Role of IPv6 over Fibre (FIPv6): Issues and Challenges.

Hanumanthappa.J.[1], Manjaiah.D.H [2], Aravinda.C.V.[3]
[1]Teacher Fellow, Dos in CS, University of Mysore, Manasagangothri, Mysore, INDIA.
[2]Reader &Chairman, Mangalore University, Mangalagangotri, Mangalore, INDIA.
[3]M.Tech, K.S.O.U, Manasagangothri, Mysore.
hanums_j@yahoo.com
ylm321@yahoo.co.in
aravinda.cv@gmail.com

Abstract
Deploying the next generation Internet protocol (IPv6) over Fibre is facing an important challenge as the Fibre standard is failing to support IPv6 functionalities. In fact unlike the other standards Fibre optic links is based on how to reduce the over head in terms of header processing at data link layer by removing CRC field and Transport layer in IPv6 packet format. As a result the IPv6 packets over Fibre optic links standard shows that error handling can be performed at the network layer of ISO/OSI model instead of Data link layer and Transport layer. As a result our simulation results shows that error handling using IPv6 extension header at network layer has a smaller packer processing time as compared to error handling at data link layer and Transport layer in ISO/OSI. In this paper, we present different architectures to consider when deploying IPv6 packets over Fibre such as FIPv6.Also we point out challenges and solutions related to this deployment by focusing particularly on the role of FIPv6 impact on hardware and software, network layer error handling issues, challenges, facts etc.

Index terms: FIPv6, IPv6, etc.

I. Introduction

In the last 20 years, the internet undertook a huge and unexpected explosion of growth [].There was an effort to develop a protocol that can solve problems in the current Internet protocol which is in the current internet protocol which is in Internet protocol version 4(IPv4).It was soon realized that the current internet protocol the IPv4, would be inadequate to handle the internet’s continued growth. The internet Engineering task force (IETF) was started to develop a new protocol in 1990’s and it was launched IPng in 1993 which is stand for Internet Protocol Next Generation. So a new generation of the Internet Protocol (IPv6) was developed [7], allowing for millions of more IP addresses. The person in charge of Ipng area of the IETF recommended the idea of IPv6 in 1994 at Toronto IETF[1].But mainly due to the scarcity of unallocated IPv4 address the IPv4 protocol cannot satisfy all the requirements of the always expanding Internet because however its 32 bit address space being rapidly exhausted[2]alternative solutions are again needed[3].It is reported that the unallocated IPv4 allocated IPv4 addresses will be used with 6 to 7 years short period[2].The Long term solution is a transition to IPv6[5]which is designed to be an evolutionary step from IPv4 where the most transport and application –layer protocol need little or no modification to the work. The deployment of NAT [3] can alleviate this problem to some extent but it breaks end to end characteristic of the Internet, and it cannot resolve the problems like depletion (exhaustion) of IPv4 addresses.

1.1. Features of IPv6.

The main reason for designing this new Internet protocol(IPv6) was the need to increase the number of addresses(address spaces).The IPv6 address was designed with a 128-bit address scheme instead of 32-bit scheme in IPv4.So the number of possible addresses in IPv6 is $3.4X10^{38}$ unique addresses.IPv6 will have enough to uniquely address every device (example Telephone, Cell phone,mp3 player,hosts,routers,bridges etc) on the surface of earth with full end-to-end connectivity(about 32 addresses per square inch of dry land).In addition IPv6 is designed to support IPSec,Scalability,Multimedia transmissions,Security,Routing, Mobility, Real time applications like audio,Video,Cryptography techniques like encryption and Decryption, Large address space, Better support for QoS.

1.2. Data Link and Transport layer error handling function.

In this paper the performance of a network can be measured in terms of many ways by using transit time and the response time. The transit time (TT) can be defined as the amount of time for message to travel from one source node (end node) to destination node (another end node).Whereas the response time (RT) can be defined as elapsed time between an inquiry and response. Like any computer system, however computer networks are also expected to perform well, since the effectiveness of computations distributed over the network often depends directly on the efficiency with which the network delivers the computation's data. It is therefore important to understand the various factors that impact network performance. Network performance can be measured in two fundamental ways like bandwidth (Throughput) and Latency (delay).The bandwidth can be defined as the number of bits that can be transmitted over the network in a certain period of time. For logical process to process channels bandwidth is also influenced by the other factors like how many times the software that implements the channel has to be handling and possibly transform each bit of a data. First of all the bandwidth can be defined as the literally a measure of the width of a frequency band. The second one more important performance metric is latency. Latency corresponds to how long it takes a message to travel from one end of a network to the other. Latency can be measured strictly in terms of time. The Total latency (TL) is made up of three important components.

Total Latency (TL) = Propogation+Transit+Queue.

Where Propagation=Distance/Speed of Light, and Transmit=Size/Bandwidth.

Where Distance is the length of the wire over which the data will travel, Speed of light is the effective speed of light over that wire, Size is size of the packet, and Bandwidth is the bandwidth at which the packet is transmitted. Bandwidth and Latency combined to define the performance characteristics of a given channel. The fourth one more important characteristic feature is RTT (Round –trip time) which is defined as the "The packet which takes transit time in bidirectional manner".

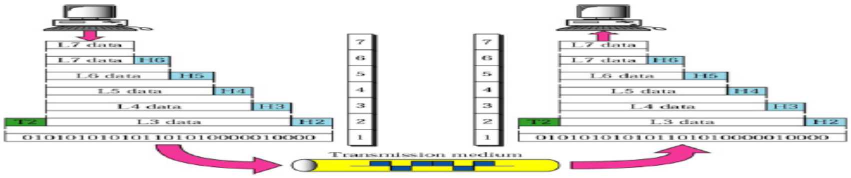


Fig.1: An Exchange using the OSI model

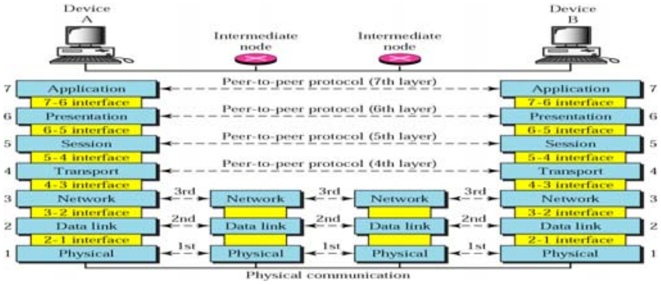


Fig.2: The Interaction between layers in the ISO/OSI model.

1.3. Layered architecture.

The OSI model is composed of seven ordered layers, Physical(layer1),DataLink(layer2),Network(layer3),Transport(layer4),Session(layer5),Presentation(layer6),Application(layer 7).To reduce the design complexity, computer networks follow a layered architecture[1].Each layer clearly defines based on the previous layers and has a set of well defined functions with clear cut boundaries .Also with layered architecture the implementation details of each layer is independent of other layers.Fig.2.shows the layers involved when a message is sent from device A to device B.As a message travels from A to B it may pass through many intermediate nodes. These intermediate nodes usually involved only the first three layers of OSI model. Each layer defines a family of functions distinct from those of the other layers. By defining and localizing functionality in this fashion, the designers created an architecture that is both comprehensive and flexible. Most importantly the ISO/OSI model allows complete interoperability between otherwise incompatible systems. Within a single machine, each layer calls upon the services of the layer just below it. The processes on each machine that communicates at a given layer are called peer-to-peer processes. The passing of the data and network information down through the layers of the sending device and back up through the layers of the receiving device is made possible by an interface between each pair of adjacent layers. Layers 1, 2 and 3–physical, data link and network are the network support layers. Layers 5, 6, and 7–session, presentation and application can be thought of as the user support layers. The upper OSI layers are almost always implemented in software; lower layers are a combination of hardware and software except for the physical layer, which is mostly hardware. In Fig.1.which gives an overall view of the OSI layers, D7 means the data unit at layer 7.The process starts at layer 7,then moves from layer to layer in descending, sequential order. At each layer commonly a header or trailer can be added to the data unit. At each layer the packet is encapsulated with a header that contains control information to handle the data received at other side by the corresponding layer. This paper also states that how to take care of error handling function very efficiently by reducing the overall packet processing time, and thus improve the transmission of IPv6 packets. This can be achieved by utilizing the characteristics or capabilities of the communication medium used to transfer data, and by improving the existing error handling mechanisms at the lower layer. In Data communication and networking and computer networks the errors are broadly divided into single bit error and Burst errors. The term single-bit error means that only 1 bit of a given data unit (such as a byte, character or packet)from 0 to 1.The Fig.4.shows Burst error with Length 5.The most important common approaches to detect the errors are parity check(PC),Cyclic redundancy check(CRC) and Checksum.[17][19].

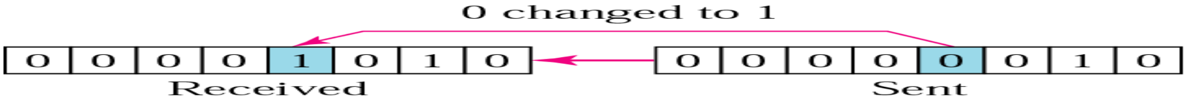


Fig.3: Single-bit error.

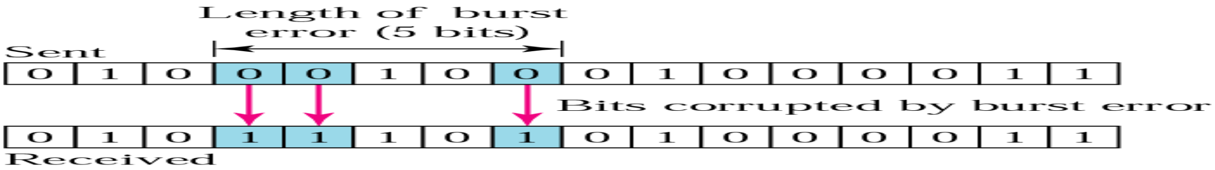


Fig.4: Burst error of Length 5.

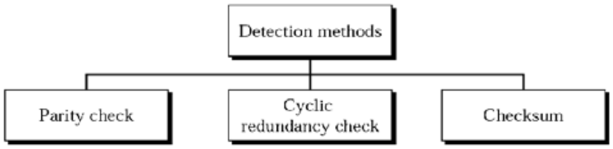


Fig.5: Error Detection methods.

The errors that are detected by either redundancy, parity check, or cyclic redundancy check, or checksum can be corrected by with two types of mechanisms called Automatic repeat request(ARQ),and Forward error correction(FEC).This paper is organized as follows: We briefly described Introduction to IPv6 in 4G networks and its on-going work in Section 1.We described,IPv6 transition in terms of 4G in section-2.Section-3 clearly specifies related work meant for the translation of IPv4/IPv6 BD-SIIT a novel transition algorithms. Finally we concluded the whole paper in section 4.The ISO/OSI and TCP/IP are the two most important popular network architectures that have been widely used. The ISO/OSI reference model has remained as a popular model for its simplicity, and clarity of its functions where the TCP/IP was a more working model that is popularly used over the Internet. The Fig.6.shows the Transport layer communication process. The data from the user on the sender side, passes through a series of layers before it is transmitted over the internet to reach the other machine(recipient side).On the receiver side data received by the Physical layer goes up to the application layer, by neglecting the header in each layer. It can be observed from the Fig.6.the original length of the data remains same, but the length of the header increases with each layer.

II. Background and Related work.

2.1. The ISO/OSI Packet Transmission

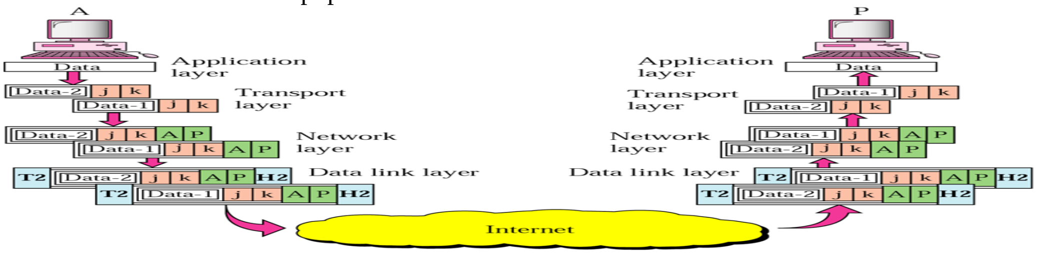


Fig.6: The Transport layer communication process.

2.2. *IPv6 Packet format and Ethernet Frame Format (IEEE 802.3)*

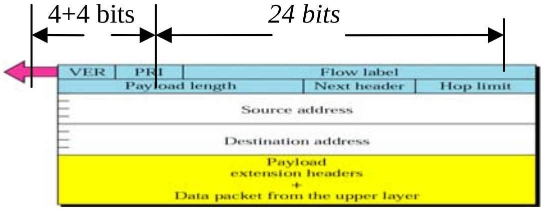


Fig.7: The IPv6 Packet format.

The IPv6 packet consists of IPv6 base header, extension headers, and upper layer protocol data unit.IPv6 base header is of fixed size, and is of 40 bytes in length. Payload length may change due to the presence of extension headers. The IPv6 packet format can also support for multiple extension headers and the use of extension header is optional. The IPv6 based header consists of 8 fields as shown in the Fig.7.Extension headers are inserted into the packet only if options are needed. All the 8 fields are processed according to their sequential order. The Fig.8.clearly shows an Ethernet format. The Ethernet is most easily and successful local area networking technology and is developed in the year 1970 by research innovators at the Xerox Palo Alto research center(PARC).It is also a working example of the more general CSMA/CD local area working technology. The Ethernet frame consists of 64 bits preamble(7 Bytes of preamble and 1 Byte SFD)which allows the receiver to synchronize with the signal(which represents a sequence of alternating 0's and 1's).The Source and Destination addresses are represented with a 48 bits address. The length of protocol data unit is 16 bits and each contains up to 1500 bytes of data, minimally a frame must contain at least 46 bytes of data, even if this means the host has to pad the frame before transmitting it. One of the reasons for this smallest size frame must be long enough to detect a collision.

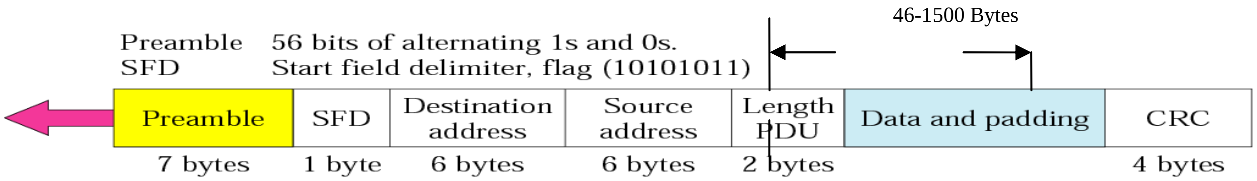


Fig.8: The Ethernet Frame Format.

.

2.3. *Error handling aspects and its issues by using CRC in Data link layer.*

It should be clear by now that a major goal in designing error detection algorithms is to maximize the probability of detecting errors using only a small number of redundant bits. Cyclic redundancy checks can use fairly small mathematics to achieve this goal.CRC is one of the most popular error detection mechanism that is currently being used at data link layer. Cyclic codes are special linear block codes with one extra property. In a cyclic code if a code word is cyclically shifted then the result is another code word. For ex–if a 1011000 is a code word and when cyclically left shifted then 0110001 is also a code word.

2.4. *Cyclic redundancy check.*

CRC is a cyclic code method to correct errors in networks like LAN and WANs.CRC is a popular method used simple to implement in binary hardware, and easy to analyze mathematically and are particularly good at detecting common errors caused by noise in transmission channels. In our proposed method by removing CRC from the Ethernet frame format and fix it in the IPv6 packet format of the extension header at network layer of ISO/OSI model. The Fig.9.shows the novel IPv6 packet format [25].

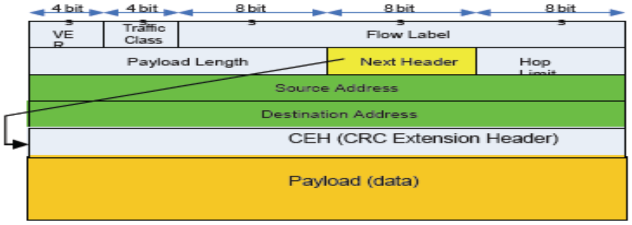


Fig.9:IPv6 new packet format with CEH (Cyclic redundancy check Extension Header).

2.5. *Applications of CRC.*

1.Cyclic codes performing very good performance in detecting single-bit errors, double errors, an odd number of errors, and burst errors.
2. CRC is easy to implement in hardware and software.
3. CRC is very fast to correct errors when implemented in hardware.
4. Cyclic code has made a good candidate for many networks [25]

III.Deploying IPv6 over Fiber optic link.

3.1. *Introduction to Fiber optic links.*

Fibre optic link is a High speed serial interface technology that supports various upper layer protocols, including small computer system interface(SCSI) and IPv4.Fibre channel is a gigabit speed network technology, primarily used for storage networking.Fibre optic link is standardized in the T11 technical committee for information technology . standards(INCITS) and ANSI accredited standards committee. The resources which belong to a Fibre optic links are called as nodes. Each resource connected to a network has one or more port addresses that connect to ports of other devices.Fibre optic links are implemented using any combination of the following three topologies.

1. A point-to-point link between two port addresses.
2. A set of ports interconnected by using a switching network called as Fibre.
3. A set of ports interconnected with a loop topology.

3.2. *Types of Fibre optic link ports*.

Fibre optic ports are broadly divided into two types.1.Node port (N_port), 2.NL_port:-A node which is capable of operating in a loop topology using the loop specific protocols.3.Fabric port (F_port), 4.FL_port.4.Fibre optic link Frame format.

SOF	FC Header	Data Field		CRC	EOF
		Optional Header(OH)	Frame Payload.		

Fig.10.Fibre channel Frame format.

The Fibre optic link format is depicted in Fig.10.The Start of Frame (SOF) and End of Frame (EOF) are special transmission Fibre link words that act as Frame delimiters. The CRC is 4 Octets long and uses the same 32-bit polynomial used in FDDI.The FC Header is 24 octets long and contains various fields associated with the identification and control of the data field. The data field is type variable size which ranges from 0 to 2112 octets and includes the user data in the Frame payload field and optional headers. The optional defined header contains ESP_Header, Network_Header, Association_Header, Device_Header etc.

In this, paper we considered to place error detection in the network layer to check IPv6 whole packet including header and payload. The error detection (check) method used will be same as CRC method that is currently being used with the existing systems. The CRC extension header (CRCEC) is a new IPv6 extension header to handle error detection for the entire IPv6 packet shown in Fig.9.

Simulation Scenario-1: The first simulation states that when sender generates an IPv6 packet, and the corresponding FIPv6EC (CRCEC) code to be inserted to the IPv6 packet format as CRCEC.The packet with CRCEH is sent through a network with a topology as mentioned in Fig.10.The routers are mainly used to connect sender host and a recipient host will not verify the FIPv6H (CRCEH) instead it will identify the next route of the packet. When the receiver upon receiving the packet will verify the CRCEH (FIPv6EH) in its network layer to check whether the packet is error free, and then deliver to the upper layers. If suppose the received packet contains an error it will be discarded and wait for retransmission [21].

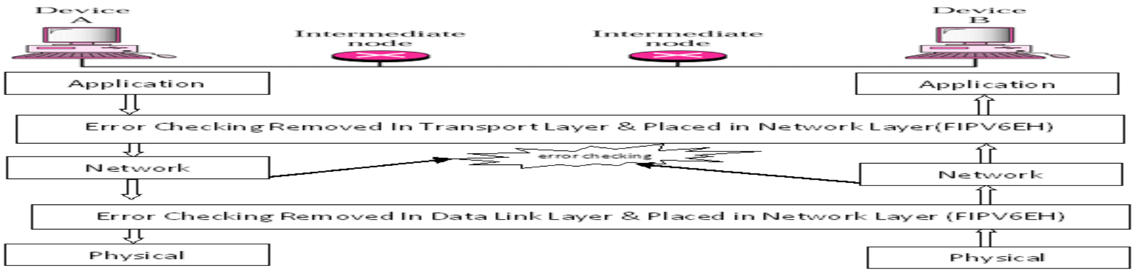

Device A
Intermediate node
Intermediate node
Device B
Application
Application
Error Checking Removed In Transport Layer & Placed in Network Layer(FIPV6EH)
Network
error checking
Network
Error Checking Removed In Data Link Layer & Placed in Network Layer (FIPV6EH)
Physical
Physical

Fig.10: Novel FIPv6EH Error detection model in Network Layer behalf of Data link and Transport Layer.

Simulation-2: Second simulation also covers error control in data link layer, the sender generates the IPv6 packet without, any extension header inside. It is embedded in data link layer with header and trailer. The FCS in the trailer is actually CRC-32 code generated from the whole frame. The Fig.10.shows when the intermediate node-1 which is also called router-1 receives a packet, and verifies the CRC code inside, when the verification process generated no code in the packet then only the packet is processed to next router-2 of a network layer. . Each time the bad packets are rejected and then the receiving station will be waiting for the retransmission of a packet. This process will continue in all the intermediate routers, which connects the sender with receiver. We have analyzed from the simulation-1 and Simulation-2 there is no error control in data link layer and Transport layer and it takes place only at the end workstations, and will not be done at every routers. The Fig.11.clearly specifies what IPv6 is over Fibre

Fig.11:IPv6 over Fibre.

IV. **Effectiveness Evaluation Metrics and Simulation Parameters.**

In this paper we have calculated two performance evaluation metrics like throughput, end-to-end delay. The throughput can be calculated as follows. The throughput is a measure of how fast we can actually send data through a network. Although at first glance throughput and bandwidth in bits per second seem the same, but totally there are different. The bandwidth is a total measurement of a link; the throughput is an actual measurement of how fast we can send data. We measured the throughput performance metric value in order to find out the rate of received and processed data at the router (intermediate device) during the time of simulation. The mean throughput for a sequence of packets of specific size can be calculated by using the formula.

$$MeanThr = \sum_{i=1}^{n} \frac{Thri}{N} \quad \text{----- (1)}$$

Whereas

$$Thri=P_{accept}/P_{created}*100\ \%\text{----(2)}$$

where P_{accept} =Packet accepted and $P_{created}$=Packet created. Where Thr_i is the throughput value when the packet “i” is accepted at the intermediate device like router. and “n” is the total number of packets received packets at the router, and P_{rec}

is the number of received packets at router and P_{crea} is the number of packets created by the source hosts, and the mean throughput is the mean value for each communication.

Latency (Delay):

The latency or delay defines how long the entire message takes to completely arrive as at the destination from the time the first bit is sent out from the source. Therefore we can conclude latency is made up of four important components: Propagation time, Transmission time, Queuing time and Processing delay.

Delay = Propagation time (Pt) +Transmission time (Tt) + Queuing time (Qt) +Processing delay (Pd).
Where Pt=Distance/Propagation speed.
Transmission Time =Message Size/Bandwidth.
Queuing time=Time needed for each Intermediate or n devices to hold the message before it can be processed

5.1. Simulation Results.

The below Table-1 shows the Simulation results that are mainly used to calculate, the Performance measurements using the NS-2 Simulator. The Simulation parameters as shown below.

Simulation Parameters	Value
1.Buffer Size	200 packets
2.Delay	5ms
3.Pay load size	100 Bytes
4.Vary traffic load	6~ 150 nodes.
5.Queue management Scheme	Drop tail

Table-1: Simulations parameters in NS-2.

5.1.1. ***Calculation of processing Time of CEH.***

The Fig.12. Shows that CEH totally dependent on the existing CRC-32 generator code which is standardized by IEEE 802.3 for Ehernet.It also clearly specifies rapport which exists between the Processing time of IPv6 packets with CEH and IPv6 packet size. By analyzing Fig.12.It can be seen that the processing time of IPv6 with CEH increases with the IPv6 packet length. The Figure.13.shows that there various differences between processing time required for the first IPv6 packet and the correlation exists between processing time and a packet sequence shows that it is negative exponential.ie the processing time of successive packets is smaller both sender side and receiver side.

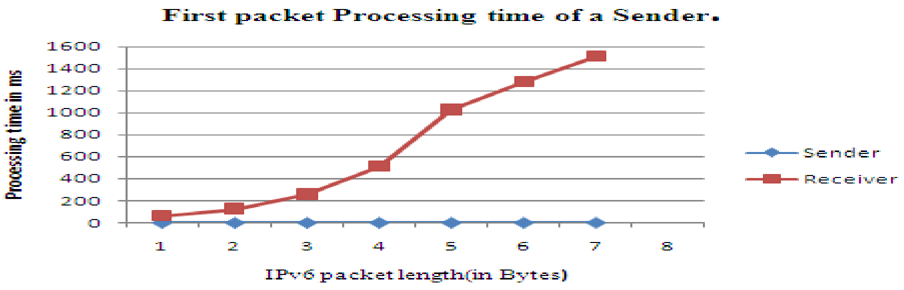


Fig.12.Calculation of processing time of IPv6 Vs CEH.

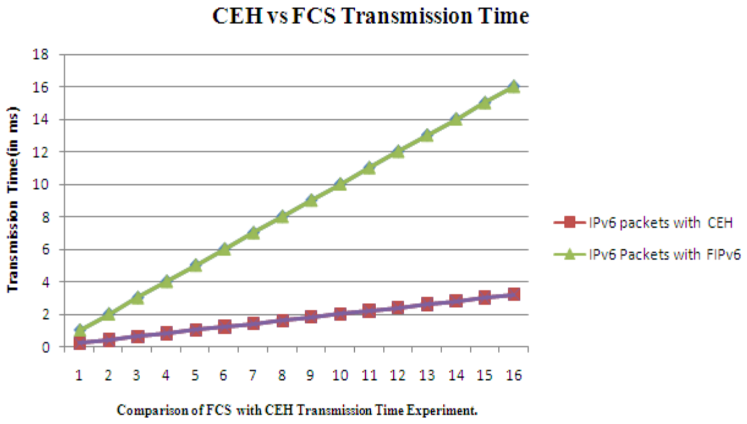
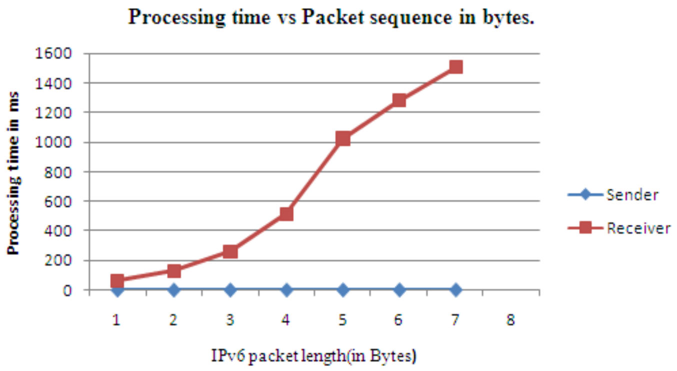


Fig.13.Comparison and Contrast between Transmissions between CEH vs. FCS Transmission Time.



V. Issues, Challenges, Impact of IPv6 over Fibre on Hardware and Software.

5.1. Challenges of IPv6 over Fibre (FIPv6)

1. To minimize the header overheads by handling efficiently similar or redundant functionalities among layers.
2. To maximize the performance of data transmission in terms of packet data rate, throughput, and bandwidth utilization.
3. To maximize the efficiency of operations for data transmission.
4.To propose a new new frame work by simplifying the existing network models like ISO/OSI and TCP/IP model through possible changes in data link layer and network layer.
5. By collapsing data link layer and network layer for similar functions and try to eliminate redundant functions.
6. It is also possible to enhance performance of IPv6 packet transmission in terms of frame rate, throughput and bandwidth.
7. To Simplify the ISO/OSI layered architecture by reducing the size of the data link layer header or removing it completely [21].

*5.2. **Necessity of IPv6 over Fibre**.*

1. Ellimination of MAC addresses.
2. Discard data Link layer.
3. No framing process.
4. Increase speed transfer.
5. Reduce worm and virus outbreak.
6. Efficiency can be increased and Buffering can be reduced.
7. ARP currently being used is not required.
8. Data is encapsulated into many headers.

9.26 bytes of Data Link Layer header for each frame. Max data size in each frame is 1500 bytes. Some amount

Of frame size is allocated for the headers and it is waste of bandwidth [21].

*5.3. **Impact of IPv6 over Fibre on Hardware**.*

The impact of IPv6 over Fibre can updates some of the changes in hardware. The following are some of the changes in IPv6 over Fibre.

1. Only drivers can be re-written for NIC.No changes required for manufacturing NIC.
2. Layer 2 switches will be obsolete or will have to run dual stack.
3. Layer 3 switches will experience faster packet processing
4. Routing Table will consist of IPv6 Address and smaller routing table entry.
5. No MAC address to IP mapping is required resulting in router performing faster and more efficient [21].

*5.4. **Impact of IPv6 over Fibre on Dual Stack.***

1. Once a new architecture is in its place, a dual stack is required to process the packets transmitted from both current architecture as well as new architecture.
2. The initiated protocol will automatically choose the appropriate stack.
3. This will be an international standard to be used by all Internet applications especially for real time applications.

VI. Conclusions.

A comprehensive research has been carried out on the enhanced performance of IPv6 over Fibre.This research is just a very good attempt to show the current scenario of the impact of the role of IPv6 over Fibre.In this paper we have presented innovative ideas, facts, and research challenges related to IPv6 packets over Fibre optic links. The proposed teaches us how we can do error handling only in network layer instead of data link and transport layer in ISO/OSI reference model by utilizing the capabilities and various features of the IPv6 protocol and the salient features of High speed data networks communication medium namely IPv6 over Fibre.The proposed concept would increases the network performance of IPv6 packet transmission and it also reduces the overhead in terms of header processing at data link layer and transport layer. The error handling concept in transport layer takes place from process to process where as in data link layer it takes place from node to node between sender and receiver host.

References

[1] Hanumanthappa.J.,Manjaiah.D.H.,Vinayak.B.Joshi.,"*A Study on IPv6 in IPv4 Static Tunneling threat issues in 4G Networks using OOAD Class and Instance Diagrams"*, Proceedings of the International Conference on Emerging Trends in Computer Science, Communication and Information Technology,(CSCIT2010)organized by Dept of CS and Information Technology,Yeshwanth Mahavidyalaya,Nanded,Maharastra,INDIA, January 09-11,2010,[Paper code CSCIT-152][CSCITOP113].

[2] Hanumanthappa.J.,Manjaiah.D.H.,Vinayak.B.Joshi.,"*An IPv4-to-IPv6 threat reviews with dual stack transition mechanism considerations a transitional threat model in 4G Wireless networks* "Proceedings of the International Conference on Emerging Trends in Computer Science, Communication and Information Technology,(CSCIT2010)organized by Dept of CS and Information Technology,Yeshwanth Mahavidyalaya,Nanded,Maharastra,INDIA,January 09-11,2010,[Paper code CSCIT-157] [CSCITOP115].

[3] Hanumanthappa.J.,Manjaiah.D.H.,Vinayak.B.Joshi.,"*Implementati on,Comparative and Performance Analysis of IPv6 over IPv4 QoS metrics in 4G Networks: Single-source-destination paths Delay, Packet Loss Performance and Tunnel Discovery Mechanisms"*, Proceedings of the International Conference on Information Science and Applications(ICISA-2010)organized by Dept. of Master of Computer Applications,Panimalar Engineering College,Chennai-600 123,Tamilnadu,India.,February-06-2010,[Paper code ICISA-293(with serial no-101)].

[4] Hanumanthappa.J., Manjaiah.D.H, Vinayak.B.Joshi, *" High Performance evaluation of Multimedia Video Streaming over IP networks"*, Proceedings of the National conference on Computing communications and Information systems(NCCCIS-2010)organized by Department of Information Technology Sri Krishna College of Engineering and Technology,Kuniamuthur,Coimbatore-641008,INDIA,February-12-13,2010,[Paper id NCCCIS-MM-03],pp-88-92.

[5] Hanumanthappa.J.,Manjaiah.D.H,Aravinda.C.V. *"IPv6 Tunneling Algorithms in 4G Networks*", Proceedings of the National conference on KNOWLEDGE,KNOWLEDGE BANKS AND INFORMATION NETWORKING (KKBNET-2010) organized by National Institute of Technology(NIT),Karnataka,Surathkal,INDIA,April,8th and 9th 2010.

[6] Sridevi.,Hanumanthappa.J.,Manjaiah.D.H,"*A Novel IPv4/IPv6 Transition scenarios in 4G Networks*", Proceedings of the National conference on KNOWLEDGE,KNOWLEDGE BANKS AND INFORMATION NETWORKING(KKBNET-2010),organized by National Institute of Technology(NIT),Karnataka,Surathkal,INDIA,April,8th and 9th 2010.

[7] Hanumanthappa.J.,Manjaiah.D.H,Aravinda.C.V.,"*A Comparison of Performance evaluation metrics and Simulation parameters*", Proceedings of the National conference on KNOWLEDGE,KNOWLEDGE BANKS AND INFORMATION NETWORKING(KKBNET-2010), organized by National Institute of Technology (NIT), Karnataka,Surathkal,INDIA,April,8th and 9th 2010.

[8] Hanumanthappa.J.,Manjaiah.D.H.,*"IPv6 and IPv4 Threat reviews with Automatic Tunneling and Configuration Tunneling Considerations Transitional Model: A Case Study for University of Mysore Network"*, International Journal of Computer Science and Information(IJCSIS)Vol.3.,No.1,July-2009,ISSN 1947-5500,Paper ID: 12060915]

[9] Hanumanthappa.J.,Manjaiah.D.H.,*"Transition of IPv4 Network Applications to IPv6 Applications"[TIPv4 to TIPv6]*,Proceedings of IEEE International Conference on emerging,trends,incomputing(ICETiC-2009), Virudhunaga Tamilnadu,8-10,January 2009, INDIA. [Paper ID 234].

[10] Hanumanthappa.J. Manjaiah.D.H. Thippeswamy.K. *"IPv6 over Bluetooth: Security Aspects, Issues and its Challenges"*, Proceedings of National Conference on, Wireless Communications and Technologies(NCWCT-09)-Theme: Mobile and Pervasive Computing**,** Nitte, Karnataka,Udupi Dist, Karnataka ,INDIA,February-5-6 **,** 2009,[Paper id -104]

[11] Hanumanthappa.J. Manjaiah.D.H. Kumar.B.I.D. *"Economical and Technical costs for the Transition of IPv4–to-IPv6 Mechanisms[ETCTIPv4 to ETCTIPv6]"*,Proceedings of National Conference on Wireless Communications and Technologies(NCWCT-09)-Theme: Mobile and Pervasive Computing**,**Nitte ,Karnataka,Udupi Dist,Karnataka,INDIA,February-5-6 **,**2009,[Paper id -103]

[12] Hanumanthappa.J. Manjaiah.D.H**.** Tippeswamy.K. *"An Overview of Study on Smooth Porting Process Scenario during IPv6 Transition" [TIPv6]*, Proceedings of IEEE International Conference on the IEEE International Advance Computing Conference IACC-2009 on March 5-8 at Patiala, Punjab [Paper ID IEEE-APPL-1278].

[13] Hanumanthappa.J. Manjaiah.D.H. Tippeswamy.K. "*IPv6 over IPv4 QoS metrics in 4G Networks: Delay, Jitter, Packet Loss Performance, Throughput and Tunnel Discovery Mechanisms",* Proceedings of the National Conference on Wireless Networks-09(NCOWN-2009) , RLJIT,Kodigehalli, Doddaballapur,Karnataka, INDIA, November 21-22nd ,2009,[Paper code NCOWN-19].

[14] Hanumanthappa.J.,Manjaiah.D.H.,"*A Study on Comparison and Contrast between IPv6 and IPv4 Feature Sets"* Proceedings of International Conference on Computer Networks and Security(ICCNS-2008),Pune,Sept 27-28th,2008,[Paper code CP 15].

[15] Hanumanthappa.J., Dr.Manjaiah."A Comparative and Behavioral Performance evaluation and analysis of a Novel IPv4/IPv6 Transition Mechanisms-BD-SIIT vs. DSTM in 4G Advanced wireless Technologies",Proc of First International Conference on Integrated Computing (ICIIC2010),Conducted by Dept of CS and IS, SJBIT,Kengeri,Bangalore,INDIA,August-05-07,2010(paper id-ICIIC-2010-114).

[16] Larry L.Peterson and Bruce S.Dave., "Computer Networks a System approach", 4th edition.

[17] Leon–Garcia, Widjaja "Communication Networks, Fundamental concepts and Key Architectures", Tata McGraw-Hill edition.

[18] S.Deering and R. Hinden "Internet Protocol Version 6(IPv6) Specification", RFC 2460, December 1998.

[19] J.Postel, INTERNET PROTOCOL, RFC 0791, September 1981.

[20] S.Tanenbaum, "Computer Networks", Third Edition, Prentice Hall Inc., 1996, pp.686, 413-436,437-449.

[21] Behrouz A.Forouzan, Third Edition, "TCP/IP Protocol Suite".

[22] Atul Kahate, "Cryptography and Network Security", Tata McGraw-Hill, 2003, pp-8-10.

[23] Kurose.J. & Ross.K. (2005)Computer Networking: A top-down approach featuring the Internet.3rd ed, (Addison Wesley).

[24] S.Hagen:"IPv6 essentials", Orielly, July 2002, ISBN-0-5960-0125-8.

[25] Behrouz A Forouzan, Fourth edition Data communication and Networking, pp-7-8.

Author's Profile.

Hanumanthappa.J is Senior. Asst. professor at the DoS in CS, University of Mysore, Manasagangothri, Mysore-06 and currently pursuing PhD in Computer Science and Engineering, from Mangalore University under the supervision of Dr.Manjaiah.D.H on entitled "Design and Implementation of IPv6 Transition Technologies for University of Mysore Network (6TTUoM)". His teaching and Research interests include Computer Networks, Wireless and Sensor Networks, Mobile Ad-Hoc Networks, Intrusion detection System, Network Security and Cryptography, Internet Protocols, Mobile and Client Server Computing, Traffic management, Quality of Service, RFID, Bluetooth, Unix internals, Linux internal, Kernel Programming, Object Oriented Analysis and Design etc.His most recent research focus is in the areas of Internet Protocols and their applications. He received his Bachelor of Engineering Degree in Computer Science and Engineering from University B.D.T College of Engineering ,Davanagere,Karnataka(S),India(C),Kuvempu university, Shimoga in the year 1998 and Master of Technology in CS&Engineering from NITK Surathkal,Karnataka(S),India (C) in the year 2003.He has been associated as a faculty of the Department of Studies in Computer Science since 2004.He has worked as lecturer at SIR. M. V. I. T, Y. D. I. T ,S.V.I.T,of Bangalore. He has guided about 250 Project theses for BE,B.Tech,M.Tech,MCA,MSc/MS.He has published about 15 technical articles in International, and National Peer reviewed conferences. He is a Life member of CSI, ISTE,AMIE,IAENG,Embedded networking group of TIFAC–CORE in Network Engineering,ACM,Computer Science Teachers Association (CSTA) , ISOC, IANA, IETF, IAB,IRTG,etc.He is also a BOE Member of all the Universities of Karnataka,INDIA.He has also visited Republic of China as a Visiting Faculty of HUANG HUAI University of ZHUMADIAN,Central China, to teach Computer Science Subjects like OS and System Software and Software Engineering, Object Oriented Programming With C++,Multimedia Computing for B.Tech Students. In the year 2008.He has also visited Thailand and Hong Kong as a Tourist.

Dr.Manjaiah.D.H . is currently Reader and Chairman of BoS in both UG/PG in the Computer Science at Dept.of Computer Science, Mangalore University, and Mangalore. He is also the BoE Member of all Universities of Karnataka and other reputed universities in India. He received PhD degree from University of Mangalore, M.Tech. From NITK, Surathkal and B.E., from Mysore University.Dr.Manjaiah.D.H D.H have an **extensive** academic, Industry and Research experience. He has worked at many technical bodies like IAENG, WASET, ISOC, CSI, ISTE, and ACS.He has authored more than 40 research papers in international conferences and reputed journals. He is the recipient of the several talks for his area of interest in many public occasions. He is an expert committee member of an AICTE and various technical bodies. He had written Kannada text book, with an entitled, "COMPUTER PARICHAYA",for the benefits of all teaching and Students Community of Karnataka.Dr.Manjaiah D.H's areas interest are Computer Networking & Sensor Networks, Mobile Communication, Operations Research, E-commerce, Internet Technology and Web Programming.

Aravinda.C.V. currently pursuing M.Tech (I.T) K.S.O.U., Manasagangotri, Mysore-06.He as received M.Sc., M.Phil in Computer Science. He has worked as a Lecturer in the following institutions.1. CIST, Manasagangotri, Mysore, 2. Vidya Vikas Institute of Engg and Technology, Mysore.3.Govt First Grade college, Srirangapatna and Kollegal. & Technical Coordinator for NIIT Bangalore.

He has published two papers in National Conference hosted by NITK, Surathkal at Mangalore. And at Vellamal Engineering,College,Madurai,ICCCI,2010,PESIT,ICEMC220 10Kupam,And ICICI2010.