INTERNATIONAL JOURNAL OF ENHANCED RESEARCH IN MANAGEMENT & COMPUTER APPLICATIONS
VOL. 2, ISSUE 1, JAN. 2013 ISSN NO: 2319-7471

A look back at Issues in the layers of TCP/IP Model

Gayatri Bhatti[1], Rajinder Singh[2], Prabhdeep Singh[3]
[123]Department of Computer Science and Engineering, PIT, Kapurthala, India.
[1]gayatribhatti.pit@gmail.com, [2]rajindersinghpit@gmail.com, [3]ssingh.prabhdeep@gmail.com

Abstract: In terms of Data Communications, TCP/IP model has remarkable role. TCP/IP is a set of network standards that specify the details that how computers communicate for interconnecting networks. This research paper gives detailed information about TCP/IP model and will explain the work of every layer in brief. The complete study of hardware components required for data communication is also provided. The drawbacks or problems originated in the earlier hardware components led to the foundation of new components, there by solving all those problems. These components are required for exchanging data among several entities. Every layer provides various services that describe the different functionalities of every layer. Besides, these services also contain several issues which have been examined in detail and can be resolved by using new strategies.

Keywords: Bandwidth, Network error, Network services, Performance efficiency, Routing.

I. INTRODUCTION

TCP/IP (Transmission Control Protocol/Internet Protocol) is the basic communication language or protocol of the Internet. It can also be used as a communication protocol in a private network (either an intranet or an extranet). When you are set up with direct access to the Internet, your computer is provided with a copy of the TCP/IP program just as every other computer that you may send messages to or get information from also has a copy of TCP/IP [1].
Many Internet users are familiar with the even higher layer application protocols that use TCP/IP to get to the Internet. These include the World Wide Web's Hypertext Transfer Protocol (HTTP), the File Transfer Protocol (FTP), Telnet (Telnet) which lets you to logon to remote computers, and the Simple Mail Transfer Protocol (SMTP).

II. PHYSICAL LAYER

The physical layer deals with transmission of data via physical medium like wires. Encoding of data in signals is done at physical layer. Thus physical layer sets up physical communication between two devices. In physical layer mostly error is present in cables[2].

A. Twisted Pair Cable

The twisted pair cable consists of two conductors each with its own plastic insulation, twisted together. In twisted cable the main problem is, when we send data on longer distance, the noise occur in data. The main problem in twisted cables is that it is used in telephone lines to provide voice and data channels. When we send large packet they cannot perform very well and gives some times error message automatically, due to noise error.

B. Coaxial Cable

In coaxial cable while sending data in long distance sometimes noise error occurs like packet error, transmitting error, flow control error etc.

C. Fibre Optic

The fibre optic cable is secure but it can only send data in a limited range.

III. DATA LINK LAYER

Data link layer provides the functional and procedural meaning to transfer data between network entities and might provide the meaning to detect and possibly correct errors that may occur in the physical layer. The data link layer defines the error when they receive the data from physical layer [3].

In data link layer mostly error is present in hub and switch. In hub and switch when data is transmitted sender to receiver the main error is data error.

A. Data Error

Data can be corrupted during transmission. The main error in Data link layer is:

1) Single Bit error

In this, single bit of data has changed during transmission.

2) Burst Bit error

Burst errors are large clumps of bit errors. However, all single bit errors are isolated strains on a computer data code. In burst error, more than one bit is changed.

B. Design Issues

The data link layer has a number of specific functions it can carry out. These functions include:

- Providing a well- defined service interface to the network layer.
- Dealing with transmission errors.
- Regulating the flow of data so that slow receivers are not swamped by fast senders.

IV. NETWORK LAYER

The network layer delivers data in the form of a *packet* from source to destination. The biggest difference between the network layer and the data link layer is that the data link layer is in charge of data delivery between *adjacent* systems (directly connected systems one hop away), while the network layer delivers data to systems that are not directly connected to the source [4].

Routers with switching are used to detect optimal route for packets. The use of cache in routers and how it affects performance of router is explained [6].

A. Basic Router Functions

Here are some functions of router:

- Route detection for packets.
- Layer 3 switching.
- Drops packets whose lifetime is expired.

The data is transferred in between interfaces or line cards respectively known as inbound interface and outbound interface. The packets are received at inbound network interface; processed by the processing unit (CPU), possibly stored in the buffers. The packets are then forwarded through the switching fabric to outbound interface that transmits the packet to the next hop route.The fig. 1 shows architecture of a conventional router as following.

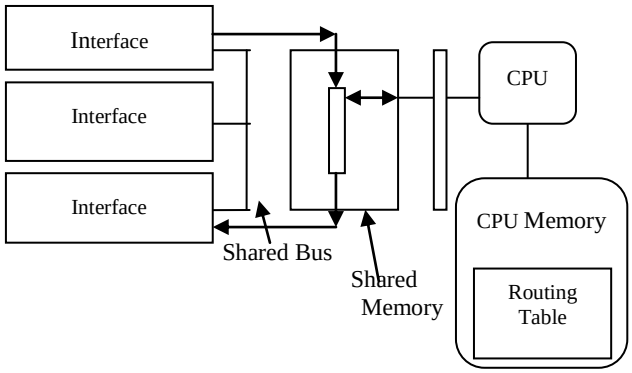

Figure 1. Architecture of Router

Performance bottleneck: To finding address of next hop is one of the performance bottlenecks in router.

B. Performance Improvement Strategies

Strategies for improving router performance are as following:

1) Route Caching

Router's CPU maintains route lookup for packets but it makes a lot of load on the CPU. To overcome this problem, routers now moved towards providing interfaces with own CPU and cache to determine outbound for that inbound interface. This step boosts up the packet forwarding speed from between two interfaces. This strategy lights up load on the system bus. The fig. 2 explains how route caching works.

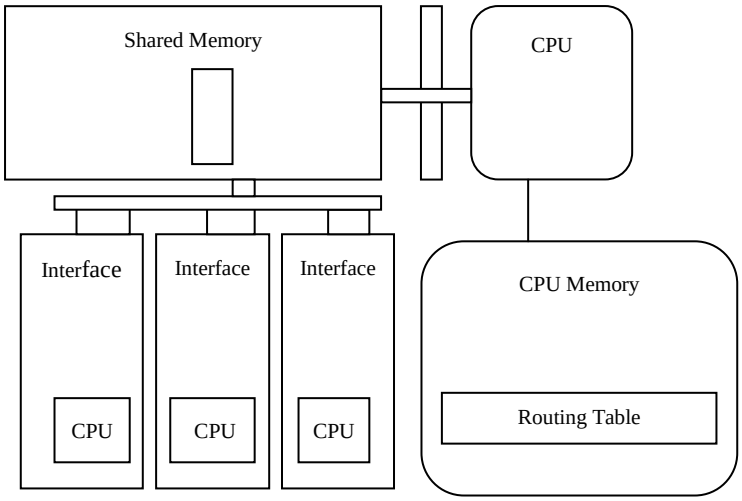

Figure 2. Route Cache and Distributed Processing

2) Switching

Now the route lookup is added in cache of interfaces so the CPU became less of a bottleneck. Interfaces use shared bus which limits speed of packet transmission. This leads to the next improvement in routers; the shared bus being replaced by a switch fabric. The switch fabric provides a large bandwidth for transmitting packets between interface cards, and increases throughput considerable.

3) Forwarding Engines

The purpose to use DMA technique for accessing headers from CPU by forwarding engines. It will speed up lookup method. Thus overall time complexity of sending data from one interface to other interface will be improved.

4) Distributed Processing Architecture

Distributed Processing architecture plays an important role for increasing speed of transmission. This architecture is a combination of all the techniques discussed above. Switch fabric increases packet throughput so that more and more packets can be transmitted between interfaces. Distributed Processing architecture contains a switch fabric.

5) Space Division or Crossbar Switch Fabric

This switch due to its various advantages as low cost, scalable, convenient establishes connection between the interfaces. It must operate at a speed equal to the all input links. It may also result in queuing up of packets which is a major problem known as head of line blocking due to which head of the input queue gets blocked leading to forwarding rate slows down. By taking care of the traffic on every output port, this problem can be removed. One method is to assign input buffer to every port and other is to match input and output port in every cycle. Allocator is used to allocate output ports to input ports. This problem can be optimized by increasing the speed of input/output channel there by increasing the throughput. Another problem in the crossbar switch is the fabrication density which results in showing down the speed of crossbar switch. The fig. 3 shows head of line problem in switches.

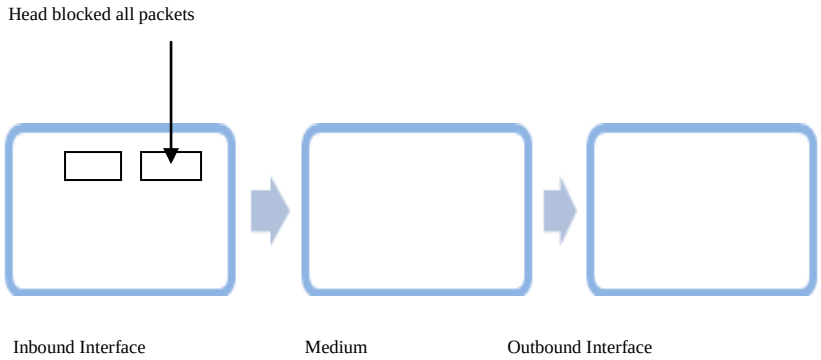

Figure 3. Head of Line Problem

C. Other Issues

Queuing up of packets effect the performance of the router. The packet size should be larger which helps in reducing the overhead for lookup also. The fig. 4, displays a graph indicating the number of packet transmitted per second depending on the frame size over various connections like T1, Ethernet and T3[5].

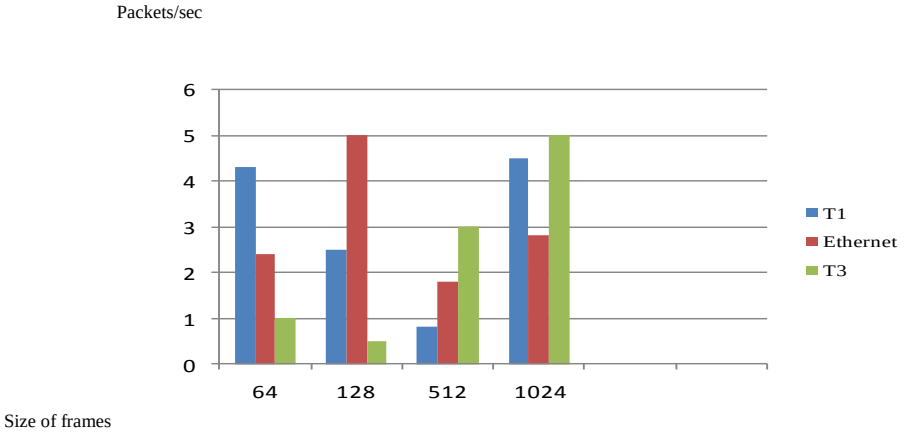

Figure 4. Packet per second vs Size of Frames

V. TRANSPORT LAYER

Transport Layer has remarkable role in the TCP/IP Model, especially where network layer is unreliable. When network layer provides unreliable service then transport layer handles all the functions like flow control and error control [7]. The issues related to transport layer are discussed.

A. Issues in Transport layer with Connection Less Unreliable Network Layer

In this, responsibility of transport layer increases because of unreliable network layer. Now transport layer has to take care of issues like error control, ordered delivery, retransmission of segments and reliability. All these issues should be taken care of besides issues which can be there as they were with connection-oriented reliable network layer [8]. So the following issues are there

- Ordered delivery
- Retransmission Strategy
- Duplicate Detection
- Flow Control
- Connection Establishment and Termination
- Crash Recovery

VI. APPLICATION LAYER

This layer handles issues like network transparency, resource allocation and problem partitioning. In TCP/IP model, application layer also constitutes features of session layer and presentation layer of OSI (Open System Interconnect) model. This layer identifies local applications to give them connection of remote applications or clients. This layer provides access as well as control access to remote and unauthorized applications. For data communication, authorization and secured connection is provided by application layer to users. Cryptography techniques are performed on original data to make it secure from attackers. Thus one issue of this layer is to keep original data safe from unauthorized access and authentication mechanism. Secured passwords and usernames are used for authentication purpose.
This layer has to convert the data in the standard format so that communication can be done between dissimilar hosts or networks. This layer deals with data organization and use compression and encryption strategies for data formatting. Another issue at this layer is to handle attacks. An attacker can access data on this layer and can also modify it. The modification done at data can also lead to application crashes. Solution to this problem is to use optimal cryptography and authorization techniques so that data or information can be made more secure.

Application layer provides applications like network management (SNMP), file sharing (FTP, HTTP), mail or messaging (SMTP), access (Telnet) etc. This layer‘s primary issue is to make secure connection for two communicating entities. For security purpose, an application uses firewall systems. Firewall systems are used to prevent unauthorized access or use of network [9].
So application layer deals with all the issues like security, presentation, compression, authentication, synchronization of data and provides access to communication entities [10].

VII. HOW NETWORK PROBLEMS MASKED AS BANDWIDTH ISSUES IDENTIFY

The main objective in the Auditing phase is to categorize the traffic, especially at the peak loads with sufficient bandwidth, according to the business needs. If the traffic is toxic, the goal is to eliminate the traffic, instead of providing more bandwidth. Bandwidth management concentrates on the various media over which the traffic travels, and the type of networking equipment used. These equipments can have a variety of capabilities and features due to the different media with different capabilities and demands, thereby choosing the best media. We can re-route some of this traffic to keep it safe from more congested network segments. The measurement phase which is an iterative process, concentrates on validating the modifications giving expected bandwidth, achieving the same results over and over again etc. The fig. 5 has shown flow chart.

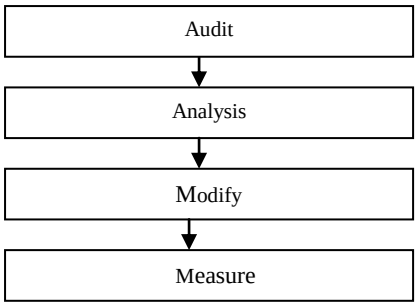

Figure 5. Flow Chart

TABLE I. ERROR TABLE OF LAYERS

Type of Layer	**Type of Error**	**Classification of Error**	**How to Remove the Error**
Physical layer	Cables error	Twisted cable error	In a twisted cable, the bandwidth is very low so data can not transmit at longer distance.
		Coaxial cable error	Coaxial cable is used for longer distances because it provides higher bandwidth than twisted pair.
		Fibre optic cable error.	Fibre optic is used for very high speed.
Data link layer	Error in hub	Data is send from sender but it is not properly receiver	Check the data error when we transmit the data. Single bit error or burst error if error is present than solve the error with checking technique like CRC(cyclic redundancy check),checksum etc.
	Error in switch	In switch data is send a particular node but it is not received by receiver and when that particular node is received that data but error is present in that data	
Network layer	Problem in Router	Router's CPU maintains route lookup for packets make a lot of load on it.	Provides interfaces with their own CPU and cache.
	Problem in Switch	Head of Line Blocking in crossbar switch	One method is to assign input buffer to every port and other is to match input and output port in every cycle.
Transport layer	Problem in Retransmission policy	Retransmission leads to duplicity of segments.	Use of three way handshaking technique.
	Problem in System	Crashing of sender or receiver system.	Use of persistent timer.
	Problem in Retransmission Strategy	What should be value of timer after that sender has to start retransmission.	The value of timer should be variable. It is a major research topic.
Application layer	Application crash	In this attacker modify transmitted data due to which application crashes.	Use optimal cryptography techniques, firewalls and authentication strategies.

ACKNOWLEDGMENT

Foremost, we Gayatri Bhatti and Rajinder Singh would like to express our sincere gratitude to our Head of the Department, Dr. Krishan Saluja and our guide Mr. Prabhdeep Singh for their continuous support, their patience, motivation, immense knowledge and their complete guidance for this research paper.

CONCLUSION

For communicating between two or more entities, a language is required. They cannot communicate without any language. In terms of computer networks, TCP/IP acts as a basic communication language for communicating two or more network entities. This paper basically includes study of TCP/IP five layered model and discussed Issues of every layer. The physical layer deals with physical media and issues come under it. Mainly three types of cables are used i.e. twisted pair cable, coaxial cable and optical fibre. Twisted pair cable has low bandwidth than coaxial cable so coaxial cable is used for longer distances. Optical fibre is used for higher speed and for getting higher security. The data link layer provides the functional and procedural means to transfer data between network entities and might provide the means to detect and possibly correct errors that may occur in the physical layer. This layer has some design issues and provides service interface to network layer which deals with flow and error control. The network layer uses high speed routers that must be robust and must have enough parallelism to support multi cast and broadcast. The transport layer provides end to end delivery between sender and receiver which may work with connection oriented or connection less underlying network layer. The topmost layer is application layer that includes features of session layer and presentation layer. The application layer is provided by the program that uses TCP/IP for communication. Examples of applications are Telnet, FTP, e-mail, HTTP and SNMP. In this paper, TCP/IP model and each layer's issues have been covered.

REFERENCES

[1]. Reed and Damon, "Applying the OSI Seven Layer Network Model to Information Security", SANS Institute – The Information Security Reading Room, November 2003.
[2]. Wang, Omatu, and Abe, "Identification of the Defective Transmission Devices using the Wavelet Transform", IEEEPAMI 27, 2005.
[3]. William, "Data and Computer Communications", Prentice Hall, 7th edition, ISBN 0-13-100681-9, 2006.
[4]. James Aweya, "IP Router Architectures: An Overview", Nortel Networks, Ottawa, Canada, K1Y 4H7, July 2003.
[5]. White Paper, "The Evolution of high-end Router Architectures-Basic Scalability and Performance Considerations for Evaluating Large-Scale Router Designs", http://www.csico.com.
[6]. P. Newman, G. Minshall, T. Lyon and L. Hutson, "IP Switching and Gigabit Routers," IEEE Communications Magazine, Vol. 35, No. 1, 1997.
[7]. Thomas Karagiannis, Andre Broido, Michalis faloutsos, and C. Claffy, "Transport layer identification of P2P traffic", October 2004.
[8]. Ming Zhang, Junwen Lai, Arvind Krishnamurthy, Larry Peterson, and Randolph Wang., "A Transport Layer Approach for Improving End-to-End Performance and Robustness Using Redundant Paths", Proc. of the USENIX 2004 Annual Technical Conference, June 2004.
[9]. John Rouda, "Application Layer Security", July 2006.
[10]. Tanenbaum, " Computer Networks", Teora Publishing House, ISBN:973-97706-3-0, Bucharest, Romania, 1998.