International Journal of Engineering Research in Electronic and Communication Engineering (IJERECE) Vol 1, Issue 1, December 2014

IPV4 to IPV6 Transition Complaint Media Streaming Using Arm 11

[1]Manju Priya G,[2]K. Rajasekar M.Tech
[1]P G Scholar [2]Assiant Professor
Department of Communication Systems,
Sree Sastha Institute of Engineering and Technology, Chennai (India

Abstract*—Internet Protocol version 6 (IPv6) is the next version of Internet Protocol (IP) which is currently in the transition phase from its predecessor, Internet Protocol version 4 (IPv4). With the number of IPv4 addresses almost completely depleted, the implementation of IPv6 has become a priority for many organizations. However, it is not all that feasible to just switch everything over to IPv6 without some type of transition. This project reconsiders the basic problems and key differences in IPv4-Ipv6 transition. IPv6 transition mechanisms are the technology that facilitates the transition of internet from its initial and current IPv4 infrastructure to the successor addressing and routing system of IPv6 (Internet Protocol Version 6). As IPv4 and IPv6 networks are not directly interoperable, these technologies are designed to permit hosts on either network to participate in networking with the other network. To meet its technical criteria, IPv6 must have a straight forward transition plan from the current IPv4. Internet Engineering Task Force (IETF) conducts working groups and discussions through the IETF Internet Drafts (ID) and Request for Comments (RFC) processes to develop these transition technologies towards that goal. This will overcomes the issues of scalability and an another challenge is that operates are facing situations in which IPv6 only access networks are deployed but the majority of internet services remain in IPv4. Also the application layer translation is the key issues in the previous translation methods that will be analyzed and found better solution by this. ARM 11 processor design a flexible, low cost IPv4/Ipv6 converter which support the Session Initiation Protocol (SIP), Real Time Streaming Protocol (RTSP) in the IPv4 network data can be achieved through IPv6 network. It also automatically configure the routers depending on the destination network instead of manual routing. Streaming technology will be analyzed and it will be done between two or more PC (Personal Computer) in which one PC will be in IPv4 network and the other is on Ipv6 network where the Raspberry Pi will acts as the server to do the transition mechanism.
***Keywords:*Nutritional deficiency, LabVIEW, Image processing, RGB color.**

***Keywords*.IPv4, IPv6, Raspberry pi, Streaming, SIP, Transition, Auto configuration**

I. INTRODUCTION

As many are already aware, an increasingly likely candidate for the next-generation Internet Protocol is version 6 (IPv6), defined by Internet Engineering Task Force (IETF) .The proponents of IPv6 do not consider it a revolutionary protocol, designed to replace the existing IPv4, but more a long awaited improvement on the original IETF designed bac in 1981. Much of its development has been influenced by les learned is in the existing.

A. Motivation

The main motivation of this document is to provide general recommendations to be taken into account during the porting process of applications and services to IPv6. This will allow developers to move smoothly their applications into the new environment. The document is divided in three parts. The first analyzes in which conditions is possible the transition to IPv6 without changing applications. This chapter includes recommendations on how to proceed when source code is not available and explains which mechanisms can be used. The second is the main document part. It starts for characteristics, which usually should be reviewed during transition to IPv6. The document concludes providing general recommendations for new IPv6 applications. In the future all IPv4 networks will be IPv6; however during a long period mixed scenarios with both IPv4 and IPv6 will be the real environments. Therefore, new applications should designed to work only in a pure IPv6 environment, but a design to allow mixed IPv4 and IPv6 environment is better now. The PC 1 will be acting as the source and PC 2 as the destination and vice versa. The PC 1 will be having the IP (Internet Protocol) address of version 4 i.e. IPv4 address whereas the PC 2 destination will be working in IPv6 address. Both the source and the destination will be connected to a LAN (Local Area Network) with the help of router. Generally the router can be configured to any of one network either IPv4 or IPV6 but here the router can be configured to both IPv4 and IPv6 network simultaneously. This can be achieved by the Pi which provides the auto configuration depending on the end user applications.

II. BASICS OF TRANSITION FROM IPv4 TO IPv6

In order for systems to locate each other in a distributed environment, nodes are given explicit addresses that uniquely identify the particular network the system is on and uniquely identify the system to that particular network. When these two identifiers are combined, the result is a globally-unique address. This address, known as IP address as IP number or merely as IP is a code made up of numbers separated by three dots that identifies a particular computer on the internet.

These addresses are actually 32 - bit binary numbers, consisting of the two sub addresses (identifiers) mentioned above which, respectively, identify the network and the host to the network, with an imaginary boundary separating the two. An IP address is, as such, generally shown as 4 octets of numbers from 0 - 255 represented in decimal form instead of binary form. The binary number is important because that will determine which class of network the IP address belongs. The class of the address determines which part belongs to the network address and which part belongs to the node address.

A. Block Diagram of Proposed System

The block diagram of the transition system shown in the fig. 1 says that the router designed in this system will supports both of the internet protocol versions i.e. both IPv4 and IPv6 networks. And the source can forward the packet from IPv4 to IPv4 as well as IPv6 network and vice versa is also possible in this proposed system.

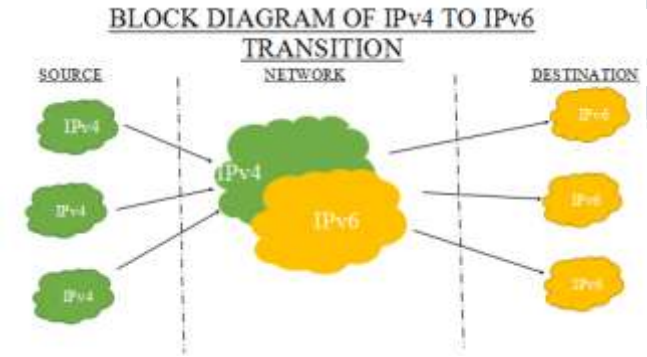

Fig. 1 Block Diagram of Proposed System

B. Working of Transition System

In this transition system the PC 1 and PC 2 will be connected to the router as well as raspberry pi processor. The PC 1 will be acting as the source and PC 2 as the destination and vice versa. The PC 1 will be having the internet protocol address of version 4 i.e. IPv4 address whereas the PC 2 destination will be working in IPv6 address. Both the source and the destination will be connected to a LAN with the help of router. Along with this Raspberry Pi will also be connected. Generally the router can be configured to any of one network either IPv4 or IPv6 but here with the help of Pi the router can be configured to both IPv4 and IPv6 network simultaneously. This can be achieved by the Pi which provides the auto configuration depending on the end user applications. Both the IP versions can be used at the same time and it will achieve the transition in a simple way without making any complex connections.

III. INTERNET PROTOCOL VERSION 4

IPv4 is the fourth version in the development of the internet protocol. Internet and routes most traffic on the internet. IPv4 is a connection less protocol for use on packet-switched networks. It operates on a best effort delivery model, in that it does not guarantee delivery, nor does it assure proper sequencing or avoidance of duplicate delivery. These aspects, including data integrity, are addressed by an upper layer transport protocol, such as the TCP.

A. IPv4 Addressing

An IPv4 addressing uses 32-bit (four-byte) addresses, which limits the address space to 4294967296 (232) addresses. As addresses were assigned to users, the number of unassigned addresses decreased. IPv4 address exhaustion occurred on February 3, 2011, although it had been significantly delayed by address changes such as class full network design, Classless Inter-Domain Routing (CIDR), and network address translation. This limitation of IPv4 stimulated the development of IPv6 in the 1990s, which has been in commercial deployment since 2006.

B. Ipv4 header format

An IP packet consists of a header section and a data section. An IP packet has no data checksum or any other footer after the data section. IPv4 packet header consists of 14 fields, of which 13 are required. The 14 th field is optional. The fields in the header are packed with the most significant byte first big endian, and for the diagram and discussion, the most significant bits are considered to come first (MSB 0 bit numbering). The most significant bit is numbered 0, so the version field is actually found in the four most significant bits of the first byte, IPv4 frame is shown in fig. 2

C.Version and Internet Header Length

The first header field in an IP packet is the four-bit version field. For IPv4, this has a value of 4 (hence the name IPv4). The second field (4 bits) is the Internet Header Length (IHL), which is the number of 32-bit words in the header. Since an IPv4 header may contain a variable number

of options, this field specifies the size of the header (this also coincides with the offset to the data). The minimum value for this field is 5, which is a length of 5 × 32 = 160 bits = 20 bytes. Being a 4-bit value, the maximum length is 15 words (15 × 32 bits) or 480 bits = 60 bytes.

D.Differentiated Services Code Point (DSCP)

Originally defined as the type of service field, this field is now defined by for differentiated services. New technologies are emerging that require real-time data streaming and therefore make use of the DSCP field. An example is Voice over IP (VoIP), which is used for interactive data voice exchange.

E.Explicit Congestion Notification (ECN)

This field is defined and allows end-to-end notification of network congestion without dropping packets. ECN is an optional feature that is only used when both endpoints support it and are willing to use it. It is only effective when supported by the underlying network.

F.Total Length

This 16-bit field defines the entire packet (fragment) size, including header and data, in bytes. The minimum-length packet is 20 bytes (20 byte header + 0 bytes data), the maximum is 65,535 bytes and the maximum value of a 16 bit word. All hosts are required to be able to reassemble datagrams of size up to 576 bytes, but most modern hosts handle much larger packets.

G.Identification

This field is an identification field and is primarily used for uniquely identifying the group of fragments of a single IP datagram. Some experimental work has suggested using the ID field for other purposes, such as for adding packet-tracing information to help trace datagrams with spoofed source addresses.

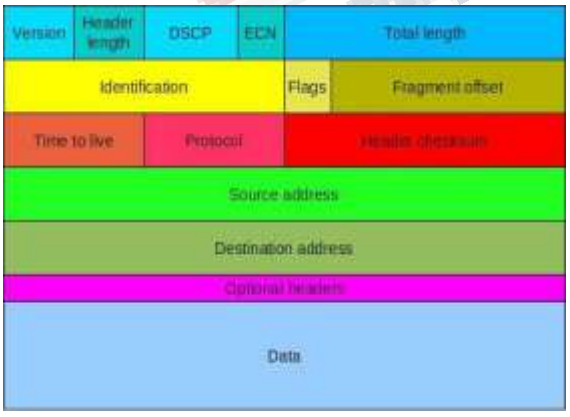

Fig. 2 IPv4 Header Frame Format

H.Source and Destination Address

This field is the IPv4 address of the sender of the packet. Note that this address may be changed in transit by a network address translation device. This destination field is the IPv4 address of the receiver of the packet. As with the source address, this may be changed in transit by a network address translation device.

IV. TRANSITION TO IPv6

The transition between today's IPv4 internet and the future IPv6 - based one will be a long process during which both protocol versions will coexist. Moving from IPv4 to IPv6 is not straightforward and guidelines to simplify transition between the two versions have to be standardized. Existing applications are written assuming IPv4. Only very recently IPv6 has been taken into account. Unless most of basic distributed applications are available now; there is too much work to do yet. The aim of this project is to provide general recommendations to be taken into account during the porting process of applications and services to IPv6. This will allow developers to move smoothly their applications into the new environment. In the future all IPv4 networks will be IPv6 however during a long period mixed scenarios with both IPv4 and IPv6 will be the real environments. Therefore, new applications should designed to work only in a pure IPv6 environment, but a design to allow mixed IPv4 and IPv6 environment is better now.

A. Internet protocol version 6 (Ipv6)

It is the latest version of the internet protocol, the communications protocol that provides an identification and location system for computers on networks and routes traffic across the internet. IPv6 was developed by the IETF to deal with the long-anticipated problem of exhaustion. The two protocols are not designed to be interoperable, complicating the transition to IPv6. However, several IPv6 transition mechanisms have been devised to permit communication between IPv4 and IPv6 hosts.

IPv6 addresses are represented as eight groups of four hexadecimal digits separated by colons, for e.g. The following are the features of the IPv6 protocol:

1. New header format
2. Large address space
3. Efficient and routing infrastructure
4. Stateless and stateful address configuration
5. Built-in security
6. Better support for prioritized delivery
7. Neighbouring node interaction
8. Extensibility

B. Ipv6 frame format

An IPv6 packet has two parts: a header and payload. The header consists of a fixed portion with minimal functionality

required for all packets and may be followed by optional extensions to implement special features in fig. 3.

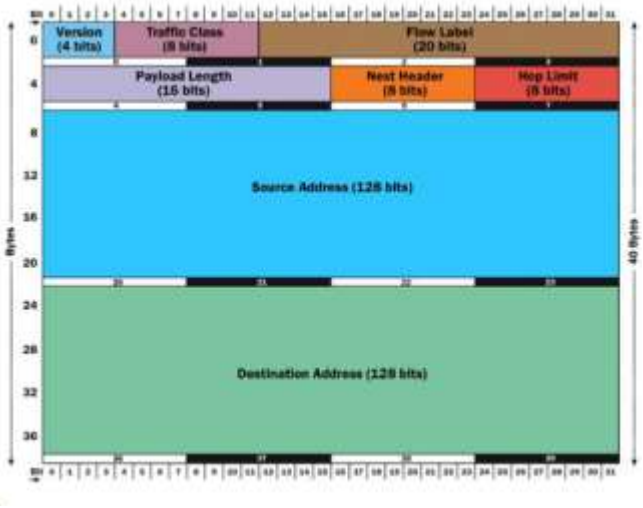

Fig. 3 IPv6 Frame Format

The fixed header occupies the first 40 octets (320 bits) of the IPv6 packet. It contains the source and destination addresses, traffic classification options, a hop counter and the type of the optional extension or payload which follows the header. This next header field tells the receiver how to interpret the data which follows the header. If the packet contains options, this field contains the option type of the next option. The next header field of the last option, points to the upper-layer protocol that is carried in the packet's payload. Extension headers carry options that are used for special treatment of a packet in the network, e.g., for routing, fragmentation, and for security using the IPsec framework.

V. PROTOCOLS USED

A. Session initiation protocol

The session initiation protocol is a signaling communication protocol, widely used for controlling multimedia communication sessions such as voice and video calls over internet protocol networks. It is widely used for initiation and for connection establishment. SIP can be used for two-party (unicast) or multiparty (multicast) sessions. Other SIP applications include video conferencing, streaming multimedia distribution, instant messaging, presence information, file transfer, fax over IP and online games. It is an application layer protocol designed to be independent of the underlying transport layer; it can run on TCP, user datagram protocol or Stream Control Transmission Protocol (SCTP).

B.Protocol Operation

SIP employs design elements similar to the http request / response transaction model. Each transaction consists of a client request that invokes a particular method or function on the server and at least one response. SIP reuses most of the header fields, encoding rules and status codes of http, providing a readable text-based format. Each resource of a SIP network, such as a user agent or a voicemail box, is identified by a Uniform Resource Identifier (URI), based on the general standard syntax also used in web services and e-mail. The URI scheme used for SIP is the form: sip:username:password@host:port.

If secure transmission is required, the scheme is used and mandates that each hop over which the request is forwarded up to the target domain must be secured with Transport Layer Security (TLS). The last hop from the proxy of the target domain to the user agent has to be secured according to local policies. TLS protects against attackers who try to listen on the signaling link but it does not provide real end-to-end security to prevent espionage and law enforcement interception, as the encryption is only hop-by-hop and every single intermediate proxy has to be trusted.

C.Working Scenario

SIP is primarily used in setting up and tearing down voice or video calls. It also allows modification of existing calls. The modification can involve changing addresses or ports, inviting more participants, and adding or deleting media streams. SIP has also found applications in messaging applications, such as instant messaging and event subscription and notification.

D.Hyper Text Transfer Protocol

The Hyper Text Transfer Protocol (HTTP) is an application-level protocol for distributed and collaborative hypermedia information systems. HTTP is a generic and stateless protocol which can be used for other purposes as well using extension of its request methods, error codes and headers. Basically, HTTP is an TCP/IP based communication protocol, which is used to deliver data (HTML files, image files, query results etc.) on the World Wide Web (WWW).

E.Basic Features

There are following three basic features which makes HTTP a simple but powerful protocol **Connection less** - The HTTP client i.e. browser initiates an HTTP request and after a request is made, the client disconnects from the server and waits for a response. The server process the request and re-establish the connection with the client to send response back.

F.Media Independent

This means, any type of data can be sent by HTTP as long as both the client and server know how to handle the data content. This is required for client as well as server to specify the content type using appropriate Multi-purpose Internet Mail Extension (MIME) type.

Stateless - As mentioned above, HTTP is a direct result that HTTP is a stateless protocol. The server and client are aware

of each other only during a current request. Afterwards, both of them forget about each other. HTTP 1.0 uses a new connection for each request / response exchange whereas HTTP 1.1 connection may be used for one or more request / response exchanges.

VI. RASPBERRY PI

The Raspberry Pi is a credit-card sized processor that plugs into television and a keyboard. It's a capable little PC which can be used for many of the things that desktop PC does, like spreadsheets, word-processing and games. It also plays high-definition video. It is being used by kids all over the world to learn programming. Combining both real-time and a time-sharing subsystem, hybrid operating systems can provide both predictable real-time task execution and non-real-time services with well-known interfaces and lots of existing applications.

The Raspberry Pi has a broad com BCM2835 system on a chip, which includes an ARM1176JZF-S 700 MHz processor video core IV GPU, and originally shipped with 256 megabytes of Random Access Memory (RAM), later upgraded to 512 megabytes. It does not include a built-in hard disk or solid-state drive, but uses a secure digital card for booting and long-term storage.

A.Software Tools

Kernel is heart of Linux Operating System (OS). It manages resource of Linux OS. Resources means facilities available in Linux. For e.g. facility to store data, print data on printer, memory and file management etc. kernel decides who will use this resource, for how long and when. It runs the programs (or set up to execute binary files). It's memory resident portion of Linux. It performs the following task.

B.Advanced Reduced Instruction Set Computer Machine

ARM11 is an Advanced RISC Architecture 32-bit RISC microprocessor family which introduced the ARMv6 architectural additions. These include Single Instruction Multiple Data (SIMD) media instructions, multiprocessor support and a new cache architecture. It delivers extreme low power and a range of performance from 350 MHz in small area designs up to 1 GHz in speed-optimized designs in 45 and 65 nm. The implementation included significantly improved instruction processing pipeline, compared to previous ARM9 or ARM10 families, and is used in smart phones from Apple, Nokia, and others. The various features in ARM are as follows

C. Raspberry pi ports

There are various hardware ports available in raspberry pi they are secure digital cards, Ethernet LAN, power supply module etc.

D. Secure Digital Card

Secure Digital or (SD) is a non-volatile memory card format for use in portable devices, such as mobile phones, digital cameras and tablet computers. The Secure Digital standard is maintained by the SD card association. SD technologies have been implemented in more than 400 brands across dozens of product categories and more than 8,000 models some are shown in fig. 4

Fig. 4 Secure Digital Cards

E. Broadcom

Broadcom Corporation is a fables semiconductor company in the wireless and broadband communication business. The company is head quartered in Irvine, California and USA. Broadcom was founded by a professor-student pair Henry Samuel and Henry T. Nicholas III from University of California, Los Angeles (UCLA) at Los Angeles, California in 1991. In 1995, the company moved from its Westwood, California, office to Irvine, California. Broadcom first landed on the fortune 500 in 2009. The Broadcom logo is inspired by the mathematical sink function.

F. Ethernet Local Area Network

Ethernets a family of computer networking technologies for LAN. Ethernet was commercially introduced in 1980 and standardized in 1985 as IEEE (Institute of Electrical and Electronics Engineers) 802.3. Ethernet has largely replaced competing wired LAN technologies. The ethernet standards comprise several wiring and signaling variants of the physical layer in use with ethernet. Systems communicating over ethernet divide a stream of data into shorter pieces called frames. Each frame contains source and destination addresses and error-checking data so that damaged data can be detected and retransmitted shown in fig. 5

Fig. 5 Ethernet Local Area Network

VII.RESULTS

In the configuration window for putty by typing the IP address in the host name block the IP will be configured to raspberry pi then the command window will be opened. Here various commands are used in each protocol to initiate the protocols. The Jitsi software window helps us to log in to the software. Then the window for the SIP account registration with the secure user identity and password will appear. It shows the status window of SIP protocol. It shows the online and offline status of the session communication by showing in the respective tab. Finally the streaming will takes place between the client and the server shown in fig. 6 shows the video streaming includes both the local live video and the remote live video.

Fig. 6 Streaming of video

VIII.CONCLUSION AND FUTURE WORK

As mentioned in the introduction, the streaming of video from the internet protocol version 4 to the IPv4 network have been shown. By extending this project the coding's for IPv4 to IPv6 transition and vice versa will be designed in the raspberry pi processor. Where the raspberry pi will acts as the gateway to convert the transition if it is needed depending on the end user applications. By using the web rtc without using internet or any application the transition will be done. It is an application independent transition of networks. This project can also be extended to applications such as

A. Video conferencing in college
B. Video conferencing in intra as well as internet

REFERENCES

1. Alain Durand (2011) 'Deploying IPv6', IEEE Internet computing Vol. 5, No. 2, pp. 79-81.

2. Baker F., Li X, and Bao C. (2011) 'Frame work for IPV4 to IPV6 translation', IETF RFC 6144.

3. Chen W.E., Taiwan I. and Ssushien (2012) 'Client based IPv4 to IPv6 transition for session initiation protocol multimedia services in next generation networks', IEEE Internet Computing RFC 2529.

4. Clercq J. and Pervost. S. (2007) 'Connecting IPv6 islands over MPLS using provider edge routers', IETF RFC 4798.

5. Cynthia E. Martin SI International Reston, VA and Jeffrey (2007) 'Internet Protocol Version 6 (IPV6) security assessment', IEEE Internet Computing RFC 2460.

6. Jianping Wu and X.Li, (2006) 'Tunnel based Ipv6 transition' IEEE Internet Computing RFC 6144.

7. Waddington and Fangzhe chang Bell Research laboratories (2011) 'Realizing the transition to IPv6', IEEE Communication magazine RFC 4291.

8. Xin Cao , DaLing Jiang and Xiufen Wang (2011) 'The design of Embedded IPv4 /IPv6 protocol converter based on ARM 9', 2nd International Conference on Digital Manufacturing &Automation vol 53 pp no 1256-1260.

9. Yongcui, Quisun, Ke Xu,Wiendong Wang, Ted Lemon (2007) 'Configuring IPv4 over IPv6 networks transitioning with DHCP', IEEE Internet Computing Vol.18, No. 3, pp. 84-88.

10. YongCui, Pengwu, Jianping Wu and Chris Metz (2013) 'Transition from IPv4 to IPv6 A state of the art survey', IEEE communication surveys and tutorials Vol. 15, No. 3, pp. 1407-1424.

11.Yungcui, Jiaunping Wu, Xing Li and Mingwei Xux (2006) 'The transition to part II the soft wire mesh framework', IEEE Internet Computing Vol. 11, No.6, pp.76-80.