# The Process Behind Communication

Hello guys!

So far we all use so many apps like WhatsApp, Snapchat, Twitter, Instagram, etc to communicate with our friends…

But only few knows how actually the message transmission takes place…

No worries this article explain how communication takes place in-detail….

Before going into the concept let me explain u guys some basic terminologies…

In-order to have a communication one should have a connection, so to have a connection physically, We use some devices including Switch, Router, Firewall, Server, and each serves different purpose…

For a better understanding I'm going to make it simple,

**SWITCH:** Usually switch uses MAC Address (a unique address linked with each devices, simply a unique identification for a device) to transmit data packet (small segment or a part of the large data) within a LAN (Local Area Network)

**ROUTER:** A router is also similar to a switch which transmits the data packet but the main difference between the switch and a router is that the router uses an IP address (a unique address which is assigned to a device, the main difference between the Ip-address and target mac address is mac address identifies the device in a local area network whereas the IP address identifies the device globally) and transmit the data over a LAN and WAN (Wide area network).

**FIREWALL:** A firewall is a device which filters the incoming and outgoing traffic, it blocks unauthorised access and malicious content.

**SERVER:** Generally, a server is of many types but commonly a server processes and respond for the request.

Types of servers: DNS server(used for domain name resolution from IP address), web server(whenever users request a services like HTTP and HTTPS then the web server helps in delivering the web content to the user), Database Server( this provide database and storage which helps in web interaction and retrieve the requested data to the user), mail server( used for communication using mails and generally it uses SMTP protocol), proxy server( used for speed deliver the web content ), FTP server(file transmission protocol used to transmits the files from any devices with some login credentials).

Why all these servers?

One should have a clear understanding about the servers, to know how internet actually works...

Whenever a user searches something like (www.xyz.com) over the internet he/she immediately get the response.

How this responds comes? Have you ever questioned?

Don’t worry now I’m going to make it clear..

Generally, when we search a domain name the web site asks the server for the IP address and the IP address of the domain name contains the information. It is difficult to remember the Ip address of every website over the internet,so each website is linked to a name, when we search a name like google.com the DNS server retrieve the IP address of the domain name ,which is stored in its server and gives out the response according to your web search.

So how a website knows to check the DNS server?

Usually web get linked with these server internally using the port numbers, according to our requirements web uses those servers.

Can’t we stop those serveries?

Yes, we can start and stop those services using some simple commands. This is about a DNS server similarly according to the server property remaining servers also works and the servers get linked inbuilt over the internet.

Don’t you guys ever questions why only DNS server? Or any particular server…?how internet knows that which server it should connect?

when we search something in the internet, the data we search is linked with port number (which is the identity of a server), so according to the port number linked with the data, the web access of the particular server for service... this is how the internet take the input and request the service which is already pre-installed in the web and gives out the related output (which is stored in the server storage) for the user.

I think u guys got a clear understating on how actually internet works. But we are not here to know about this so, Let’s dive deeper.

So as we already discussed that we have to connect with the other, in-order to have communication we generally connect in two ways one is wired connection and the other is wireless connection, we use this protocols for communication, UDP(user datagram protocol) and TCP(transmission control protocol) ,Both are used for communication where in TCP is a connection oriented protocol whenever a user need a response then he/she need to connect with server for the response(used in http request, mails, file transfer protocol) where as in UDP where we don’t need to interact directly with the client data is transmitted even if the client don’t receive mostly it is used in fast delivery(used in video streaming, online games, etc…)

Now its time to learn how communications takes places in a network…..!

In-order to understand this we have to know what are the different layers of OSI (Open Systems Interconnection) model and their protocols.

Firstly, what is OSI model?

OSI model is a seven layer model which describes how the data is transmitted from one system to another.

The 7 layers of OSI model are

1. Physical Layer
2. Data link Layer
3. Network Layer
4. Transportation Layer
5. Session Layer
6. Presentation Layer
7. Application Layer

Why this layers?

These layers helps in encryption and decryption.

Whenever a message sends from one device to another then the message go through all these layers two times, one from the receiver side for decryption and one from the sender side for encryption.

Let's see how this layers functions and the protocols in these layers…

Now, initially in-order to send a message, one should use some applications, so these applications are operated in the application layer.

**Application Layer:** where all the applications (Twitter, WhatsApp, Discloed,...)present in this layer. Application layer plays an important role in provide service to the user.

Then the question raises,

How application layer provides services?

As the application layer is already pre-defines with certain port numbers,

How it works?

According to the user request, the layer analysis and send the user request it to the transport layer. The protocol part in the URL (HTTP, HTTPS, FTP, SMTP) determines the which type of service the user request. These protocol is already linked with the port number (Port number is added in the transport layer ( transport header)), the transport layer responds with the port number and send it to the application layer. Then, the application layer responds with the user request.

**Presentation Layer:** In-order to prove secured communication data need to get encrypted which is done in this layer. Whenever the data is entered it should be encoded to the machine readable format (ASCIII, jpeg, etc…)With the help of the presentation layer the data get encoded accordingly for transmission. Now this data need to be encrypted so that it can only readable by the receiver. After that receiver get the data it get decoded in this layer with the same secret key (it is used to encrypt the data, only with the same secret key it get decrypted ). This is how it provides encryption and decryption for secure communication

**Session Layer:** Here, the session or a link between the two computers or a devices are established, simply build a connection (RPC {Remote Procedure Call Protocol}, PAP {password authentication protocol}) this layer establish a connection, authenticates the users and terminate the connection.

In-order to establish a session it uses session ID (which is a unique identification of the two/ more devices for establishing a connection and also helps in syncing the audio and video stream in order to maintain data integrity). Let's see how this session establishes and maintained.

Whenever a user wants to communicate, then he/she initiate the connection with a session request with a session id, it get stored in the server, whenever a client with proper session id request for the session, after proper authentication and authorisation(note: only with the proper session id, the session is established) session is created after accepting the request through a handshake process and maintained properly without any breakdown miscommunication ( this will maintained with the help of session id) and then this layer is also responsible for proper termination of the session, after it is complete . The session id is unique once the session id is used it cannot be used again if it get expired.

How u know the message delivers successfully?

So to know this,

**Transportation Layer:** The transport layer helps us in successful delivery, error control, using TCP and UDP protocols.

As we unable to send whole data at once, so to send the data, Generally we partition the data, The transport layer responsible for partitioning into segments. There may be chance of clumsiness in the data transfer as the data got divided, so for reliable delivery the data is linked together using a sequence number.in-order to provide error free and ensure flow control.

Now data got divided into segments(the size of the segment is based on the network capacity of transmission), these segments got added with a transport header, transport header contains the port number which helps in requesting the server for services over the internet. According to the application layer request, the transport layer add port number in the header part based on the protocol used (HTTP:80, HTTPS:443, FTP:21, SMTP:25…).transport layer contains pre-defined ports.

How a TCP connection establishes?

First the client sends SYN(synchronization) message to the server to start a connection.

Now the server responds with SYN-ACK(Synchronization-Acknowledgement) message which contains initial sequence number(ISN)(which is generated randomly)

Now the client sends ACK message which indicates the message is received.

How sequence number is added?

Lets assume that the first ISN from client is x and the first is from sever is y.

At the first SYN message is sends x and the server responds with x+1 indicates successful delivery, after receiving the acknowledgment, client responds with y+1.

This is the first segment the next segment contains the sequence number as x+ (size of first segment). If there is a failure in transmission(if there is no acknowledgment from server), then according to the sequence number the client retransmit the data segment. This is how it provide successful delivery.

**Network Layer :** Here the segments again sub divide into packets and add some more information called network header, which contains the logical address (Ip address).This IP address helps in routing the packets to the correct network. This layer helps in routing the packet s to the correct destination and helps in providing the best route/ path .Usually routers are operated in this layer.

How?

Whenever a device with a destination IP address send a packet, then it reaches to the available router. The router contains a routing table (contains information about the all available routers, networks address, best paths information). Now the router analyse the packet which contain the destination IP address. On the basis of the longest prefix of the destination address router determine whether the packet need to send to the next router or to the destination network.

With the help of ARP (Address resolution protocol) router finds the mac address of the destination device.

**ARP Protocol :** here the router with the destination IP address sends a request for mac address to all the available devices in the network, the device with the same destination IP address responds with the mac address of the destination device), this helps in trouble shooing IP address conflicts and helps in successful delivery to the correct device.

**Data Link Layer:** Now the packets again subdivide into flames, here the data header is added, what a data header contain?

A data header consists of mac address, which is used to identify the device, u guys already know how the mac and Ip address are differ from. This also helps in error free data transfer. Generally switches are operate in this layer.

I think you guys have a doubt how the data link layer knows the correct destination mac address?

To find the correct mac address off the destination, this layer take the help of layer 3, with the help of ARP protocol data link layer finds the correct mac address of the destination device.

Then what is the role of a switch?

Switch contain mac address table (which contains information about switch port and the mac address) when the switch receives the data frame, the frame contain the mac address of the source and destination along with this the switch records the port number of the source mac address in the table. Now any frame with the same mac address is received to the switch then it forward through the port to the destination address. If no data about the port and destination is available in the table, then switch send the frames to all connected ports and the device with the same destination address responds and then the port is recorded. Also if any unused port are available then the switch avoid those port and Remove its data from the mac address table in-order to maintain only active ports.

**Physical Layer:** Finally the frames from the DLL layer is transmitted in the form of bits (0's and 1's). We cannot send the data directly, so the data finally got converted in the form of binary format.

Why only binary format?

All the computers are capable of receiving data in only two form (on/off). So 1 is used as high voltage and 0 is as low voltage in electrical signals and in optical, 1 is a light pulse and 0 is no light pulse and in wireless, 1 as high amplitude radio wave and 0 as low amplitude radio wave or perfect transmission we use amplification, noise filtration in-order to transmit data error free and ensure successful delivery without any loss of data.

What's next?

Now the bits will transfer through either in wired medium or wireless medium to the other system. On the receiver side the signals get demodulated (converting signals into binary format). Now this data is send to signal processing ( validates, error detection) we use various techniques to validate the bits (parity bits, checksums, cyclic redundancy check) of any error occurs then the system request for the data again if not it get validated. In Wi-Fi, we check signal-to-noise ratio and in physical medium, we use CRC if the CRC value of the receiver and the sender matches then the data is valid.

What about the data received?

1. After the data signals converted into binary bits in the in the physical layer.
2. Those bits are sent to the data link layer, as already said here the data get validated and error check is done over here. And validate the mac address as the data is reached to the correct device.one its verified then it sent to network layer
3. At the network layer, it is responsible for routing, here its checks for the network address and verify weather the data is reached to correct destination network. Now it is sent to transport layer.
4. Here the segments are reassembled into correct order and check for errors of any error occurred it ask for retransmission of lost segments. And then sent to session layer.
5. Here after accepting the session request by handshake process from the sender, the session establishment, processing, and termination takes place and send it to presentation layer.
6. Hare the data translation takes place to make it understandable, here only the decryption of data takes place.
7. This layer where the user interacts and get the response according to the user request.
8. This is the total process behind the successful communication.

So far u guys understood how internally the massages got transmitted from one device to another device for better understanding.

Let's take a real world example:

Before going into the example u guys need to know about two types of communication models which are peer-to-peer model and client-server-mode.

Bother are used in communication but different purpose.

In peer-to-peer mode, there is no any centralized server and both the users directly communicate with each other(it is used in video calling, VOIP) where as in the client-server model the client request the service from the server to get the desired response(mostly used in

web search, cloud services, video streaming by YouTube, Netflix.)

Now let's understand the how communication takes place with a real world example:

For example let us consider WhatsApp,

To have a successful communication it is necessary for the devices to connect to the server.

When user1 sends a message to user2 who is far away.

1. Application layer as u guys already know that the data the applications like WhatsApp are operated over this layer. As WhatsApp use end-to-end encryption which is a signal protocol.

2. end-to-end encryption?
   Message is encrypted at the sender side with a sender's public key itself before transmitting, and only decrypted at the receiver side using receiver's private key. So that, no person in between cannot able to read the message content even if it is available).

   WhatsApp uses XMPP protocol (extensible messaging and presence protocol which is used for chatting, video calls).

Over the presentation layer which is inside the WhatsApp application itself the message which is entered, it may contains any files, images, videos and all so to have fast delivery the data here is compressed and over this layer the data get encrypted using AES( advanced encryption standard).

Do whatsApp creates different keys for every connection?

No, the keys remain same for every communication. Whenever a connection is established these keys are exchanged between the two uses via server, so we use RSA or ECDSA algorithms for key generation, exchange and authentication.

3. Now the message need transmission, over the transport layer where the routers exits. Here the messages from our device is transmitted to the router in the form of radio signals. After receiving the signals. Router analyze the data with the destination IP address if it is in the same network then it is send the data to the switch or itself, the mac address of the destination device is analyzed and then it send to the correct location or else, if the destination address is not in the same network then it sends to the ISP (internet service provider)
4. Now the ISP is a gateway which sends the data to various networks until it reaches the destination router.
5. Once the data/packet reaches the destination router ( we use so many protocols like OSPF, RIP, BGP, for fast delivery by getting best path)before going to the destination device it undergoes through security authentication for malicious content with the help of firewall.
6. Now the data packets reaches the WhatsApp server until the receiver comes online it get stored here and then when the receiver is online it creates the session and transmit the data.
7. Finally the data is received by the user2(receiver)

Here the whole data is transmitted in the form of bits (binary information) or the data, now a days we use optical fibres as a mode of transmission which provide a very fast delivery in terms of milliseconds.

Then what about the voice and video calls!

How communication takes place in a voice and video call?

In Unified Process of communication whether it is a text or a normal call or a video call the process behind is same. Everything is transmitted in the form of binary data.

So when a user send messages to another person the message got transmitted with in seconds, The technology has been improved a lot in providing fast services. This is the whole process behind data transmission.

I think u guys got a very clear understanding on background process of communication!

Written by,

K. Satyanarayana

Contact number : 7702479107