International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 15 (2017) pp. 4904-4907

A Conceptual View of Dynamic Protocol for Effective Data Communication

T. Vengatesh[1] and Dr. S. Thabasu Kannan[2]

*[1]**M.C.A, M.Phil.,** Research Scholar, Research and Development Center, Bharathiar University, Coimbatore, India.*
HOD, Dept. of .MCA, VPMM Arts & Science College For Women, Krishnankoil,

[1]Orcid Id: 0000-0001-8717-3657

[2]M.Tech, Ph.D, MBA, Principal, PCET, Sivagangai, India.

[2]Orcid Id: 0000-0002-5841-4623

Abstract
Due to increasing usage of internet now a days the main challenges is retrieval time. It means that a large of retrieval of data within a shorts span of time. In the existing protocols used for internet may support for some situations of time. That is for more time the existing protocol does not support to meet the present scenario of communication data from source to designation. Here our main thrust is to meets not only the present scenario but also the features expectation. For achieving the above we have proposed and simulate a newer version protocol for effective and efficient communication of data in large network. This protocol is dynamic in nature for selection of dimensionality for large data in volume. So this new version protocol may suite even for the application of big data. For the purpose of evaluating the performance of newer version protocol, we have taken two measurement namely throughput and latency. In near feature we have proposed to insert one more measurement called CPU utilization. Surely the newer version protocol assured for getting more reliability level from small scale to very large scale.

Keywords: Protocol, Throughput, Latency, Intelligence

INTRODUCTION

The IP is the principal communications protocol, comes under network-layer protocol, used for relaying datagram. IP is responsible for delivering datagram from the source host to the destination host on the basis of addresses. IP encapsulate the data to be delivered and addressing methods. IP was the connectionless datagram service. IP makes no guarantee that the packet will arrive without error. IP packet consists of a segment of data passed down from the transport or higher layer, plus a small IP header pretended to the data. IP Address is a unique identifier on a TCP/IP network to connect a private network to the Internet. IP address contains four segments of numbers (0 – 255) separated by periods. Here each node makes its forwarding decision based on the destination address within the IP packet header. The source address is examined when an error occurs. Routing decisions are based on the network-prefix of the IP destination address. The host portion of the IP address is used to differentiate among individual hosts on the same link. The first major version of IP is IPv4, which is the dominant protocol of the internet. Its successor is IPV6. It contains two functions: identifying hosts and providing a logical location service. Now days each and every company are running on IPv4 network but in future they will have to transfer into IPv6 network because of the limited number of IPv4 addresses has left. For that we need to change all the network into IPv6 which is time consuming and much costlier procedure or we can implement IPv6 as a future network remaining past IPv4network as they are. But IPv4 and IPv6 cannot communicate directly, so we have to use Tunneling for their communication. Tunneling allows communication between existing IPv4 networks with currently establishing IPv6 Networks.

In terms of performance we consider the time taken during the packet transfer between two IP addressing schemes, packet loss, packet sent and throughput. Tunneling gives a secret way or method through which all the information transfer take place by segregating packet and overriding of headers and trails of packets as well as using port security for providing security to network Internet Protocol version 4 (IPv4) is one of the key foundations of the Internet, which is currently serving up to four billion hosts over diverse networks. Despite this, IPv4 has still been successfully functioned well since 1981. Over the last couple of years, the massive growth of the Internet has been evident requiring an evolution of the whole architecture of the Internet Protocol. Therefore, in order to strengthen the existing architecture of Internet Protocol, IETF has developed IPv6, which offers a significant improvement of IPv4 when it comes to the unlimited address space, the built-in mobility and the security support, easy configuration of end systems, as well as enhanced multicast features, etc. On the other hand, due to the fascination of end users of the World Wide Web (WWW) and the popularity of real-time applications, we can now observe new increasing demands on real-time multimedia services over the Internet. The results from this study have shown the throughput where IPv6 maintains higher the transmission rate

than that of IPv4. IPv4 is an unreliable, connectionless protocol used within the packet-switched networks. It operates on a best effort delivery model; means it does not guarantee delivery, nor does it assure proper sequencing and avoidance of duplicate delivery. IP also provides fragmentation and reassembly of packets into original message.

IPv6 is the second version of the Internet Protocol to be used generally over the virtual world. IPv6 is specially designed to replace IPv4 in which device mobility, security, and configuration aspects also considered during designing of the protocol. The IPv4 and IPv6 protocols are not designed to be interoperable and made transition to IPv6 complicated. However, various IPv6 transition mechanisms have been discovered to allow communication between IPv4 and IPv6 hosts.

IPv6 provides technical benefits like larger addressing space, it allows hierarchical address allocation methods that facilitate aggregating route across the Internet, and thus limit the expansion of routing tables, use of multicast addressing, auto-configuration, and true quality of service, simplified routing and provides additional optimization for the delivery of services. It also has Mandatory authentication and data integrity protocols, through IP sec which is optional in IPv4.

Two computers with similar hardware (CPU: Intel Pentium C2D, RAM 2GB, NIC PCI Intel Pro 100, HDD1TB) were connected using a cross-over cable and each of the OSs (W2K and Linux Ubuntu) to be tested were installed one at a time on P2P test-bed. IPv4 as the communication protocol was configured first and data was collected. Later this was replaced with IPv6 ensuring that all other parameters remained the same. D-ITG 2.6.1d was the primary tool used to evaluate performance of protocols on both the OSs. IPv4 and IPv6 network protocols using both TCP and UDP transport protocols under W2k and Linux Ubuntu OSs. Throughput was empirically measured on P2P test-bed. In P2P test bed, there are no routers between the end nodes. The PCs had a direct communication link via twisted pair Ethernet cable from one end to the other. These tests are important to eliminate as many variables as possible and get a base performance evaluation of IPv4 and IPv6

THE FORE VIEW OF NEWER VERSION PROTOCOL

A.) Fragmentation:

Our newer simulated version protocol concentrates on both the routers available in sender as well as receiver part. By this there is guarantee for sending as well as receiving. Hence the level of reliability will be increased. here the synchronization of various parts is also possible by getting the acknowledgement from the receiving part .

B.) Checksum:

Our newer version contains checksum procedure for calculating the number of parts send/Receiver. Hence the perdition level can be measured and can easily find out the pending parts if any.

C.) ARP(Address Resolution Protocol):

Our newer version interacts multicast facility for address resolution to Send/Receiver frames. This process is used to reduce the burden various layers above link layer. Hence the rate of utilization will be minimized and the speed will be increased by reducing the cycle time of execution.

D.) IGMP(Internet group management protocol):

This Multicasting facilities engage by using multicast listener discovery message. The burden of traffic jam is not considered by using the above multicast listener discovery message(MLDM).Our newer version protocol can be easily configured with out any tedious process. Here auto configuration is possible.

E.) PRR(Pointer resource records):

The DNS can be mapped directly with IPVT.INT DNS domain to map IPVT address to host names.

F.)Payload:

The QoS of newer version can be maintained by using hash table. This table points the routers quality level. Hence the failure will be minimized and reliability level can be increased . so all the measurement used for QoS can be identified. The bypassing of inefficient use of header bits possible the speeding retrieval of data is possible by removing the unused data header. It maintains a separate and default gateway for determining the address of our newer version.

PERFORMANCE EVALUATION

We proposed to construct a protocol, which is used to overcome all the drawbacks of both IPV4 and IPV6.The new protocol is an integration of all the merits of IPV4 and IPV6 and remove some percentage(%) of weakness in both IPV4 and IPV6. Symbolically the efficiency $\sum$.

We come to know from the below solution it is symbolically represent that

α = IPV4 Strength,

β = IPV6 Strength,

α ∧ β = Both IPV4 and IPv6 Strength

┐α ∧ ┐ β = Both IPV4 and IPv6 ˜Weakness.

From the given proof, it is clearly shown that α refers to the Strength of IPv4. Then β refers to the strength of IPv6. The relation (α ∧ β) refers to the common Strength of Both IPV4 and IPV6 Network. Where as the relation (┐α ∧ ┐ β) refers to the weakness of both IPV4 and IPv6. The result ∑ refers to the efficiency of new simulated version protocol.

∑ = (α ∨ β) ∨ (┐α ∨ ┐ β) ∨ (α ∧ β)

= (α ∨ β) ∨ ┐α ∨ (α ∧ β) ∨ ┐β ∨ (α ∧β)

= (α ∨ β ∨ ┐α) ∨ (α ∨ β ∨ ┐β) ∨ (α ∧ β)

= (α ∨ ┐α) ∨ β ∨ (β ∨ ┐β ') ∨ α ∨ (α ∧ β)

= (α ∨ β) ∨ β ∨ (α ∨ β) ∨ (α ∨ (α ∧ β)

= (α ∨ β) ∨ (α ∧ β)

= (α ∨ β)----- ----- 1

∑ = (α ∨ β) ∨ (α ∧ β)

= (α ∨ β)--------- 2

∑ = (α ∨ β) ∨ (┐α ∨ ┐β)

= (α ∨ β) ∨ (┐α ∨ (α ∨ β) ∨ ┐β

= (α ∨ ┐α) ∨ β ∨ (β ∨ ┐β ') ∨ α

= (α ∨ β) ∨ (α ∨ β) ∨ (α ∨ β)

= (α ∨ β) ---------- 3

The equation 2 shows the result of both IPV4 and IPV6 strength. Then equation 3 shows the result of both IPV4 and IPV6 weakness. Then we can get our new simulated version protocol by combining both equation 2 and equation 3. The resulting new protocol is obtained from equation 1. Hence the efficiency and effectiveness of our newly designed protocol can be measured in terms of integration both IPV4 and IPV6. It is nothing but the removal of the negative aspects of IPV4,IPV6 and both IPV4 and IPV6. For proving the efficiency of the new simulated version of protocol we have taken two measurement namely throughput and latency.

A.)Throughput:

Throughput means the rate at which bulk data transfers can be transmitted from one host to another over a long period of time (Mbit/s).

Throughput = *W* / RTT // W = Window size if no loss

Throughput = *W*/2RTT // If loss occurs

Avg Throughput = 0.75*W*/RTT

// between *W*/2 and *W*

Round Trip Time (RTT) is the amount of time it takes one packet to travel from one host to another and back to the originating host (RTT in microseconds). The throughput can be measured in terms of three factors namely packet size, overhead, and CPU utilization.

A.a.)Packet size:

For all size set of packet sizes including smaller, medium and larger even very larger this new protocol surely gives an effective role for sending data. This new version can be used for getting efficiency in terms of 256 bytes and 384 bytes accruing the characteristic of IPV4. In addition to this, both A and B they are characteristics derived for our newer version if the packet size extreme 384 bytes Irrespective the packet size from 100 MB to 1000 MB the performance will be degraded by our new simulated version protocol. Hence the respective packet size, our simulated version protocol surely performs well.

A.b.)Overhead:

The second point discussed on measuring the performance our newly simulated version of protocol is overhead. Overhead means each packet requires extra bytes of format information that is stored in the packet header, which combined with the assembly and disassembly of packets, reduces the overall transmission speed of the raw data. Here up to 35% of packet sizes no overhead occurs for existing protocol by implementing our newer version. Our newer version contains no overhead up to 60% on top of IPV4 and IPV4 range. Both TCP and UDP used to overcome the difficulty while the sending the packet size up to 0 to 8192 Byte. For file size 64 byte to 1408 byte also here the major deviation occurred from 768 byte With respective overhead, there is a common deviation between IPV4 and IPV6 for both TCP and UDP with an exemption that no exemption beyond 7000 packet size. It is also recover in our new simulated version protocol. In our newer version the total cost for overhead also minimized by this CPU cycles to minimized.

B.)Latency:

Our newer version produce no delay for latency. The CPU Utilization time is also minimized for our newer simulated version protocol. No change in latency while sending low level packet and high level packet. Our newer version take minimized time for sending low level packet and also no delay occurred.

CONCLUSION

There is no doubt about the fault tolerance of the newer version protocol when compared with the existing protocol IPv4 and IPv6. The newer version protocol may be suitable even for near feature enhancements for this study of measuring the performance we have taken P2P as a platform for evaluating our newer version protocol with any other existing protocols. In near feature we planned to added two more platform Ericson test bet and IBM test bet. For all the test bets the operating system taken for testing are Linux ubundu and windows 2000 under TCP and UDP. Hence this may be a protocol which is used to integrate the intelligence as built in for effective and efficient communication.

REFERENCES

[1] T.Vengatesh, Dr.Thabasukannan, "Throughput Evaluation of IPV4/IPV6 Networks" International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE), ISSN: 0976-1353 ,Volume 12, Issue 2 –JANUARY 2015.

[2] T.Vengatesh, Dr.Thabasukannan, "Concert Estimation of IPV4 and IPV6 on its Throughput" International Journal of Computer Science and Network,(IJCSN) ISSN (Online) : 2277-5420 Volume 4, Issue 1, February 2015.

[3] T.Vengatesh, Dr.Thabasukannan, "QoS Provisioning Using Latency for IPV6" International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064, Volume 4 Issue 9, September 2015 .

[4] T.Vengatesh, Dr.Thabasukannan, "QoS Provisioning Using Jitter for IPV6" International Journal of Modern Electronics and Communication Engineering (IJMECE), ISSN: 2321-2152,Volume - 5, Issue 1, January, 2017.

[5] P. Srisuresh, M. Holdrege, "IP Network Address Translator (NAT) Terminology and Considerations,", Internet Engineering Task Force, August 2008.

[6] Dr.S.ThabasuKannan **"**Packet delay performance evaluation in IPv4/IPv6 networks" International Journal of P2P Network Trends and Technology Vol-2, Iss-4, Jul 2012.

[7] Dr.S.ThabasuKannan **"**Jitter for evaluating the performance of IPv4/IPv6 Networks" International Journal of Scientific and Engineering Research (IJSER) - (ISSN 2229-5518) Volume 3, Issue 9, September 2012.

[8] B. Carpenter, C. Jung, "Transmission of IPv6 over IPv4 Domains without Explicit Tunnels,", Internet Engineering Task Force, March 2009.

[9] Karuppiah, EttikanKandasamy, et al. "Application Performance Analysis in Transition Mechanism from IPv4 to IPv6". Research & Business Development Department, Faculty of Information Technology, Multimedia University (MMU), Jalan Multimedia, June 2009.

[10] Draves, Richard P., et al. "Implementing IPv6 for Windows NT", Proceedings of the 2nd USENIX Windows NT Symposium, Seattle, WA, August 3-4, 2009.

[11] Seiji Ariga, Kengo Nagahashi, Asaki Minami, Hiroshi Esaki, Jun Murai. "Performance Evaluation of Data Transmission Using IPSec over IPv6 Networks", INET 2006 Proceedings, Japan,.

[12] R. Banerjee, S. P. Malhotra, and M. Mahaveer,"A Modified Specification for use of the IPv6latency for providing an efficient Quality of Service using a hybrid approach", IETF IPv6Working Group Internet Draft, 2013.

[13] Guozhen Tan, Hengwei Yao, Yi Liu, and Ningning Han, "QoS Provision for IPv6 Traffic Using Dynamic Packet State", Proceeding of the joint international conference on Autonomic and Autonomous Systems and International Conference on Networking and Services, pp. 23-28, Oct. 2014.

[14] S. Thomson, T. Narten, "IPv6 Stateless Address Auto configuration," Request for Comments 1971, Internet Engineering Task Force, August 2012.

[15] T. Narten, E. Nordmark, W. Simpson, "Neighbor Discovery for IP Version 6 (IPv6)," Request for Comments 1970, Internet Engineering Task Force, August 2013.

[16] G. Tsirtsis, P. Srisuresh, "Network Address Translation – Protocol Translation (NAT-PT)," Request for Comments 2766, Internet Engineering Task Force, February 2013.

[17] B. Carpenter, C. Jung, Transmission of IPv6 over IPv4 Domains without Explicit Tunnels, Request for Comments 2529, Internet Engineering Task Force, March 2013.

[18] Fiuczynski, Marc E et. Al. "The Design and Implementation of an IPv6/IPv4 Network Adress and Protocol Translator".2012.