

**katLAB 1**

**CONSTRUCT A SIMPLE NETWORK**



Name: Lê Hoàng Minh Quân

ID: B2206008

Group: M02

**Exercise 1:**

Answer: kathara vstart -n pc1 --eth 0:A

kathara vstart -n pc2 --eth 0:A

Wireshark ~/capture.pcap

pc1:

Ifconfig eth0 10.0.0.1 netmask 255.255.255.0 broadcast 10.0.0.255 up

Ping 10.0.0.2

pc2:

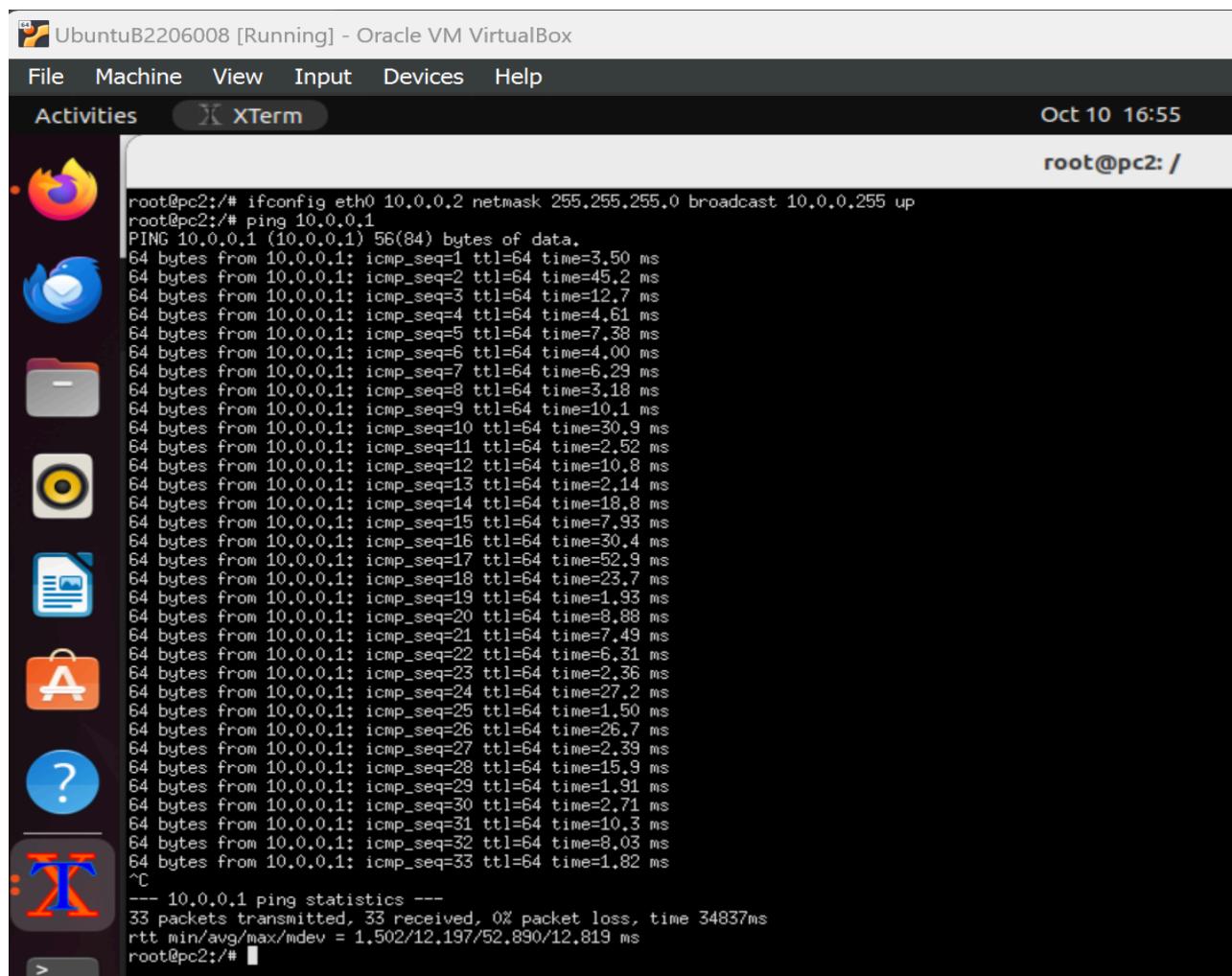
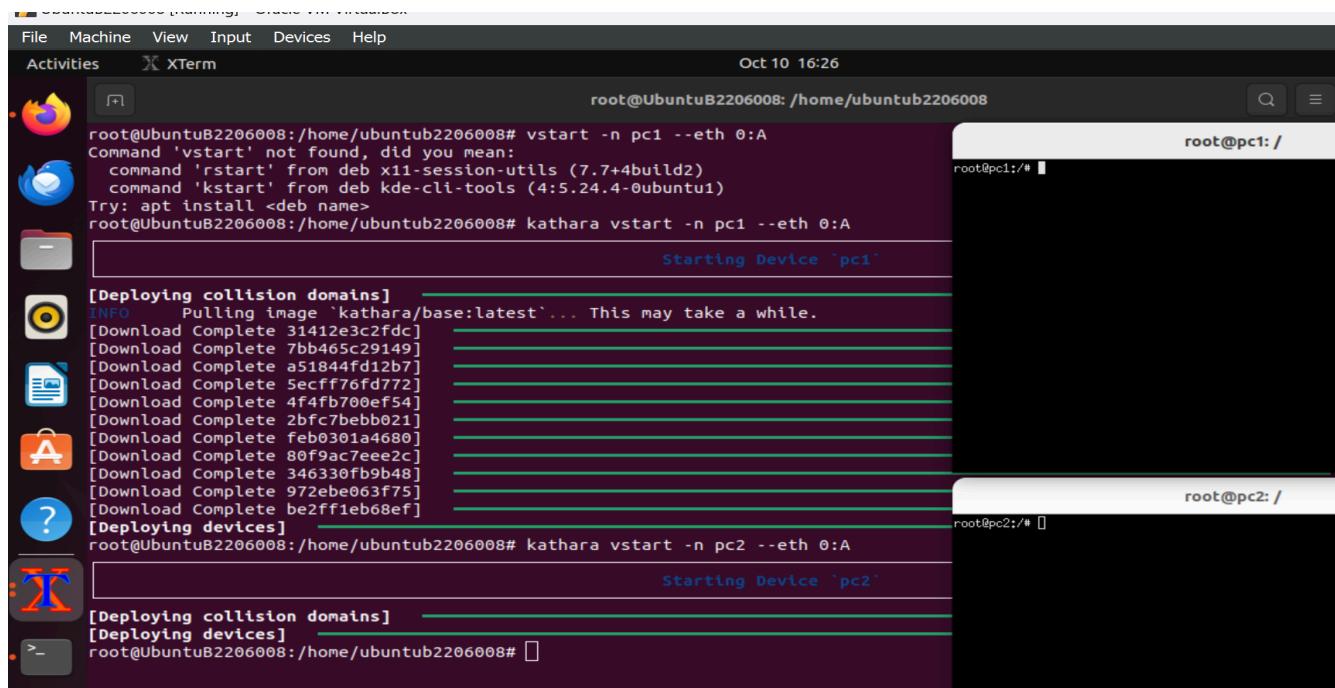
Ifconfig eth0 10.0.0.2 netmask 255.255.255.0 broadcast 10.0.0.255 up

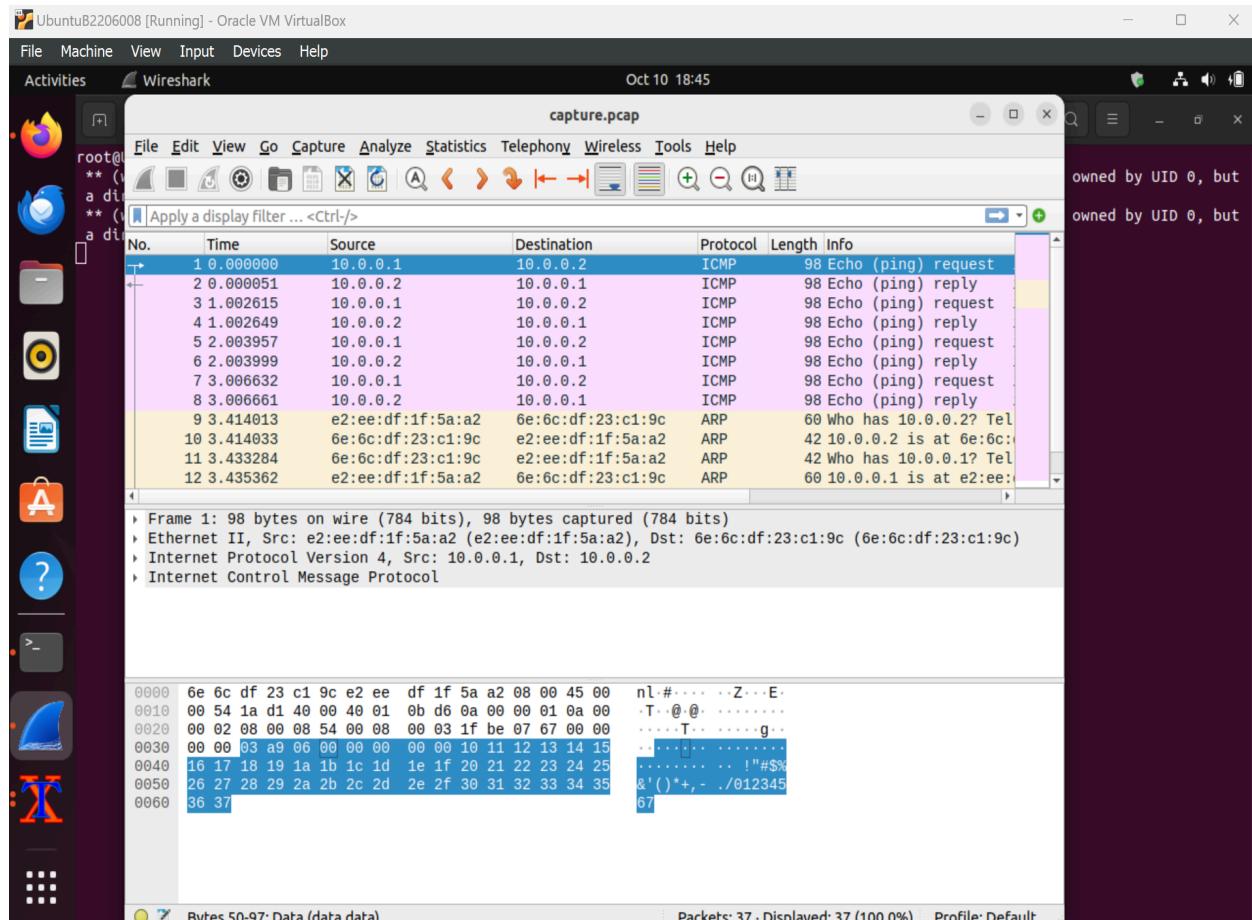
Ping 10.0.0.1

Tcpdump -telli eth0

Tcpdump -telli eth0 -w /hosthome/capture.pcap

## CT106H – Computer Network





## Exercise 2:

Solution:

Command: kathara lstart

File:

Lab.conf:

```
pc1[0]=A
pc3[0]=A
pc2[0]=B
pc4[0]=B
router1[0]=A
router1[1]=B
```

Pc1:

```
Ifconfig eth0 10.0.0.101/24 up
Route add default gw 10.0.0.1
```

Pc2:

```
Ifconfig eth0 10.0.1.101/24 up
Route add default gw 10.0.1.1
```

Pc3:

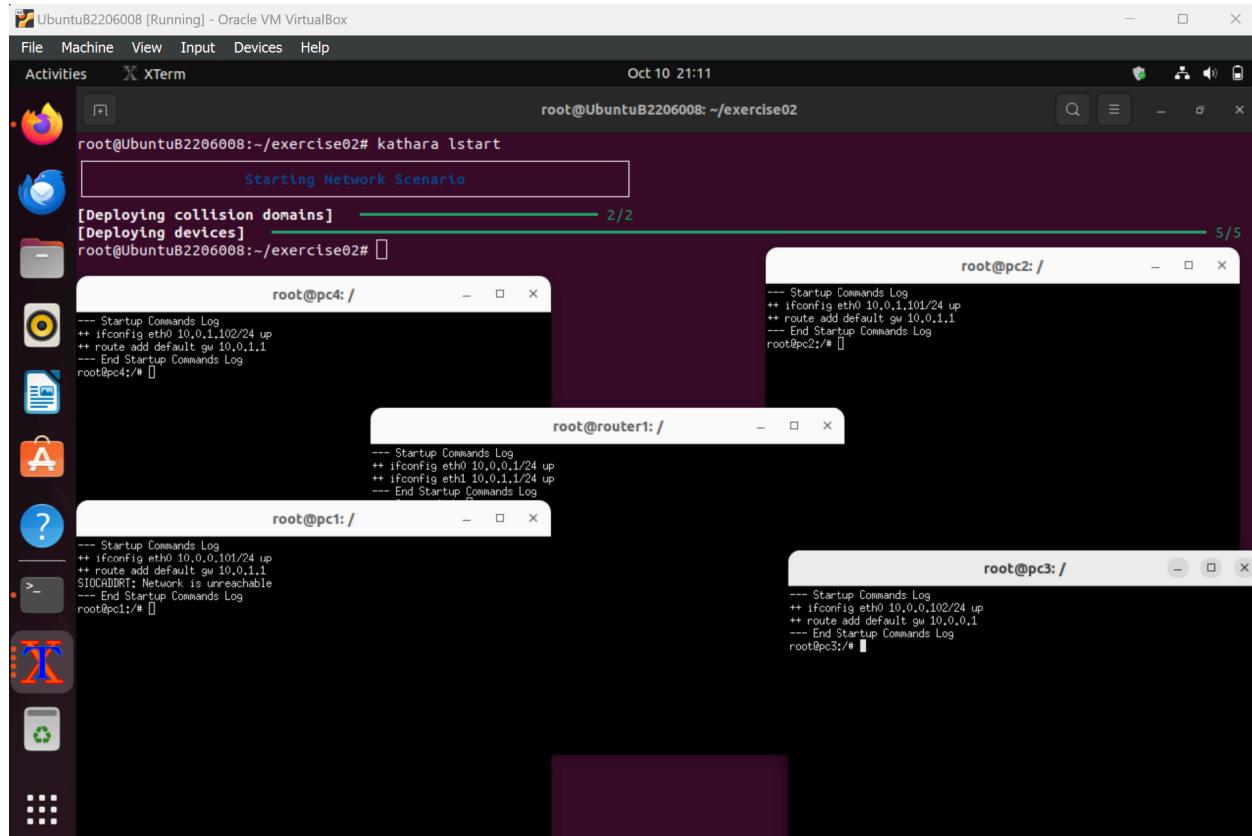
```
Ifconfig eth0 10.0.0.102/24 up  
Route add default gw 10.0.0.1
```

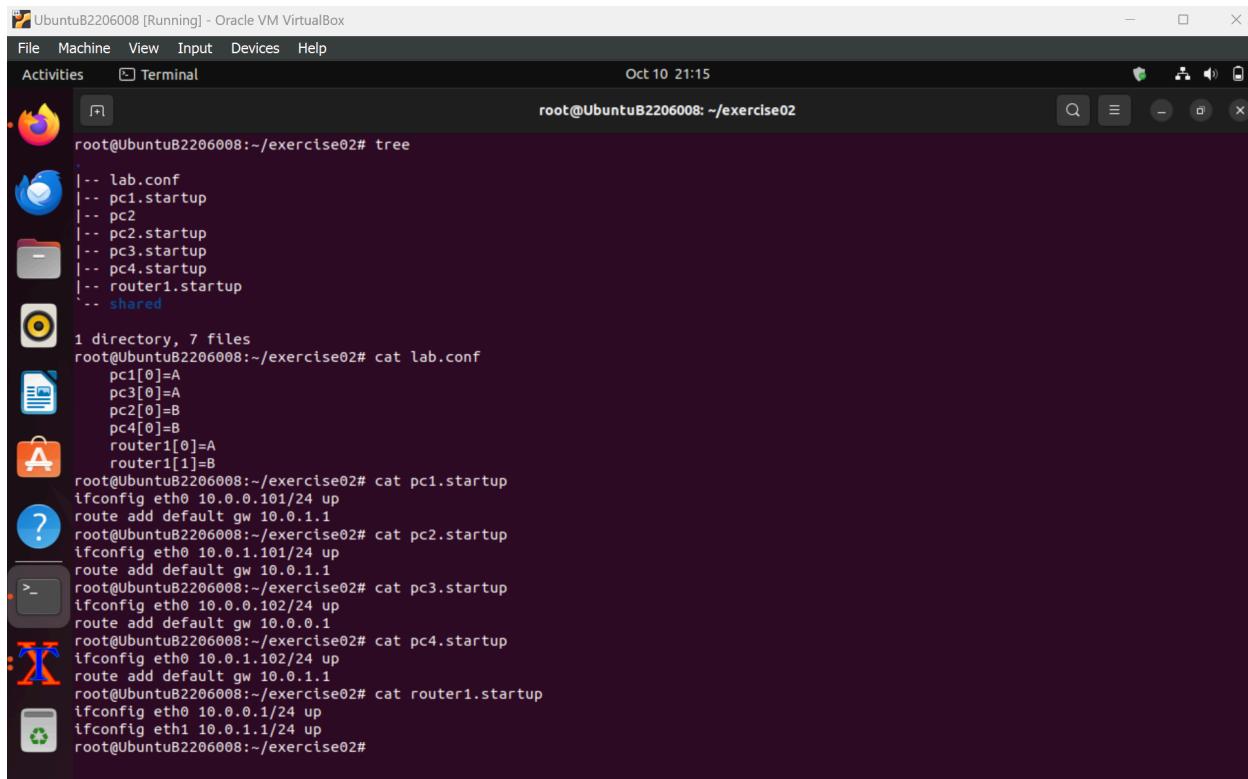
Pc4:

```
Ifconfig eth0 10.0.1.102/24 up  
Route add default gw 10.0.1.1
```

Router1.startup:

```
Ifconfig eth0 10.0.0.1/24 up  
Ifconfig eth0 10.0.1.1/24 up
```





The screenshot shows a terminal window titled "root@UbuntuB2206008: ~/exercise02#". The terminal displays the following commands and their outputs:

```
root@UbuntuB2206008:~/exercise02# tree
.
|-- lab.conf
|-- pc1.startup
|-- pc2
|-- pc2.startup
|-- pc3.startup
|-- pc4.startup
|-- router1.startup
`-- shared

1 directory, 7 files
root@UbuntuB2206008:~/exercise02# cat lab.conf
pc1[0]=A
pc3[0]=A
pc2[0]=B
pc4[0]=B
router1[0]=A
router1[1]=B
root@UbuntuB2206008:~/exercise02# cat pc1.startup
ifconfig eth0 10.0.0.101/24 up
route add default gw 10.0.0.1
root@UbuntuB2206008:~/exercise02# cat pc2.startup
ifconfig eth0 10.0.1.101/24 up
route add default gw 10.0.1.1
root@UbuntuB2206008:~/exercise02# cat pc3.startup
ifconfig eth0 10.0.0.102/24 up
route add default gw 10.0.0.1
root@UbuntuB2206008:~/exercise02# cat pc4.startup
ifconfig eth0 10.0.1.102/24 up
route add default gw 10.0.1.1
root@UbuntuB2206008:~/exercise02# cat router1.startup
ifconfig eth0 10.0.0.1/24 up
ifconfig eth1 10.0.0.1/24 up
root@UbuntuB2206008:~/exercise02#
```

## Exercise 3:

Solution:

File:

lab.conf:

```
r1[0]=A
r1[1]=B
r2[0]=C
r2[1]=B
pc1[0]=A
pc2[0]=C
```

Pc1.startup:

```
ifconfig eth0 195.11.14.5/24 up
```

Pc2.startup:

```
ifconfig eth0 200.1.1.7/24 up
```

R1.startup:

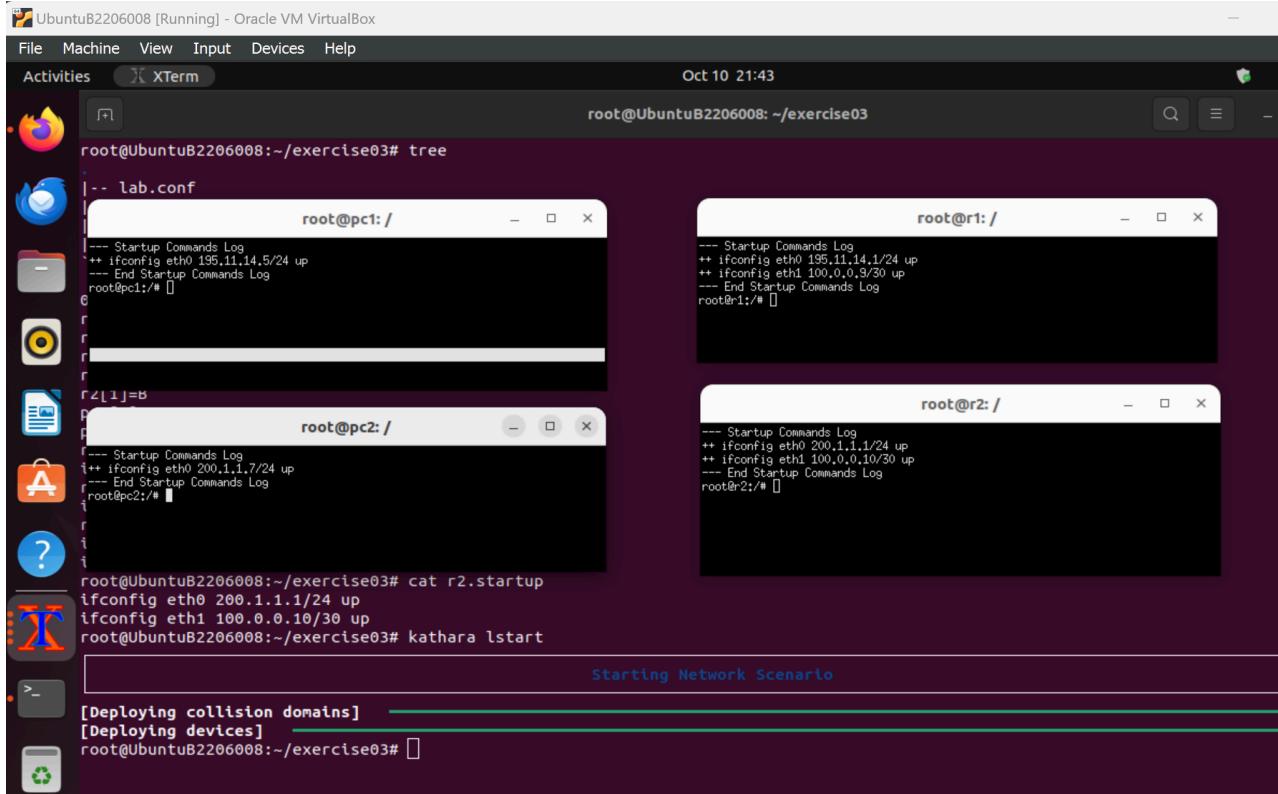
```
ifconfig eth0 195.11.14.1/24 up
ifconfig eth1 100.0.0.9/30 up
```

R2.startup

```
ifconfig eth0 200.1.1.1/24 up
ifconfig eth1 100.0.0.10/30 up
```

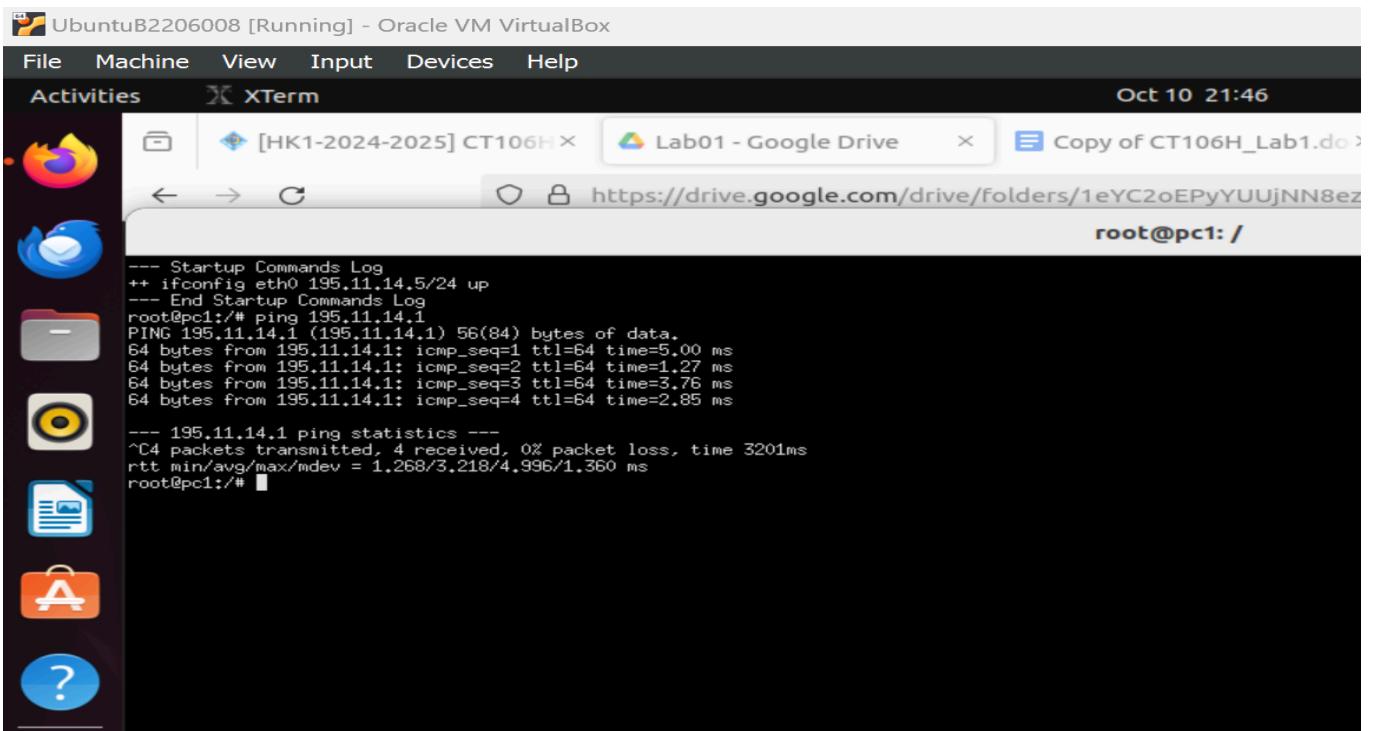
- Start Scenario

Kathara lstart



- Ping from pc1 to r1 eth0 (195.11.14.1)

Ping 195.11.14.1



- **Ping from pc1 to r1 eth1(100.0.0.9)**

Ping 100.0.0.9

UbuntuB2206008 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Activities XTerm Oct 10 23:14

root@UbuntuB2206008:~/exercise03# tree

root@pc1: /

```
--- Startup Commands Log
++ ifconfig eth0 195.11.14.5/24 up
--- End Startup Commands Log
root@pc1:/# ping 195.11.14.1
PING 195.11.14.1 (195.11.14.1) 56(84) bytes of data,
64 bytes from 195.11.14.1: icmp_seq=1 ttl=64 time=5.00 ms
64 bytes from 195.11.14.1: icmp_seq=2 ttl=64 time=1.27 ms
64 bytes from 195.11.14.1: icmp_seq=3 ttl=64 time=3.76 ms
64 bytes from 195.11.14.1: icmp_seq=4 ttl=64 time=2.85 ms
--- 195.11.14.1 ping statistics ---
^C4 packets transmitted, 4 received, 0% packet loss, time 3201ms
rtt min/avg/max/mdev = 1.268/3.218/4.996/1.360 ms
root@pc1:/# ping 100.0.0.9
ping: connect: Network is unreachable
root@pc1:/#
```

- **Interfaces on different domains cannot be reached. Can you tell why?**

- **Both routers and PCs don't know how to reach networks that are not directly connected to them.**
- **Directly connected networks are automatically inserted into the routing table when the corresponding interface is brought up.**

- Add default route to pc1, from pc1 to r1 eth1

## Route -n

Route add default gw 195.11.14.1

Route -n

Ping 100.0.0.9

UbuntuB2206008 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Activities X XTerm Oct 10 23:23

root@UbuntuB2206008: ~/exercise03

root@pc1: /

```
--- Startup Commands Log
++ ifconfig eth0 195.11.14.5/24 up
--- End Startup Commands Log
root@pc1:# ping 195.11.14.1
PING 195.11.14.1 (195.11.14.1) 56(84) bytes of data.
64 bytes from 195.11.14.1: icmp_seq=1 ttl=64 time=5.00 ms
64 bytes from 195.11.14.1: icmp_seq=2 ttl=64 time=1.27 ms
64 bytes from 195.11.14.1: icmp_seq=3 ttl=64 time=3.76 ms
64 bytes from 195.11.14.1: icmp_seq=4 ttl=64 time=2.85 ms

--- 195.11.14.1 ping statistics ---
4 packets transmitted, 4 received. 0% packet loss, time 3201ms
rtt min/avg/max/mdev = 1.268/3.218/4.996/1.360 ms
root@pc1:# ping 100.0.0.9
ping: connect: Network is unreachable
root@pc1:# route -n
Kernel IP routing table
Destination      Gateway          Genmask        Flags Metric Ref    Use Iface
195.11.14.0      0.0.0.0        255.255.255.0   U     0      0        0 eth0
root@pc1:# route add default gw 195.11.14.1
root@pc1:# route -n
Kernel IP routing table
Destination      Gateway          Genmask        Flags Metric Ref    Use Iface
0.0.0.0          195.11.14.1    0.0.0.0        UG    0      0        0 eth0
195.11.14.0      0.0.0.0        255.255.255.0   U     0      0        0 eth0
root@pc1:#
```

UbuntuB2206008 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Activities XTerm Oct 10 23:34

root@UbuntuB2206008: ~/exercise03

root@pc1: /

```
64 bytes from 195.11.14.1: icmp_seq=3 ttl=64 time=3.76 ms
64 bytes from 195.11.14.1: icmp_seq=4 ttl=64 time=2.85 ms

--- 195.11.14.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3201ms
rtt min/avg/max/mdev = 1.268/3.218/4.996/1.360 ms
root@pc1:/# ping 100.0.0.9
ping: connect: Network is unreachable
root@pc1:/# route -n
Kernel IP routing table
Destination     Gateway         Genmask        Flags Metric Ref  Use Iface
195.11.14.0     0.0.0.0       255.255.255.0   U      0      0      0 eth0
root@pc1:/# route add default gw 195.11.14.1
root@pc1:/# route -n
Kernel IP routing table
Destination     Gateway         Genmask        Flags Metric Ref  Use Iface
0.0.0.0         195.11.14.1   0.0.0.0       UG      0      0      0 eth0
195.11.14.0     0.0.0.0       255.255.255.0   U      0      0      0 eth0
root@pc1:/# ping 100.0.0.9
PING 100.0.0.9 (100.0.0.9) 56(84) bytes of data.
64 bytes from 100.0.0.9: icmp_seq=1 ttl=64 time=42.9 ms
64 bytes from 100.0.0.9: icmp_seq=2 ttl=64 time=1.90 ms
64 bytes from 100.0.0.9: icmp_seq=3 ttl=64 time=1.17 ms
64 bytes from 100.0.0.9: icmp_seq=4 ttl=64 time=1.71 ms
^C
--- 100.0.0.9 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3094ms
rtt min/avg/max/mdev = 1.174/11.934/42.949/17.908 ms
root@pc1:/#
```

- Ping from pc1 to r2 eth1 and sniff at r2

Ping 100.0.0.10

Tcpdump -tenni eth1

```

UbuntuB2206008 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities XTerm Oct 10 23:35
[HK1-2024-2025] CT106H × Lab01 - Google Drive × Copy of CT106H_Lab1.d × +
root@pc1: /root@pc1: ~
--- 195.11.14.1 ping statistics ---
^C4 packets transmitted, 4 received, 0% packet loss, time 3201ms
rtt min/avg/max/mdev = 1.268/3.218/4.996/1.360 ms
root@pc1:/# ping 100.0.0.9
ping: connect: Network is unreachable
root@pc1:/# route -n
Kernel IP routing table
Destination     Gateway         Genmask        Flags Metric Ref    Use Iface
195.11.14.0     0.0.0.0       255.255.255.0   U     0      0        0 eth0
root@pc1:/# route add default gw 195.11.14.1
root@pc1:/# route -n
Kernel IP routing table
Destination     Gateway         Genmask        Flags Metric Ref    Use Iface
0.0.0.0          195.11.14.1   0.0.0.0       UG    0      0        0 eth0
195.11.14.0     0.0.0.0       255.255.255.0   U     0      0        0 eth0
root@pc1:/# ping 100.0.0.9
PING 100.0.0.9 (100.0.0.9) 56(84) bytes of data.
64 bytes from 100.0.0.9: icmp_seq=1 ttl=64 time=42.9 ms
64 bytes from 100.0.0.9: icmp_seq=2 ttl=64 time=1.90 ms
64 bytes from 100.0.0.9: icmp_seq=3 ttl=64 time=1.17 ms
64 bytes from 100.0.0.9: icmp_seq=4 ttl=64 time=1.71 ms
^C
--- 100.0.0.9 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3094ms
rtt min/avg/max/mdev = 1.174/11.934/42.949/17.908 ms
root@pc1:/# ping 100.0.0.10
PING 100.0.0.10 (100.0.0.10) 56(84) bytes of data.

```

```

UbuntuB2206008 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities XTerm Oct 10 23:46
root@pc1: /root@pc1: ~
root@pc1:/# route add default gw 195.11.14.1
root@pc1:/# route -n
Kernel IP routing table
Destination     Gateway         Genmask        Flags Metric Ref    Use Iface
0.0.0.0          195.11.14.1   0.0.0.0       UG    0      0        0 eth0
195.11.14.0     0.0.0.0       255.255.255.0   U     0      0        0 eth0
root@pc1:/# ping 100.0.0.9
PING 100.0.0.9 (100.0.0.9) 56(84) bytes of data.
64 bytes from 100.0.0.9: icmp_seq=1 ttl=64 time=42.9 ms
64 bytes from 100.0.0.9: icmp_seq=2 ttl=64 time=1.90 ms
64 bytes from 100.0.0.9: icmp_seq=3 ttl=64 time=1.17 ms
64 bytes from 100.0.0.9: icmp_seq=4 ttl=64 time=1.71 ms
^C
--- 100.0.0.9 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3094ms
rtt min/avg/max/mdev = 1.174/11.934/42.949/17.908 ms
root@pc1:/# ping 100.0.0.10
PING 100.0.0.10 (100.0.0.10) 56(84) bytes of data.
^C
--- 100.0.0.10 ping statistics ---
49 packets transmitted, 0 received, 100% packet loss, time 53356ms
root@pc1:/# ping 100.0.0.10
PING 100.0.0.10 (100.0.0.10) 56(84) bytes of data.
^C
--- 100.0.0.10 ping statistics ---
13 packets transmitted, 0 received, 100% packet loss, time 12399ms
root@pc1:/# 

```

```

root@r2: /root@r2: ~
--- Startup Commands Log
++ ifconfig eth0 195.11.1.1/24 up
++ ifconfig eth1 100.0.0.10/30 up
--- End Startup Commands Log
root@r2:/# tcpdump -tenni eth1
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), snapshot length 262144 bytes
06:23:5a:81:4c:d5 > ce:d5:b:e4:25:d5, ethertype IPv4 (0x0800), length 98: 195.1
1.14.5 > 100.0.0.10: ICMP echo request, id 12, seq 7, length 64
06:23:5a:81:4c:d5 > ce:d5:b:e4:25:d5, ethertype IPv4 (0x0800), length 98: 195.1
1.14.5 > 100.0.0.10: ICMP echo request, id 12, seq 8, length 64
06:23:5a:81:4c:d5 > ce:d5:b:e4:25:d5, ethertype IPv4 (0x0800), length 98: 195.1
1.14.5 > 100.0.0.10: ICMP echo request, id 12, seq 9, length 64
06:23:5a:81:4c:d5 > ce:d5:b:e4:25:d5, ethertype IPv4 (0x0800), length 98: 195.1
1.14.5 > 100.0.0.10: ICMP echo request, id 12, seq 10, length 64
06:23:5a:81:4c:d5 > ce:d5:b:e4:25:d5, ethertype IPv4 (0x0800), length 98: 195.1
1.14.5 > 100.0.0.10: ICMP echo request, id 12, seq 11, length 64
06:23:5a:81:4c:d5 > ce:d5:b:e4:25:d5, ethertype IPv4 (0x0800), length 98: 195.1
1.14.5 > 100.0.0.10: ICMP echo request, id 12, seq 12, length 64
06:23:5a:81:4c:d5 > ce:d5:b:e4:25:d5, ethertype IPv4 (0x0800), length 98: 195.1
1.14.5 > 100.0.0.10: ICMP echo request, id 12, seq 13, length 64
^C
7 packets captured
7 packets received by filter
0 packets dropped by kernel
root@r2:/# 

```

- Interfaces on r2 seem unreachable, can you tell why?
  - R2 only echo requests.
  - Because we just added a gateway for pc1 so r2 still can't know where to forward the replies when it receives packets.
- Add route r2 - r1 eth0, gateway r1 eth1
  - Route -n
  - Route add-net 195.11.14.0/24 gw 100.0.0.9 dev eth1
  - Route -n

```

root@UbuntuB2206008:~/exercise03# tree
.
root@UbuntuB2206008:~/exercise03# tcpdump -tnei eth1
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), snapshot length 262144 bytes
06:23:5a:81:4c:d5 > ce:d5:b5:e4:25:d5, ethertype IPv4 (0x0800), length 98: 195.1
1.14.5 > 100.0.0.10: ICMP echo request, id 12, seq 7, length 64
06:23:5a:81:4c:d5 > ce:d5:b5:e4:25:d5, ethertype IPv4 (0x0800), length 98: 195.1
1.14.5 > 100.0.0.10: ICMP echo request, id 12, seq 8, length 64
06:23:5a:81:4c:d5 > ce:d5:b5:e4:25:d5, ethertype IPv4 (0x0800), length 98: 195.1
1.14.5 > 100.0.0.10: ICMP echo request, id 12, seq 9, length 64
06:23:5a:81:4c:d5 > ce:d5:b5:e4:25:d5, ethertype IPv4 (0x0800), length 98: 195.1
1.14.5 > 100.0.0.10: ICMP echo request, id 12, seq 10, length 64
06:23:5a:81:4c:d5 > ce:d5:b5:e4:25:d5, ethertype IPv4 (0x0800), length 98: 195.1
1.14.5 > 100.0.0.10: ICMP echo request, id 12, seq 11, length 64
06:23:5a:81:4c:d5 > ce:d5:b5:e4:25:d5, ethertype IPv4 (0x0800), length 98: 195.1
1.14.5 > 100.0.0.10: ICMP echo request, id 12, seq 12, length 64
06:23:5a:81:4c:d5 > ce:d5:b5:e4:25:d5, ethertype IPv4 (0x0800), length 98: 195.1
1.14.5 > 100.0.0.10: ICMP echo request, id 12, seq 13, length 64
^C
7 packets captured
7 packets received by filter
0 packets dropped by kernel
root@r2:/#
Kernel IP routing table
Destination     Gateway         Genmask        Flags Metric Ref    Use Iface
100.0.0.8        0.0.0.0        255.255.255.252 U        0      0        0 eth1
200.1.1.0        0.0.0.0        255.255.255.0   U        0      0        0 eth0
root@r2:/# route add -net 195.11.14.0/24 gw 100.0.0.9 dev eth1
root@r2:/# route -n
Kernel IP routing table
Destination     Gateway         Genmask        Flags Metric Ref    Use Iface
100.0.0.8        0.0.0.0        255.255.255.252 U        0      0        0 eth1
195.11.14.0     100.0.0.9      255.255.255.0   UG       0      0        0 eth1
200.1.1.0        0.0.0.0        255.255.255.0   U        0      0        0 eth0
root@r2:/# 
```

- **Ping from pc1 to r2 eth1**  
ping 100.0.0.10
  - **Sniff packets sent from pc1 to r2 eth1**  
Tcpcdump -t r2 eth1

- **Add route r1 to r2 eth0, through r1 eth1**  
Route add –net 200.1.1.0/24 gw 100.0.0.10 dev eth1

UbuntuB2206008 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Activities X XTerm Oct 11 00:46

root@r1:/# route add -net 200.1.1.0/24 gw 100.0.0.10 dev eth1  
SIOCADDRT: File exists  
root@r1:/# route -n  
Kernel IP routing table  

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
100.0.0.8	0.0.0.0	255.255.255.252	U	0	0	0	eth1
195.11.14.0	0.0.0.0	255.255.255.0	U	0	0	0	eth0
200.1.1.0	100.0.0.10	255.255.255.0	UG	0	0	0	eth1

root@r1:/#

- Add default gateway r2 - pc2

```
route -n
```

```
route add default gateway 200.1.1.1
```

```
route -n
```

```
root@pc2:/# route add -net 195.11.14.0/24 gw 100.0.0.9 dev eth1
SIOCADDRT: No such device
root@pc2:/# route -n
Kernel IP routing table
Destination      Gateway          Genmask         Flags Metric Ref  Use Iface
200.1.1.0        0.0.0.0          255.255.255.0   U     0      0      0 eth0
root@pc2:/# route add default gateway 200.1.1.1
root@pc2:/# route -n
Kernel IP routing table
Destination      Gateway          Genmask         Flags Metric Ref  Use Iface
0.0.0.0          200.1.1.1        0.0.0.0         UG    0      0      0 eth0
200.1.1.0        0.0.0.0          255.255.255.0   U     0      0      0 eth0
root@pc2:/# route add -net 195.11.14.0/24 gw 100.0.0.9 dev eth1
SIOCADDRT: No such device
root@pc2:/#
```

- Ping from p2 to p1

```
Ping 195.11.14.5
```

```
root@pc2:/# ping 195.11.14.5
PING 195.11.14.5 (195.11.14.5) 56(84) bytes of data.
64 bytes from 195.11.14.5: icmp_seq=1 ttl=62 time=128 ms
64 bytes from 195.11.14.5: icmp_seq=2 ttl=62 time=6.58 ms
^C
--- 195.11.14.5 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1022ms
rtt min/avg/max/mdev = 6.580/67.500/128.420/60.920 ms
root@pc2:/#
```

### **Proposed Exercise:**

- A command to configure a static route that is equivalent to the default route (route add default gw 195.11.14.1 dev eth0):  
route add -net 0.0.0.0/0 gw 195.11.14.1 dev eth0

### **Exercise 4:**

#### **Solution:**

- Create exercise04 directory and config the lab

#### **File:**

Lab.conf:

```
r1[0]="A"  
r1[1]="B"  
r2[0]="C"  
r2[1]="B"  
pc1[0]="A"  
pc2[0]="C"  
pc3[0]="C"
```

Pc1.startup:

```
ifconfig eth0 195.11.14.5 up  
route add default gw 195.11.14.1
```

Pc2.startup:

```
ifconfig eth0 200.1.1.7 up  
route add default gw 200.1.1.1
```

Pc3.startup:

```
ifconfig eth0 200.1.1.3 up  
route add default gw 200.1.1.1
```

R1.startup:

```
ifconfig eth0 195.11.14.1 up  
ifconfig eth1 100.0.0.9 netmask 255.255.255.252 broadcast 100.0.0.11 up  
route add -net 200.1.1.0 netmask 255.255.255.0 gw 100.0.0.10 dev eth1
```

R2.startup:

```
ifconfig eth0 200.1.1.1 up  
ifconfig eth1 100.0.0.10 netmask 255.255.255.252 broadcast 100.0.0.11 up  
route add -net 195.11.14.0 netmask 255.255.255.0 gw 100.0.0.9 dev eth1ls
```

UbuntuB2206008 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Activities Terminal

```
root@UbuntuB2206008:~/exercise04# tree
.
|-- lab.conf
|-- pc1.startup
|-- pc2.startup
|-- pc3.startup
|-- r1.startup
`-- r2.startup

0 directories, 6 files
root@UbuntuB2206008:~/exercise04# cat lab.conf
r1[0]="A"
r1[1]="B"
r2[0]="C"
r2[1]="B"
pc1[0]="A"
pc2[0]="C"
pc3[0]="C"
root@UbuntuB2206008:~/exercise04# cat pc1.startup
ifconfig eth0 195.11.14.5 up
route add default gw 195.11.14.1
root@UbuntuB2206008:~/exercise04#
```

UbuntuB2206008 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help Oct 11 19:01

Activities Terminal

```
r2[1]="B"
pc1[0]="A"
pc2[0]="C"
pc3[0]="C"
root@UbuntuB2206008:~/exercise04# cat pc1.startup
ifconfig eth0 195.11.14.5 up
route add default gw 195.11.14.1
root@UbuntuB2206008:~/exercise04# cat pc2.startup
ifconfig eth0 200.1.1.7 up
route add default gw 200.1.1.1
root@UbuntuB2206008:~/exercise04# cat pc3.startup
ifconfig eth0 200.1.1.3 up
route add default gw 200.1.1.1
root@UbuntuB2206008:~/exercise04# cat r1.startup
ifconfig eth0 195.11.14.1 up
ifconfig eth1 100.0.0.9 netmask 255.255.255.252 broadcast 100.0.0.11 up
route add -net 200.1.1.0 netmask 255.255.255.0 gw 100.0.0.10 dev eth1
root@UbuntuB2206008:~/exercise04# cat r2.startup
ifconfig eth0 200.1.1.1 up
ifconfig eth1 100.0.0.10 netmask 255.255.255.252 broadcast 100.0.0.11 up
route add -net 195.11.14.0 netmask 255.255.255.0 gw 100.0.0.9 dev eth1
root@UbuntuB2206008:~/exercise04#
```

- Start the scenario

Kathara lstart

UbuntuB2206008 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Activities XTerm Oct 11 19:15

root@UbuntuB2206008:~/exercise04# kathara lstart

Starting Network Scenario

[Deploying collision domains] 3/3  
[Deploying devices] 5/5

root@UbuntuB2206008:~/exercise04#

root@r2: / --- Startup Commands Log  
++ ifconfig eth0 200.1.1.1 up  
++ ifconfig eth1 100.0.0.10 netmask 255.255.255.252 broadcast 100.0.0.255  
++ route add -net 195.11.14.0 netmask 255.255.255.0 gw 100.0.0.1  
--- End Startup Commands Log  
root@r2:/#

root@pc3: / --- Startup Commands Log  
++ ifconfig eth0 200.1.1.3 up  
++ route add default gw 200.1.1.1  
--- End Startup Commands Log  
root@pc3:/#

root@pc1: / --- Startup Commands Log  
++ ifconfig eth0 195.11.14.5 up  
++ route add default gw 195.11.14.1  
--- End Startup Commands Log  
root@pc1:/#

root@pc2: / --- Startup Commands Log  
++ ifconfig eth0 200.1.1.7 up  
++ route add default gw 200.1.1.1  
--- End Startup Commands Log  
root@pc2:/#

root@r1: / --- Startup Commands Log  
++ ifconfig eth0 195.11.14.1 up  
++ ifconfig eth1 100.0.0.9 netmask 255.255.255.255 broadcast 100.0.0.255  
++ route add -net 200.1.1.0 netmask 255.255.255.255 gw 195.11.14.1  
--- End Startup Commands Log  
root@r1:/#

- Inspect arp cache (local traffic)

Pc3:

```
Arp  
Ping 200.1.1.7 (pc2)  
Arp -n
```

Pc2:

```
Arp -n
```

The screenshot shows a Linux desktop environment with two terminal windows open in a window manager.

The top bar includes "File", "Machine", "View", "Input", "Devices", "Help", "Activities", and "XTerm". The date and time "Oct 11 19:33" are also displayed.

The left terminal window (root@pc3: /) contains the following commands and output:

```
root@pc3:/# arp  
root@pc3:/# ping 200.1.1.7  
PING 200.1.1.7 (200.1.1.7) 56(84) bytes of data.  
64 bytes from 200.1.1.7: icmp_seq=1 ttl=64 time=22.8 ms  
64 bytes from 200.1.1.7: icmp_seq=2 ttl=64 time=3.02 ms  
^C  
--- 200.1.1.7 ping statistics ---  
2 packets transmitted, 2 received, 0% packet loss, time 1090ms  
rtt min/avg/max/mdev = 3.019/12.929/22.840/9.910 ms  
root@pc3:/# arp -n  
Address      HWtype  HWaddress          Flags Mask  
200.1.1.7    ether    2e:d9:15:a4:4b:7a  C  
root@pc3:/# 
```

The right terminal window (root@pc2: /) contains the following command and output:

```
root@pc2:/# arp -n  
--- Startup Commands Log  
++ ifconfig eth0 200.1.1.7 up  
++ route add default gw 200.1.1.1  
--- End Startup Commands Log  
root@pc2:/# Address      HWtype  HWaddress          Flags Mask  
200.1.1.3    ether    8e:ea:83:d4  C  
:84:3b      C  
root@pc2:/# 
```

- **Inspect arp cache (non-local traffic)**

Pc2:

Ping 195.11.14.5 (pc1)

Arp -n (r2 eth0 MAC address added instead of pc1 MAC address)

```
root@UbuntuB2206008 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities XTerm Oct 11 19:52
root@UbuntuB2206008:~/exercise04# kathara lstart
root@pc2: / 3/3
root@pc2: / 5/5
root@pc2:/# ping 195.11.14.5
PING 195.11.14.5 (195.11.14.5) 56(84) bytes of data.
64 bytes from 195.11.14.5: icmp_seq=1 ttl=62 time=58.1 ms
64 bytes from 195.11.14.5: icmp_seq=2 ttl=62 time=10.5 ms
^C
--- 195.11.14.5 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1010ms
rtt min/avg/max/mdev = 10.496/34.284/58.072/23.788 ms
root@pc2:/# arp -n
Address      Iface      Hwtype   Hwaddress      Flags Mask
200.1.1.1    eth0      ether     06:f1:e7:bb:6b:9f  C
200.1.1.3    eth0      ether     8e:ea:83:d4:84:3b  C
root@pc2:/#
```

- **Restart scenario to clear arp caches**

Kathara lclean

Kathara lstart

```
root@UbuntuB2206008 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Oct 11 20:33
root@UbuntuB2206008:~/exercise04# kathara lstart
Starting Network Scenario
[Deploying collision domains] 3/3
[Deploying devices] 5/5
root@UbuntuB2206008:~/exercise04# kathara lclean
Stopping Network Scenario
[Deleting devices] 5/5
[Deleting collision domains] 3/3
root@UbuntuB2206008:~/exercise04# kathara lstart
Starting Network Scenario
[Deploying collision domains] 3/3
[Deploying devices] 5/5
root@UbuntuB2206008:~/exercise04#
```

- Sniffing arp traffic

Pc2:

Ping 195.11.14.5

R2:

Tcpdump -telli eth0

R1:

Tcpdump -telli eth1

Pc1:

Tcpdump -telli eth0

```

UbuntuB2206008 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities XTerm Oct 11 20:44
root@UbuntuB2206008:~/exercise04# kathara lstart
root@pc2:/ 
--- Startup Commands Log
++ ifconfig eth0 200.1.1.7 up
++ route add default gw 200.1.1.1
--- End Startup Commands Log
root@pc2:/# ping 195.11.14.5
PING 195.11.14.5 (195.11.14.5) 56(84) bytes of data.
64 bytes from 195.11.14.5: icmp_seq=1 ttl=62 time=1.79 ms
64 bytes from 195.11.14.5: icmp_seq=2 ttl=62 time=7.72 ms
^C
--- 195.11.14.5 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1005ms
rtt min/avg/max/mdev = 7.720/95.383/179.047/85.663 ms
root@pc2:/# 

root@r2:/ 
--- Startup Commands Log
++ ifconfig eth0 200.1.1.1 up
++ ifconfig eth1 100.0.0.10 netmask 255.255.255.252 broadcast 100.0.0.11 up
++ route add -net 195.11.14.0 netmask 255.255.255.0 gw 100.0.0.9 dev eth1
--- End Startup Commands Log
root@r2:/# tcpdump -telli eth0
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
5: f4:5b:8e:aa:86 > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 60: Request who-has 200.1.1.1 tell 200.1.1.7, length 46
ba:3f:39:f2:90:22 > 5:f4:5b:8e:aa:86, ethertype ARP (0x0806), length 42: Reply 200.1.1.1 is-at ba:3f:39:f2:90:22, length 28
5:f4:5b:8e:aa:86 > ba:3f:39:f2:90:22, ethertype IPv4 (0x0800), length 98: 200.1
.1.7 > 195.11.14.5 ICMP echo request, id 5, seq 1, length 64
ba:3f:39:f2:90:22 > 5:f4:5b:8e:aa:86, ethertype IPv4 (0x0800), length 98: 195.1
.1.4.5 > 200.1.1.7 ICMP echo reply, id 5, seq 1, length 64
5:f4:5b:8e:aa:86 > ba:3f:39:f2:90:22, ethertype IPv4 (0x0800), length 98: 200.1
.1.7 > 195.11.14.5 ICMP echo request, id 5, seq 2, length 64
ba:3f:39:f2:90:22 > 5:f4:5b:8e:aa:86, ethertype IPv4 (0x0800), length 98: 195.1

root@r1:/ 
--- Startup Commands Log
++ ifconfig eth0 195.11.14.1 up
++ ifconfig eth1 100.0.0.9 netmask 255.255.255.252 broadcast 100.0.0.11 up
++ route add -net 200.1.1.0 netmask 255.255.255.0 gw 100.0.0.10 dev eth1
--- End Startup Commands Log
root@r1:/# tcpdump -telli eth1
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), snapshot length 262144 bytes
5:5d:d8:dc:40:b4 > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 60: Request who-has 195.11.14.5 tell 195.11.14.1, length 46
c6:b2:68:6:c:c:24 > 5:5d:d8:dc:40:b4, ethertype ARP (0x0806), length 42: Reply 100.0.0.9 is-at c6:b2:68:6:c:c:24, length 28
5:5d:d8:dc:40:b4 > c6:b2:68:6:c:c:24, ethertype IPv4 (0x0800), length 98: 200.1
.1.7 > 195.11.14.5 ICMP echo request, id 5, seq 1, length 64
c6:b2:68:6:c:c:24 > 5:5d:d8:dc:40:b4, ethertype IPv4 (0x0800), length 98: 195.1
.1.4.5 > 200.1.1.7 ICMP echo reply, id 5, seq 1, length 64
5:5d:d8:dc:40:b4 > c6:b2:68:6:c:c:24, ethertype IPv4 (0x0800), length 98: 200.1
.1.7 > 195.11.14.5 ICMP echo request, id 5, seq 2, length 64

root@pc1:/ 
--- Startup Commands Log
++ ifconfig eth0 195.11.14.5 up
++ route add default gw 195.11.14.1
--- End Startup Commands Log
root@pc1:/# tcpdump -telli eth0
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
be:97:4f:9f:f1:ac > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 60: Request who-has 195.11.14.5 tell 195.11.14.1, length 46
62:38:30:1:c:ec:1f > be:97:4f:9f:f1:ac, ethertype ARP (0x0806), length 42: Reply 195.11.14.5 is-at 62:38:30:1:c:ec:1f, length 28
be:97:4f:9f:f1:ac > 62:38:30:1:c:ec:1f, ethertype IPv4 (0x0800), length 98: 200.1
.1.7 > 195.11.14.5 ICMP echo request, id 5, seq 1, length 64
62:38:30:1:c:ec:1f > be:97:4f:9f:f1:ac, ethertype IPv4 (0x0800), length 98: 195.1
.1.4.5 > 200.1.1.7 ICMP echo reply, id 5, seq 1, length 64
be:97:4f:9f:f1:ac > 62:38:30:1:c:ec:1f, ethertype IPv4 (0x0800), length 98: 200.1
.1.7 > 195.11.14.5 ICMP echo request, id 5, seq 2, length 64
62:38:30:1:c:ec:1f > be:97:4f:9f:f1:ac, ethertype IPv4 (0x0800), length 98: 195.1

```

```

UbuntuB2206008 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities XTerm Oct 11 20:47
root@UbuntuB2206008: ~/exercise04#
root@pc2: / root@r2: / root@r1: / root@pc1: /
root@pc2:~# kathara lstart
root@pc2:~# ping 195.11.14.5
PING 195.11.14.5 56(84) bytes of data.
64 bytes from 195.11.14.5: icmp_seq=1 ttl=62 time=179 ms
64 bytes from 195.11.14.5: icmp_seq=2 ttl=62 time=7.72 ms
--- 195.11.14.5 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1005ms
rtt min/avg/max/mdev = 7.720/93.383/179.047/85.663 ms
root@pc2:~# []
root@pc2:~# 

root@r2: / root@r1: / root@pc1: /
root@r2:~# ba:3f:39:f2:90:22 > 5e:f4:5b:8e:aa:86, ethertype ARP (0x0806), length 42: Reply
200.1.1.1 is-at ba:3f:39:f2:90:22, length 28
5e:f4:5b:8e:aa:86 > ba:3f:39:f2:90:22, ethertype IPv4 (0x0800), length 98: 200.1
.1.7 > 195.11.14.5: ICMP echo request, id 5, seq 1, length 64
ba:3f:39:f2:90:22 > 5e:f4:5b:8e:aa:86, ethertype IPv4 (0x0800), length 98: 195.1
.1.4.5 > 200.1.1.7: ICMP echo reply, id 5, seq 1, length 64
5e:f4:5b:8e:aa:86 > ba:3f:39:f2:90:22, ethertype IPv4 (0x0800), length 98: 200.1
.1.7 > 195.11.14.5: ICMP echo request, id 5, seq 2, length 64
ba:3f:39:f2:90:22 > 5e:f4:5b:8e:aa:86, ethertype IPv4 (0x0800), length 98: 195.1
.1.4.5 > 200.1.1.7: ICMP echo reply, id 5, seq 2, length 64
ba:3f:39:f2:90:22 > 5e:f4:5b:8e:aa:86, ethertype ARP (0x0806), length 42: Request
t who-has 200.1.1.7 tell 200.1.1.1, length 28
5e:f4:5b:8e:aa:86 > ba:3f:39:f2:90:22, ethertype ARP (0x0806), length 60: Reply
200.1.1.7 is-at 5e:f4:5b:8e:aa:86, length 46
^C
8 packets captured
8 packets received by filter
0 packets dropped by kernel
root@r2:~# []

root@r1: / root@pc1: /
root@r1:~# 100.0.0.9 is-at c6:b2:68:6c:cc:24, length 28
5e:5d:d8:dc:40:b4 > c6:b2:68:6c:cc:24, ethertype IPv4 (0x0800), length 98: 200.1
.1.7 > 195.11.14.5: ICMP echo request, id 5, seq 1, length 64
c6:b2:68:6c:cc:24 > 5e:5d:d8:dc:40:b4, ethertype IPv4 (0x0800), length 98: 195.1
.1.4.5 > 200.1.1.7: ICMP echo reply, id 5, seq 1, length 64
5e:5d:d8:dc:40:b4 > c6:b2:68:6c:cc:24, ethertype IPv4 (0x0800), length 98: 200.1
.1.7 > 195.11.14.5: ICMP echo request, id 5, seq 2, length 64
c6:b2:68:6c:cc:24 > 5e:5d:d8:dc:40:b4, ethertype IPv4 (0x0800), length 98: 195.1
.1.4.5 > 200.1.1.7: ICMP echo reply, id 5, seq 2, length 64
c6:b2:68:6c:cc:24 > 5e:5d:d8:dc:40:b4, ethertype ARP (0x0806), length 42: Request
t who-has 100.0.0.10 tell 100.0.0.9, length 28
5e:5d:d8:dc:40:b4 > c6:b2:68:6c:cc:24, ethertype ARP (0x0806), length 60: Reply
100.0.0.10 is-at 5e:5d:d8:dc:40:b4, length 46
^C
8 packets captured
8 packets received by filter
0 packets dropped by kernel
root@r1:~# []

root@pc1: / root@pc1: /
root@pc1:~# 195.11.14.5 is-at 62:38:30:1c:ec:1f, length 28
be:97:4f:9f:f1:ac > 62:38:30:1c:ec:1f, ethertype IPv4 (0x0800), length 98: 200.1
.1.7 > 195.11.14.5: ICMP echo request, id 5, seq 1, length 64
62:38:30:1c:ec:1f > be:97:4f:9f:f1:ac, ethertype IPv4 (0x0800), length 98: 195.1
.1.4.5 > 200.1.1.7: ICMP echo reply, id 5, seq 1, length 64
be:97:4f:9f:f1:ac > 62:38:30:1c:ec:1f, ethertype IPv4 (0x0800), length 98: 200.1
.1.7 > 195.11.14.5: ICMP echo request, id 5, seq 2, length 64
62:38:30:1c:ec:1f > be:97:4f:9f:f1:ac, ethertype IPv4 (0x0800), length 98: 195.1
.1.4.5 > 200.1.1.7: ICMP echo reply, id 5, seq 2, length 64
62:38:30:1c:ec:1f > be:97:4f:9f:f1:ac, ethertype ARP (0x0806), length 42: Request
t who-has 195.11.14.1 tell 195.11.14.5, length 28
be:97:4f:9f:f1:ac > 62:38:30:1c:ec:1f, ethertype ARP (0x0806), length 60: Reply
195.11.14.1 is-at be:97:4f:9f:f1:ac, length 46
^C
8 packets captured
8 packets received by filter
0 packets dropped by kernel
root@pc1:~# []

```

- **Proposed Exercise:**

If we keep pinging from pc2 to pc1, there are only unicast packets since the ARP resolution from pc2 to pc1 has been completed, so there's no need of broadcast transmitting.

- **Proposed Exercise**

**Local destination:** the source device keep broadcasting ask for the MAC address of destination device, but no device reply since they don't know.

**Non-local destination:** Error: Destination net unreachable

**Packages captured:**

**Local destination:** just ARP requests but no ARP replies.

**Non-local destination:** no packet is exchanged in local domain

**Exercise 5:**

**Solution:**

**File:**

lab.conf:

```
pc1[0]="A"
pc2[0]="B"
pc3[0]="C"
router1[0]="A"
router1[1]="B"
router2[0]="A"
router2[1]="C"

router1.startup:
    ifconfig eth0 10.0.0.1/24 up
    ifconfig eth1 10.0.1.1/24 up
    route add -net 10.0.2.0/24 gw 10.0.0.2

router2.startup:
    ifconfig eth0 10.0.0.2/24 up
    ifconfig eth1 10.0.2.1/24 up
    route add -net 10.0.1.0/24 gw 10.0.0.1

pc1.startup:
    ifconfig eth0 10.0.0.101/24 up
    route add -net 10.0.1.0/24 gw 10.0.0.1
    route add -net 10.0.2.0/24 gw 10.0.0.2

pc2.startup:
    ifconfig eth0 10.0.1.101/24 up
    route add default gw 10.0.1.1

pc3.startup:
    ifconfig eth0 10.0.2.101/24 up
    route add default gw 10.0.2.1
```

- Config scenario

The screenshot shows a terminal window titled "root@UbuntuB2206008 [Running] - Oracle VM VirtualBox". The terminal content displays the following configuration steps:

```
root@UbuntuB2206008:~/exercise05# ls
lab.conf  pc1.startup  pc2.startup  pc3.startup  router1.startup  router2.startup
pc1        pc2        pc3        router1      router2

root@UbuntuB2206008:~/exercise05# cat lab.conf
pc1[0]="A"
pc2[0]="B"
pc3[0]="C"
router1[0]="A"
router1[1]="B"
router2[0]="A"
router2[1]="C"

root@UbuntuB2206008:~/exercise05# cat router1.startup
ifconfig eth0 10.0.0.1/24 up
ifconfig eth1 10.0.1.1/24 up
route add -net 10.0.2.0/24 gw 10.0.0.2
root@UbuntuB2206008:~/exercise05# cat router2.startup
ifconfig eth0 10.0.0.2/24 up
ifconfig eth1 10.0.2.1/24 up
route add -net 10.0.1.0/24 gw 10.0.0.1
root@UbuntuB2206008:~/exercise05# cat pc1.startup
ifconfig eth0 10.0.0.101/24 up
route add -net 10.0.1.0/24 gw 10.0.0.1
route add -net 10.0.2.0/24 gw 10.0.0.2
root@UbuntuB2206008:~/exercise05# cat pc2.startup
ifconfig eth0 10.0.1.101/24 up
route add default gw 10.0.1.1
root@UbuntuB2206008:~/exercise05# cat pc3.startup
ifconfig eth0 10.0.2.101/24 up
route add default gw 10.0.2.1
root@UbuntuB2206008:~/exercise05#
```

- Ping check the network

Pc1:

```
Route -n
Ping 10.0.1.101
Ping 10.0.2.101
```

Pc2:

```
Route -n
Ping 10.0.2.101
```

Pc3:

```
Route -n
Ping 10.0.0.101
```

Router1:

```
Router -n
```

Router2:

```
Router -n
```

The screenshot shows an Ubuntu desktop environment with three terminal windows (XTerm) running on different hosts (pc1, pc2, pc3). Each window displays command-line output for route configuration and ping tests.

**Terminal 1 (root@pc1: /)**

```
--- End Startup Commands Log
root@pc1:~# route -n
Kernel IP routing table
Destination     Gateway         Genmask        Flags Metric Ref  Use Iface
10.0.0.0         0.0.0.0       255.255.255.0 U     0      0      0 eth0
10.0.1.0         10.0.1.1      255.255.255.0 UG    0      0      0 eth0
10.0.2.0         10.0.2.0      255.255.255.0 UG    0      0      0 eth0
root@pc1:~# ping 10.0.1.101
PING 10.0.1.101 (10.0.1.101) 56(84) bytes of data.
64 bytes from 10.0.1.101: icmp_seq=1 ttl=63 time=56.9 ms
64 bytes from 10.0.1.101: icmp_seq=2 ttl=63 time=5.37 ms
^C
--- 10.0.1.101 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1100ms
rtt min/avg/max/mdev = 5.367/31.121/56.876/25.754 ms
root@pc1:~# ping 10.0.2.101
PING 10.0.2.101 (10.0.2.101) 56(84) bytes of data.
64 bytes from 10.0.2.101: icmp_seq=1 ttl=63 time=28.5 ms
64 bytes from 10.0.2.101: icmp_seq=2 ttl=63 time=3.41 ms
^C
--- 10.0.2.101 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 3.406/15.977/28.548/12.571 ms
root@pc1:~# 
```

**Terminal 2 (root@pc2: /)**

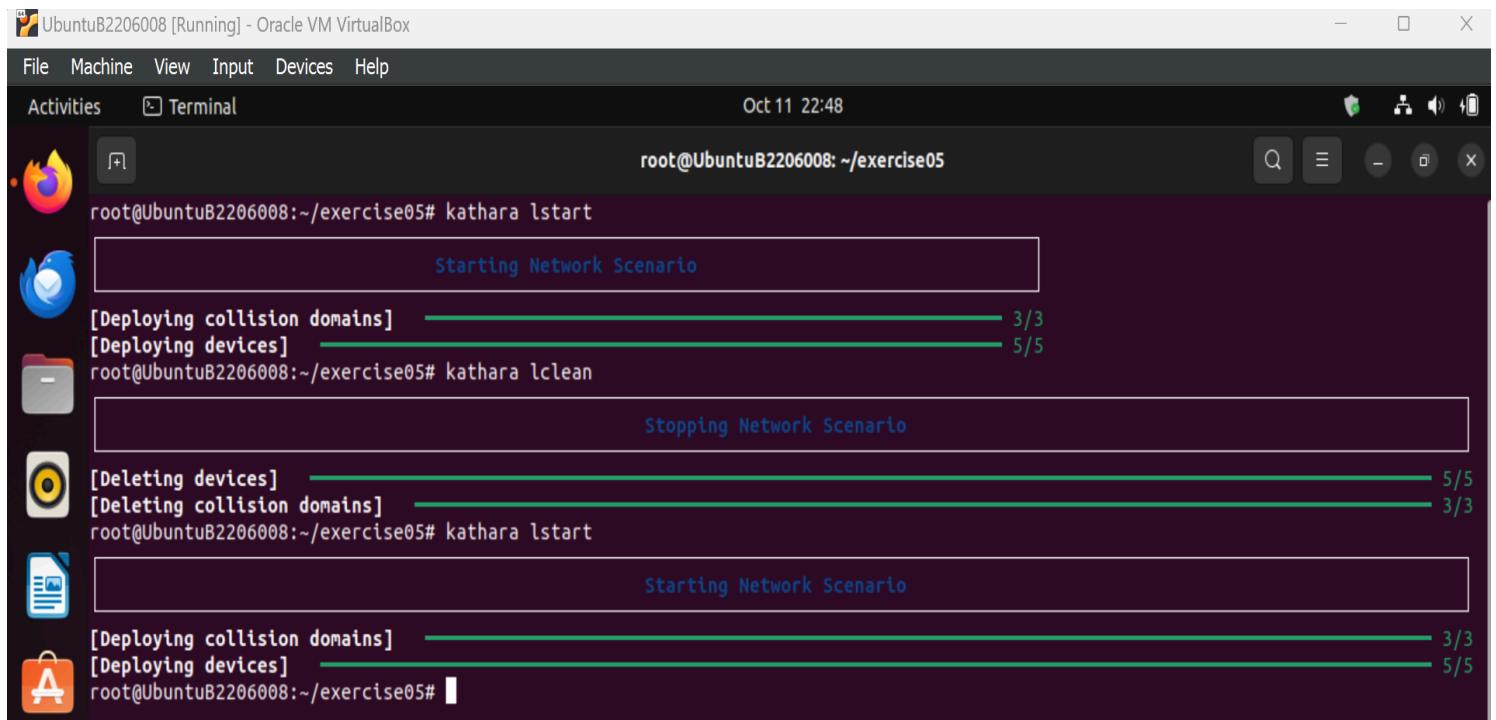
```
--- Startup Commands Log
++ ifconfig eth0 10.0.1.101/24 up
++ route add default gw 10.0.1.1
--- End Startup Commands Log
root@pc2:~# route -n
Kernel IP routing table
Destination     Gateway         Genmask        Flags Metric Ref  Use Iface
0.0.0.0         10.0.1.1      0.0.0.0       UG    0      0      0 eth0
10.0.1.0        0.0.0.0       255.255.255.0 U     0      0      0 eth0
root@pc2:~# ping 10.0.2.101
PING 10.0.2.101 (10.0.2.101) 56(84) bytes of data.
64 bytes from 10.0.2.101: icmp_seq=1 ttl=62 time=78.6 ms
64 bytes from 10.0.2.101: icmp_seq=2 ttl=62 time=2.65 ms
^C
--- 10.0.2.101 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 2.648/40.643/78.638/37.995 ms
root@pc2:~# 
```

**Terminal 3 (root@pc3: /)**

```
--- Startup Commands Log
++ ifconfig eth0 10.0.2.101/24 up
++ route add default gw 10.0.2.1
--- End Startup Commands Log
root@pc3:~# route -n
Kernel IP routing table
Destination     Gateway         Genmask        Flags Metric Ref  Use Iface
0.0.0.0         10.0.2.1      0.0.0.0       UG    0      0      0 eth0
10.0.2.0        0.0.0.0       255.255.255.0 U     0      0      0 eth0
root@pc3:~# ping 10.0.0.101
PING 10.0.0.101 (10.0.0.101) 56(84) bytes of data.
64 bytes from 10.0.0.101: icmp_seq=1 ttl=63 time=56.8 ms
64 bytes from 10.0.0.101: icmp_seq=2 ttl=63 time=5.79 ms
64 bytes from 10.0.0.101: icmp_seq=3 ttl=63 time=21.3 ms
^C64 bytes from 10.0.0.101: icmp_seq=4 ttl=63 time=39.1 ms
64 bytes from 10.0.0.101: icmp_seq=5 ttl=63 time=6.80 ms
64 bytes from 10.0.0.101: icmp_seq=6 ttl=63 time=17.1 ms
^C
--- 10.0.0.101 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5362ms
rtt min/avg/max/mdev = 5.791/24.494/56.797/18.186 ms
root@pc3:~# 
```

## Wireshark

- Start the scenario



The screenshot shows a terminal window titled "UbuntuB2206008 [Running] - Oracle VM VirtualBox". The window has a dark theme. The terminal output is as follows:

```
File Machine View Input Devices Help
Activities Terminal Oct 11 22:48
root@UbuntuB2206008:~/exercise05# kathara lstart
Starting Network Scenario
[Deploying collision domains] 3/3
[Deploying devices] 5/5
root@UbuntuB2206008:~/exercise05# kathara lclean
Stopping Network Scenario
[Deleting devices] 5/5
[Deleting collision domains] 3/3
root@UbuntuB2206008:~/exercise05# kathara lstart
Starting Network Scenario
[Deploying collision domains] 3/3
[Deploying devices] 5/5
root@UbuntuB2206008:~/exercise05#
```

- Ping from pc3 and sniffing at pc2, router1, router2

Pc2:

```
Tcpdump -s 1536 -w /shared/Ex5_pc2.pcap
```

Router1:

```
Tcpdump -s 1536 -w /shared/Ex5_router1.pcap
```

Router2:

```
Tcpdump -s 1536 -w /shared/Ex5_router2.pcap
```

Pc3:

```
Ping 10.0.1.101
```

The screenshot shows a desktop environment with a window titled "UbuntuB2206008 [Running] - Oracle VM VirtualBox". The desktop has a dark theme with icons for various applications like a browser, file manager, and terminal. There are four terminal windows open in XTerm tabs:

- root@pc3:/**: Shows the output of a ping command to 10.0.1.101, displaying 14 packets transmitted with 0% loss.
- root@router1:/**: Shows the output of a tcpdump session capturing 32 ICMP packets from 10.0.1.101.
- root@router2:/**: Shows the output of a tcpdump session capturing 32 ICMP packets from 10.0.1.101.
- root@pc2:/**: Shows the output of a tcpdump session capturing 32 ICMP packets from 10.0.1.101.

The terminal windows are arranged vertically on the right side of the screen, and the desktop environment includes a dock with various application icons at the bottom.

```
root@pc3:/# ping 10.0.1.101
PING 10.0.1.101 (10.0.1.101) 56(84) bytes of data.
64 bytes from 10.0.1.101: icmp_seq=1 ttl=62 time=49.9 ms
64 bytes from 10.0.1.101: icmp_seq=2 ttl=62 time=4.87 ms
64 bytes from 10.0.1.101: icmp_seq=3 ttl=62 time=6.38 ms
64 bytes from 10.0.1.101: icmp_seq=4 ttl=62 time=49.9 ms
64 bytes from 10.0.1.101: icmp_seq=5 ttl=62 time=23.8 ms
64 bytes from 10.0.1.101: icmp_seq=6 ttl=62 time=21.8 ms
64 bytes from 10.0.1.101: icmp_seq=7 ttl=62 time=3.80 ms
64 bytes from 10.0.1.101: icmp_seq=8 ttl=62 time=5.25 ms
64 bytes from 10.0.1.101: icmp_seq=9 ttl=62 time=5.53 ms
64 bytes from 10.0.1.101: icmp_seq=10 ttl=62 time=10.6 ms
64 bytes from 10.0.1.101: icmp_seq=11 ttl=62 time=8.68 ms
64 bytes from 10.0.1.101: icmp_seq=12 ttl=62 time=16.2 ms
64 bytes from 10.0.1.101: icmp_seq=13 ttl=62 time=9.25 ms
64 bytes from 10.0.1.101: icmp_seq=14 ttl=62 time=3.39 ms
^C
--- 10.0.1.101 ping statistics ---
14 packets transmitted, 14 received, 0% packet loss, time 14580ms
rtt min/avg/max/mdev = 3.387/15.659/49.893/15.258 ms
root@pc3:/# 
```

```
root@router1:/# tcpdump -s 1536 -w /shared/Ex5_router1.pcap
tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 1536 bytes
^C32 packets captured
32 packets received by filter
0 packets dropped by kernel
root@router1:/# 
```

```
root@router2:/# tcpdump -s 1536 -w /shared/Ex5_router2.pcap
tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 1536 bytes
^C32 packets captured
32 packets received by filter
0 packets dropped by kernel
root@router2:/# 
```

```
root@pc2:/# tcpdump -s 1536 -w /shared/Ex5_pc2.pcap
tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 1536 bytes
^C32 packets captured
32 packets received by filter
0 packets dropped by kernel
root@pc2:/# 
```

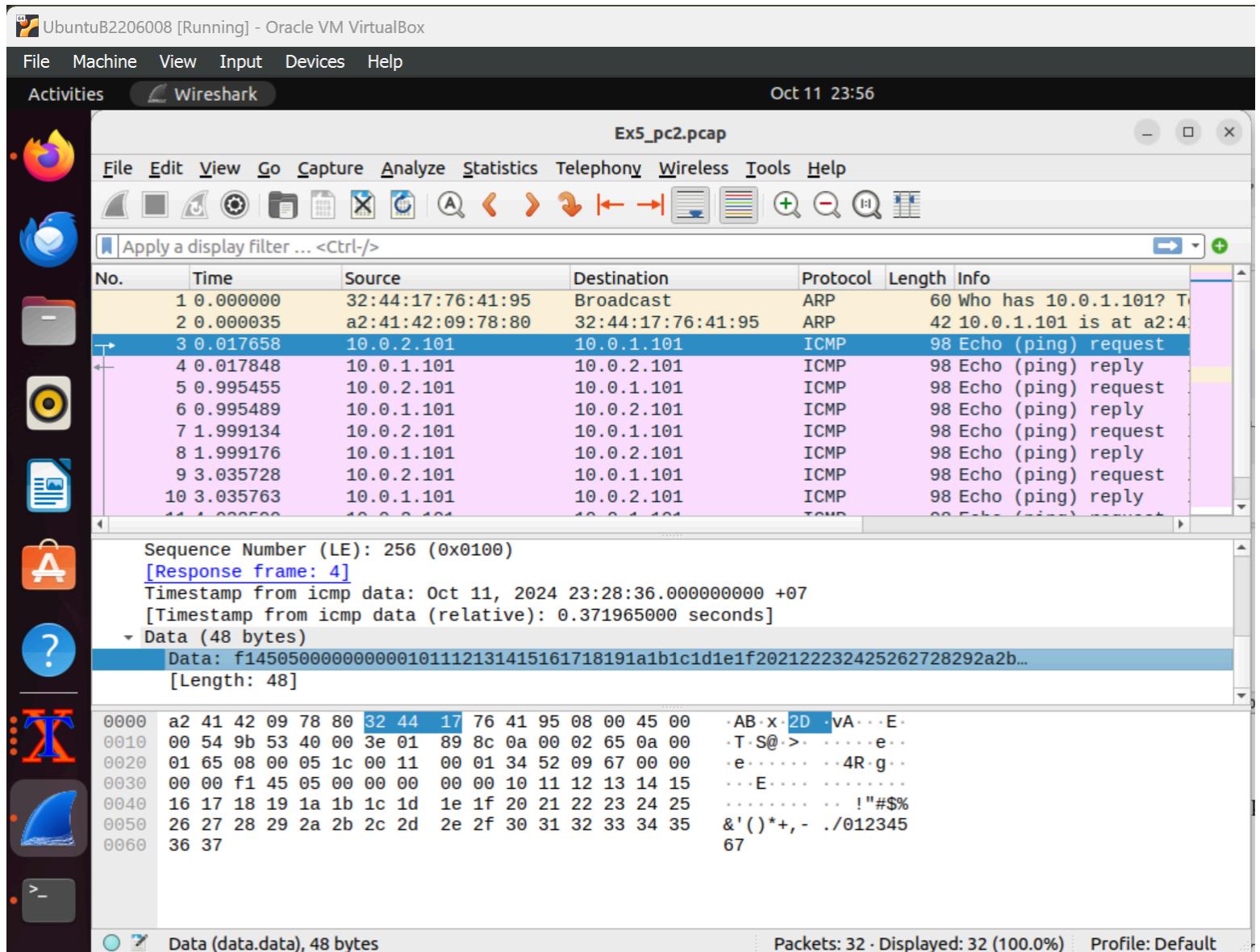
- **Open Ex5\_pc2 with Wireshark**

Wireshark ~/exercise05/shared/Ex5\_pc2.pcap

The screenshot shows the Wireshark interface with the following details:

- Title Bar:** UbuntuB2206008 [Running] - Oracle VM VirtualBox
- Menu Bar:** File, Machine, View, Input, Devices, Help
- Toolbar:** Activities, Wireshark
- Display Filter:** Ex5\_pc2.pcap
- Packet List:** Shows 32 captured packets. Packet 3 is highlighted, showing an ICMP Echo request from 10.0.2.101 to 10.0.1.101. Subsequent packets show ICMP Echo replies from 10.0.1.101 back to 10.0.2.101.
- Details Pane:** Displays the ICMP message structure for selected packet 3. It shows fields like Type (8), Code (0), Checksum (45), Identifier (32), Sequence Number (44), and Data.
- Bytes Pane:** Displays the raw hex and ASCII data for the selected ICMP frame.
- Status Bar:** Header length in 32-bit words (ip.hdr\_len), 1 byte | Packets: 32 · Displayed: 32 (100.0%) | Profile: Default

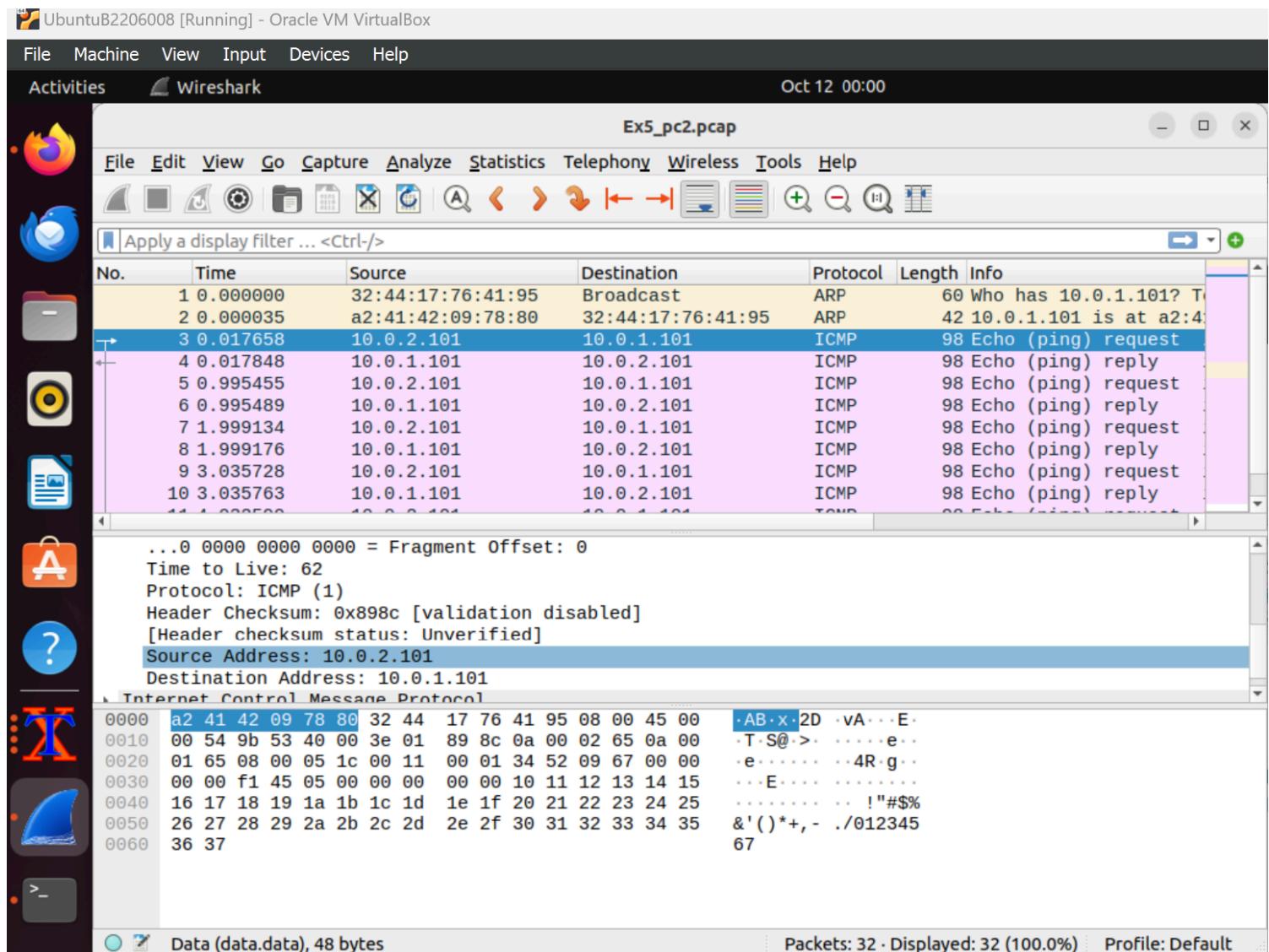
- **Size of frame #3 in bytes?** - 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
- **Protocol is using?** - ICMP  
This protocol operate in which OSI layer? - Network Layer



**Content of message? -**

f145050000000000101112131415161718191a1b1c1d1e1f20212223242526  
2728292a2b2c2d2e2f3031323334353637

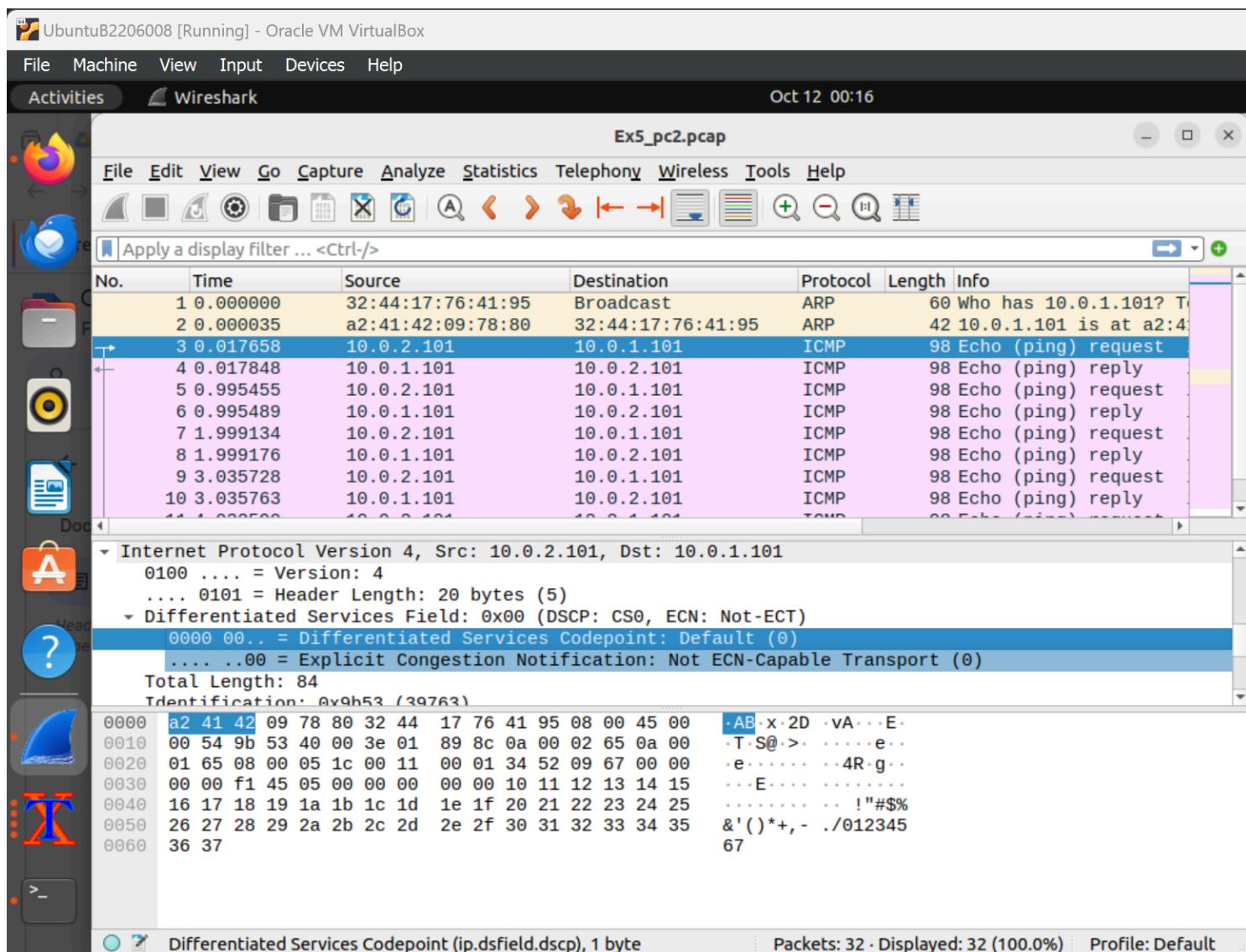
**Size of message in bytes? -** 48 bytes



- IP address of source and destination? -

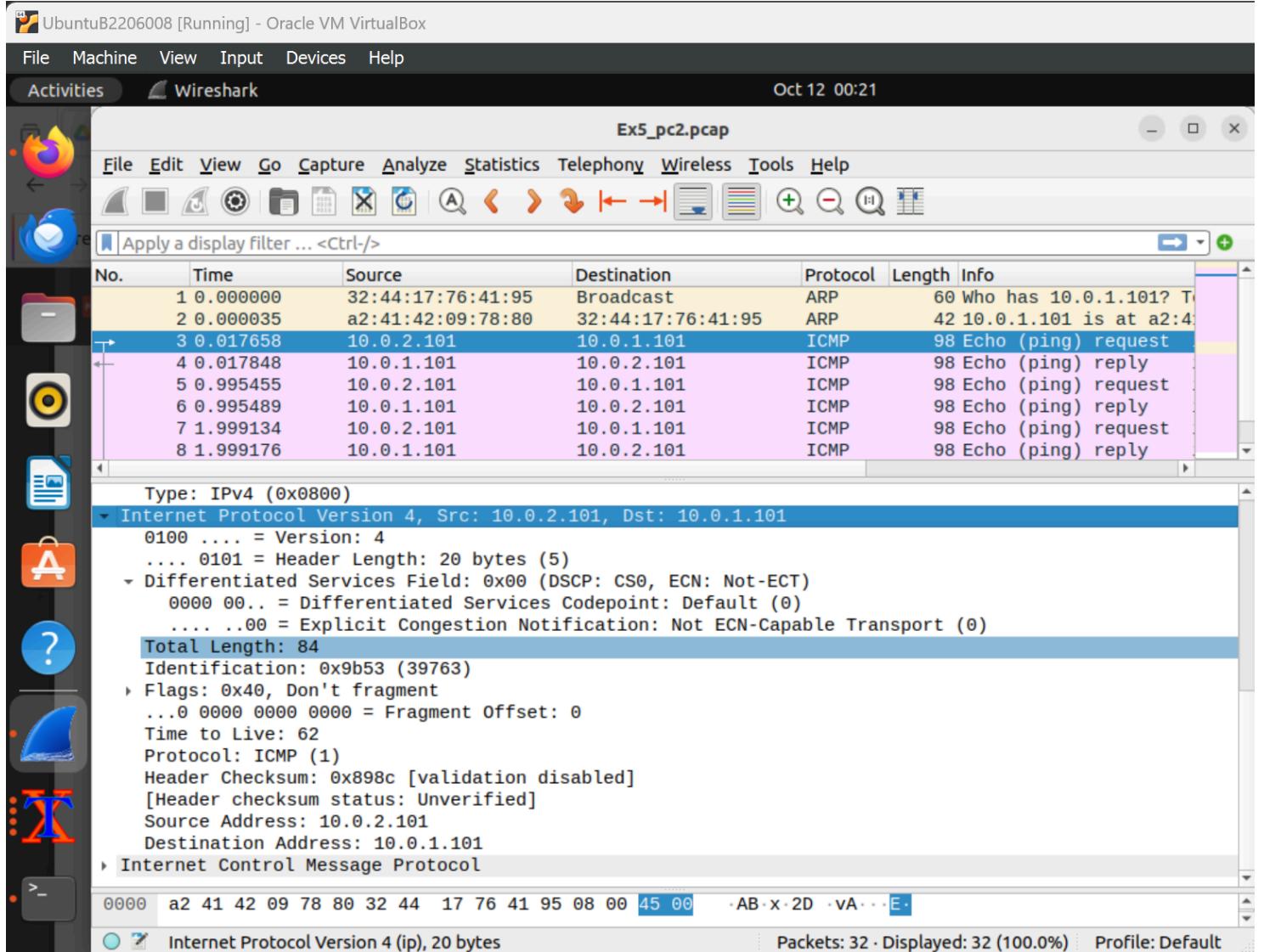
source: 10.0.2.101

destination: 10.0.1.101



- What is the length of the IP packet header? - 20 bytes

- **What fields does the Header include? - from Version field to Destination Address field**



- **How long is each field (Bytes)?**

UbuntuB2206008 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Activities Wireshark Oct 12 00:28

Ex5\_pc2.pcap

No. Time Source Destination Protocol Length Info

1	0.000000	32:44:17:76:41:95	Broadcast	ARP	60	Who has 10.0.1.101? T
2	0.000035	a2:41:42:09:78:80	32:44:17:76:41:95	ARP	42	10.0.1.101 is at a2:4
3	0.017658	10.0.2.101	10.0.1.101	ICMP	98	Echo (ping) request
4	0.017848	10.0.1.101	10.0.2.101	ICMP	98	Echo (ping) reply
5	0.995455	10.0.2.101	10.0.1.101	ICMP	98	Echo (ping) request
6	0.995489	10.0.1.101	10.0.2.101	ICMP	98	Echo (ping) reply
7	1.999134	10.0.2.101	10.0.1.101	ICMP	98	Echo (ping) request
8	1.999176	10.0.1.101	10.0.2.101	ICMP	98	Echo (ping) reply

Type: IPv4 (0x0800)

- Internet Protocol Version 4, Src: 10.0.2.101, Dst: 10.0.1.101

- 0100 .... = Version: 4
- .... 0101 = Header Length: 20 bytes (5)
- Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  - 0000 00.. = Differentiated Services Codepoint: Default (0)
  - .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
- Total Length: 84
- Identification: 0x9b53 (39763)
- Flags: 0x40, Don't fragment
  - ...0 0000 0000 0000 = Fragment Offset: 0
- Time to Live: 62
- Protocol: ICMP (1)
- Header Checksum: 0x898c [validation disabled]
- [Header checksum status: Unverified]
- Source Address: 10.0.2.101
- Destination Address: 10.0.1.101

Internet Control Message Protocol

0000 a2 41 42 09 78 80 32 44 17 76 41 95 08 00 45 00 .AB·x·2D·vA··E·

Version (ip.version), 1 byte

Packets: 32 · Displayed: 32 (100.0%) · Profile: Default

=> Version: 1 byte (4 bits)

UbuntuB2206008 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Activities Wireshark Oct 12 00:29

Ex5\_pc2.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	32:44:17:76:41:95	Broadcast	ARP	60	Who has 10.0.1.101? T
2	0.000035	a2:41:42:09:78:80	32:44:17:76:41:95	ARP	42	10.0.1.101 is at a2:4
3	0.017658	10.0.2.101	10.0.1.101	ICMP	98	Echo (ping) request
4	0.017848	10.0.1.101	10.0.2.101	ICMP	98	Echo (ping) reply
5	0.995455	10.0.2.101	10.0.1.101	ICMP	98	Echo (ping) request
6	0.995489	10.0.1.101	10.0.2.101	ICMP	98	Echo (ping) reply
7	1.999134	10.0.2.101	10.0.1.101	ICMP	98	Echo (ping) request
8	1.999176	10.0.1.101	10.0.2.101	ICMP	98	Echo (ping) reply

Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: 10.0.2.101, Dst: 10.0.1.101

0100 .... = Version: 4

.... 0101 = Header Length: 20 bytes (5)

Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

0000 00.. = Differentiated Services Codepoint: Default (0)

.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)

Total Length: 84

Identification: 0xb53 (39763)

Flags: 0x40, Don't fragment

...0 0000 0000 0000 = Fragment Offset: 0

Time to Live: 62

Protocol: ICMP (1)

Header Checksum: 0x898c [validation disabled]

[Header checksum status: Unverified]

Source Address: 10.0.2.101

Destination Address: 10.0.1.101

Internet Control Message Protocol

0000 a2 41 42 09 78 80 32 44 17 76 41 95 08 00 45 00 AB x 2D vA E

Header length in 32-bit words (ip.hdr\_len), 1 byte

Packets: 32 · Displayed: 32 (100.0%) · Profile: Default

=> Header length in words: 1 byte (4 bits)

=> Version + Header length in words = 1 byte

UbuntuB2206008 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Activities Wireshark Oct 12 00:30

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Ex5\_pc2.pcap

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	32:44:17:76:41:95	Broadcast	ARP	60	Who has 10.0.1.101? T
2	0.000035	a2:41:42:09:78:80	32:44:17:76:41:95	ARP	42	10.0.1.101 is at a2:4
3	0.017658	10.0.2.101	10.0.1.101	ICMP	98	Echo (ping) request
4	0.017848	10.0.1.101	10.0.2.101	ICMP	98	Echo (ping) reply
5	0.995455	10.0.2.101	10.0.1.101	ICMP	98	Echo (ping) request
6	0.995489	10.0.1.101	10.0.2.101	ICMP	98	Echo (ping) reply
7	1.999134	10.0.2.101	10.0.1.101	ICMP	98	Echo (ping) request
8	1.999176	10.0.1.101	10.0.2.101	ICMP	98	Echo (ping) reply

Type: IPv4 (0x0800)

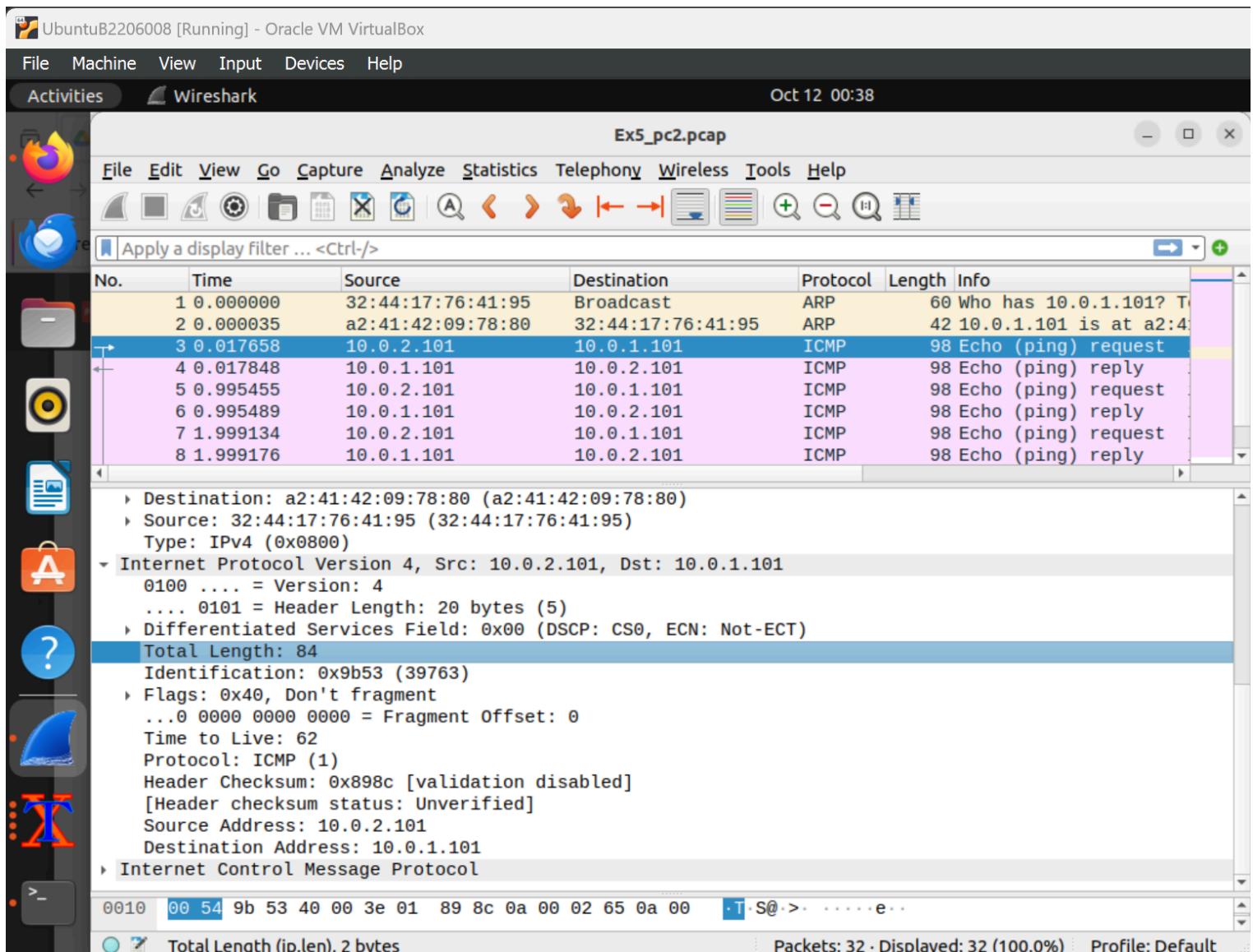
- Internet Protocol Version 4, Src: 10.0.2.101, Dst: 10.0.1.101
  - 0100 .... = Version: 4
  - .... 0101 = Header Length: 20 bytes (5)
  - Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    - 0000 00.. = Differentiated Services Codepoint: Default (0)
    - .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
  - Total Length: 84
  - Identification: 0x9b53 (39763)
  - Flags: 0x40, Don't fragment
    - ...0 0000 0000 0000 = Fragment Offset: 0
  - Time to Live: 62
  - Protocol: ICMP (1)
  - Header Checksum: 0x898c [validation\_disabled]
    - [Header checksum status: Unverified]
  - Source Address: 10.0.2.101
  - Destination Address: 10.0.1.101
- Internet Control Message Protocol

0000 a2 41 42 09 78 80 32 44 17 76 41 95 08 00 45 00 AB x 2D vA E

Differentiated Services Field (ip.dsfield), 1 byte

Packets: 32 · Displayed: 32 (100.0%) · Profile: Default

=> Differentiated Services Field: 1 byte



=> Total Length: 2 bytes

UbuntuB2206008 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Activities Wireshark Oct 12 00:39

Ex5\_pc2.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	32:44:17:76:41:95	Broadcast	ARP	60	Who has 10.0.1.101? To
2	0.000035	a2:41:42:09:78:80	32:44:17:76:41:95	ARP	42	10.0.1.101 is at a2:4
3	0.017658	10.0.2.101	10.0.1.101	ICMP	98	Echo (ping) request
4	0.017848	10.0.1.101	10.0.2.101	ICMP	98	Echo (ping) reply
5	0.995455	10.0.2.101	10.0.1.101	ICMP	98	Echo (ping) request
6	0.995489	10.0.1.101	10.0.2.101	ICMP	98	Echo (ping) reply
7	1.999134	10.0.2.101	10.0.1.101	ICMP	98	Echo (ping) request
8	1.999176	10.0.1.101	10.0.2.101	ICMP	98	Echo (ping) reply

```

    > Destination: a2:41:42:09:78:80 (a2:41:42:09:78:80)
    > Source: 32:44:17:76:41:95 (32:44:17:76:41:95)
      Type: IPv4 (0x0800)
    - Internet Protocol Version 4, Src: 10.0.2.101, Dst: 10.0.1.101
      0100 .... = Version: 4
      .... 0101 = Header Length: 20 bytes (5)
    - Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      Total Length: 84
      Identification: 0x9b53 (39763)
    - Flags: 0x40, Don't fragment
      ...0 0000 0000 0000 = Fragment Offset: 0
      Time to Live: 62
      Protocol: ICMP (1)
      Header Checksum: 0x898c [validation disabled]
        [Header checksum status: Unverified]
      Source Address: 10.0.2.101
      Destination Address: 10.0.1.101
    - Internet Control Message Protocol
  
```

0010 00 54 9b 53 40 00 3e 01 89 8c 0a 00 02 65 0a 00 T S@> .....e...

Identification (ip.id), 2 bytes Packets: 32 · Displayed: 32 (100.0%) Profile: Default

=> Identification: 2 bytes

UbuntuB2206008 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Activities Wireshark Oct 12 00:41

Ex5\_pc2.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	32:44:17:76:41:95	Broadcast	ARP	60	Who has 10.0.1.101? T
2	0.000035	a2:41:42:09:78:80	32:44:17:76:41:95	ARP	42	10.0.1.101 is at a2:4:
3	0.017658	10.0.2.101	10.0.1.101	ICMP	98	Echo (ping) request
4	0.017848	10.0.1.101	10.0.2.101	ICMP	98	Echo (ping) reply
5	0.995455	10.0.2.101	10.0.1.101	ICMP	98	Echo (ping) request
6	0.995489	10.0.1.101	10.0.2.101	ICMP	98	Echo (ping) reply
7	1.999134	10.0.2.101	10.0.1.101	ICMP	98	Echo (ping) request
8	1.999176	10.0.1.101	10.0.2.101	ICMP	98	Echo (ping) reply

Destination: a2:41:42:09:78:80 (a2:41:42:09:78:80)  
 Source: 32:44:17:76:41:95 (32:44:17:76:41:95)  
 Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: 10.0.2.101, Dst: 10.0.1.101  
 0100 .... = Version: 4  
 .... 0101 = Header Length: 20 bytes (5)  
 Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)  
 Total Length: 84  
 Identification: 0xb53 (39763)  
 Flags: 0x40, Don't fragment  
 ...0 0000 0000 0000 = Fragment Offset: 0  
 Time to Live: 62  
 Protocol: ICMP (1)  
 Header Checksum: 0x898c [validation disabled]  
 [Header checksum status: Unverified]  
 Source Address: 10.0.2.101  
 Destination Address: 10.0.1.101

Internet Control Message Protocol

0010 00 54 9b 53 40 00 3e 01 89 8c 0a 00 02 65 0a 00 .T.S>.. e..  
 Flags (3 bits) (ip.flags), 1 byte  
 Packets: 32 · Displayed: 32 (100.0%) · Profile: Default

=> Flags: 1 byte (3 bit)

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	32:44:17:76:41:95	Broadcast	ARP	60	Who has 10.0.1.101? T
2	0.000035	a2:41:42:09:78:80	32:44:17:76:41:95	ARP	42	10.0.1.101 is at a2:4
3	0.017658	10.0.2.101	10.0.1.101	ICMP	98	Echo (ping) request
4	0.017848	10.0.1.101	10.0.2.101	ICMP	98	Echo (ping) reply
5	0.995455	10.0.2.101	10.0.1.101	ICMP	98	Echo (ping) request
6	0.995489	10.0.1.101	10.0.2.101	ICMP	98	Echo (ping) reply
7	1.999134	10.0.2.101	10.0.1.101	ICMP	98	Echo (ping) request
8	1.999176	10.0.1.101	10.0.2.101	ICMP	98	Echo (ping) reply

Details pane for the selected ICMP request (Index 3):

- Destination: a2:41:42:09:78:80 (a2:41:42:09:78:80)
- Source: 32:44:17:76:41:95 (32:44:17:76:41:95)
- Type: IPv4 (0x0800)
- Internet Protocol Version 4, Src: 10.0.2.101, Dst: 10.0.1.101
- Version: 4
- Header Length: 20 bytes (5)
- Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 84
- Identification: 0x9b53 (39763)
- Flags: 0x40, Don't fragment
- Fragment Offset: 0
- Time to Live: 62
- Protocol: ICMP (1)
- Header Checksum: 0x898c [validation disabled]
- [Header checksum status: Unverified]
- Source Address: 10.0.2.101
- Destination Address: 10.0.1.101

Bytes pane for the selected ICMP request:

```

0010  00 54 9b 53 40 00 3e 01 89 8c 0a 00 02 65 0a 00  .T.S@.>.....e...

```

Selected item: Fragment offset (13 bits) (ip. frag\_offset), 2 bytes

=> Fragment Offset: 1 byte

=> Flags(3 bit) and Fragment Offset (13 bit) combine and take 2 bytes.

UbuntuB2206008 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Activities Wireshark Oct 12 00:44

Ex5\_pc2.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	32:44:17:76:41:95	Broadcast	ARP	60	Who has 10.0.1.101? T...
2	0.000035	a2:41:42:09:78:80	32:44:17:76:41:95	ARP	42	10.0.1.101 is at a2:4...
3	0.017658	10.0.2.101	10.0.1.101	ICMP	98	Echo (ping) request
4	0.017848	10.0.1.101	10.0.2.101	ICMP	98	Echo (ping) reply
5	0.995455	10.0.2.101	10.0.1.101	ICMP	98	Echo (ping) request
6	0.995489	10.0.1.101	10.0.2.101	ICMP	98	Echo (ping) reply
7	1.999134	10.0.2.101	10.0.1.101	ICMP	98	Echo (ping) request
8	1.999176	10.0.1.101	10.0.2.101	ICMP	98	Echo (ping) reply

Destination: a2:41:42:09:78:80 (a2:41:42:09:78:80)  
 Source: 32:44:17:76:41:95 (32:44:17:76:41:95)  
 Type: IPv4 (0x0800)

- Internet Protocol Version 4, Src: 10.0.2.101, Dst: 10.0.1.101  
 0100 .... = Version: 4  
 .... 0101 = Header Length: 20 bytes (5)  
 Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)  
 Total Length: 84  
 Identification: 0x9b53 (39763)  
 Flags: 0x40, Don't fragment  
 ...0 0000 0000 0000 = Fragment Offset: 0  
 Time to Live: 62  
 Protocol: ICMP (1)  
 Header Checksum: 0x898c [validation disabled]  
 [Header checksum status: Unverified]  
 Source Address: 10.0.2.101  
 Destination Address: 10.0.1.101  
 Internet Control Message Protocol

0010 00 54 9b 53 40 00 3e 01 89 8c 0a 00 02 65 0a 00 .T S@ > .....e..  
 Time to Live (ip.ttl), 1 byte Packets: 32 · Displayed: 32 (100.0%) Profile: Default

=> Time to Live: 1 bytes

UbuntuB2206008 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Activities Wireshark Oct 12 00:44

Ex5\_pc2.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	32:44:17:76:41:95	Broadcast	ARP	60	Who has 10.0.1.101? T...
2	0.000035	a2:41:42:09:78:80	32:44:17:76:41:95	ARP	42	10.0.1.101 is at a2:4...
3	0.017658	10.0.2.101	10.0.1.101	ICMP	98	Echo (ping) request
4	0.017848	10.0.1.101	10.0.2.101	ICMP	98	Echo (ping) reply
5	0.995455	10.0.2.101	10.0.1.101	ICMP	98	Echo (ping) request
6	0.995489	10.0.1.101	10.0.2.101	ICMP	98	Echo (ping) reply
7	1.999134	10.0.2.101	10.0.1.101	ICMP	98	Echo (ping) request
8	1.999176	10.0.1.101	10.0.2.101	ICMP	98	Echo (ping) reply

Destination: a2:41:42:09:78:80 (a2:41:42:09:78:80)  
Source: 32:44:17:76:41:95 (32:44:17:76:41:95)  
Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: 10.0.2.101, Dst: 10.0.1.101  
0100 .... = Version: 4  
.... 0101 = Header Length: 20 bytes (5)  
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)  
Total Length: 84  
Identification: 0x9b53 (39763)  
Flags: 0x40, Don't fragment  
...0 0000 0000 0000 = Fragment Offset: 0  
Time to Live: 62

Protocol: ICMP (1)  
Header Checksum: 0x898c [validation disabled]  
[Header checksum status: Unverified]  
Source Address: 10.0.2.101  
Destination Address: 10.0.1.101

Internet Control Message Protocol

0010 00 54 9b 53 40 00 3e 01 89 8c 0a 00 02 65 0a 00 .T.S@->. .... e..

Protocol (ip.proto), 1 byte

Packets: 32 · Displayed: 32 (100.0%) · Profile: Default

=> Protocol: 1 byte

UbuntuB2206008 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Activities Wireshark Oct 12 00:45

Ex5\_pc2.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	32:44:17:76:41:95	Broadcast	ARP	60	Who has 10.0.1.101? T...
2	0.000035	a2:41:42:09:78:80	32:44:17:76:41:95	ARP	42	10.0.1.101 is at a2:4...
3	0.017658	10.0.2.101	10.0.1.101	ICMP	98	Echo (ping) request
4	0.017848	10.0.1.101	10.0.2.101	ICMP	98	Echo (ping) reply
5	0.995455	10.0.2.101	10.0.1.101	ICMP	98	Echo (ping) request
6	0.995489	10.0.1.101	10.0.2.101	ICMP	98	Echo (ping) reply
7	1.999134	10.0.2.101	10.0.1.101	ICMP	98	Echo (ping) request
8	1.999176	10.0.1.101	10.0.2.101	ICMP	98	Echo (ping) reply

Destination: a2:41:42:09:78:80 (a2:41:42:09:78:80)  
 Source: 32:44:17:76:41:95 (32:44:17:76:41:95)  
 Type: IPv4 (0x0800)

- Internet Protocol Version 4, Src: 10.0.2.101, Dst: 10.0.1.101  
 0100 .... = Version: 4  
 .... 0101 = Header Length: 20 bytes (5)  
 Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)  
 Total Length: 84  
 Identification: 0x9b53 (39763)  
 Flags: 0x40, Don't fragment  
 ...0 0000 0000 0000 = Fragment Offset: 0  
 Time to Live: 62  
 Protocol: ICMP (1)  
 Header Checksum: 0x898c [validation disabled]  
 [Header checksum status: Unverified]  
 Source Address: 10.0.2.101  
 Destination Address: 10.0.1.101  
 Internet Control Message Protocol

0010 00 54 9b 53 40 00 3e 01 89 8c 0a 00 02 65 0a 00 .T.S@>... e...  
 Header Checksum (ip.checksum), 2 bytes Packets: 32 · Displayed: 32 (100.0%) Profile: Default

=>Header Checksum: 2 bytes

UbuntuB2206008 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Activities Wireshark Oct 12 00:46

Ex5\_pc2.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	32:44:17:76:41:95	Broadcast	ARP	60	Who has 10.0.1.101? T
2	0.000035	a2:41:42:09:78:80	32:44:17:76:41:95	ARP	42	10.0.1.101 is at a2:4
3	0.017658	10.0.2.101	10.0.1.101	ICMP	98	Echo (ping) request
4	0.017848	10.0.1.101	10.0.2.101	ICMP	98	Echo (ping) reply
5	0.995455	10.0.2.101	10.0.1.101	ICMP	98	Echo (ping) request
6	0.995489	10.0.1.101	10.0.2.101	ICMP	98	Echo (ping) reply
7	1.999134	10.0.2.101	10.0.1.101	ICMP	98	Echo (ping) request
8	1.999176	10.0.1.101	10.0.2.101	ICMP	98	Echo (ping) reply

► Destination: a2:41:42:09:78:80 (a2:41:42:09:78:80)  
 ► Source: 32:44:17:76:41:95 (32:44:17:76:41:95)  
 Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: 10.0.2.101, Dst: 10.0.1.101  
 0100 .... = Version: 4  
 .... 0101 = Header Length: 20 bytes (5)  
 Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)  
 Total Length: 84  
 Identification: 0x9b53 (39763)  
 Flags: 0x40, Don't fragment  
 ...0 0000 0000 0000 = Fragment Offset: 0  
 Time to Live: 62  
 Protocol: ICMP (1)  
 Header Checksum: 0x898c [validation disabled]  
 [Header checksum status: Unverified]  
 Source Address: 10.0.2.101  
 Destination Address: 10.0.1.101

Internet Control Message Protocol

0010 00 54 9b 53 40 00 3e 01 89 8c 0a 00 02 65 0a 00 .T.S@>... .e..  
 Header checksum status (ip.checksum.status) Packets: 32 · Displayed: 32 (100.0%) Profile: Default

=> Header checksum status: 0 byte

UbuntuB2206008 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Activities Wireshark Oct 12 00:46

Ex5\_pc2.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	32:44:17:76:41:95	Broadcast	ARP	60	Who has 10.0.1.101? T
2	0.000035	a2:41:42:09:78:80	32:44:17:76:41:95	ARP	42	10.0.1.101 is at a2:4
3	0.017658	10.0.2.101	10.0.1.101	ICMP	98	Echo (ping) request
4	0.017848	10.0.1.101	10.0.2.101	ICMP	98	Echo (ping) reply
5	0.995455	10.0.2.101	10.0.1.101	ICMP	98	Echo (ping) request
6	0.995489	10.0.1.101	10.0.2.101	ICMP	98	Echo (ping) reply
7	1.999134	10.0.2.101	10.0.1.101	ICMP	98	Echo (ping) request
8	1.999176	10.0.1.101	10.0.2.101	ICMP	98	Echo (ping) reply

Destination: a2:41:42:09:78:80 (a2:41:42:09:78:80)  
 Source: 32:44:17:76:41:95 (32:44:17:76:41:95)  
 Type: IPv4 (0x0800)

- Internet Protocol Version 4, Src: 10.0.2.101, Dst: 10.0.1.101  
 0100 .... = Version: 4  
 .... 0101 = Header Length: 20 bytes (5)  
 Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)  
 Total Length: 84  
 Identification: 0xb53 (39763)  
 Flags: 0x40, Don't fragment  
 ...0 0000 0000 0000 = Fragment Offset: 0  
 Time to Live: 62  
 Protocol: ICMP (1)  
 Header Checksum: 0x898c [validation disabled]  
 [Header checksum status: Unverified]  
 Source Address: 10.0.2.101  
 Destination Address: 10.0.1.101  
 Internet Control Message Protocol

0010 00 54 9b 53 40 00 3e 01 89 8c 0a 00 02 65 0a 00 .T.S@.>.. . . . . e ..

Source Address (ip.src), 4 bytes Packets: 32 · Displayed: 32 (100.0%) Profile: Default

=> Source Address: 4 bytes

UbuntuB2206008 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Activities Wireshark Oct 12 00:47

Ex5\_pc2.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

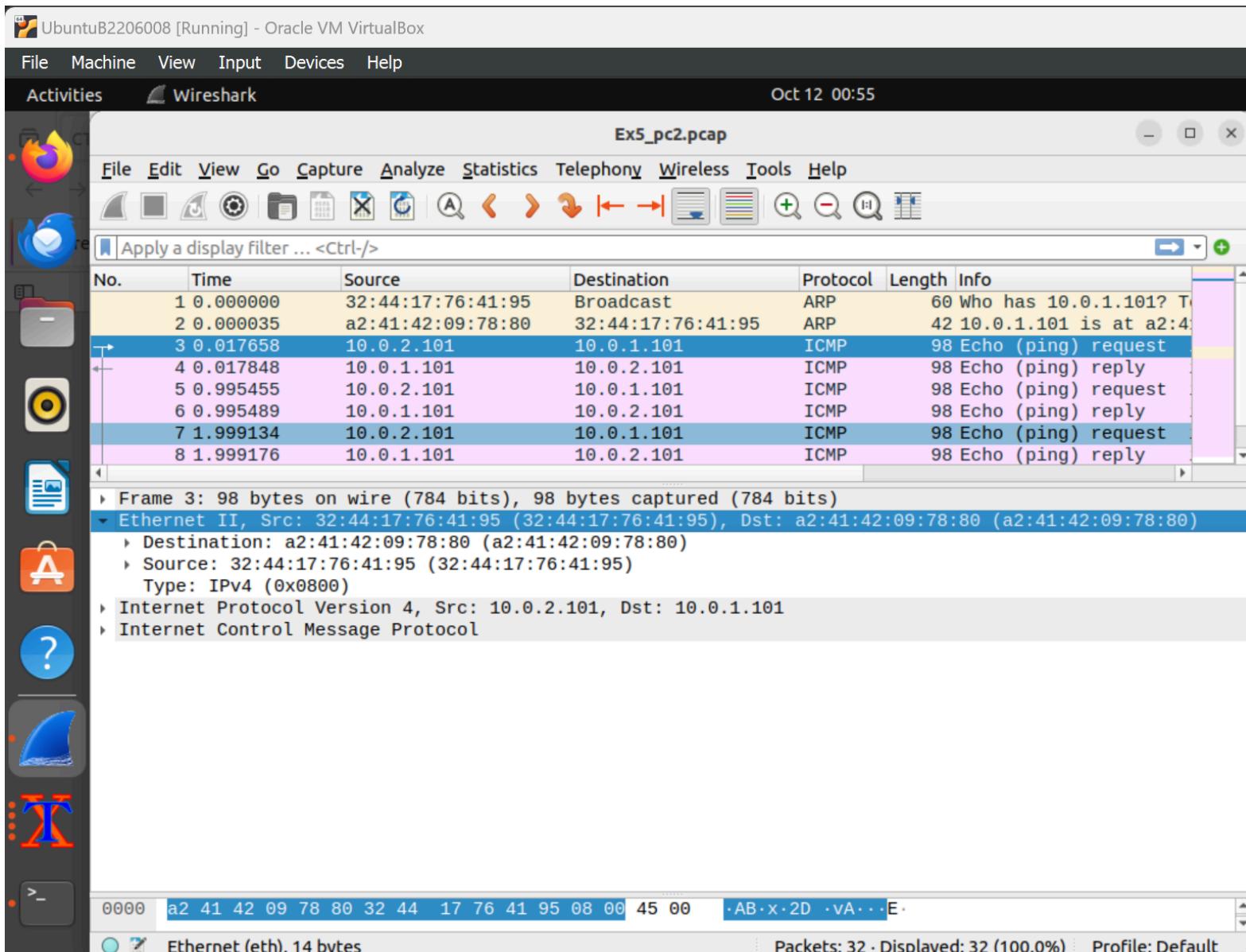
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	32:44:17:76:41:95	Broadcast	ARP	60	Who has 10.0.1.101? T...
2	0.000035	a2:41:42:09:78:80	32:44:17:76:41:95	ARP	42	10.0.1.101 is at a2:4...
3	0.017658	10.0.2.101	10.0.1.101	ICMP	98	Echo (ping) request
4	0.017848	10.0.1.101	10.0.2.101	ICMP	98	Echo (ping) reply
5	0.995455	10.0.2.101	10.0.1.101	ICMP	98	Echo (ping) request
6	0.995489	10.0.1.101	10.0.2.101	ICMP	98	Echo (ping) reply
7	1.999134	10.0.2.101	10.0.1.101	ICMP	98	Echo (ping) request
8	1.999176	10.0.1.101	10.0.2.101	ICMP	98	Echo (ping) reply

► Destination: a2:41:42:09:78:80 (a2:41:42:09:78:80)  
 ► Source: 32:44:17:76:41:95 (32:44:17:76:41:95)  
 Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: 10.0.2.101, Dst: 10.0.1.101  
 0100 .... = Version: 4  
 .... 0101 = Header Length: 20 bytes (5)  
 ► Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)  
 Total Length: 84  
 Identification: 0x9b53 (39763)  
 ► Flags: 0x40, Don't fragment  
 ...0 0000 0000 0000 = Fragment Offset: 0  
 Time to Live: 62  
 Protocol: ICMP (1)  
 Header Checksum: 0x898c [validation disabled]  
 [Header checksum status: Unverified]  
 Source Address: 10.0.2.101  
 Destination Address: 10.0.1.101  
 ► Internet Control Message Protocol

0010 00 54 9b 53 40 00 3e 01 89 8c 0a 00 02 65 0a 00 .T S@-> . . . e .  
 Destination Address (ip.dst), 4 bytes Packets: 32 · Displayed: 32 (100.0%) Profile: Default

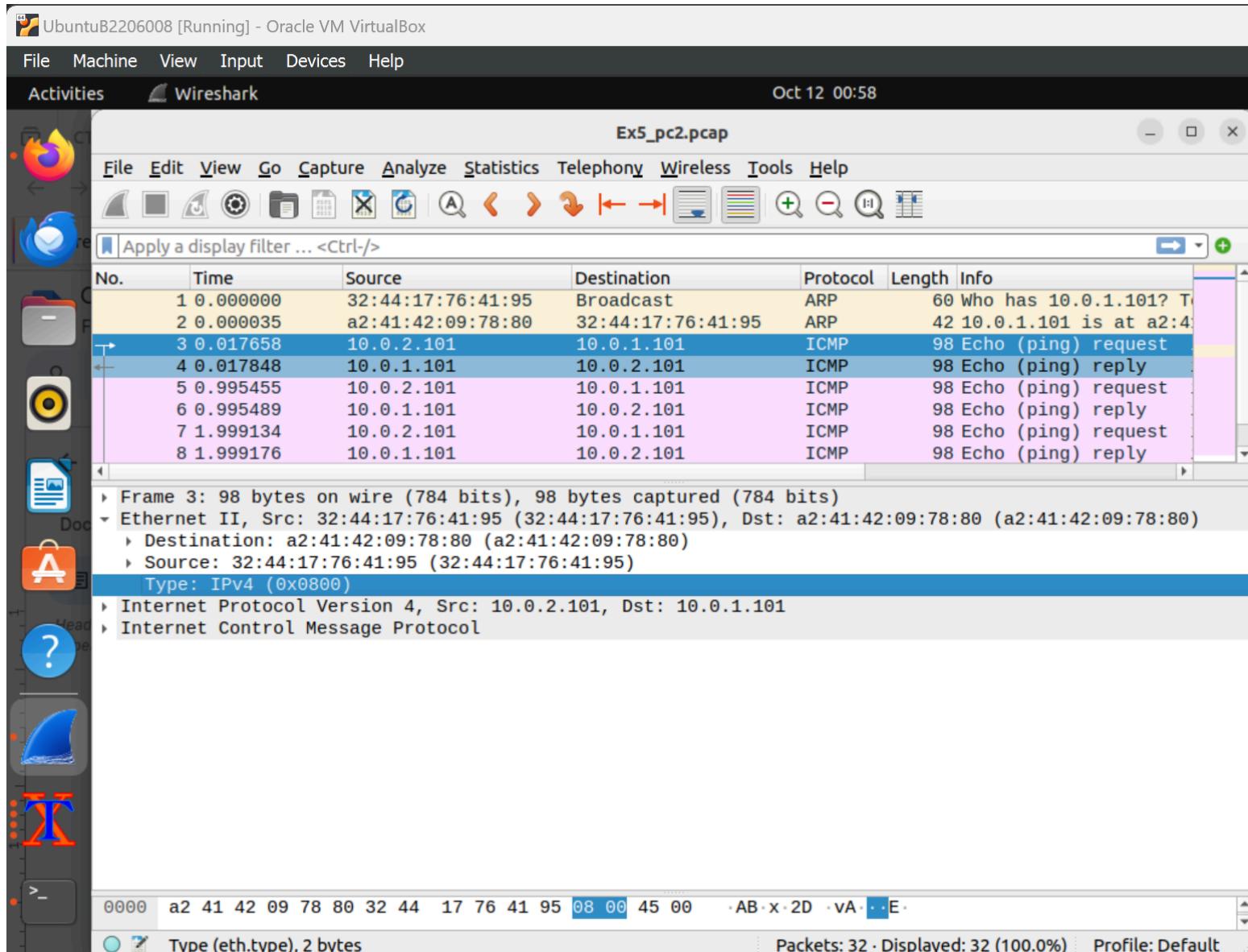
=> Destination Address: 4 bytes



- **MAC address of source and destination host?**

Destination: a2:41:42:09:78:80

Source: 32:44:17:76:41:95



- What is the Type value? - 0x0800