International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi : https://doi.org/10.32628/CSEIT206420

TCP/IP Protocol Suite

Ashima Tyagi
Master of Computer Applications (MCA), Jagan Institute of Management Studies, New Delhi, India

Article Info
Volume 6, Issue 4
Page Number: 59-71
Publication Issue :
July-August-2020

Article History
Accepted : 10 July 2020
Published : 15 July 2020

ABSTRACT

TCP/IP has become an undeniable leader in the areas of Information Technology. It is a well-established fact that data transfer between devices occur by the rules defined by the TCP/IP protocol. Each layer of TCP/IP model generally has more than one protocol for carrying out the functions that the layer complies to. TCP/IP model is used widely and it is essential to understand how different protocols work to provide different functionalities. In this article, through the deep consideration of TCP/IP protocol the understanding of the protocols at five layers of TCP/IP is specified.

Keywords : Internet Protocol, OSI Model, Transmission Control Protocol

I. INTRODUCTION

With the outbreak of Internet, the protocol that is chosen widely is the Internet Protocol with the apprehension of Transmission Control Protocol/Internet Protocol (TCP/IP). Communication taking place amid networks by virtue of Internet occurs with the help of TCP/IP suite between two devices/hosts or entities. Entity is anything that sends or receives some information. Entities cannot just send the information to each other rather the sender and receiver has to agree on a protocol. The communication is governed by some set of rules called protocol i.e. it describes the communication in terms of what, how and when. Protocol Suite refers to the collection of protocols on all the layers.

The TCP/IP model has various protocols on its five layers. These protocols define the way the information flow from layer to layer. The protocols are explained along with the adaptability of the TCP/IP model.

II. PHYSICAL LAYER PROTOCOLS

Physical Layer is responsible for the representation of data into bits, synchronization of data, the data rate and it also defines the transmission medium and the transmission modes. The protocols defined in the physical layer are:

A. Ethernet

Ethernet is a LAN technology that is used to connect the systems to form a LAN with the help of protocols to control the passing of information and to avoid collision. There are 4 generation of Ethernet mentioned in the figure 1.

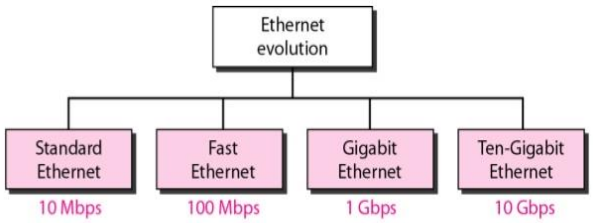

Figure 1 : Generations of Ethernet

The Standard Ethernet uses digital signaling that is baseband transmission at 10Mbps. The first implementation is 10Base5 or Thick Ethernet that uses the bus topology and coaxial cable with a length of 500m. The second is 10Base2 or Thin Ethernet which uses the bus topology having coaxial cable with a length of 185m and the cable is more flexible, thinner and less expensive. The t implementation is 10Base-T that uses the star topology and twisted pair cable with a length of 100m. The coaxial cable is replaced by hub to remove collision. The fourth and the last implementation is 10Base-F that connects devices to hub using star topology. Fiber optic cable is used with a length of 100m.

The Fast Ethernet transmits at a rate of 100Mbps which is 10 times faster. It has three implementations. First is 100Base-TX that uses two pairs of unshielded twisted pair cable of 100m. Second is 100Base-FX that uses two wires of fiber optic cable of 100m. Third is 100Base-T4 that uses 4 wires of unshielded twisted pair cable of 100m.

The Gigabit Ethernet transmits data at a rate of 1000Mbps or 1Gbps. There are four implementations of Gigabit Ethernet. The first is 1000Base-SX that uses 2 wires of short-wave fiber of length 550m. The second is 1000Base-LX that uses 2 wires of long wave fiber of length 5000m. The third one is 1000Base-CX that uses 2 wires of shielded twisted pair cable of length 25m. The last is 1000Base-T that uses 4 wires of short-wave fiber of length 100m.

The Ten-Gigabit Ethernet transmits that data at a rate of 10Gbps. Cable can be used for long distances. 10GBase-S uses short wave fiber of length 300m. 10Base-L uses long wave fiber of length 10km. 10Gbase-E uses extender fiber of length 40km.

B. Bluetooth

A LAN technology that is created to connect different devices like mobile phones, tablets, computers, laptops, cameras, telephones and so on is known as Bluetooth. With the help of Bluetooth different devices or gadgets can share data by forming a network. Two types of networks are there in Bluetooth: piconet and scatternet. Piconet is a small network that can have up to 8 stations in which one is primary station and other seven stations are secondary. Scatternet is formed by combining several piconets where secondary station of a piconet can become the primary station of another. This station receives data from first piconet and transmits data to another piconet.

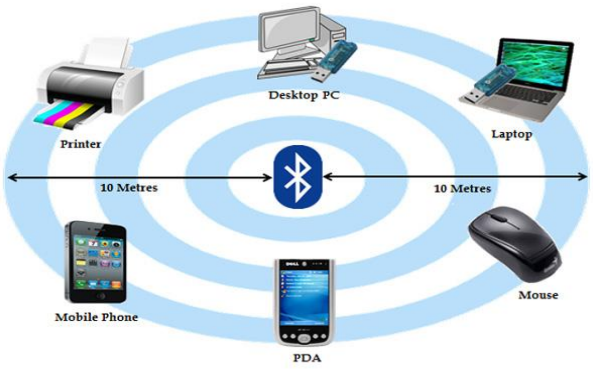

Figure 2 : Bluetooth

C. Digital Subscriber Line

DSL technology is used to provide higher-speed Internet access over the local loops. DSL uses higher frequency band for transmission of data so that data transmission occurs simultaneously with voice

transmission. The question is how both telephone and internet facility can be achieved, then the answer is by using splitters or filters which splits the frequency and make sure they can't get interrupted. Multiple users can be connected by Digital Subscriber Line Access Multiplexer (DSLAM) that is used by the telephone company at its end office.

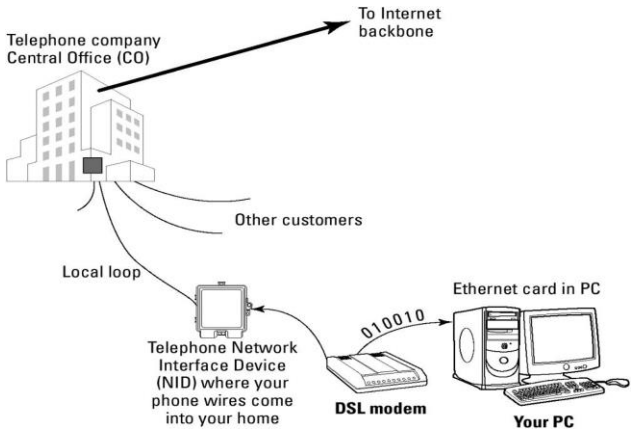

Figure 3 : Working of DSL technology

There are four variations of DSL.

Asymmetric digital subscriber line (ADSL) provides data rate at a higher speed in the downstream direction(13.4Mbps) as compared to the data rate in upstream direction(1.44Mbps).

SDSL or symmetric digital subscriber line provides symmetric communication with the data rate up to 768kbps in each direction.

HDSL or high-bit-rate digital subscriber line provides date rate of 1.5-2.0Mbps in upstream and downstream directions.

Very high-bit-rate digital subscriber line (VDSL) is used for short distances and provides upstream data rate of 3.2Mbps and downstream data rate of 25-55Mbps.

D. Universal Serial Bus

USB is an interface for fast transmission of data by connecting various peripherals to computers. These interfaces are available on personal computers and laptops, to peripheral devices, mobile phones, cameras, hard-drives and so on.

Figure 4 : USB cable and port

III. DATA LINK LAYER PROTOCOLS

The Link layer breaks the stream of bits into frames and provides physical addressing. It is responsible for flow control and error control by adding a trailer to the frames along with the header. The protocols defined under this layer are described below.

A. Noiseless Channel Protocols

Noiseless channels are the error-free channels where no frames are lost, duplicated or corrupted. So, error control is not there. Noiseless channel consists of two protocols.

Simplest Protocol

The simplest protocol provides neither flow control nor error control and it's a unidirectional protocol that means data travels only in one direction that is from sender to the receiver. There is no flow control that means the receiver can hold any number of frames with a very small processing time.

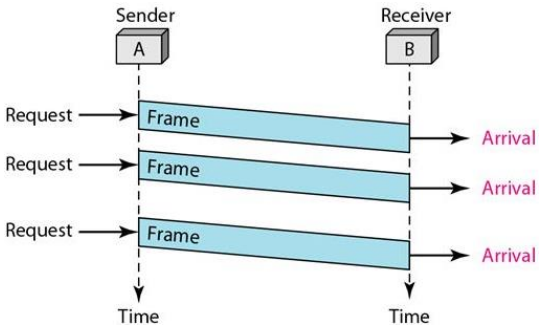

Figure 5 : Working of Simplest Protocol.

Stop-and-Wait Protocol

Generally, the receiver does not have enough storage to handle large number of data frames from different sources and hence it may lead to discarding of frames. So, there is a feedback mechanism called 'Acknowledgement' that is sent by the receiver to the sender in order to tell the sender to slow down. This mechanism is called as flow control where sender sends the next frame only after it receives acknowledgement from the receiver. Unidirectional communication is there for data frames but acknowledgement frames travel from the other direction.

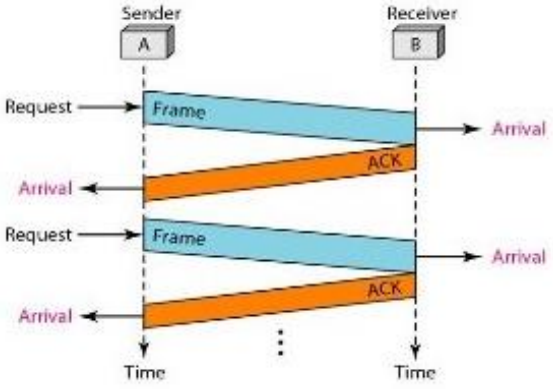

Figure 6 : Working of Stop and Wait protocol

B. Noisy Channel Protocols

Noisy channels are the error-creating channels where the frames can be lost, duplicated and corrupted. So, error control and flow control both are added in these protocols. There are 3 protocols for noisy channels: Stop-and-Wait ARQ, Go-back-n ARQ and Selective Repeat.

Stop-and-Wait ARQ Protocol

Error control mechanism to the Stop-and-Wait Protocol is added by this protocol. Detection of errors is done by adding redundancy bits to the frame and if the receiver finds that the data is corrupted then the frame is discarded. Lost frames or duplicated frames ae handled by adding numbers to the frames. Sequence numbers are used to number the frames that start from 0 to 2^m-1 (if the field is m bits long). When the frames are received out of order then they are lost or duplicated and hence they are discarded. Errors are corrected by keeping a replica of the sent frame and transmittal of the frame again when the timer expires. The flow control is established into this protocol by adding acknowledgement numbers that declare the number of next frame that the receiver expects.

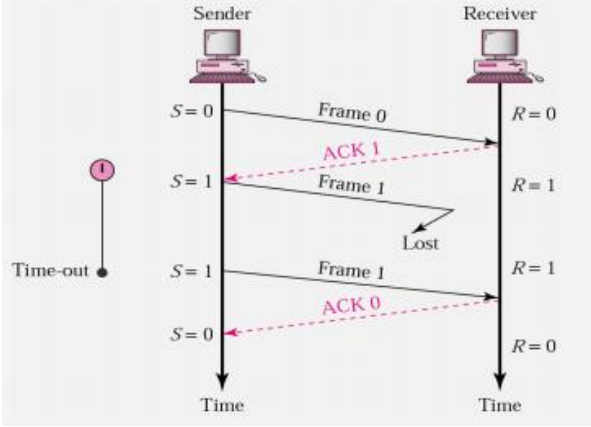

Figure 7: Working of Stop and Wait ARQ protocol

Go-Back-N ARQ Protocol

Go-Back-N Automatic Repeat Request works on the concept of pipelining which states that the sender can send several frames before the acknowledgement arrives for previous frames rather than waiting for the acknowledgements before the next frame can be sent. This protocol uses sequence numbers ranging from 0 to 2^m-1 where m is the size (in bits) of the sequence number field. The sliding window describes

the length of the sequence numbers that will be handled by sender and receiver. For instance, when m=4 then frames with sequence numbers 0 to 15 will be included in the sliding window. The sender's sliding window size is 2^m-1 and the receiver's sliding window size is 1 that is the only frame the receiver is expecting to receive. The acknowledgement in go-back-n is cumulative which signifies that an ACK frame can acknowledge more than one frame. In this protocol, the receiver keeps track of only 1 variable and does not buffer out of order segments. When the receiver receives out of order frames then receiver sends no ACK frame and then sender goes back to n (the starting frame of sliding window) and then sends all the frames again. A special case of Go-Back-N ARQ is stop and wait ARQ where the send window size is 1.

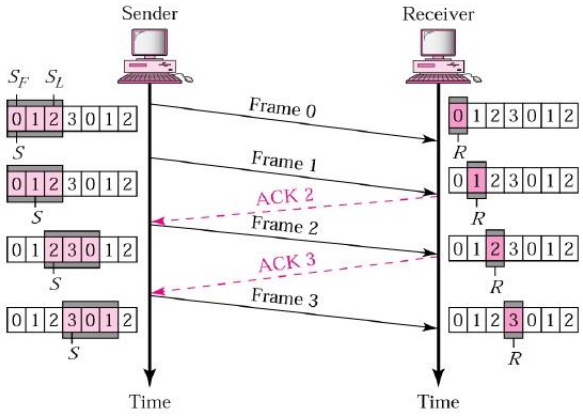

Figure 8 : Working of Go-back-n ARQ protocol

i. Selective Repeat ARQ Protocol

In Selective Repeat Automatic Repeat Request protocol, only the damaged or lost frame is resent rather than sending N frames because resending n frames needs the bandwidth that delays the transmission. The sliding window size ranges from 0 to 2^{m-1}, for example, if m is 4 then frames with sequence numbers from 0 to 7 will be included in the sliding window. The send window size and receiving window size is same that is 2^{m-1}. Here the concept of negative acknowledgement NAK comes into play. Instead of sending the ACK frame for lost or corrupted frame, a NAK frame is sent for that damaged frame and when the valid NAK arrives the sender just resends the corresponding frame rather than resending all the N frames.

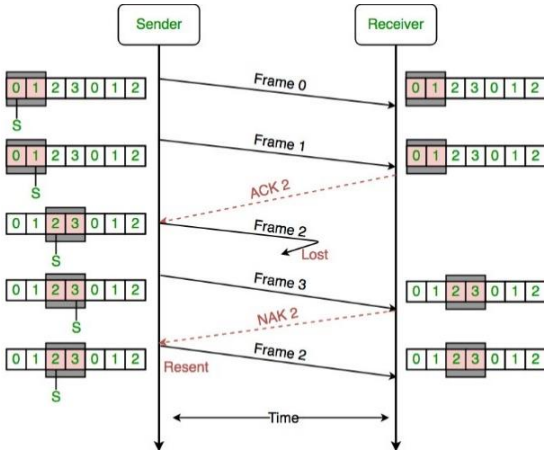

Figure 9 : Working of Selective Repeat ARQ protocol

C. Random Access Protocols

In the above-mentioned protocols, there is a dedicated channel between the sender and a receiver. But in the random-access protocols there is no dedicated link. Two stations might be using the same link for data transmission that may lead to a conflict or collision and thus the frames will be destroyed. Let us discuss some random-access protocols.

ALOHA

It is the earliest random-access method also called Pure ALOHA in which when two stations want to send data simultaneously then there will be a collision and the data might be destroyed. The pure ALOHA works on acknowledgements from the receiver. If the acknowledgement doesn't arrive after the time-out cycle, then the sending station considers that the frame has been collided and sends the frame again.

CSMA

Carrier Sense Multiple Access (CSMA) protocol was made to reduce the collision. The station senses the

medium before sending a frame i.e. "sense before transmit". CSMA decreases the chances of collision but can't eradicate it due to delay in propagation. The sending station after sending a frame, takes time for the first bit to reach each station. In other words, when a station senses the channel and finds it idle that is due to the fact that first bit sent by other station is not received yet. There are three persistence methods which tells what the station should do if the channel is busy or idle.

1-Persistent method states that the station continuously senses the channel and when the medium is idle then it immediately sends frame with a probability of 1. 1-Persistent has the maximum chances of collision as many stations can find the channel idle and send the frame.

Non-Persistent method states that when the station finds the link idle while sensing then it immediately sends the message but if the link is not idle or busy then the station waits for arbitrary amount of time and again starts sensing. This approach decreases the chances of collision as it is rare that more than two stations will wait for the same amount of time.

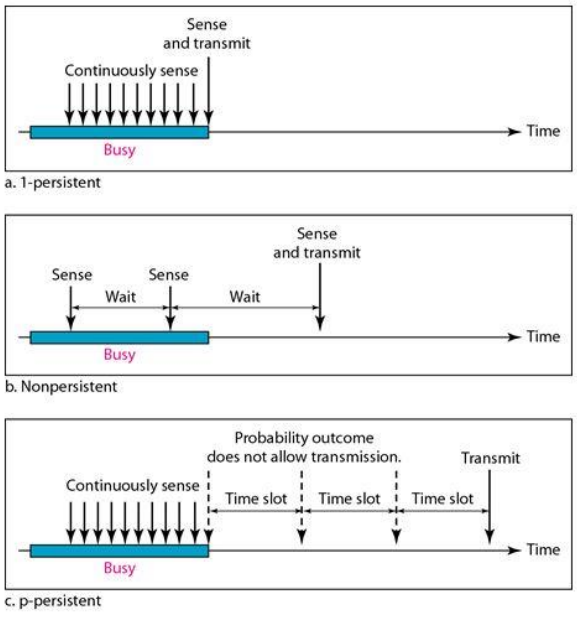

Figure 10 : Working of CSMA protocol.

p-Persistent is a method that diminishes the chances of collision and enhances efficiency. Whenever any station finds idle channel, it proceeds with some steps: first, it sends the frame with a probability p. With a probability q=1-p, the station waits for a random time for the starting of the next time slot and tests the channel again, then if an idle channel is found it does the first step and if busy channel is found, it behaves as collision has happened and thus utilizes the back-off strategy.

CSMA-CD

Carrier Sense Multiple Access-Collision Detection protocol (CSMA-CD) detects the collision in the transmission. In this protocol, the station checks the channel after sending a frame to check whether the transfer succeeded and if there is a collision then the frame is resent. The bits of every frame are sent until a collision is detected.

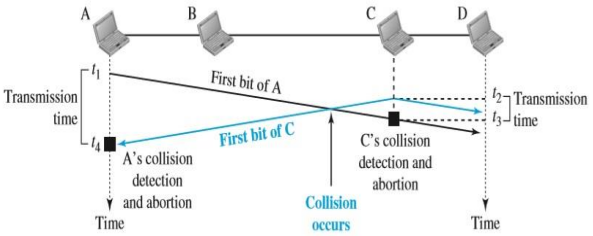

Figure 11 : Working of CSMA-CD protocol

In the above figure, the station C sends a frame at time t2 when A has already sent the frame at time t1 because C hasn't yet sensed the first bit of A and thus finds the channel idle. Collision happens after time t2, collision is detected by C, at time t3 and immediately aborts the transmission. At t4, A senses the collision, and as soon as the first bits of C reaches A, it also terminates the transmission.

CSMA-CA

Carrier Sense Multiple Access- Collision Avoidance protocol is used to avoiding collisions on wireless systems because they can't be detected. Three strategies are used to avoid collisions. First, whenever an idle link is found by the station, it doesn't send a

frame immediately but waits for a time period known as interframe space or IFS because the channel may turn out to be idle but another station may already has started transmitting.

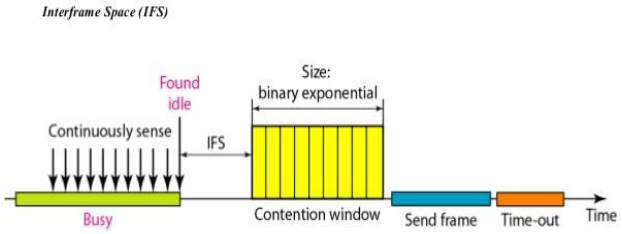

Figure 12 : Working of CSMA-CA protocol

Now, after interframe space time, if channel is still idle, station again waits for a time same as the contention time i.e. the time described by the contention window. The contention window is a time that is broken down in slots. The slots are changed in the window according to the binary exponential strategy. A station that is ready to send chooses a random number as its wait time. At first, time is set to one slot and then become twice each time the station is unable to uncover an idle channel after IFS time. However, if busy channel is there then the sender doesn't start the contention time again but starts the timer and restarts it as soon as channel is idle.

IV. NETWORK LAYER PROTOCOLS

The need of network layer arises when two systems are connected to two different networks. Network Layer accomplishes source to destination delivery and is responsible for logical addressing and routing. The protocols of the network layer are described below.

A. ARP

Address Resolution Protocol is developed to map the logical address to physical address. The host or the router has logical address of another host whenever it wants to send some data. To pass the message through the physical network the IP datagram must be contained in a frame, hence the receiver's physical address is required by the sender. So, to know the physical address the sender sends an ARP request message that is broadcasted and the expected recipient determines its logical address and sends an ARP reply that is a unicast message.

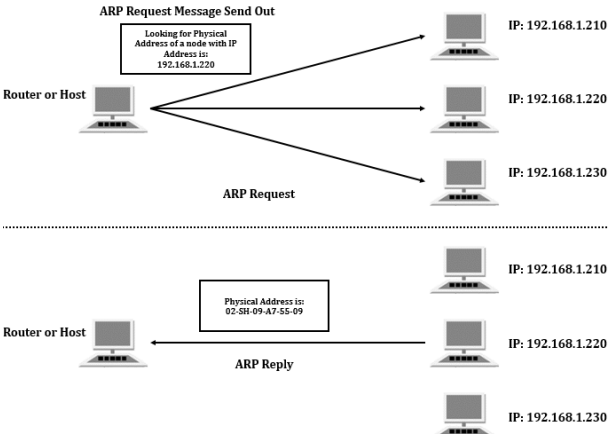

Figure 13: ARP request and ARP reply

B. RARP

Reverse Address Resolution Protocol finds the logical (IP) address of the machine that knows it physical address only. The device can know its physical address from the Network Interface card (NIC card). The logical address of the machine can be known from the configuration file stored on a disk file but a diskless machine there is no IP address information. So, the physical address is used to determine the logical address by employing RARP packets. An RARP request message is broadcasted on the local network and the RARP reply sent by another machine is unicasted.

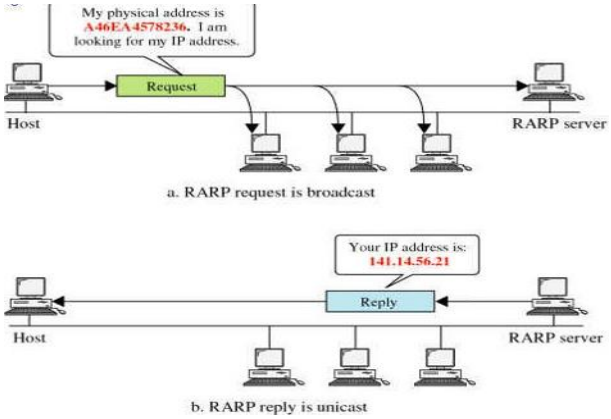

Figure 14 : RARP request and RARP reply

The limitation of RARP is that the broadcast message (all 1s) does not pass the boundaries of a network and thus there is a need to assign an RARP server for each network. BOOTP and DHCP replaced RARP protocol.

C. BOOTP

The Bootstrap Protocol finds the logical address of a machine. When the client and the server are on the same network then the BOOTP client sends a broadcast message and receives a unicast reply with a logical address from the BOOTP server. But when they are on different networks one of the hosts is used as a **relay agent** because any router cannot pass a broadcast IP datagram.

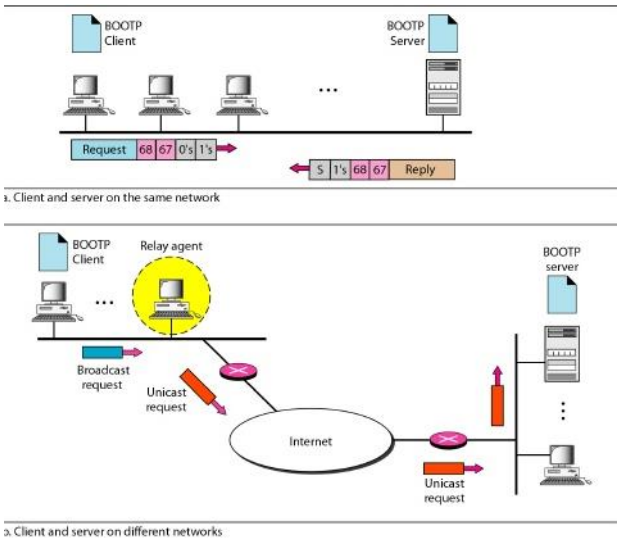

Figure 15: Working of BOOTP protocol

The unicast address of the BOOTP server is known by the relay agent and it sends a unicast request to the server. The BOOTP server identifies the IP address of the relay agent and sends a reply. The relay agent sends the reply back to the BOOTP client.

D. DHCP

Whenever an address is requested by a client, the BOOTP server considers a table which already exists to match the physical address to the corresponding logical address. So, BOOTP provides static address allocation that is manual. Dynamic Host Configuration Protocol (DHCP) grants both static and dynamic address allocation that is manual or automatic. The static address allocation is done by manually checking into the table that already exists to bind the physical address to the logical address. For the dynamic allocation, the server maintains another database with the present IP addresses. When a client asks for a temporary IP address then the server assigns an IP/logical address from the pool of available address only for a negotiable time span. When the time or the lease expires the client either has to stop using that address or the lease is renewed.

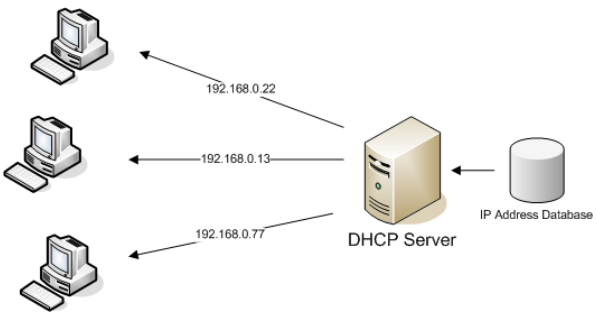

Figure 16 : Working of DHCP protocol

E. Internet Protocol

IP is a protocol that defines some set of rules for routing and addressing of packets so that they can travel from one station to another across networks. Every device or host that connects to the internet is given an IP address that is unique. There are two versions of Internet Protocol discussed below.

IPv4

Internet protocol version 4 is a connectionless and unreliable protocol. No flow control or error control is provided by this protocol. IPv4 addresses are unique and 32-bits long. By unique it means that no two devices can use the same logical (IP) address on the internet. The total number of addresses defined in IPv4 protocol are 2^{32}.

IPv6

Internet protocol version 6 was designed to overcome the limitations of IPv4. The changes introduced in IPv6 were bigger address space, improved format of header, advanced options, extension headers, more security. The address length is 128 bit and the address space of IPv6 is 2^{128} which is four times of the length of IPv4.

F. ICMP

IP protocol lacks error-reporting and error-correcting mechanism and there is absence of host and management queries. Internet Control Message Protocol was developed to report error messages and query messages to the original source.

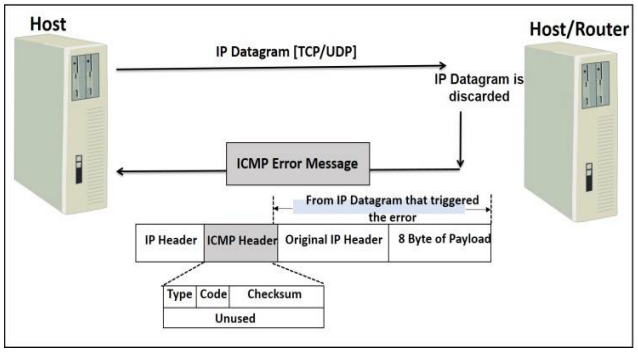

Figure 17: ICMP protocol header

There are 5 error reporting messages:

Destination unreachable that is sent when a router or a host is not able to transfer a message to the destination.

Source quench is sent when a host discard the message because of congestion.

Time Exceeded message is sent when every fragment that generate the whole message do not arrive at the receiving host in time.

Parameter problem message is used when a host or a router finds a missing value in any region of the datagram.

Redirection message is used by the host or a router to tell the most efficient routing choice for the data transmission.

G. IPSec

IPSec i.e. Internet Protocol Security is a combination of protocols that provides security at the network layer. IPSec works in 2 different modes: transport mode and tunnel mode. The transport mode secures the data coming from the transport layer and does not secure the IP header whereas the tunnel mode protects both the information from above layer and the IP header.

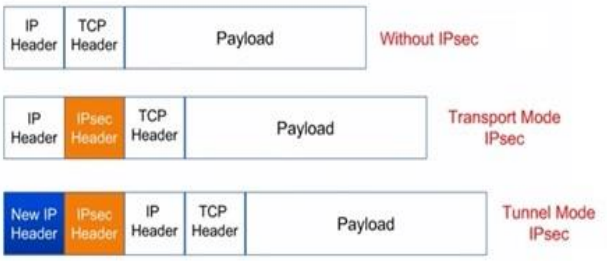

Figure 18 : IPSec protocol modes

IPSec consists of 2 protocols that are- Authentication Header (AH) Protocol and Encapsulating Security Payload (ESP).

The Authentication Header ensures the integrity of the message that is present in the IP packet. It makes use of a hash function along with a symmetric key to make a message digest and this digest is added in the authentication header.

The above protocol produces only authentication and integrity to the data and no privacy. A protocol that provides integrity, authentication and privacy was developed which is Encapsulating Security Payload (ESP). It inserts header and trailer to the message. IPv4 and IPv6 both are supported by IPSec but in IPv6 the two protocols are part of the extension header.

V. TRANSPORT LAYER PROTOCOLS

The transport layer does process-to-process delivery of a datagram. The responsibilities of the transport layer are segmentation and reassembly, connection control, flow control and error control. There are various protocols on this layer some of which are described below.

A. UDP

User Datagram Protocol is a connectionless and unreliable protocol which has no flow control or error control. It is same as IP protocol except it performs process-to-process delivery rather than host-to-host delivery. UDP uses a minimum of overhead and it can be used for simple transmissions like a process sending a short message without focusing on reliability. This protocol does not provide congestion control also. UDP can be used for protocols like TFTP (Trivial File Transfer Protocols) that have internal flow and error control mechanism. It is very appropriate in multicasting as multicasting is not in the TCP. Well known ports used with UDP are TFTP, RPC, SNMP, NTP and so on.

B. TCP

Transmission Control Protocol is a connection-oriented and a reliable protocol which has both flow control and error control. Like UDP, TCP also uses port numbers to deliver data from one process to another process. It is stream-oriented protocol which means the data travels in the form of stream of bytes that travels in segments. Full-duplex communication takes place in TCP that means data has the ability to travel in each direction simultaneously. The connection in TCP is established by three-way handshaking mechanism in which at first sender sends a SYN segment to establish the connection and the receiver sends an ACK for acknowledgement of the next frame so that the sender can then send the data. After the connection is established, data transfer takes place and at last connection is terminated by the same three-way handshaking process in which FYN segment is used to terminate the connection.

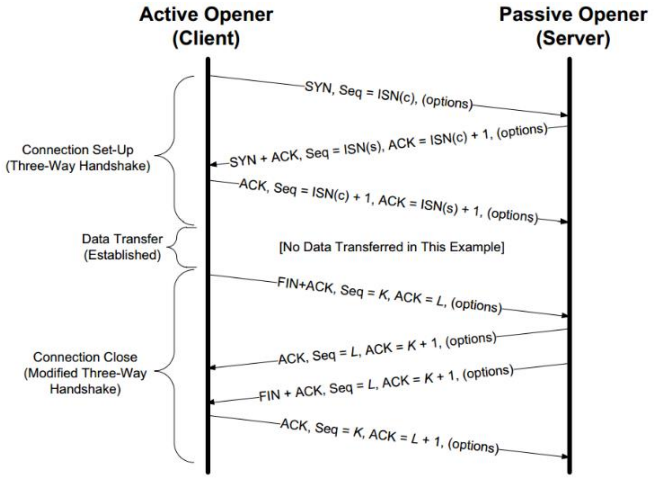

Figure 19 : Working TCP protocol

TCP offers flow control by the sliding window mechanism that makes the transmission efficient by controlling the data flow so that receiver is not overwhelmed with the data. The sliding window in TCP is byte oriented and has three phases: opening, closing and shrinking.

TCP offers error control by detecting duplicate or lost segments, segments that are out of order and corrupt segments. Detection and correction of error is achieved with the help of: checksum, acknowledgement and time-out.

TCP offers congestion control by maintaining a window size that is minimum of congestion window and receiving window.

C. SSL/TLS

Secure Socket Layer Protocol provides security on transport layer by providing end-to-end security services for applications that make use of protocols like TCP. It provides security on the Internet. SSL provides security services to the data that is developed from application layer by receiving data from an application layer protocol such as HTTP. The data is compressed, signed and encrypted and then it is passed to TCP. The services provided by SSL are: fragmentation, compression, message integrity, confidentiality and framing. SSL doesn't provide error detection and correction. Four protocols are defined by SSL that are explained below.

The Handshake Protocol builds the cipher set and provides keys and security parameters and performs authentication.

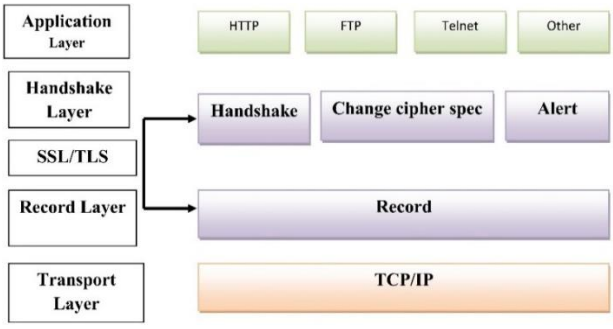

Figure 20 : SSL/TLS protocol

The ChangeCipherSpec Protocol is used as a single message that informs that the sender wants to change to a new set of keys that are made from the information that is exchanged by handshake protocol.

The Alert Protocol reports the abnormal conditions and errors.

The Record Route Protocol is the carrier that transfers the data from above three protocols that is coming from the application layer and forwards the data to the transport layer.

VI. APPLICATION LAYER PROTOCOLS

The main function of application layer is to provide services to the user like file transfer, access and management, mail services, directory services and so on. Some of the application layer protocols are explained below.

A. TELNET

TErminal NETwork is a standard protocol of TCP that establishes a connection to the remote device such that the local terminal looks as a terminal at the remote system. It allows a u to communicate to a device at a remote location. Network administrators use Telnet to access and manage remote devices by connecting to the IP address or hostname of the remote device.

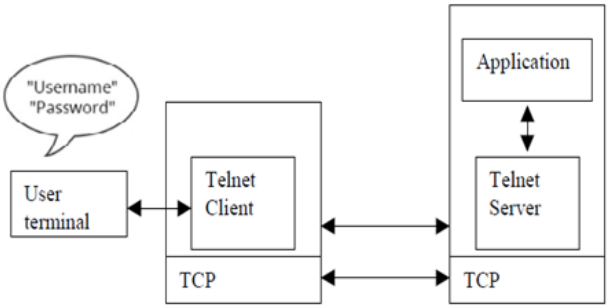

Figure 21 : TELNET protocol

B. SSH

SSH, or Secure Shell allows users to regulate and also to modify the remote servers on the Internet. SSH is a secure replacement of Telnet and uses cryptography to assure that all communications are encrypted and secure. It also provides authentication of a remote user. Types of encryption techniques used by SSH are:

Symmetric Encryption makes use of a secret key for encryption and decryption that means the same key

is shared between receiver and sender. Some ciphers are DES, AES, Triple DES etc.

Asymmetric Encryption uses 2 distinguishable keys for encryption and for decryption which are called as public and private key. For encryption public key of the receiver is used and for decryption private key of the receiver is used. Some ciphers are RSA, Diffie-Hellman, Man-in-the-middle attack etc.

C. SMTP

Simple Mail Transfer Protocol is a message transfer agent (MTA) with a port no 25. To send an e-mail, sender or the client must have a client MTA and for receiving the mail the receiver or the server must have the server MTA. On the Internet, SMTP defines the MTA client and the MTA server. It simply defines how MTA client and MTA server transfer data using commands and responses.

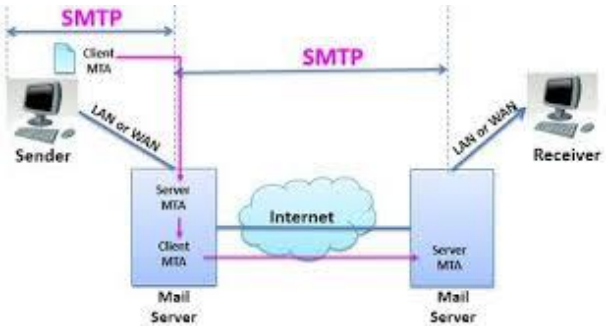

Figure 22 : SMTP protocol

SMTP is used twice, between the sender and the sender's mail server and between the sender's mail server and the receiver's mail server. It pushes the messages from sender or from the client to the mail server and hence called as a push protocol.

D. POP3

In the third stage, a pull program is needed that will pull the message from the mail server and pass it to the receiver. This stage uses message access agents (MAA) that are used to retrieve the data from the mail server. Post Office Protocol version 3 is a message access agent with a port no 110.

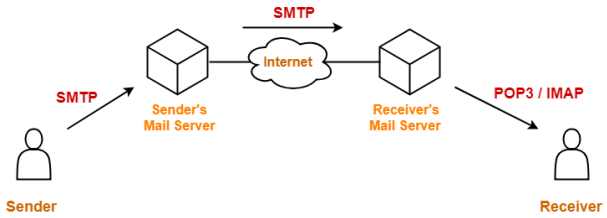

Figure 23 : POP3 and IMAP protocol

Mail access gets started when user wants to download e-mail from the mailbox on the mail server and for that client opens a connection to the server on the port 110. The client then uses the user name and password to get the mailbox access and thus the users can get the messages.

E. IMAP4

Internet Mail Access Protocol (Port 993), version 4 is more powerful and more complex than POP3. POP3 doesn't allow user to create the mails on server, users can't have separate folders and also users cannot check the mail before downloading. With the help of IMAP4 e-mails can be checked before downloading, users can partially download the e-mail, and users can also create, delete or rename mailboxes on the mail server.

F. FTP

File transfer protocol is used to copy a file from one host to another by using TCP services. Two connections are made between the hosts, one for data transfer with port number20 and other for control information with port number 21.

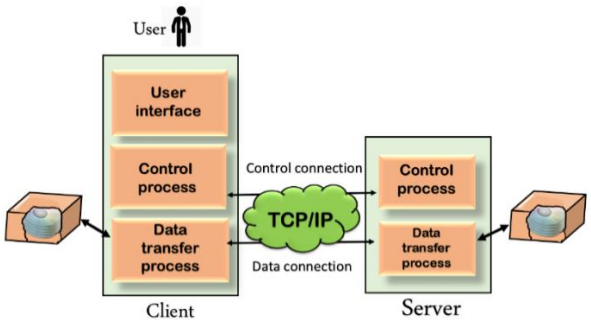

Figure 24 : Connections in FTP protocol

The basic model of FTP is shown in the figure above. The control processes use the control connection which is opened for the entire FTP session. The data transfer processes use data connection which is opened for file transfer and then closed.

VII. CONCLUSION

Transmission Control Protocol model is used widely in the field of communication. It works along with Internet Protocol. The TCP/IP model is hierarchical meaning that every protocol of lower layer supports the protocol on the above higher layers. In this article, we have covered the working of protocols that function over all the five layers of TCP/IP protocol i.e. from bottom layer called physical layer to the top layer called the application layer.

VIII. REFERENCES

[1]. TCP IP Protocol Suite 4th Ed. B. Forouzan
[2]. Christoph Meinel, Harald Sack. "Internetworking", Springer Science and Business Media LLC, 2013
[3]. D.D. Isci, F. Alagoz, M.U. Caglayan. "IPSEC over Satellite Links: A New Flow Identification Method", 2006 International Symposium on Computer Networks, 2006
[4]. "Informatics Engineering and Information Science", Springer Science and Business Media LLC, 2011
[5]. Singh, Er. Gurjot, and Er. Sandeep Kaur Dhanda. "Quality of Service Enhancement of Wireless Sensor Network Using Symmetric Key Cryptographic Schemes", International Journal of Information Technology and Computer Science, 2014.
[6]. "Web and Communication Technologies and Internet-Related Social Issues — HSI 2003", Springer Science and Business Media LLC, 2003
[7]. "Synchronizing Internet Protocol Security (SIPSec)", Springer Science and Business Media LLC, 2007

Cite this article as :

Ashima Tyagi, "TCP/IP Protocol Suite", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 6 Issue 4, pp. 59-71, July-August 2020. Available at doi : https://doi.org/10.32628/CSEIT206420
Journal URL : http://ijsrcseit.com/CSEIT206420