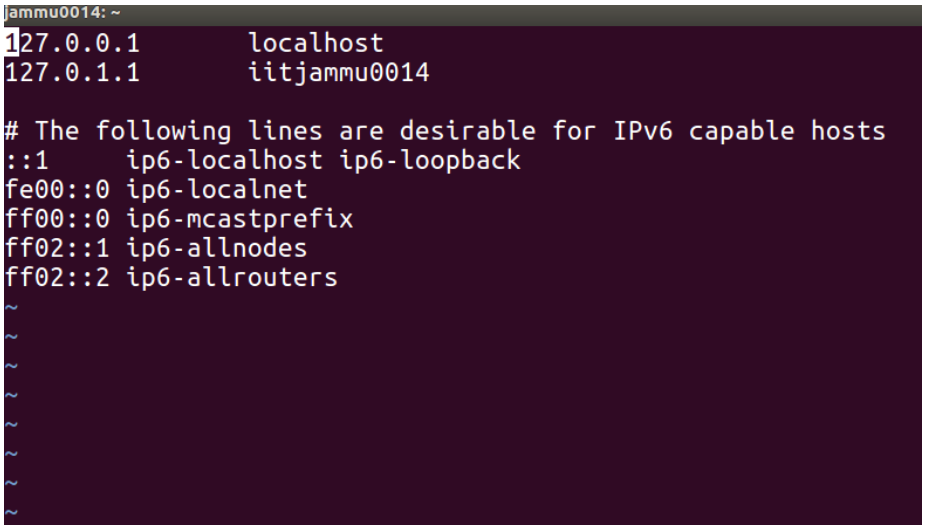
CSP334 : Computer Networks
Lab Assignment No 2
Assignment on Linux Networking Commands

Sahil
2016UCS0008

August 23, 2018

1 Problem 1:

1.1 /etc/hosts



```
jammu0014: ~
127.0.0.1       localhost
127.0.1.1       iitjammu0014

# The following lines are desirable for IPv6 capable hosts
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
~
~
~
~
~
~
~
~
```

It is used to bypass DNS resolution. Any match found in it will be used before DNS entry. It can be used to given human readable names to some local machines on a small network.

1.2 /etc/sysconfig/network

This file stores the host name and default gateway IP address.

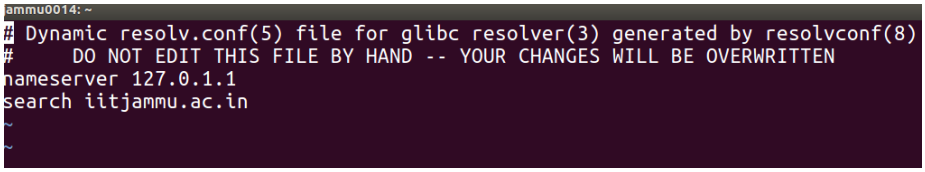
1.3 /etc/sysconfig/network-scripts/ifcfg-eth0

This stores the IP address of the first ethernet interface.

1.4 /etc/default-route

This stores a default gateway i.e. the IP address/domain name of the default router.

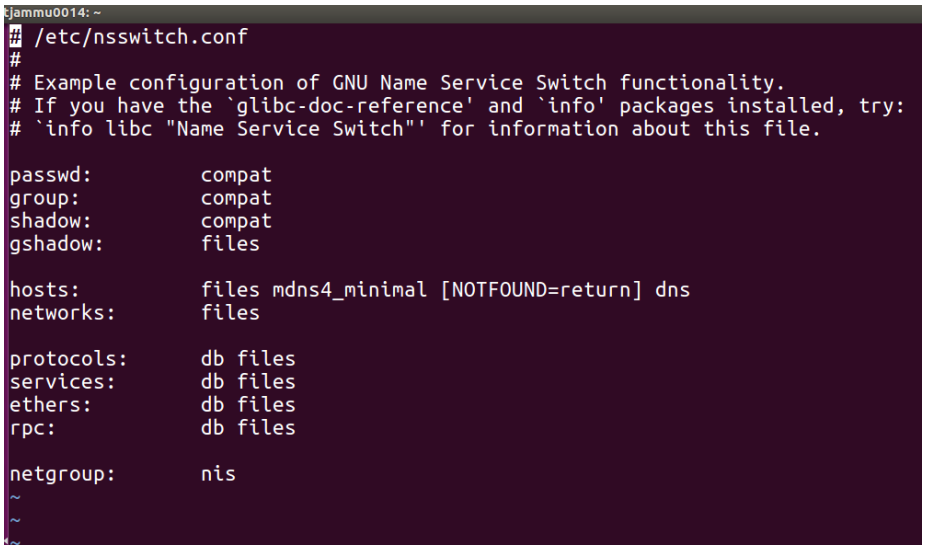
1.5 /etc/resolv.conf



```
jammu0014: ~
# Dynamic resolv.conf(5) file for glibc resolver(3) generated by resolvconf(8)
#     DO NOT EDIT THIS FILE BY HAND -- YOUR CHANGES WILL BE OVERWRITTEN
nameserver 127.0.1.1
search iitjammu.ac.in
~
~
```

It is used to store the information about the paramters of the DNS resolver which allows the system to translate human friendly domain names into IP addresses.

1.6 /etc/nsswitch.conf



```
jammu0014: ~
# /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
~
~
```

It is used to specify the order of name resolution, for e.g.**hosts: files dns** means that first check in files and if not found, then try DNS.

2 Problem 2: /etc/services

```
itjammu0014: ~
# 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
systat          11/tcp          users
daytime         13/tcp
daytime         13/udp
netstat         15/tcp
qotd            17/tcp          quote
msp             18/tcp                          # message send protocol
msp             18/udp
chargen         19/tcp          ttytst source
chargen         19/udp          ttytst source
ftp-data        20/tcp
ftp             21/tcp
fsp             21/udp          fspd
ssh             22/tcp                          # SSH Remote Login Protocol
ssh             22/udp
telnet          23/tcp
smtp            25/tcp          mail
time            37/tcp          timserver
time            37/udp          timserver
rlp             39/udp          resource        # resource location
nameserver      42/tcp          name            # IEN 116
whois           43/tcp          nicname
tacacs          49/tcp                          # Login Host Protocol (TACACS)
tacacs          49/udp
re-mail-ck      50/tcp                          # Remote Mail Checking Protocol
re-mail-ck      50/udp
domain          53/tcp                          # Domain Name Server
domain          53/udp
mtp             57/tcp                          # deprecated
tacacs-ds       65/tcp                          # TACACS-Database Service
tacacs-ds       65/udp
bootps          67/tcp                          # BOOTP server
bootps          67/udp
bootpc          68/tcp                          # BOOTP client
bootpc          68/udp
tftp            69/udp
gopher          70/tcp                          # Internet Gopher
gopher          70/udp
rje             77/tcp          netrjs
finger          79/tcp
http            80/tcp          www             # WorldWideWeb HTTP
http            80/udp                          # HyperText Transfer Protocol
link            87/tcp          ttylink
kerberos        88/tcp          kerberos5 krb5 kerberos-sec     # Kerberos v5
kerberos        88/udp          kerberos5 krb5 kerberos-sec     # Kerberos v5
```

2.1 Use

This file provides the details of the port no. associated with a service and thus when the packet is sent from the local machine, the port no. is attached from this file.

2.2 Layer

It uses the transport layer as that provides process-to-process message delivery.

2.3 Port numbers

The port numbers shown are ONLY **well-known** port numbers. This is because we must know the port number on the remote machine before sending a request using transport layer, so they are recognized through this file.

3 Problem 3: Basic linux commands

S.No	Name	Purpose	App. Layer Protocol	Trans - port Layer Protocol	Network Layer Protocol
1	arp	It is used to convert the IP address to the Physical address or the MAC address.	-	-	-
2	arping	It is used to send ARP requests to a machine on local network. In response, we get the physical address of the machine.	-	-	ARP
3	ifconfig	It basically tells about the network interfaces and the assigned IP address to the local machine.	-	-	-
4	tcpdump	It is used to capture packets on a network interface and the type of packets to be captured can be defined on the protocol or IP addresses associated.	-	-	-
5	ping	It is used to test the ability of the source computer to reach a specified destination computer. It sends ICMP request messages to the destination computer.	-	ICMP	IP
6	netstat	It is used to display routing tables, active TCP connections and some other network protocol stats.	-	-	-
7	route	It is used to modify the network routing tables.	-	-	-

4 Problem 4: Capturing tcpdump traffic

```
sahilbansal at Bluecp0cod3r in ~
$ sudo tcpdump -tttt -c 10 host 10.10.41.131 -w output
Password:
tcpdump: data link type PKTAP
tcpdump: listening on pktap, link-type PKTAP (Apple DLT_PKTAP), capture size 262144 bytes
10 packets captured
14 packets received by filter
0 packets dropped by kernel
sahilbansal at Bluecp0cod3r in ~
$ sudo tcpdump -tttt -c 10 host 10.10.41.131 -r output
reading from PCAP-NG file output
2018-08-22 11:48:56.031299 ARP, Request who-has 10.10.41.131 (e4:02:9b:11:fb:4d (oui Unknown)) tell 10.10.41.16
4, length 28
2018-08-22 11:48:56.031328 IP 10.10.41.164 > 10.10.41.131: ICMP echo request, id 11269, seq 0, length 64
2018-08-22 11:48:56.116080 ARP, Reply 10.10.41.131 is-at e4:02:9b:11:fb:4d (oui Unknown), length 28
2018-08-22 11:48:56.116671 IP 10.10.41.131 > 10.10.41.164: ICMP echo reply, id 11269, seq 0, length 64
2018-08-22 11:48:57.033292 IP 10.10.41.164 > 10.10.41.131: ICMP echo request, id 11269, seq 1, length 64
2018-08-22 11:48:57.140498 IP 10.10.41.131 > 10.10.41.164: ICMP echo reply, id 11269, seq 1, length 64
2018-08-22 11:48:58.038505 IP 10.10.41.164 > 10.10.41.131: ICMP echo request, id 11269, seq 2, length 64
2018-08-22 11:48:58.061970 IP 10.10.41.131 > 10.10.41.164: ICMP echo reply, id 11269, seq 2, length 64
2018-08-22 11:48:59.040632 IP 10.10.41.164 > 10.10.41.131: ICMP echo request, id 11269, seq 3, length 64
2018-08-22 11:48:59.085760 IP 10.10.41.131 > 10.10.41.164: ICMP echo reply, id 11269, seq 3, length 64
sahilbansal at Bluecp0cod3r in ~
$ vi output
sahilbansal at Bluecp0cod3r in ~
$ sudo tcpdump -tttt -c 10 host 10.10.41.131 > output.txt
tcpdump: data link type PKTAP
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on pktap, link-type PKTAP (Apple DLT_PKTAP), capture size 262144 bytes
10 packets captured
14 packets received by filter
0 packets dropped by kernel
sahilbansal at Bluecp0cod3r in ~
$ more output.txt
2018-08-22 11:49:53.862310 IP 10.10.41.164 > 10.10.41.131: ICMP echo request, id 23557, seq 0, length 64
2018-08-22 11:49:53.970077 IP 10.10.41.131 > 10.10.41.164: ICMP echo reply, id 23557, seq 0, length 64
2018-08-22 11:49:54.862787 IP 10.10.41.164 > 10.10.41.131: ICMP echo request, id 23557, seq 1, length 64
2018-08-22 11:49:54.891759 IP 10.10.41.131 > 10.10.41.164: ICMP echo reply, id 23557, seq 1, length 64
2018-08-22 11:49:55.863834 IP 10.10.41.164 > 10.10.41.131: ICMP echo request, id 23557, seq 2, length 64
2018-08-22 11:49:55.915542 IP 10.10.41.131 > 10.10.41.164: ICMP echo reply, id 23557, seq 2, length 64
2018-08-22 11:49:56.869063 IP 10.10.41.164 > 10.10.41.131: ICMP echo request, id 23557, seq 3, length 64
2018-08-22 11:49:56.939537 IP 10.10.41.131 > 10.10.41.164: ICMP echo reply, id 23557, seq 3, length 64
2018-08-22 11:49:57.874278 IP 10.10.41.164 > 10.10.41.131: ICMP echo request, id 23557, seq 4, length 64
2018-08-22 11:49:57.964342 IP 10.10.41.131 > 10.10.41.164: ICMP echo reply, id 23557, seq 4, length 64
output.txt (END)
```

```
sahilbansal at Bluecp0cod3r in ~
$ ping 10.10.41.131
PING 10.10.41.131 (10.10.41.131): 56 data bytes
64 bytes from 10.10.41.131: icmp_seq=0 ttl=64 time=85.436 ms
64 bytes from 10.10.41.131: icmp_seq=1 ttl=64 time=107.267 ms
64 bytes from 10.10.41.131: icmp_seq=2 ttl=64 time=23.522 ms
64 bytes from 10.10.41.131: icmp_seq=3 ttl=64 time=45.192 ms
64 bytes from 10.10.41.131: icmp_seq=4 ttl=64 time=64.031 ms
64 bytes from 10.10.41.131: icmp_seq=5 ttl=64 time=82.766 ms
64 bytes from 10.10.41.131: icmp_seq=6 ttl=64 time=102.335 ms
c64 bytes from 10.10.41.131: icmp_seq=7 ttl=64 time=249.674 ms
c64 bytes from 10.10.41.131: icmp_seq=8 ttl=64 time=146.317 ms
64 bytes from 10.10.41.131: icmp_seq=9 ttl=64 time=62.264 ms
^C
--- 10.10.41.131 ping statistics ---
10 packets transmitted, 10 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 23.522/96.880/249.674/60.488 ms
sahilbansal at Bluecp0cod3r in ~
$ ping 10.10.41.131
PING 10.10.41.131 (10.10.41.131): 56 data bytes
64 bytes from 10.10.41.131: icmp_seq=0 ttl=64 time=107.837 ms
64 bytes from 10.10.41.131: icmp_seq=1 ttl=64 time=29.032 ms
64 bytes from 10.10.41.131: icmp_seq=2 ttl=64 time=51.770 ms
64 bytes from 10.10.41.131: icmp_seq=3 ttl=64 time=70.538 ms
64 bytes from 10.10.41.131: icmp_seq=4 ttl=64 time=90.124 ms
64 bytes from 10.10.41.131: icmp_seq=5 ttl=64 time=111.458 ms
^C
--- 10.10.41.131 ping statistics ---
6 packets transmitted, 6 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 29.032/76.793/111.458/29.691 ms
sahilbansal at Bluecp0cod3r in ~
$
```

The options used for the tcpdump command are -tttt, to display a better time format, -c 10, to restrict the no. of packets captured to 10, and the output is redirected to a text file using > command. If we use -w option, then the file would contain data in unreadable format, which can only be recognized using -r option or using wireshark.

5 Problem 5: tcpdump -enx -w exe5.out

```
sahilbansal at Bluecp0cod3r in ~
$ sudo tcpdump -enx -w exe5.out
tcpdump: data link type PKTAP
tcpdump: listening on pktap, link-type PKTAP (Apple DLT_PKTAP), capture size 262144 bytes
^C4 packets captured
4 packets received by filter
0 packets dropped by kernel
```

The above command captures the packets in the file named **exe5.out** from the **ethernet (enx)** interface, because **-w** option is used. Thus, the details of packets captured is not output on the screen. Although, it shows the statistics at the end, i.e.:

- No. of packets captured
- No. of packets received by filter
- No. of packets dropped by kernel

6 Problem 6: Capture packets generated using telnet utility

```
clab@iitjammu0013: ~
clab@iitjammu0014:~$ telnet 10.10.40.174
Trying 10.10.40.174...
Connected to 10.10.40.174.
Escape character is '^]'.
Ubuntu 16.04.3 LTS
iitjammu0013 login: clab
Password:
Last login: Thu Aug 23 00:47:42 IST 2018 from 10.10.43.47 on pts/22
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.15.0-32-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage
```

```
clab@iitjammu0014: ~
clab@iitjammu0014:~$ tcpdump -enx -w exe5.out
tcpdump: wlx00177c7a429e: You don't have permission to capture on that device
(socket: Operation not permitted)
clab@iitjammu0014:~$ sudo tcpdump -enx -w exe5.out
[sudo] password for clab:
tcpdump: listening on wlx00177c7a429e, link-type EN10MB (Ethernet), capture size
262144 bytes
^C46 packets captured
46 packets received by filter
0 packets dropped by kernel
clab@iitjammu0014:~$
```

6.1 Format of the packet saved:

Link Header:

```
    [Coloring Rule String: tcp]
Ethernet II, Src: Smartlin_7a:42:8a (00:17:7c:7a:42:8a), Dst: Smartlin_7a:42:9e (00:17:7c:7a:42:9e)
    Destination: Smartlin_7a:42:9e (00:17:7c:7a:42:9e)
        Address: Smartlin_7a:42:9e (00:17:7c:7a:42:9e)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Source: Smartlin_7a:42:8a (00:17:7c:7a:42:8a)
        Address: Smartlin_7a:42:8a (00:17:7c:7a:42:8a)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
```

Destination Address: 00:17:7c:7a:42:9e	Source Address: 00:17:7c:7a:42:8a	Frame Type: IPv4 (0x0800)

IP Header:

```
Internet Protocol Version 4, Src: 10.10.40.174, Dst: 10.10.43.47
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x10 (DSCP: Unknown, ECN: Not-ECT)
        0001 00.. = Differentiated Services Codepoint: Unknown (4)
        .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 52
    Identification: 0xdb5b (56155)
    Flags: 0x02 (Don't Fragment)
        0... .... = Reserved bit: Not set
        .1.. .... = Don't fragment: Set
        ..0. .... = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (6)
    Header checksum: 0xf767 [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.10.40.174
    Destination: 10.10.43.47
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
```

Version: 4	Header Length: 20	Differentiated Services: 16	Total length: 52
Identification: 56155		Flags: 2	Fragment Offset: 0
Time to live: 64	Protocol: TCP	Header Checksum: 63335	
Source IPA: 10.10.40.174			
Destination IPA: 10.10.43.47			

TCP Header:

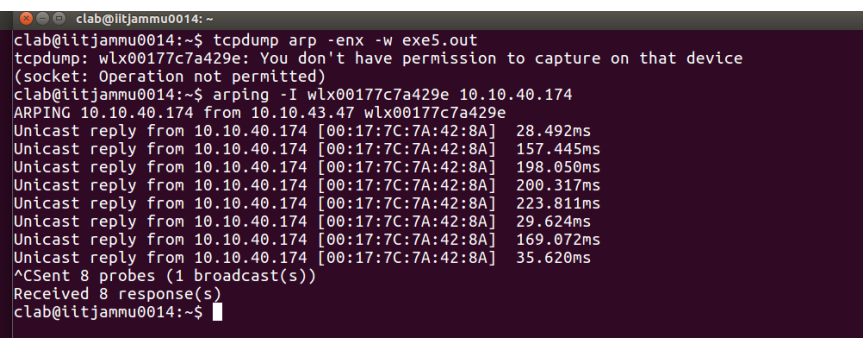
```
Transmission Control Protocol, Src Port: 23, Dst Port: 37148, Seq: 114, Ack: 139, Len: 0
    Source Port: 23
    Destination Port: 37148
    [Stream index: 0]
    [TCP Segment Len: 0]
    Sequence number: 114    (relative sequence number)
    Acknowledgment number: 139    (relative ack number)
    Header Length: 32 bytes
    Flags: 0x010 (ACK)
        000. .... .... = Reserved: Not set
        ...0 .... .... = Nonce: Not set
        .... 0... .... = Congestion Window Reduced (CWR): Not set
        .... .0.. .... = ECN-Echo: Not set
        .... ..0. .... = Urgent: Not set
        .... ...1 .... = Acknowledgment: Set
        .... .... 0... = Push: Not set
        .... .... .0.. = Reset: Not set
        .... .... ..0. = Syn: Not set
        .... .... ...0 = Fin: Not set
        [TCP Flags: ·····A····]
    Window size value: 227
    [Calculated window size: 29056]
    [Window size scaling factor: 128]
    Checksum: 0x8ece [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
    Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
        No-Operation (NOP)
            Type: 1
                0... .... = Copy on fragmentation: No
                .00. .... = Class: Control (0)
                ...0 0001 = Number: No-Operation (NOP) (1)
        No-Operation (NOP)
            Type: 1
                0... .... = Copy on fragmentation: No
                .00. .... = Class: Control (0)
                ...0 0001 = Number: No-Operation (NOP) (1)
        Timestamps: TSval 1984648074, TSecr 4086425990
            Kind: Time Stamp Option (8)
            Length: 10
            Timestamp value: 1984648074
            Timestamp echo reply: 4086425990
    [SEQ/ACK analysis]
        [This is an ACK to the segment in frame: 35]
        [The RTT to ACK the segment was: 0.210504000 seconds]
        [iRTT: 0.207672000 seconds]
```

<table>
<tr><td colspan="2">Source Port No: 23</td><td colspan="2">Destination Port No: 37148</td></tr>
<tr><td colspan="4">Sequence Number: 114 (relative)</td></tr>
<tr><td colspan="4">Acknowledgement Number: 139 (relative)</td></tr>
<tr><td>Header Length: 32</td><td>Reserved</td><td>Flags: 16</td><td>Window Size: 227</td></tr>
<tr><td colspan="2">TCP Checksum: 36558</td><td colspan="2">Urgent Pointer: 0</td></tr>
<tr><td colspan="4">Options: 12 bytes</td></tr>
</table>

6.2 Protocol field in the IP header of the packet:

The value in this field is **TCP** and it tells which protocol will be used in the above layer as network layer forwards the packet to transport layer at the destination. In other words, it specifies the transport-layer protocol encapsulated by the datagram.

7 Problem 7: Capture ARP requests and replies using tcpdump



```
     51 110.297028     Smartlin_7a:42:9e     Smartlin_7a:42:8a     ARP      42     Who has 10.10.40.174?
Tell 10.10.43.47
Frame 51: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
    Encapsulation type: Ethernet (1)
    Arrival Time: Aug 22, 2018 13:03:19.224101000 IST
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1534923199.224101000 seconds
    [Time delta from previous captured frame: 0.831821000 seconds]
    [Time delta from previous displayed frame: 0.831821000 seconds]
    [Time since reference or first frame: 110.297028000 seconds]
    Frame Number: 51
    Frame Length: 42 bytes (336 bits)
    Capture Length: 42 bytes (336 bits)
    [Frame is marked: True]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:arp]
    [Coloring Rule Name: ARP]
    [Coloring Rule String: arp]
Ethernet II, Src: Smartlin_7a:42:9e (00:17:7c:7a:42:9e), Dst: Smartlin_7a:42:8a (00:17:7c:7a:42:8a)
    Destination: Smartlin_7a:42:8a (00:17:7c:7a:42:8a)
        Address: Smartlin_7a:42:8a (00:17:7c:7a:42:8a)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Source: Smartlin_7a:42:9e (00:17:7c:7a:42:9e)
        Address: Smartlin_7a:42:9e (00:17:7c:7a:42:9e)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: ARP (0x0806)
Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: Smartlin_7a:42:9e (00:17:7c:7a:42:9e)
    Sender IP address: 10.10.43.47
    Target MAC address: Smartlin_7a:42:8a (00:17:7c:7a:42:8a)
    Target IP address: 10.10.40.174
     52 110.332071     Smartlin_7a:42:8a     Smartlin_7a:42:9e     ARP      42     10.10.40.174 is at
00:17:7c:7a:42:8a
```

```
Frame 52: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
    Encapsulation type: Ethernet (1)
    Arrival Time: Aug 22, 2018 13:03:19.259144000 IST
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1534923199.259144000 seconds
    [Time delta from previous captured frame: 0.035043000 seconds]
    [Time delta from previous displayed frame: 0.035043000 seconds]
    [Time since reference or first frame: 110.332071000 seconds]
    Frame Number: 52
    Frame Length: 42 bytes (336 bits)
    Capture Length: 42 bytes (336 bits)
    [Frame is marked: True]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:arp]
    [Coloring Rule Name: ARP]
    [Coloring Rule String: arp]
Ethernet II, Src: Smartlin_7a:42:8a (00:17:7c:7a:42:8a), Dst: Smartlin_7a:42:9e (00:17:7c:7a:42:9e)
    Destination: Smartlin_7a:42:9e (00:17:7c:7a:42:9e)
        Address: Smartlin_7a:42:9e (00:17:7c:7a:42:9e)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Source: Smartlin_7a:42:8a (00:17:7c:7a:42:8a)
        Address: Smartlin_7a:42:8a (00:17:7c:7a:42:8a)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: ARP (0x0806)
Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: Smartlin_7a:42:8a (00:17:7c:7a:42:8a)
    Sender IP address: 10.10.40.174
    Target MAC address: Smartlin_7a:42:9e (00:17:7c:7a:42:9e)
    Target IP address: 10.10.43.47
```

7.1 Frame type field in an Ethernet frame carrying an ARP request and ARP reply:

This value is **ARP (0x0806)** in both the request and the reply.

7.2 Frame type field in an Ethernet frame carrying an IP datagram in previous exercise:

This value is **IPv4 (0x0800)**.

7.3 Use of frame type field:

This tells which protocol is to be used in the network layer, i.e. provides the information about the type of the payload.

8 Problem 8: Some tcpdump expressions and their meanings

8.1 tcpdump udp port 520

It captures UDP packets on port no. 520.

8.2 tcpdump -x -s 120 ip proto 89

The -x option is used to print the data in hex and the -s option defines the snaplength, i.e. the maximum bytes of data which can be captured for a packet. Here, the size is 120 bytes. The **ip proto 89** option restricts the capture of only the protocol having no. 89, i.e. OSPF (Open Shortest Path First).

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

It captures those packets which involve communication between ip address 1 and either of the ip address 2 or the ip address 3.

```
lab@iitjammu0014:~$ sudo tcpdump -x -s -tttt 70 host 10.10.43.47 and ( 10.10.41.164 or 10.10.40.174
)
ash: syntax error near unexpected token `('
lab@iitjammu0014:~$ sudo tcpdump -x -s -tttt 70 host 10.10.43.47 and 10.10.41.164 or 10.10.40.174
cpdump: invalid snaplen -tttt
lab@iitjammu0014:~$ sudo tcpdump -x -tttt -s 70 host 10.10.43.47 and 10.10.41.164 or 10.10.40.174
cpdump: verbose output suppressed, use -v or -vv for full protocol decode
istening on wlx00177c7a429e, link-type EN10MB (Ethernet), capture size 70 bytes
^C
 packets captured
 packets received by filter
 packets dropped by kernel
lab@iitjammu0014:~$ sudo tcpdump -x -tttt -s 70 -c 10 host 10.10.43.47 and 10.10.41.164 or 10.10.40.
174
cpdump: verbose output suppressed, use -v or -vv for full protocol decode
istening on wlx00177c7a429e, link-type EN10MB (Ethernet), capture size 70 bytes
2018-08-22 14:31:55.799042 IP 10.10.43.47 > 10.10.41.164: ICMP echo request, id 3875, seq 1, length 6
4
        0x0000:  4500 0054 38bd 4000 4001 9905 0a0a 2b2f
        0x0010:  0a0a 29a4 0800 ef55 0f23 0001 8326 7d5b
        0x0020:  0000 0000 2e31 0c00 0000 0000 1011 1213
        0x0030:  1415 1617 1819 1a1b
2018-08-22 14:31:55.901144 IP 10.10.41.164 > 10.10.43.47: ICMP echo reply, id 3875, seq 1, length 64
        0x0000:  4500 0054 0000 4000 4001 d1c2 0a0a 29a4
        0x0010:  0a0a 2b2f 0000 f755 0f23 0001 8326 7d5b
        0x0020:  0000 0000 2e31 0c00 0000 0000 1011 1213
        0x0030:  1415 1617 1819 1a1b
2018-08-22 14:32:00.923324 ARP, Request who-has 10.10.41.164 tell 10.10.43.47, length 28
        0x0000:  0001 0800 0604 0001 0017 7c7a 429e 0a0a
        0x0010:  2b2f 0000 0000 0000 0a0a 29a4
2018-08-22 14:32:01.021547 ARP, Reply 10.10.41.164 is-at f0:79:60:24:e0:94 (oui Unknown), length 28
        0x0000:  0001 0800 0604 0002 f079 6024 e094 0a0a
        0x0010:  29a4 0017 7c7a 429e 0a0a 2b2f
2018-08-22 14:32:04.101864 IP 10.10.43.47 > 10.10.40.174: ICMP echo request, id 3878, seq 1, length 6
4
        0x0000:  4500 0054 a966 4000 4001 2952 0a0a 2b2f
        0x0010:  0a0a 28ae 0800 4af6 0f26 0001 8c26 7d5b
        0x0020:  0000 0000 d48d 0100 0000 0000 1011 1213
        0x0030:  1415 1617 1819 1a1b
```

```
clab@iitjammu0014:~$ ping 10.10.41.164
PING 10.10.41.164 (10.10.41.164) 56(84) bytes of data.
64 bytes from 10.10.41.164: icmp_seq=1 ttl=64 time=102 ms
^C
--- 10.10.41.164 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 102.122/102.122/102.122/0.000 ms
clab@iitjammu0014:~$ ping 10.10.40.174
PING 10.10.40.174 (10.10.40.174) 56(84) bytes of data.
^C
--- 10.10.40.174 ping statistics ---
1 packets transmitted, 0 received, 100% packet loss, time 0ms

clab@iitjammu0014:~$
```

8.4 tcpdump -x -s 70 host ip addr1 and not ip addr2

It used to capture those packets which involve ip address 1 but do not involve ip address 2.

```
lab@iitjammu0014:~$ sudo tcpdump -x -s 70 host 10.10.43.47 and not 10.10.41.164
cpdump: verbose output suppressed, use -v or -vv for full protocol decode
istening on wlx00177c7a429e, link-type EN10MB (Ethernet), capture size 70 bytes
4:30:06.519090 IP 10.10.43.47 > 10.10.40.174: ICMP echo request, id 3844, seq 1, length 64
        0x0000:  4500 0054 444b 4000 4001 8e6d 0a0a 2b2f
        0x0010:  0a0a 28ae 0800 f4ba 0f04 0001 1626 7d5b
        0x0020:  0000 0000 9aeb 0700 0000 0000 1011 1213
        0x0030:  1415 1617 1819 1a1b
4:30:06.519883 IP 10.10.43.47.49232 > google-public-dns-a.google.com.domain: 62643+[|domain]
        0x0000:  4500 0047 ec70 4000 4011 08ed 0a0a 2b2f
        0x0010:  0808 0808 c050 0035 0033 e7f4 f4b3 0100
        0x0020:  0001 0000 0000 0000 0331 3734 0234 3002
        0x0030:  3130 0231 3007 696e
4:30:06.519908 IP 10.10.43.47.49232 > b.resolvers.Level3.net.domain: 62643+[|domain]
        0x0000:  4500 0047 fa04 4000 4011 0565 0a0a 2b2f
        0x0010:  0402 0202 c050 0035 0033 f200 f4b3 0100
        0x0020:  0001 0000 0000 0000 0331 3734 0234 3002
        0x0030:  3130 0231 3007 696e
4:30:06.608745 IP google-public-dns-a.google.com.domain > 10.10.43.47.49232: 62643 NXDomain[|domain]
        0x0000:  4500 0047 77d7 0000 7611 8786 0808 0808
        0x0010:  0a0a 2b2f 0035 c050 0033 6771 f4b3 8183
        0x0020:  0001 0000 0000 0000 0331 3734 0234 3002
        0x0030:  3130 0231 3007 696e
4:30:06.609180 IP 10.10.43.47.49232 > google-public-dns-a.google.com.domain: 4812+[|domain]
        0x0000:  4500 0046 ec76 4000 4011 08e8 0a0a 2b2f
        0x0010:  0808 0808 c050 0035 0032 01d6 12cc 0100
        0x0020:  0001 0000 0000 0000 0234 3702 3433 0231
        0x0030:  3002 3130 0769 6e2d
4:30:06.646151 IP 10.10.40.174 > 10.10.43.47: ICMP echo reply, id 3844, seq 1, length 64
        0x0000:  4500 0054 83cf 0000 4001 8ee9 0a0a 28ae
        0x0010:  0a0a 2b2f 0000 fcba 0f04 0001 1626 7d5b
        0x0020:  0000 0000 9aeb 0700 0000 0000 1011 1213
        0x0030:  1415 1617 1819 1a1b
```

```
clab@iitjammu0014:~$ ping 10.10.41.164
PING 10.10.41.164 (10.10.41.164) 56(84) bytes of data.
64 bytes from 10.10.41.164: icmp_seq=1 ttl=64 time=144 ms
64 bytes from 10.10.41.164: icmp_seq=2 ttl=64 time=150 ms
64 bytes from 10.10.41.164: icmp_seq=3 ttl=64 time=275 ms
^C
--- 10.10.41.164 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 144.227/190.007/275.311/60.373 ms
clab@iitjammu0014:~$ ping 10.10.40.174
PING 10.10.40.174 (10.10.40.174) 56(84) bytes of data.
64 bytes from 10.10.40.174: icmp_seq=1 ttl=64 time=127 ms
^C
--- 10.10.40.174 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 127.085/127.085/127.085/0.000 ms
clab@iitjammu0014:~$
```

9 Problem 9: Analyze port numbers in telnet communication

```
clab@iitjammu0014:~$ telnet 10.10.40.174
Trying 10.10.40.174...
Connected to 10.10.40.174.
Escape character is '^]'.
Ubuntu 16.04.3 LTS
iitjammu0013 login: ^CConnection closed by foreign hos
clab@iitjammu0014:~$ telnet 10.10.40.174
Trying 10.10.40.174...
Connected to 10.10.40.174.
Escape character is '^]'.
Ubuntu 16.04.3 LTS
iitjammu0013 login:
Login timed out after 60 seconds.
Connection closed by foreign host.
clab@iitjammu0014:~$ telnet 10.10.40.174
Trying 10.10.40.174...
Connected to 10.10.40.174.
Escape character is '^]'.
Ubuntu 16.04.3 LTS
iitjammu0013 login: ^CConnection closed by foreign hos
clab@iitjammu0014:~$
```

```
clab@iitjammu0014:~$ tcpdump -n -nn host 10.10.43.47 and 10.10.40.174
tcpdump: wlx00177c7a429e: You don't have permission to capture on that device
(socket: Operation not permitted)
clab@iitjammu0014:~$ sudo tcpdump -n -nn host 10.10.43.47 and 10.10.40.174
[sudo] password for clab:
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on wlx00177c7a429e, link-type EN10MB (Ethernet), capture size 262144
13:59:41.670370 IP 10.10.43.47.37210 > 10.10.40.174.23: Flags [S], seq 2802530
le 7], length 0
13:59:42.115698 IP 10.10.40.174.23 > 10.10.43.47.37210: Flags [S.], seq 226911
79 ecr 3299511003,nop,wscale 7], length 0
13:59:42.115753 IP 10.10.43.47.37210 > 10.10.40.174.23: Flags [.], ack 1, win
13:59:42.115936 IP 10.10.43.47.37210 > 10.10.40.174.23: Flags [P.], seq 1:28,
h 27 [telnet DO SUPPRESS GO AHEAD, WILL TERMINAL TYPE, WILL NAWS, WILL TSPEED,
telnet]
13:59:42.531731 IP 10.10.40.174.23 > 10.10.43.47.37210: Flags [.], ack 28, win
13:59:42.628458 IP 10.10.40.174.23 > 10.10.43.47.37210: Flags [P.], seq 1:13,
th 12 [telnet DO TERMINAL TYPE, DO TSPEED, DO XDISPLOC, DO NEW-ENVIRON [|telne
13:59:42.628491 IP 10.10.43.47.37210 > 10.10.40.174.23: Flags [.], ack 13, win
13:59:43.074996 IP 10.10.40.174.23 > 10.10.43.47.37210: Flags [P.], seq 13:52,
gth 39 [telnet WILL SUPPRESS GO AHEAD, DO NAWS, DO LFLOW, DONT LINEMODE, WILL
B TERMINAL TYPE SEND SE [|telnet]
13:59:43.075030 IP 10.10.43.47.37210 > 10.10.40.174.23: Flags [.], ack 52, win
13:59:43.075230 IP 10.10.43.47.37210 > 10.10.40.174.23: Flags [P.], seq 28:123
ngth 95 [telnet SB NAWS IS 0x65 0 0x3c SE, SB TSPEED IS 0x33 0x38 0x34 0x30 0x
x61 0x6d 0x6d 0x75 0x30 0x30 0x31 0x34 0x3a 0x30 SE, SB NEW-ENVIRON IS 0 0x44
 0x30 0x30 0x31 0x34 0x3a 0x30 SE, SB TERMINAL TYPE IS 0x78 0x74 0x65 0x72 0x6
13:59:43.517813 IP 10.10.40.174.23 > 10.10.43.47.37210: Flags [.], ack 123, wi
13:59:43.517847 IP 10.10.40.174.23 > 10.10.43.47.37210: Flags [P.], seq 52:55
```

```
    [Destination Port: Unknown]
Transmission Control Protocol, Src Port: 23, Dst Port: 37168, Seq
    Source Port: 23
    Destination Port: 37168
    [Stream index: 0]
    [TCP Segment Len: 0]
    Sequence number: 52    (relative sequence number)
    Acknowledgment number: 123    (relative ack number)
    Header Length: 32 bytes
    Flags: 0x010 (ACK)
        000. .... .... = Reserved: Not set
        ...0 .... .... = Nonce: Not set
        .... 0... .... = Congestion Window Reduced (CWR): Not set
        .... .0.. .... = ECN-Echo: Not set
        .... ..0. .... = Urgent: Not set
        .... ...1 .... = Acknowledgment: Set
        .... .... 0... = Push: Not set
        .... .... .0.. = Reset: Not set
```

9.1 Port numbers used:

The port no. used by the local machine is 37168 and that by the remote machine is 23.

9.2 Port number matching the one for telnet:

That of the **remote** machine matches to the port no. of telnet (23). This is because it acts like a server and must use a well-known port number for the TCP communication.

10 Problem 10: Analyzing port numbers when two telnet sessions open simultaneously

```
clab@iitjammu0014:~$ tcpdump -n -nn 10.10.43.47 and 10.10.40.174
tcpdump: wlx00177c7a429e: You don't have permission to capture on that device
(socket: Operation not permitted)
clab@iitjammu0014:~$ sudo tcpdump -n -nn 10.10.43.47 and 10.10.40.174
[sudo] password for clab:
tcpdump: syntax error
clab@iitjammu0014:~$ sudo tcpdump -n -nn host 10.10.43.47 and 10.10.40.174
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on wlx00177c7a429e, link-type EN10MB (Ethernet), capture size 262144 bytes
14:06:49.463766 IP 10.10.43.47.37292 > 10.10.40.174.23: Flags [S], seq 2437714828, win 29200, options [mss 1460,sackOK,TS val 3299
938796 ecr 0,nop,wscale 7], length 0
14:06:49.481447 IP 10.10.40.174.23 > 10.10.43.47.37292: Flags [S.], seq 1233615118, ack 2437714829, win 28960, options [mss 1460,s
ackOK,TS val 2167490160 ecr 3299938796,nop,wscale 7], length 0
14:06:49.481488 IP 10.10.43.47.37292 > 10.10.40.174.23: Flags [.], ack 1, win 229, options [nop,nop,TS val 3299938814 ecr 21674901
60], length 0
14:06:49.481627 IP 10.10.43.47.37292 > 10.10.40.174.23: Flags [P.], seq 1:28, ack 1, win 229, options [nop,nop,TS val 3299938814 e
cr 2167490160], length 27 [telnet DO SUPPRESS GO AHEAD, WILL TERMINAL TYPE, WILL NAWS, WILL TSPEED, WILL LFLOW, WILL LINEMODE, WIL
L NEW-ENVIRON, DO STATUS, WILL XDISPLOC [|telnet]
14:06:49.500473 IP 10.10.40.174.23 > 10.10.43.47.37292: Flags [.], ack 28, win 227, options [nop,nop,TS val 2167490177 ecr 3299938
814], length 0
14:06:49.531098 IP 10.10.40.174.23 > 10.10.43.47.37292: Flags [P.], seq 1:13, ack 28, win 227, options [nop,nop,TS val 2167490202
ecr 3299938814], length 12 [telnet DO TERMINAL TYPE, DO TSPEED, DO XDISPLOC, DO NEW-ENVIRON [|telnet]
14:06:49.531125 IP 10.10.43.47.37292 > 10.10.40.174.23: Flags [.], ack 13, win 229, options [nop,nop,TS val 3299938863 ecr 2167490
202], length 0
14:06:49.556334 IP 10.10.40.174.23 > 10.10.43.47.37292: Flags [P.], seq 13:52, ack 28, win 227, options [nop,nop,TS val 2167490230
 ecr 3299938863], length 39 [telnet WILL SUPPRESS GO AHEAD, DO NAWS, DO LFLOW, DONT LINEMODE, WILL STATUS, SB TSPEED SEND SE, SB X
DISPLOC SEND SE, SB NEW-ENVIRON SEND SE, SB TERMINAL TYPE SEND SE [|telnet]
14:06:49.556362 IP 10.10.43.47.37292 > 10.10.40.174.23: Flags [.], ack 52, win 229, options [nop,nop,TS val 3299938889 ecr 2167490
230], length 0
14:06:49.556530 IP 10.10.43.47.37292 > 10.10.40.174.23: Flags [P.], seq 28:123, ack 52, win 229, options [nop,nop,TS val 329993888
9 ecr 2167490230], length 95 [telnet SB NAWS IS 0x65 0 0x3c SE, SB TSPEED IS 0x33 0x38 0x34 0x30 0x30 0x2c 0x33 0x38 0x34 0x30 0x3
0 SE, SB XDISPLOC IS 0x69 0x69 0x74 0x6a 0x61 0x6d 0x6d 0x75 0x30 0x30 0x31 0x34 0x3a 0x30 SE, SB NEW-ENVIRON IS 0 0x44 0x49 0x53
0x50 0x4c 0x41 0x59 0x1 0x69 0x69 0x74 0x6a 0x61 0x6d 0x6d 0x75 0x30 0x30 0x31 0x34 0x3a 0x30 SE, SB TERMINAL TYPE IS 0x78 0x74 0x
65 0x72 0x6d 0x2d 0x32 0x35 0x36 0x63 0x6f 0x6c 0x6f 0x72 SE [|telnet]
14:06:49.573522 IP 10.10.40.174.23 > 10.10.43.47.37292: Flags [P.], seq 52:55, ack 123, win 227, options [nop,nop,TS val 216749025
3 ecr 3299938889], length 3 [telnet DO ECHO [|telnet]
14:06:49.573637 IP 10.10.43.47.37292 > 10.10.40.174.23: Flags [P.], seq 123:126, ack 55, win 229, options [nop,nop,TS val 32999389
06 ecr 2167490253], length 3 [telnet WONT ECHO [|telnet]
14:06:49.586826 IP 10.10.40.174.23 > 10.10.43.47.37292: Flags [P.], seq 55:58, ack 126, win 227, options [nop,nop,TS val 216749026
8 ecr 3299938906], length 3 [telnet WILL ECHO [|telnet]
14:06:49.586956 IP 10.10.43.47.37292 > 10.10.40.174.23: Flags [P.], seq 126:129, ack 58, win 229, options [nop,nop,TS val 32999389
19 ecr 2167490268], length 3 [telnet DO ECHO [|telnet]
14:06:49.604034 IP 10.10.40.174.23 > 10.10.43.47.37292: Flags [P.], seq 58:98, ack 129, win 227, options [nop,nop,TS val 216749028
4 ecr 3299938919], length 40
14:06:49.646372 IP 10.10.43.47.37292 > 10.10.40.174.23: Flags [.], ack 98, win 229, options [nop,nop,TS val 3299938979 ecr 2167490
284], length 0
14:07:07.385017 IP 10.10.43.47.37294 > 10.10.40.174.23: Flags [S], seq 1206761992, win 29200, options [mss 1460,sackOK,TS val 3299
956717 ecr 0,nop,wscale 7], length 0
14:07:07.501208 IP 10.10.40.174.23 > 10.10.43.47.37294: Flags [S.], seq 3446771540, ack 1206761993, win 28960, options [mss 1460,s
ackOK,TS val 2167508185 ecr 3299956717,nop,wscale 7], length 0
```

```
clab@iitjammu0014:~$ telnet 10.10.40.174
Trying 10.10.40.174...
Connected to 10.10.40.174.
Escape character is '^]'.
Ubuntu 16.04.3 LTS
iitjammu0013 login:
```

```
clab@iitjammu0014: ~
clab@iitjammu0014:~$ telnet 10.10.40.174
Trying 10.10.40.174...
Connected to 10.10.40.174.
Escape character is '^]'.
Ubuntu 16.04.3 LTS
iitjammu0013 login:
```

```
0 packets dropped by kernel
clab@iitjammu0014:~$ sudo tcpdump -n -nn host 10.10.43.47 and 10.10.40.174 -w exe10.out
tcpdump: listening on wlx00177c7a429e, link-type EN10MB (Ethernet), capture size 262144 bytes
```

```
Transmission Control Protocol, Src Port: 23, Dst Port: 37296,
    Source Port: 23
    Destination Port: 37296
    [Stream index: 0]
    [TCP Segment Len: 0]
    Sequence number: 52    (relative sequence number)
    Acknowledgment number: 123    (relative ack number)
    Header Length: 32 bytes
    Flags: 0x010 (ACK)
        000. .... .... = Reserved: Not set
        ...0 .... .... = Nonce: Not set
```

```
Transmission Control Protocol, Src Port: 23, Dst Port: 37298,
    Source Port: 23
    Destination Port: 37298
    [Stream index: 1]
    [TCP Segment Len: 0]
    Sequence number: 52    (relative sequence number)
    Acknowledgment number: 123    (relative ack number)
    Header Length: 32 bytes
```

10.1 Port number used on the remote machine:

Port number 23 is used on the remote machine, which is the same for both the sessions.

10.2 Port number used on the local machine:

The port numbers used on the local machine for both the sessions are different and are 37296 & 37298.

10.3 Well-known port numbers and consistency:

- The range of internet-wide well-known port no is from 0 to 1023.
- The range of well-known port numbers for Unix/Linux specific service is from 0 to 1023.
- The range for a client port number is from 1024 to 65535.
- **Consistency:** It is not consistent with the well-known port numbers given in the /etc/services file, since this file also contains ports above no. 1024 which are still considered well-known in the file. This is because most of them are not running on the server, and thus the client can use those ports.