

CSP334: Computer Networks, Lab Assignment No 2, Assignment on Linux Networking Commands

Rahul Byas Sherwan
Entry No. : 2016UCS0028

1: The First Problem

Note : If the screenshot is not available in the subparts below then it is because I am not able to find the file(iam using ubuntu 16.04 lts).So, in that case i have gathered information from internet and wrote that after understanding it.

(a) /etc/hosts:

/etc/hosts is an operating system file that translate hostname or domain names to IP addresses.

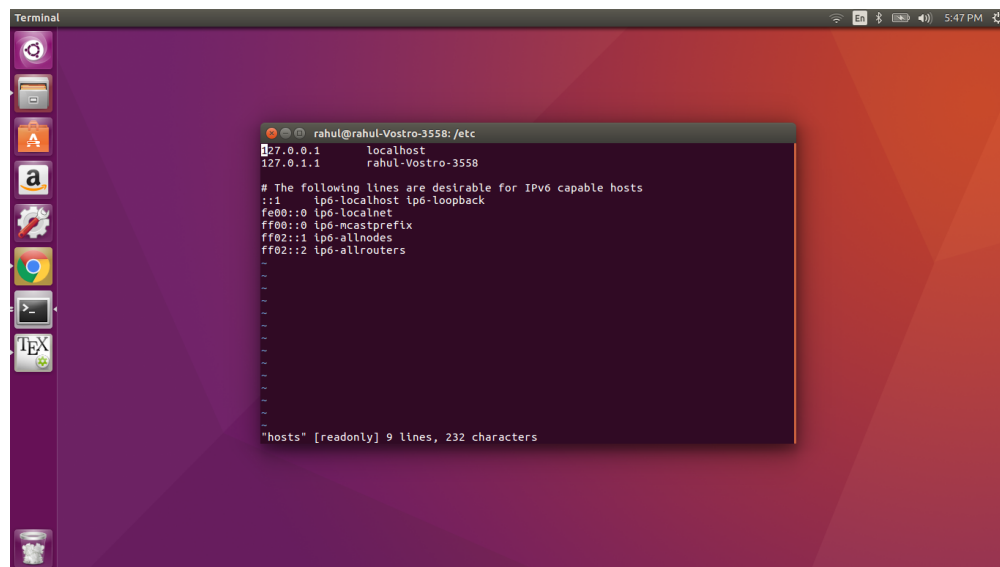


Figure 1: hosts file

As we can see a hosts file ,in the screenshot above,notice that 127.0.0.1 is written which is an IP address and many other addresses.So,the IP address 127.0.0.1 is a special-purpose IPv4 address called localhost or loopback address.

(b) /etc/sysconfig/network:

Used to specify information about the desired network configuration on our server. The following entries from /etc/sysconfig/network define that IPv4 networking is enabled, IPv6 networking is not enabled, the host name of the system, and the IP address of the default network gateway:

```
NETWORKING = yes
NETWORKING_IPV6 = no
HOSTNAME = host20.rahul.com
GATEWAY = 192.168.1.1
```

(c) /etc/sysconfig/network-scripts/ifcfg-eth0:

It controls the first Ethernet network interface card or NIC in the system. In a system with multiple NICs, there are multiple ifcfg-ethX files (where X is a unique number corresponding to a specific interface). Because each device has its own configuration file, an administrator can control how each interface functions individually.

(d) /etc/default-route:

The default route is a setting on a computer that defines the packet forwarding rule to use when no specific route can be determined for a given Internet Protocol (IP) destination address. All packets for destinations not established in the routing table are sent via the default route. The default route generally points to another router, which treats the packet the same way: if a route matches, the packet is forwarded accordingly, otherwise the packet is forwarded to the default route of that router.

(e) /etc/resolv.conf:

resolv.conf is the name of a computer file used in various operating systems to configure the system's Domain Name System (DNS) resolver.

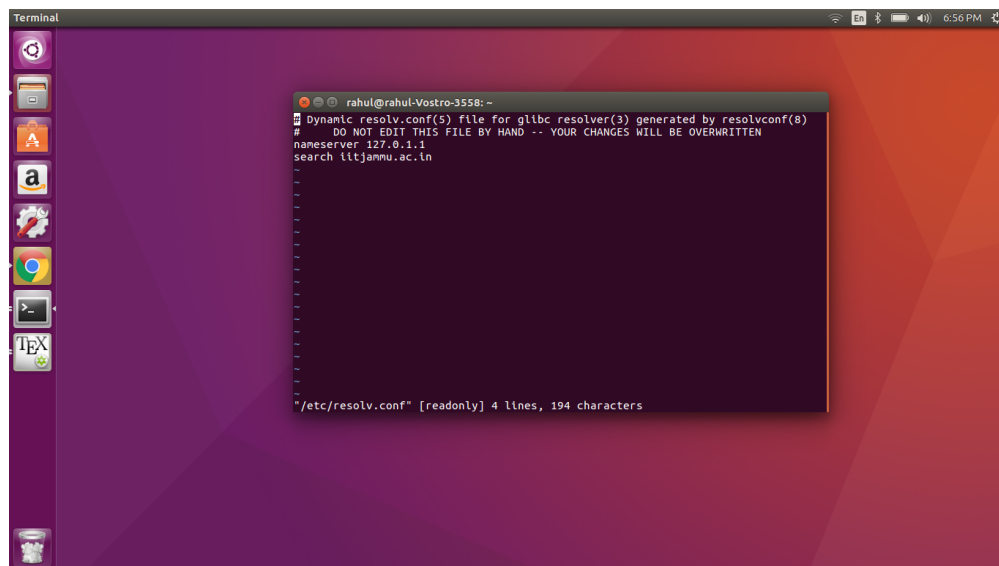


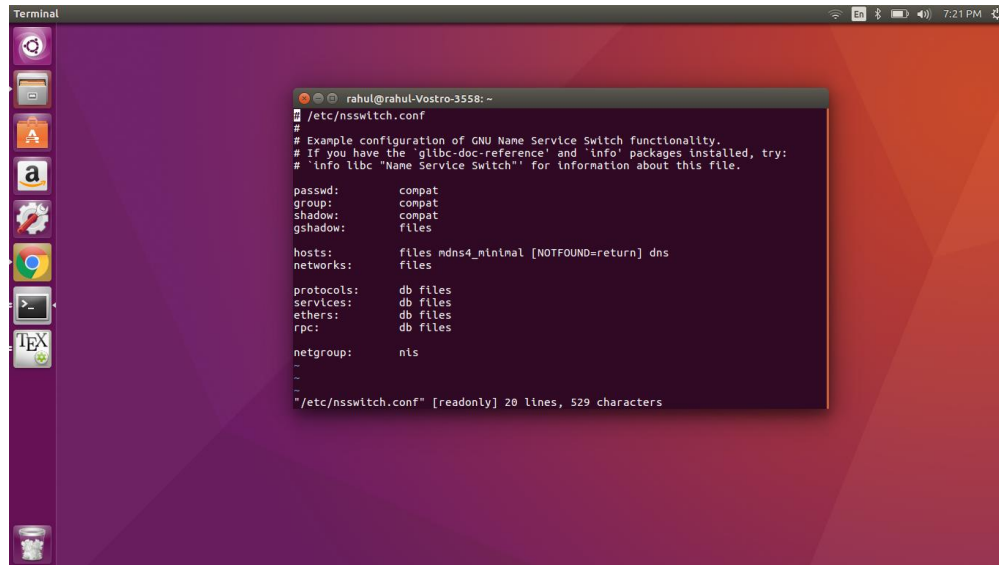
Figure 2: resolv.conf

As you can see in the above screenshot, the file resolv.conf typically contains directives that specify the default search domains, in my case it is iitjammu.ac.in.

(f) /etc/nsswitch.conf

The /etc/nsswitch.conf file defines the order in which to contact different name services. For Internet use, it's important that dns shows up in the "hosts" line. This instructs your computer

to look up hostnames and IP addresses first in the `/etc/hosts` file, and to contact the DNS server if a given host does not occur in the local hosts file.



The image shows a terminal window on a Linux desktop. The terminal title is "rahul@rahul-Vostro-3558: ~". The command `# /etc/nsswitch.conf` has been entered, and the output shows the configuration of the GNU Name Service Switch. The configuration includes settings for passwd, group, shadow, gshadow, hosts, networks, protocols, services, ethers, rpc, and netgroup. The hosts and networks lines are highlighted in blue. The terminal also shows the file path `"/etc/nsswitch.conf" [readonly] 20 lines, 529 characters`.

```
# /etc/nsswitch.conf
# Example configuration of GNU Name Service Switch functionality.
# If you have the 'glibc-doc-reference' and 'info' packages installed, try:
# 'info libc "Name Service Switch"' for information about this file.

passwd:         compat
group:          compat
shadow:         compat
gshadow:        files

hosts:          files mdns4_minimal [NOTFOUND=return] dns
networks:       files

protocols:      db files
services:       db files
ethers:         db files
rpc:            db files

netgroup:       nis

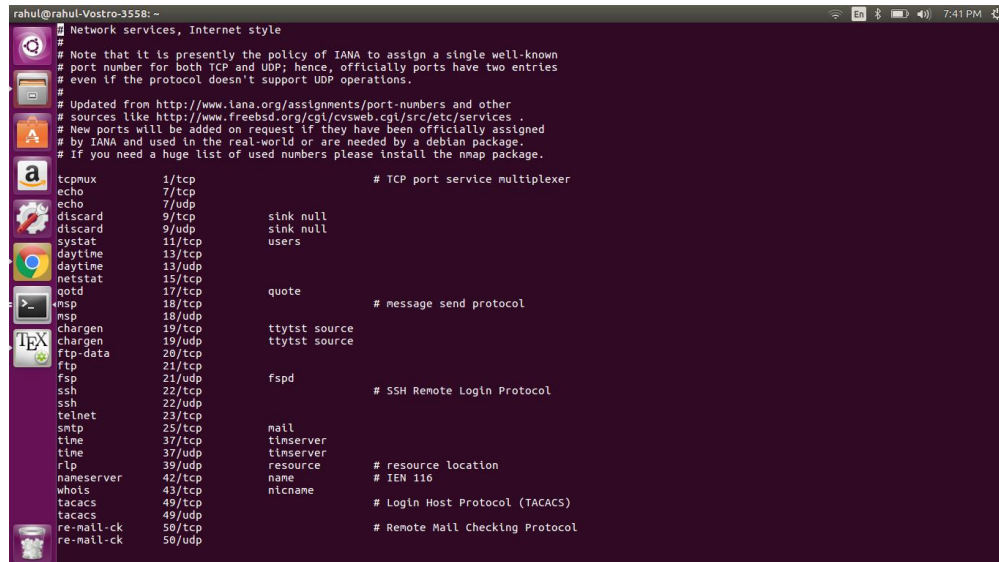
"/etc/nsswitch.conf" [readonly] 20 lines, 529 characters
```

Figure 3: nsswitch.conf

2: The second problem

(a) Screenshots of services file:

Since the file content is quiet large . So, I have clicked 3 important parts of the file .In "service file b." (figure 5) you can notice the port no. of famous server (http) which is 80.

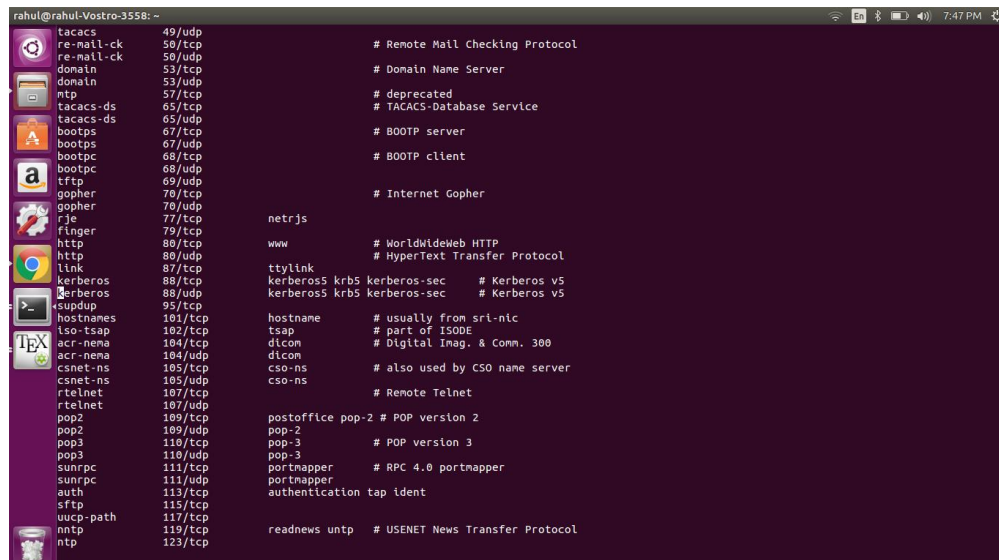


```

rahul@rahul-Vostro-3558:~$ cat /etc/passwd
# Network services, Internet style
#
# Note that it is presently the policy of IANA to assign a single well-known
# port number for both TCP and UDP; hence, officially ports have two entries
# even if the protocol doesn't support UDP operations.
#
# Updated from http://www.iana.org/assignments/port-numbers and other
# sources like http://www.freebsd.org/cgi/cvsweb.cgi/src/etc/services .
# New ports will be added on request if they have been officially assigned
# by IANA and used in the real-world or are needed by a debian package.
# If you need a huge list of used numbers please install the nmap package.
tcpmux      1/tcp          # TCP port service multiplexer
echo        7/tcp
echo        7/udp
discard     9/tcp          sink null
discard     9/udp          sink null
sysstat     11/tcp
daytime     13/tcp
daytime     13/udp
netstat     15/tcp
qotd        17/tcp
nsp         18/tcp          # message send protocol
nsp         18/udp
chargen     19/tcp          ttytst source
chargen     19/udp          ttytst source
ftp-data    20/tcp
ftp         21/tcp
ftp         21/udp          fsp
ssh         22/tcp          # SSH Remote Login Protocol
ssh         22/udp
telnet      23/tcp
smtp        25/tcp          mail
time        37/tcp          tinserver
time        37/udp          tinserver
rtp         39/udp          resource
nameserver  42/tcp          name
whois       43/tcp          ntcname
tacacs      49/tcp          # Login Host Protocol (TACACS)
tacacs      49/udp
re-mail-ck  50/tcp          # Remote Mail Checking Protocol
re-mail-ck  50/udp

```

Figure 4: services file a.



```

rahul@rahul-Vostro-3558:~$ cat /etc/passwd
tacacs      49/udp          # Remote Mail Checking Protocol
re-mail-ck  50/tcp
re-mail-ck  50/udp
domain      53/tcp          # Domain Name Server
domain      53/udp
ntp         57/tcp          # deprecated
tacacs-ds   65/tcp          # TACACS-Database Service
tacacs-ds   65/udp
bootps      67/tcp          # BOOTP server
bootps      67/udp          # BOOTP client
bootpc      68/tcp
bootpc      68/udp
rtftp       69/udp
gopher      70/tcp          # Internet Gopher
gopher      70/udp
rje         77/tcp
finger      79/tcp
http        80/tcp          www
http        80/udp          # WorldWideWeb HTTP
link        87/tcp          # HyperText Transfer Protocol
kerberos    88/tcp          kerberos5 krb5 kerberos-sec # Kerberos v5
kerberos    88/udp          kerberos5 krb5 kerberos-sec # Kerberos v5
supdup      95/tcp
hostnames   101/tcp
iso-tsap    102/tcp          tsap
acr-nema    104/tcp          dicon
acr-nema    104/udp
csnet-ns    105/tcp          cso-ns
csnet-ns    105/udp          # also used by CSO name server
rtelnet     107/tcp          # Remote Telnet
rtelnet     107/udp
pop2        109/tcp          postoffice pop-2 # POP version 2
pop2        109/udp
pop3        110/tcp          pop-2
pop3        110/udp          pop-3
sunrpc      111/tcp          portmapper
sunrpc      111/udp          # RPC 4.0 portmapper
auth        113/tcp          portmapper
sftp        115/tcp          authentication tap ident
uucp-path   117/tcp
nnntp       119/tcp
nntp        123/tcp          readnews untp # USENET News Transfer Protocol

```

Figure 5: services file b.

```
rahul@rahul-Vostro-3558: ~
# Kerberos (Project Athena/MIT) services
# Note that these are for Kerberos v4, and are unofficial. Sites running
# v4 should uncomment these and comment out the v5 entries above.
#
kerberos4 750/udp      kerberos-lv kdc # Kerberos (server)
kerberos4 750/tcp      kerberos-lv kdc # Kerberos authentication
kerberos-master 751/tcp    kerberos-master # Kerberos authentication
passwd-server 752/udp    passwd_server # Kerberos passwd server
krb_prop 754/tcp    krb_prop krb5_prop hprop # Kerberos slave propagation
krbupdate 760/tcp    kreg # Kerberos registration
swat 901/tcp    # swat
kpop 1109/tcp    # Pop with Kerberos
knetd 2053/tcp    # Kerberos de-multiplexor
zephyr-srv 2102/udp    # Zephyr server
zephyr-clt 2103/udp    # Zephyr serv-hm connection
zephyr-hm 2104/udp    # Zephyr hostmanager
eklogin 2105/tcp    # Kerberos encrypted rlogin
# Hmm. Are we using Kv4 or Kv5 now? Worrying.
# The following is probably Kerberos v5 --- ajt@debian.org (11/02/2000)
kx 2111/tcp    # X over Kerberos
kprop 2121/tcp    # Incremental propagation
#
# Unofficial but necessary (for NetBSD) services
#
supfilesrv 871/tcp    # SUP server
supfiledbg 1127/tcp    # SUP debugging
#
# Services added for the Debian GNU/Linux distribution
#
linuxconf 98/tcp    # LinuxConf
poppassd 106/tcp    # Eudora
poppassd 106/udp
moira-db 775/tcp    # Moira database
moira-update 777/tcp    # Moira update protocol
moira-ureg 779/udp    # Moira user registration
spand 783/tcp    # spanassassin daemon
onlrr 808/tcp    onlrrd # online mirror
onlrr 808/udp    onlrrd
customs 1001/tcp    # pnae customs server
```

Figure 6: services file c.

(b) Use of services file:

It stores information about numerous services that client applications might use on the computer. Within the file is the service name, port number and protocol it uses.

The port numbers are mapped to specific services. However, the UNIX operating system's services file does not include IP addresses but instead information like whether the service is TCP or UDP and what common names it might go by.

(c) Which layer in the TCP/IP protocol stack do you think would make use of this file ?:

Answer: Application layer.

(d) Are the port numbers shown in this file well-known port numbers or ephemeral port numbers ? Why are they so ?:

Answer: As we know that well known port numbers are upto 1023 and well registered port numbers are from 1024 - 49000(approx.) and finally comes the dhcp which is from 49000 to 65534 . So, as we can see in the screenshots above , we have both well-known port numbers and ephemeral port numbers.

3: The third problem

Command	Purpose	Data Link Layer	Network Layer	Transport Layer	Network Interface Configuration
arp	To map IP network addresses to the hardware addresses	YES	NO	NO	NO
arping	To send arp request to a neighbour host	YES	NO	NO	NO
ifconfig	To view and change the configuration of network interface	NO	NO	NO	YES
tcpdump	To capture or filter TCP/IP packets that received or transferred over a network on a specific interface	NO	YES	NO	NO
ping	To test the reachability of a host on an IP network	NO	YES	NO	NO
netstat	To print network connections, routing tables, interface statistics etc	NO	NO	YES	NO
route	To edit kernel routing tables	NO	YES	NO	NO

4: The fourth problem

Given below are some screenshots of remote connections establishment check. In figure-7 as we can see that ping is working properly. In figure - 9 we can see the packages captured tcpdump packages (which is further written in a file named as "four.pcap") opened in wireshark.

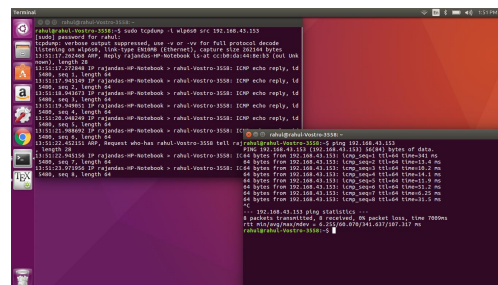


Figure 7: tcpdump and ping command

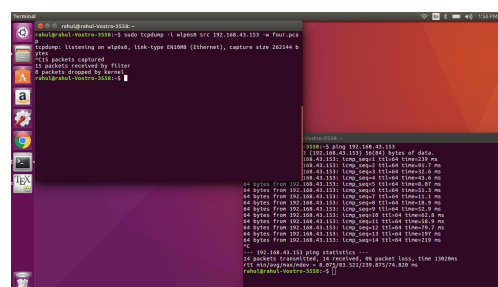


Figure 8: tcpdump packets being saved in four.pcap file

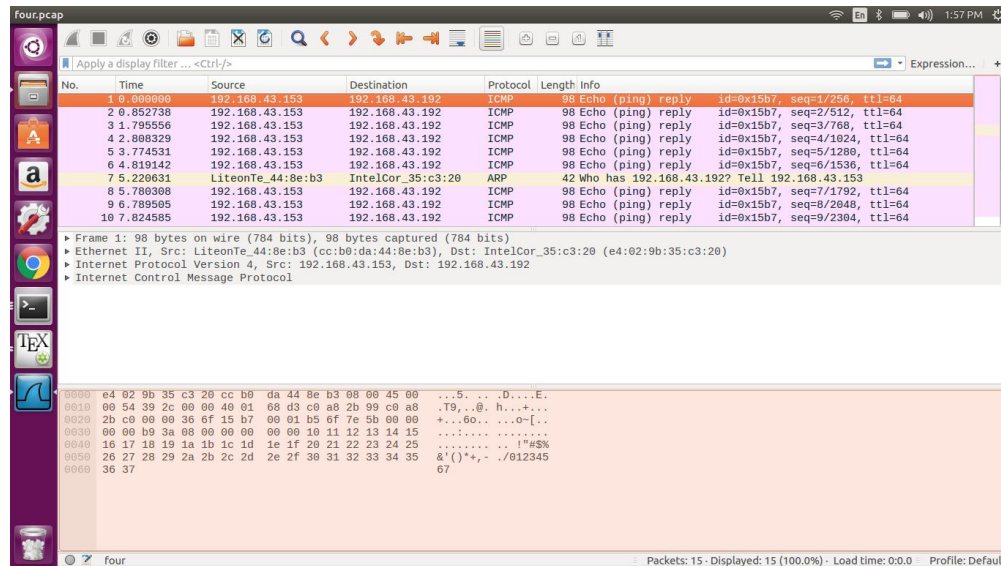


Figure 9: captured packages written in four.pcap file

5: The fifth problem

QUESTION: Run the command `tcpdump enx w exe5.out`. Do you see any output on the screen ? Why ?

ANSWER: After running the command , it says : "tcpdump: listening on wlp6s0, link-type EN10MB (Ethernet), capture size 262144 bytes" and writes the data into exe5.out. Here -enx is used for ethernet network.

Except these things ,we don't see any thing on the screen as the packages captured are being written to exe5.out file.

Here wlp6s0 is the wireless network interface which enables wifi.

6: The sixth problem

Some screenshots

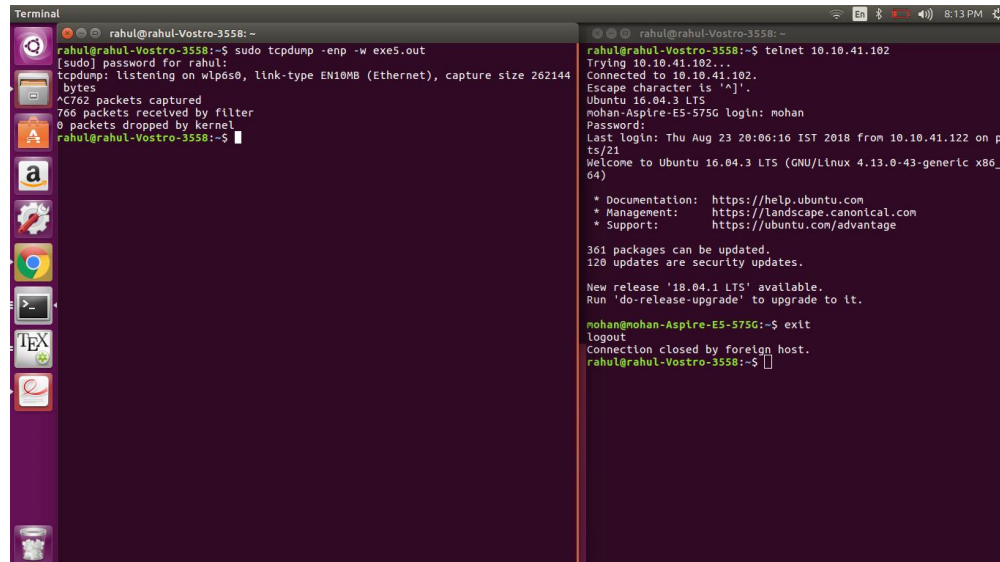


Figure 10: remote accessing

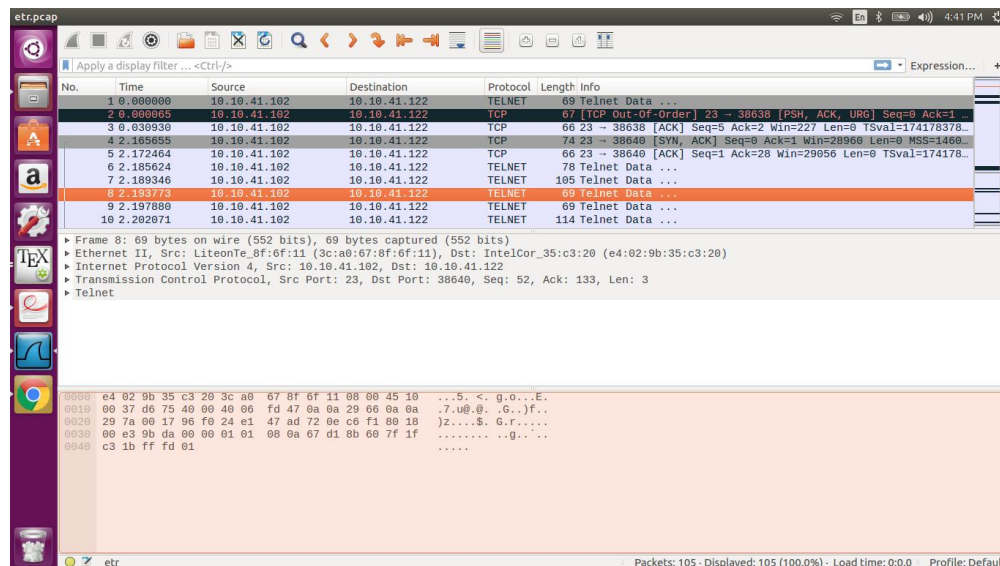


Figure 11: captured packages

(a) Draw the format of the packet you saved, including the link, IP, and TCP headers (See Figs in the handouts given to you for reference), and identify the value of each field in these headers.

Table 1: IP header format

Version:4	Hdrlen 20bytes(5)	DifrentiatedServices:0x10()	TotalLength:55	
Identification:0xe51b(58651)			Flag:0x02(Don't Fragment	FragementOffset:0
TimeToLive:64		Protocols:TCP (6)	HeaderChecksum:0xeea1	
Source IP Address:10.10.41.102				
Destination IP Address:10.10.41.122				
Options				
Data				

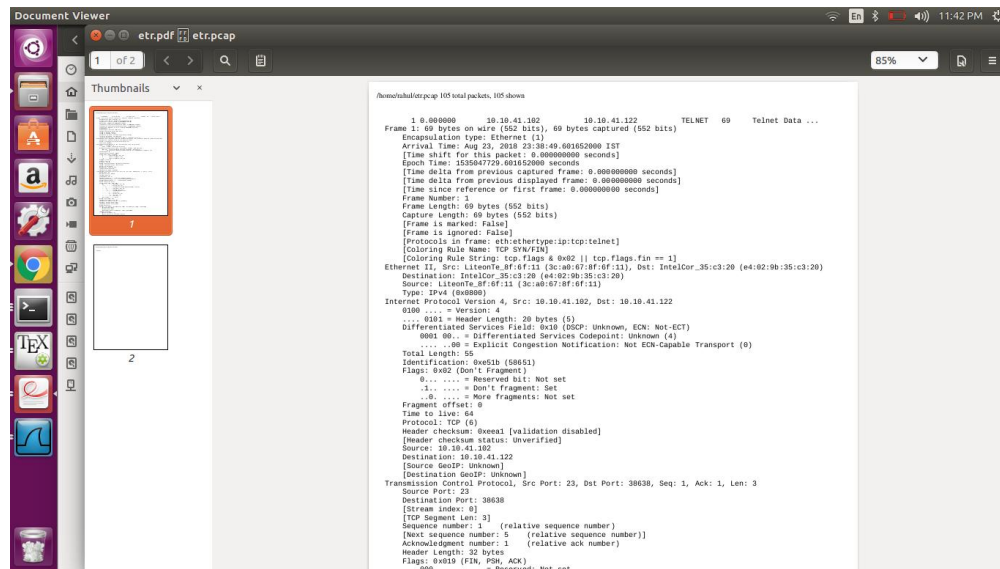


Figure 12: headers

Table 2: TCP header format

Source Port Number:23			Destination Port Number:38638		
Sequence Number:1					
Acknowledgement Number:1					
Hdr Len:32 bytes	Reserved:Not Set	Flags:0x019 (FIN, PSH, ACK)		Window Size:227	
Tcp CheckSum:0xa4ad				Urgent Pointer:0	
Options:(12 bytes), No-Operation(NOP) , No-Operation(NOP)					
Data:					

Table 3: Link header format

IntelCor ₃₅ : c3 : 20 (e4:02:9b:35:c3:20)	LiteonTe _{8f} : 6f : 11 (3c:a0:67:8f:6f:11)	FT:IPv4	Data	CRC
--	--	---------	------	-----

(b) What is the value of the protocol field in the IP header of the packet you saved?

What is the use of the protocol field?

The field value is : 6. It is used to indicate the type of data found in the portion of the datagram.

7: The seventh problem

(a) What is the value of the frame type field in an Ethernet frame carrying an ARP request and in an Ethernet frame carrying an ARP reply, respectively?

Answer: Type: ARP (0X0806)

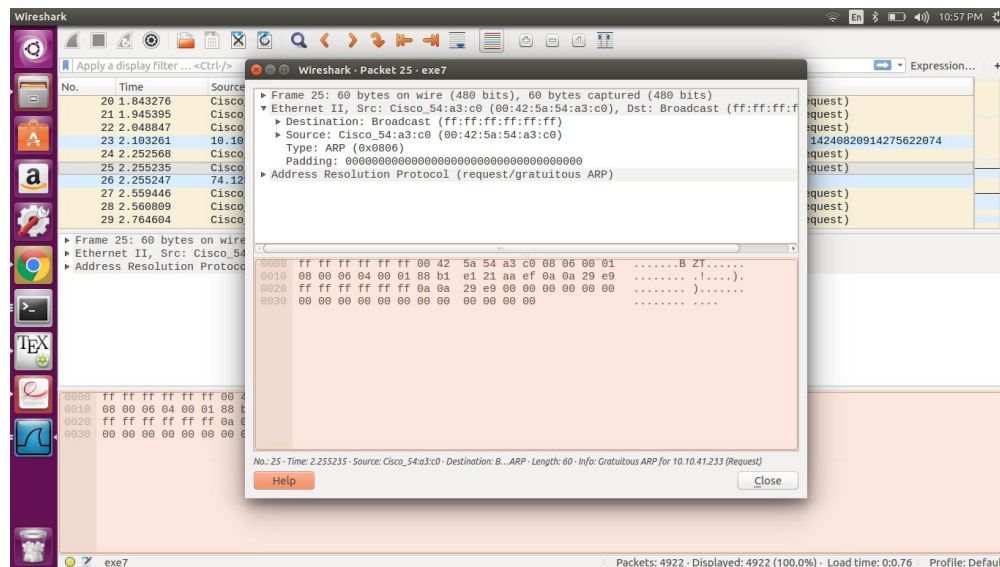


Figure 13: ethernet frame type

(b) What is the value of the frame type field in an Ethernet frame carrying an IP datagram captured in the previous exercise?

Answer: Type: IPv4 (0X0800)

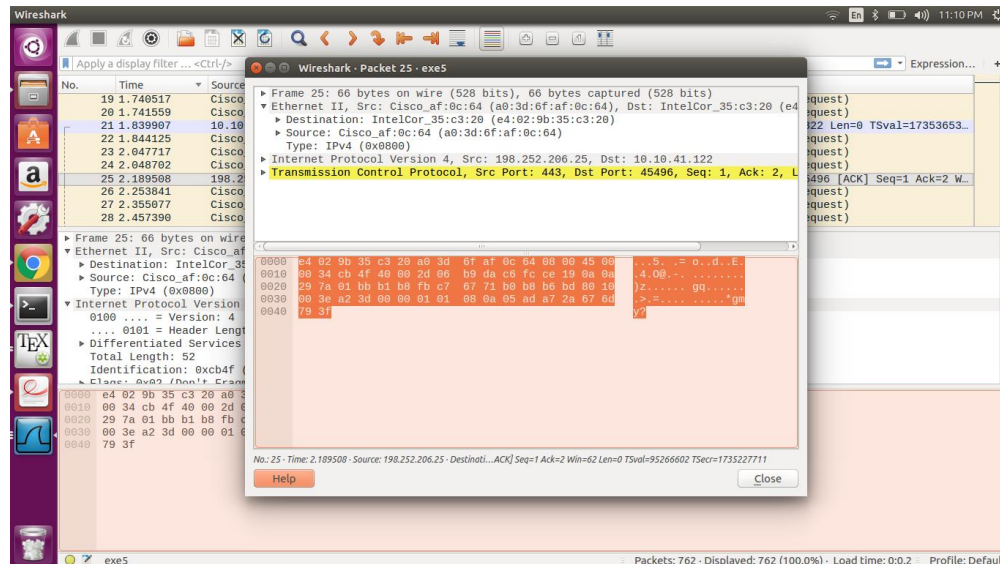


Figure 14: ethernet frame type

(c) What is the use of the frame type field?

Answer: It carries small but useful information. It allows to recognize the many protocols that may go over Ethernet, be it IPv4, ARP, IPv6, IPX, AppleTalk, and so on.

8: The eighth problem

man page of tcpdump

(a) tcpdump udp port 520:

tcpdump udp command by default captures the traffic of udp port 80. Since, the command is tcpdump udp port 520 implies that it captures the traffic of udp port 520.

(b) tcpdump -x -s 120 ip proto 89:

-x: It print the data of each packet (minus its link level header) in hex.

-s 120 : It is for snaplen of 120 bytes.

ip proto 89: is for IP protocol number 89.

So, tcpdump -x -s 120 ip proto 89 means it outputs the packets in hex whose snaplen is of 120 bytes and only uses IP number 89 for capturing the traffic.

(c) tcpdump -x -s 70 host ip addr1 and (ip addr2 or ip addr3):

As explained in above part .So, tcpdump -x -s 70 host ip addr1 and (ip addr2 or ip addr3) means it outputs the packets in hex whose snaplen is of 70 bytes and only uses IP addr1 and (ip addr2 or ip addr3) for capturing the traffic.

(d) tcpdump -x -s 70 host ip addr1 and not ip addr2:

As the command itself suggests it prints the packets in hex whose snaplen is of 70 bytes and only uses IP addr1 and not ip addr2 for capturing the traffic.

9: The ninth problem

(a) What are the port numbers used by the remote and the local computer?:

Answer : Remote machine's port number : 23

Local machine's port number : 37838

(b) Which machine's port number matches the port number listed for telnet in the /etc/services file?:

Answer : Remote machine's port number matches the port number listed for telnet. (as you can see in the screenshot below)

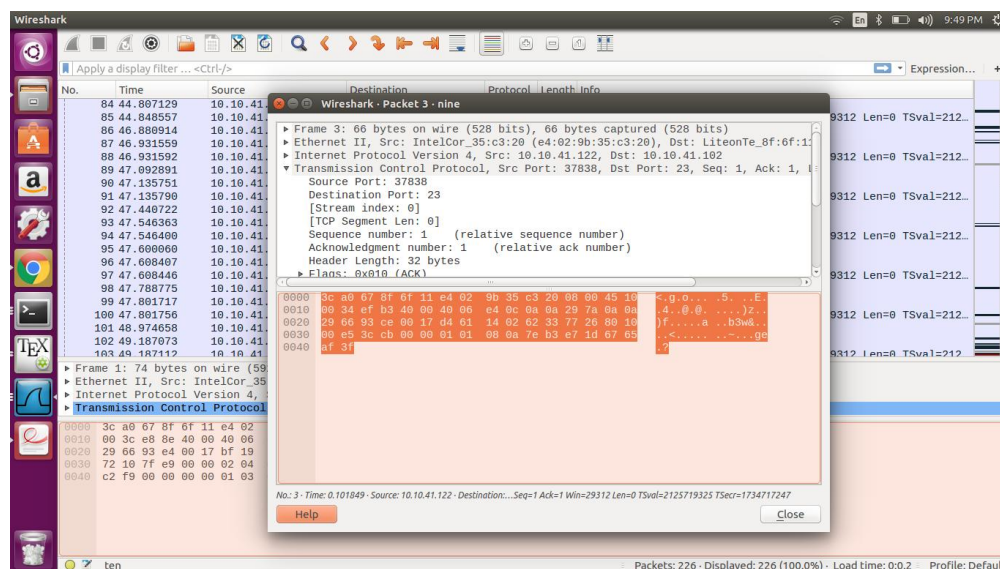


Figure 15: captured packages

10: The tenth problem

(a) When you have two telnet sessions with your machine, what port number is used on the remote machine? Are both sessions connected to the same port number on the remote machine?:

Answer: Even in case of two telnet session , the remort machine has a single port number ,i.e. 23 (remote machine's port number).

Yes, both sessions connected to the same port number on the remote machine.(as one can notice in the screenshot given below).

(b) What port numbers are used in your machine for the first and second telnet, respectively?:

Answer: For our machine ,
the first session's port number is : 37860
the first session's port number is : 37862
(one can verify it by the image given below)

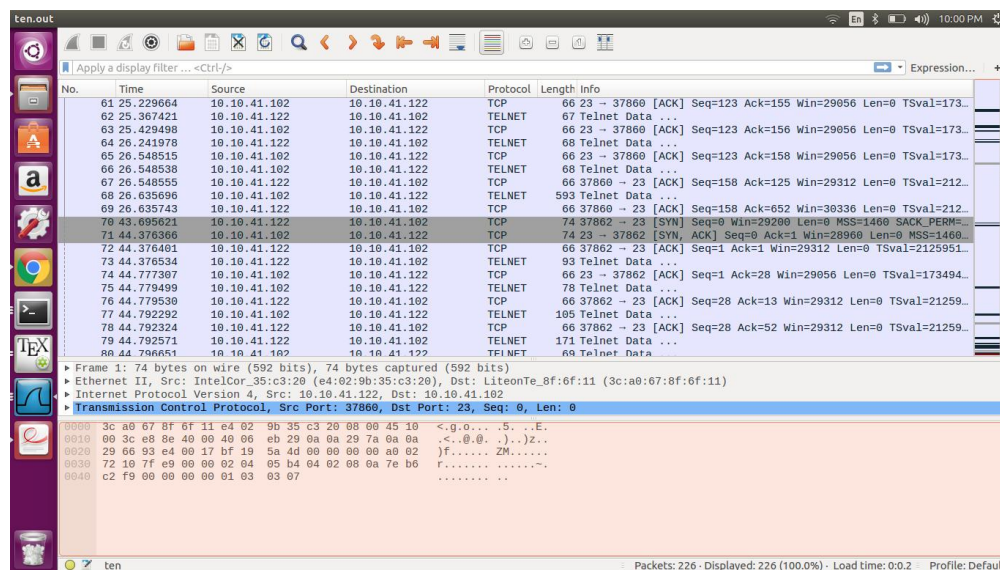


Figure 16: captured packages

(c) What is the range of Internet-wide well-known port numbers? What is the range of well-known port numbers for Unix/Linux specific service? What is the range for a client port number? Compare your answer to the well-known port numbers defined in the /etc/services file. Are they consistent? In case they are not, try to discuss amongst peers and specify your view of the reason why they are not.:

Answer: The well-known ports cover the range of possible port numbers from 0 through 1023. The client ports cover the range of possible port numbers from 49152 to 65535.No,they are not consistent.It is because of the fact that Unix/Linux specific services run on these ports .