International Journal of Latest Trends in Engineering and Technology
Vol.(8)Issue(1), pp.097-105
DOI: http://dx.doi.org/10.21172/1.81.013
e-ISSN:2278-621X

SCENARIOS IN MIGRATION OF NETWORKS FROM IPV4 TO IPV6

Smt. I Kullayamma[1] and Sai Gururaju Goud G[2]

Abstract: With the unexpected growth, Internet has been facing for several years the exhaustion of available IPV4 addresses. To handle this unexpected condition, many solutions have been proposed for effective usage of the available addresses. Out of the proposed ones, the most popular solution is the Network Address Translation(NAT), in which the internal hosts are addressed with private IPV4 addresses are represented by NAT server in Internet. But it can't meet the growing need of IP addresses with the expasion of internet worldwide. Another solution to this problem is the use of Internet Protocol version 6(IPV6). This new version of IP has 128-bit addresses, while IPV4 is limited to 32-bit addresses. Apart from this IPV6 provides security,multicasting, mobility, routing and network auto configuration some of which not available or improved compared to IPV4.Also majority of current operating systems support IPV6. It is not posssible to move from iPV4 to IPV6 in a short period of time. Hence,during the transition,IPV4 and IPV6 will coexist. Many reasons extend the time of coexistence ,includes cost, support for IPV6, training of technical staff, upgradation of all ISPs etc. So IPV6 must be deployed gradually. Accordingly, we need to choose the transition mechanism.In this paper, we will present the available three mechanisms i.e., Dual stack mechanism, Tunnelling and NAT-PT. Opting the mechanism depends on various conditions like cost ,support of IPV6 in both hosts, ISPs upgradation.Hence we discuss the optimal choice of mechanism according to the situation.We will pressent an analysis of all the avaiable scenarios in transition.
Keywords: Automatic tunnelling, Dual stack mechanism, GNS3, IPV4,IPV6 addressing, ISATAP tunnelling, Manual tunnelling , NAT-PT mechanism.

I. INTRODUCTION

The Internet is a worldwide collection of networks that links together millions of businesses, government agencies, educational institutions and individuals. The magnificence of the Internet is we can access it from a computer anywhere Computers and the Internet have become a vital part of everyday life, from finding information and staying in touch to searching for jobs and shopping online that are linked by a broad array of electronic and optical networking technologies. Different Network elements such as routers, switches, gateways etc. has been interconnected together for communication of information over the Data networks. The Layer 3 devises are connecting the WAN interfaces for data transmission and forwarding the packets using routing tables whereas switches are connecting the LAN. The first major version of IP, Internet Protocol Version 4 (IPv4), is the dominant protocol of the internet. But Challenges in Today's Internet are Address depletion, Loss of peer-to-peer model, Increasing need for security, wireless/mobile devices accessing Internet services.

[1] *Assistant Professor,Department of ECE, SVU College of Engineering, Tirupati*
[2] *M Tech, Department of ECE, SVU College of Engineering, Tirupati*

IPv6 provides a platform for new Internet functionality that will be needed in the immediate future, and provide flexibility for further growth and expansion. IPv6 (Internet Protocol version 6) is a revision of the Internet Protocol (IP) developed by the Internet Engineering Task Force (IETF). IPv6 is intended to succeed IPv4, which is the dominant communications protocol for most Internet traffic as of 2013. IPv6 was developed to deal with the long-anticipated problem of IPv4 running out of addresses. IPv6 implements a new addressing system that allows for far more addresses to be assigned than with IPv4.

Each device on the Internet, such as a computer or mobile telephone, must be assigned an IP address in order to communicate with other devices. With the ever-increasing number of new devices being connected to the Internet, there is a need for more addresses than IPv4 can accommodate. IPv6 uses 128-bit IPv6, with some 340 trillion, trillion, trillion addresses. The deployment of IPv6 is accelerating, with a World IPv6 Launch having taken place on 6 June 2012, in which major internet service providers, especially in countries that had been lagging in IPv6 adoption, deployed IPv6 addresses to portions of their users. IPv6 has a new feature called auto configuration. This feature allows a device to generate an IPv6 address as soon as it is given power.

Migrating from IPv4 to IPv6 in an instant is impossible because of the huge size of the Internet and of the great number of IPv4 networks. Moreover, many organizations are becoming more and more dependent on the Internet for their daily work, and they therefore cannot tolerate downtime for the replacement of the IP protocol. As a result, there will not be one special day on which IPv4 will be turned off and IPv6 turned on because the two protocols can coexist without any problems. The migration from IPv4 to IPv6 must be implemented node by node by using auto-configuration procedures to eliminate the need to configure IPv6 hosts manually. This way, users can immediately benefit from the many advantages of IPv6 while maintaining the possibility of communicating with IPv4 users or peripherals.

II. IPv4 vs Ipv6

IPV4 addressing is a 32-bit addressing method in which it can provide a maximum of 4,294,967,296 addresses.Initially, the addresses were expected to be enough as the internet was in usage at initial level. Later on in a view of future usage,the need of addresses to use effectively came into action. As a part of this, classful and classless addresses categorisation came into existence. Still to avoid the address exhaution NAT ing method was introduced. However, to meet the growing needs of the current digital world, its inevitable to avoid the need of more addresses. Hence introduction of IPV6 came into existence. However, we will discuss the limitations of current IPV4 addressing mechanims and lets discuss the method of overcoming these disadvantages with the introduction of new IPV6 Addressing method by stating its features.

Limitations of Ipv4 addressing:

The limitations of Ipv4 addressing are stated below:

1.Scarcity of IPv4 Addresses: The IPv4 addressing system uses 32-bit address space. This 32-bit address space is further classified to usable A, B, and C classes. 32-bit address space allows for 4,294,967,296 IPv4 addresses, but the previous and current Ipv4 address allocation practices

limit the number of available public IPv4 addresses. Many addresses which are allocated to many companies were not used and this created scarcity of IPv4 addresses.

Because scarcity of IPv4 addresses, many organizations implemented NAT (Network Address Translation)to map multiple addresses to a single public IPv4 address. By using NAT (Network Address Translation)we can map many internal private IPV4 addresses to a public IPv4 address, which helped in conserving IPv4 addresses. But NAT (Network Address Translation)also have many limitations.NAT (Network Address Translation)do not support network layer security standards and it do not support the mapping of all upper layer protocols. NAT can also create network problems when two organizations which use same private Ipv4 address ranges communicate. More servers, workstations and devices which are connected to the internet also demand the need for more addresses and the current statistics prove that public Ipv4 address space will be depleted soon. The scarcity of Ipv4 address is a major limitation of Ipv4 addressing system.

2. Security Related Issues: Internet Protocol Security (IPSec) is a protocol suit which enables network security by protecting the data being sent from being viewed or modified. Internet Protocol Security (IPSec)provides security for IPv4 packets, but Internet Protocol Security (IPSec) is not built-in and optional. Many IPSecimplementations are proprietary.

Features of IPv6

The features of IPv6 are listed below.

1. New Packet Format and Header:IPv6 specifies a new packet format. The new Ipv6 packet helps to minimize packet header processing by routers. This is achieved by moving both nonessential and optional fields to extension headers that are placed after the IPv6 header.Since Ipv4 packet and IPv6 packets are significantly different, the two protocols are not interoperable.

2. Large Address Space:IPv4 has 32 bit (4-byte) address space, but IPv6 has 128-bit (16-byte) address space. The very large IPv6 address space supports a total of 2^{128} (3.4×10^{38}) addresses. This large address space allow a better, systematic, hierarchical allocation of addresses and efficient route aggregation. With the large number of available addresses we can eliminate address-conservation techniques like NAT (Network Address Translation).

3. Statefull and Stateless IPv6 address configuration: In IPv6 statefull or stateless configuration is possible. Hosts on a link can automatically configure with IPv6 addresses called link-local addresses and with addresses derived from prefixes advertised by local routers. When first connected to a network, a host sends a link-local router solicitation multicast request for its configuration parameters. The router which is available in the link responds to the request from the host with a router advertisement packet that contains network-layer configuration parameters. Hosts can configure link local addresses automatically and communicate each other without manual configuration even there is no router available. The hosts may also have stateful configuration with the Dynamic Host Configuration Protocol version 6 (DHCPv6) or static configurations, as Ipv4.

4. Multicast: The three types of communication available in in IPv4 are unicast, multicast and broadcast.; Unicast is one-to-one communication;multicast is one-to-many communication and broadcast is one-to-all communication. The transmission of a packet to all hosts was performed by using special broadcast addresses in IPv4.Broadcastcommunication is not available in IPv6

and therefore does not define broadcast addresses. In IPv6, the effect of broadcast can be achieved by sending a packet to the link-local all nodes multicast group at address ff02::1.

5. Integrated Internet Protocol Security (IPSec):Internet protocol security(IPsec) is a set of Internet standards that uses cryptographic security services to provide Confidentiality, Authentication, Data integrity. The support for Internet Protocol Security (IPSec)was optional in IPv4. Internet protocol security(IPsec) is an integral part of the base protocol suite in IPv6.Internet Protocol Security (IPSec)support is mandatory in IPv6.

6. Neighbour Discovery Protocol:The Neighbor Discovery Protocol (NDP) is a protocol available IPv6. The Neighbor Discovery protocol (NDP) is based on Internet Control Message Protocol Version 6 (ICMPv6) messages that manage the interaction nodes on the same link. There is no Address Resolution Protocol(ARP) for IPv6 and the role of the Address Resolution Protocol (ARP)is replaced by Neighbor Discovery Protocol (NDP).

7. Extensibility: The features of IPv6 can be extended by adding extension headers after IPv6 header. The size IPv6 extension headers is constrained only by the size of the IPv6 datagram packet, unlike 40 bytes of options of IPv4.

III.MIGRATION MECHANISMS

Moving from IPv4 to IPv6 will not need to be done at the same time because such approach is difficult and it will take time. In addition, public networks now a days has no single point of control so it is not possible to enforce like this change. In addition, such change to most companies and organizations already connected to the internet is not welcomed and not profitable. The best approach for this move is to implement IPV6 along with existing IPV4.To make this approach much easier and coexist with existing IPV4 many transition techniques have been implemented . There are three types: Dual Stack, Tunneling and Translation (NATPT).
There are mainly three migration mechanisms available.
1.Dual stack: Here we implement both IPV4 and IPV6 protocols in the network elements.
2.Tunnelling: Encapsulation of an IPV6 packet in IPV4 packet.
3.NAT-PT: Address translation of gateway device or translation of code in TCP/IP code of router.
The above methods are explained below in brief :

1.Dual-stack method:

The term dual stack means that the host or router uses both IPV4 and IPV6 at the same time. For hosts, this means that the host has both an IPV4 and IPV6 address associated with each NIC, that the host can send IPV4 packets to other IPV4 hosts, and that the host can send IPV6 packets to other IPV6 hosts. For routers, it means that in addition to the usual IPV4 IP addresses and routing protocols, the routers would also have IPV6 addresses and routing protocols . To support both IPV4 and IPV6 hosts, the router could then receive and forward both IPV4 packets and IPv6 packets.
STEPS:
1.Configure both ipv4 and ipv6 initial configurationon host.
2.Configure both ipv4 and ipv6 routing protocols on routers.

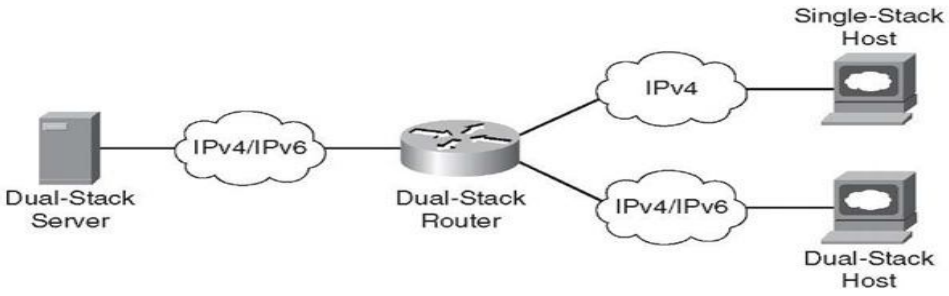


Figure 1: Dual Stack implementation

This method is advisable in the initial stages of migration. Due to this the routers has to maintain both routing protocols which leads to a huge load on the routers which sometimes may affect the performance of the network. The implementation of IPv6 on all routers that might one day receive an IPv6 packet that needs to be forwarded. Alternatively, using tunnels may be more reasonable to support smaller packets of IPv6 hosts, because tunnels require fewer routers to be configured with IPv6 at all.

2.Tunnelling

Basic concept of tunnelling lies in encapsulation of IPV6 packet(payload) within the IPV4 packet and transfer it over IPV4 network as an IPV4 packet.The packet is decapsulated at the destination.Hence some routers only need V6 configuration ,less operational risk.

Basic two types of tunnells:

1.Point to point : An exclusive tunnel cinfigured between two routers.
2.Multipoint :Only a tunnel from one router which may later reach destination using another tunnels.
Point to point tunnels are considered in the case of two routers only need ipv6 whereas multipoint tunnels are advicable in large networks.

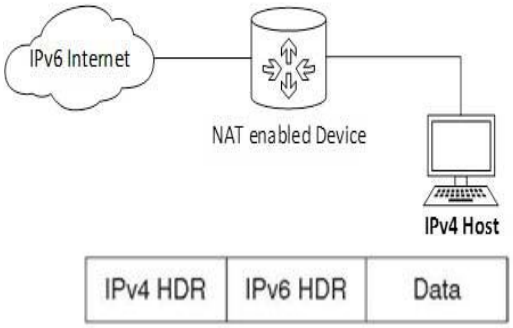
Types of tunnelling methods:

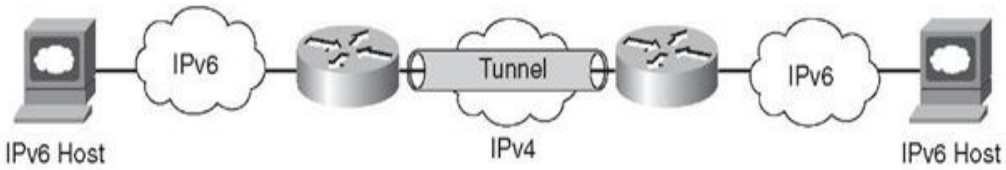
Available tunnelling mechanisms are explained below in brief:
1.Manual configured tunnels:Involves manual configuring of tunnels between the required routers.
*2Automatic tunnels:*Only a single tunnel is evolved from a router.Packet from the source consists of ipv4 address informat
of destination in the 2nd and 3rd quartets.
3.ISATAP (Intra-Site Automatic Tunnel Addressing Protocol) tunnels: Similar to automatic tunnels except this one has ipv4 adress information in 7th and 8th quartets.5th and 6th will be always 0000:5EFE.

Basic steps in tunnelling:

Steps involved in tunnelling are explained in brief and these are generalised steps for all the tunnelling mechaisms.

Step 1. Find the tunnel IPv4 addresses planned for the tunnel, and ensure that each router can forward IPv4 packets between the addresses. If using a new loopback interface, create the





loopback using the interface loopback number command, assign it an IPv4 address with the ip address command, and confirm that routes for this interface will be advertised by Ipv4.

Step 2. Create a tunnel interface using the interface tunnel number command, selecting a locally significant integer as the
tunnel interface number.

Step 3. Define the source IPv4 address of the tunnel using the tunnel source {interface-type interface-number | ipv4-address} interface subcommand. (This address must be an IPv4 address configured on the local router.)

Figure 2: Basic concept of tunnelling

Step 4. Define the destination IPv4 address for the encapsulation using the tunnel destination ipv4-address interface subcommand; the address must match the tunnel source command on the other router.

Step 5. Define the type of tunnel (manual/automatic/ISATAP), using the tunnel mode

a. tunnel mode ipv6ip interface subcommand for manual.
b. tunnel mode ipv6ip 6 to 4 interface command for automatic.
c. tunnel mode ipv6ip isatap interface command for ISATAP.

Automatic tunnels are suitable for intrasite communication whereas isatap tunnels support intersite communications.

3.NAT-PT:

NATing is a method being used in ipv4 for effective usage of addresses. Same method is being implemented including the protocol translations(TCP,ICMP) for tranition. This is more preferable when the two hosts are of different configuratios. We have to make translation before routing it to the router.

Figure 3 : NAT-PT mechanism

Two cases arise overhere.

a. ISP is IPV4: In this case NAT-PT is to be performed at IPV6 host.
b.ISP is IPV6: In this case NAT_PT is to be performed at IPV4 host.
However,it is not recommended by IETF to use NAT-PT method as it may lead improper workimg of the router and method is exhausted

IV.RESULTS

The deployment of IPV6 does not occur in a short period of time.There are a lot of considerations whie moving from v4 to v6. The main factor being cost. Companies which are using the old devices which does not have an option to support IPV6, cannot afford to shift at a time to the IPV6 which involves replacemet of all the current devices. Hence it is necessary for them to start the usage of transition mechanisms for smooth running with the newly deployed systems(IPV6). Simiarly for an ISP ,it is a unbearable burden to change all the existing routers to IPV6 since the cost of a router is huge.Hence ISPs need this transition mechanisms to support the both type of users. After studying all the scenarios, let us now see the possible cases that arise in the corporates and the type of migartion to be used.
Table 1: Selection of appropriate mechanism for the situation.

CASE	HOST 1	ISP	HOST 2	MECHANISM
1	V4	V4	V4	GENERAL CASE(IPV4)
2	V4/V6	V4	V4	GENERAL CASE(IPV4)
3	V4/V6	V4	V4/V6	GENERAL CASE(IPV4)/Dual Stack
4	V6	V4	V4	NAT-PT
5	V6	V4	V6	TUNNELLING
6	V6	V4/V6	V4	NAT-PT
7	V6	V4/V6	V6	DUAL STACK
8	V4	V6	V4	TUNNELLING
9	V4	V6	V4	NAT-PT
10	V6	V6	V6	GENERAL CASE(COMPLETE IPV6)

.

The cases in the table sited are explained below.

- In case 1 both the hosts and ISP are using only V4 enabled systems.In this case they can go in IPV4 addressing.This is the present scenario in our nation.
- In case 2 , one host have both ip versions support,other host with pure v4 and the ISP with V4.In this scenario, if we want to incude the migration technique ,we can go with NAT-PT.But as three can support v4 we can establish communcation in v4 level ,which is economical.
- In case 3, both the hosts have v4 and v6 compatibiilty,whie the ISP still in V4.Here we can go with the dual stack at both ends.But ,the most economical solution is using V4 communcation.
- In case 4, one host is pure V6 and another one pure V4.The intermediate ISP is V4.In this case the communication to the V6 host and V4 host should be done in V6 and V4 versions respectively.To enable communcationin such scenarios the best available and suggestable solution is implementing NAT-PT migration method.
- In case 5, both the hosts are enabled with pure V6 version and the intermediate ISP still in V4 version.This scenario arises as it is difficult for an ISP which involves huge amount of routers and is impossible to modify them all economicaly.in such cases, communcation can be done by using one of the avaialble tunnelling mechanims.Again choosing the best tunnelling mechanims as per conidering all the economic issues is important.When the network involves more number of entities, its advicable to go with the automatic tunnelling rather than manual.
- In case 6, the intermediate ISP is able to support both the versions.Both the hosts are supporting different versions purely.Such scenario can be addressed with NAT-PT mechanism.
- In case 7, the hosts able to move to V6 version and the ISP supporting both versions.This case can be addressed with dual stack in the ISP.Here we have choosen dual stack because some hosts might be still with the v4 version as its impossible to move all the entities to V6 for a small firms.
- In case 8, when the ISP started only V6 services.It is difficult for a host still using V4,hence we need tunnelling mechanism to overcome the situation.
- In case 9 ,the ISP has shifted totally to v6 .In such case it can service the v4 hosts using address translation mechanism.
- In case 10, total world shifted to the V6 and communication can be smoothly established in V6 environment.This is the final stage, where all the existing V4 entitites are ended and world started using V6 entities.And no need of any migration mechanism.

V.CONCLUSION

To meet the need of current requirement of addresses in the internet world, the only solution is introduction of IPV6 addressing. Hence the whole world is migrating towards IPV6.It is imposible to shift at a time to IPV6. Moreover, many organizations are becoming more and more dependent on the Internet for their daily work, and they therefore cannot tolerate downtime for the replacement of the IP protocol. As a result, there will not be one special day on which IPv4 will be turned off and IPv6 turned on because the two protocols can coexist without any problems. IPv6 provides a platform for new Internet functionality that will be needed in the immediate future, and provide flexibility for further growth and expansion. Migration mechanisms are helpful in achieving the target.Migration mechanism must be choosen

depending upon the criteria. Native Dual-Stack is the technology that companies should consider for their deployment in the initia stages of migration. It keeps both IPv4 and IPv6 running at the same time, hence those who can move to IPV6 and who are not unable to have IPV6 can also be serviced at the same time. In the next step some may shift purely to the IPV6 ,still the ISPs can support both the users.It is difficut for the ISPs to move to IPV6 ,hence they can achieve it in a very gradual process. When the network is fully transitioned to IPv6, operators can stop supporting IPv4. The two protocols must be supported until native IPv6 is the only protocol in use. The cost of operation for Dual-Stack is more than single stack for operators because they have to support both stacks. If it is difficult for operators to move directly to native IPv6, then they can go implement transition technologies. Once the operators move to ipv6 ,the customer with still in ipv4 has to use the migration method depending upon the destination and requirement.

REFERENCES

[1]. Chiranjit Dutta1, Ranjeet Singh Sustainable2 IPv4 to IPv6 Transition Volume 2, Issue 10, October 2012 ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Software Engineering Research Paper .

[2]. Ghaida Yagoub Ahmed Yosif Al-Gadi 1, Dr. Amin Babiker A/Nabi Mustafa 2, Mahmoud Ahmed Hamied3, Evaluation and Comparisons of Migration Techniques From IPv4 To IPv6 Using GNS3 Simulator Vol. 04, Issue 08 (August. 2014), ||V4|| PP 51-57 IOSR Journal of Engineering (IOSRJEN).

[3]. Grosse, E. and Lakshman, Y. (2003). Network processors applied to IPv4/IPv6 transition, IEEE Network, 17(4), pp.35-39.

[4]. Ali, A. (2012). Comparison study between IPv4 & IPv6, International Journal of Computer Science Issues (IJCSI), 9(3), pp.314-317.

[5]. Batiha, K. (2013). Improving IPv6 Addressing Type and Size, International Journal of Computer Networks & Communications (IJCNC), 5(4), pp.41-51.

[6]. Ibáñez Parra, J. (2014). Comparison of IPv4 and IPv6 Networks Including Concepts for Deployment and Interworking, INFOTECH Seminar Advanced Communication Services (ACS), pp.1-13.

[7]. Sailan, M., Hassan, R. and Patel, A. (2009). A comparative review of IPv4 and IPv6 for research test bed, Proceedings of International Conference on Electrical Engineering and Informatics (ICEEI '09), Malaysia, pp.427-433.

[8]. Ahmad, N. and Yaacob, A. (2012). IPSec over Heterogeneous IPv4 and IPv6Networks: Issues and Implementation, International Journal of Computer Networks & Communications (IJCNC), 4(5), pp. 57-72

[9]. Arafat, M., Ahmed, F. and Sobhan, M. (2014). On the Migration of a Large Scale Network from IPv4 to IPv6 Environment, International Journal of Computer Networks & Communications (IJCNC), 6(2), pp.111-126.

[10]. Wu, P., Cui, Y., Wu, J., Liu, J. and Metz, C. (2013). Transition from IPv4 to IPv6: A state-of-the-art survey, IEEE Communications Surveys & Tutorials, 15(3), pp.1407--1424.

[11]. Wu, Y. and Zhou, X. (2011). Research on the IPv6 performance analysis based on dual-protocol stack and Tunnel transition, Proceedings of the 6th International Conference on Computer Science & Education (ICCSE), pp.1091--1093.

[12]. Interface and Hardware Component Configuration Guide, Cisco IOS XE Release 3S. (2014). 1st ed. [ebook] San Jose: Cisco Systems, Inc., pp.18-26. Available at: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/configuration/xe-3s/ir-xe-3s-book.pdf [Accessed 10 May 2014].