

CSS LAB NO.1

Task No.1

VM1: 192.168.100.100

VM2: 192.168.100.101

VM3: 192.168.100.102

Task 1.a:

promiscuous mode is on:

Vm1 Seed Ubuntu:



```
[08/27/2020 13:35] seed@ubuntu:~/LAB/lab1$ sudo ifconfig eth13 promisc
[08/27/2020 13:35] seed@ubuntu:~/LAB/lab1$ gcc -o sniffex sniffex.c -lpcap
[08/27/2020 13:37] seed@ubuntu:~/LAB/lab1$ sudo ./sniffex
sniffex - Sniffer example using libpcap
Copyright (c) 2005 The Tcpdump Group
THERE IS ABSOLUTELY NO WARRANTY FOR THIS PROGRAM.

Device: eth13
Number of packets: 10
Filter expression: ip

Packet number 1:
  From: 192.168.0.100
  To: 239.255.255.250
  Protocol: UDP

Packet number 2:
  From: 192.168.0.100
  To: 239.255.255.250
  Protocol: UDP

Packet number 3:
  From: 192.168.0.100
  To: 239.255.255.250
  Protocol: UDP

Packet number 4:
  From: 192.168.0.25
  To: 224.0.0.251
  Protocol: UDP

Packet number 5:
  From: 192.168.0.100
  To: 224.0.0.251
  Protocol: UDP
```



Vm2 (Kali linux)

```
File Edit View Search Terminal Help
root@kali:~/marium# sudo ifconfig eth0 promisc
root@kali:~/marium# ifconfig
eth0: flags=419<UP,BROADCAST,RUNNING,PROMISC,MULTICAST> mtu 1500
    inet 192.168.0.111 netmask 255.255.255.0 broadcast 192.168.0.255
    inet6 fe80::a00:27ff:fee4:7203 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:e4:72:03 txqueuelen 1000 (Ethernet)
    RX packets 20311 bytes 20789752 (19.8 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 17119 bytes 1431080 (1.3 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.100.102 netmask 255.255.255.0 broadcast 192.168.100.255
    ether 08:00:27:01:95:6e txqueuelen 1000 (Ethernet)
    RX packets 16190 bytes 20049796 (19.1 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 7 bytes 420 (420.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 76 bytes 13723 (13.4 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 76 bytes 13723 (13.4 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@kali:~/marium# ping 192.168.0.112
PING 192.168.0.112 (192.168.0.112) 56(84) bytes of data.
64 bytes from 192.168.0.112: icmp_seq=1 ttl=64 time=0.586 ms
64 bytes from 192.168.0.112: icmp_seq=2 ttl=64 time=0.769 ms
```

```

64 bytes from 192.168.0.112: icmp_seq=15 ttl=64 time=3.05 ms
64 bytes from 192.168.0.112: icmp_seq=16 ttl=64 time=0.957 ms
64 bytes from 192.168.0.112: icmp_seq=17 ttl=64 time=1.05 ms
64 bytes from 192.168.0.112: icmp_seq=18 ttl=64 time=0.623 ms
64 bytes from 192.168.0.112: icmp_seq=19 ttl=64 time=0.553 ms
64 bytes from 192.168.0.112: icmp_seq=20 ttl=64 time=1.42 ms
64 bytes from 192.168.0.112: icmp_seq=21 ttl=64 time=0.547 ms
64 bytes from 192.168.0.112: icmp_seq=22 ttl=64 time=0.749 ms
64 bytes from 192.168.0.112: icmp_seq=23 ttl=64 time=0.921 ms
64 bytes from 192.168.0.112: icmp_seq=24 ttl=64 time=0.885 ms
64 bytes from 192.168.0.112: icmp_seq=25 ttl=64 time=0.750 ms
64 bytes from 192.168.0.112: icmp_seq=26 ttl=64 time=0.780 ms
64 bytes from 192.168.0.112: icmp_seq=27 ttl=64 time=0.711 ms
64 bytes from 192.168.0.112: icmp_seq=28 ttl=64 time=0.596 ms
64 bytes from 192.168.0.112: icmp_seq=29 ttl=64 time=0.783 ms
64 bytes from 192.168.0.112: icmp_seq=30 ttl=64 time=0.764 ms
64 bytes from 192.168.0.112: icmp_seq=31 ttl=64 time=0.790 ms
64 bytes from 192.168.0.112: icmp_seq=32 ttl=64 time=0.774 ms
64 bytes from 192.168.0.112: icmp_seq=33 ttl=64 time=0.849 ms
64 bytes from 192.168.0.112: icmp_seq=34 ttl=64 time=0.806 ms
64 bytes from 192.168.0.112: icmp_seq=35 ttl=64 time=1.01 ms
64 bytes from 192.168.0.112: icmp_seq=36 ttl=64 time=0.683 ms
64 bytes from 192.168.0.112: icmp_seq=37 ttl=64 time=0.825 ms
64 bytes from 192.168.0.112: icmp_seq=38 ttl=64 time=0.536 ms
64 bytes from 192.168.0.112: icmp_seq=39 ttl=64 time=0.746 ms
64 bytes from 192.168.0.112: icmp_seq=40 ttl=64 time=0.931 ms
64 bytes from 192.168.0.112: icmp_seq=41 ttl=64 time=0.586 ms
64 bytes from 192.168.0.112: icmp_seq=42 ttl=64 time=1.13 ms
64 bytes from 192.168.0.112: icmp_seq=43 ttl=64 time=0.862 ms
64 bytes from 192.168.0.112: icmp_seq=44 ttl=64 time=0.566 ms
64 bytes from 192.168.0.112: icmp_seq=45 ttl=64 time=0.573 ms
64 bytes from 192.168.0.112: icmp_seq=46 ttl=64 time=0.574 ms

```

VM3 (Ubuntu)

```

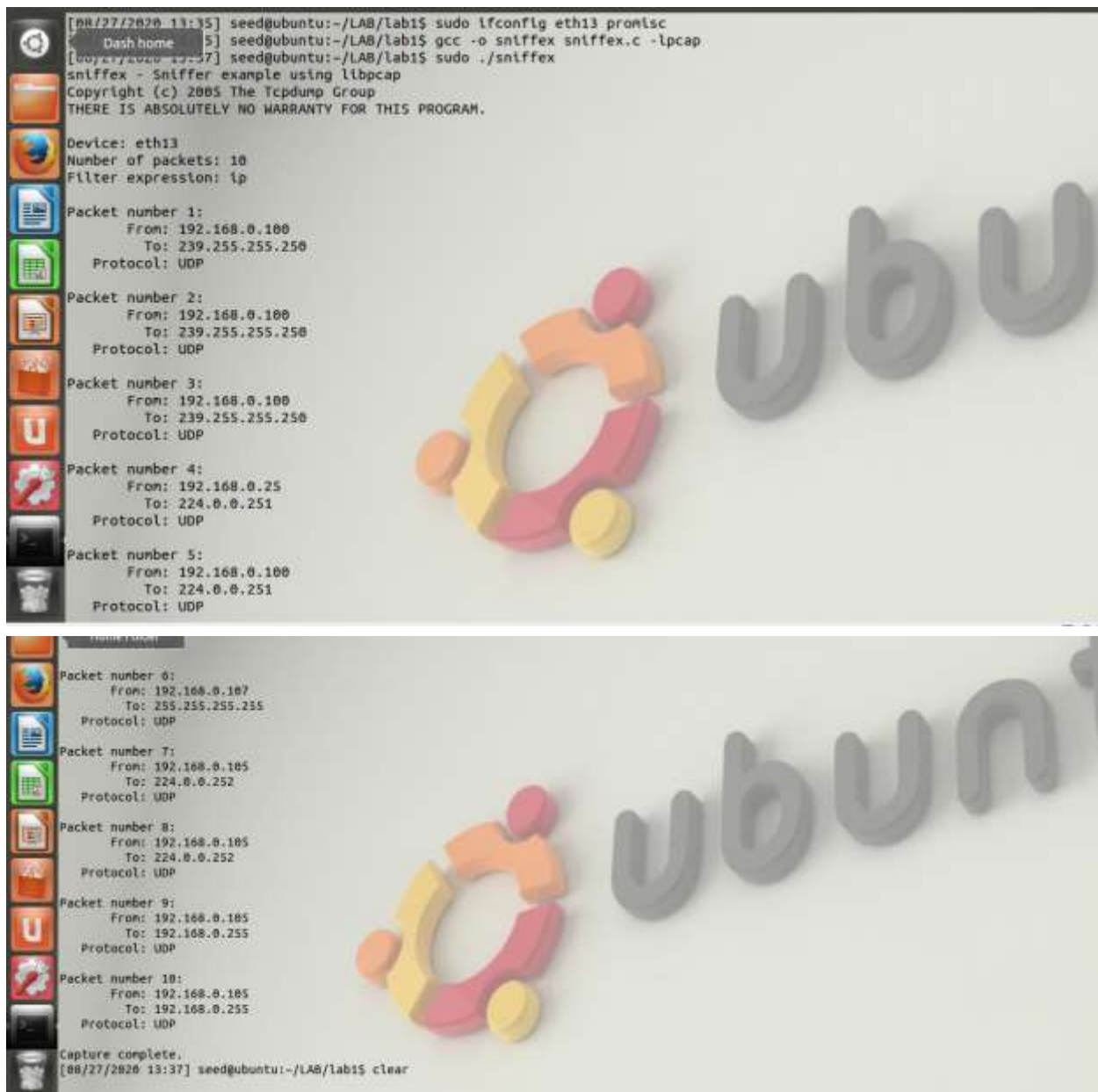
File Edit View Terminal Tabs Help
ubuntu@sdnhubvm:~$ sudo ifconfig eth0 promisc
ubuntu@sdnhubvm:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:6a:b1:b6
          inet addr:192.168.0.112 Bcast:192.168.0.255 Mask:255.255.255.0
          UP BROADCAST RUNNING PROMISC MULTICAST  MTU:1500 Metric:1
          RX packets:5714 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2611 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:940232 (940.2 KB)  TX bytes:262424 (262.4 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:65536 Metric:1
          RX packets:25762 errors:0 dropped:0 overruns:0 frame:0
          TX packets:25762 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1292836 (1.2 MB)  TX bytes:1292836 (1.2 MB)

ubuntu@sdnhubvm:~$
ubuntu@sdnhubvm:~$

```

Now ping from Vm3 to Vm2



```
[08/27/2020 13:35] seedubuntu:~/LAB/lab1$ sudo ifconfig eth1 promisc
Dash home 5 seedubuntu:~/LAB/lab1$ gcc -o sniffex sniffex.c -lpcap
[08/27/2020 13:37] seedubuntu:~/LAB/lab1$ sudo ./sniffex
sniffex - Sniffer example using libpcap
Copyright (c) 2005 The Tcpdump Group
THERE IS ABSOLUTELY NO WARRANTY FOR THIS PROGRAM.

Device: eth1
Number of packets: 10
Filter expression: ip

Packet number 1:
  From: 192.168.0.100
  To: 239.255.255.250
  Protocol: UDP

Packet number 2:
  From: 192.168.0.100
  To: 239.255.255.250
  Protocol: UDP

Packet number 3:
  From: 192.168.0.100
  To: 239.255.255.250
  Protocol: UDP

Packet number 4:
  From: 192.168.0.25
  To: 224.0.0.251
  Protocol: UDP

Packet number 5:
  From: 192.168.0.100
  To: 224.0.0.251
  Protocol: UDP

Packet number 6:
  From: 192.168.0.100
  To: 255.255.255.255
  Protocol: UDP

Packet number 7:
  From: 192.168.0.105
  To: 224.0.0.252
  Protocol: UDP

Packet number 8:
  From: 192.168.0.105
  To: 224.0.0.252
  Protocol: UDP

Packet number 9:
  From: 192.168.0.105
  To: 192.168.0.255
  Protocol: UDP

Packet number 10:
  From: 192.168.0.105
  To: 192.168.0.255
  Protocol: UDP

Capture complete.
[08/27/2020 13:37] seedubuntu:~/LAB/lab1$ clear
```


Vm 3 (Ubutu)

```
Terminal - ubuntu@sdnhubvm: ~
File Edit View Terminal Tabs Help
64 bytes from 192.168.0.111: icmp_seq=76 ttl=64 time=0.772 ms
64 bytes from 192.168.0.111: icmp_seq=77 ttl=64 time=0.782 ms
64 bytes from 192.168.0.111: icmp_seq=78 ttl=64 time=5.62 ms
64 bytes from 192.168.0.111: icmp_seq=79 ttl=64 time=0.512 ms
64 bytes from 192.168.0.111: icmp_seq=80 ttl=64 time=0.715 ms
64 bytes from 192.168.0.111: icmp_seq=81 ttl=64 time=1.05 ms
64 bytes from 192.168.0.111: icmp_seq=82 ttl=64 time=0.727 ms
64 bytes from 192.168.0.111: icmp_seq=83 ttl=64 time=0.516 ms
64 bytes from 192.168.0.111: icmp_seq=84 ttl=64 time=1.36 ms
64 bytes from 192.168.0.111: icmp_seq=85 ttl=64 time=1.22 ms
64 bytes from 192.168.0.111: icmp_seq=86 ttl=64 time=0.600 ms
64 bytes from 192.168.0.111: icmp_seq=87 ttl=64 time=0.552 ms
64 bytes from 192.168.0.111: icmp_seq=88 ttl=64 time=0.726 ms
64 bytes from 192.168.0.111: icmp_seq=89 ttl=64 time=0.588 ms
64 bytes from 192.168.0.111: icmp_seq=90 ttl=64 time=2.03 ms
64 bytes from 192.168.0.111: icmp_seq=91 ttl=64 time=0.780 ms
64 bytes from 192.168.0.111: icmp_seq=92 ttl=64 time=0.709 ms
64 bytes from 192.168.0.111: icmp_seq=93 ttl=64 time=0.558 ms
64 bytes from 192.168.0.111: icmp_seq=94 ttl=64 time=0.749 ms
64 bytes from 192.168.0.111: icmp_seq=95 ttl=64 time=0.597 ms
64 bytes from 192.168.0.111: icmp_seq=96 ttl=64 time=0.934 ms
64 bytes from 192.168.0.111: icmp_seq=97 ttl=64 time=0.497 ms
64 bytes from 192.168.0.111: icmp_seq=98 ttl=64 time=0.559 ms
64 bytes from 192.168.0.111: icmp_seq=99 ttl=64 time=1.02 ms
64 bytes from 192.168.0.111: icmp_seq=100 ttl=64 time=0.654 ms
64 bytes from 192.168.0.111: icmp_seq=101 ttl=64 time=0.721 ms
64 bytes from 192.168.0.111: icmp_seq=102 ttl=64 time=0.941 ms
64 bytes from 192.168.0.111: icmp_seq=103 ttl=64 time=0.689 ms
64 bytes from 192.168.0.111: icmp_seq=104 ttl=64 time=0.778 ms
64 bytes from 192.168.0.111: icmp_seq=105 ttl=64 time=0.466 ms
64 bytes from 192.168.0.111: icmp_seq=106 ttl=64 time=0.606 ms
64 bytes from 192.168.0.111: icmp_seq=107 ttl=64 time=0.685 ms
64 bytes from 192.168.0.111: icmp_seq=108 ttl=64 time=0.906 ms
64 bytes from 192.168.0.111: icmp_seq=109 ttl=64 time=0.771 ms
```

Unsetting promiscuous mode:



```

[08/27/2020 13:48] seed@ubuntu:~/LAB/lab1$
[08/27/2020 13:48] seed@ubuntu:~/LAB/lab1$ sudo ifconfig eth13 -promisc
[08/27/2020 13:48] seed@ubuntu:~/LAB/lab1$ gcc -o sniffex sniffex.c -lpcap
[08/27/2020 13:49] seed@ubuntu:~/LAB/lab1$ sudo ./sniffex
sniffex - Sniffer example using libpcap
Copyright (c) 2005 The Tcpdump Group
THERE IS ABSOLUTELY NO WARRANTY FOR THIS PROGRAM.

Device: eth13
Number of packets: 10
Filter expression: ip

Packet number 1:
  From: 192.168.0.100
  To: 239.255.255.250
  Protocol: UDP

Packet number 2:
  From: 192.168.0.100
  To: 239.255.255.250
  Protocol: UDP

Packet number 3:
  From: 192.168.0.100
  To: 239.255.255.250
  Protocol: UDP

Packet number 4:
  From: 192.168.0.1
  To: 239.255.255.250
  Protocol: UDP

Packet number 5:
  From: 192.168.0.1
  To: 239.255.255.250
  Protocol: UDP

Packet number 6:
  From: 192.168.0.1
  To: 239.255.255.250
  Protocol: UDP

Packet number 7:
  From: 192.168.0.1
  To: 239.255.255.250
  Protocol: UDP

Packet number 8:
  From: 192.168.0.1
  To: 239.255.255.250
  Protocol: UDP

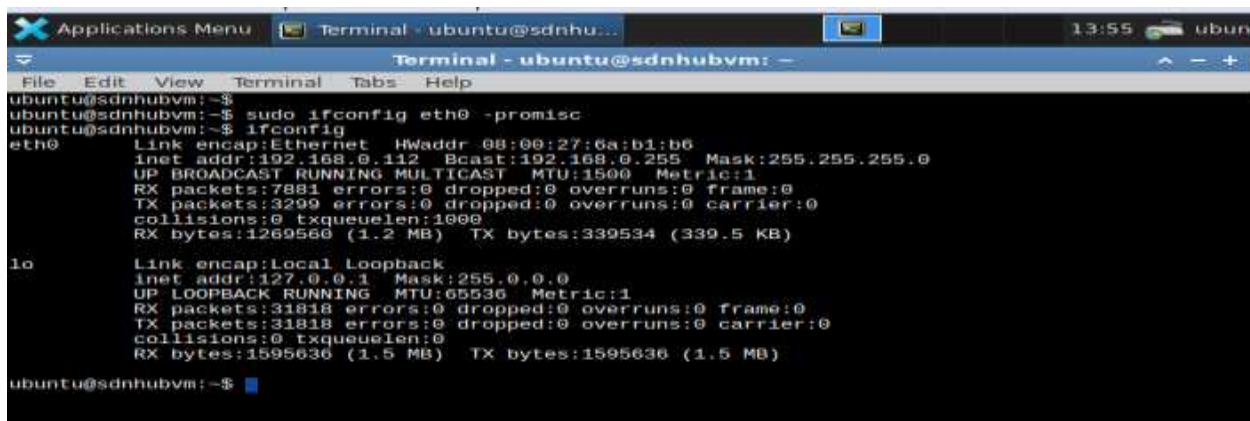
Packet number 9:
  From: 192.168.0.1
  To: 239.255.255.250
  Protocol: UDP

Packet number 10:
  From: 192.168.0.1
  To: 239.255.255.250
  Protocol: UDP

Capture complete.
[08/27/2020 13:49] seed@ubuntu:~/LAB/lab1$

```

Vm2 (Ubuntu):



```

ubuntu@sdnhubvm:~$
ubuntu@sdnhubvm:~$ sudo ifconfig eth0 -promisc
ubuntu@sdnhubvm:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:6a:b1:b6
          inet addr:192.168.0.112 Bcast:192.168.0.255 Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:7881 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3299 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1269560 (1.2 MB)  TX bytes:339534 (339.5 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:31818 errors:0 dropped:0 overruns:0 frame:0
          TX packets:31818 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1595636 (1.5 MB)  TX bytes:1595636 (1.5 MB)

ubuntu@sdnhubvm:~$

```

Vm 3(Kali Linux):

```

root@kali: ~/marium
File Edit View Search Terminal Help
root@kali:~/marium#
root@kali:~/marium# sudo ifconfig eth0 -promisc
root@kali:~/marium# ping 192.168.0.112
PING 192.168.0.112 (192.168.0.112) 56(84) bytes of data:
64 bytes from 192.168.0.112: icmp_seq=1 ttl=64 time=1.17 ms
64 bytes from 192.168.0.112: icmp_seq=2 ttl=64 time=0.625 ms
64 bytes from 192.168.0.112: icmp_seq=3 ttl=64 time=1.09 ms
64 bytes from 192.168.0.112: icmp_seq=4 ttl=64 time=0.853 ms
64 bytes from 192.168.0.112: icmp_seq=5 ttl=64 time=0.889 ms
64 bytes from 192.168.0.112: icmp_seq=6 ttl=64 time=0.779 ms
64 bytes from 192.168.0.112: icmp_seq=7 ttl=64 time=0.678 ms
64 bytes from 192.168.0.112: icmp_seq=8 ttl=64 time=0.907 ms
64 bytes from 192.168.0.112: icmp_seq=9 ttl=64 time=0.806 ms
64 bytes from 192.168.0.112: icmp_seq=10 ttl=64 time=1.85 ms
64 bytes from 192.168.0.112: icmp_seq=11 ttl=64 time=0.602 ms
64 bytes from 192.168.0.112: icmp_seq=12 ttl=64 time=0.698 ms
64 bytes from 192.168.0.112: icmp_seq=13 ttl=64 time=0.603 ms
64 bytes from 192.168.0.112: icmp_seq=14 ttl=64 time=0.944 ms
64 bytes from 192.168.0.112: icmp_seq=15 ttl=64 time=0.842 ms
64 bytes from 192.168.0.112: icmp_seq=16 ttl=64 time=0.787 ms
64 bytes from 192.168.0.112: icmp_seq=17 ttl=64 time=0.898 ms
64 bytes from 192.168.0.112: icmp_seq=18 ttl=64 time=1.37 ms
64 bytes from 192.168.0.112: icmp_seq=19 ttl=64 time=0.591 ms
64 bytes from 192.168.0.112: icmp_seq=20 ttl=64 time=0.668 ms
64 bytes from 192.168.0.112: icmp_seq=21 ttl=64 time=0.615 ms
64 bytes from 192.168.0.112: icmp_seq=22 ttl=64 time=0.777 ms
64 bytes from 192.168.0.112: icmp_seq=23 ttl=64 time=0.776 ms
64 bytes from 192.168.0.112: icmp_seq=24 ttl=64 time=0.822 ms
64 bytes from 192.168.0.112: icmp_seq=25 ttl=64 time=0.998 ms
64 bytes from 192.168.0.112: icmp_seq=26 ttl=64 time=1.52 ms
64 bytes from 192.168.0.112: icmp_seq=27 ttl=64 time=0.655 ms
64 bytes from 192.168.0.112: icmp_seq=28 ttl=64 time=0.639 ms

```

Problem 1:

Please use your own words to describe the sequence of the library calls that are essential for sniffer programs:

- • Ethernet interface that the program will utilize. (Such as eth13 in my case).
- • The initialization of the PCAP to create a session, typically there is one session per device to be sniffed.
- • The call to set traffic filtering rules, this ensures that the type of traffic sniffed on an interface is the type one is going for.
- • The execution of the sniff.
- • Termination of the session.

Problem 2:

Why do you need the root privilege to run sniffex? Where does the program fail if executed without the root privilege?

Pcap_lookupdev() function needs root access because it wants to access network interfaces and it is impossible without root access in linux. Sniffer programs need raw sockets that allow direct sending of packets by the applications bypassing all applications in network software of operating system. And we need to be a root to create raw socket as we can't discover NIC until we are root.

Problem 3:

Please turn on and turn off the promiscuous mode in the sniffer program:

Screenshots are attached above.

Can you demonstrate the difference when this mode is on and off? Please describe how you demonstrate this.

Promiscuous mode is one in which all the packets are sent to a computer or sniffed by sniffer and not only those which are addressed to it whereas in a non-promiscuous mode only those packets are sent to the computer or sniffed by sniffer which are addressed to it.

TASK NO.2

On VM1,,rawudp.. Run the program rawudp.c on VM 1:



```
File Edit View Search Terminal Help
[08/27/2020 14:45] seed@ubuntu:~/LAB/lab1$ gcc rawudp.c -o rawudp
[08/27/2020 14:46] seed@ubuntu:~/LAB/lab1$ sudo ./rawudp 10.10.10.100 21 192.168.0.111 8080
socket() - Using SOCK_RAW socket and UDP protocol is OK.
setsockopt() is OK.
Trying...
Using raw socket and UDP protocol
Using Source IP: 10.10.10.100 port: 21, Target IP: 192.168.0.111 port: 8080.
Count #1 - sendto() is OK.
Count #2 - sendto() is OK.
Count #3 - sendto() is OK.
Count #4 - sendto() is OK.
Count #5 - sendto() is OK.
Count #6 - sendto() is OK.
Count #7 - sendto() is OK.
Count #8 - sendto() is OK.
Count #9 - sendto() is OK.
Count #10 - sendto() is OK.
Count #11 - sendto() is OK.
Count #12 - sendto() is OK.
Count #13 - sendto() is OK.
Count #14 - sendto() is OK.
Count #15 - sendto() is OK.
Count #16 - sendto() is OK.
Count #17 - sendto() is OK.
Count #18 - sendto() is OK.
Count #19 - sendto() is OK.
Count #20 - sendto() is OK.
[08/27/2020 14:46] seed@ubuntu:~/LAB/lab1$
```



```
root@kali:~/marium# sudo tcpdump -vv
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
17:47:12.727156 IP (tos 0x0, ttl 1, id 48707, offset 0, flags [DF], proto UDP (17), length 153)
    192.168.0.100.35776 > 239.255.255.250.1900: [udp sum ok] UDP, length 125
17:47:12.788522 ARP, Ethernet (len 6), IPv4 (len 4), Request who-has_gateway tell kali, length 28
17:47:12.791981 ARP, Ethernet (len 6), IPv4 (len 4), Reply_gateway is-at 10:fe:ed:fa:5e:8a (oui Unknown), length 46
17:47:13.803150 ARP, Ethernet (len 6), IPv4 (len 4), Request who-has_gateway tell kali, length 28
17:47:13.818235 ARP, Ethernet (len 6), IPv4 (len 4), Reply_gateway is-at 10:fe:ed:fa:5e:8a (oui Unknown), length 46
17:47:14.827324 ARP, Ethernet (len 6), IPv4 (len 4), Request who-has_gateway tell kali, length 28
17:47:14.843298 ARP, Ethernet (len 6), IPv4 (len 4), Reply_gateway is-at 10:fe:ed:fa:5e:8a (oui Unknown), length 46
17:47:29.994810 IP (tos 0x0, ttl 64, id 37426, offset 0, flags [DF], proto UDP (17), length 70)
    kali.45206 > _gateway.domain: [bad udp cksun 0x8204 -> 0xac80!] 37890+ PTR? 1.0.168.192.in-addr.arpa. (42)
17:47:30.545119 IP (tos 0x0, ttl 255, id 12181, offset 0, flags [DF], proto UDP (17), length 89)
    192.168.0.102.mdns > 224.0.0.251.mdns: [udp sum ok] 131 [2q] PTR (QM)?_googlecast_tcp.local.PTR (QM)?_googlecast_tcp.local.(61)
17:47:30.545550 IP (tos 0x0, ttl 64, id 37470, offset 0, flags [DF], proto UDP (17), length 70)
    kali.39098 > _gateway.domain: [bad udp cksun 0x8204 -> 0xc651!] 39441+ PTR? 251.0.0.224.in-addr.arpa. (42)
17:47:30.552614 IP (tos 0x0, ttl 56, id 64978, offset 0, flags [DF], proto UDP (17), length 143)
    _gateway.domain > kali.39098: [udp sum ok] 39441 NXDomain q: PTR? 251.0.0.224.in-addr.arpa. 0/1/0 ns: 224.in-addr.arpa. SOA sns.dns.icann.org. noc
.ndns.icann.org. 2020080315 7200 3600 604800 3600 (115)
17:47:30.553249 IP (tos 0x0, ttl 64, id 37472, offset 0, flags [DF], proto UDP (17), length 72)
    kali.54022 > _gateway.domain: [bad udp cksun 0x8206 -> 0x4e34!] 40360+ PTR? 102.0.168.192.in-addr.arpa. (44)
17:47:30.560007 IP (tos 0x0, ttl 56, id 27096, offset 0, flags [DF], proto UDP (17), length 72)
    _gateway.domain > kali.54022: [udp sum ok] 40360 NXDomain q: PTR? 102.0.168.192.in-addr.arpa. 0/0/0 (44)
17:47:32.387420 IP (tos 0x0, ttl 1, id 51652, offset 0, flags [DF], proto UDP (17), length 153)
    192.168.0.100.51483 > 239.255.255.250.1900: [udp sum ok] UDP, length 125
17:47:32.715651 IP (tos 0x0, ttl 1, id 51721, offset 0, flags [DF], proto UDP (17), length 153)
    192.168.0.100.51483 > 239.255.255.250.1900: [udp sum ok] UDP, length 125
17:47:33.958492 IP6 (hlen 1, next-header UDP (17) payload length: 32) fe80::1lab:b103:2392:a105:50654 > ff02::1:3.hostmon: [udp sum ok] UDP, length 24
17:47:33.958902 IP (tos 0x0, ttl 64, id 37690, offset 0, flags [DF], proto UDP (17), length 118)
    kali.40624 > _gateway.domain: [bad udp cksun 0x8234 -> 0x07c3!] 25551+ PTR? 3.0.0.0.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.f.ip6.ar
--(not)
pv6-server: [udp sum ok] dhcp6 solicit (xid=5d0dfc (elapsed-time 3100) (client-ID hwaddr/time type 1 time 605267580 38aaa75f479a) (IA_NA IAID:37541660
0 T1:0 T2:0) (Client-FQDN) (vendor-class) (option-request DNS-search-list DNS-server vendor-specific-info Client-FQDN))
17:50:26.775894 IP (tos 0x0, ttl 1, id 714, offset 0, flags [none], proto UDP (17), length 50)
    10.17.202.100.52258 > 224.0.0.252.hostmon: [udp sum ok] UDP, length 22
17:50:27.077596 IP (tos 0x0, ttl 1, id 121, offset 0, flags [none], proto UDP (17), length 52)
    10.17.202.202.60569 > 224.0.0.252.hostmon: [udp sum ok] UDP, length 24
17:50:27.181597 IP (tos 0x0, ttl 1, id 122, offset 0, flags [none], proto UDP (17), length 52)
    10.17.202.202.60569 > 224.0.0.252.hostmon: [udp sum ok] UDP, length 24
17:50:28.306536 IP (tos 0x0, ttl 255, id 22163, offset 0, flags [DF], proto UDP (17), length 89)
    192.168.0.100.mdns > 224.0.0.251.mdns: [udp sum ok] 76 [2q] PTR (QM)?_233637DE_sub_googlecast_tcp.local.PTR (QM)?_googlecast_tcp.local.(61)
}
17:50:29.023216 IP (tos 0x0, ttl 1, id 126, offset 0, flags [none], proto UDP (17), length 56)
    10.17.202.202.55587 > 224.0.0.252.hostmon: [udp sum ok] UDP, length 28
17:50:29.023618 IP (tos 0x0, ttl 1, id 127, offset 0, flags [none], proto UDP (17), length 57)
    10.17.202.202.49757 > 224.0.0.252.hostmon: [udp sum ok] UDP, length 29
17:50:29.023844 IP (tos 0x0, ttl 1, id 128, offset 0, flags [none], proto UDP (17), length 60)
    10.17.202.202.61459 > 224.0.0.252.hostmon: [udp sum ok] UDP, length 32
17:50:29.125541 IP (tos 0x0, ttl 1, id 129, offset 0, flags [none], proto UDP (17), length 56)
    10.17.202.202.55587 > 224.0.0.252.hostmon: [udp sum ok] UDP, length 28
17:50:29.126063 IP (tos 0x0, ttl 1, id 130, offset 0, flags [none], proto UDP (17), length 57)
    10.17.202.202.49757 > 224.0.0.252.hostmon: [udp sum ok] UDP, length 29
17:50:29.126578 IP (tos 0x0, ttl 1, id 131, offset 0, flags [none], proto UDP (17), length 60)
    10.17.202.202.61459 > 224.0.0.252.hostmon: [udp sum ok] UDP, length 32
17:50:29.637501 IP (tos 0x0, ttl 1, id 135, offset 0, flags [none], proto UDP (17), length 52)
    10.17.202.202.62270 > 224.0.0.252.hostmon: [udp sum ok] UDP, length 24
17:50:29.739924 IP (tos 0x0, ttl 1, id 136, offset 0, flags [none], proto UDP (17), length 52)
    10.17.202.202.62270 > 224.0.0.252.hostmon: [udp sum ok] UDP, length 24
17:50:29.740491 IP (tos 0x0, ttl 255, id 10486, offset 0, flags [DF], proto UDP (17), length 89)
    192.168.0.138.mdns > 224.0.0.251.mdns: [udp sum ok] 13 [2q] PTR (QM)?_233637DE_sub_googlecast_tcp.local.PTR (QM)?_googlecast_tcp.local.(61)
```


No.	Time	Source	Destination	Protocol	Length	Info
351	2020-08-28 14:50:22.86	192.168.100.94	192.168.100.255	NBNS	92	Name query NB
352	2020-08-28 14:50:22.86	192.168.100.94	192.168.100.255	NBNS	92	Name query NB
353	2020-08-28 14:50:22.81	192.168.100.94	192.168.100.255	NBNS	92	Name query NB
354	2020-08-28 14:50:22.95	192.168.100.15	224.0.0.251	MDNS	152	Standard query
357	2020-08-28 14:50:24.27	10.10.10.100	192.168.100.102	UDP	60	Source port: f
358	2020-08-28 14:50:24.27	192.168.100.102	10.10.10.100	ICMP	70	Destination un
359	2020-08-28 14:50:26.33	10.10.10.100	192.168.100.102	UDP	60	Source port: f
360	2020-08-28 14:50:26.33	192.168.100.102	10.10.10.100	ICMP	70	Destination un
361	2020-08-28 14:50:28.23	10.10.10.100	192.168.100.102	UDP	60	Source port: f
362	2020-08-28 14:50:28.23	192.168.100.102	10.10.10.100	ICMP	70	Destination un
363	2020-08-28 14:50:29.26	192.168.100.19	239.255.255.250	SSDP	167	M-SEARCH * HTT
364	2020-08-28 14:50:29.56	192.168.100.19	239.255.255.250	SSDP	167	M-SEARCH * HTT
365	2020-08-28 14:50:29.75	192.168.100.19	239.255.255.250	SSDP	167	M-SEARCH * HTT
366	2020-08-28 14:50:30.23	10.10.10.100	192.168.100.102	UDP	60	Source port: f
367	2020-08-28 14:50:30.23	192.168.100.102	10.10.10.100	ICMP	70	Destination un
368	2020-08-28 14:50:32.36	10.10.10.100	192.168.100.102	UDP	60	Source port: f
369	2020-08-28 14:50:32.36	192.168.100.102	10.10.10.100	ICMP	70	Destination un
370	2020-08-28 14:50:32.64	192.168.100.19	224.0.0.251	MDNS	152	Standard query
371	2020-08-28 14:50:33.96	fe80::1	ff05::c	SSDP	188	M-SEARCH * HTT
372	2020-08-28 14:50:34.24	fe80::1	ff05::c	SSDP	188	M-SEARCH * HTT
373	2020-08-28 14:50:34.24	10.10.10.100	192.168.100.102	UDP	60	Source port: f
374	2020-08-28 14:50:34.24	192.168.100.102	10.10.10.100	ICMP	70	Destination un

Run the program rawtcp.c on VM 1:

```

Terminal
[08/27/2020 14:52] seed@ubuntu:~/LAB/lab1$ gcc rawtcp.c -o rawtcp
[08/27/2020 14:52] seed@ubuntu:~/LAB/lab1$ sudo ./rawtcp 10.0.0.100 23 192.168.0.111 8008
socket()-SOCK_RAW and tcp protocol is OK.
setsockopt() is OK
Using::::Source IP: 10.0.0.100 port: 23, Target IP: 192.168.0.111 port: 8008.
Count #0 - sendto() is OK
Count #1 - sendto() is OK
Count #2 - sendto() is OK
Count #3 - sendto() is OK
Count #4 - sendto() is OK
Count #5 - sendto() is OK
Count #6 - sendto() is OK
Count #7 - sendto() is OK
Count #8 - sendto() is OK
Count #9 - sendto() is OK
Count #10 - sendto() is OK
Count #11 - sendto() is OK
Count #12 - sendto() is OK
Count #13 - sendto() is OK
Count #14 - sendto() is OK
Count #15 - sendto() is OK
Count #16 - sendto() is OK
Count #17 - sendto() is OK
Count #18 - sendto() is OK
Count #19 - sendto() is OK
[08/27/2020 14:54] seed@ubuntu:~/LAB/lab1$

```


Verification on VM 2:

```

root@kali: ~/mariam
File Edit View Search Terminal Help
root@kali:~/mariam# sudo tcpdump -vv
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
17:55:15.580912 IP (tos 0x10, ttl 63, id 54321, offset 0, flags [none], proto TCP (6), length 44)
    10.0.0.100.telnet > kali.8008: Flags [none], cksum 0x7fff (incorrect -> 0xc305), seq 1:5, win 512, length 4
17:55:15.582700 ARP, Ethernet (len 6), IPv4 (len 4), Request who-has gateway tell kali, length 28
17:55:15.584785 ARP, Ethernet (len 6), IPv4 (len 4), Reply gateway is-at 10:fe:ed:fa:5e:8a (oui Unknown), length 46
17:55:16.587525 ARP, Ethernet (len 6), IPv4 (len 4), Request who-has gateway tell kali, length 28
17:55:16.589414 ARP, Ethernet (len 6), IPv4 (len 4), Reply gateway is-at 10:fe:ed:fa:5e:8a (oui Unknown), length 46
17:55:16.760740 IP (tos 0x0, ttl 255, id 33539, offset 0, flags [DF], proto UDP (17), length 89)
    192.168.0.138.mdns > 224.0.0.251.mdns: [udp sum ok] 5 [2q] PTR (QM)? 2336370E. sub. googlecast. tcp.local. PTR (QM)? googlecast. tcp.local. (61)
17:55:16.965325 IP (tos 0x0, ttl 255, id 517, offset 0, flags [DF], proto UDP (17), length 89)
    192.168.0.5.mdns > 224.0.0.251.mdns: [udp sum ok] 93 [2q] PTR (QM)? 2336370E. sub. googlecast. tcp.local. PTR (QM)? googlecast. tcp.local. (61)
17:55:21.437208 IP (tos 0x0, ttl 64, id 24513, offset 0, flags [DF], proto UDP (17), length 70)
    kali.56881 > gateway.domain: [bad udp cksum 0x8204 -> 0x204e!] 62105+ PTR? 1.0.168.192.in-addr.arpa. (42)
17:55:21.446143 IP (tos 0x0, ttl 64, id 24515, offset 0, flags [DF], proto UDP (17), length 70)
    kali.33256 > gateway.domain: [bad udp cksum 0x8204 -> 0xb266!] 50382+ PTR? 251.0.0.224.in-addr.arpa. (42)
17:55:21.578814 IP (tos 0x10, ttl 63, id 54321, offset 0, flags [none], proto TCP (6), length 44)
    10.0.0.100.telnet > kali.8008: Flags [none], cksum 0x7fff (incorrect -> 0xc305), seq 1:5, win 512, length 4
17:55:21.947227 IP (tos 0x0, ttl 56, id 13997, offset 0, flags [DF], proto UDP (17), length 143)
    gateway.domain > kali.33256: [udp sum ok] 50382 NXDomain q: PTR? 251.0.0.224.in-addr.arpa. 0/1/0 ns: 224.in-addr.arpa. SOA sns.dns.icann.org. noc
    .dns.icann.org. 2020080315 7200 3600 604800 3600 (115)
17:55:21.947922 IP (tos 0x0, ttl 64, id 24548, offset 0, flags [DF], proto UDP (17), length 72)
    kali.34953 > gateway.domain: [bad udp cksum 0x8206 -> 0x8eea!] 42089+ PTR? 138.0.168.192.in-addr.arpa. (44)
17:55:21.958427 IP (tos 0x0, ttl 64, id 24550, offset 0, flags [DF], proto UDP (17), length 70)
    kali.40199 > gateway.domain: [bad udp cksum 0x8204 -> 0xb5c4!] 40521+ PTR? 5.0.168.192.in-addr.arpa. (42)
17:55:22.085875 IP (tos 0x0, ttl 1, id 43397, offset 0, flags [DF], proto UDP (17), length 153)
    192.168.0.100.33541 > 239.255.255.250.1900: [udp sum ok] UDP, length 125
17:55:22.086427 IP (tos 0x0, ttl 64, id 24553, offset 0, flags [DF], proto UDP (17), length 74)
    kali.37655 > gateway.domain: [bad udp cksum 0x8208 -> 0x179b!] 57072+ PTR? 250.255.255.239.in-addr.arpa. (46)
17:55:22.097887 IP (tos 0x0, ttl 55, id 14110, offset 0, flags [DF], proto UDP (17), length 147)
    gateway.domain > kali.37655: [udp sum ok] 57072 NXDomain q: PTR? 250.255.255.239.in-addr.arpa. 0/1/0 ns: 239.in-addr.arpa. SOA sns.dns.icann.org.
    noc.dns.icann.org. 2020080304 7200 3600 604800 3600 (119)
17:55:22.105734 IP (tos 0x0, ttl 56, id 39315, offset 0, flags [DF], proto UDP (17), length 72)
    gateway.domain > kali.36008: [udp sum ok] 29375 NXDomain q: PTR? 100.0.168.192.in-addr.arpa. 0/0/0 (44)
17:55:22.106322 IP (tos 0xc0, ttl 64, id 11597, offset 0, flags [none], proto ICMP (1), length 100)
    kali > gateway: ICMP kali udp port 36008 unreachable, length 80
    IP (tos 0x0, ttl 56, id 39315, offset 0, flags [DF], proto UDP (17), length 72)
    gateway.domain > kali.36008: [udp sum ok] 29375 NXDomain q: PTR? 100.0.168.192.in-addr.arpa. 0/0/0 (44)
17:55:22.392425 IP (tos 0x0, ttl 1, id 43463, offset 0, flags [DF], proto UDP (17), length 153)
    192.168.0.100.33541 > 239.255.255.250.1900: [udp sum ok] UDP, length 125
17:55:22.700061 IP (tos 0x0, ttl 1, id 43497, offset 0, flags [DF], proto UDP (17), length 153)
    192.168.0.100.33541 > 239.255.255.250.1900: [udp sum ok] UDP, length 125
17:55:23.576269 IP (tos 0x10, ttl 63, id 54321, offset 0, flags [none], proto TCP (6), length 44)
    10.0.0.100.telnet > kali.8008: Flags [none], cksum 0x7fff (incorrect -> 0xc305), seq 1:5, win 512, length 4
17:55:25.576728 IP (tos 0x10, ttl 63, id 54321, offset 0, flags [none], proto TCP (6), length 44)
    10.0.0.100.telnet > kali.8008: Flags [none], cksum 0x7fff (incorrect -> 0xc305), seq 1:5, win 512, length 4
17:55:26.078794 IP (tos 0x0, ttl 4, id 0, offset 0, flags [DF], proto UDP (17), length 292)
    gateway.51261 > 239.255.255.250.1900: [udp sum ok] UDP, length 264
17:55:26.101270 IP (tos 0x0, ttl 4, id 0, offset 0, flags [DF], proto UDP (17), length 381)
    gateway.51261 > 239.255.255.250.1900: [udp sum ok] UDP, length 273
17:55:26.204034 IP (tos 0x0, ttl 4, id 0, offset 0, flags [DF], proto UDP (17), length 364)
    gateway.51261 > 239.255.255.250.1900: [udp sum ok] UDP, length 336
17:55:26.385957 IP (tos 0x0, ttl 4, id 0, offset 0, flags [DF], proto UDP (17), length 356)
    gateway.51261 > 239.255.255.250.1900: [udp sum ok] UDP, length 328
17:55:26.475335 ARP, Ethernet (len 6), IPv4 (len 4), Request who-has gateway tell kali, length 28
17:55:26.477342 ARP, Ethernet (len 6), IPv4 (len 4), Reply gateway is-at 10:fe:ed:fa:5e:8a (oui Unknown), length 46
17:55:26.488267 IP (tos 0x0, ttl 4, id 0, offset 0, flags [DF], proto UDP (17), length 301)
    gateway.51261 > 239.255.255.250.1900: [udp sum ok] UDP, length 273
17:55:26.590774 IP (tos 0x0, ttl 4, id 0, offset 0, flags [DF], proto UDP (17), length 340)
    gateway.51261 > 239.255.255.250.1900: [udp sum ok] UDP, length 312
17:55:26.693651 IP (tos 0x0, ttl 4, id 0, offset 0, flags [DF], proto UDP (17), length 372)
    gateway.51261 > 239.255.255.250.1900: [udp sum ok] UDP, length 344
17:55:26.795643 IP (tos 0x0, ttl 4, id 0, offset 0, flags [DF], proto UDP (17), length 381)
    gateway.51261 > 239.255.255.250.1900: [udp sum ok] UDP, length 273
17:55:26.900204 IP (tos 0x0, ttl 4, id 0, offset 0, flags [DF], proto UDP (17), length 360)

```

Filter: tcp

Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
3	2020-08-28 14:56:55.6210.0.0.100	192.168.100.102	TELNET	60	Telnet Data ..	
7	2020-08-28 14:56:57.7110.0.0.100	192.168.100.102	TELNET	60	[TCP Retransmission]	
44	2020-08-28 14:56:59.6210.0.0.100	192.168.100.102	TELNET	60	[TCP Retransmission]	
53	2020-08-28 14:57:01.6210.0.0.100	192.168.100.102	TELNET	60	[TCP Retransmission]	
56	2020-08-28 14:57:03.6210.0.0.100	192.168.100.102	TELNET	60	[TCP Retransmission]	
61	2020-08-28 14:57:05.6210.0.0.100	192.168.100.102	TELNET	60	[TCP Retransmission]	
64	2020-08-28 14:57:07.7510.0.0.100	192.168.100.102	TELNET	60	[TCP Retransmission]	
67	2020-08-28 14:57:09.6810.0.0.100	192.168.100.102	TELNET	60	[TCP Retransmission]	
77	2020-08-28 14:57:11.8110.0.0.100	192.168.100.102	TELNET	60	[TCP Retransmission]	
82	2020-08-28 14:57:13.6210.0.0.100	192.168.100.102	TELNET	60	[TCP Retransmission]	
95	2020-08-28 14:57:15.6210.0.0.100	192.168.100.102	TELNET	60	[TCP Retransmission]	

Question 1:

Can you set the IP packet length field to an arbitrary value, regardless of how big the actual packet is?

When sending a packet larger than its actual size, the additional data in the payload is a chunk of zeroes. Let say the TCP packet to google.com is (178.60.128.48). The payload is "ABC...XYZ", but the IP's *total_length* has been manually increased. The result is zero padding in the payload until completing the total length of the packet. So, the problem can be of *sendto* system call. This is the call that actually sends a packet on the socket. But this call also sets the *total_length* of the packet. If the *len* parameter on the *sendto* call has not been modified, so the packet's total length is overwritten to its original size when is sent.

Question 2:

Using the raw socket programming, do you have to calculate the checksum for the IP header?

No, the computer generally the system automatically does this, or rather it fills it in.

Question 3:

Why do you need the root privilege to run the programs that use raw sockets? Where does the program fail if executed without the root privilege?

In short this is how it is defined by the authorities who set networking rules. Due to the fact one can create custom packets that could prove detrimental to a network configuration