A Survey on TCP/IP Protocols Suite For communication

Mr. Shahid Navaj Jamadar[1], Mr. Aditya Rajesh Kulkarni[2], Mr. Abhijeet Balaso Jainapure[3], Prof. S.D. Sawant[4]

[1,2,3,4] Sharad Institute of Technology Polytechnic, Yadav, Kolhapur, Maharashtra, India

Abstract- *Protocols are the set of rules and conventions that are used in exchanging of information between two machines in various layers of the network. A Protocol that support the sharing of resources that exist in different packet switching networks is presented. But the communication and resource sharing between different networks is not possible because of variation in induvial network such as packet sizes, transmission failure, error checking, flow control, sequencing etc. Some implementations issues are considered and problems, such as routing, accounting and timeouts are exposed.*

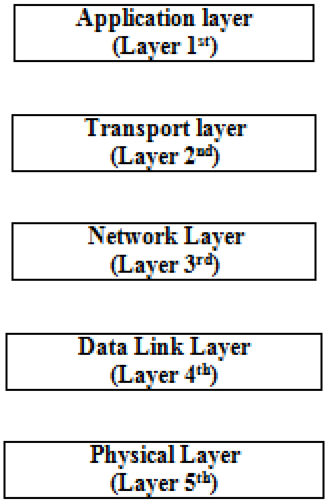
In this paper, we present TCP/IP Protocol suite, Host to Network layer protocol, Internet Protocols and many more our main aim of paper is to introduce TCP/IP protocols.

Keywords- Host to Network Layer Protocol, Internet Protocols (IP), Transmission Control Protocol (TCP), IP Addressing and its Some types.

I. INTRODUCTION

About understanding what is TCP/IP first of all we have to know about what is Protocols [6]. The meaning of protocol is “It is allowed communication between networks”. For Sharing particular Data, you have made both devices as a friend or they have to agree some rules and Regulations between each other. A Protocol suite is defined as collection of protocols organized in different layers. The TCP/IP protocol suite is used in Internet today. To make the data meaningful, the computer and terminals share some common protocols (i.e. A set of agreed upon conventions). However, some protocols have addressed only the problem of communication on the same network.

TCP/IP is short form of two important protocols namely Transmission Control Protocol/Internet protocol [1]. TCP/IP is hierarchical protocol means that each upper layer protocol receives support and services from either one or more lower level protocols. In original TCP/IP protocol suite, there were four software layers built upon the hardware. But today’s TCP/IP protocol suite uses five-layer model as shown in below figure [2].


Application layer (Layer 1st)
Transport layer (Layer 2nd)
Network Layer (Layer 3rd)
Data Link Layer (Layer 4th)
Physical Layer (Layer 5th)

Layers in TCP/IP protocol suite

Brief description of TCP/IP Layers [14]:

A. Physical Layer: This layer contains all the functions that are needed to carry the bit stream/packets from source to destination over a physical medium. Ethernet, PPP, etc.

B. Data Link Layer: In this layer the bit stream reorganizes into a data unit. This data units are also called as “frame” and this frame are delivers to an adjacent system. Wi-Fi, SLIP, etc.

C. Network Layer: At this layer, data is converted in the form of packets from source to destination, across as many links as necessary. It can also able to transmit to non-adjacent system. It is responsible for sending and receiving TCP/IP packets on the network medium. E.g. IP (IPv4, IPv6), ICMP, IGMP, etc.

D. Transport Layer: This layer is concerned with process-to-process delivery of information. A system can be running file transfer, email, and other network processes all at the same time. This all can be possible over a single physical interface. TCP, UDP, etc.

E. Application Layer: It is topmost layer of OSI model. It provides services that directly support user application such as database access, e-mail and file transfer. New protocols and services are always being developed in this category and this is concerned with differences in internal representation, user interfaces, and anything else that the user requires. E.g., SSH, POP3, TLS/SSL, HTTP, FTP, SMTPDNS, etc.

II. HOST TO NETWORK LAYER

SLIP and PPP are the data link layer protocols. They are used by the systems for wide area connections using the telephone lines and other types of physical layer connections. SLIP is simpler between the two and PPP is more complex. PPP uses additional protocols to establish connection between two systems. Both these protocols are in hot to network layer of TCP/IP protocol suite.

1.1) Serial Line IP(SLIP):

This protocol was device in 1984, to connect a workstation to the internet over dial-up line using a modem. It is connection-oriented protocol. This protocol is very simple. The workstation sends raw IP packets over the line with a flag byte at end for framing purpose. If the flag format appears in the data, then a two-byte sequence (OXDB, OXDC) is sent in its place [1].

If OXDB occurs in the flag byte, then it is also stuffed. In some SLIP implementations, a flag byte is attached at the front and back of each IP packet sent.

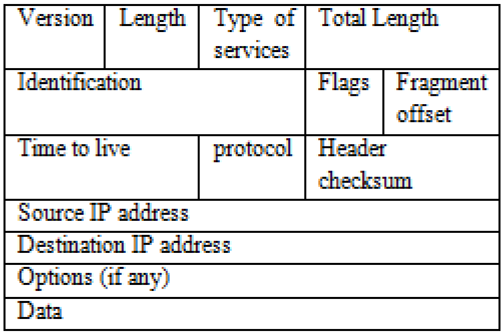
1.2) Point to Point Protocol (PPP):

One of the most common protocols used for access is PPP. The long form of PPP is Point to Point Protocol. This protocol is used by lot of internet users to connect their home computers to the server of an internet service provider (ISP). The PPP is used for controlling and managing the data transfer. Most of these users have a traditional modem and they are connected to the internet through a telephone line or TV cable.

III. INTERNET PROTOCOL (IP)

This is the host delivery protocol which belongs to the network layer and its designed for the internet. IP is a connectionless datagram protocol with no guarantee of reliability. It is an unreliable protocol because it does not provide any error control or flow control. IP can only detect the error and discards the packet if it is corrupted. If IP is to be made reliable, then it must be paired with a reliable protocol such as TCP at the transport layer.

Each IP datagram is handled independently and each one can follow a different route to destination. So, there is possibility of receiving out of order packets at the destination. Some packets may even be lost or corrupted. IP relies on higher level protocol to take care of all these problems. The header includes a 4-bit protocol version number, length of header, a 16-bit total length, along with some control fields, a header checksum for error checking and the 32-bit source and destination IP addresses.



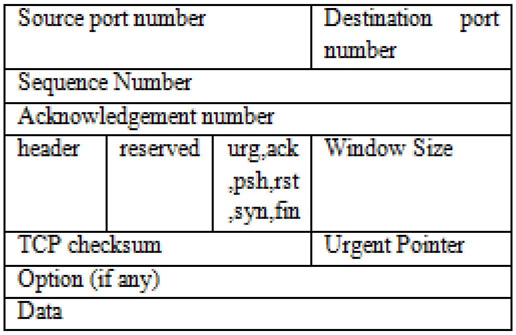
Version	Length	Type of services	Total Length	
Identification			Flags	Fragment offset
Time to live		protocol	Header checksum	
Source IP address				
Destination IP address				
Options (if any)				
Data				

Within IP header, there is some important information available like source IP address, destination IP address, which is important for routing the packet around the network through the internet [2][3].

IV. TRANSMISSION CONTROL PROTOCOL (TCP)

The Internet has two main protocols in the transport layer. One of them is connection oriented and the other one supports the connectionless service [4]. TCP (transmission Control Protocol) is connection-oriented protocol and UDP (User Datagram Protocol) is the connectionless protocol. UDP is basically just IP with an additional short header. The TCP provides reliable transmission of data in an IP environment. TCP corresponds to the transport layer (Layer 4) of OSI model.

TCP offers reliability by providing connection-oriented, end-to-end reliable packet delivery through an internetwork. TCP offers efficient flow control, which means that, when sending acknowledgements back to the source, the receiving TCP process indicates the highest number that it can receive without overflowing its internal buffers [5].



Source port number			Destination port number
Sequence Number			
Acknowledgement number			
header	reserved	urg,ack ,psh,rst ,syn,fin	Window Size
TCP checksum			Urgent Pointer
Option (if any)			
Data			

Fig. TCP Header Format [2][3]

TCP sends data using IP, in blocks which are called segments. Each segment contains 20 bytes of header information with IP header [7]. The TCP header starts with 16-bit source and destination port number fields, these fields specify the application layers that have sent and are to receive the data.

V. IP ADDRESSING AND ITS TYPES

IP Address stands for Internet Protocol address and is an identifying number that is associated with a specific computer or computer network.An IP address consists of four numbers; each can contain one to three digits. These numbers are separated with a single dot (.). These four numbers can range from 0 to 255. The IP address allow you to pinpoint a particular device from the billions of devices on the Internet [8]. To send you a letter, someone needs your mailing address. In the same sense, one computer needs the IP address of another computer to communicate with it.

Types of IP addresses

The IP addresses can be classified into two. They are listed below.

1) Static IP addresses
2) Dynamic IP addresses

Let us see each type in detail.

1. Static IP Address: As the name indicates, the static IP addresses usually never change but they may be changed as a result of network administration. They serve as a permanent Internet address and provide a simple and reliable way for the communication. From the static IP address of a system, we can get many details such as the continent, country, region and city in which a computer is located, The Internet Service Provider (ISP) that serves that particular computer and non-technical information such as precise latitude and longitude of the country, and the locale of the computer. A static IP address is useful if you host a website from home, have a file server in your network, use networked printers, forward ports to a specific device, run a print server, or use a remote access program. Because a static IP address never changes, other devices always know exactly how to contact a device that uses one [9].

2. Dynamic IP Address: Dynamic IP address are the second category. These are temporary IP addresses. These IP addresses are assigned to a computer when they get connected to the Internet each time. They are actually borrowed from a pool of IP addresses, shared over various computers. A dynamic Internet Protocol address (dynamic IP address) isa temporary IP address that is assigned to a computing device or node when it's connected to a network. A dynamic IP address is an automatically configured IP address assigned by a DHCP server to every new network node.

The assigning, reassigning and modification of dynamic IP addresses is managed by a Dynamic Host Configuration Protocol (DHCP) server. One of the primary reasons behind having dynamic IP addresses is the shortage of static IP address on IPv4. Dynamic IP addresses allow a single IP address to be shuffled between many different nodes to circumvent this problem.

IP Version 4 and IP Version 6

The two versions of IP addresses currently running are IP versions 4 (IPv4) and IP versions 6 (IPv6). There are many features with these two versions.

IP Version 4

IP Version 4 (IPv4) was defined in 1981. It has not undergone much changes from that time. Unfortunately, there is a need of IP addresses more than IPv4 could supply. This is a little more than four billion IP addresses. An IPv4 address is typically formatted as four 8-bit fields. Each 8-bit field represents a byte of the IPv4 address [10]. As we have seen earlier, each field will be separated with dots. This method of representing the byte of an IPv4 address is referred to as the dotted-decimal format.

IP Version 6

The IPv6 is the most recent version of Internet Protocol. As the Internet is growing rapidly, there is a global shortage for IPv4. IPv6 was developed by the Internet Engineering Task Force (IETF). IPv6 is intended to replace the IPv4. IPv6 uses a 128-bit address and it allows 2128 i.e. approximately 3.4×1038 addresses. The actual number is slightly smaller as some ranges are reserved for special use or not used. The IPv6 addresses are represented by 8 groups of four hexadecimal digits with the groups being supported by colons. An example is given below:

E.g.: 2001:0db8:0000:0042:0000:8a2e:0370:7334

The features of IPv6

The main features of the IPv6 are listed below.

1) IPv6 provides better end-to-end connectivity than IPv4.
2) Comparatively faster routing.
3) IPv6 offers ease of administration than IPv4.
4) More security for applications and networks.
5) It provides better Multicast and Anycast abilities.
6) Better mobility features than IPv4.

VI. CONCLUSION

The Internet protocol suite does not presume any specific hardware or software environment. It only requires that hardware and a software layer exist that is capable of sending and receiving packets on a computer network. As a result, the suite has been implemented on essentially every computing platform. A minimal implementation of TCP/IP includes the following: Internet Protocol (IP), Internet Control Message Protocol, Transmission Control Protocol (TCP).As seen from the history, one of the giant steps with growing use of the internet has been demonstrated that TCP protocol may evolve into a more flexible to manage all the networking process perfectly. As the digitalization grows the. The complexity of networks evolution also growing in parallel so for proper suiting this situation TCP/IP perform its task of data transfer and all networking activities properly along with the other layers and protocol. We can also say that the TCP/IP suite is the only way to support the strong increase of users demand and the fast-technological development. Along with these useful features, there are some design flaws of TCP/IP suite of protocols that leads to most of the attacks on the Internet. So, it always requires security to be applied as an external layer to the TCP/IP suite.

Several points are immediately obvious from this analysis. The first, surely, is that in general, relying on the IP source address for authentication is extremely dangerous13. Fortunately, the Internet community is starting to accept this on more than an intellectual level.

REFERENCES

[1] TCP/IP Fundamentals [Online] available: http://www.sfisaca.org/download/lam.pdf

[2] TCP/IP Tutorial [Online] available: documentation.netgear.com/reference/sve/tcpip/pdfs/FullManual.pdf

[3] The TCP/IP Reference Model [Online] available: http://www.mif.vu.lt/~adam/courses/npij/scsu-mcs426-fall-1999-3.pdf.

[4] David Espina, DariuszBaha, “The present and the future of TCP/IP”. pdf.

[5] Postel, J. (1981), Transmission Control Protocol, RFC793.

[6] W. R. Stevens, TCP/IP Illustrated Vol. 1 – The Protocols, Addison-Wesley, 1994.

[7] Guang Yang, “Introduction to TCP/IP Network Attacks”, Department of Computer Science, Iowa State University, Ames, IA 50011.

[8] Kh. Shazzad, J. Sou Park. Optimization of Intrusion Detection through Fast Hybrid Feature Selection. The Sixth International Conference on Parallel and Distributed Computing, Applications and Technologies, 2005, (PDCAT'05), Page(s): 264 - 267, 0508 Dec, 2005.

[9] McCloghrie, K. and Rose, M. Management Information Base for Network Management of TCP/IPbased Internets. RFC 1066. 1988.

[10] Abdullah H. Alqahtani, MohsinIftikhar, “TCP/IP Attacks, Defenses and Security Tools”, International Journal of Science and Modern Engineering (IJISME) ISSN: 2319-6386, Volume-1, Issue-10, September 2013.