Indian Institute of Engineering Science and Technology, Shibpur
Department of Computer Science and Technology
Computer Network Lab (CS 3272)

Assignment 5: Application development using RAW Socket

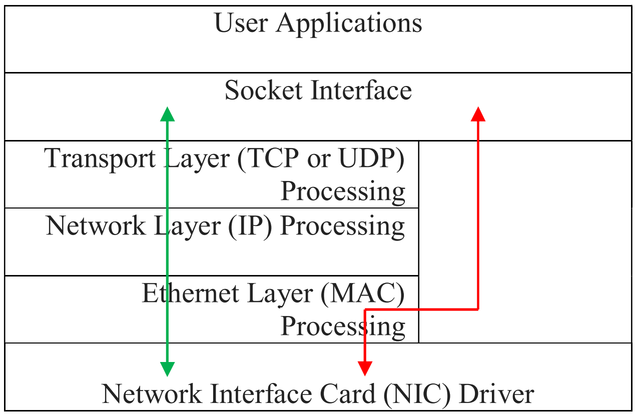
Time: 2 weeks

Objective
This assignment aims to develop ARP (Address Resolution Protocol) functionalities as a user space application, we call that as ARP-App. In reality, ARP acts as a module in Network Layer as part of the Kernel (TCP/IP stack). However, in this assignment, we would like to develop the basic ARP functionalitiesas an application using RAW sockets.

RAW Socket Overview
The regular sockets, like stream and datagram sockets, receive data from the transport layer that contains no headers but only the payload. This means there is no information about the source IP and MAC addresses. On the contrary, a raw socket is used to receive raw packets. This means packets received at the Ethernet layer will directly pass to the raw socket. Precisely, a RAW socket bypasses the regular TCP/IP processing and sends the packets to the specific user space application.

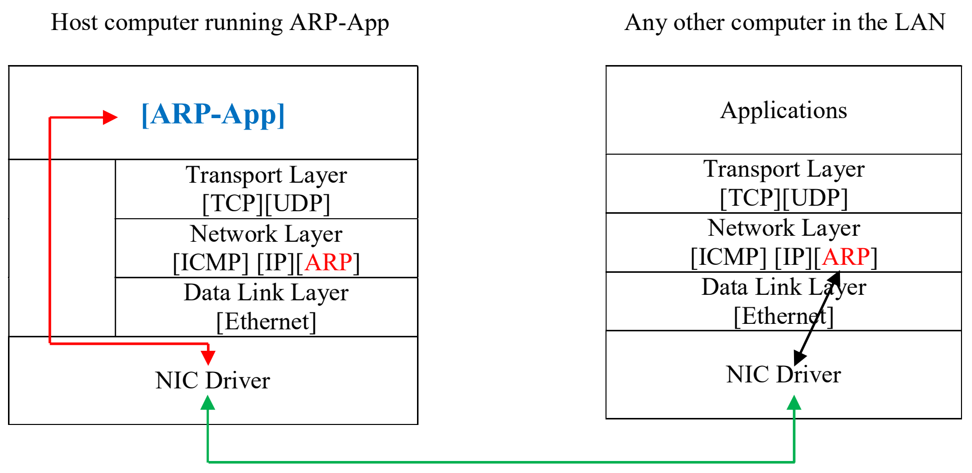
Similarly, when an application sends data into the network using the stream and datagram sockets, it is processed by various network layers. Before sending data, it is wrapped in multiple protocol layer headers, like TCP or UDP, IP, and Ethernet. The wrapped form of data, which contains all the information, like the source and destination address, is called a network packet. However, while sending data using a RAW socket, it is the responsibility of the user space application to perform the header addition and wrapping the payload.

In the following diagram, the raw socket is shown in red color, and other kinds of sockets are in green color.


User Applications
Socket Interface
Transport Layer (TCP or UDP) Processing
Network Layer (IP) Processing
Ethernet Layer (MAC) Processing
Network Interface Card (NIC) Driver

Technique
The ARP-App will be implemented and executed on a computer from where the ARP query will be performed. The ARP query aims to obtain the MAC address of a target computer for a giver IP address. The ARP-App should be implemented as a user space application without hampering Kernel's ARP module, as shown in the following figure. The RAW socket interface should bypass the Kernel TCP/IP stack as well as Ethernet and directly communicate to the NIC. The ARP-App should prepare the ARP-REQUEST message and wrap it by the required Ethernet framing and send it to the network. As the destination MAC address of the Ethernet frame is

broadcast type, the ARP-REQUEST message will be accepted by all the computers of the LAN. The NIC driver of the respective computer will pass the ARP-REQUEST message to the Kernel's ARP module of the Network Layer. If the IP Address provided in the ARP-REQUEST message matches the IP of the computer, the ARP module of the target computer responds with the ARP-RESPONSE message stating the MAC address of the interface.


Host computer running ARP-App
Any other computer in the LAN
[ARP-App]
Transport Layer [TCP][UDP]
Network Layer [ICMP] [IP][ARP]
Data Link Layer [Ethernet]
NIC Driver
Applications
Transport Layer [TCP][UDP]
Network Layer [ICMP] [IP][ARP]
Data Link Layer [Ethernet]
NIC Driver

Once the ARP-RESPONSE message reaches the host computer running ARP-App, the NIC driver accepts the message as the destination MAC address matches. In this context, the ARP-App is a packet sniffer that continuously polls all the packets received at the NIC driver. However, the ARP-App discards all kinds of packets except the ARP-RESPONSE message. On getting the intended ARP-RESPONSE message, it displays the enquired MAC address against the IP address of the target computer.

To tackle the failure situation, for example, if the enquired IP address doesn't exist in the LAN, the ARP-App starts a timer (of a reasonable duration) upon sending the ARP-REQUEST message. If the intended ARP-RESPONSE message is received in that duration, it cancels the timer. However, if the timer expires, it displays an error message stating that the ARP query failed as no ARP response was received for the queried IP address.