Design Concept and Simulation of Migration from Present IPv4 Network to Future IPv6 Network Using Three Transition Mechanisms

Ms. Salama Sumara
RK University Rajkot.Gujarat

Prof. Arjav Bavarva
RK University Rajkot,Gujarat India

Shree Ajay Shrivastava
SDE RTTC Ahmadabad.Gujarat-India

***Abstract*— Currently, the Internet world is facing the big problem that is depletion of IP addresses with the IPv4 protocol. This paper contains the very important theoretical concepts of new generation Internet Protocol IPv6 which solve the problem of IP addressing and also focus on IPv6 address format, routing and three mechanism of migration from IPv4 to IPv6 network: Dual Stack, Translation and Tunneling using Network Simulator as Packet tracer. This paper more emphasis on network migration from IPv4 to IPv6 which is near future trend.**

Keywords— IPv4, IPv6, Dual stack, Translation, Tunneling.

I. INTRODUCTION

Today, with the increasing of technology, the number of users of Internet is increasing fast, and so it must need more number of IP addresses because each device which uses internet needs unique IP address. Yet many devices that connect through Internet are using Internet Protocol version 4, since IPv4 has 32-bit address space, it allows 2^32 addresses and it is approximately 4 billion addresses. With the increasing the technology, not only personal computers, but also laptop, mobiles, iPod, printer, video games, other medical instruments, auto mobiles and other electronics devices also uses Internet service. So with the limited address space of IPv4 it is like a burden since it has no more facility to support to give IP address to every existed device which is uses Internet.

Address space of currently used internet protocol version 4 is too limited to handle the new addresses. As previous some methods was developed to overcome this address space problem to extend the future of Internet Protocol version 4 (IPv4) along with Network Address Translation (NAT), Variable Length Subnet Mask (VLSM), Classless Inter domain Routing (CIDR) and others [1], after that, these all technology not enough to save the future of Internet Protocol version 4 (IPv4). Currently IPv4 Internet is facing a series of problems including address exhaustion, routing scalability and broken end-to-end property. IANA

(Internet Assigned Number Authority) had run out of global IPv4 address pool in Feb. 2011, while simulations show that within 3 years all the RIRs (Regional Internet Registries) will exhaust their IPv4 address space [2].

June 6, 2012 was the selected date by the Internet Society (ISOC) and other organizations in the field as the worldwide launch of IPv6. On that day number of companies and organizations from all over the world enables the operations of their portals and other forms of presence on the Internet with the IPv6 protocol in a definitive way [3].

II. IPV6

Internet Protocol version 6 (IPv6) is developed as the next-generation network layer protocol, to overcome the issues of IPv4 [4].The IPv6 protocol address is 128-bit long, instead of 32-bit of IPv4 address. So it creates 3.4*10^38 possible addresses. This is very large number. These new IPv6 address will meet the Internet demand for the grooving future [5].

Every device on the internet must be assigned an IP address in order to communicate with other devices. With the ever-increasing number of new device being connected to the Internet, the need for more addresses than IPv4 is able to accommodate. IPv6 is uses 128-bit address allowing 2^128 or a four times bigger than an IPv4. [5]. As the IPv4 developed and introduced in the 90's [6] by Internet Engineering Task Force (IETF). The reason for adoption of new protocol is the expansion of addresses.

A. IPv6 Address Format

IPv6 uses a 128-bit or 16 bytes, these addresses are represented as eight groups of four hexadecimal digits separated by colons, ":". For example: 2002:db80:0449:5a63:0000:0000:0000:0001. The hexadecimal digits are case- sensitive, but IETF suggest the use of lower case letters. In an IPv6 address the leading zeros in a group may be omitted and also contiguous block of zeros can be simplified using double colons "::". Thus the example address may be written as: 2002:db80:449:5a63::1.

As IPv6 network uses an address block that is continues group of IPv6 addresses of a size that is a power of two. Network address ranges are written in Classless Inter Domain Routing (CIDR) notations. A network is denoted by the first address in the block, a slash (/) and a decimal value equal to the size in bits of the prefix. For example, the

network written as 2002:db80:449:5a63::/64 start at address 2002:db80:5a63:0000:0000:0000:0000 and ends at 2001:db80:449:5a63:ffff:ffff:ffff:ffff [7]

B. Address Assignment

IPv6 address `can be assigned either by statically or auto configured. Address that can statically assign is using identifier (ID) of manual interface or an ID of EUI-64 interface. And it is also dynamically configured by using stateless auto configuration or by DHCPv6.

Static configuration: Manually enter the IPv6 address of a node in a file or it is through any relevant tools of the operative system. Information to be included is the IPv6 address and the network prefix size [7]. Static routes are not scalable, since it has to configure each route and any redundant paths for that route on each router. This configuration is divided into static configuration using the ID of manual interface, in which the hole IPv6 address is used for the network section and the device identifier section [8] and into static configuration using the ID of EUI-64 interface, in which to obtain the ID, the host takes the MAC address from the link layer device, however as the MAC address has only 48 bits, then the MAC address is split in half and in the middle is inserted the default 16 bits hexadecimal value FFFE of in order to complete an unique interface ID of 64 bit [8].

Dynamic configuration: Through this method network administrators centrally manage and automate the assignment of Internet Protocol (IP) addresses in an organization's network. Using the Internet Protocol, each machine that can connect to the Internet needs a unique IP address, which is assigned when an Internet connection is created for a specific computer. It is divided into stateless auto configuration, in that each router broadcast the network information including the prefix assigned to each of its interfaces. As a result, the end system uses the obtained information in this broadcasting. The stateless name comes from that no device keeps track of the assigned IP addresses [9]. IPv6 uses DHCPv6 and its operation and function is as similar as DHCP in IPv4.

Routing can be done by static routing and dynamic routing on IPv6 protocol. Static routes are manually defined by the administrator. Static route can be used in that environment where network traffic is predictable and the network design is not so hard. Static route cannot be used in large, continually changing networks because static routes cannot give any action to network changes.

Most networks use dynamic routes for communication. In case of dynamic routing protocols, IPv6 uses updated versions of the same routing protocol that is available for IPv4. The dynamic routing protocol are RIPng, OSPFv3 for IPv6, IS-IS for IPv6 and MP- BGP4 (MultiProtocol BGP) [9].

In this research, more concentration has been done on OSPFv3 (Open Shortest Path First) protocol. It is a link state routing protocol and is the most widely used interior gateway protocol (IGP), operating within a single autonomous system. For IPv4, it is defined as OSPF version 2 in RFC 2328[10] and for IPv6, it is OSPF version 3 in RFC 5340 [11].

C. Benefits of IPv6:

The main benefits using IPv6 protocol is its larger address space which provides several enhancements and therefore allows extensibility, the simplified header format, enhance mobility and support for more security [12].

III. MECHANISMS FOR TRANSITION:

Transition from IPv4 to IPv6 network is not an overnight process, but it takes several years to coexist together. Some mechanisms have been developed that have to permit the co-existence of both the protocol and migration from current version of protocol to future version of protocol. But it is also one issue that which mechanism will be select for the establishment of process to get smooth and seamless translation.

As IPv4 and IPv6 have different protocol profile, there is large difference between these two protocols. It is clear that one protocol cannot communicate easily with another protocol. Most of the developed countries like China, USA, and Korea have shifted their Network on IPV6. Govt. of India has instructed to all ISPs to get ready for migration to IPV6 Network [13]. Hence it has now been the need of the hour to convert this existing IPv4 networks to IPv6 network and it is also a booming field in the near future.

There are several mechanisms to transition from IPv4 network to IPv6 network.

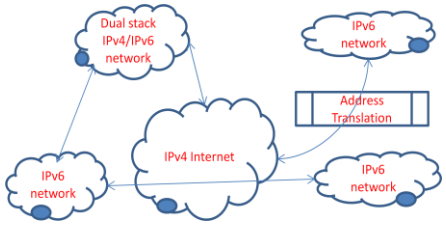

Fig. 1 transition technologies

As shown in above figure, there are some technologies which can be applied for transition from IPv4 to IPv6. Transition mechanisms generally come in one of the three forms: dual stack, address translation and tunnelling mechanisms.

Dual stack:

In dual stack network, node should support both IPv4 and IPv6 protocols. Node may be design to use either one or both protocol depending on the deployment situation. Dual stack technique is reported in RFC 4231[14]. The dual stack method is literally to use two protocol stacks which operate parallel and thus allow the device to functions via either IPv4 protocol or IPv6 protocol. Dual stack can be applied on both end systems and network devices. At the initial stage of migration from IPv4 to IPv6, dual stack is used, but dual stack mechanisms do not solve by themselves IPv4 and IPv6 internetworking situation. And dual stack has the disadvantage that network topology requires two tables and two routing processes. [15]. Translation is required for that.

Translation:

The goal of the translation is to translate packets with IPv6 address to those with IPv4 address. So that the IPv6 - only hosts can talk to the IPv4 - only internet. This capability is

advantages in data centre deployments in that the existing IPv4 infrastructure can remain unchanged, or originally, NAT-protocol Translation (NAT-PT:RFC 2766) was proposed for this purpose.

Translation mechanism is either stateless or stateful. As stateless translation is able to process each conversion individually without any reference to previously translated packets; a stateful translator needs to maintain same form of state with translator to previous translations. The translator must maintain a mapping between the two types of IP addresses. [p 3].

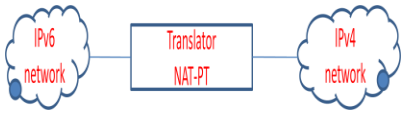

Fig.2 translation method

Tunnelling:

Tunnelling technique involve transport through encapsulation of one protocol within another protocol. IPv6 tunnelling encapsulates IPv6 packet within IPv4 packets and uses the existing IPv4 core to allow IPv6 end systems to communicate IPv4 infrastructure between them. Because IPv6 will be developed over the IPv4 infrastructure, tunnelling provides a way to use the existing routing infrastructure to carry IPv6 traffic. Tunnelling IPv6 packets over IPv4 infrastructure is done by encapsulating IPv6 packets inside IPv4 packets. Up to date, there are different tunnelling methods such as 6to4, ISATAP, Teredo, DSTM, and 6over4 exist. Tunnels may be manually or automatically configured. (Qing-weil and Lin 2007.

IV. DEVELOPMENT OF THE PROBLEM:

Simulator used for the development of research is Packet Tracer (version 6.0.1). Packet Tracer is a network simulator of provided by CISCO that allows users to create network topologies, configured devices, insert packets and check the communication link between devices and simulates a network with multiple visual representations.

The bellowed network described the network for dual stack using Packet Tracer in which there are dual stack three routers 2811 and three generic switches are configured in simulation. Figure 2 shows the dual stack topology in packet tracer.

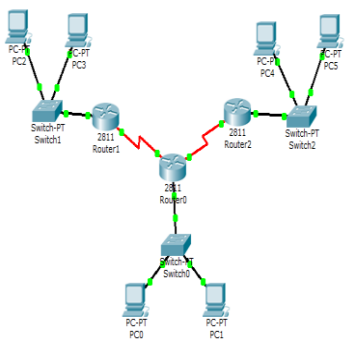

Fig. 2 Dual stack topology in the Packet Tracer simulator.

We shows the process to configure the PC0 is as follow: First PC0 is selected and unfolds a visual interface that has four tabs, Physical, Config, Desktop and Software/Service. In the tab Physical, there are Physical components that could be adopted by the host like, USB hard drive, headphones, wireless cards, microphones and cameras. In the tab Config, there are IP addresses are configured, both of addresses IPv4 and IPv6. In this problem, PC0 is selected and the gateway addresses was defined statically and were for IPv4 is 10.72.26.153 and that for IPv6 is fe80::20b:bedd:fedd:8301. The FastEthernet is statically configured and that is 10.72.26.154/30 for IPv4 and 001:4490:d140:0:290:2bff:fe68:ea4b/64 for IPv6 and this process is same way repeats for other PCs of the figure topology. In the tab Desktop, different utilities are situated, such as a command prompt, web browser, IP configuration, traffic generator and text editor. In the command prompt, using with different commands, it is easy to get information about IP addresses, routes and also send eco massages and checking the communication link and others. See fig 3.

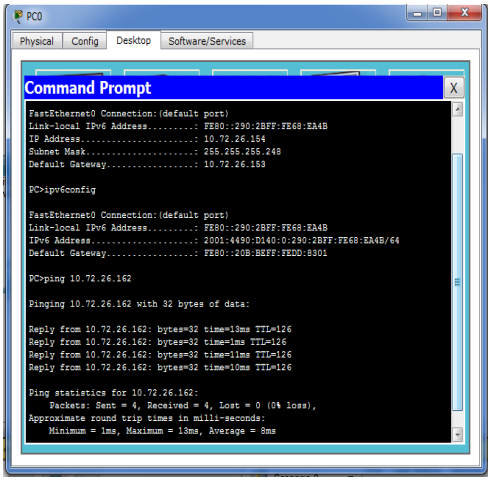

Fig 3: checking IP address and communication link in command prompt.

Configuration of router: The following describes the configuration of router here taking router 0 as example. Router 0 is selected and unfolds a visual interface and there are three tabs, physical, config and CLI. The physical tab is as same as described for host, the tab config is used to perform the router basic configuration in graphical mode and the tab CLI (Command Line Interface) is used for perform configuration with using different commands.

Before configuration of the router, it is necessary to have serial link that is for communication between other routers, since router 2811 have no serial interface, this was add through WIC-2T module to the slot in the router, on the physical tab. And the router was configured using CLI tab.

Configuration of IPv4 router R0 using OSPF: The commands in CLI prompt for configuration of router R0 for IPv4 network using OSPF is as shown in fig 4.

```
R0>enable
R0#config t
R0#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R0(config)#interface fastethernet 0/0
R0(config-if)#ip address 10.72.26.153 255.255.255.248
R0(config-if)#no shut down
```

Fig 4: Configuration of Interface's IPv4.

For the other routers the same procedures are following as described above. Some changes in serial interface 0/0/1 as well as fastethernet 0/0.

Procedure for the configuration using OSPF routing protocol is shown in fig 4. In our example problem there are consider three networks, and the procedure shown is for router R0.

```
R0#enable
R0#config t
R0#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R0(config)#router ospf 1
R0(config-router)#network 10.72.26.152 255.255.255.248 area 0
R0(config-router)#network 10.72.26.128 255.255.255.252 area 0
R0(config-router)#network 10.72.26.132 255.255.255.252 area 0
```

Fig 5: Configuration of OSPF

Configuration of IPv6 and OSPF on the router R0:

Figure 6 shows the steps that are used to enables the IPv6 traffic forwarding.

```
R0#config t
R0#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R0(config)#ipv6 uni
R0(config)#ipv6 unicast-routing
R0(config)#int fa 0/0
R0(config-if)#ipv6 enable
R0(config-if)#ipv6 address 2001:4490:d140::/64
```

Fig 6: Enabling IPv6 and OSPF

Below fig 7 is show that the required step to enable the IPv6 protocol in the serial interface 0/0/0, the routing protocol OSPF matching the process identifier. This process is done in a same way in the other interfaces and routers for the example topology.

```
R0#config t
R0#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R0(config)#ipv6 uni
R0(config)#ipv6 unicast-routing
R0(config)#int se 0/0/0
R0(config-if)#ipv6 ospf 1 area 0
```

Fig 7: configuration of IPv6 and OSPF on the serial interface

With the entire above performed configuration the network that is represented in fig. 2 is ready to carry out communication using the dual-stack transition mechanism.

In translation mechanism NAT-PT Cisco IOS software was designed using RFC 2766 and RFC 2765 as a migration tool to help customers transition their IPv4 networks to IPv6 networks. Using a protocol translator between IPv6 and IPv4 allows direct communication between hosts speaking a different network protocol. Users can use either static definitions or IPv4-mapped definitions for NAT-PT operation. Example topology for translation using NAT-PT router is shown in figure-8 below, where one side network is IPv4- only network and the other side network is IPv6- only network. The router and host configuration is as same way as described for dual stack mechanism, only difference in that is IPv4- only network is configured with only IPv4 addresses and IPv6- only network is configured with only IPv6 addresses. The middle one router is Network Address Translation –Protocol Translation (NAT-PT) which mapping both IPv4 and IPv6 network. Two servers are also described in the topology in which one server is from IPv4 network side and other is from IPv6 network side.

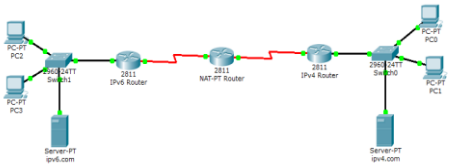

Fig 8: translation method using NAT-PT

Configuration is shown below:

IPv4 router configuration and IPv6 router configuration are same as described above dual stack mechanism, here NAT-PT router configuration is describes. IPv6 network nodes communicate with IPv4 network nodes using an IPv6 mapping of the IPv4 address configured on the NAT-PT router. Configuration of basic IPv4 to IPv6 connectivity for NAT-PT, which consists of configuring NAT-PT prefix globally and enables NAT-PT on an interface, has been included. An IPv6 prefix with a prefix length of 96 must be specified for NAT-PT to use. The IPv6 prefix can be a unique local unicast prefix. The NAT-PT prefix is used to match a destination address of an IPv6 packet. If the match is successful, NAT-PT will use the configured address mapping rules to translate the IPv6 packet to an IPv4 packet.

IPv6 NAT router programming:

```
Router>enable
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ipv6 u
Router(config)#ipv6 unicast-routing
Router(config)#ipv6 nat prefix 2002:1::/96
Router(config)#ipv6 nat v4v6 source 10.72.26.1 2002:1::1
Router(config)#ipv6 nat v4v6 source 10.72.26.2 2002:1::2
Router(config)#ipv6 nat v4v6 source 10.72.26.3 2002:1::3
Router(config)#ipv6 nat v4v6 source 10.72.26.4 2002:1::4
Router(config)#ipv6 nat v6v4 source 2001:4490:D140:0:201:96FF:FE21:BAC1 10.72.26
.33
Router(config)#ipv6 nat v6v4 source 2001:4490:D140:0:201:C7FF:FEEC:D6CB 10.72.26
.34
Router(config)#ipv6 nat v6v4 source 2001:4490:D140:0:290:21FF:FE3C:EC2E 10.72.26
.35
```

Fig. 9 Configuration of NAT-PT router for translation mechanism

The last mechanism for transition process of IPv6 is Tunnelling. Out of above described tunnelling technique, here in this paper Teredo technique is used and simulation is done in Packet Tracer. The following describes the network configuration using Packet Tracer simulator, in which the tunnelling transition method was implemented using two ends IPv6 network in between that IPv4 network was exist. Fig shows one topology which describes the tunnelling technique in that Router 4 and Router 5 are IPv4 and IPv6 dual stack network and all other routers is only IPv4 network. The packet should transfer from router 4 to router 5 using tunnelling. One tunnel has been created inbetween this two router and the packet is only passing through this tunnel only.

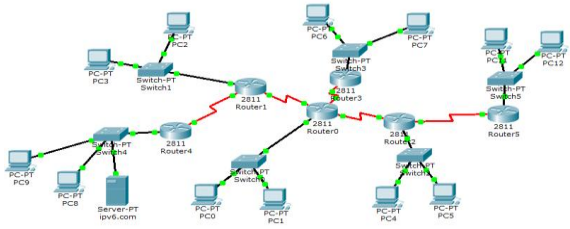

Fig. 10 Tunnelling mechanism in packet tracer simulator

Configuration of router that has IPv6 addresses and wants to communicate with IPv6 network.

```
Router(config)#int tunnel0
Router(config-if)#ipv6 en
Router(config-if)#ipv6 address 2002::1/127
Router(config-if)#tunnel source se0/0/0
Router(config-if)#tunnel destination 10.72.26.145
Router(config-if)#no shut
Router(config-if)#tunnel mode ipv6ip
```

Fig 11. Configuration of router with tunnel source and destination address

To make the settings of routers these were initiated in the same way as the PCs; also were configured in the same manner the IPv4 and IPv6 address in the required interface and the same routing protocols used with the dual stack mechanism; after that the tunnels in the routers were configured, taking router 4 , in the global configuration mode of the router was introduces the command to enable the interface: "interface tunnel", followed by an identifier, here in this case, 0; an address was assigned with the command "ipv6 address" followed by the address and prefix; then it was specified the tunnel source and destination with the command "tunnel source" and "tunnel destination" followed by their respective IPv4 addresses; it was introduced the command "tunnel mode ipv6ip" to specify that the tunnel was manual and that IPv6 is the passenger protocol, being IPv4 in charge of encapsulate and transport IPv6, this was done in a same way In other routers so that the network would be ready to communicate using tunnels.

V. CONCLUSION

Connectivity test has been performed successfully between IPv4 and IPv6 networks. Dual stack transition mechanism gives the results of communication for both the IPv4 and IPv6 protocol. In the case of transition mechanism communication was possible for IPv4 – only network with the IPv6 – only network. For the tunnelling transition mechanism, the encapsulation of IPv6 packets within IPv4 was successfully done.

The above analysis gives the results that all three mechanisms are good according to the scope of the network; each transition mechanism can be beneficial depending on situation of network. Since the Dual Stack mechanism is easier to implement at the initial stage of migration from IPv4 to IPv6 but this device must support both addressing protocols (IPv4 and IPv6), which makes the routing tables to increases considerably and this want process and longer times. The transition mechanism is good choice when IPv4 – only network wants to communicate with IPv6 – only network. On the other side, the tunnelling transition mechanism is chosen for that networks where two sided networks are IPv6 network and intermediate networks are IPv4 network.

REFERENCES

[1] M. Francisco, Planificación y Administración de Redes, Ra- Ma, 2010.
[2] G. Huston, "IPv4 Address Report," Tech. Rep., Sep. 2010. [Online]. Available: http://www.potaroo.net/tools/ipv4
[3] Lanzamiento Mundial de IPv6 2012, http://www.isocmex.org.mx/ipv6_2012.html, última consulta 7 Junio de 2012.
[4] S. Deering and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification," 1998, IETF RFC 2460.
[5] D. Yezid, et al, Prueba de conectividad y tiempo de respuesta del protocolo IPv6 en redes LAN, Redalyc, No. 011, 2002, pp. 55 – 68.
[6] Request for Comments: 2460, Internet Protocol Version 6 (IPv6) Specification, December 1998: Internet Engineering Task Force. http://www.ietf.org/rfc/rfc2460.txt..
[7] H. Silvia, IPv6 Essentials, O"Reilly, 2006.
[8] V. Bob, et al, Acceso a la Wan, Guía de Estudio De CCNA Exploratión, Cisco Press, 2009
[9] A. Ernesto, B. Enrique, Redes Cisco CCNP a fondo, Guía de estudio para profesionales, Alfaomega, 2010.
[10] RFC-2328, Moy, J. (April 1998). "OSPF Version 2". The Internet Society. OSPFv2. Retrieved 2007-09-28
[11] Coltun, R.; D. Ferguson, J Moy, A. Lindem (July 2008). "OSPF for IPv6". The Internet Society. OSPFv3.Retrieved 2008-07-23
[12] V. Bob, et al, Acceso a la Wan, Guía de Estudio de CCNA Exploratión, Cisco Press, 2009.
[13] India, Department of Telecommunication, National IPv6 Deployment Roadmap, policy Guidelines [Online] Available: http://www.dot.gov.in/ipv6/ipv6activities.html.
[14] E. Nordmark and R. Gilligan". Basic Transition Mechanisms for IPv6 Hosts and Routers. RFC 4213 (Proposed Standard), Oct. 2005.
[15] A. Oscar, Migración del protocolo IPv4 a IPv6, ContactoS 79, 2011, pp. 55 – 60.