Computer Networking Chapter 1 (Layer 3-7)

Garen Ikezian

TCP/IP Protocol Suite

TCP/IP is a protocol that allows communication happen between two networks that spans 3 to 7 levels of the OSI model.

It is protocol suite with a patch of different protocols working together. TCP/IP is named TCP/IP because both TCP and IP are extremely powerful protocols.

TCP/IP consists of:

- Transmission Control Protocol (TCP)
- Internet Protocol (IP),
- User Datagram Protocol (UDP)
- Address Resolution Protocol (ARP),
- Internet Control Message Protocol (ICMP)
- Reverse Address Resolution Protocol (RARP)

And more...

TCP/IP deals with packets and segments, not frames. Although frames are a superset of packets, we distinguish them in order to properly identify their roles with their respective levels.

Important words to remember:

PDU (Protocol data unit): The small data units used to slice chunks into smaller more specialized chunks. Segments, packets, datagram, and frames are all PDU.

Segmentation: The process of dividing or slicing data stream into smaller pieces.

Packets: The PDU of the Internet layer in the TCP/IP model.

Segments: PDU for OSI layer 4 (transport layer) for TCP related tasks.

Datagram: PDU for OSI layer 4 (transport layer) for UDP related tasks.

TCP (Transmission Control Protocol): - A protocol for loading a webpage, exchanging messages, email, and anything else that involves reliability instead of speed. - It uses segmentation before being transmitted. - Unicast uses TCP only.

UDP (User Datagram Protocol): - A protocol for game servers, VoIP (Viber, WhatsApp, Telegram etc.) and other time-sensitive applications. - It does NOT use segmentation before being transmitted. - Multicast and broadcast usually use UDP.

IP: A protocol that defines how to address and route packets for delivery.

Header: The initial position of a packet or that is wrapped to packets by TCP and UDP.

Note: "Datagrams", "packets", and maybe "segments" may all be collectively known as "packets" or used interchangeably. Unless otherwise noted, it is best to be specific.

Layer 3 and 4

Layer 3 (network layer) is the layer where routing takes place. It is where former frames (now called packets), move from one network to another. It forms the basis of the **inter**net.

All about IP (Layer 3)

IP (Internet protocol) is the most important protocol determines how data can be sent to the receiving device. IP lays the foundation or rules for routing:

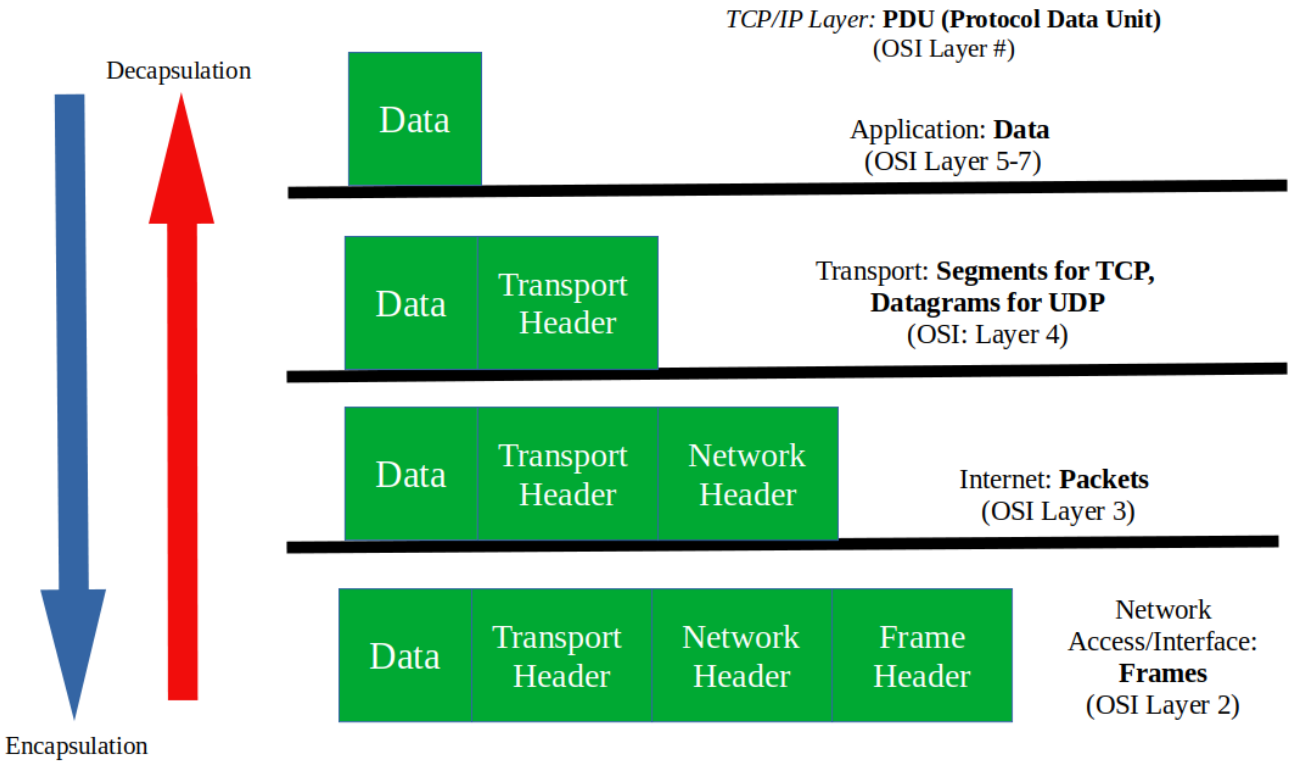

Figure 1: A Basic Layout of Encapsulation of Decapsulation

- It implements the logical aspect of networking. It helps create IP addresses and enable internetwork routing.
- It is a connectionless protocol. IP relies on other protocols for verification and to establish a secure connection.
- IP is responsible to help route packets between different networks. It implements the routing aspect of the network but it does not oversee them. It is only for identification purposes.

IP comes with IP addresses. They sit on top of interfaces on any computer. They are either routers, switches, PCs, etc. as they all connect together to perform the tasks needed for a network to exist.

The most popular devices that belong in layer 3 are routers and switches (not to be confused with layer 2 switches).

IP addresses sit on top of interfaces (like gigabitEthernet0/0/0, fastEthernet0/0/0, etc.) on a router and a switch to make IP reliable.

Explaining IP Addresses

Recall that layer 2 relies on MAC address. Layer 3 however, relies on *IP addresses*.

IP (internet protocol) address: In contrast to MAC addresses that are stored in NICs, they are stored in operating systems. IP addresses identify a device in a local network. It belongs to the level 3 of the OSI model.

The IP addresses uses a dotted decimal notation. There are two popular IP addresses, IPv4 and IPv6. They can all be either public, private, static, or dynamic.

Static IP address: IP addresses that do not change over time.

Dynamic IP address: IP addresses that can be changed over time.

Public/external IP address: IP addresses that are acccessible outside the local network. It is no different to email or home addresses.

Private IP address: Only accessible to hosts that are connected on the same network.

It is based on 8-bits that ranges from 0 to 255 inclusive and have four numbers separated by periods.

Ex (for IPv4):

```
126.115.32.53
```

Ex (for IPv6):

```
2001:db8:3333:4444:5555:6666:7777:8888
```

Like Layer 2 for MAC addresses, there cannot be two systems in a network that share the same IP address.

In a home environment, it is the responsbility of the Internet Service Provider (ISP) to configure dynamic IP addresses automatically through a protocol called DHCP (Dynamic Host Control Protocol). They also provide other parameters like subnet masks and default gateways automatically.

How does TCP or UDP work? (Layer 4)

It is the layer 4 that helps coordinate packets to their destination. It is the "how" for layer 3. There are two protocols with each serving its own purpose.

Networks can either send or receive data abroad with either TCP or UDP. They serve the same purpose but function differently and are both run on top of IP.

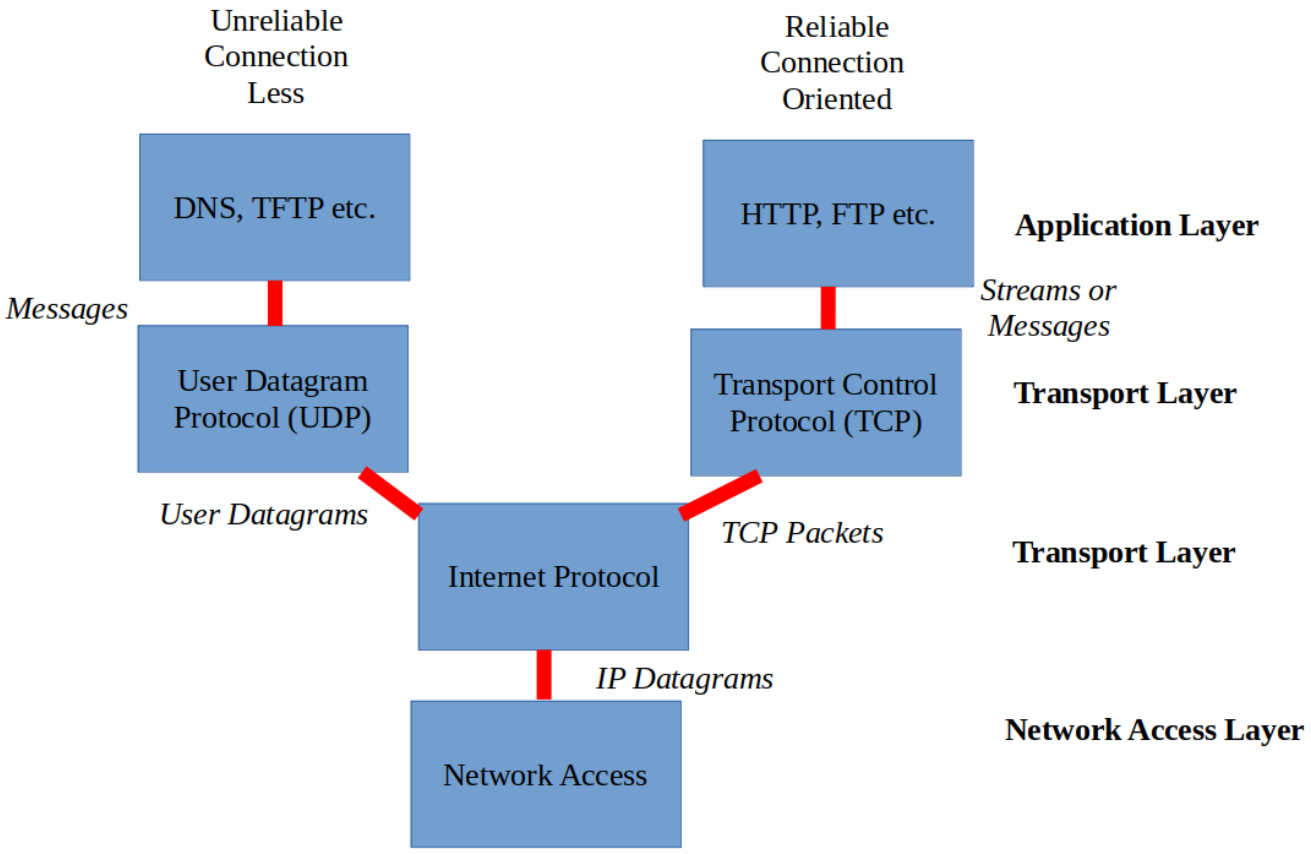

Figure 2: The path of TCP/IP

If TCP is involved:

- It enables host-to-host communication as two computers need to be authenticated before a transmission is made ("three-way handshaking").
  - The sender sends a packet with the SYN bit set to 1.
  - The receiver sends back a packet with both the ACK bit and SYNC bit set to 1.
  - The sender then reacknowledges by replying back a packet with its ACK bit set to 1.

```
Computer 1: "Are you there?" (Synchronizing...)
Computer 2: "Yes, I am here." (Acknowledging AND Synchronizing...)
Computer 1: "Ok, I am here if you need me" (Acknowledging...)
```

- As computers start sending each other data, each TCP/IP layer (*see Figure 1*) will start stripping (*segmentation*) or joining chuncks of data together before they are being sent to the application layer.

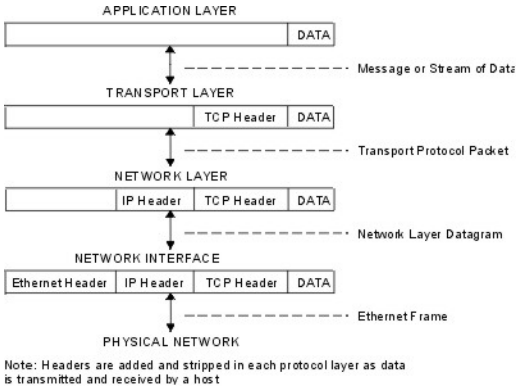

Figure 3: How packets are decapsulated

If the receiver were to transmit data, TCP will slice and wrap each data packet with a header (with all the necessary info) before being sent to the sender.

If UDP is involved,

- The application layer has to strip data on its own before being transmitted.
- Packets will be sent and can be dropped in a different order than they were transmitted.
- They are sent to the receiver directly without authentication (no three-way handshaking).