What's Network?

Network is the way how two devices are communicating, The data sent between the two devices are called `packets`

Communication protocol:

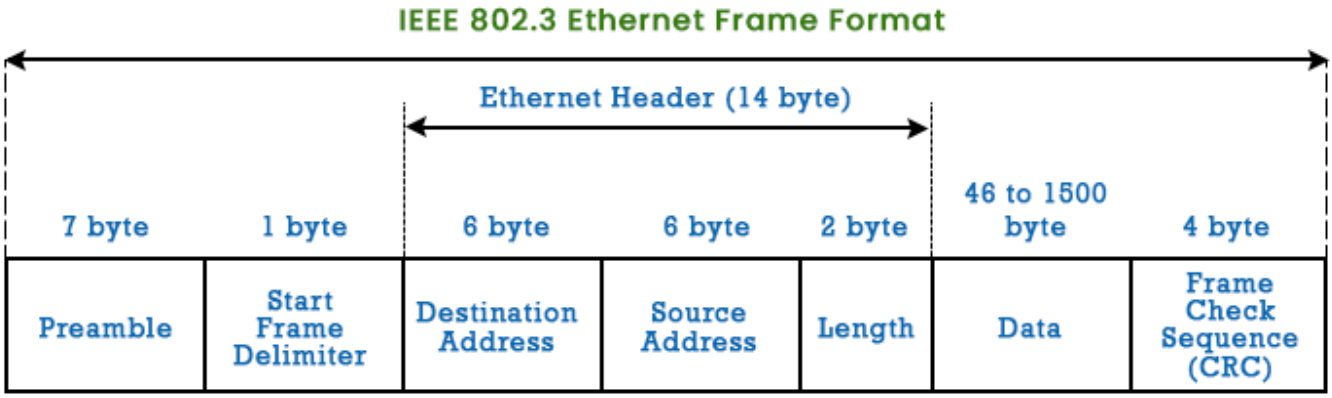
It's the way that the two devices are using to communicate with each others, we will use `SomeIp` it's a protocol used in the automotive industry.

- **Remote Process Communication:** Communication between two machines.
- **Inter-Process Communication:** Communication between two processes on the same machine.

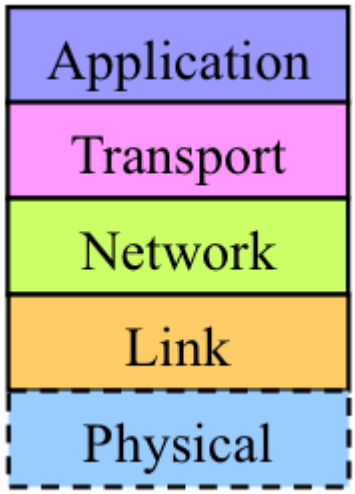
TCP/IP Layers and Protocols

1. **Application Layer** Communication Protocol installed over that layer to be communicated with: `http` , `https`, `SOMEIP`, `ssh`.
2. **Transport Layer** Communication Protocol installed over that layer to be communicated with: `TCP`, `UDP`.
3. **Network Layer** Communication Protocol installed over that layer to be communicated with: `IP-protocol`.
4. **Network Access Layer** Communication Protocol installed over that layer to be communicated with: `Ethernet`, `Wifi`, `Bluetooth`.

The Ethernet Frame stages:

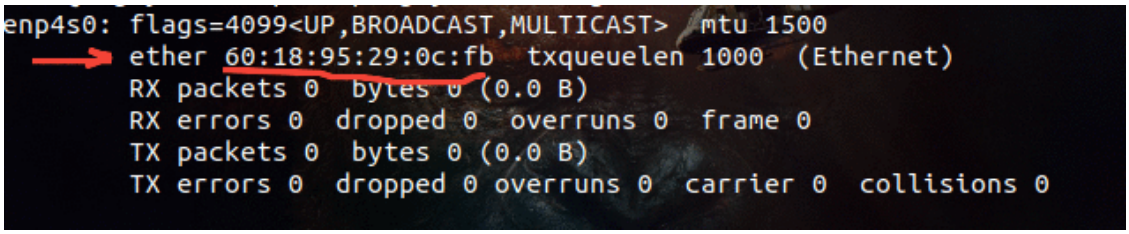


1. When a two Network cards are communicating they send Ethernet frames to each ohters, The receiver one start By comparing the Destination address with it's own MacAdress,If matched it start analysing the data and take the subFrame to another stage
2. Then the subFrame goes to the network stack Layes as shown in fig

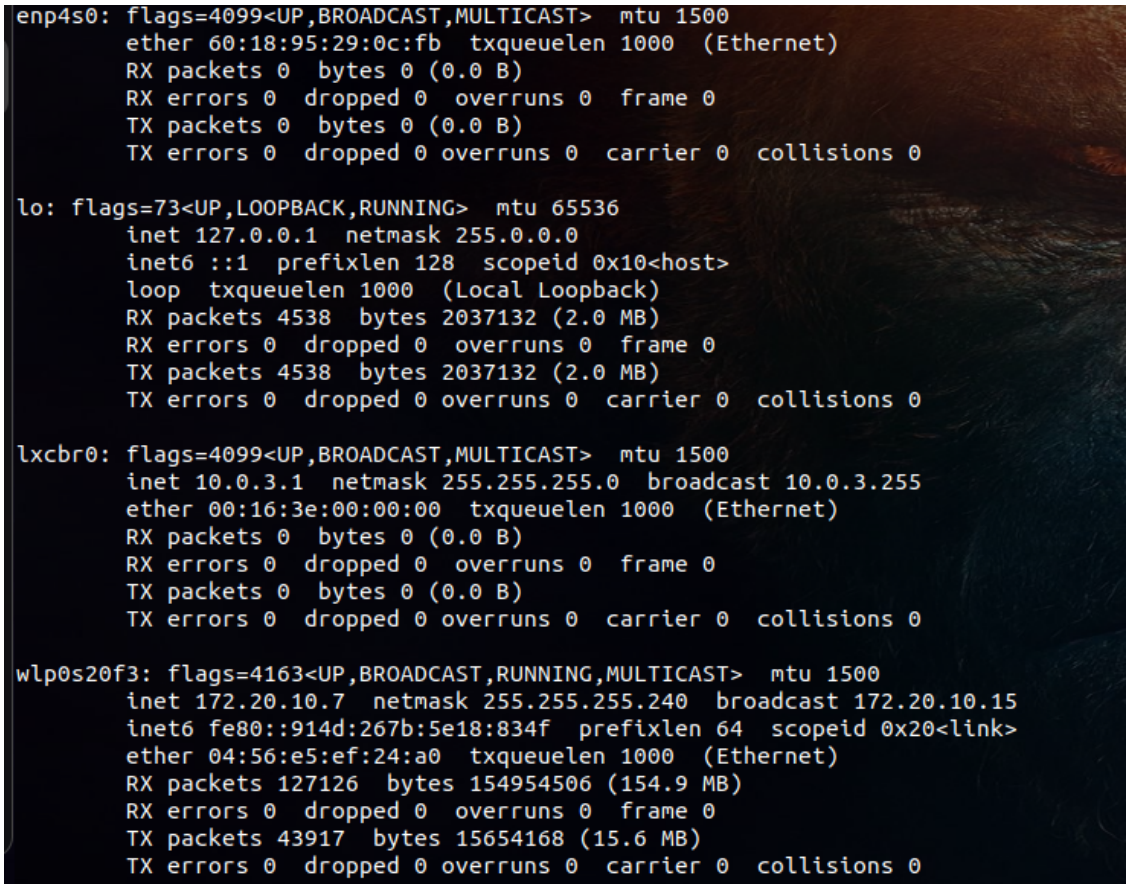


3. In the Network We compare with the IP and port
4. Transport layer will deal with the sockets and ports

Useful Commands and Tools

1. `ifconfig -a`**:** Displays all network interfaces and their MAC addresses.
    - ***NIC Information***:
        - **MAC Address:** A unique identifier for each NIC, assigned at the factory.
        - 

        - **IP Address:** Can be dynamically assigned by the router.
    - ***NIC Status***:
        - **Up:** The NIC is ready to transmit data.
        - **Down:** The NIC is disabled and cannot transmit data.



- The `enp4s0`, `lo`, `wlp0s20f3` all of them are network interfaces cards.

  - The `mtu` (Maximum Transmission Unit) defines the largest packet size that can be transmitted over the NIC.

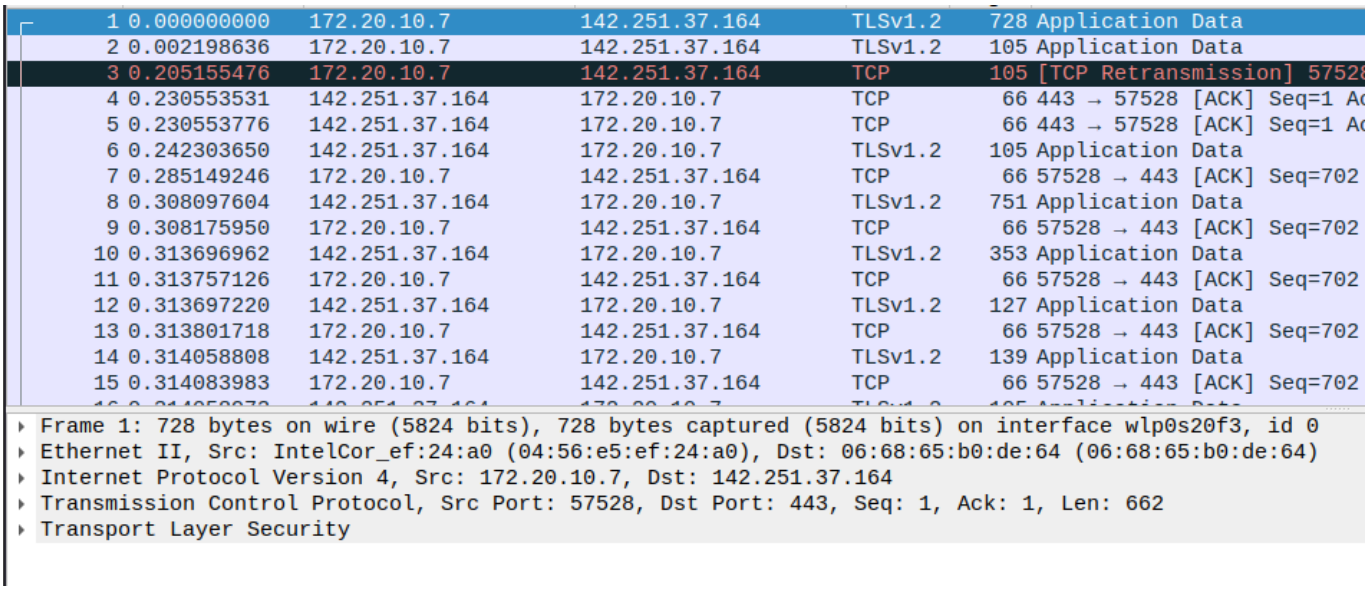
2. **`ethtool`:** Displays current NIC settings.

3. **`ping`:** Verifies connectivity between two IP addresses, utilizing the `ICMP` protocol.

4. **`tcpdump`:** Captures network traffic and saves it for analysis.

Wireshark

We are going to use the wireshark to analyse the data, The layers in the wireshark are ordered from the physical layer up to the application layer



Ping and ICMP Protocol

The `ping` command uses the `ICMP` protocol to check if two machines can communicate. It sends an echo request and listens for an echo reply, verifying connectivity.

Capturing and Analyzing Traffic

For systems without GUI tools like Wireshark, `tcpdump` can capture network traffic. The captured data can be transferred to another system for analysis with Wireshark.

> [!TIP] The wireshark is a gui tool we can't use it with the embedded systems like rasperryPi, so we need to use the tcpdump tool to capture the traffic and save it to file called pcap, then take the pcap file and analyse it on the wireshark

> we will use tcpdump tool to capture the traffic and save it to file called pcap, then take the pcap file and analyse it on the wireshark