

## 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.

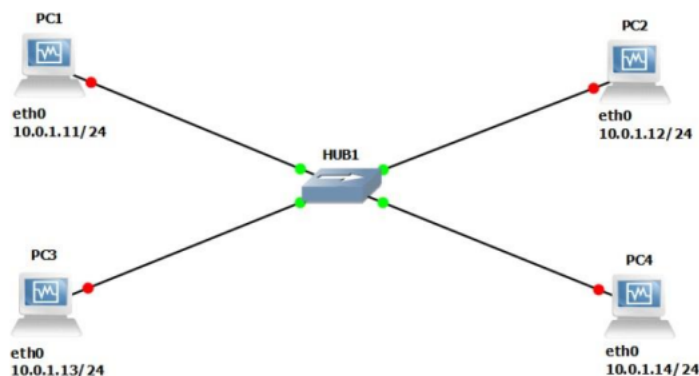
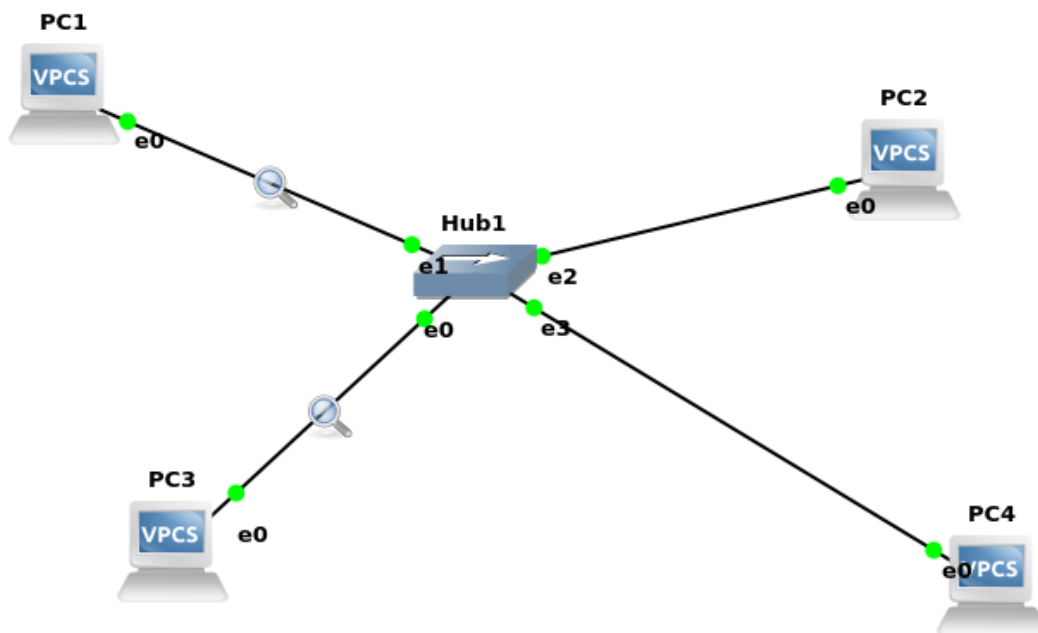


Figure 5.29: Network Design

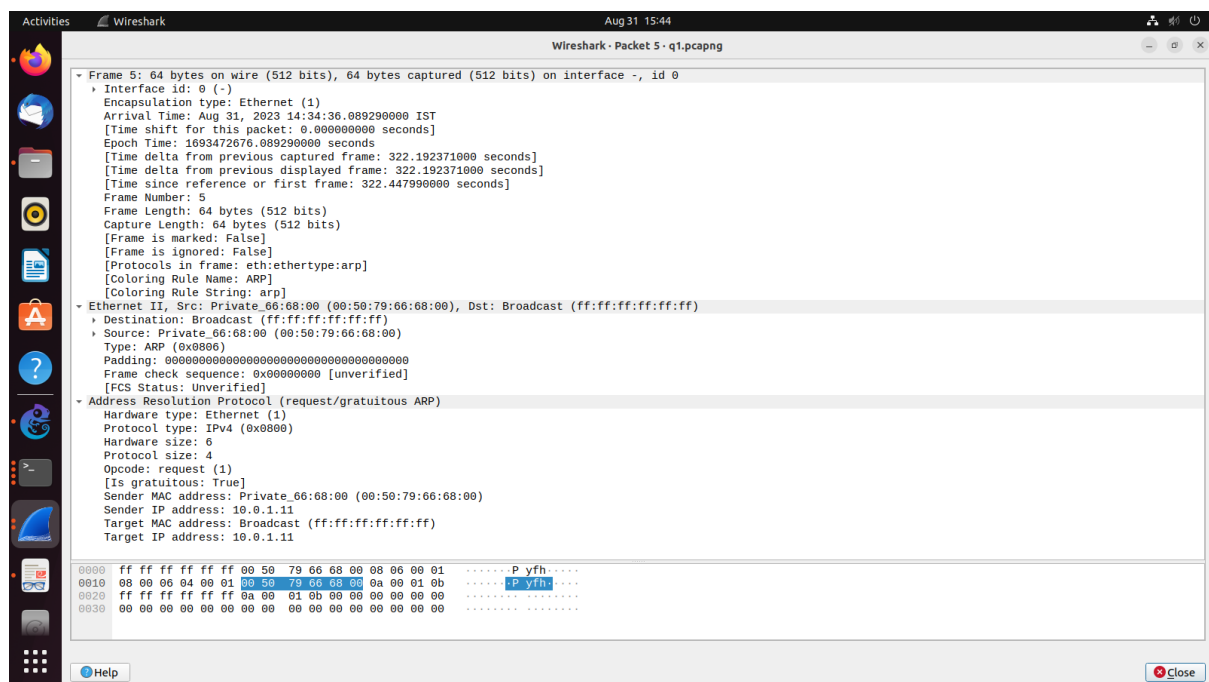
VMS	IP Addresses of Ethernet Interface eth0
PC1	10.0.1.11 / 24
PC2	10.0.1.12 / 24
PC3	10.0.1.13 / 24
PC4	10.0.1.14 / 24

ANS)



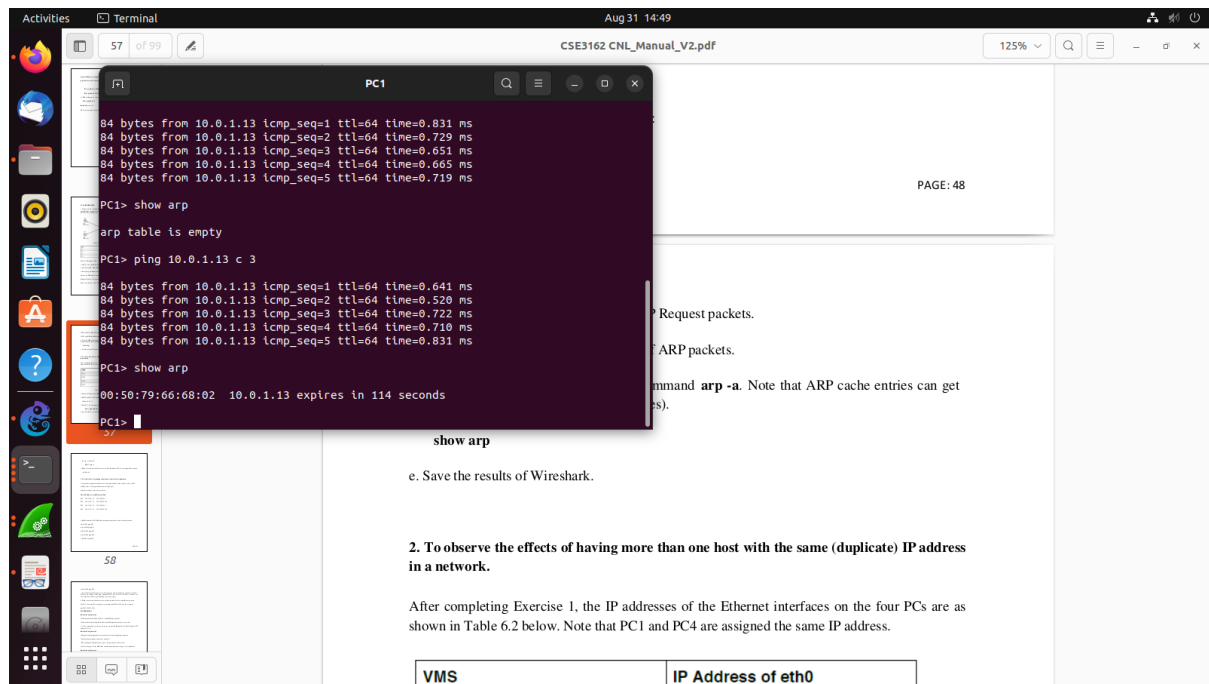
Direct our attention to the following fields:

- 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 using the `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.

```

Aug 31 14:51
PC4
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^J'.

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

PC4> 10.0.1.14/24
Bad command: "10.0.1.14/24". Use ? for help.

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

PC4> ip 10.0.1.11/24
Checking for duplicate address...
10.0.1.11 is being used by MAC 00:50:79:66:68:00
Address not changed

PC4>

```

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

```
Activities Terminal Aug 31 14:58 PC3
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

PC3> ip 10.0.1.13/24
Checking for duplicate address...
PC3 : 10.0.1.13 255.255.255.0

PC3> ping 10.0.1.11 c 5
84 bytes from 10.0.1.11 icmp_seq=1 ttl=64 time=0.695 ms
84 bytes from 10.0.1.11 icmp_seq=2 ttl=64 time=0.810 ms
84 bytes from 10.0.1.11 icmp_seq=3 ttl=64 time=0.928 ms
84 bytes from 10.0.1.11 icmp_seq=4 ttl=64 time=0.819 ms
84 bytes from 10.0.1.11 icmp_seq=5 ttl=64 time=0.704 ms

PC3> ping 10.0.1.11 c 5
84 bytes from 10.0.1.11 icmp_seq=1 ttl=64 time=0.767 ms
84 bytes from 10.0.1.11 icmp_seq=2 ttl=64 time=0.858 ms
84 bytes from 10.0.1.11 icmp_seq=3 ttl=64 time=0.780 ms
84 bytes from 10.0.1.11 icmp_seq=4 ttl=64 time=0.695 ms
84 bytes from 10.0.1.11 icmp_seq=5 ttl=64 time=0.832 ms

PC3> arp -a
Invalid ID

PC3> arp -n
Invalid ID
```

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

PC3% `arp -a`

```
Activities Terminal Aug 31 14:59 PC4
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

PC4> 10.0.1.14/24
Bad command: "10.0.1.14/24". Use ? for help.

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

PC4> ip 10.0.1.11/24
Checking for duplicate address...
10.0.1.11 is being used by MAC 00:50:79:66:68:00
Address not changed

PC4> show arp
arp table is empty

PC4> show arp
```

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

PC1 10.0.1.100 / 24 255.255.255.0

PC2 10.0.1.101 / 28 255.255.255.240

PC3 10.0.1.120 / 24 255.255.255.0

PC4 10.0.1.121 / 28 255.255.255.240

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.

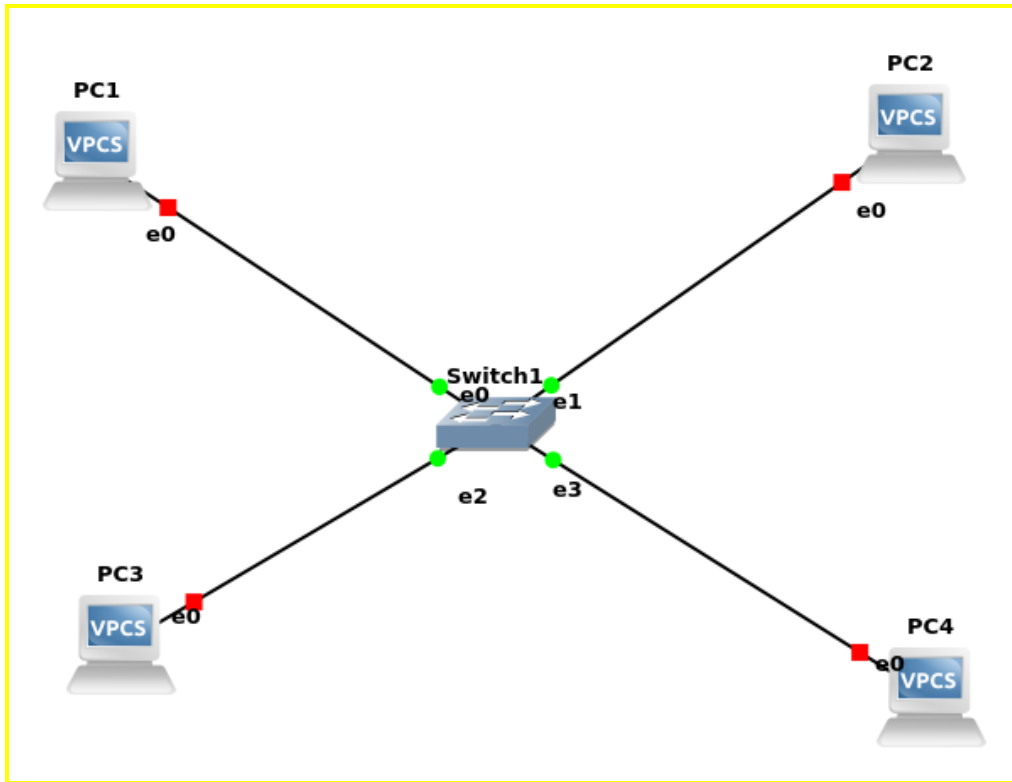
v. From PC2 ping PC4.

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.

Wireshark capture data for 1to2and1to4.pcapng [PC1 Ethernet0 to Switch1 Ethernet0]

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Private::66:68:00	Broadcast	ARP	64	Who has 10.0.1.120? Tell 10.0.1.100
2	0.000313	Private::66:68:02	Private::66:68:00	ARP	64	10.0.1.120 is at 00:50:79:66:68:02
3	0.001042	10.0.1.100	10.0.1.120	ICMP	98	Echo (ping) request id=0x4965, seq=1/256, ttl=64 (reply in 4)
4	0.001244	10.0.1.120	10.0.1.100	ICMP	98	Echo (ping) reply id=0x4965, seq=1/256, ttl=64 (request in 3)
5	0.002339	10.0.1.100	10.0.1.120	ICMP	98	Echo (ping) request id=0x4a65, seq=2/512, ttl=64 (reply in 6)
6	0.002698	10.0.1.120	10.0.1.100	ICMP	98	Echo (ping) reply id=0x4a65, seq=2/512, ttl=64 (request in 5)
7	0.003610	10.0.1.100	10.0.1.120	ICMP	98	Echo (ping) request id=0x4b65, seq=3/768, ttl=64 (reply in 8)
8	0.004152	10.0.1.120	10.0.1.100	ICMP	98	Echo (ping) reply id=0x4b65, seq=3/768, ttl=64 (request in 7)
9	0.004732	10.0.1.100	10.0.1.120	ICMP	98	Echo (ping) request id=0x4c65, seq=4/1024, ttl=64 (reply in 10)
10	0.005130	10.0.1.120	10.0.1.100	ICMP	98	Echo (ping) reply id=0x4c65, seq=4/1024, ttl=64 (request in 9)
11	0.005803	10.0.1.100	10.0.1.120	ICMP	98	Echo (ping) request id=0x4d65, seq=5/1280, ttl=64 (reply in 12)
12	0.006139	10.0.1.120	10.0.1.100	ICMP	98	Echo (ping) reply id=0x4d65, seq=5/1280, ttl=64 (request in 11)
13	0.007267	Private::66:68:00	Broadcast	ARP	64	Who has 10.0.1.101? Tell 10.0.1.100
14	0.007378	Private::66:68:01	Private::66:68:00	ARP	64	10.0.1.101 is at 00:50:79:66:68:01
15	0.007458	10.0.1.100	10.0.1.101	ICMP	98	Echo (ping) request id=0x9665, seq=1/256, ttl=64 (request in 16)
16	0.007527	10.0.1.101	10.0.1.100	ICMP	98	Echo (ping) reply id=0x9665, seq=1/256, ttl=64 (request in 15)
17	0.007844	10.0.1.100	10.0.1.101	ICMP	98	Echo (ping) request id=0x9765, seq=2/512, ttl=64 (request in 18)
18	0.007844	10.0.1.101	10.0.1.100	ICMP	98	Echo (ping) reply id=0x9765, seq=2/512, ttl=64 (request in 17)
19	0.007855	10.0.1.100	10.0.1.101	ICMP	98	Echo (ping) request id=0x9865, seq=3/768, ttl=64 (request in 20)
20	0.007855	10.0.1.101	10.0.1.100	ICMP	98	Echo (ping) reply id=0x9865, seq=3/768, ttl=64 (request in 19)
21	0.007863	10.0.1.100	10.0.1.101	ICMP	98	Echo (ping) request id=0x9965, seq=4/1024, ttl=64 (request in 22)
22	0.007863	10.0.1.101	10.0.1.100	ICMP	98	Echo (ping) reply id=0x9965, seq=4/1024, ttl=64 (request in 21)
23	0.007863	10.0.1.100	10.0.1.101	ICMP	98	Echo (ping) request id=0x9a65, seq=5/1280, ttl=64 (request in 24)
24	0.007863	10.0.1.101	10.0.1.100	ICMP	98	Echo (ping) reply id=0x9a65, seq=5/1280, ttl=64 (request in 23)
25	0.007863	10.0.1.100	10.0.1.101	ICMP	98	Echo (ping) request id=0xb365, seq=1/256, ttl=64 (request in 26)
26	0.007863	10.0.1.101	10.0.1.100	ICMP	98	Echo (ping) reply id=0xb365, seq=1/256, ttl=64 (request in 25)
27	0.007863	10.0.1.100	10.0.1.101	ICMP	98	Echo (ping) request id=0xb465, seq=2/512, ttl=64 (request in 28)
28	0.007863	10.0.1.101	10.0.1.100	ICMP	98	Echo (ping) reply id=0xb465, seq=2/512, ttl=64 (request in 27)
29	0.007863	10.0.1.100	10.0.1.101	ICMP	98	Echo (ping) request id=0xb565, seq=3/768, ttl=64 (request in 30)
30	0.007863	10.0.1.101	10.0.1.100	ICMP	98	Echo (ping) reply id=0xb565, seq=3/768, ttl=64 (request in 29)
31	0.007863	10.0.1.100	10.0.1.101	ICMP	98	Echo (ping) request id=0xb665, seq=4/1024, ttl=64 (request in 32)
32	0.007863	10.0.1.101	10.0.1.100	ICMP	98	Echo (ping) reply id=0xb665, seq=4/1024, ttl=64 (request in 31)
33	0.007863	10.0.1.100	10.0.1.101	ICMP	98	Echo (ping) request id=0xb765, seq=5/1280, ttl=64 (request in 34)
34	0.007863	10.0.1.101	10.0.1.100	ICMP	98	Echo (ping) reply id=0xb765, seq=5/1280, ttl=64 (request in 33)
35	0.007863	Private::66:68:00	Broadcast	ARP	64	Who has 10.0.1.121? Tell 10.0.1.100
36	0.007863	Private::66:68:03	Private::66:68:00	ARP	64	10.0.1.121 is at 00:50:79:66:68:03

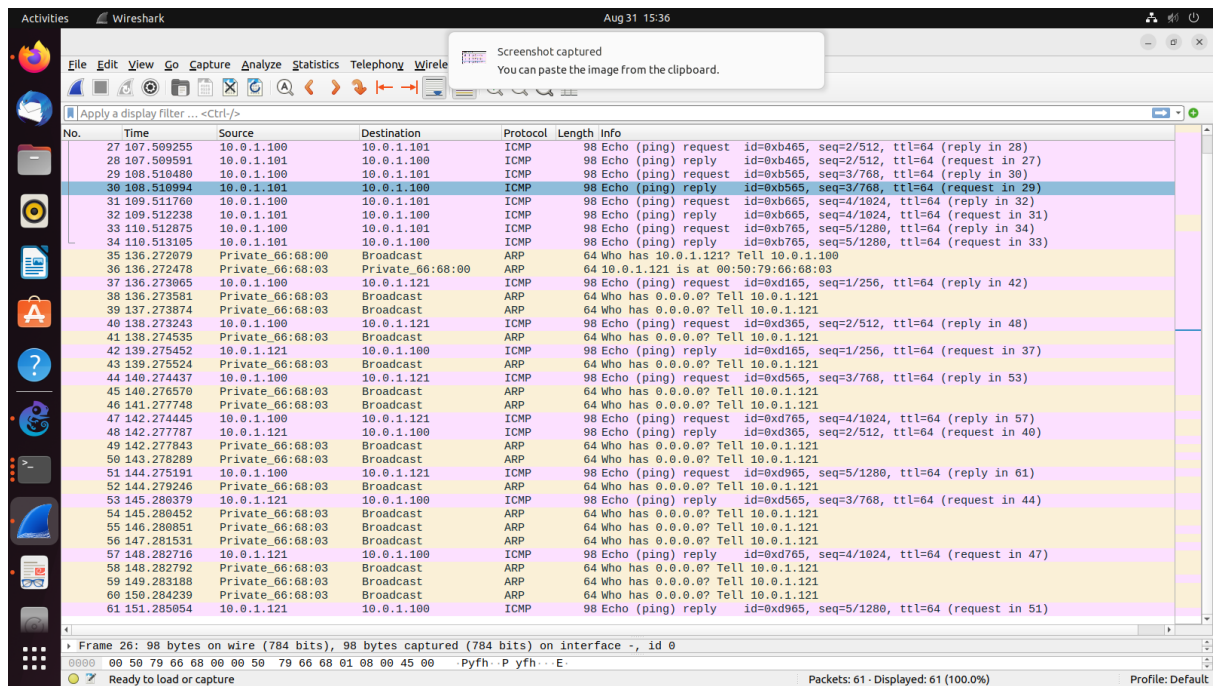
Frame 26: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface -, id 0

0000 00 50 79 66 68 00 00 50 79 66 68 01 00 00 45 00 Pyfh...E

Ready to load or capture

Packets: 61 · Displayed: 61 (100.0%)

Profile: Default



### iii. From PC1 ping PC4.

```
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

PC1>
```

### iv. From PC4 ping PC1.

```
PC4> ping 10.0.1.100/24

No gateway found

PC4> █
```

### 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 IP address 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 IP 10.0.0.11, 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.