**TCP/IP**

|  |  |
| --- | --- |
| Prepared by | Kiran Kumar |
| Reviewed by | Aamod Kumar |

TCP/IP stands for **Transmission Control Protocol/Internet Protocol** and is a suite of communication protocols used to interconnect network devices on the internet.

TCP is important because it **establishes the rules and standard procedures for the way information is communicated over the internet**. It is the foundation for the internet as it currently exists and ensures that data transmission is carried out uniformly, regardless of the location, hardware or software involved.

* The TCP/IP model was developed prior to the OSI model.
* It contains five layers, unlike the seven layers in the OSI model.

The layers are:

1. Application Layer
2. Transport Layer (TCP/UDP)
3. Network/Internet Layer (IP)
4. Data Link Layer (MAC)
5. Physical Layer

**1.Application Layer:**

Application layer is used by the user applications that passes data from one computer to another computer in a network.

EX: 1. Web browser – uses **HTTP and HTTPS –** HTTP stands for Hypertext transfer protocol. It is used by the World Wide Web to manage communications between web browsers and servers. HTTPS stands for HTTP-Secure. It is a combination of HTTP with SSL (Secure Socket Layer). It is efficient in cases where the browser needs to fill out forms, sign in, authenticate, and carry out bank transactions.

2. EMAILS – SMTP (simple mail transfer protocol), FTP (file transfer protocol)

Q. Which layer does authentication in TCP/IP model?

A. The **application layer** helps in managing the network connections. It combines the functionalities of the session layer, the presentation layer, and the application layer of the OSI model.

Q. Which layer will convert data from different format to standard format?

A. The **Application layer** receives the data from the application layer and translates it into a format and syntax that's readable by other computers. For the other systems to recognize this data, it's converted into a generic format that is not application specific.

### 2. Transport Layer:

The TCP/IP transport layer protocols exchange data receipt acknowledgments and retransmit missing packets to ensure that packets arrive in order and without error. End-to-end communication is referred to as such. Transmission Control Protocol (TCP) and User Datagram Protocol are transport layer protocols at this level (UDP).

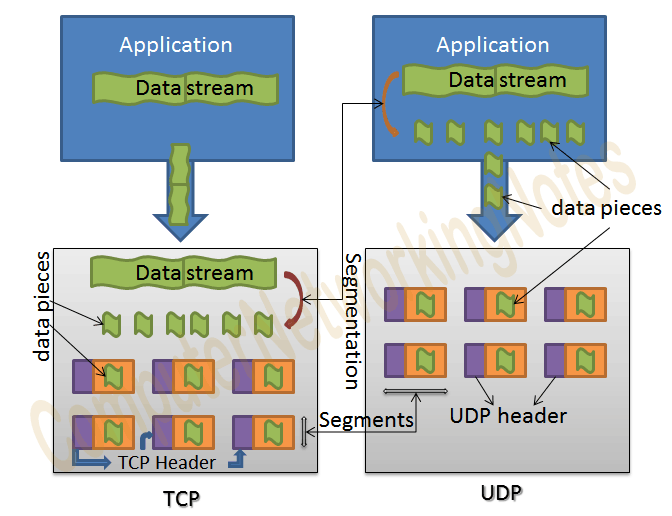
Transport layer performs 3 Operations

* 1. Segmentation
  2. Flow control
  3. Error control

1. Segmentation:

Large data is divided into small groups of data is called Segments.

* Each segment is assigned as a unique number called sequence number in TCP.



Q. UDP segmentation will happen or not?

A. TCP supports segmentation while **UDP does not**. It means if an application wants to use the TCP to send its data, it can give the data to TCP in actual size.

If a applications wants to use UDP then how data will be device in small parts?

1. Flow control:

Managing the flow of data that is transmitted between one computer to another computer.

Example: suppose we can consider system A and system B.

System A can transfer a data to system B at rate of 10 Mbps, but system B can’t receive 10Mbps of data, because system B has a speed of 5 mbps.

So, then system B will ask System A to send data at 5 mbps speed.

Then the sender will send data at 5mbps of speed.

Q. How flow control will happen between A and B

A. The window size field in TCP header specifies the size of the message the system can receive.

1. Error control:

Error control is the technique of detecting and correcting blocks of data during communication. In other words, it checks the reliability of characters both at the bit level and packet level.

Q. How error control will happen between A and B

A. Error control in TCP/IP is done by using the checksum,

**CHECKSUM:** A **checksum** is error checking bits derived from a block of data for the purpose of detecting errors that may have been introduced during its transmission

* Before sending the data, it will perform XOR operation with the data and 1’s complement of that result and add it to the checksum field
* After sending the data the receiver performs same operations and compares it with sender’s checksum.
* If checksum is all 1s then the data is error free or else data will having some errors.
* After data received, the receiver sends acknowledgment to the sender, if data did not receive no acknowledgement will be sent.

**3.Network Layer:**

In network layer, source IP and destination IP are added to the TCP segments or UDP datagrams converts into IP packets.

In network layer mainly have 3 functions.

1. Logical addressing
2. Routing
3. Path determination.
4. Logical addressing:

Here Adding source IP and destination IP to a segment is called Logical addressing.

Every computer in a network has a unique IP address. network layer assigns senders and receivers IP address to each segment to form a IP packet.

IP addresses are assigned to ensure that each data packet can reach correct destination.

Q. How sending station will know about destination IP?

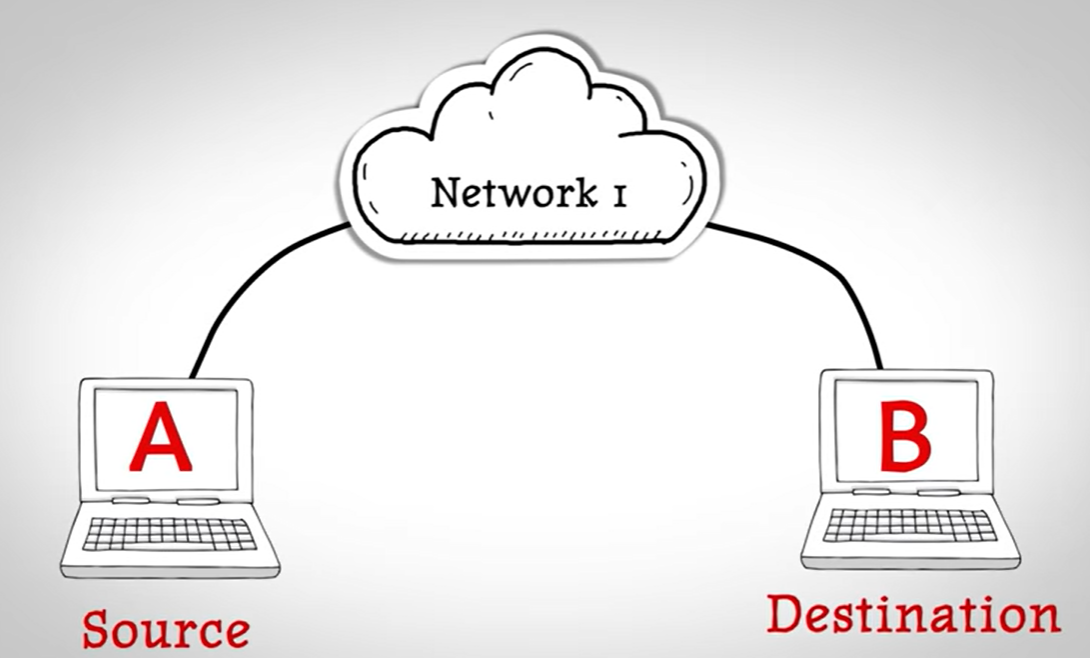
A. By using DNS servers the sending station will know the IP address.

1. Routing:

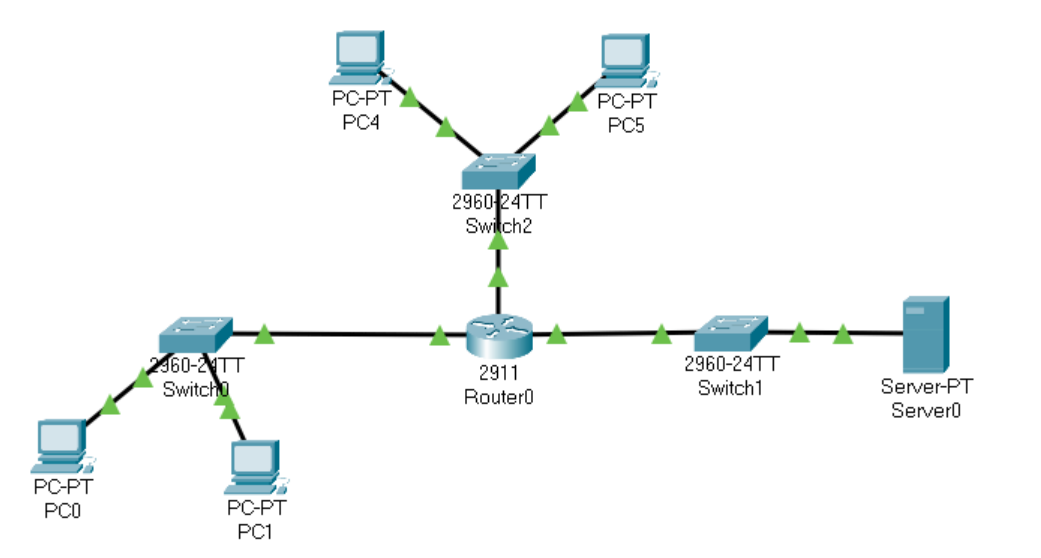
A method of moving data packet from source to destination present in different network.

**WITH IN NETWORK**:

* Routing is not needed if the source and destination computer are present in same network.
* What happens is that ARP module takes the destination IP address from the IP packets return the mac address of the computer.
* ARP module is nothing, but it monitors request and replies and builds a data base of all known mac and IP address and their corelation.



**OUTSIDE NETWORK**:



Consider 2 networks connected with a router. Computer A needs to send data to comp B and both computers are present in different network, hence routing is needed.

We know that to create on ethernet frames we need mac address of destination computer, but in case destination present in a different network, so ARP module cannot provide destinations mac address because it only provides mac address which as present in same network

Since the intermediate to the network is router, the destination mac address is kept as routers mac address and now the frame is forwarded to the router the router finds the mac address in the frame matches its own address.

Then the network layer founds a mismatch for the destination IP address, so it sends the IP packets the destination mac address with the mac address of computer B.

But how router knows the mac address of computer B? simple by the help of ARP module. Since it is within network, ARP module will work. Finally, the ethernet frame is delivered to computer B.

* Destination IP address never changes for inter network communication, but physical address or Mac address changes at every time.

1. Path determination:

A computer can be connected to internet server in a number of ways , choosing the best possible path for data delivering from source to destination is called path determination.

Network layer uses some protocols such as,

* OSPF (open shortest path)
* BGP (Border gateway protocol)
* IS-IS (Intermediate system to intermediate system)

.

### 4.Data Link Layer:

In Data link layer IP packets becomes ethernet Frames after adding source mac address and destination mac address to the IP packets.

In this case TCP/IP, is identified by the data-link layer. Error prevention and “framing” are also provided by the data-link layer. Point-to-Point Protocol (PPP).

It has 2 sublayers

1. **MAC layer (Medium Access Control)**
2. **LLC layer (Logical Link Layer)**

1. **MAC layer:**

In MAC layer we can add source mac address and destination mac address to the IP packets.

1. **LLC layer**:

In LLC layer it does flow control and Error control.

1. **Flow control:**

Managing the flow of data that is transmitted between one computer to another computer.

Example: suppose we can consider system A and system B.

System A can transfer a data to system B at rate of 10 Mbps, but system B can’t receive 10Mbps of data, because system B has a speed of 5mbps.

So, then system B will ask System A to send data at 5 mbps speed.

Then the sender will send data at 5mbps of speed.

The window size field in TCP header specifies the size of the message the system can receive.

1. **Error control:**

Error control is the technique of detecting and correcting blocks of data during communication. In other words, it checks the reliability of characters both at the bit level and packet level.

Error control in TCP/IP is done by using the checksum.

**CHECKSUM:** A **checksum** is error checking bits derived from a block of data for the purpose of detecting errors that may have been introduced during its transmission

* Before sending the data, it will perform XOR operation with the data and 1’s complement of that result and add it to the checksum field
* After sending the data the receiver performs same operations and compares it with sender’s checksum.
* If checksum is all 1s then the data is error free or else data will having some errors.
* After data received, the receiver sends acknowledgment to the sender, if data did not receive no acknowledgement will be sent.

## **Checksum Example-**

Consider the data unit to be transmitted is-

10011001111000100010010010000100

Consider 8-bit checksum is used.

**Step-01:**

At sender side, The given data unit is divided into segments of 8 bits as-



 Now, all the segments are added, and the result is obtained as-

* 10011001 + 11100010 + 00100100 + 10000100 = 1000100011
* Since the result consists of 10 bits, so extra 2 bits are wrapped around.
* 00100011 + 10 = 00100101 (8 bits)
* Now, 1’s complement is taken which is 11011010.
* Thus, checksum value = 11011010

 The data along with the checksum value is transmitted to the receiver.

**Step-03:**

 At receiver side,

* The received data unit is divided into segments of 8 bits.
* All the segments along with the checksum value are added.
* Sum of all segments + Checksum value = 00100101 + 11011010 = 11111111
* Complemented value = 00000000
* Since the result is 0, receiver assumes no error occurred in the data and therefore accepts it.

1. **Physical Layer:**

In Physical layer, Data frames are converted to bits and Signals.

* Ethernet Protocol is used in physical layer.
* These signals will be transformed via different mediums

They are 2 types of mediums:

1. Wired medium
2. Wireless medium

1**.Wired medium:**

In wired medium we can transfer light and electrical signals, like optical fibres and coaxial cables.

2.**Wireless medium:**

In wireless medium we can transfer Radio waves.

***Conclusion:***

| **Layer Number** | **Layer Name** | **Protocol** | **Protocol Data-unit** | **Addressing** |
| --- | --- | --- | --- | --- |
| 5(innermost) | Application | HTTP, SMTP | Messages | n/a |
| 4 | Transport | TCP/UDP | Segments | Ports |
| 3 | Network | IP | Packets | IP Address |
| 2 | Datalink | Ethernet/wi-fi | Frames | MAC Address |
| 1(outermost) | Physical | ethernet | Bits | n/a |

**Difference between TCP and UDP**

| **Basis** | **Transmission control protocol (TCP)** | **User datagram protocol (UDP)** |
| --- | --- | --- |
| **Reliability** | TCP is reliable as it guarantees the delivery of data to the destination router. | The delivery of data to the destination cannot be guaranteed in UDP. |
| **Error checking mechanism** | TCP provides extensive error-checking mechanisms. It is because it provides flow control and acknowledgment of data. | UDP has only the basic error checking mechanism using checksums. |
| **Acknowledgment** | An acknowledgment segment is present. | No acknowledgment segment. |
| **Sequence** | Sequencing of data is a feature of Transmission Control Protocol (TCP). this means that packets arrive in order at the receiver. | There is no sequencing of data in UDP. If the order is required, it has to be managed by the application layer. |
| **Speed** | TCP is comparatively slower than UDP. | UDP is faster, simpler, and more efficient than TCP. |
| **Retransmission** | Retransmission of lost packets is possible in TCP, but not in UDP. | There is no retransmission of lost packets in the User Datagram Protocol (UDP). |
| **Header Length** | TCP has a (20-60) bytes variable length header. | UDP has an 8 bytes fixed-length header. |
| **Handshaking Techniques** | Uses handshakes such as SYN, ACK, SYN-ACK | It’s a connectionless protocol i.e. No handshake |
| **Broadcasting** | TCP doesn’t support Broadcasting. | UDP supports Broadcasting. |
| **Applications** | TCP is used in sending mails, online shopping etc. | UDP is used in live streaming, online gaming etc. |
| **Protocols** | TCP is used by [HTTP, HTTPs](https://www.geeksforgeeks.org/difference-between-http-and-https-2/),[FTP](https://www.geeksforgeeks.org/file-transfer-protocol-ftp/), [SMTP](https://www.geeksforgeeks.org/simple-mail-transfer-protocol-smtp/) and [Telnet](https://www.geeksforgeeks.org/introduction-to-telnet/). | UDP is used by [DNS](https://www.geeksforgeeks.org/details-on-dns/), [DHCP](https://www.geeksforgeeks.org/dynamic-host-configuration-protocol-dhcp/), TFTP, [SNMP](https://www.geeksforgeeks.org/simple-network-management-protocol-snmp/), [RIP](https://www.geeksforgeeks.org/routing-information-protocol-rip/), and [VoIP](https://www.geeksforgeeks.org/voice-over-internet-protocol-voip/). |