EL5373
INTERNET ARCHITECTURE AND PROTOCOLS

Jiayang Sun

N19938926

Js8510@nyu.edu

Workstation: Ophelia1

Mac: f8:0f:41:c3:88:0d

IP: 128.238.66.103

Lab Report 1

Due Oct 2, 2015

Exercise 1

Login to the system. The login ID is guest, and the login password is guest1.

Exercise 2

My default home directory is /home/guest

My working directory /home/guest/jiayang_FE. With commend *mkdir*, I created this directory.

Exercise 3

Xineted is running and whose pid=997

Ineted is not running.

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

guest@ophelia1:~/jiayang_FE/lab0$ ls -l

total 88

-rw-rw-r-- 1 guest guest 0 Sep 18 19:04 ex4

-rw-rw-r-- 1 guest guest 162 Sep 18 18:58 README.md

-rw-rw-r-- 1 guest guest 158 Sep 18 18:55 README.md~

-rw-rw-r-- 1 guest guest 39116 Sep 18 19:10 ser_cat

-rw-rw-r-- 1 guest guest 19558 Sep 18 19:08 ser_copy

-rw-rw-r-- 1 guest guest 19558 Sep 18 19:06 ser_more

Q1: *cmp ser_more ser_cp*

No output. According to the man page, no output means these two files are identical.

Q2: What are the sizes of ser_more, ser_cp, and ser_cat?

ser_more & ser_cp: *19558 bytes, ser_cat: 39116 bytes*

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

(a)

Ethernet Frame Format

Destination Address	Source Address	Frame Type	Data	CRC
6 bytes	6 bytes	2 bytes	46-1500 bytes	4 bytes
F8:0f:41:c3:88:0d	F8:0f:41:c4:7f:aa	2048(0x0800)		

IP Header Format

Version: 4	Hdr len: 20 bytes	Differentiated Services: 0x10 (16)	Total Length: 52bytes
Identification: 34877		Flag: 0x02 (2)	Fragment Offset: 0
Time to Live: 64	Protocol: 6 (TCP)	Header Checksum: 25713 (0x2bcb)	
Source IP Address: 128.238.66.103			
Destination IP Address: 128.238.66.104			
Options (if any, <=40 bytes)			
Data			

TCP header Format

Source Port Number: 40418		Destination Port Number: 23	
Sequence Number: 3			
Acknowledgement Number: 3			
Hdr Len: 32 bytes	Reserved	Flags: 0x010 (ACK)	Window Size: 304
TCP Checksum: 0x86d2		Urgent Pointer: 0	
Options(if any): 12 bytes			
Data			

(b)

The value in the protocol field is 6(TCP 6).

This value is used to indicate the upper layer the upper layer protocol. 1 for ICMP, 2 for IGMP, 6 for TCP, and 17 for UDP.

Exercise 7

(a)

The frame type value in an Ethernet frame carrying an ARP request is 0x86.

The frame type value in an Ethernet frame carrying an ARP reply is 0x86.

(b)

The frame type value in previous exercise is 0x0800

(c)

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

Exercise 8

tcpdump udp port 230

Use tcpdump to capture only udp traffic packet on port 520.

sudo tcpdump -x -s 120 ip proto 89

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

sudo tcpdump -s 70 host ip_addr1 and (ip_addr2 or ip_addr3)

To print 70 bytes from ip_addr1 and (ip_addr2 or ip_addr3)

sudo tcpdump host ip_addr1 and not ip_addr2

To print all IP packets between host ip_addr1 and any host expect ip_addr2

Exercise 9

The port number of remote computer is 23.

The port number of local computer is 40418.

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

Exercise 10

(a) When I have telnet sessions with remote machine, the port number in remote machine is 23. Yes, both sessions connect to the same port.

(b) 40418 and 40427 are used for two clients.

(c) The range of Internet-wide well-known port number is 0 ~ 1023.

The range of well-known port numbers for Unix/Linux specific services 0~1023.

The range for a client port number is 49152~65535

Yes, they are constant.

(d) A socket is and endpoint instance define by and IP address and a port in the context of either a particular connection or the listening state. A port is a virtualization identifier defining a service endpoint. A socket is not a connection, it is the endpoint of a specific connection. There can only be one listener socket for a given address/port combination.