Assignment 2
Computer Networks

Vikas Gola

August 25, 2018

Question 1 Examine the following files in Linux and find out what is the purpose served by each. Write at least two sentences mentioning the purpose of each.

- /etc/hosts
- /etc/sysconfig/network
- /etc/sysconfig/network-scripts/ifcfg-eth0
- /etc/default-route
- /etc/resolv.conf
- /etc/nsswitch.conf

Answer

- **/etc/hosts**
  This file is used to find the IPA of corresponding hostname and to do that it has mapping from hostname to IP address which will be accessed whenever corresponding hostname tried to be reach on the machine. Whenever some hostname is requested by user first this file will run and try to find IP address of destination address that has to be reached and if no IPA is founded then request goes to DNS to do the same thing.

- **/etc/sysconfig/network**
  This file contains the settings or network configuration that is needed on your server.

- **/etc/sysconfig/network-scripts/ifcfg-eth0**
  This file contains the details of your network interface like should it start onboot or not,name of device, device address etc.

- **/etc/default-route**
  File does not exist. Didn't find anything on internet also.

- **/etc/resolv.conf**
  This file contains and used to find the IP address of hostname by system.

- **/etc/nsswitch.conf**
  This file is configuration file which configures the service to use for finding password, groups and hostnames.

Question 2 Display the file /etc/services on your screen, using appropriate Linux command. What is the use of /etc/services file? Which layer in the TCP/IP protocol stack do you think would make use of this file ? Are the port numbers shown in this file well-known port numbers or ephemeral port numbers ? Why are they so ? Give appropriate reasoning for your answer

Answer This file is one most important file as it contains details about all service on system which port it use, which protocol it is using and aliases to services. This file is used in the Transport Layer Protocol(TLP). All port numbers on this file are well known port numbers and the reason for this is that all service has to respond to some requests and so answer to request can be easily handle by OS or system if it already no where to or which service to serve the request that can find service easily by mapped well known port numbers in this file.

Question 3 Read the man pages for the following programs:

- arp
- arping
- ifconfig
- tcpdump
- ping
- netstat
- route

Find out the the purpose of each of these commands. In those cases whereever applicable, list out the application layer, transport layer and the network layer protocols used by each command. Pre- pare a table with the following

columns to answer your question viz. command name, Purpose, Trans- port layer protocol used, Network layer protocol used.

Answer Following table list out the layers used by given the commands:

Commands	**Application Layer Protocol**	**Transport Layer Protocol**	**Network Layer Protocol**
arp	NA	NA	ARP
arping	NA	NA	ARP
ifconfig	NA	NA	IP
tcpdump	NA	TCP	ARP
ping	NA	ICMP	IP
netstat	NA	TCP	IP
route	NA	UDP	IP

- arp Stands for "Address Resolution Protocol." ARP is a protocol used for mapping an IP address to a computer connected to a local network LAN. Since each computer has a unique physical address called a MAC address, the ARP converts the IP address to the MAC address. This ensures each computer has a unique network identification.

- arping It's purpose is to send ARP request on the local network and to print received responses.

- ifconfig This command is used to get info about network interfaces. This command can also be used to configure, disable and enable a network interface.

- tcpdump This command is used to capture packets on network and analyze different network interfaces.

- ping This command is used to send ICMP request to the given ip address and print the response.

- netstat This command is used to get network details and statistics. Also, used to get routing table of network.

- route Main use of route command is used to edit and get the routing table.

Question 4 This exercise is a simple exercise that only requires you to capture the tcpdump traffic. The problem requires you to either use two virtual machines on your laptop or two different machines in the computer lab - ask the administrator for the host name of both the machines, if so. Then run the tcpdump command on one machine say PC1 (saving the output for your lab report) so that it monitors all the packets that contain the IP address of PC2 only and none else. Next, open a new terminal window on PC1 and execute a ping command to PC2. It may be necessary to press Ctrl-C to terminate the tcpdump session. It may sometimes be best to simply redirect the output of tcpdump straight to a file and view it afterward with the more command or a text editor. Find out how can you do so.

Answer The output of tcpdump has been redirect to file using the comand sudo tcpdump icmp > ping.txt and the output in the file is
01:38:38.435936 IP 10.10.42.119 > 10.10.60.30: ICMP echo request, id 6716, seq 131, length 64
01:38:38.435987 IP 10.10.60.30 > 10.10.42.119: ICMP echo reply, id 6716, seq 131, length 64
01:38:39.438031 IP 10.10.42.119 > 10.10.60.30: ICMP echo request, id 6716, seq 132, length 64
01:38:39.438081 IP 10.10.60.30 > 10.10.42.119: ICMP echo reply, id 6716, seq 132, length 64
01:38:40.439569 IP 10.10.42.119 > 10.10.60.30: ICMP echo request, id 6716, seq 133, length 64
01:38:40.439620 IP 10.10.60.30 > 10.10.42.119: ICMP echo reply, id 6716, seq 133, length 64
01:38:41.438408 IP 10.10.42.119 > 10.10.60.30: ICMP echo request, id 6716, seq 134, length 64
01:38:41.438458 IP 10.10.60.30 > 10.10.42.119: ICMP echo reply, id 6716, seq 134, length 64

Question 5 Run the command tcpdump -enx -w exe5.out. Do you see any output on the screen ? Why ?

Answer We don't see any output on screen on running the command tcpdump -enx -w tcpdump.out because all the output and details of captured

packet has been write to file tcpdump.out file.

```
vikasgola@identity:/media/vikasgola/tutorials/IIT_JAMMU/sem 5/network/assignment 2$ sudo tcpdump -enx -w ~/tcpdump.out
tcpdump: listening on enp2s0, link-type EN10MB (Ethernet), capture size 262144 bytes
^C92 packets captured
98 packets received by filter
0 packets dropped by kernel
```

Question 6 This question is in continuation of the question no 5. Run telnet remote host. remote host is the host name of either another virtual machine in your machine or it is the host name of any other machine in the network used in the lab (Ask the lab technical suport staff about the name of other machine). This command would generate some TCP traffic. After you login the remote machine, terminate the telnet session and terminate the tcpdump program. Next, you will use wireshark to open the packet trace captured by tcpdump and analyze the captured packets. To do this, run wireshark -r exe5.out &. The wireshark Graphical User Interface (GUI) will pop up and the packets captured by tcpdump will be displayed. For your report, you need to save any one of the packets that contain the link, IP, and TCP headers. Carry out the following instructions.

- Click on a TCP packet from the list of captured packets in the wireshark window. Then go to the Edit menu and choose Mark Frame.
- Go to the File menu and choose Print. In the Wireshark:Print dialog that pops up, check File, Plain Text, Expand all levels, Print detail and supress unmarked frames. Then, enter the output text file name, e.g., headers.txt, and click the OK button. The marked packet is now dumped into the text file, with a detailed list of the name and value of every field in all the three headers.

Now answer the following questions:

- 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. Express the values in the decimal format.
- 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?

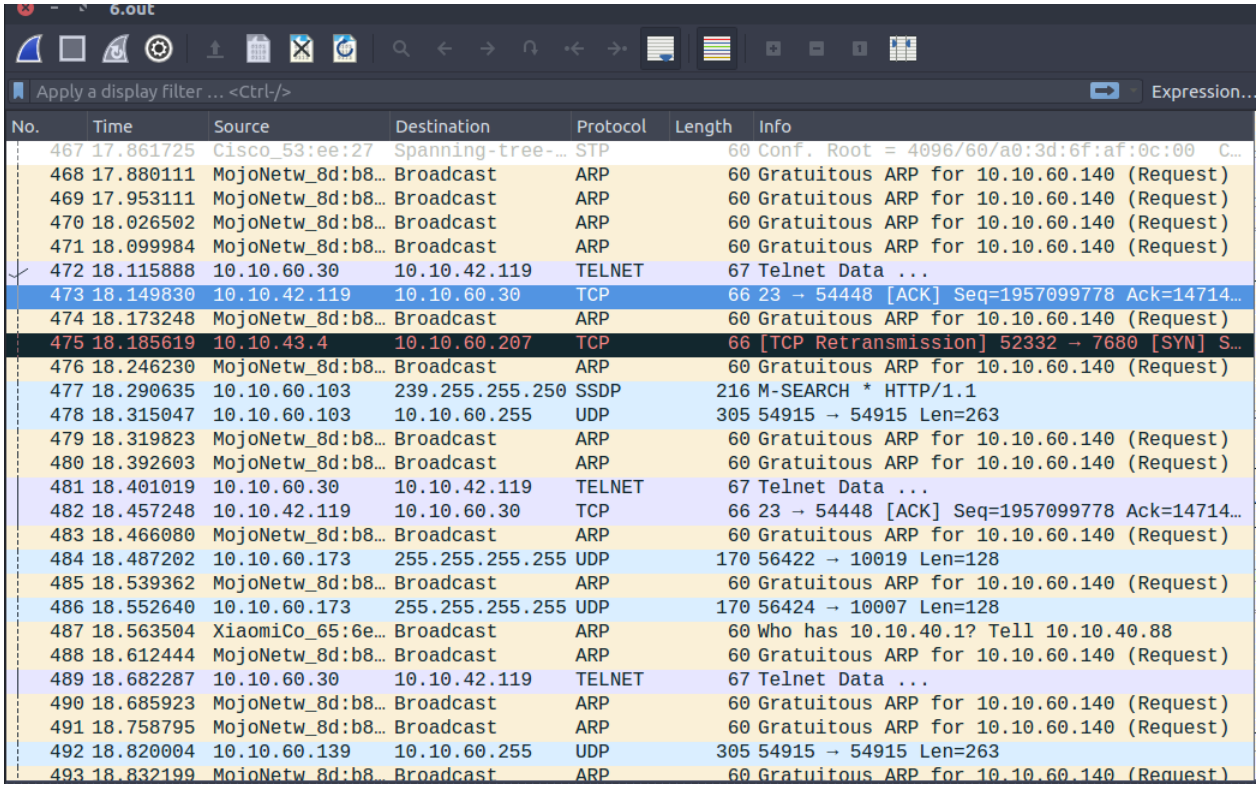
Answer The header pdf file has been included in this pdf that is on page 9(headers.pdf).

- Link Header Frame
  - Destination Address: HewlettP_2d:7f:92 (a0:8c:fd:2d:7f:92)
  - Source Address: Cisco_af:0c:44 (a0:3d:6f:af:0c:44)
- IP Header
  - Version: 4
  - Header Length: 20 bytes
  - 0x10 (DSCP: Unknown, ECN: Not-ECT)
  - Total Length: 52
  - Identification: 0xc88a (51338)
  - Flags: 0x4000, Don't fragment
    0... .... = Reserved bit: Not set
    .1.. .... = Don't fragment: Set
    ..0. .... = More fragments: Not set
    ...0 0000 0000 0000 = Fragment offset: 0
  - Time to live: 63
  - Protocol: TCP (6)
  - Header checksum: 0xf880 [validation disabled] [Header checksum status: Unverified]
  - Source: 10.10.42.119
  - Destination: 10.10.60.30
- TCP Header
  - Source Port: 23
  - Destination Port: 54448 [Stream index: 2] [TCP Segment Len: 0]
  - Sequence number: 1957099778 [Next sequence number: 1957099778]
  - Acknowledgment number: 1471419429 1000 .... =
  - Header Length: 32 bytes (8)

- 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
- Checksum: 0x544d [unverified] [Checksum Status: Unverified]
- Urgent pointer: 0
- Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  TCP Option - No-Operation (NOP)
  Kind: No-Operation (1)
  TCP Option - No-Operation (NOP)
  Kind: No-Operation (1)
  TCP Option - Timestamps: TSval 2224601295, TSecr 3851670941
  Kind: Time Stamp Option (8) Length: 10 Timestamp value: 2224601295 Timestamp echo reply: 3851670941

The value of protocol field in IP header is "TCP". This field tell us which Transport layer protocol has been used in packet.

```
    473 18.149830      10.10.42.119          10.10.60.30           TCP      66     23 → 54448 [ACK] Seq=1957099778
Ack=1471419429 Win=29056 Len=0 TSval=2224601295 TSecr=3851670941
Frame 473: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
    Encapsulation type: Ethernet (1)
    Arrival Time: Aug 24, 2018 02:10:40.362523000 IST
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1535056840.362523000 seconds
    [Time delta from previous captured frame: 0.033942000 seconds]
    [Time delta from previous displayed frame: 0.033942000 seconds]
    [Time since reference or first frame: 18.149830000 seconds]
    Frame Number: 473
    Frame Length: 66 bytes (528 bits)
    Capture Length: 66 bytes (528 bits)
    [Frame is marked: True]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp]
    [Coloring Rule Name: TCP]
    [Coloring Rule String: tcp]
Ethernet II, Src: Cisco_af:0c:44 (a0:3d:6f:af:0c:44), Dst: HewlettP_2d:7f:92 (a0:8c:fd:2d:7f:92)
    Destination: HewlettP_2d:7f:92 (a0:8c:fd:2d:7f:92)
        Address: HewlettP_2d:7f:92 (a0:8c:fd:2d:7f:92)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Source: Cisco_af:0c:44 (a0:3d:6f:af:0c:44)
        Address: Cisco_af:0c:44 (a0:3d:6f:af:0c:44)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 10.10.42.119, Dst: 10.10.60.30
    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: 0xc88a (51338)
    Flags: 0x4000, Don't fragment
        0... .... .... .... = Reserved bit: Not set
        .1.. .... .... .... = Don't fragment: Set
        ..0. .... .... .... = More fragments: Not set
        ...0 0000 0000 0000 = Fragment offset: 0
    Time to live: 63
    Protocol: TCP (6)
    Header checksum: 0xf880 [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.10.42.119
    Destination: 10.10.60.30
Transmission Control Protocol, Src Port: 23, Dst Port: 54448, Seq: 1957099778, Ack: 1471419429, Len: 0
    Source Port: 23
    Destination Port: 54448
    [Stream index: 2]
    [TCP Segment Len: 0]
    Sequence number: 1957099778
    [Next sequence number: 1957099778]
    Acknowledgment number: 1471419429
    1000 .... = Header Length: 32 bytes (8)
    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: 0x544d [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
    Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
        TCP Option - No-Operation (NOP)
            Kind: No-Operation (1)
        TCP Option - No-Operation (NOP)
            Kind: No-Operation (1)
        TCP Option - Timestamps: TSval 2224601295, TSecr 3851670941
            Kind: Time Stamp Option (8)
            Length: 10
            Timestamp value: 2224601295
            Timestamp echo reply: 3851670941
    [SEQ/ACK analysis]
        [This is an ACK to the segment in frame: 472]
        [The RTT to ACK the segment was: 0.033942000 seconds]
        [iRTT: 0.111150000 seconds]
    [Timestamps]
        [Time since first frame in this TCP stream: 10.350415000 seconds]
        [Time since previous frame in this TCP stream: 0.033942000 seconds]
```



Question 7 In a manner similar to the previous exercise, now run tcpdump to capture an ARP request and an ARP reply and then use wireshark to analyze the frames. If there are no arp requests and replies in the network, generate some using arping a remote machine. After you see several ARP replies in the arping output, terminate the arping and the tcpdump program. Open the tcpdump trace using Wireshark -r exe7.out &. Print one ARP request and one ARP reply using wireshark. Now answer the following questions:

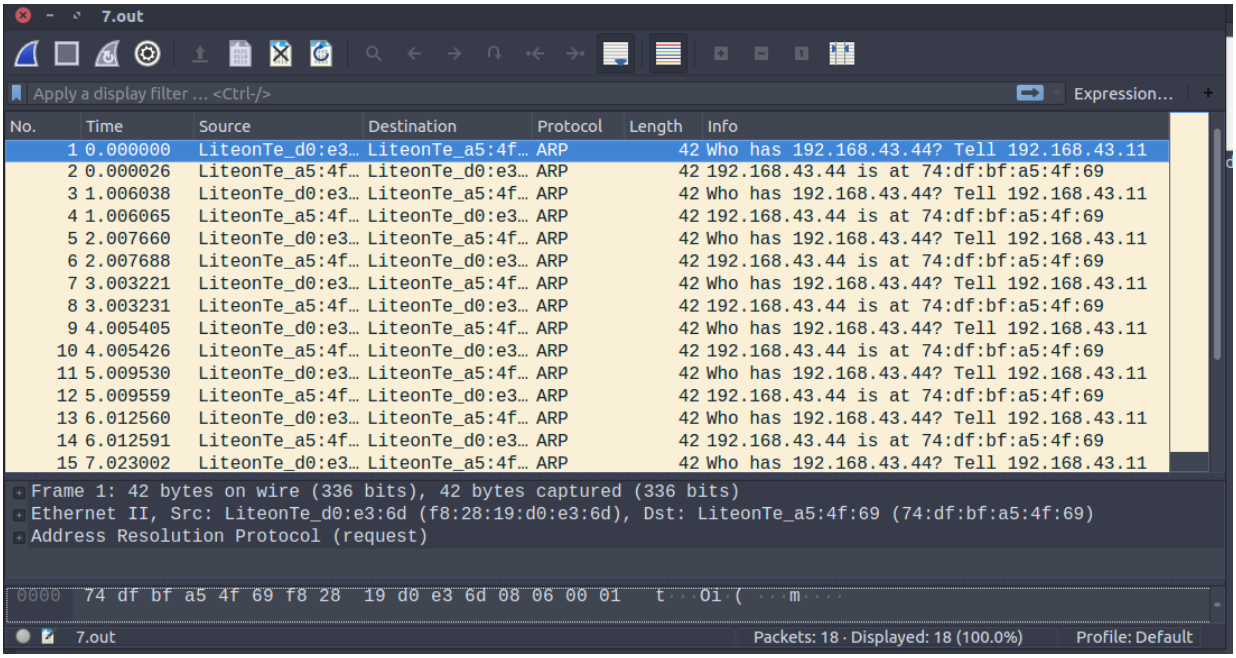
- What is the value of the frame type field in an Ethernet frame carrying an ARP request and in an Ethernet frame carrying an ARP reply, respectively?
- What is the value of the frame type field in an Ethernet frame carrying an IP datagram captured in the previous exercise?
- What is the use of the frame type field?

Answer The printed ARP reply and request has been included in pdf you can check them in next pages 12(reply) and 13(request).

- The value of the frame type field in Ethernet frame of an ARP request and reply are ARP(0x0806),ARP(0x0806) respectively.
- The value of the frame type field in an Ethernet frame carrying an IP datagram is IPv4(0x0800).
- The frame type field is use to payload of the internet frame and help recognizing the protocols.

```
      2 0.000026       LiteonTe_a5:4f:69     LiteonTe_d0:e3:6d     ARP      42     192.168.43.44 is at 74:df:bf:a5:4f:69
Frame 2: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
    Encapsulation type: Ethernet (1)
    Arrival Time: Aug 24, 2018 03:34:27.609139000 IST
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1535061867.609139000 seconds
    [Time delta from previous captured frame: 0.000026000 seconds]
    [Time delta from previous displayed frame: 0.000026000 seconds]
    [Time since reference or first frame: 0.000026000 seconds]
    Frame Number: 2
    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: LiteonTe_a5:4f:69 (74:df:bf:a5:4f:69), Dst: LiteonTe_d0:e3:6d (f8:28:19:d0:e3:6d)
    Destination: LiteonTe_d0:e3:6d (f8:28:19:d0:e3:6d)
        Address: LiteonTe_d0:e3:6d (f8:28:19:d0:e3:6d)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Source: LiteonTe_a5:4f:69 (74:df:bf:a5:4f:69)
        Address: LiteonTe_a5:4f:69 (74:df:bf:a5:4f:69)
        .... ..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: LiteonTe_a5:4f:69 (74:df:bf:a5:4f:69)
    Sender IP address: 192.168.43.44
    Target MAC address: LiteonTe_d0:e3:6d (f8:28:19:d0:e3:6d)
    Target IP address: 192.168.43.11
```

```
      1 0.000000       LiteonTe_d0:e3:6d     LiteonTe_a5:4f:69     ARP      42     Who has 192.168.43.44? Tell 192.168.43.11
Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
    Encapsulation type: Ethernet (1)
    Arrival Time: Aug 24, 2018 03:34:27.609113000 IST
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1535061867.609113000 seconds
    [Time delta from previous captured frame: 0.000000000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 0.000000000 seconds]
    Frame Number: 1
    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: LiteonTe_d0:e3:6d (f8:28:19:d0:e3:6d), Dst: LiteonTe_a5:4f:69 (74:df:bf:a5:4f:69)
    Destination: LiteonTe_a5:4f:69 (74:df:bf:a5:4f:69)
        Address: LiteonTe_a5:4f:69 (74:df:bf:a5:4f:69)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Source: LiteonTe_d0:e3:6d (f8:28:19:d0:e3:6d)
        Address: LiteonTe_d0:e3:6d (f8:28:19:d0:e3:6d)
        .... ..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: LiteonTe_d0:e3:6d (f8:28:19:d0:e3:6d)
    Sender IP address: 192.168.43.11
    Target MAC address: LiteonTe_a5:4f:69 (74:df:bf:a5:4f:69)
    Target IP address: 192.168.43.44
```



Question 8 Explain briefly the purposes of the following tcpdump expressions.

- tcpdump udp port 520
- tcpdump -x -s 120 ip proto 89
- tcpdump -x -s 70 host ip addr1 and (ip addr2 or ip addr3)
- tcpdump -x -s 70 host ip addr1 and not ip addr2

Answer

- This command tcpdump udp port 520 is use to capture UDP packets on port number 520.
- The command tcpdump -x -s 120 ip proto 89 is use to truncated packet to 120 byte and print the data of packet with header
- This command tcpdump -x -s 70 host ip addr1 and (ip addr2 or ip addr3) is use capture packet which have host ip addr1 and remote host ip addr2 or remote host ip addr3 and also use to truncated packet to 70 with print data of the packet with header.

- This command tcpdump -x -s 70 host ip addr1 and not ip addr2 is use capture packet which have host ip addr1 and remote host not ip addr2 and also use to truncated packet to 70 with print data of the packet with header.

Question 9 Start tcpdump in a command window to capture packets between your machine and a remote host using: tcpdump -n -nn host your host and remote host. Execute a TCP utility, telnet for example - as in the problem before, in another command window. When you see a TCP packet in the tcpdump output, terminate tcpdump and save its output. Now answer the following question:

- What are the port numbers used by the remote and the local computer?
- Which machine port's port number matches the port number listed for telnet in the /etc/services file?

Answer

- The port numbers of remote and local computer are 23 and 46434 respectively.
- The port number of remote computer which is port 23 match with port number of telnet in /etc/services.

Question 10 Start tcpdump in one command window using tcpdump -n -nn host your host and remote host. Then, telnet to the remote host from a second command window by typing telnetremote h ost. Again issue the same telnetremote h ost command from a third command window. Now you are opening two telnet sessions to the same remote host simultaneously, from two different command windows. Check the port numbers being used on both sides of the two connections from the output in the tcpdump window. Save a TCP packet from each of the connections. Now answer the following questions:

- 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?

- What port numbers are used in your machine for the first and second telnet, respectively?

- 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

- Yes, both sessions of telnet connected to same port number on remote host that is 23.

- 46686 and 46688 port numbers are used in my machine in first and second telnet sessions.

- The range of well known port numbers is 0 to 1023. The range of unix/linux specific services is 512 to 995. The range of client port number is 49152 to 65535. Yes, they are consistent.