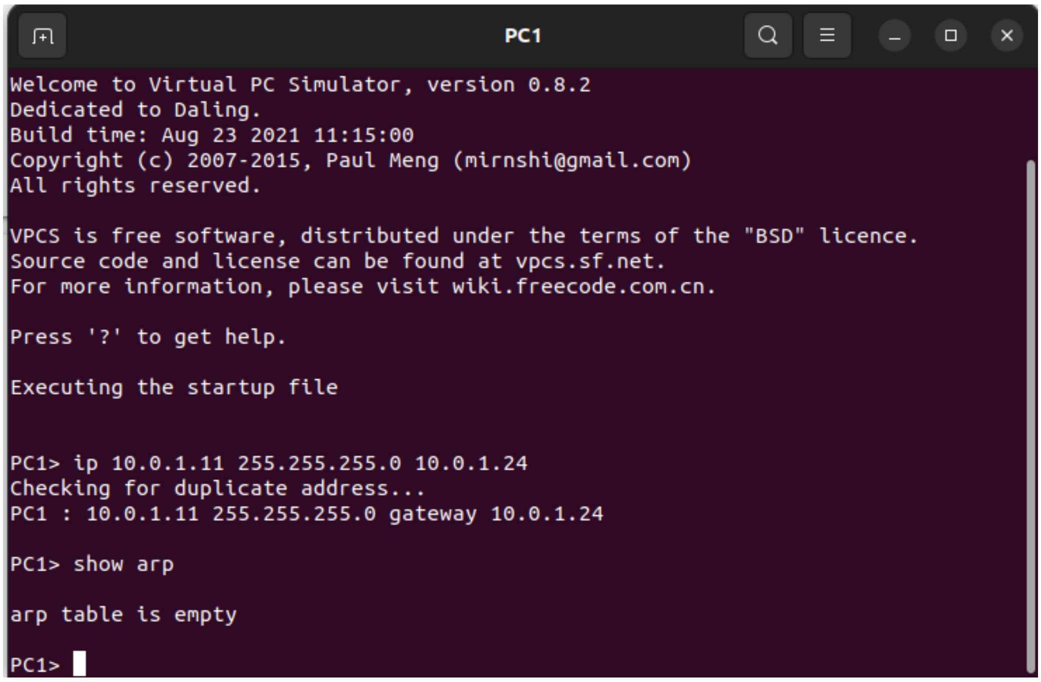
LAB NO: 5 **Aditi Shrivastava-210905244**

Computer Network Design using HUB in GNS3

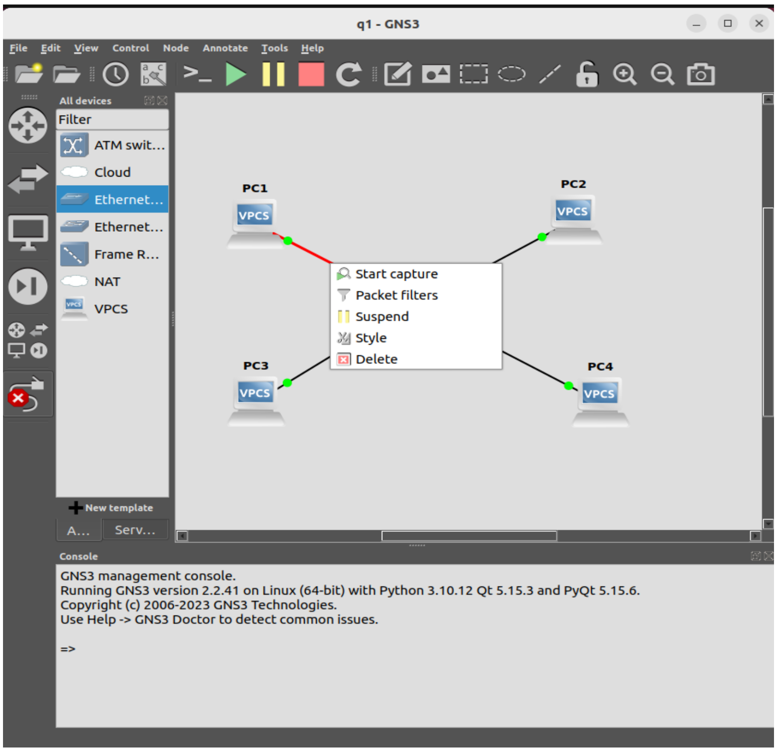
1. Design network configuration shown in Figure 5.29 for all parts. Connect all four VMs to a single Ethernet segment via a single hub as shown in Figure 5.29. Configure the IP addresses for the PCs as shown in Table 6.1.

a. On PC1, view the ARP cache with show arp



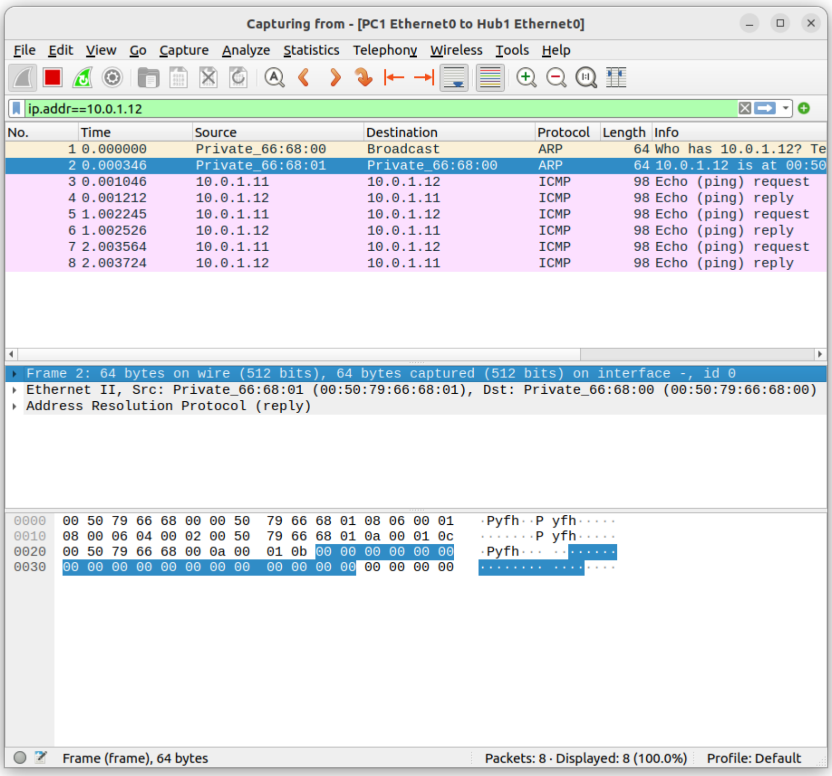
```
Welcome to Virtual PC Simulator, version 0.8.2
Dedicated to Daling.
Build time: Aug 23 2021 11:15:00
Copyright (c) 2007-2015, Paul Meng (mirnshi@gmail.com)
All rights reserved.

VPCS is free software, distributed under the terms of the "BSD" licence.
Source code and license can be found at vpcs.sf.net.
For more information, please visit wiki.freecode.com.cn.

Press '?' to get help.

Executing the startup file


PC1> ip 10.0.1.11 255.255.255.0 10.0.1.24
Checking for duplicate address...
PC1 : 10.0.1.11 255.255.255.0 gateway 10.0.1.24

PC1> show arp

arp table is empty

PC1>
```

b. Start Wireshark on PC1-Hub1 link with a capture filter set to the IP address of PC2.



```
GNS3 management console.
Running GNS3 version 2.2.41 on Linux (64-bit) with Python 3.10.12 Qt 5.15.3 and PyQt 5.15.6.
Copyright (c) 2006-2023 GNS3 Technologies.
Use Help -> GNS3 Doctor to detect common issues.

=>
```

c. Issue a ping command from PC1 to PC2:
PC1% ping 10.0.1.13 –c 3



Capturing from - [PC1 Ethernet0 to Hub1 Ethernet0]

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr==10.0.1.12

```
No.  Time      Source             Destination        Protocol Length Info
   1 0.000000  Private_66:68:00   Broadcast          ARP         64 Who has 10.0.1.12? Te
   2 0.000346  Private_66:68:01   Private_66:68:00   ARP         64 10.0.1.12 is at 00:50
   3 0.001046  10.0.1.11          10.0.1.12          ICMP        98 Echo (ping) request
   4 0.001212  10.0.1.12          10.0.1.11          ICMP        98 Echo (ping) reply
   5 1.002245  10.0.1.11          10.0.1.12          ICMP        98 Echo (ping) request
   6 1.002526  10.0.1.12          10.0.1.11          ICMP        98 Echo (ping) reply
   7 2.003564  10.0.1.11          10.0.1.12          ICMP        98 Echo (ping) request
   8 2.003724  10.0.1.12          10.0.1.11          ICMP        98 Echo (ping) reply
```

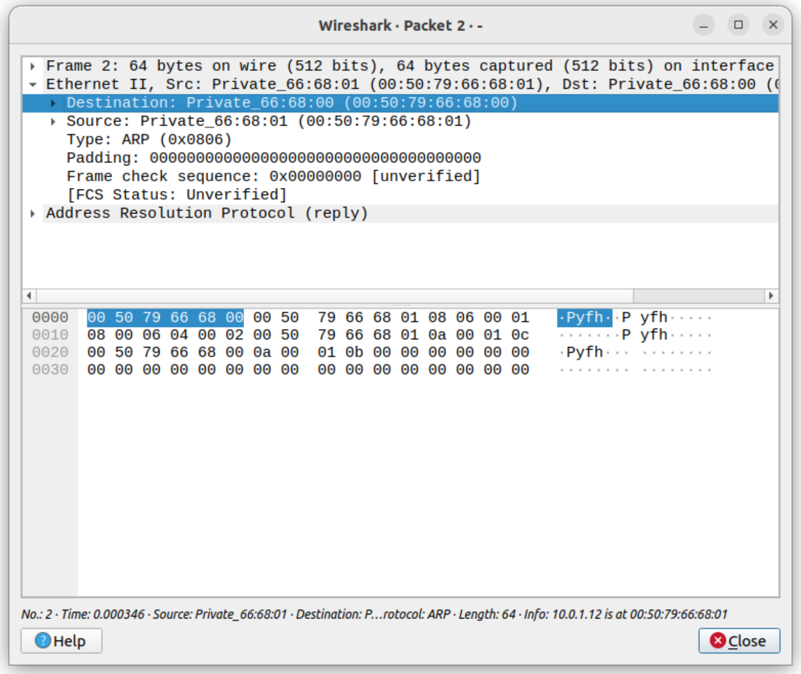
```
› Frame 2: 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on interface -, id 0
› Ethernet II, Src: Private_66:68:01 (00:50:79:66:68:01), Dst: Private_66:68:00 (00:50:79:66:68:00)
› Address Resolution Protocol (reply)
```

```
0000  00 50 79 66 68 00 00 50  79 66 68 01 08 06 00 01   ·Pyfh··P yfh·····
0010  08 00 06 04 00 02 00 50  79 66 68 01 0a 00 01 0c   ·······P yfh·····
0020  00 50 79 66 68 00 0a 00  01 0b 00 00 00 00 00 00   ·Pyfh··· ········
0030  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
```

Frame (frame), 64 bytes   Packets: 8 · Displayed: 8 (100.0%)   Profile: Default

Observe the ARP packets in the Wireshark window. Explore the MAC addresses in the Ethernet headers of the captured packets.

Direct our attention to the following fields:
• The destination MAC address of the ARP Request packets.
MAC Address- 00:50:79:66:68:00



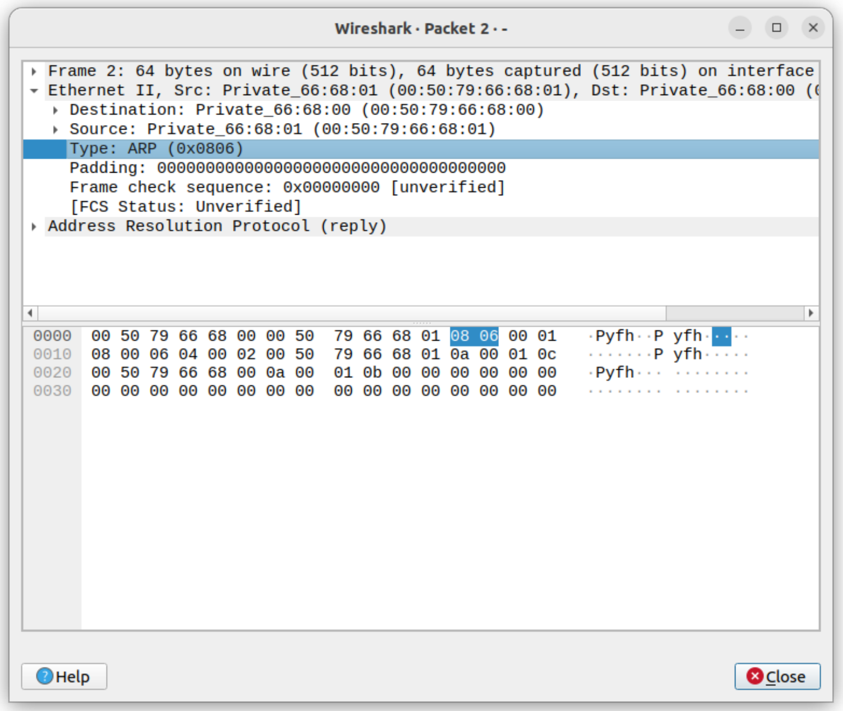
Wireshark · Packet 2 · -

```
› Frame 2: 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on interface
⌄ Ethernet II, Src: Private_66:68:01 (00:50:79:66:68:01), Dst: Private_66:68:00 ((
  › Destination: Private_66:68:00 (00:50:79:66:68:00)
  › Source: Private_66:68:01 (00:50:79:66:68:01)
    Type: ARP (0x0806)
    Padding: 000000000000000000000000000000000000
    Frame check sequence: 0x00000000 [unverified]
    [FCS Status: Unverified]
› Address Resolution Protocol (reply)
```

```
0000  00 50 79 66 68 00 00 50  79 66 68 01 08 06 00 01   ·Pyfh··P yfh·····
0010  08 00 06 04 00 02 00 50  79 66 68 01 0a 00 01 0c   ·······P yfh·····
0020  00 50 79 66 68 00 0a 00  01 0b 00 00 00 00 00 00   ·Pyfh··· ········
0030  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
```

No.: 2 · Time: 0.000346 · Source: Private_66:68:01 · Destination: P...rotocol: ARP · Length: 64 · Info: 10.0.1.12 is at 00:50:79:66:68:01

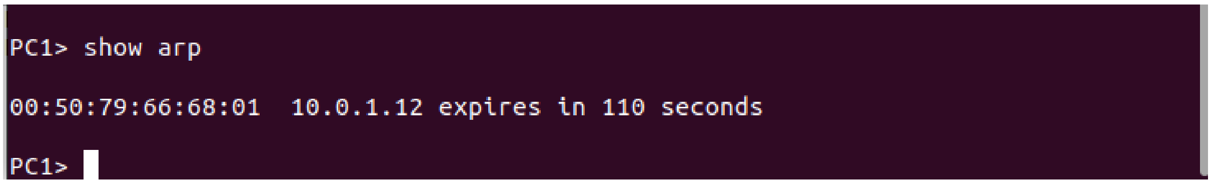
• The Type Field in the Ethernet headers of ARP packets.
0x0806



```
▸ Frame 2: 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on interface
▾ Ethernet II, Src: Private_66:68:01 (00:50:79:66:68:01), Dst: Private_66:68:00 ((
   ▸ Destination: Private_66:68:00 (00:50:79:66:68:00)
   ▸ Source: Private_66:68:01 (00:50:79:66:68:01)
     Type: ARP (0x0806)
     Padding: 000000000000000000000000000000000000
     Frame check sequence: 0x00000000 [unverified]
     [FCS Status: Unverified]
▸ Address Resolution Protocol (reply)
```

```
0000  00 50 79 66 68 00 00 50  79 66 68 01 08 06 00 01   ·Pyfh··P yfh····
0010  08 00 06 04 00 02 00 50  79 66 68 01 0a 00 01 0c   ·······P yfh·····
0020  00 50 79 66 68 00 0a 00  01 0b 00 00 00 00 00 00   ·Pyfh··· ········
0030  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
```

d. View the ARP cache again with the command arp -a. Note that ARP cache entries can get refreshed/deleted fairly quickly (~2 minutes).
show arp



```
PC1> show arp

00:50:79:66:68:01  10.0.1.12 expires in 110 seconds

PC1>
```

e. Save the results of Wireshark.

Exercises

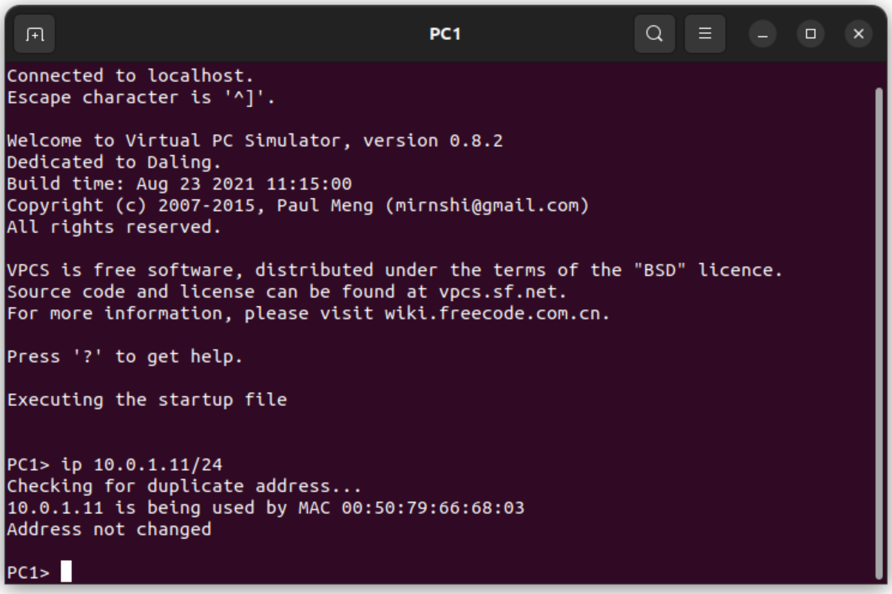
• What is the destination MAC address of an ARP Request packet?
=> 00:50:79:66:68:00

• What are the different Type Field values in the Ethernet headers that you observed?
=> 0x0806

• Use the captured data to analyse the process in which ARP acquires the MAC address for IP address 10.0.1.12.

2. To observe the effects of having more than one host with the same (duplicate) IP address in a network. After completing Exercise 1, the IP addresses of the Ethernet interfaces on the four PCs are as shown in Table 6.2 below. Note that PC1 and PC4 are assigned the same IP address.

=> Two PCs cannot have the same IP address in the same network.



```
Connected to localhost.
Escape character is '^]'.

Welcome to Virtual PC Simulator, version 0.8.2
Dedicated to Daling.
Build time: Aug 23 2021 11:15:00
Copyright (c) 2007-2015, Paul Meng (mirnshi@gmail.com)
All rights reserved.

VPCS is free software, distributed under the terms of the "BSD" licence.
Source code and license can be found at vpcs.sf.net.
For more information, please visit wiki.freecode.com.cn.

Press '?' to get help.

Executing the startup file


PC1> ip 10.0.1.11/24
Checking for duplicate address...
10.0.1.11 is being used by MAC 00:50:79:66:68:03
Address not changed

PC1> 
```

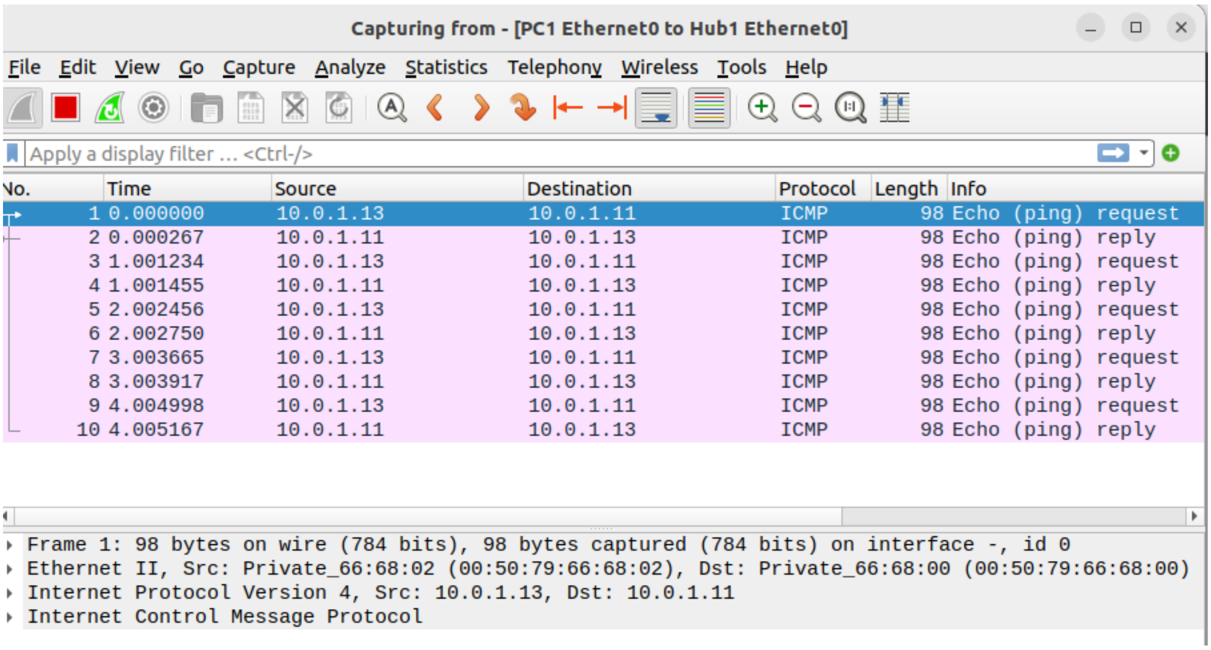
a. Delete all entries in the ARP cache on all PCs.

b. Run Wireshark on PC3-Hub1 link and capture the network traffic to and from the duplicate IP address 10.0.1.11.

c. From PC3, issue a ping command to the duplicate IP address, 10.0.1.11, by typing

PC3% ping 10.0.1.11 –c 5

=> PC3 is pinging to PC1 who’s ip address is 10.0.1.11

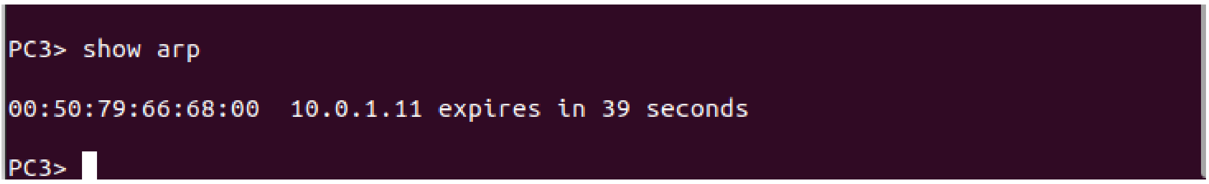

Capturing from - [PC1 Ethernet0 to Hub1 Ethernet0]
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.0.1.13	10.0.1.11	ICMP	98	Echo (ping) request
2	0.000267	10.0.1.11	10.0.1.13	ICMP	98	Echo (ping) reply
3	1.001234	10.0.1.13	10.0.1.11	ICMP	98	Echo (ping) request
4	1.001455	10.0.1.11	10.0.1.13	ICMP	98	Echo (ping) reply
5	2.002456	10.0.1.13	10.0.1.11	ICMP	98	Echo (ping) request
6	2.002750	10.0.1.11	10.0.1.13	ICMP	98	Echo (ping) reply
7	3.003665	10.0.1.13	10.0.1.11	ICMP	98	Echo (ping) request
8	3.003917	10.0.1.11	10.0.1.13	ICMP	98	Echo (ping) reply
9	4.004998	10.0.1.13	10.0.1.11	ICMP	98	Echo (ping) request
10	4.005167	10.0.1.11	10.0.1.13	ICMP	98	Echo (ping) reply

```
Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface -, id 0
Ethernet II, Src: Private_66:68:02 (00:50:79:66:68:02), Dst: Private_66:68:00 (00:50:79:66:68:00)
Internet Protocol Version 4, Src: 10.0.1.13, Dst: 10.0.1.11
Internet Control Message Protocol
```

d. Stop Wireshark, save all ARP packets and screenshot the ARP cache of PC3 using the arp –a command:

PC3% arp – a



```
PC3> show arp

00:50:79:66:68:00  10.0.1.11 expires in 39 seconds

PC3> 
```

e. When you are done with the exercise, reset the IP address of PC4 to its original value as given in Table 6.1.

Exercises

• Explain how the ping packets were issued by the hosts with duplicate addresses.

• Did the ping command result in error messages?

=> No error messages were displayed, because there was a PC with the address pinged, PC4 had no configured IP address, since PC1 had the same ip address.

• How can duplicate IP addresses be used to compromise the data security?

=> Duplicate IP addresses can be exploited to intercept or redirect network traffic, potentially gaining access to sensitive data or compromising the integrity of communications.

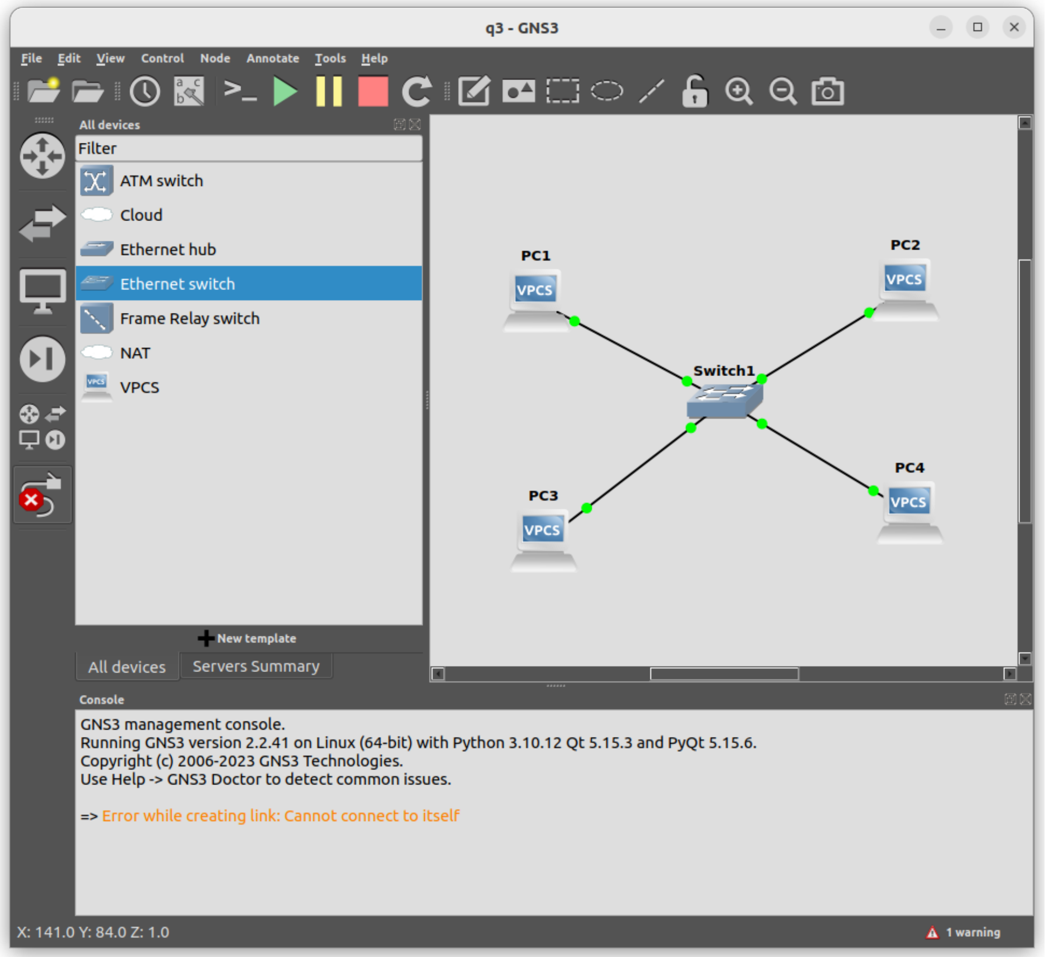
• Give an example. Use the ARP cache and the captured packets to support your explanation.

=> Duplicate IP addresses can be exploited through ARP cache poisoning. Attackers trick devices into sending data to the wrong address, letting them intercept, manipulate, aor redirect sensitive information

3. To test the effects of changing the netmask of a network configuration.

a. Design the configuration as Exercise 1 and replace the hub with a switch, two hosts (PC2 and PC4) have been assigned different network prefixes.

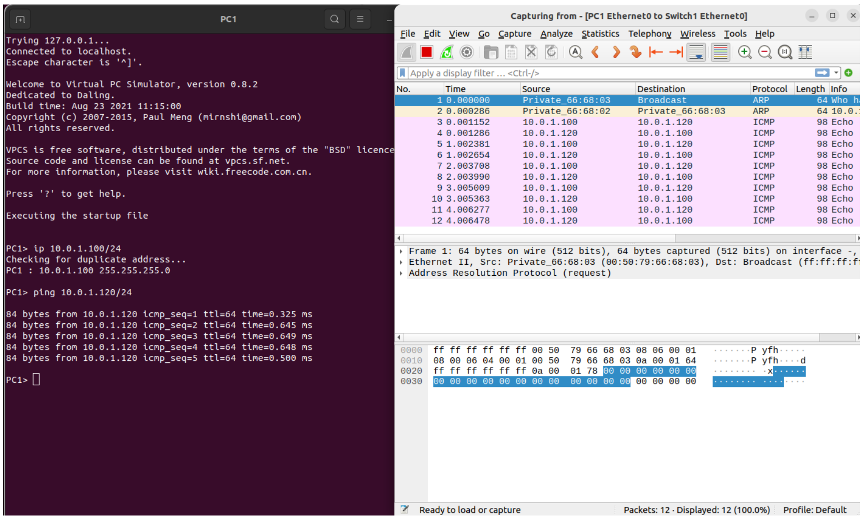
Setup the interfaces of the hosts as follows:
VPCS IP Address of eth0 Network Mask
PC110.0.1.100 / 24255.255.255.0
PC210.0.1.101 / 28255.255.255.240
PC310.0.1.120 / 24255.255.255.0
PC410.0.1.121 / 28255.255.255.240



```
GNS3 management console.
Running GNS3 version 2.2.41 on Linux (64-bit) with Python 3.10.12 Qt 5.15.3 and PyQt 5.15.6.
Copyright (c) 2006-2023 GNS3 Technologies.
Use Help -> GNS3 Doctor to detect common issues.

=> Error while creating link: Cannot connect to itself
```

b. Run Wireshark on PC1-Hub1 link and capture the packets for the following scenarios

i. From PC1 ping PC3.

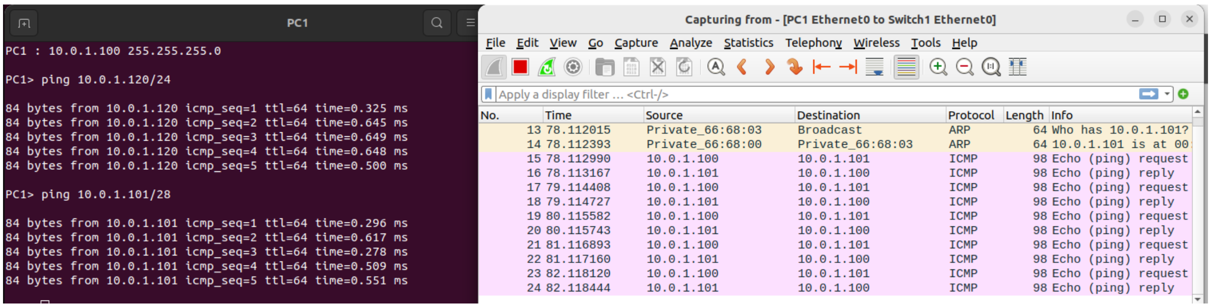


PC1
Capturing from - [PC1 Ethernet0 to Switch1 Ethernet0]
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.

Welcome to Virtual PC Simulator, version 0.8.2
Dedicated to Daling.
Build time: Aug 23 2021 11:15:00
Copyright (c) 2007-2015, Paul Meng (mirnshi@gmail.com)
All rights reserved.

VPCS is free software, distributed under the terms of the "BSD" licence
Source code and license can be found at vpcs.sf.net.
For more information, please visit wiki.freecode.com.cn.

Press '?' to get help.

Executing the startup file


PC1> ip 10.0.1.100/24
Checking for duplicate address...
PC1 : 10.0.1.100 255.255.255.0

PC1> ping 10.0.1.120/24

84 bytes from 10.0.1.120 icmp_seq=1 ttl=64 time=0.325 ms
84 bytes from 10.0.1.120 icmp_seq=2 ttl=64 time=0.645 ms
84 bytes from 10.0.1.120 icmp_seq=3 ttl=64 time=0.649 ms
84 bytes from 10.0.1.120 icmp_seq=4 ttl=64 time=0.648 ms
84 bytes from 10.0.1.120 icmp_seq=5 ttl=64 time=0.500 ms

PC1> 
```

```
No.  Time      Source             Destination        Protocol Length Info
   1 0.000000  Private_66:68:03   Broadcast          ARP       64 Who h
   2 0.000286  Private_66:68:02   Private_66:68:03   ARP       64 10.0.
   3 0.001152  10.0.1.100         10.0.1.120         ICMP      98 Echo
   4 0.001286  10.0.1.120         10.0.1.100         ICMP      98 Echo
   5 1.002381  10.0.1.100         10.0.1.120         ICMP      98 Echo
   6 1.002654  10.0.1.120         10.0.1.100         ICMP      98 Echo
   7 2.003708  10.0.1.100         10.0.1.120         ICMP      98 Echo
   8 2.003990  10.0.1.120         10.0.1.100         ICMP      98 Echo
   9 3.005009  10.0.1.100         10.0.1.120         ICMP      98 Echo
  10 3.005363  10.0.1.120         10.0.1.100         ICMP      98 Echo
  11 4.006277  10.0.1.100         10.0.1.120         ICMP      98 Echo
  12 4.006478  10.0.1.120         10.0.1.100         ICMP      98 Echo

› Frame 1: 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on interface -,
› Ethernet II, Src: Private_66:68:03 (00:50:79:66:68:03), Dst: Broadcast (ff:ff:ff:f
› Address Resolution Protocol (request)

0000  ff ff ff ff ff ff 00 50  79 66 68 03 08 06 00 01   ·······P yfh····
0010  08 00 06 04 00 01 00 50  79 66 68 03 0a 00 01 64   ·······P yfh···d
0020  ff ff ff ff ff ff 0a 00  01 78 00 00 00 00 00 00   ········ ·x······
0030  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········

Ready to load or capture        Packets: 12 · Displayed: 12 (100.0%)    Profile: Default
```

ii. From PC1 ping PC2.

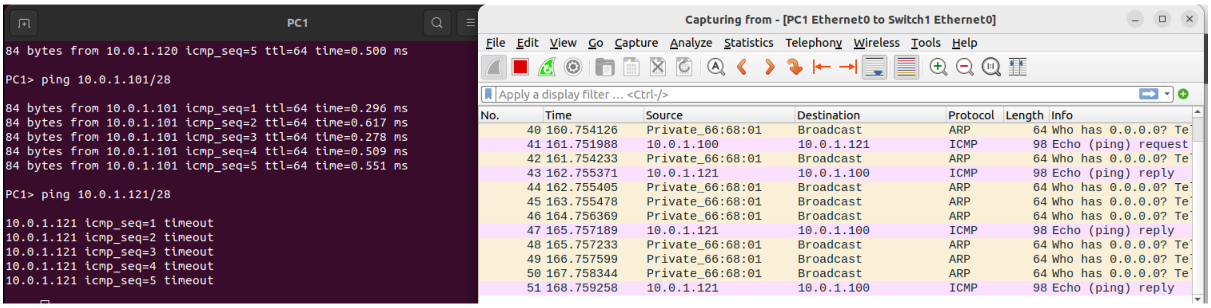


PC1
Capturing from - [PC1 Ethernet0 to Switch1 Ethernet0]
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
PC1 : 10.0.1.100 255.255.255.0

PC1> ping 10.0.1.120/24

84 bytes from 10.0.1.120 icmp_seq=1 ttl=64 time=0.325 ms
84 bytes from 10.0.1.120 icmp_seq=2 ttl=64 time=0.645 ms
84 bytes from 10.0.1.120 icmp_seq=3 ttl=64 time=0.649 ms
84 bytes from 10.0.1.120 icmp_seq=4 ttl=64 time=0.648 ms
84 bytes from 10.0.1.120 icmp_seq=5 ttl=64 time=0.500 ms

PC1> ping 10.0.1.101/28

84 bytes from 10.0.1.101 icmp_seq=1 ttl=64 time=0.296 ms
84 bytes from 10.0.1.101 icmp_seq=2 ttl=64 time=0.617 ms
84 bytes from 10.0.1.101 icmp_seq=3 ttl=64 time=0.278 ms
84 bytes from 10.0.1.101 icmp_seq=4 ttl=64 time=0.509 ms
84 bytes from 10.0.1.101 icmp_seq=5 ttl=64 time=0.551 ms
```

```
No.  Time       Source             Destination        Protocol Length Info
  13 78.112015  Private_66:68:03   Broadcast          ARP       64 Who has 10.0.1.101?
  14 78.112393  Private_66:68:00   Private_66:68:03   ARP       64 10.0.1.101 is at 00
  15 78.112990  10.0.1.100         10.0.1.101         ICMP      98 Echo (ping) request
  16 78.113167  10.0.1.101         10.0.1.100         ICMP      98 Echo (ping) reply
  17 79.114408  10.0.1.100         10.0.1.101         ICMP      98 Echo (ping) request
  18 79.114727  10.0.1.101         10.0.1.100         ICMP      98 Echo (ping) reply
  19 80.115582  10.0.1.100         10.0.1.101         ICMP      98 Echo (ping) request
  20 80.115743  10.0.1.101         10.0.1.100         ICMP      98 Echo (ping) reply
  21 81.116893  10.0.1.100         10.0.1.101         ICMP      98 Echo (ping) request
  22 81.117160  10.0.1.101         10.0.1.100         ICMP      98 Echo (ping) reply
  23 82.118120  10.0.1.100         10.0.1.101         ICMP      98 Echo (ping) request
  24 82.118444  10.0.1.101         10.0.1.100         ICMP      98 Echo (ping) reply
```

iii. From PC1 ping PC4.



PC1
Capturing from - [PC1 Ethernet0 to Switch1 Ethernet0]
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
84 bytes from 10.0.1.120 icmp_seq=5 ttl=64 time=0.500 ms

PC1> ping 10.0.1.101/28

84 bytes from 10.0.1.101 icmp_seq=1 ttl=64 time=0.296 ms
84 bytes from 10.0.1.101 icmp_seq=2 ttl=64 time=0.617 ms
84 bytes from 10.0.1.101 icmp_seq=3 ttl=64 time=0.278 ms
84 bytes from 10.0.1.101 icmp_seq=4 ttl=64 time=0.509 ms
84 bytes from 10.0.1.101 icmp_seq=5 ttl=64 time=0.551 ms

PC1> ping 10.0.1.121/28

10.0.1.121 icmp_seq=1 timeout
10.0.1.121 icmp_seq=2 timeout
10.0.1.121 icmp_seq=3 timeout
10.0.1.121 icmp_seq=4 timeout
10.0.1.121 icmp_seq=5 timeout
```

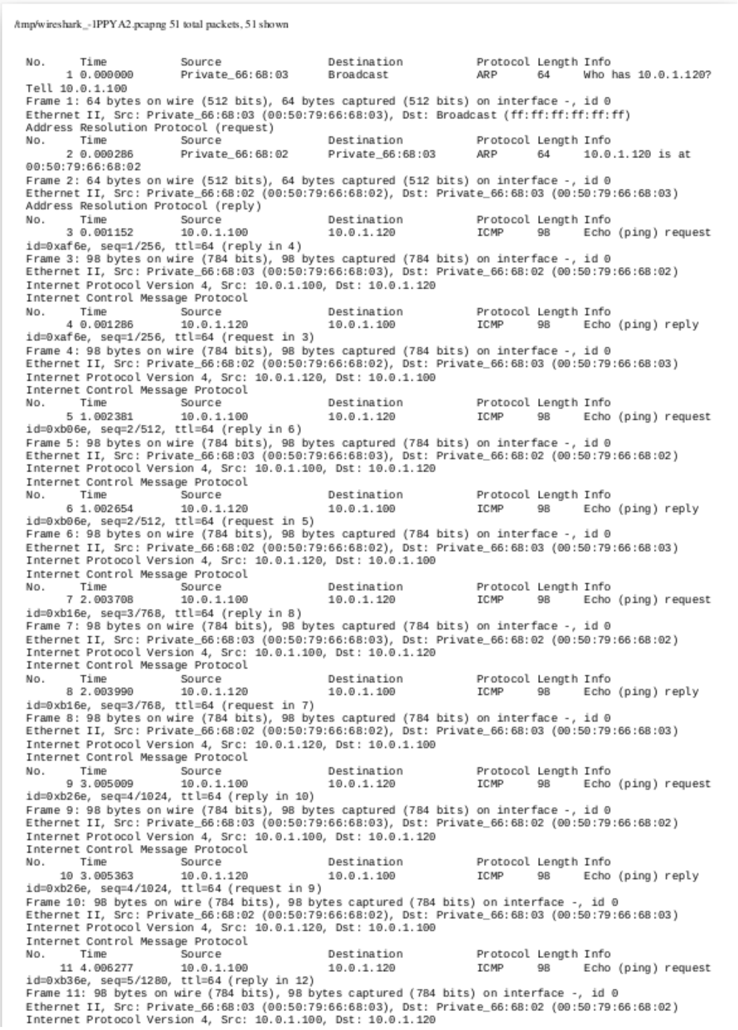
```
No.  Time        Source             Destination        Protocol Length Info
  40 160.754126  Private_66:68:01   Broadcast          ARP       64 Who has 0.0.0.0? Te
  41 161.751988  10.0.1.100         10.0.1.121         ICMP      98 Echo (ping) request
  42 161.754233  Private_66:68:01   Broadcast          ARP       64 Who has 0.0.0.0? Te
  43 162.755371  10.0.1.121         10.0.1.100         ICMP      98 Echo (ping) reply
  44 162.755405  Private_66:68:01   Broadcast          ARP       64 Who has 0.0.0.0? Te
  45 163.755478  Private_66:68:01   Broadcast          ARP       64 Who has 0.0.0.0? Te
  46 164.756369  Private_66:68:01   Broadcast          ARP       64 Who has 0.0.0.0? Te
  47 165.757189  10.0.1.121         10.0.1.100         ICMP      98 Echo (ping) reply
  48 165.757233  Private_66:68:01   Broadcast          ARP       64 Who has 0.0.0.0? Te
  49 166.757599  Private_66:68:01   Broadcast          ARP       64 Who has 0.0.0.0? Te
  50 167.758344  Private_66:68:01   Broadcast          ARP       64 Who has 0.0.0.0? Te
  51 168.759258  10.0.1.121         10.0.1.100         ICMP      98 Echo (ping) reply
```

iv. From PC4 ping PC1.
No Gateway found

v. From PC2 ping PC4.
No Gateway found

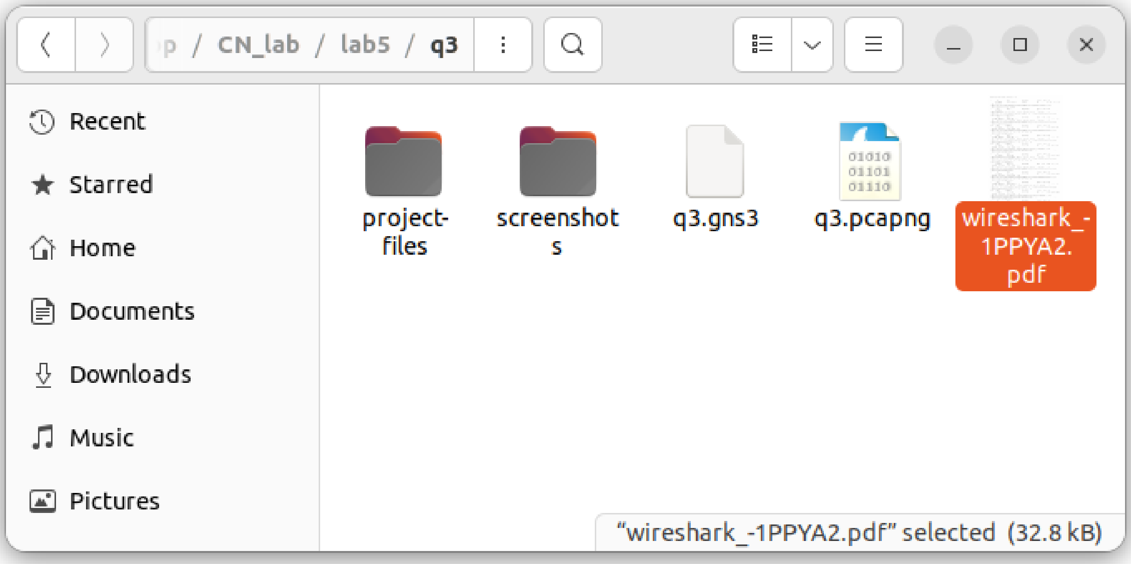
vi. From PC2 ping PC3.
No Gateway found

c. Save the Wireshark output to a text file (using the "Packet Summary" option from "Print") , and save the output of the ping commands. Note that not all of the above scenarios are successful. Save all the output including any error messages.
Saved the file as a pdf



/tmp/wireshark_-1PPYA2.pcapng 51 total packets, 51 shown

```
No.     Time           Source                 Destination            Protocol Length Info
      1 0.000000       Private_66:68:03       Broadcast              ARP      64     Who has 10.0.1.120?
Tell 10.0.1.100
Frame 1: 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on interface -, id 0
Ethernet II, Src: Private_66:68:03 (00:50:79:66:68:03), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)
No.     Time           Source                 Destination            Protocol Length Info
      2 0.000286       Private_66:68:02       Private_66:68:03       ARP      64     10.0.1.120 is at
00:50:79:66:68:02
Frame 2: 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on interface -, id 0
Ethernet II, Src: Private_66:68:02 (00:50:79:66:68:02), Dst: Private_66:68:03 (00:50:79:66:68:03)
Address Resolution Protocol (reply)
No.     Time           Source                 Destination            Protocol Length Info
      3 0.001152       10.0.1.100             10.0.1.120             ICMP     98     Echo (ping) request
id=0xaf6e, seq=1/256, ttl=64 (reply in 4)
Frame 3: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface -, id 0
Ethernet II, Src: Private_66:68:03 (00:50:79:66:68:03), Dst: Private_66:68:02 (00:50:79:66:68:02)
Internet Protocol Version 4, Src: 10.0.1.100, Dst: 10.0.1.120
Internet Control Message Protocol
No.     Time           Source                 Destination            Protocol Length Info
      4 0.001286       10.0.1.120             10.0.1.100             ICMP     98     Echo (ping) reply
id=0xaf6e, seq=1/256, ttl=64 (request in 3)
Frame 4: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface -, id 0
Ethernet II, Src: Private_66:68:02 (00:50:79:66:68:02), Dst: Private_66:68:03 (00:50:79:66:68:03)
Internet Protocol Version 4, Src: 10.0.1.120, Dst: 10.0.1.100
Internet Control Message Protocol
No.     Time           Source                 Destination            Protocol Length Info
      5 1.002381       10.0.1.100             10.0.1.120             ICMP     98     Echo (ping) request
id=0xb06e, seq=2/512, ttl=64 (reply in 6)
Frame 5: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface -, id 0
Ethernet II, Src: Private_66:68:03 (00:50:79:66:68:03), Dst: Private_66:68:02 (00:50:79:66:68:02)
Internet Protocol Version 4, Src: 10.0.1.100, Dst: 10.0.1.120
Internet Control Message Protocol
No.     Time           Source                 Destination            Protocol Length Info
      6 1.002654       10.0.1.120             10.0.1.100             ICMP     98     Echo (ping) reply
id=0xb06e, seq=2/512, ttl=64 (request in 5)
Frame 6: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface -, id 0
Ethernet II, Src: Private_66:68:02 (00:50:79:66:68:02), Dst: Private_66:68:03 (00:50:79:66:68:03)
Internet Protocol Version 4, Src: 10.0.1.120, Dst: 10.0.1.100
Internet Control Message Protocol
No.     Time           Source                 Destination            Protocol Length Info
      7 2.003708       10.0.1.100             10.0.1.120             ICMP     98     Echo (ping) request
id=0xb16e, seq=3/768, ttl=64 (reply in 8)
Frame 7: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface -, id 0
Ethernet II, Src: Private_66:68:03 (00:50:79:66:68:03), Dst: Private_66:68:02 (00:50:79:66:68:02)
Internet Protocol Version 4, Src: 10.0.1.100, Dst: 10.0.1.120
Internet Control Message Protocol
No.     Time           Source                 Destination            Protocol Length Info
      8 2.003990       10.0.1.120             10.0.1.100             ICMP     98     Echo (ping) reply
id=0xb16e, seq=3/768, ttl=64 (request in 7)
Frame 8: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface -, id 0
Ethernet II, Src: Private_66:68:02 (00:50:79:66:68:02), Dst: Private_66:68:03 (00:50:79:66:68:03)
Internet Protocol Version 4, Src: 10.0.1.120, Dst: 10.0.1.100
Internet Control Message Protocol
No.     Time           Source                 Destination            Protocol Length Info
      9 3.005009       10.0.1.100             10.0.1.120             ICMP     98     Echo (ping) request
id=0xb26e, seq=4/1024, ttl=64 (reply in 10)
Frame 9: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface -, id 0
Ethernet II, Src: Private_66:68:03 (00:50:79:66:68:03), Dst: Private_66:68:02 (00:50:79:66:68:02)
Internet Protocol Version 4, Src: 10.0.1.100, Dst: 10.0.1.120
Internet Control Message Protocol
No.     Time           Source                 Destination            Protocol Length Info
     10 3.005363       10.0.1.120             10.0.1.100             ICMP     98     Echo (ping) reply
id=0xb26e, seq=4/1024, ttl=64 (request in 9)
Frame 10: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface -, id 0
Ethernet II, Src: Private_66:68:02 (00:50:79:66:68:02), Dst: Private_66:68:03 (00:50:79:66:68:03)
Internet Protocol Version 4, Src: 10.0.1.120, Dst: 10.0.1.100
Internet Control Message Protocol
No.     Time           Source                 Destination            Protocol Length Info
     11 4.006277       10.0.1.100             10.0.1.120             ICMP     98     Echo (ping) request
id=0xb36e, seq=5/1280, ttl=64 (reply in 12)
Frame 11: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface -, id 0
Ethernet II, Src: Private_66:68:03 (00:50:79:66:68:03), Dst: Private_66:68:02 (00:50:79:66:68:02)
Internet Protocol Version 4, Src: 10.0.1.100, Dst: 10.0.1.120
```



“wireshark_-1PPYA2.pdf” selected (32.8 kB)

d. When you are done with the exercise, reset the interfaces to their original values as given Table 6.1. (Note that /24 corresponds to network mask 255.255.255.0. and /28 to network mask 255.255.255.240).

=> The interfaces have been resetted.

Exercises

- **Use your output data and ping results to explain what happened in each of the ping commands.**
- **Which ping operations were successful and which were unsuccessful? Why?**

=> PC1 to PC2 and PC3 were successful PC1 to PC4 is giving timeout.