International Journal on Applications in Information and Communication Engineering
Volume 1: Issue 5: May 2015, pp 53-56. www.aetsjournal.com ISSN (Online) : 2394-6237

Comparative Study of Ipv4 and Ipv6 in Wired Network

Kannan S, Balakumaran D

Abstract— A rapid growth of IP-based networks and services created the vast collection of resources. At the same time, advances in design of mobile electronic devices allowed them to reach utility level comparable to stationary, desktop computers, while still retaining their mobility advantage. These transitioning techniques dual stacks, tunneling and translation solutions that enable the gradual introduction of IPv6 support into an existing IPv4 infrastructure. Unfortunately, the base IPv4 protocol does not perform very well in stationary environments, due to lack of security and packet loss. In this paper we present an overview of the most popular and promising methods of performance of both IPv4 and IPv6 in wired networks.

Keywords— Mobile Ip, Ipv6, Ipv4, Dualstacks,Tunneling

I. INTRODUCTION

As many are already using IPv4 in wired network, in such cases, the next-generation Internet Protocol is version 6 (IPv6), defined by Internet Engineering Task Force (IETF) RFC 2373 [4]are used. The proponents of IPv6 do not consider it a revolutionary protocol, designed to replace the existing IPv4. Much of its development has been influenced by lessons learned in the existing Internet. As a technology it promises a number of advances, including:

- A larger address space.
- Flexible addressing scheme.
- More efficient packet forwarding
- Better support for mobility
- Inherent support for secure communications
- The ability to allow differentiated services
- Ease of management

Deployment of IPv6 is not going to happen overnight. Instead, the Internet will evolve toward IPv6, initially through isolated "islands and then gradual global saturation. One might envisage this evolution process to take the form of dual-stacked nodes, where every node in the Internet is both IPv4 and IPv6 capable. However, this would cause unnecessary complexity as functionality is replicated both in the network and the end systems. The transition to IPv6 is also not entirely transparent to the networking layers above IP. IPv6 addresses are longer than IPv4 addresses, requiring a change in application data structures that embed IP addresses. Consequently, application programming interfaces (APIs) must be extended to support IPv4 and IPv6, as well as the ability to select the appropriate protocol for each inter-host application communication.

In general, legacy applications written for IPv4 need to be either rewritten or bridged to support IPv6. For example, FTP embeds IP addresses in its protocol, thus requiring changes to both the client and server applications. In reality, the Internet is likely to become a complex conglomeration of different protocols. IPv4 will exist with IPv6 and other globally standardized protocols [6]. The likelihood that IPv6 will someday grow to be as prevalent as its predecessor is certainly increasing. The main reasons for this are twofold. First, the escalating number of IETF proposed transitioning mechanisms are giving network administrators an easier path to migration by permitting network nodes and more specifically applications on these nodes, to communicate with each other over a mix of end system and network device (e.g., switches and routers) capabilities. Second, specialized application domains with a respective market interest, particularly the mobile domain [2], are demanding IP features that cannot be fulfilled by IPv4, such as wider address space availability and ease of configuration.

In this paper we are mainly discuss the overview of most popular internet protocols such as IPv4 and IPv6 in wired network.

II. PROTOCOL OVERVIEW

Currently, the mobile nodes are managed by Internet Engineering Task Force (IETF).In this cases; internet protocols Ipv4 and IPv6 are used. The translation of IPv4 to IPv6 by promising three methods: *dual stacks tunneling and translation.* Dual stacks are the principal building blocks for translation of IPv6 from IPv4. Dual stacks are implemented in both the end systems and network devices. Tunneling is the encapsulation of IP address and addition of external header address. Translation refers to the direct conversion of protocols (e.g., between IPv4 and IPv6) and may include transformation of both the protocol header and the protocol payload [2].

- *Internet Protocol Version 4(Ipv4)*

Internet Protocol version 4 (IPv4) is the fourth version of the Internet Protocol (IP) in Internet, and routes most traffic on the Internet.IPv4 is described in Internet Engineering Task Force (IETF) publication RFC 791[3]. IPv4 is the most widely deployed Internet protocol used to connect devices to the

Kannan S,PG Scholar, Department of ECE,S.A Engineering College, Poonamallee-Avadi Main Road, Veeraraghavapuram, Thiruverkadu Post, Chennai-600 077 ,India (e-mail:thiru.kannanselvan@gmail.com)

Balakumaran D, Assistant Professor, Department of ECE, S.A Engineering College, Poonamallee-Avadi Main Road, Veeraraghavapuram, Thiruverkadu post, Chennai-600 077, India (e-mail:balakumaran.d@hotmail.com)

Internet. IPv4 uses a 32 -bit address scheme allowing for a total of 2^32 addresses [11]. IPv4 provides approximately 4.3 billion addresses. These addresses were assigned to users.IPv4 addresses are represented in dot decimal notation which contains four decimal numbers each ranging from 0 to 255, separated by dots, for e.g., 59.93.163.36. Each part represents 8 bits of address. In some cases IP addresses may be written in hexadecimal, octal and binary representation. The header format of IPv4 is given below:

1) IPV4 Header

VERSION 4	HEADER LENGTH 4	TYPE OF SERVICE 8	TOTAL PACKET LENGTH 16
IDENTIFICATION 16		FLAGS 3	FRAGMENT OFFSET 13
TIME TO LIVE 8	PROTOCOL 8	HEADER CHECKSUM 16	
32-BIT IPV4 SOURCE ADDRESS			
32-BIT DESTINATION ADDRESS			
(OPTIONS,IF PRESENT PADDED IF NEEDED)			
DATA			

a) *Version:* The Version field in all IPv4 packets contains the value 4 (4bits).the four bits represent the decimal numbers from 0 to 15.

b) *Header Length:* The internal HEADER LENGTH field (4 bits) indicates how long the IPv4 packet header is, 4 byte or 32 bits '**words**'. The minimum value will be allowed is 20 bytes (5 words). The maximum value allowed is 60 bytes (15 words).

c) *Type Of Service:* The Type of Service (TOS) field having 8 bits. This TOS is used to implement a fairly simple Quality of Service (QOS). QoS involves management of bandwidth by protocol, by sender, or by recipient [14]. 8 bits is not really enough to do a good job on QoS, and DiffServ is not widely implemented in current IPv4 networks.

d) *Total Packet Length:* The Total Length field having 16 bits, which contains length of the packet, including the packet header. The minimum length is 20 bytes and the maximum length is 65,535 bytes. In IPv4, it is possible for some devices to fragment packets by either host or router. Packets that are fragmented must be reassembled at destination point.

e) *Identification:* The Identification field having 16 bits which indicates original packet this fragment was from, to reassemble the fragmented packet. Each packet having unique identification value [7]. In IPv4, any node can fragment a packet. Some work suggested using the Identification field for other purposes, such as for adding packet-tracing, information to help datagrams.

f) *Flags:* The Flag field having three bits, which is used to control or identify fragment. The first bit is reserved and must be zero. The second bit is the Don't Fragment (DF) flag. The third bit is the More Fragment (MF) flag.

g) *Fragment Offset***:** The Fragment offset field having the 13 bits, which is used in reassembly of fragmented packets. It is measured in 8 byte blocks. It specifies the offset of a particular fragment relative to the beginning of the original unfragmented IP datagram.

h) *Time To Live:* The Time to Live (TTL) having 8 bits, which is used to prevent datagrams from persisting on an internet. It was intended to be lifetime in seconds, but it has come to be implemented as "hop count"[13]. This means that every time a packet crosses a switch or router, the TTL is decremented by one. If the TTL reaches zero, the packet is dropped and typically sends an ICMP Time Exceeded message to the sender.

i) *Protocol:* The protocol field having 8 bits which defines the protocol used in the data portion of the IP datagram. It also defines next header, which is found immediately after the IPv4 Packet Header.

j) *Header Checksum:* The Header Checksum field having the 16 bits, which is used for error checking of the header. The 16-bit one's complement of the one's complement sum of all 16 bit words in the header. For purposes of computing the checksum, the value of the checksum field is zero [11]. To validate the checksum, add all 16 bit words in the header together including the transmitted checksum.

k) *IPV4 Source Address:* The Source Address field having 32 bits, which contains the IPv4 address of the sender (may be modified by NAT). This can be 0. In certain cases, but it can never be a multicast address.

l) *IPV4 Destination Address:* The Destination Address field having 32 bits, which contains the IPv4 address of the recipient (may be modified by NAT in a reply packet). This can be a unicast or multicast IPv4 address, but it can never be 0**.**

2) Traffic Scenario For IPV4 In Wired Network

In this network we create a wired network traffic scenario by using tcl scripts which consist of seven nodes. The packet is transmitted from node 0 to node 5 via node 2 and node 4. The acknowledgement packet is from node 5 to node 0 via node 6 and node 1, it shows in snapshot below:

Snapshot 1:

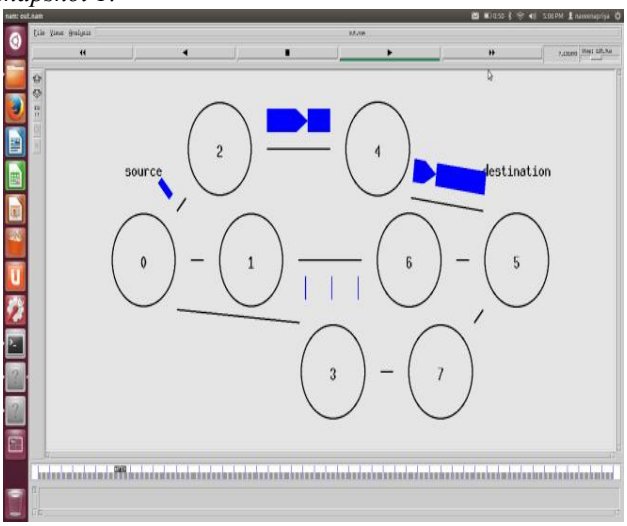


Fig. 1. Screenshot of IPv4 NAM window

In these cases we are changing the packet sizes and the time interval, it automatically changes its no of packet sends and we get the no of packet lost in data flow in IPv4 network by using Ns2, it shows in snapshot given below:

Snapshot 2:

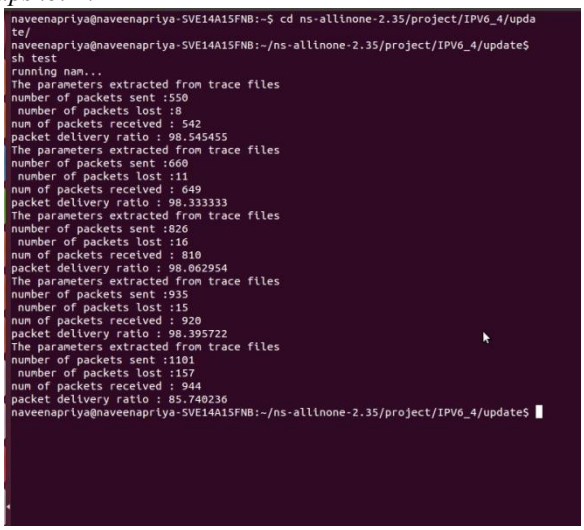


Fig. 2. Screenshot of IPv4 TERMINAL window

- *Internet Protocol Version 6(IPV6)*

Internet Protocol version 6 (IPv6) is the latest version of the Internet Protocol (IP) in Internet, and routes most traffic on the Internet.IPv6 is described in Internet Engineering Task Force (IETF) publication RFC 2460[5]. IPv6 is intended to replace IPv4, which still carries more than 96% of Internet traffic worldwide. IPv6 uses a 128-bit address supporting 2^128 (about 3.4 x 1038) addresses or more than 7.9 x 10^28 times as many as IPv4. IPv6 uses 'coloned hex' notation for address. It has 8 groups of 16 bits, each represented by hexadecimals value from 0 to 0xffff. These groups are separated by colons":" character, for e.g., 2001:0db8:0001:0002:0000:0000:0000:0013 and which compression having, 2001:0db8:1:2:: 13. Each part represents 16 bits of address. The Header format of IPv6 is given below:

1) IPV6 Header

VERSION 4	TRAFFIC CLASS 8	FLOW LABEL 20	
PAYLOAD LENGTH 16		NEXT HEADER 8	HOP LIMIT 8
128-BIT IPV6 SOURCE ADDRESS			
128-BIT DESTINATION ADDRESS			
DATA			

a) Version: The Version field in all IPv6 packets contains the 4 bit, which is for version number (0x06).

b) *Traffic Class:* The Traffic class field having 8 bits, which identifies the major class of the packet content. It forwarding routers to identify and distinguish between different classes or priorities of IPv6 traffic, in a manner identical to that of IPv4 "Type of Service".

c) *Flow Label:* The Flow Label field having 20 bits, which can be used to tag up to 2^20 distinct traffic flows. The flow label is normally 0. In the flow label information, IPv6 QoS is significantly better than that in IPv4.

d) *Payload Length:* The Payload Length field having 16 bits of length of packets in bytes, excluding the IPv6 header. The length is set to zero when a *Hop-by-Hop* extension header carries a Jumbo Payload option.

e) *Next Header:* The Next Header field having 8 bits, which specifies the type of next header immediately following the IPv6 header.

f) *Hop Limit:* The Hop Limit field having 8 bits, which replaces the TTL field of IPv4. This value is decremented by one at each intermediate node visited by the packet. When the counter reaches 0 the packet is discarded.

g) *IPV6 Source Address:* The IPv6 Source Address field having 128 bits, which indicates the IPv6 address of the sending node.

h) *IPV6 Destination Addres:* The Destination Address field having 128 bits, which indicates the IPv6 address of the destination node.

2) Traffic Scenario For IPV6 In Wired Network

In this network we create a wired network traffic scenario by using tcl scripts which consist of five nodes. The packet is transmitted from node 0 to node 2 and node 3. We create a router as node1, the packet is transmitted via router, and it shows in snapshot below:

Snapshot 3:

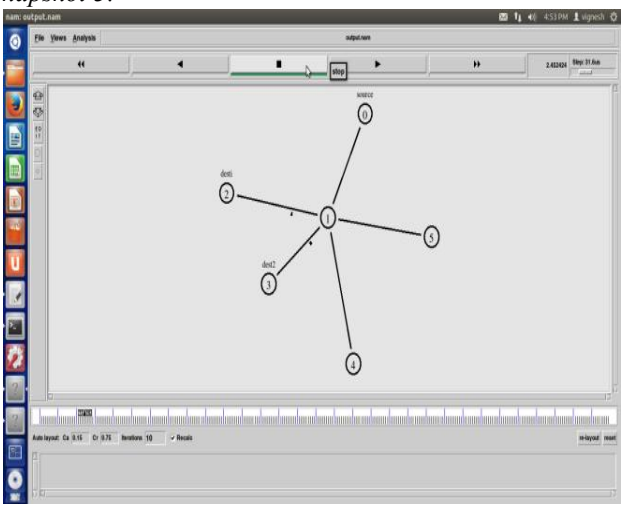


Fig. 3. Screenshot of IPv6 NAM window

In these cases we are changing the packet sizes and the time interval, it automatically changes its no of packet sends and we get the no of packet lost in data flow in IPv6 network by using Ns2, it shows in snapshot given below:

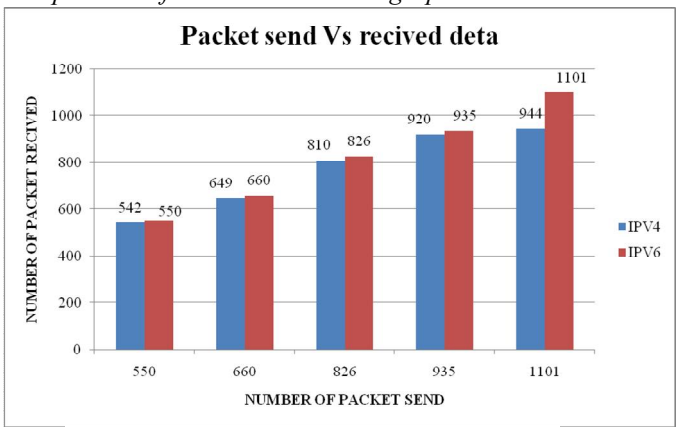
Snapshot 4:

```
channel.cc:sendUp - Calc highestAntennaZ_ and distCST_
highestAntennaZ_ = 1.5,  distCST_ = 550.0
SORTING LISTS ...DONE!
IPv6 parameters extracted
number of packets sent: 7198
number of packets lost: 0
Total no of packets successfully received is : 7198
Packet Delivery Ratio is: 100
IPv6 parameters extracted
number of packets sent: 6978
number of packets lost: 0
Total no of packets successfully received is : 6978
Packet Delivery Ratio is: 100
IPv6 parameters extracted
number of packets sent: 7599
number of packets lost: 0
Total no of packets successfully received is : 7599
Packet Delivery Ratio is: 100
IPv6 parameters extracted
number of packets sent: 8023
number of packets lost: 0
Total no of packets successfully received is : 8023
Packet Delivery Ratio is: 100
IPv6 parameters extracted
number of packets sent: 628
number of packets lost: 0
Total no of packets successfully received is : 628
Packet Delivery Ratio is: 100
vignesh@vignesh-G31M-S2L:~/ip$
```

Fig. 4. Screenshot of IPv6 TERMINAL window

III. RESULT AND CONCLUTION

Comparision of IPv4 and IPv6 with graphs



Graph .1. Packet send vs. packet received data

According to the graph IPv4 & IPv6 on the bases of Packet delivery ratio, IPv6 has some constant rate for packet delivery ratio as compared to IPv6.In these cases, IPv6 gives the 100% packet delivery ratio.

IV. CONCLUSION

In this paper firstly we analyzed the most popular and promising protocols both IPv4 and Ipv6 in wired network. There are packet loses in IPv4 network but no packet loss in IPv6 network. As a result we have more address space than IPv4 protocol. Also internet has become an integral part of 3G mobile system, which having limited address space. Besides the application requires additional demands on internet. All this has resulted in development of new protocol (IPv6), solve these problems

REFERENCES

[1] L.Jong-Hyouk, B. Jean-Marie, C.Tai-Myouny and Y. Ilsun, "Comparitive Handover Performance analysis of IPv6 Mobility Management Protocols ," IEEE Transactions on Industrial Electronics, vol. 60, no.3, March 2013.

[2] G.Daniel Waddington and C.Fangzhe, "Realizing the Transition to IPv6," IEEE Communications Magazine, June 2002.

[3] R. Marina Del, "Internet Protocol," Internet Soc., Reston, VA, IETF RFC 791, September 1981.

[4] P.Sachi and T.Vibhore, "Performance analysis of wired and wirelessnetwork using NS2 simulator," Internation Journal of Computer applications, vol. 72, no.21, June 2013.

[5] S.Deering and R.Hinden, " Internet Protocol Version 6," Internet Soc., Reston, VA, IETF RFC 2460, December 1998.

[6] D.Johnson, C.perkins, and J.Arkko, "Mobility support in ipv6," internet soc., Reston, VA, IETF RFC 3775, June 2004.

[7] R.Koodli, "Fast Handovers for Mobile IPv6," Internet Soc., Reston, VA, IETF RFC 4068, July 2005.

[8] C.Huitema, IPv6-The New Internet Protocol, 2nd ed, Prentice Hall,1997.

[9] G.walter, "Differences in Addressing between IPv4 and IPv6," Version History: First Edition, January 2014.

[10] C.Yong, W. Peng, X. Mingwie, W. Jianping, L. Yiu Lee, and M. Chris, "4over6: Network Layer Virtualization for ipv4-IPv6 Coexistance," IEEE Network, September/October 2012.

[11] M.Nicolas, and N.Thomas "Handover Management for Mobile Nodes in IPv6 Networks," IEEE Communications Magazine, August 2002.

[12] H.Ren-Hung, L.Cheng-Ying, W.Chiung-Ying,and C.Yuh-Shyan, "Mobile IPv6 Based Ad Hoc Networks:Its Development and Application," IEEE Journal on Selected Areas in Communications, vol.23, no.11, November 2005.

[13] M.Dunmore, and T.Pagtzis, "Mobile IPv6 Handovers: Performance Analysis and Evalution," 6NET Project, IST-2001-32603, May 2004.

[14] E.wedlund, and H.Schulzrinne, "Mobility Support Using Sip,"IEEE International Conference on Wireless and Mobile Multimedia, August 1999.