ISSN:0975-9646

A Secure tunnel technique using IPv6 Transition over IPv4 Channel

Kamna Chauhan[1], Asst. Prof. Pooja Jain[2]

[1]*PG Scholar,Department of Computer Science & Engineering*
Shri Vaishnav Institute of Technology And Science,Indore (M.P.), India
[2] *Asst.Prof.Department of Computer Science & Engineering*
Shri Vaishnav Institute of Technology And Science,Indore (M.P.), India

Abstract: **Web Protocol form 6 (IPv6) contains various peculiarities that make it appealing from a security outlook. It is dependable and simple to set up, with programmed design. Enormous, inadequately populated location spaces render it exceptionally impervious to pernicious outputs and ungracious to computerized, examining and spreading toward oneself worms and half breed threats.IPv6 is not a panacea for security, however, in light of the fact that few security issues get singularly from the IP layer in the system model. For instance, IPv6 does not secure against misconfigured servers, inadequately composed applications, or ineffectively secured locales. Furthermore, IPv6 and IPv6 transitional components present new, not generally comprehended, instruments and procedures that gatecrashers can use to secure unapproved movement from location. These IPv6-inferred endeavours are regularly fruitful even against existing The quick dispersion of the Internet and improvement of high velocity broadband systems have represented the issue of deficient IPv4 location space on the Internet. Also, this absence of location space has been aggravated by the advancement made toward a universal system society, in which different sorts of data hardware, versatile PCs, and electrical data apparatuses impart on the Internet. IPv6 was produced as an answer for this issue [1]. The IPv4 location structure is in light of a 32-bit address length. It can oversee around 4 billion locations, however can't be appointed to everybody living on the planet, which contains around 6.3 billion individuals. The cutting edge Internet Protocol, at first known as IP Next Generation (Ipng), and after that later as IPv6, has been created by the Internet Engineering Task Force (IETF) to supplant the current Internet Protocol (otherwise called IPv4). At the point when both IP adaptations are accessible and the clients of Internet need to associate with no limitations, a move component is needed.[1].**

Keywords: **IPV4, IPv6, Diffusion, Internet protocol (IP)**

I. INTRODUCTION

At the point when IPv4 was initially grown as an analysis for a little gathering of associations to convey, nobody ever expected the blast of gadgets that would drive the requirement for extra extraordinary tending to alternatives. Notwithstanding standard desktop PCs, servers, switches, and system gadgets that oblige IP addresses, the expansion of cell phones and shopper hardware and apparatuses that oblige IP locations have driven the consumption of the accessible IPv4 space. The Internet Engineering Task Force (IETF), Regional Internet Registries (RIRs), Internet administration suppliers (ISPs) and numerous others made a few inventive activities to grow the life of IPv4. Endeavours included system address interpretation (NAT), more snug control of location assignment, recovering unused location space and port location interpretation. Nonetheless, nothing could keep the inexorable exhaustion of locations.

An increment in system gadgets, for example, PDAs or IPTV, and in system administrations, for example, cloud administration or incorporated wire and remote administrations, has brought about developing requests of IP. This brought the consumption of pre-existed IPv4 locations and the need of IPv6 to supplant IPv4. There are numerous progressing explores in IETF (Internet Engineering Task Force) on the move of IPv4 to IPv6, as IPv6 will be connected sooner rather than later . [2]

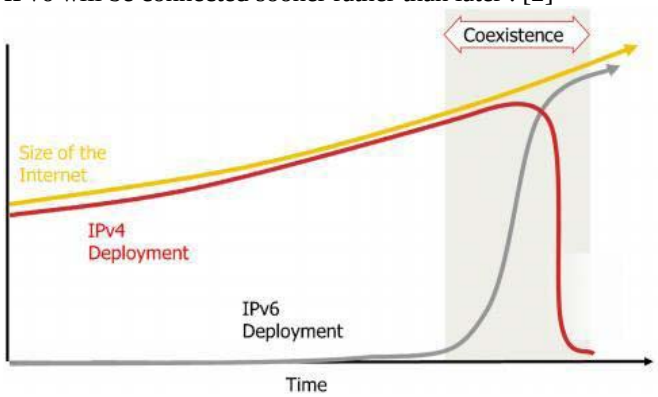

Fig 1:Time graph for IPV4 & IPV6

The perfect IPv6 execution is to introduce the convention as a stand-alone Internet convention arrangement in an undertaking domain. On the other hand, numerous associations don't see the need to change over their endeavour systems to the IPv6 convention on the grounds that they see Internet availability as yet being "adequate." As the cell phone commercial centre advances the current IPv4 address assignment won't be sufficient to stay aware of client interest for Internet openness for a wide range of gadgets. Numerous security sellers are holding up for expanded client request before actualizing backing for IPv6. Since IPv4 and IPv6 are not good conventions, associations must arrangement an approach to move from

IPv4 to IPv6. While there are a few merchants that bolster full IPv6 execution arrangement, numerous don't bolster IPv6 at all or just offer techniques for a mixture move to an IPv6 arrangement utilizing the current IPv4 building design. There are three right now three IPv4 to IPv6 move innovation methods:

1) The double stack system building design,
2) The interpretation innovation structural engineering.
3) The parcel burrowing construction modelling.

1) Dual-Stack Network Architecture

The double stack system construction modelling is a perceived venture conjunction procedure. Double stack alludes to running the two conventions, IPv4 and IPv6, in parallel. Basically, both conventions are dynamic. Generally one convention is favoured and system activity endeavours to utilize the favoured convention first. On the off chance that activity can't finish its way with the favoured technique, the movement will attempt again utilizing the auxiliary convention. The essential reason the activity would not achieve its destination utilizing the favoured convention is on the grounds that some system section in the movement's way does not bolster the favoured convention. For instance, an email from a customer PC that is double stacked and favours IPv6 will attempt to send its movement to the beneficiary PC by means of IPv6. In the event that any share of the email's way does not bolster IPv6, for example, a switch, a server, or even the accepting customer, the movement won't finish its way and the sending customer will send the message once more, yet utilizing IPv4 this time. The playing point to double stack is that the gear that exists for the IPv4 system can likely be utilized for the IPv6 system, accepting it is now IPv6 proficient. This technique permits an association to utilize IPv6 where it can, yet permit associations of an opportunity time to relocate from legacy frameworks since the IPv4 base remains.

2) Translation Architecture

The interpretation innovation construction modelling methodology is the procedure which changes over an IPv4 bundle to an IPv6 parcel and the other way around for system movement purposes. This is regularly done by a gadget at the system fringe. The point of interest of utilizing interpretation is the main change the association needs to make is the expansion of the interpretation gadgets.

3) Tunneling Architecture

The burrowing construction modelling arrangement is a technique that typifies IPv6 parcels inside IPv4 transmission streams. A few alternatives exist for burrowing conventions, for example, 6to4, Teredo, Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) and nonexclusive steering exemplification (GRE). The playing point of this strategy is additionally the minimal effort and simplicity of usage. The danger of this strategy is security. Permitting burrowing on the system may camouflage dangers from system overseers and safeguard sensor gadgets. Thus burrowing is viewed as a high hazard IPv6 move system.[3]

II LITERATURE SURVEY

Amid the last few years different examination articles had distributed which gives the subtle elements up to a certain level and in the wake of perusing those some modern methodologies had been recognized. Convey advances the study, underneath are some related works that aides this paper for further works.

[4] IPv6 has existed for almost two decades and a lot of technical research has been conducted in this area. However, in the area of managing and supporting the secure introduction of IPv6 into existing networks, literature is very scarce. Currently, we are not aware of a deep and systematic comparison of the important guidelines that support practitioners during this process. Concerning general literature, most relevant information on IPv6 can be found in the RFCs published by IETF, see the list in Appendix A, which is updating and extending an older list published by NIST.

[5] Those RFCs also cover important research in the field of IPv6, including experimental methods and protocols. The RFCs were also used as a starting point of our work, extended to a large extent during the literature review. To the best of our knowledge, no evaluation of security guidelines for the deployment of IPv6 has been conducted before that was based on relevant RFCs published by the IETF. Concerning other general literature, Silvia Hagen gives a comprehensive overview of the IPv6 in her

High level introductions to IPv6 security are given by More detailed discussions on IPv6 security include as well as books such as Another very detailed introduction to IPv6 security in gives a comparison of IPv4 with IPv6 security and threats.

[6] Focuses on network auto configuration and related security issues. A survey of secure protocols for Mobile IPv6 is presented by network.

[7] Present the result of a survey (with 11 usable responses) on security issues during transition to IPv6 as well as some limited practical security tests on production networks. In comparison to this paper, the number of respondents in our paper is larger and the result more detailed. With respect to security, our current paper does not aim at providing a concise survey of IPv6 security issues and details of recent exploits. Such a work would be an important complement to our article. Instead, we focus on the management aspects of secure IPv6 deployment and the question to what extent the relevant RFCs are reflected in the two most prominent guidelines for practitioners.

III. PROBLEM STATEMENT & PROPOSED SOLUTION

IPv4 networking node can make an attack on IPv6 node(network):The attackers(hackers) in IPv4 networks can make an attack on the IPv6 nodes through the 6to4 router(tunnel) end point by forwarding a spoofed encapsulated messages(Packets).Therefore here in this situation it is very difficult to trace back.[8]

IPv6 networking node can make an attack on IPv6 network (node): In this type the hacker in IPv6 networks can make an attack on the IPv6 network through 6-to4 relay end point and 6-to4 router by sending spoofed encapsulated packets. In this case also its very difficult to trace back.[9]

Potential reflect- DoS attack on Destination Host: The hackers in the IPv4 networks can
make a reflect–DoS attack to a normal IPv6 network (node) through the 6-to-4 router (tunnel) end point by sending the encapsulated packets with the spoofed IPv6 source address as the specific IPv6 node.

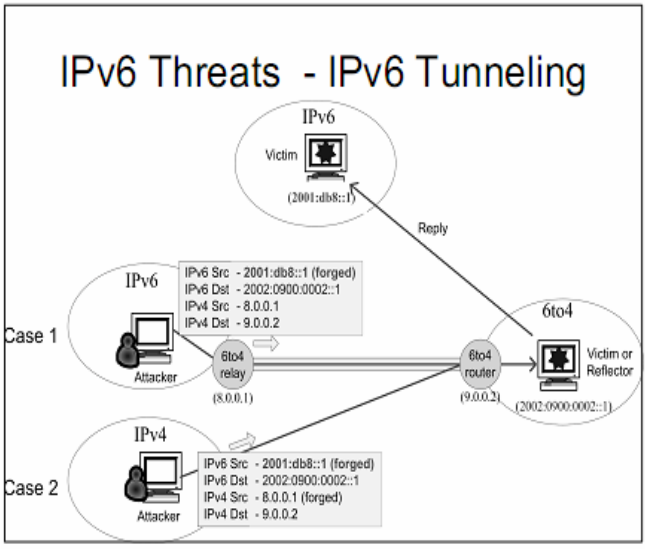

Fig 2:Issues in tunneling

Cheat by a Hacker with the IPv6 Neighbour Discovery (ND) message: Whenever IPv4 network is treated as the link layer in tunneling technology, the hackers in the IPv4 networks can cheat and DoS attack the tunnel end point by sending encapsulated IPv6 neighbour discovery (ND)messages with a spoofed IPv6 link local address. The automatic tunneling techniques like 6-to 4 and Teredo get the information of remote tunnel end point from the certain IPv6 packets.[10]

Proposed Solutione:IPv6 over IPv4 tunneling is the encapsulation of IPv6 packets with an IPv4 header so that IPv6 packets can be sent over an IPv4 infrastructure. RFC 2893 defines the following tunneling configurations
1) Router to router
2) Host to router or Router to host
3) Host- host
Following are the phases in which we can implement the required
solution.
1) Test bed development: To develop test bed for creating a tunnel which will have 2 IP v6 networks connected with IP v4 network via 6 to 4 routers.
2) Set up communication: To send packets from an IP v6 network to another IP v6 network through IP v4 to IP v4 network with the help of tunnel.
3) Outbound filtering server: outbound filtering server should capture the packets sent by 6 to 4 router.
The diagram drawn above informs about the proposed work.
There are two networks connected using a tunnel. The two networks do have gateway devices, R1 and R2. Router R1 connects 2 clients working on IP v4 and v6 whereas router R2 can have either of the clients. The test bed designed is on IP version 4 network and it is necessary to establish communication link between any clients on R1 network to any client in R2 network.

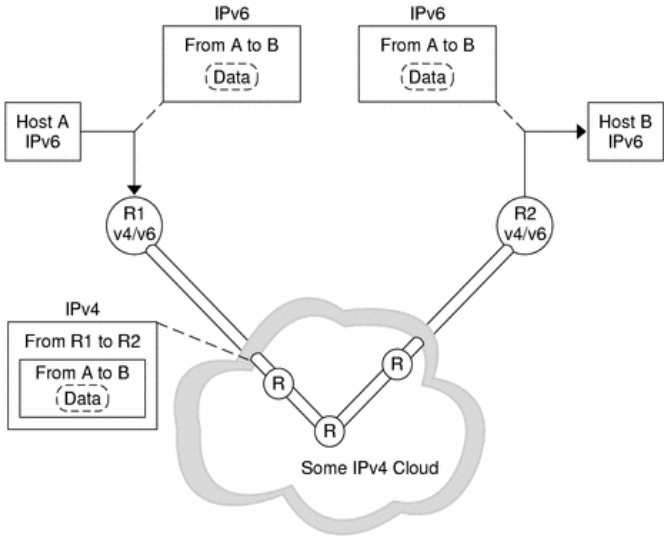

Fig. 3. Tunnel Execution

Router based mechanism
The two systems will function as Domain Name System (DNS) server. The systems running Windows XP Professional with service pack 2 are used as clients. The two systems which are running server operating systems will perform most of the activities. The roles given to the two servers are Test Server, Router Server and IDS server.
Subnet 1 uses the private IP subnet prefix and global subnet prefix

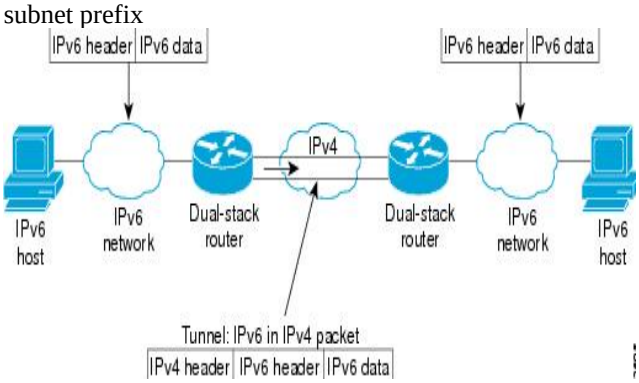

Fig. 4. Proposed Design Architecture

The clients connected to the two servers through hubs or switches. All computers on each subnet are connected to a separate common hub or Layer 2 switch. The two servers which also work as routers are named as ROUTER1 and ROUTER2. They have two network adapters installed. For the IPv4 configuration, each computer is manually configured with the appropriate IP address, subnet mask, default gateway, and DNS server IP address. For the IPv6 configuration, link-local addresses are used initially

IV. CONCLUSION

In this work will continue our evaluation with more transition mechanisms in the hopes to eventually empirically evaluate all the available transition

mechanisms. We also intend to investigate the performance of IPv6 when exploiting IPv6 features (such as the flow label field in the IPv6 header) to investigate end-to-end QoS support in IPv6 over IP-based networks. opportunity to ensure secure IPv6 deployments from the outset rather than a slow migration toward security, as occurred with IPv4, should be strongly considered by the Internet community. However, the amount of attention that IPv6 security has so far received is quite low, and new considerations will certainly be uncovered. Without adequate training and attention on the part of network operators to the new considerations with IPv6 security, it will be very difficult to ensure a smooth transition to IPv6. Further research in transition methodologies is required for successful transition to Next Generation Internet Protocol.[11]

ACKNOWLEDGEMENT

The work is evaluated and drafted with the help of some of authorities of the Shri Vaishnav Institute of Technology and Science , Department Of Computer Science And Engineering which leads me to the great outcomes. Without them it would not be possible for me to overcome the problems and issues faced. Thus, the authors thank the anonymous reviewers for their valuable comments, which strengthened the paper. They also like to give thanks **to** Dr. Anand Rajavat and Asst. Prof. Pooja Jain who had guided me throughout this research and being held always for discussion regarding the approach adapted for this paper.

REFERENCES

[1] J020 B.D. Cabrerat B. Ravichandran and Raman K. Mehra " Statistical Traffic Modelling for Intrusion Detection" 0-7695-0728-WOO$-10.00 0 2000 IEEE 466-473

[2] Wanming Luo, Baoping Yan , Xiaodong Li, Wei Mao "Network-Processor-Based IPv4/IPv6 Translator: Implementation and Fault Tolerance" Feb. 17-20, 2008 ICACT 2008 488

[3] Mohammadreza Ektefa "Intrusion Detection using Data Mining techniques" 978-1-4244-5651-2/10/$26.00 ©2010 IEEE 200-203

[4] Shaneel Narayan (Member IEEE), Shailendra S. Sodhi, Paula R. Lutui, Kaushik J. vijaykumar "Network Performance valuation of Routers in IPv4/IPv6 Environment A testbed analysis of software routers" 978-1- 4244-5849-3/10/$26.00 ©2010 IEEE

[5] Lee Ling Chuan, Kasmiran Jumari, Mahamod ismail and Khairil Anuar, Joong-Hee Leet, Jong-Hyouk Leet "Effective Value of Decision Tree with KDD99 Intrusion Detection dataset for Intrusion Detection System" Feb. 17- 20, 2008 ICACT 2008 1170-1175

[6] Yuhai Liu l, Hongbo Liu2 "The internet Traffic classification an online SVM approach"

[7] Chunling Wei "Research on Campus Network IPV6 Transition Technology". 978-0-7695-4480-9/11 $26.00 © 2011 IEEE DOI 10.1109/ISIE.2011.138

[8] Jiang Xie and Aarthi Balan "Case Study of Mobility Support for IPv4/IPv6 Transition Mechanisms over IPv6 Backbone networks"

[9] Thanh-Nghi Do " A Novel Speed-up SVM Algorithm for massive classification tasks" 978-1-4244-3279-8/08/$25.00© 2008 IEEE 215-220

[10] Debajyoti Mukhopadhayay, Byung-Jun-Oh, Sang-Heon Shim, Young-Chon Kim, "A Study on recent Approaches inHandling DDoS Attacks" Cornell University, The computing Research Repository 1012.2979, Dec 2010

[11] Sheng Liu, Na Jiang "SVM Parameters optimization Algorithm and its Application" 978-1-4244-2632-4/08/$25.00 IEEE 509-513