DHARSHINI.S 241901026

EX NO.5 DATE: 01/09/2025

**PACKET SNIFFING USING RAW SOCKETS**

**AIM:**

To capture and display Ethernet frame details (Destination MAC, Source MAC, and Protocol) from

network traffic using raw sockets.

Algorithm:

1. Create a raw socket to capture all incoming network packets.

2. Enable promiscuous mode to capture all frames, not just those directed to the machine.

3. Unpack the Ethernet frame to extract Destination MAC, Source MAC, and Protocol.

4. Continuously print the extracted details.

CODE:

import socket

import struct

import binascii

import textwrap

def main():

# Get host

host = socket.gethostbyname(socket.gethostname())

print(&#39;IP: {}&#39;.format(host))

# Create a raw socket and bind it

conn = socket.socket(socket.AF\_INET, socket.SOCK\_RAW,

socket.IPPROTO\_IP)

conn.bind((host, 0))

# Include IP headers

conn.setsockopt(socket.IPPROTO\_IP, socket.IP\_HDRINCL, 1)

# Enable promiscuous mode

conn.ioctl(socket.SIO\_RCVALL, socket.RCVALL\_ON)

while True:

# Recive data

raw\_data, addr = conn.recvfrom(65536)

# Unpack data

dest\_mac, src\_mac, eth\_proto, data = ethernet\_frame(raw\_data)

print(&#39;\nEthernet Frame:&#39;)

print(&quot;Destination MAC: {}&quot;.format(dest\_mac))

print(&quot;Source MAC: {}&quot;.format(src\_mac))

print(&quot;Protocol: {}&quot;.format(eth\_proto))

# Unpack ethernet frame

def ethernet\_frame(data):

dest\_mac, src\_mac, proto = struct.unpack(&#39;!6s6s2s&#39;, data[:14])

return get\_mac\_addr(dest\_mac), get\_mac\_addr(src\_mac),

get\_protocol(proto), data[14:]

# Return formatted MAC address AA:BB:CC:DD:EE:FF

def get\_mac\_addr(bytes\_addr):

bytes\_str = map(&#39;{:02x}&#39;.format, bytes\_addr)

mac\_address = &#39;:&#39;.join(bytes\_str).upper()

return mac\_address

# Return formatted protocol ABCD

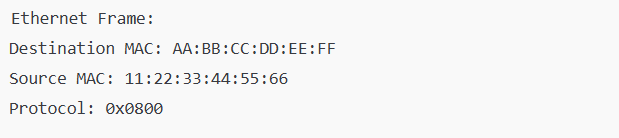
def get\_protocol(bytes\_proto):

bytes\_str = map(&#39;{:02x}&#39;.format, bytes\_proto)

protocol = &#39;&#39;.join(bytes\_str).upper()

return protocol

main()



**RESULT:**

The program continuously prints the Destination MAC, Source MAC, and Protocol

of each captured Ethernet frame, running indefinitely until manually stopped.