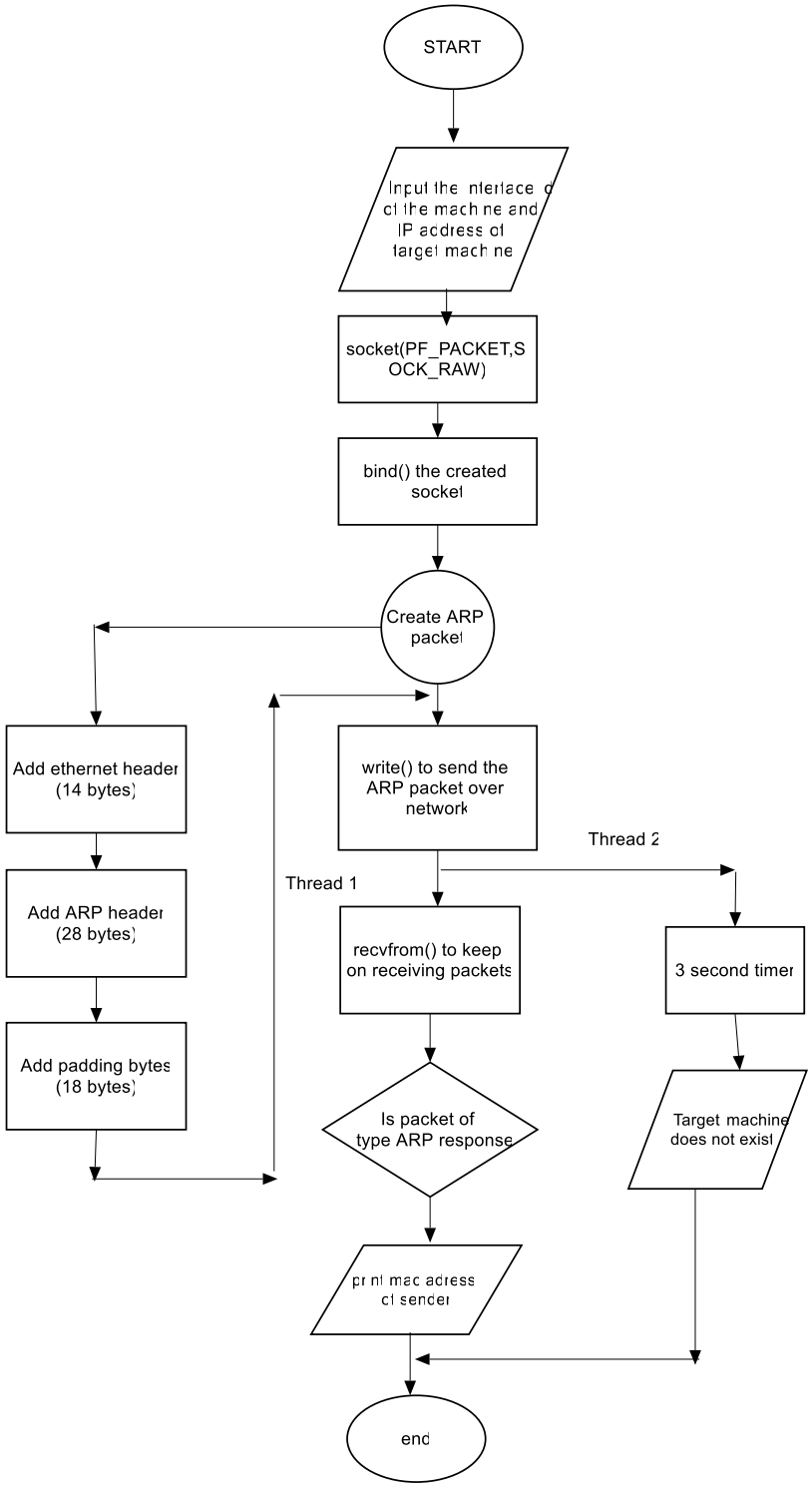
Assignment 5: Application development using RAW socket

AIM: Designing an ARP app working on the application layer that mimics the ARP protocol in determining the MAC address of a machine using raw sockets.

PROGRAM LOGIC:



STRUCTURE OF ETHERNET HEADER :

- Destination MAC address(6 bytes) – 0xFFFF to broadcast the packet
- Source MAC address(6 bytes)
- Protocol(2 bytes) – 0x0806 for ARP

STRUCTURE OF ARP HEADER :

- Hardware Type(2 bytes) – 0x0001 for Ethernet
- Protocol Type(2 bytes) – 0x0800 for IPv4
- Hardware address length(1 byte) – 6
- Protocol address length(1 byte) – 4
- Opcode(2 bytes) – 1 for Request and 2 for Reply
- Source MAC address (6 bytes)
- Source IP address (4 bytes)
- Destination MAC address(6 bytes)
- Destination IP address(4 bytes) -

Both these headers are implemented as structs and serialized in sequence while packet creation. 18 bytes of padding are added to make 60 byte sized ARP packet.

PACKET RECEIVING

After sending the packet one thread constantly receives incoming packets and checks for the following conditions:

- Total bytes received = 60
- Check if opcode is 2
- Check if sender IP address is the target IP address

If all these conditions are satisfied then the packet is the ARP response packet and thus the corresponding sender MAC address is printed out.

Otherwise, the process is repeated infinitely.

TIMER PROCEDURE

Another thread is made to sleep for 3 seconds. After waking up it displays "Target Machine Not in the network" and exits the program execution. This prevents the packet receiving method from executing infinitely long when it does not receive any response packet.

COMMAND LINE INPUTS

The program expects the interface name, Host IP address, Host MAC address and Target IP address as command line inputs. The program is executed as:

./a.out <interface name> <host IP> <host MAC> <target IP>

OUTPUT SCREENSHOTS

```
root@ayan:/home/ayan/socket_prog# gcc rawsock.c
root@ayan:/home/ayan/socket_prog# ./a.out enp0s3 192.168.0.101 08:00:27:83:03:b9 192.168.0.100
MAC address of 192.168.0.100 is : B6:85:BD:9F:1C:56
```

```
    21 12.980524204  PcsCompu_83:03:b9  Broadcast           ARP      60 Who has 192.168.0.100? Tell 192.168.0.101
    22 13.033163283  b6:85:bd:9f:1c:56  PcsCompu_83:03:b9   ARP      60 192.168.0.100 is at b6:85:bd:9f:1c:56
    23 13.975930909  PcsCompu_83:03:b9  TP-Link_f9:78:13    ARP      42 Who has 192.168.0.1? Tell 192.168.0.101
    24 13.976929508  TP-Link_f9:78:13   PcsCompu_83:03:b9   ARP      60 192.168.0.1 is at e8:48:b8:f9:78:13

▸ Frame 21: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface enp0s3, id 0
▾ Ethernet II, Src: PcsCompu_83:03:b9 (08:00:27:83:03:b9), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  ▸ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  ▸ Source: PcsCompu_83:03:b9 (08:00:27:83:03:b9)
    Type: ARP (0x0806)
    Padding: 000000000000000000000000000000000000
▾ Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: PcsCompu_83:03:b9 (08:00:27:83:03:b9)
    Sender IP address: 192.168.0.101
    Target MAC address: Broadcast (ff:ff:ff:ff:ff:ff)
    Target IP address: 192.168.0.100
```

ARP Request Packet Sent

```
    22 13.033163283  b6:85:bd:9f:1c:56  PcsCompu_83:03:b9   ARP      60 192.168.0.100 is at b6:85:bd:9f:1c:56
    23 13.975930909  PcsCompu_83:03:b9  TP-Link_f9:78:13    ARP      42 Who has 192.168.0.1? Tell 192.168.0.101
    24 13.976929508  TP-Link_f9:78:13   PcsCompu_83:03:b9   ARP      60 192.168.0.1 is at e8:48:b8:f9:78:13

▸ Frame 22: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface enp0s3, id 0
▾ Ethernet II, Src: b6:85:bd:9f:1c:56 (b6:85:bd:9f:1c:56), Dst: PcsCompu_83:03:b9 (08:00:27:83:03:b9)
  ▸ Destination: PcsCompu_83:03:b9 (08:00:27:83:03:b9)
  ▸ Source: b6:85:bd:9f:1c:56 (b6:85:bd:9f:1c:56)
    Type: ARP (0x0806)
    Padding: 000000000000000000000000000000000000
▾ Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: b6:85:bd:9f:1c:56 (b6:85:bd:9f:1c:56)
    Sender IP address: 192.168.0.100
    Target MAC address: PcsCompu_83:03:b9 (08:00:27:83:03:b9)
    Target IP address: 192.168.0.101
```

ARP Response Packet Received

```
root@ayan:/home/ayan/socket_prog# ./a.out enp0s3 192.168.0.101 08:00:27:83:03:b9 192.168.0.109
Target machine not in network
```

When Target IP address doesn’t exist in network