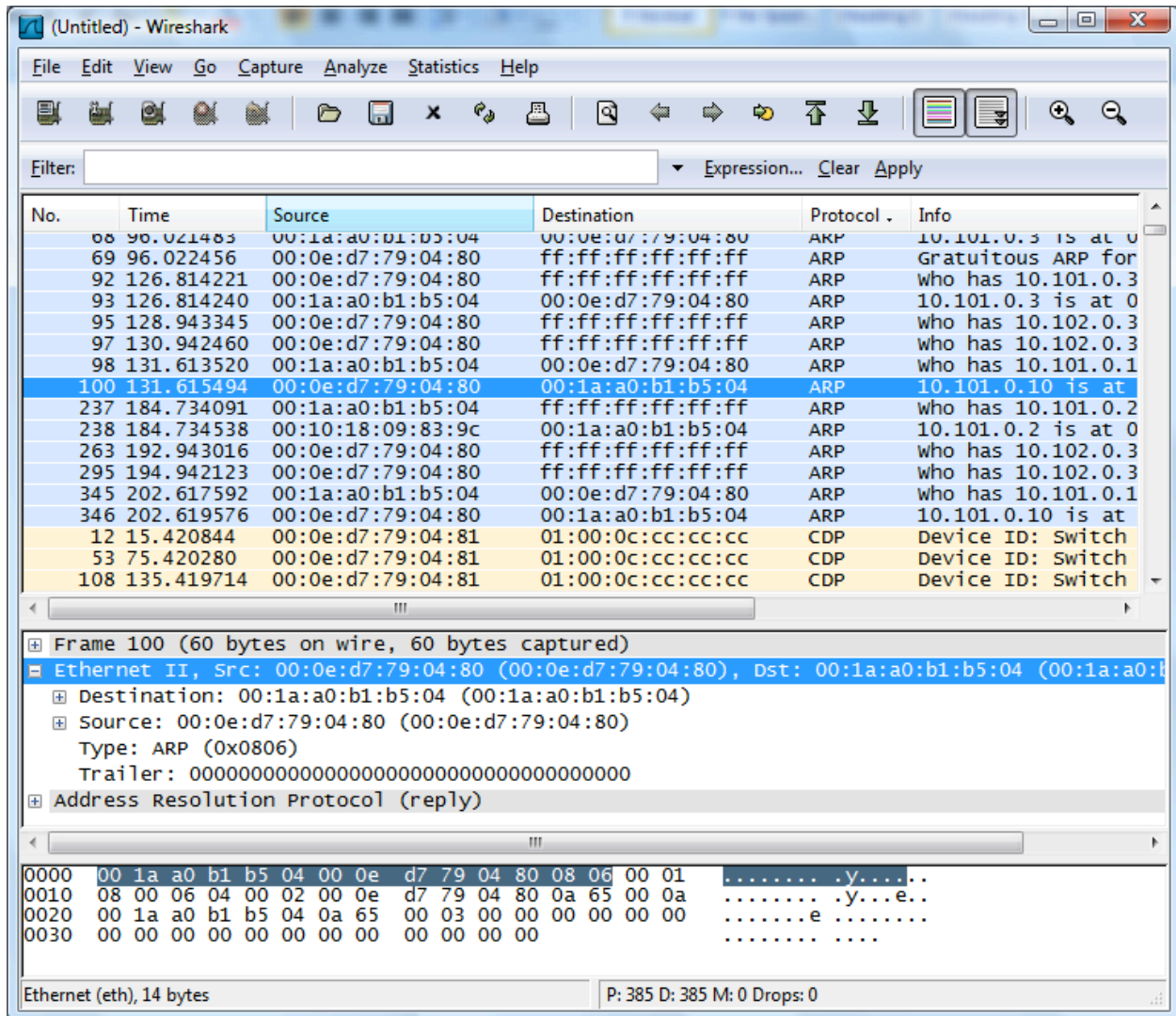


Figure 2: Ethernet II Hierarchy

The bottom panel of Ethereal is the raw packet data, displayed in 3 “columns”. The left hand side is a 4 byte hexadecimal address offset of the data within the packet, the middle lists the packet data in hexadecimal, and the right hand side attempts to display the hex data as an ASCII byte.

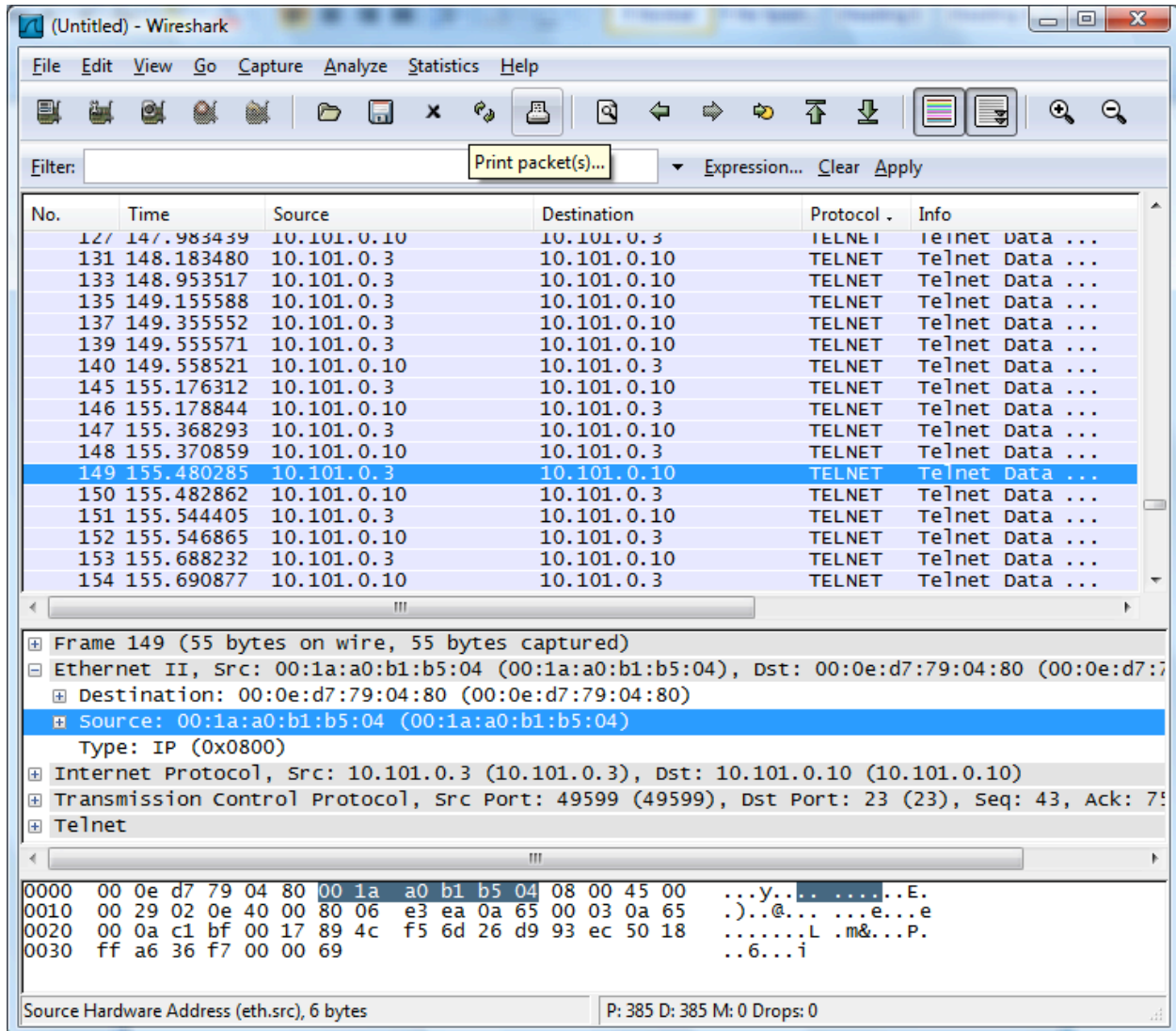


Figure 3: Raw Data Decoding

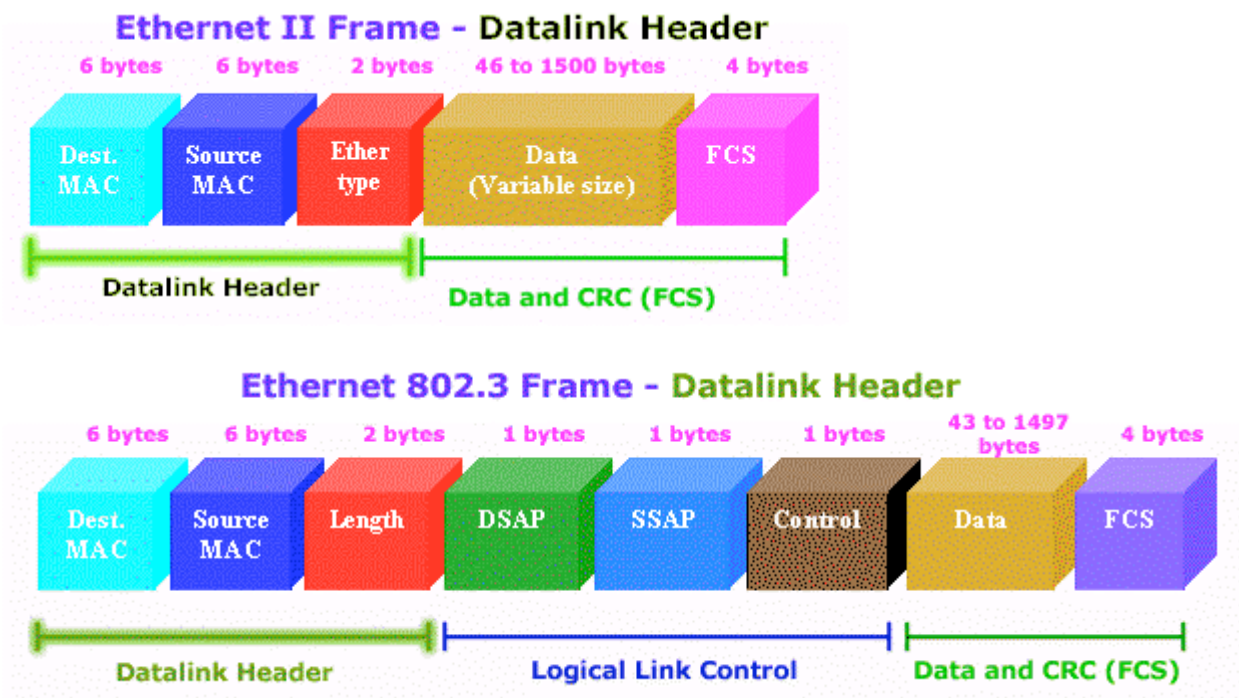
The packet raw data can be decoded with help from the middle frame's hierarchical information. Figure 3 shows a Telnet packet that is identified as an Ethernet II frame. By highlighting the **Source:** line in the middle panel, notice that the part of the raw packet that contains this information (Source Address) is highlighted in the bottom raw data panel.

## 4 Experiment

For a major portion of the lab report,

Use the Wireshark program to identify and decode as much information about a single packet/frame from each of the protocols named in the lab handout.

For a helpful reference, the Ethernet II and 802.3 are included here. (from <http://www.firewall.cx/>)



Please note that this portion should be explained in your own analysis, not as a collection of pictures and screen dumps.

## 5 Extension

With the captured packets sorted by protocol, within the same protocol, they are still sorted by time. With the knowledge that you've gotten from this lab and lecture, examine the Telnet sequence of packets captured, and try to identify data in the Telnet sequence that you typed in during the Data Capture portion of the lab. In addition, Wireshark provides a tool for following (reassembling) a TCP stream in the Analyze menu. Experiment with that tool and report your findings. Examine the SSH session in the same manner.

Provide screenshots of the Follow TCP Stream window for both the TELNET session and the SSH session.

## 6 Appendix

To set/verify the IP setup on the Linux Host, open a local terminal and run the following command to change the Linux Host's IP address to 10.10X.0.2 and configure a default route if needed.

```

misy@localhost ~ $ sudo /sbin/ifconfig eth0 10.10X.0.2 netmask
255.255.255.0
misy@localhost ~ $ sudo /sbin/route add default gw 10.10X.0.1

```