LAB No 5
Date:31/08/2023
Computer Network Design using HUB in GNS3

Kushala Sarada A V
210905189
ROLL NUMBER 33

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.Table 5.1: IP Address of PCs
a. On PC1, view the ARP cache with show arp
b. Start Wireshark on PC1-Hub1 link with a capture filter set to the IP address of PC2.
c. Issue a ping command from PC1 to PC2:
PC1% ping 10.0.1.13 –c 3
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.
• The Type Field in the Ethernet headers of ARP packets.
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
e. Save the results of Wireshark.

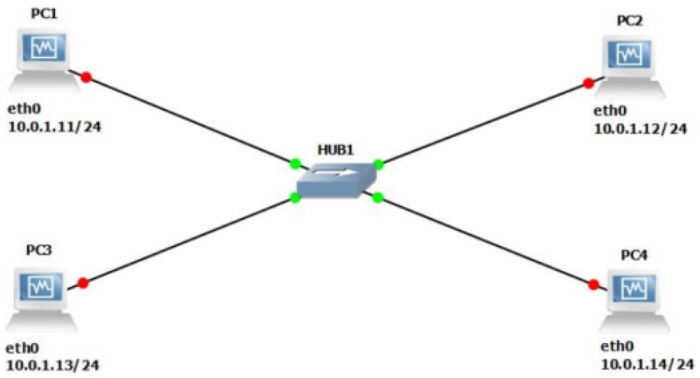
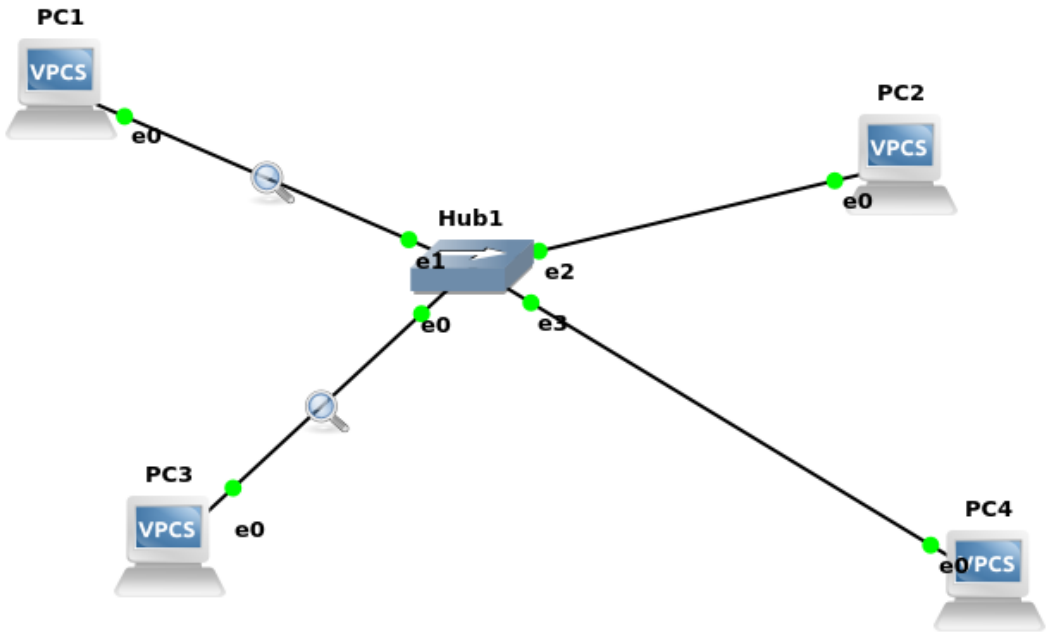


Figure 5.29: Network Design

VMS	IP Addresses of Ethernet Interface eth0
PC1	10.0.1.11 / 24
PC2	10.0.1.12 / 24
PC3	10.0.1.13 / 24
PC4	10.0.1.14 / 24

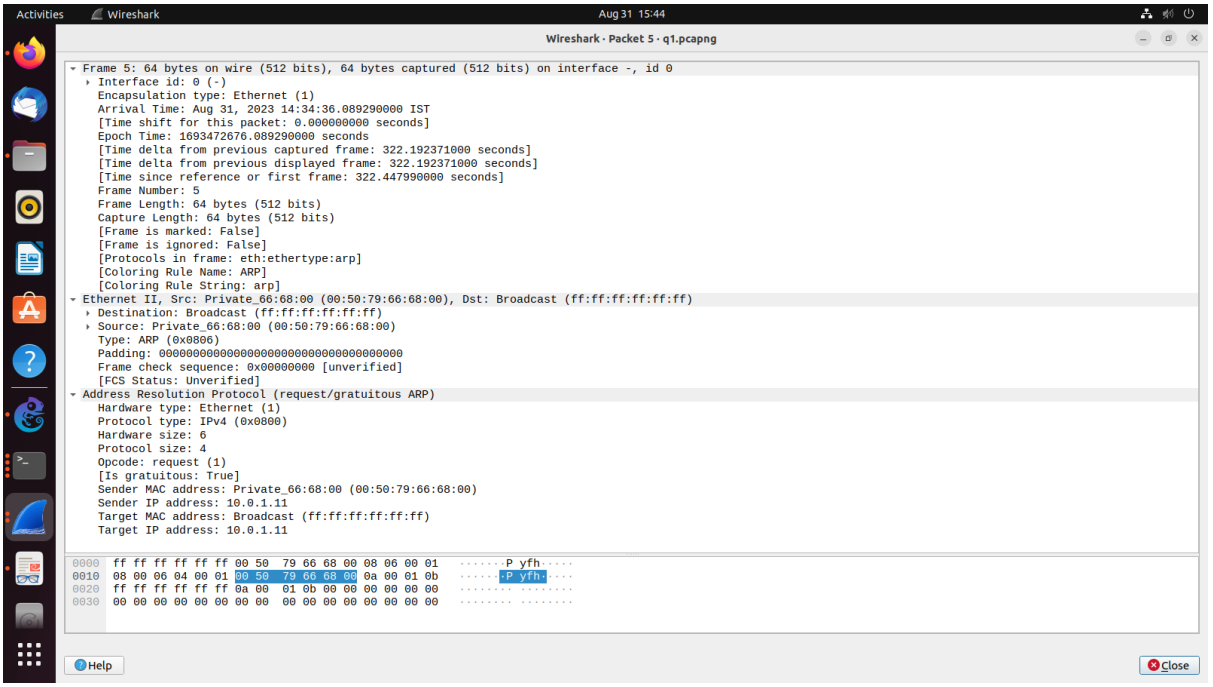
ANS)



Direct our attention to the following fields:

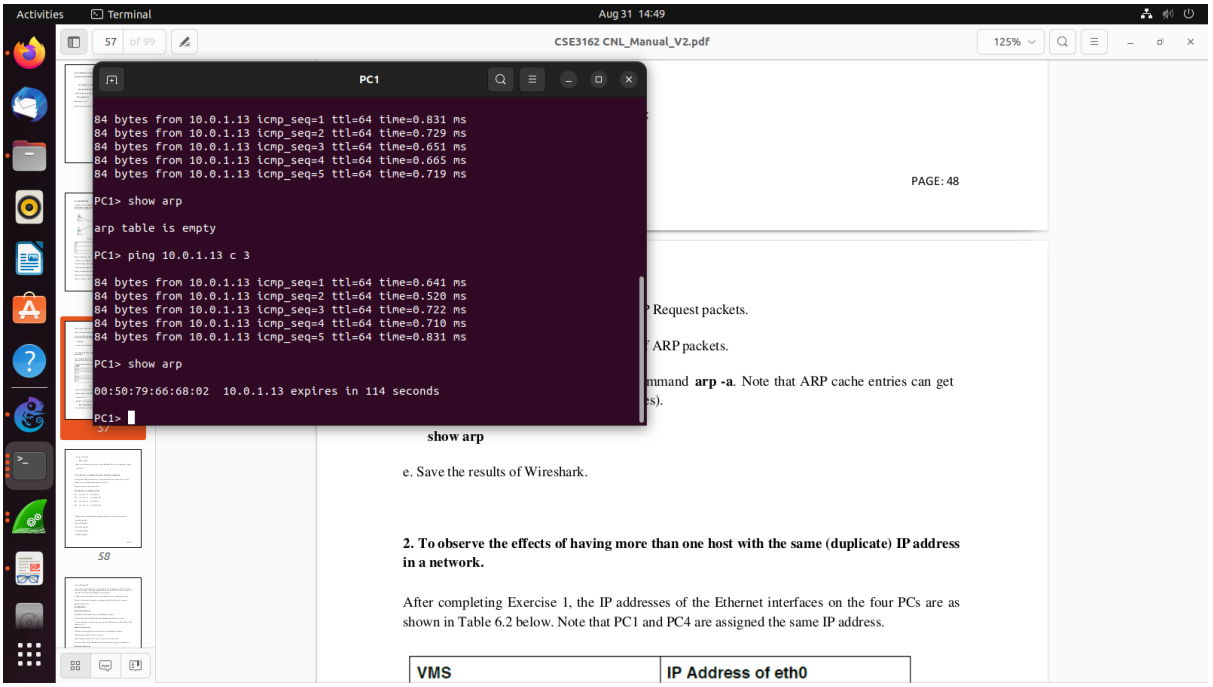
• The destination MAC address of the ARP Request packets.

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



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

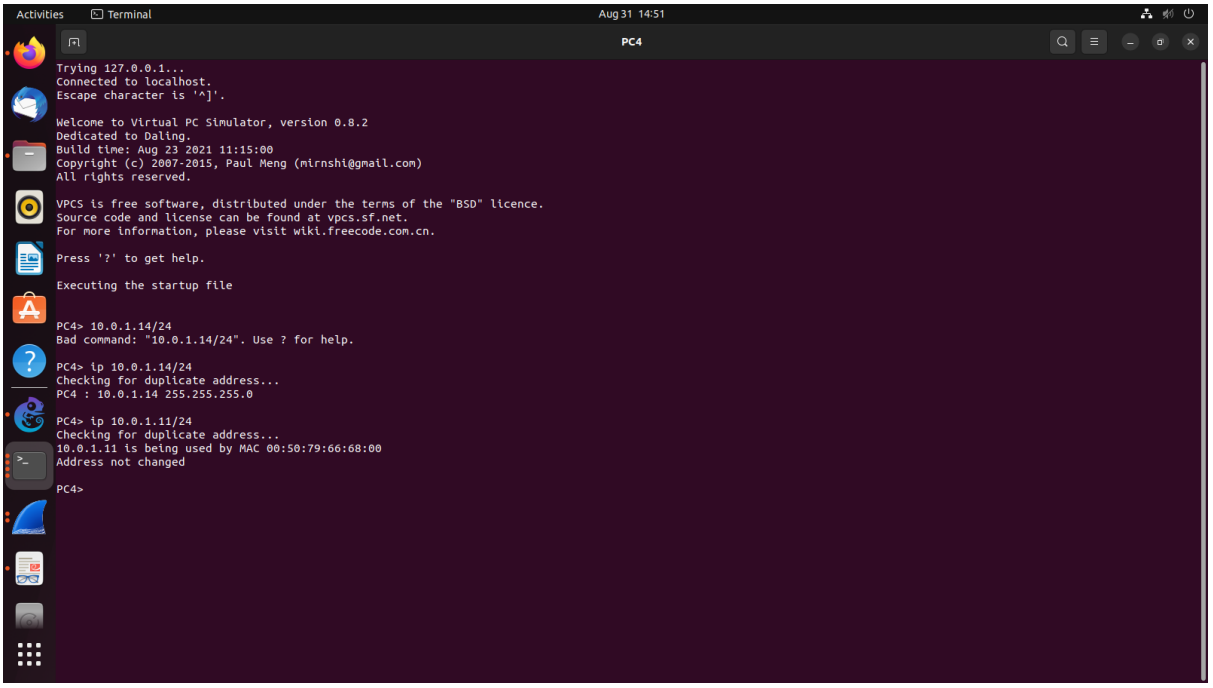


2. To observe the effects of having more than one host with the same (duplicate) IP address in a network.
After completing Exercise 1, the IP addresses of the Ethernet interfaces on the four PCs are as
shown in Table 6.2 below. Note that PC1 and PC4 are assigned the same IP address.
a. Delete all entries 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
d. Stop Wireshark, save all ARP packets and screenshot the ARP cache of PC3 usingthe arp –a command:
PC3% arp – a
e. When you are done with the exercise, reset the IP address of PC4 to its original value as given
in Table 6.1.

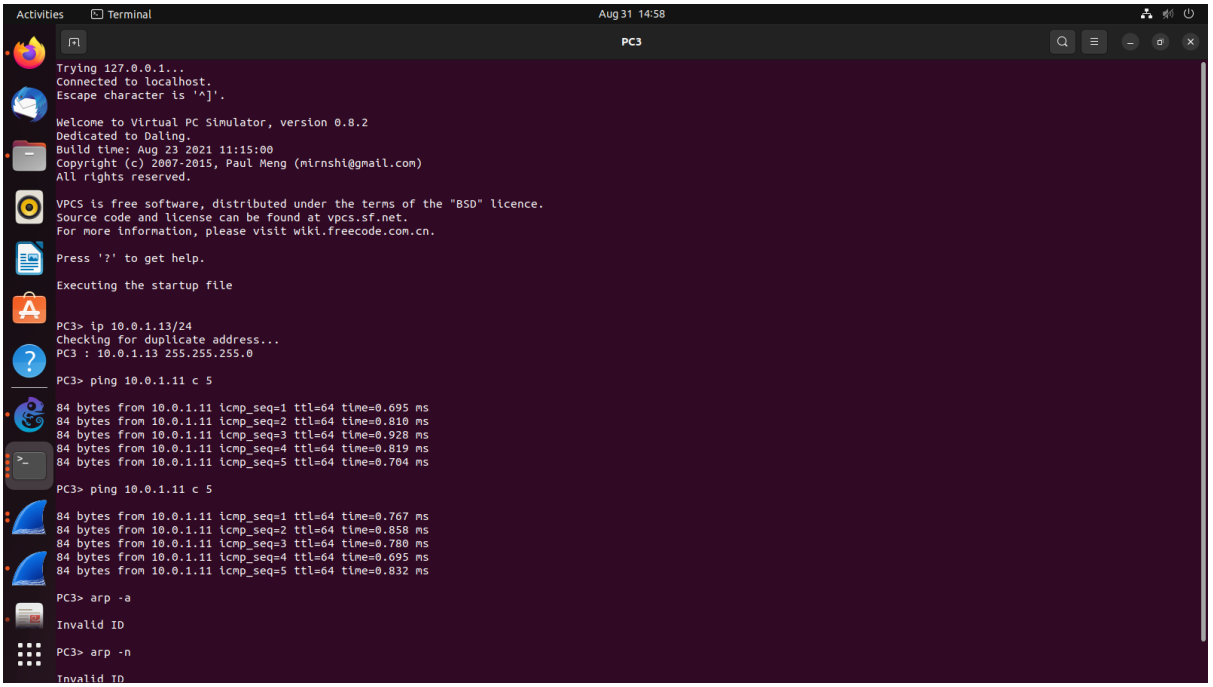
VMS	IP Address of eth0
PC1	10.0.1.11 / 24
PC2	10.0.1.12 / 24
PC3	10.0.1.13 / 24
PC4	10.0.1.11 / 24

Table 5.2: IP addresses

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

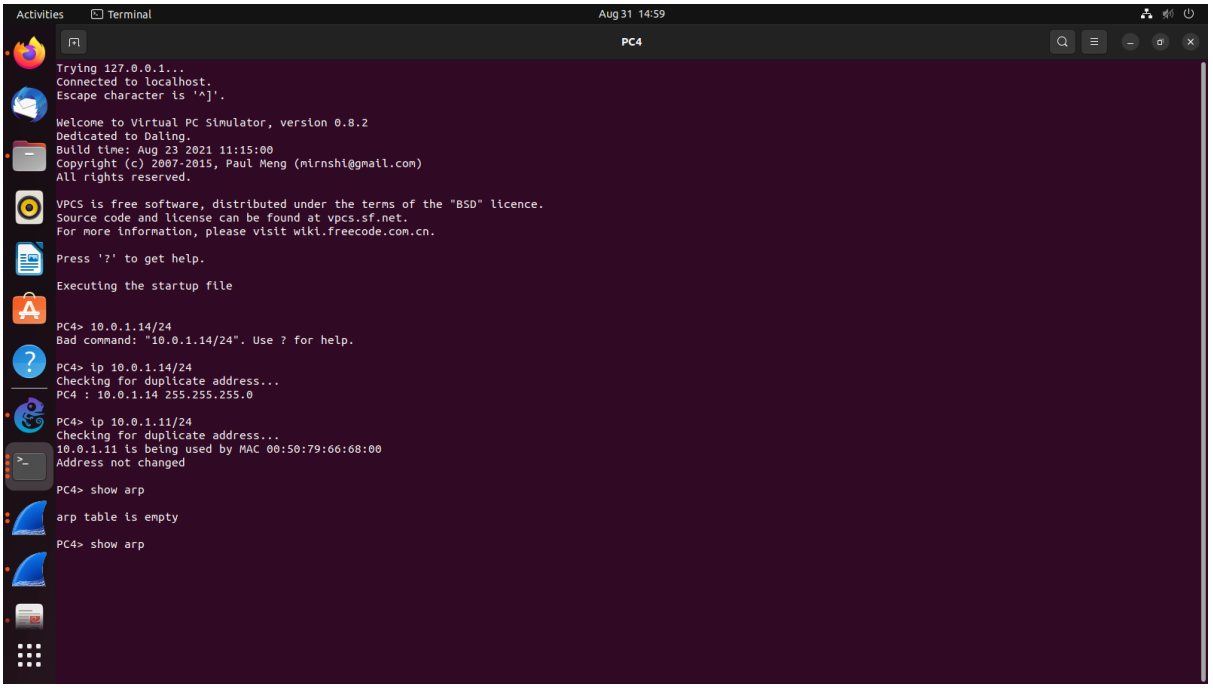


c. From PC3, issue a ping command to the duplicate IP address, 10.0.1.11, by typing
PC3% ping 10.0.1.11 –c 5



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

PC3% arp – a



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

in Table 6.1.

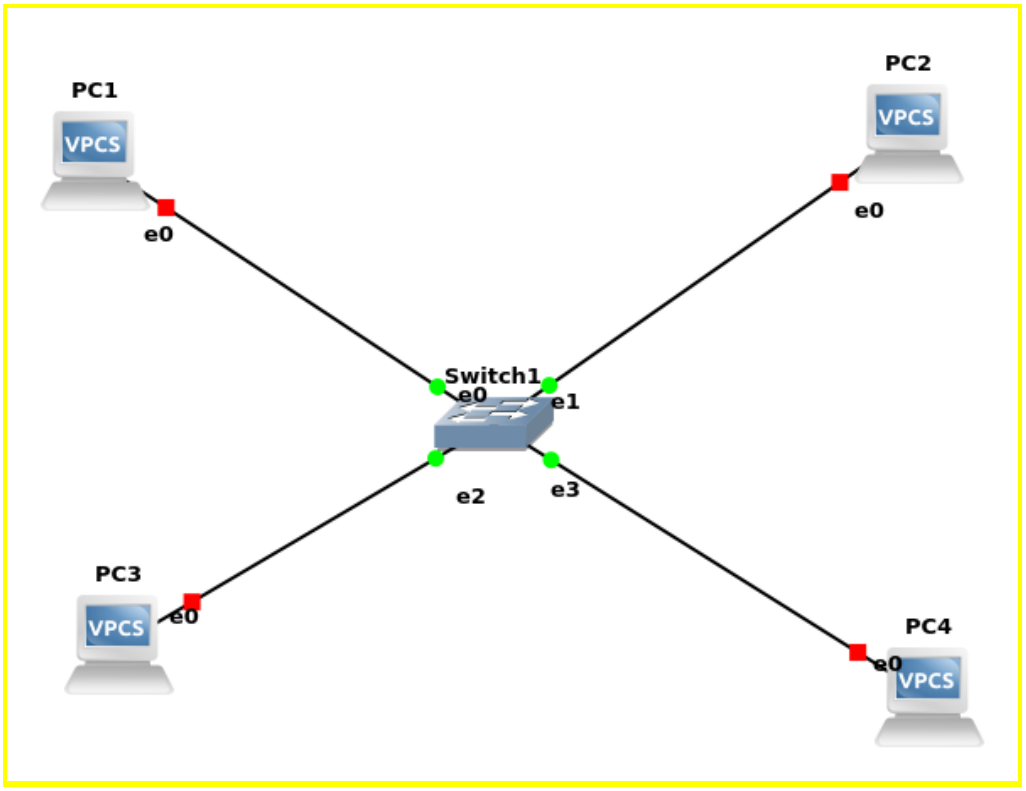
```
arp table is empty

PC4> ip 10.0.1.14/24
Checking for duplicate address..
PC4 : 10.0.1.14 255.255.255.0

PC4>
```

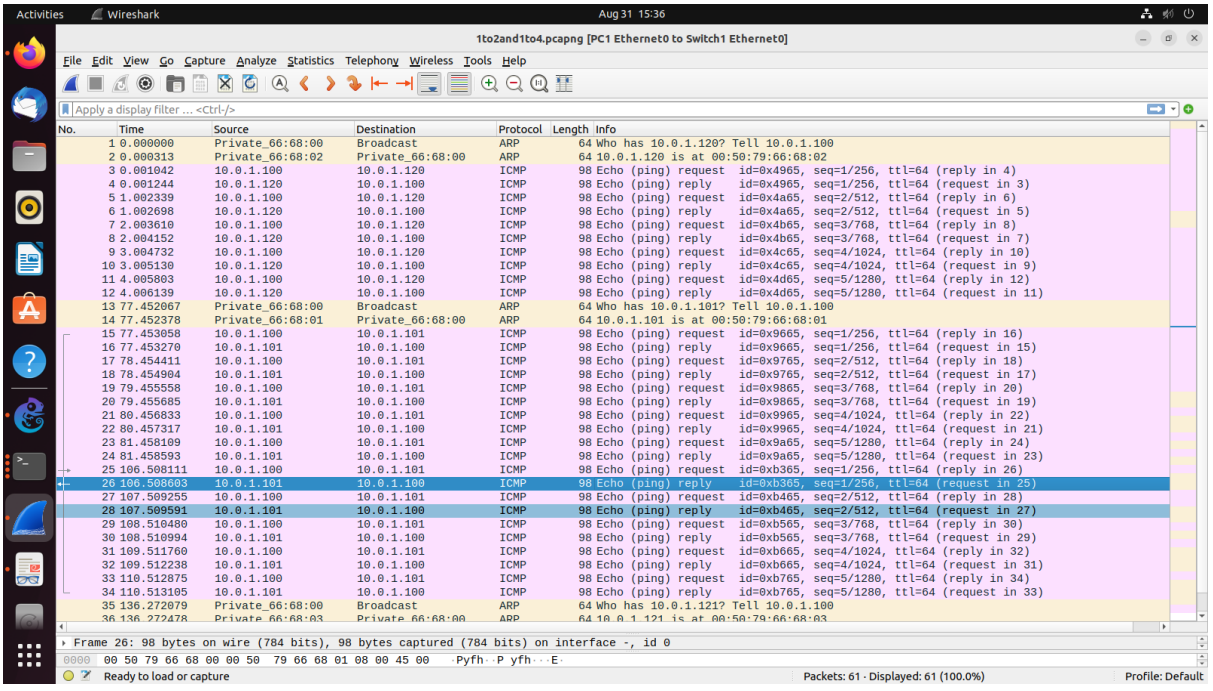
3. To test the effects of changing the netmask of a network configuration.
a. Design the configuration as Exercise 1 and replace the hub with a switch, two hosts (PC2 and PC4) have been assigned different network prefixes.
Setup the interfaces of the hosts as follows:
VPCS IP Address of eth0 Network 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
b. Run Wireshark on PC1-Hub1 link and capture the packets for the following scenarios
i. From PC1 ping PC3.
ii. From PC1 ping PC2.
iii. From PC1 ping PC4.
iv. From PC4 ping PC1.
v. From PC2 ping PC4.
vi. From PC2 ping PC3.
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.
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).

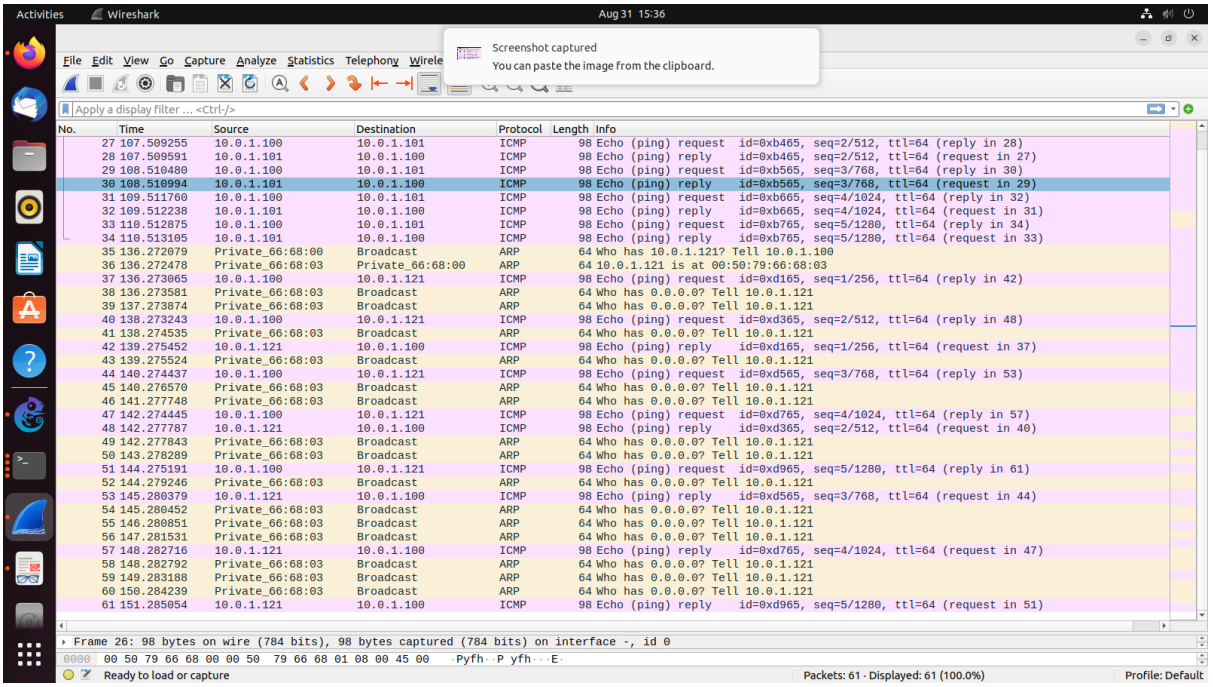
ans)



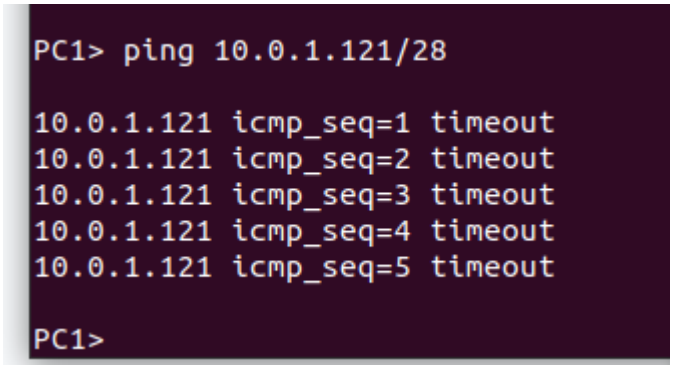
i. From PC1 ping PC3.

ii. From PC1 ping PC2.





iii. From PC1 ping PC4.



iv. From PC4 ping PC1.

v. From PC2 ping PC4.

vi. From PC2 ping PC3.

```
PC2> ping 10.0.1.121/28

No gateway found

PC2> ping 10.0.1.120/24

No gateway found

PC2>
```

VII. EXERCISES

Based On Lab Question 1

• What is the destination MAC address of an ARP Request packet?

Target MAC address: Broadcast (ff:ff:ff:ff:ff:ff)

• What are the different Type Field values in the Ethernet headers that you observed?

Type: ARP (0x0806)

• Use the captured data to analyze the process in which ARP acquires the MAC address for IPaddress 10.0.1.12

- PC1 broadcasts an ARP Request asking for the MAC address of 10.0.1.12.
- PC3, with that IP, replies with an ARP Reply containing its MAC.
- PC1 updates its ARP cache with this mapping.

Based On Lab Question 2

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

When hosts with duplicate IP addresses ping a target (10.0.1.11), both send simultaneous ICMP Echo Requests. This can confuse network responses and create inconsistent outcomes.

• Did the ping command result in error messages?

Yes, due to the duplicate IP addresses, the ping command could lead to errors like inconsistent replies or dropped packets.

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

Duplicate IP addresses can compromise security by allowing unauthorized data interception, data corruption, denial-of-service attacks, and spoofing attacks.

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

If PC1 and PC4 both have IP10.0.0.11, ARP Requests from PC1 could elicit responses from both devices. PC1's ARP cache might store multiple MAC addresses for the same IP. This can lead to intercepted data and confusion, as PC1 might send data to the wrong device or have data intercepted by PC4.

Based On Lab Question 3

• 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?

i. **PC1 pinging PC3**: This ping operation should be successful since PC1 and PC3 are on the same subnet (10.0.1.0/24). No gateway is needed for communication within the same subnet.

ii. **PC1 pinging PC2**: This ping operation was successful since PC1 and PC2.

iii. **PC1 pinging PC4**: Similar to the previous case, PC1 and PC4 are on different subnets (10.0.1.0/24 vs. 10.0.1.112/28). This ping operation also fails, resulting in the "no gateway found" message.

iv. **PC4 pinging PC1**: PC4 pinging PC1 will fail due to the same reasons mentioned in ii and iii. The "no gateway found" message indicates that PC4 doesn't have a direct route to PC1's subnet.

v. **PC2 pinging PC4**: Since PC2 and PC4 have the same network prefix (10.0.1.96/28), they are on the same subnet. This ping operation is unsuccessful. The "no gateway found" message might indicate that no gateway is required for communication within the same subnet.

vi. **PC2 pinging PC3**: This ping operation failed because PC2 and PC3 are on different subnets (10.0.1.96/28 vs. 10.0.1.0/24). The "no gateway found" message indicates that PC2 doesn't have a direct route to PC3's subnet.