Brief Design(P4)

error_packets.c is a program which when run on a host keeps printing the source ip, destination ip, source port, destination port and protocol of
the packets sent by host and dropped by any of the routers on the way.

This is done simply by capturing the ICMP packets directed to the host and printing it's information.

A raw socket is used to capture all traffic directed to the host in an infinite while. When a packet is received, the ip header is checked for the protocol of the packet. If protocol == 1(i.e. ICMP) we now know that a router must have dropped a packet and sent back the ICMP error packet back.

Now this packet is parsed for printing the source ip, dst ip, source port, dst port.
The packet's IP header can tell us at which IP was the packet dropped.
The body of the ICMP contains the IP information of the packet that was dropped. So the body is parsed to extract the source, dst IP and source, dst PORT of the original packet that was dropped.

The program can be tested by running traceroute.

The article https://www.binarytides.com/packet-sniffer-code-in-c-using-linux-sockets-bsd-part-2/ was used to help in understanding how raw socket work and how can it be used to capture and decode packet's information using the necessary structures.