EL5373

INTERNET ARCHITECTURE AND PROTOCOLS

Runze Dong

N10264442

rdong@nyu.edu

46/50

Workstation: APAH Othello_I

MAC: f8:0f:41:c4:7f:aa

IP: 128.238.66.104

Lab Report 1

Due Sept 23, 2014

[5 pages]

Exercise 1&2

The default directory when you open a new command window is **/home/guest**

My working directory is **/home/guest/runze.**

I establish a directory, runze, with mkdir runze.

Exercise 3

The Internet service daemon, **xinetd,** started in system, with **PID: 997**

The **inetd** started in your system, with **PID: 997.**

-2 xinetd replaced inetd. both cannot start

Why?

xinetd (extended Internet daemon) is used to manages Internet-based connectivity. So it should be started in system when we log in our devices. And it also an extension to **inetd** in most modern Linux distributions.

Exercise 4

more /etc/services > ser_more

We compare the file ser_more with original more output, they contain exactly same contents.

cp /etc/services ser_cp.

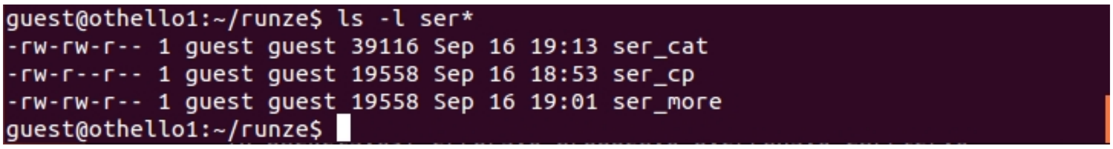
cmp ser_more ser_cp .

Nothing output. The two files are identical.

cat ser_more ser_cp > ser_ca

Ls -L ser*

sizes of these files following:



```
guest@othello1:~/runze$ ls -l ser*
-rw-rw-r-- 1 guest guest 39116 Sep 16 19:13 ser_cat
-rw-r--r-- 1 guest guest 19558 Sep 16 18:53 ser_cp
-rw-rw-r-- 1 guest guest 19558 Sep 16 19:01 ser_more
guest@othello1:~/runze$ 
```

Exercise 5

arp

Manipulate or display the kernel's IPv4 network neighbor cache. It can add entries to the table, delete ones or display the current ARP cache.

arping

Send an ARP request to a neighbor host. Ping destination on device interface by ARP packets, using source address.

ifconfig

Configure a network interface. Generally, it can display the status of the currently active interfaces and used to set up interface as necessary at boot time.

netstat

Display network connections, routing tables, interface statistics, masquerade connections, and multicast membership. Help user find problems in the network.

ping

Send ICMP ECHO_REQUEST to network hosts. It contains ICMP protocol's mandatory ECHO_REQUEST datagram to elicit an ICMP ECHO_REQUEST from a host or gateway. It's used to test the reach-ability of a host on IP network or to measure the round-trip time for a message from a host to destination.

route

Show or manipulate the IP routing table. Its primary use is to set up static routes to specific hosts or network via an interface after it has been configured.

tcpdump

Dump traffic on a network. It allows user to display TCP/IP or other packets being transmitted or received on a network. It also can be run with -w flag to save the packets data to a file for analysis.

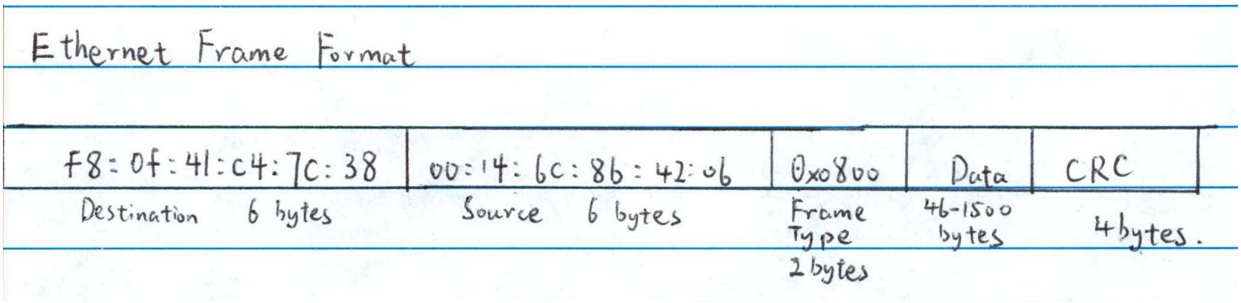
wireshark

It is a GUI network protocols analyzer. It allows user to browse packet data, which dump from a network.

Exercise 6

The format of the packet saved.

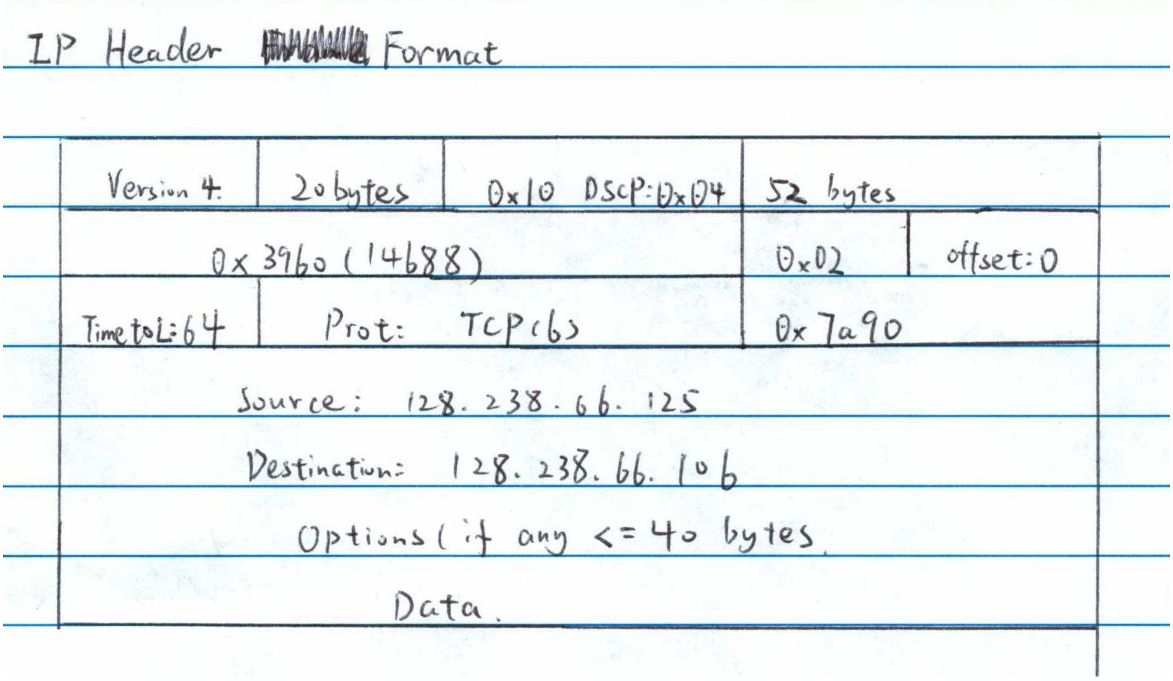
Ethernet Frame Format



Ethernet Frame Format

F8:0f:41:c4:7C:38	00:14:6c:86:42:06	0x0800	Data	CRC
Destination 6 bytes	Source 6 bytes	Frame Type 2 bytes	46-1500 bytes	4bytes.

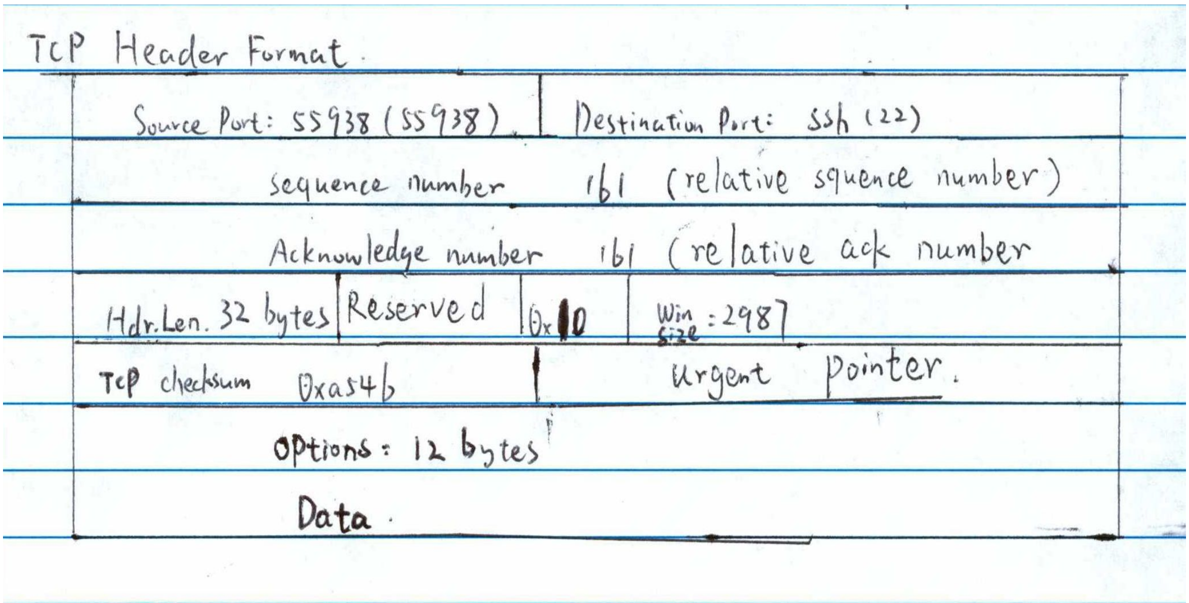
IP Header Format



IP Header Format

Version 4.	20 bytes	0x10 DSCP:0x04	52 bytes	
0x 3960 (14688)			0x02	offset:0
Time to L:64	Prot: TCP(6)		0x 7a90	
Source: 128. 238. 66. 125				
Destination: 128. 238. 66. 106				
Options (if any <= 40 bytes.				
Data.				

TCP Header Format



TCP Header Format.

Source Port: 55938 (55938).		Destination Port: ssh (22)	
sequence number 161 (relative squence number)			
Acknowledge number 161 (relative ack number			
Hdr.Len. 32 bytes	Reserved	0x10	Win size :2987
TCP checksum 0xa546		Urgent pointer.	
Options: 12 bytes			
Data.			

The value of the protocol field in the IP header of the packet is **<u>TCP(6).</u>**

The use of the protocol field is to indicate the upper layer protocol that is the source or destination of the data, 1 for ICMP, 2 for IGMP, 6 for TCP, and 17 for UDP.

Exercise 7

The value of the frame type field in an Ethernet frame carrying an ARP request is **0x0806.**

The value of the frame type field in an Ethernet frame carrying an ARP reply is **0x0806.**

The value of the frame type field in an Ethernet frame carrying an IP datagram captured in previous exercise is **0x0800.**

The use of the **frame type field** is used to identify the payload of the Ethernet frame.

Exercise 8

tcpdump udp port 520

Use tcpdump to capture packet only udp traffic on port 520

tcpdump -x -s 120 ip proto 89

Prints the packet in Hex, snap length is set to 120 bytes, and only captures ip traffic with protocol number 89.

tcpdump -x -s 70 host ip_addr1 and (ip addr_2 or ip_addr3)

Prints the packet in hex, snap length is set to 70 bytes, and only captures traffic from ip_addr1 and (ip_addr2 or ip_addr3).

Tcpdump -x -s 70 host ip_addr1 and not ip_addr2

Prints the packet in hex, snap length is set to 70 bytes, and only captures traffic form ip_addr1 and not ip_addr2.

Exercise 9

The port number used by remote computer is **23.**

The port number used by local computer is **53270.**

Remote computer's port number matches the port number listed for telnet in the /etc/services file.

Exercise 10

When we have two telnet sessions with the machine, the port number used on the remote machine is **23.**

Yes. Both sessions connect to the same port number, **23.**

53271 and 53272 are used in local machine for the first and second telnet.

The range of Internet-wide well-known port number is from **0 to 1023**

Generally, IANA has designated ports in the range **0...49151** as registered port numbers for specific services, and divided into well-known range **0...1023.**

-1

0 -> 255

255 -> 1023

The range of well-known port number for Unix/Linux specific service is **0...1023.**

The range for a client port number is from **49152 to 65535.**

-1

above 1023

Socket

A network socket is an endpoint of an inter-process communication flow across a network. a socket address is the combination of a port number and IP address. Based on this address, data packets are delivered to the appropriate application process.