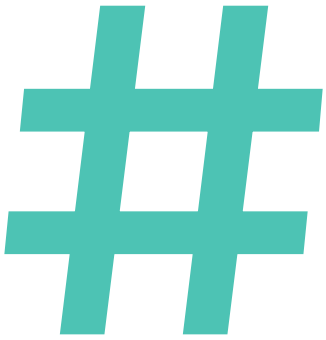


Transmission Control Protocol/Internet Protocol (TCP/IP)

Step 01 What is the TCP/IP Model?

The TCP/IP (Transmission Control Protocol/Internet Protocol) model is a standard similar to the OSI model. It categorizes the network phases and enables application programs to exchange data or messages over a network. The purpose of the TCP/IP model is to establish a reliable connection between devices.TCP/IP models help us understand how data can be transmitted between applications.

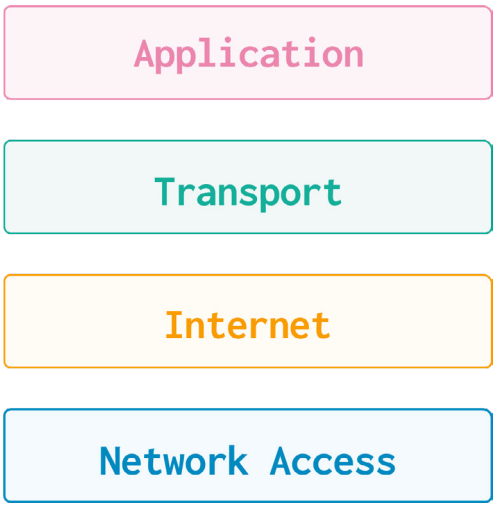
The following are the TCP/IP Model Layers

01 **Application Layer** This layer is responsible for the user interface, it is the layer that the user interacts with.

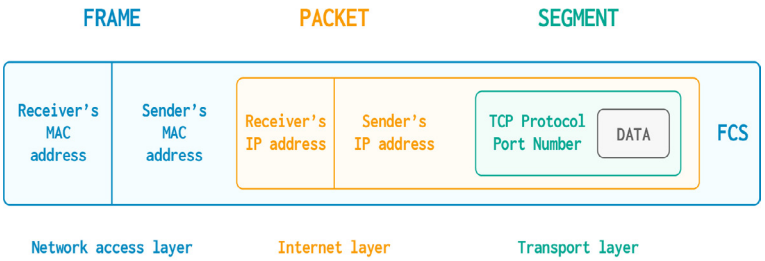
02 **Transport Layer** This layer is responsible for the transmission of data between applications.

03 **Internet Layer** IP address is assigned to the application. The data is sent to the destination.

04 **Network Access Layer** MAC address is assigned to the message.



The packet can be represented with the TCP/IP layer as the following



> **NOTE**
> We can see the packets that have been transferred in our network by using a packet analysis tool as Wireshark.

Step 02 How does TCP Work?

Transmission Control Protocol (TCP) is a core communication protocol used on the Internet. It provides reliable, ordered, and error-checked delivery of data between devices. Here is how TCP works based on the three-way handshake .process you outlined when a connection is established

01 SYN (Synchronize)

The client, let's say a web browser, sends a SYN packet to the server it wants to communicate with. This packet contains a sequence number which helps ensure data packet order.
The SYN packet indicates the start of a new connection request.

02 SYN-ACK (Synchronize-Acknowledgment)

The server receives the SYN packet from the client. It acknowledges the receipt of the SYN packet by sending a SYN-ACK packet back to the client.

The SYN-ACK packet contains an acknowledgment of the client's SYN packet and also includes the server's own SYN packet to initiate a connection with the client.

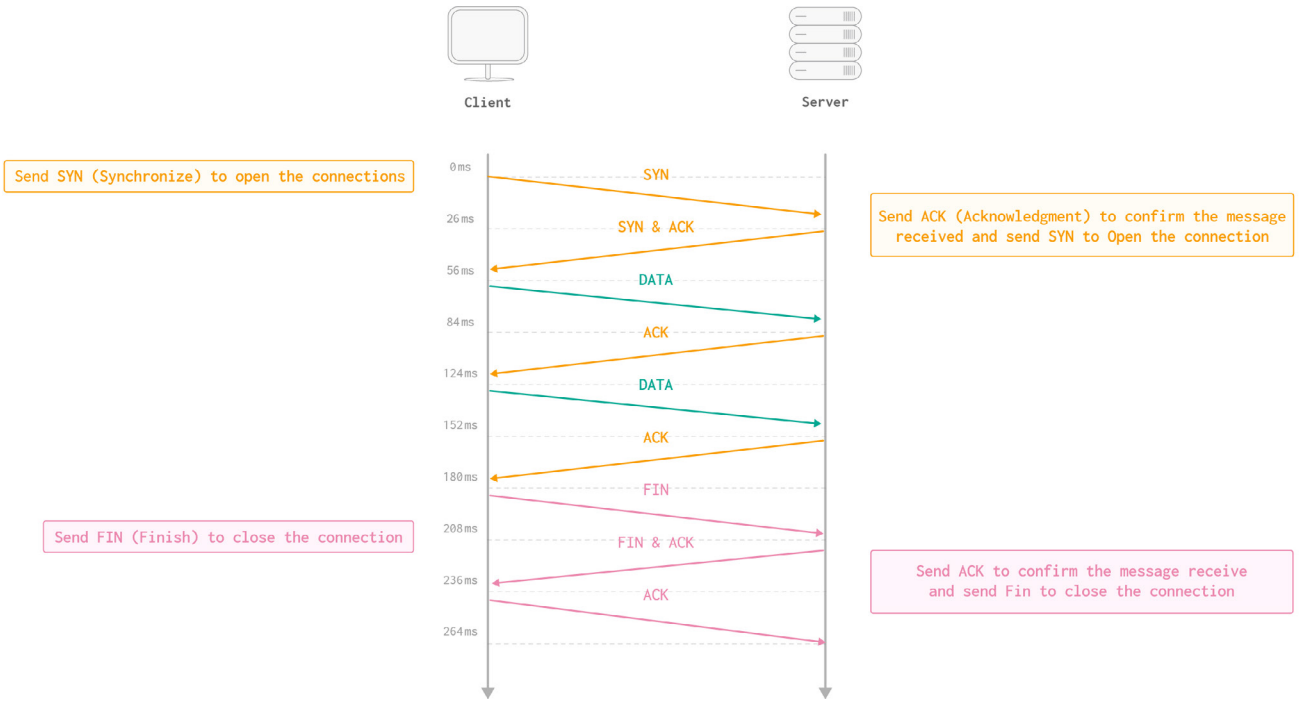
03 ACK (Acknowledgment)

Upon receiving the SYN-ACK packet from the server, the client sends an ACK packet back to the server.

The ACK packet confirms the receipt of the server's SYN-ACK packet. At this point, the TCP connection is established successfully between the client and the server.

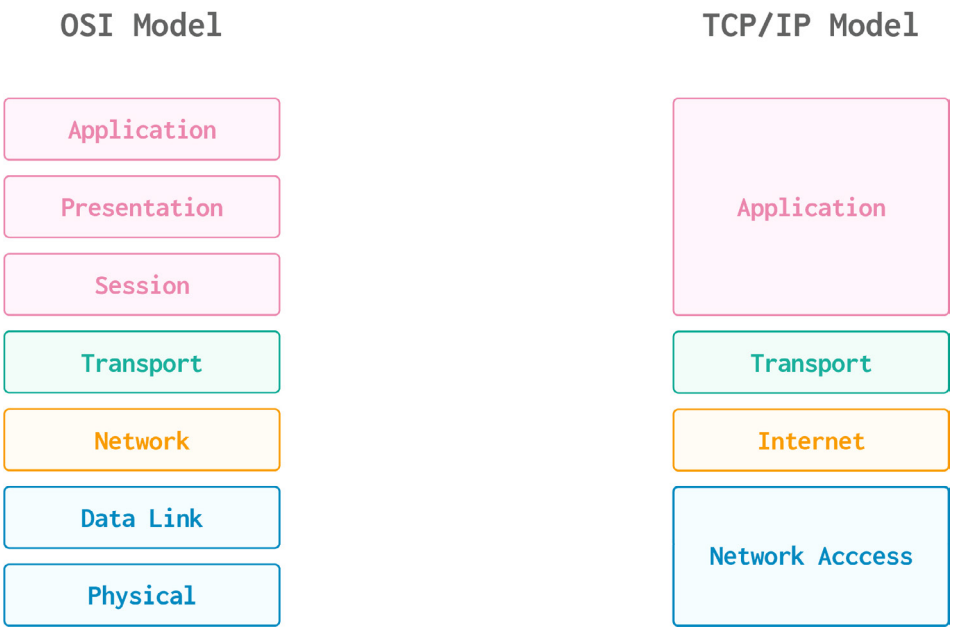
The three-way handshake helps ensure that both the client and server are ready to send and receive data, and it establishes initial sequence numbers for data transmission.

Finally, to end the connection, the client sends FIN(Finish) to close the connection, and the server sends ACK to confirm that it received the request, and sends FIN to close the connection, and the client sends ACK to confirm that it received the request.



Step 03 The Difference Between the OSI Model and TCP/IP Model

Both the TCP/IP model and OSI model help us to understand the data transmitted between applications, however, the TCP/IP model has combined the physical and data link layer into one layer called the Network Access Layer, and the session, presentation, and application layer into one layer called the Application Layer. The OSI model is primarily a theoretical framework forunderstanding networking concepts, while the TCP/IP model is a more practical implementation that is commonly used in networking protocols.

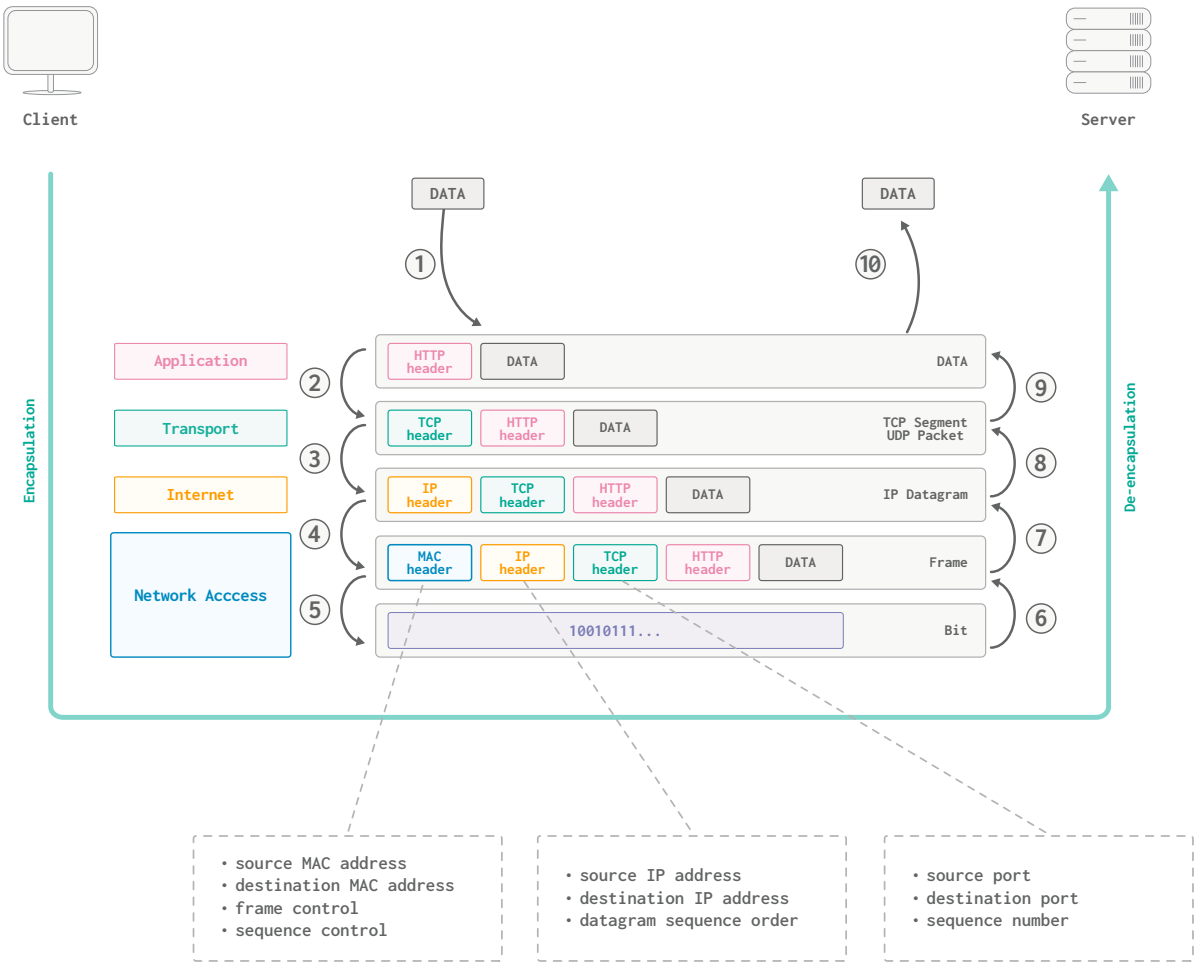


NOTE
comparison between the OSI Model and the TCP/IP Model.

Step 04 What are Encapsulation and Decapsulation?

When sending a message through the network, it should go through the layers to send the message, The TCP/IP layers describes the phases of sending and receiving a message through the network. Each layer has its own specific function, the sender side is called encapsulation in which each layer adds its own header to the message, think about it as putting a message in a box, and each layer adds another box to the previous layer, once all the layers have added their own box, the message is ready to be sent,

while on the receiver side is called decapsulation, in which each layer removes its header and passes the message to the next layer. Also, you can think about it as opening the box, each layer opens the box and passes the message to the next layer until the application receives the message.



Step 05 Network Command Line

There are command line utilities that can be used to get information about the network, such as the IP address, MAC address, and the current applications that are using the network.

01 Get the IP address of your device

- Windows

```
01 | ipconfig
```

- Linux/MacOS

```
01 | ipconfig getifaddr en0
```

> **NOTE**
> This command is used to find the IP address assigned to the network interface named «en0», it shows the IP address of a specific network connection on the system.

02 Test the connectivity of a device

- Windows/Linux/MacOS

```
01 | ping 127.0.0.1
```

> **NOTE**
> Ping is a command line that sends a message to check if the device is connected within the network, The IP address 127.0.0.1 is a special address known as the loopback address which refers to your computer. So when you ping 127.0.0.1, you are essentially pinging your own computer.

03 Get current applications that are using the network

- Linux/MacOS

```
01 | lsof -i -P -n | grep LISTEN
```

> **NOTE**
> •lsof -i: Lists open internet connections.
> •-P: Shows port numbers instead of names.
> •-n: Prevents converting IP addresses to hostnames.
> •| grep LISTEN: Filters the results to show only processes that are listening for incoming connections.

- Windows

```
01    netstat -a -b
```

> **NOTE**
> netstat -a displays a list of all active network connections and listening ports
> netstat -b provides information about active network connections and listening ports, along with the active process that is associated with each connection.

04 Get the current MAC Address of the device

- Windows

```
01    getmac
```

- Linux/MacOS

```
01    ifconfig en0
```

> **NOTE**
> when use this command you can found the mac address next the keyowrd(ether)