

LINUX NETWORKING MODULE 6 ASSESSMENT SOLUTION

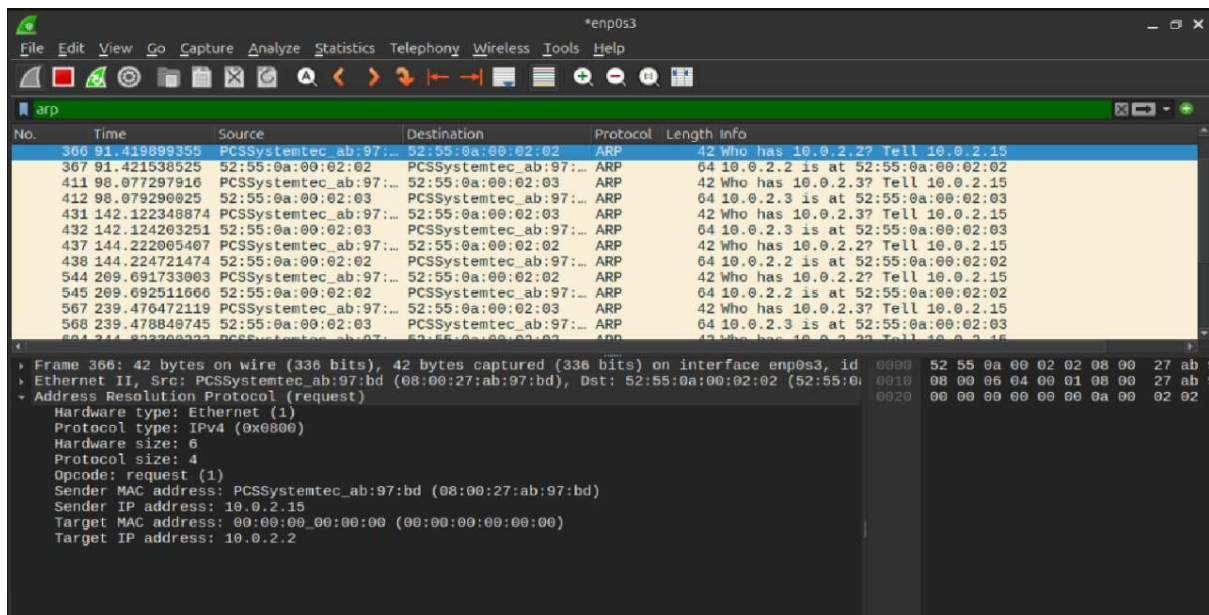
-BY SAKTHI KUMAR S

1. Capture and analyse ARP packets using Wireshark. Inspect the ARP request and reply frames when your device attempts to find the router's MAC address. Discuss the importance of ARP in packet forwarding.

To Trigger ARP to find Router's MAC address:

```
sakthi-kumar-s@sakthi-kumar-s-VirtualBox: ~  
(base) sakthi-kumar-s@sakthi-kumar-s-VirtualBox:~$ ip route | grep default  
default via 10.0.2.2 dev enp0s3 proto dhcp src 10.0.2.15 metric 100  
(base) sakthi-kumar-s@sakthi-kumar-s-VirtualBox:~$ ping 10.0.2.2  
PING 10.0.2.2 (10.0.2.2) 56(84) bytes of data:  
64 bytes from 10.0.2.2: icmp_seq=1 ttl=255 time=1.57 ms  
64 bytes from 10.0.2.2: icmp_seq=2 ttl=255 time=2.34 ms  
64 bytes from 10.0.2.2: icmp_seq=3 ttl=255 time=2.06 ms  
64 bytes from 10.0.2.2: icmp_seq=4 ttl=255 time=5.17 ms  
  
^Z  
[1]+  Stopped                  ping 10.0.2.2  
(base) sakthi-kumar-s@sakthi-kumar-s-VirtualBox:~$ arp -a  
_gateway (10.0.2.2) at 52:55:0a:00:02:02 [ether] on enp0s3
```

Wireshark Output:



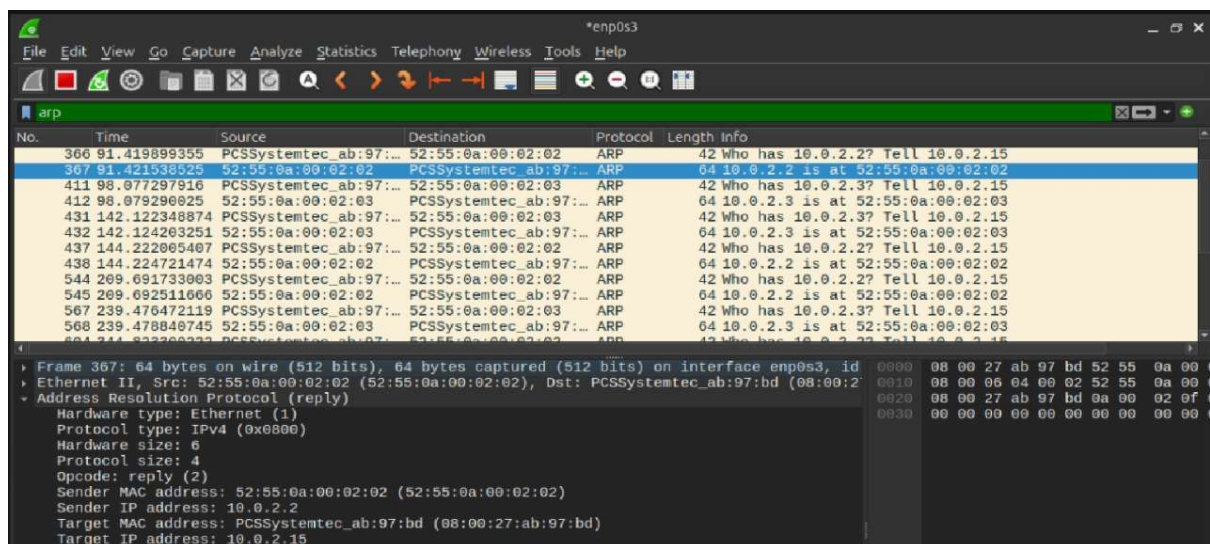
```
*enp0s3  
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help  
arp  
No. Time Source Destination Protocol Length Info  
366 91.419899355 PCSSystemtec_ab:97:bd 52:55:0a:00:02:02 ARP 42 Who has 10.0.2.2? Tell 10.0.2.15  
307 91.421538525 52:55:0a:00:02:02 PCSSystemtec_ab:97:bd ARP 64 10.0.2.2 is at 52:55:0a:00:02:02  
411 98.077297916 PCSSystemtec_ab:97:bd 52:55:0a:00:02:03 ARP 42 Who has 10.0.2.3? Tell 10.0.2.15  
412 98.079290925 52:55:0a:00:02:03 PCSSystemtec_ab:97:bd ARP 64 10.0.2.3 is at 52:55:0a:00:02:03  
431 142.122348874 PCSSystemtec_ab:97:bd 52:55:0a:00:02:03 ARP 42 Who has 10.0.2.3? Tell 10.0.2.15  
432 142.124263251 52:55:0a:00:02:03 PCSSystemtec_ab:97:bd ARP 64 10.0.2.3 is at 52:55:0a:00:02:03  
437 144.222065407 PCSSystemtec_ab:97:bd 52:55:0a:00:02:02 ARP 42 Who has 10.0.2.2? Tell 10.0.2.15  
438 144.224721474 52:55:0a:00:02:02 PCSSystemtec_ab:97:bd ARP 64 10.0.2.2 is at 52:55:0a:00:02:02  
544 269.691733003 PCSSystemtec_ab:97:bd 52:55:0a:00:02:02 ARP 42 Who has 10.0.2.2? Tell 10.0.2.15  
545 269.692511666 52:55:0a:00:02:02 PCSSystemtec_ab:97:bd ARP 64 10.0.2.2 is at 52:55:0a:00:02:02  
567 239.476472119 PCSSystemtec_ab:97:bd 52:55:0a:00:02:03 ARP 42 Who has 10.0.2.3? Tell 10.0.2.15  
568 239.478848745 52:55:0a:00:02:03 PCSSystemtec_ab:97:bd ARP 64 10.0.2.3 is at 52:55:0a:00:02:03  
594 244.452200725 PCSSystemtec_ab:97:bd 52:55:0a:00:02:02 ARP 42 Who has 10.0.2.2? Tell 10.0.2.15  
Frame 366: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface enp0s3, id 0000 52 55 0a 00 02 02 08 00 27 ab 97 bd  
Ethernet II, Src: PCSSystemtec_ab:97:bd (08:00:27:ab:97:bd), Dst: 52:55:0a:00:02:02 (52:55:0a:00:02:02)  
Address Resolution Protocol (request)  
Hardware type: Ethernet (1)  
Protocol type: IPv4 (0x0800)  
Hardware size: 6  
Protocol size: 4  
Opcode: request (1)  
Sender MAC address: PCSSystemtec_ab:97:bd (08:00:27:ab:97:bd)  
Sender IP address: 10.0.2.15  
Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)  
Target IP address: 10.0.2.2
```

ARP Request Packet

- Source MAC Address: device's MAC.
- Destination MAC Address: FF:FF:FF:FF:FF:FF (Broadcast).
- Source IP Address: device's IP.
- Target IP Address: The router's IP.

ARP Reply Packet:

- Source MAC Address: Router's MAC.
- Destination MAC Address: device's MAC.
- Source IP Address: Router's IP.
- Target IP Address: device's IP.



Importance of ARP in Packet Forwarding:

- ARP (Address Resolution Protocol) is essential for mapping an IP address to a MAC address in a local network.
- When sending packets to another network device, the sender needs the MAC address of the destination or gateway.
- Without ARP, devices wouldn't know the MAC address of other hosts, preventing communication.