RESEARCH ARTICLE OPEN ACCESS

Implementation of "Traslator Strategy" For Migration of Ipv4 to Ipv6

Dr. K.R.R.Mohan Rao[1], Saiteja Kanneganti[2,] Chandra Venkata Sai Rohith[3]
Professor 4.Charan Teja Somepalli B.Tech Project Scholar
B.Tech Project Scholar 5.Kantamneni Ravi Teja
B.Tech Project Scholar
Department of Electronics and Communications Engineering, K L University, Guntur

Abstract
This paper is focused on the Translator strategy for migration of IPv4 to Ipv6 implemented in Cisco packet tracer. It describes the design and configuration of network devices and packet transfer between devices of IPv4 and IPv6 networks using NAT-PT as transition mechanism. First major version of IP, IPv4 is the dominant protocol of internet.IPv6 is developed to deal with long anticipated problem of IPv4 running out of addresses. 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.

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. . Different Network elements such as routers, switches, gateways etc., have been interconnected together for communication of information over the Data networks. The Layer 3 devices are connecting the WAN interfaces for data transmission and forwarding the packets using routing tables where as 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.

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 now. 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.

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.
Although IPv6 solves addressing issues for customers, a long transition period is likely before customers move to an exclusive IPv6 network environment. During the transition period, any new IPv6-only networks will need to continue to communicate with existing IPv4 networks **.**NAT-PT is designed to be deployed to allow direct communication between IPv6-only networks and IPv4-only networks**.**

One of the benefits of NAT-PT is that no changes are required to existing hosts, because all the NAT-PT configurations are performed at the NAT-PT router. Customers with existing stable IPv4 networks can introduce an IPv6 network and use NAT-PT to allow communication without disrupting the existing network.

II. IPv6

The IPv6 protocol is an upgrade of the IPv4 protocol, belonging to the TCP/IP (Transmission Control Protocol /Internet Protocol) suite's protocol stack, used to identify, by means of an IP address, each computer interface or device that connects to Internet or to an Intranet [7]. 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

users. [8]

IPv6 is basic to the operation of the network and the first specifications of this protocol were developed by Internet Engineering Task Force (IETF) at the 90‟s. An important factor for the adoption of the new protocol is the expansion in use of new technologies based on the concept „always on‟, such as Ethernet, optical fiber, and Power Line Communication; however, but the main motivation for the transition to the new protocol is the expansion of available public addresses for Internet, which will allow the connection to the network for multiple devices such as PDAs and mobile phones, among others[8]. The size of an IPv6 address is 128 bits, 4 times bigger than an IPv4 address; an 32 bits address space allows up to 4.294.967.296 combinations, while the 128 bits of an IPv6 address allows up to 340.282.266.920.938.463.463.374.607.431.768.211.4 65 (or 3,4 x 1038), therefore it is obvious the increase in available addresses [10].

At the end of the seventies, when the IPv4 address space was designed, was unimaginable that it could be exhausted; however due to technological changes and assignation politics that did not foreseen the recent increase in the Internet hosts quantity, the IPv4 address space was depleted to such an extent that in 1992 was made evident the need for a replacement [10].

IPv6 Address Format

As mentioned, an IPv6 address has 128 bits or 16 bytes, this address is divided into eight hexadecimal blocks of 16 bits separated by colons ":"; for example:
FE80:0000:0000:0000:0202:B3FF:FE1E:8329 [11].

In an IPv6 address, the zeros on the left on the block containing them can be omitted, and also contiguous blocks of zeros can be simplified using double colon "::".

On the basis of the above, starting from the previous address can be obtained the following address, FE80::202:B3FF:FE1E:8329.

The network prefix in an IPv6 address is represented in the same way that IPv4, for example, take the IPv4 address 192.168.1.0/27, this means that the first 27 bits are network's and the remaining 5 are which identify a device, thus in IPv6 the following address ffe:b00:c18:1::1/64 indicates that the first 64 bits identifies the network (3ffe:b00:c18:1) and the remaining 64 bits identifies the device in that network (::1) [12].

2.2 Assignment of Addresses

IPv6 addresses can be statically assigned using an identifier (ID) of manual interface or an ID of EUI-64 interface, it also can be dynamically configured by using stateless address auto configuration.

Static configuration: Consists on manually enter the IPv6 address of a node in a configuration file or through the use of proper tools of the operative system. Information to be included is the IPv6 address and the network prefix size [12]. This configuration is divided into static configuration using the ID of manual interface, in which the entire IPv6 address is used, both the network section and the device identifier section [11]; and into static configuration using the ID of EUI-64 interface, in which in order to obtain the ID, the host takes the MAC address from the link layer device, however as the MAC address only has 48 bits, then the MAC address is split in half and in the middle is inserted the default hexadecimal value FFFE of 16 bits in order to complete an unique interface ID of 64 bits [11].

Dynamic configuration: Through this method the host automatically learns the necessary parameters to obtain an IP address that will be used in the communication process with end devices. It is divided into stateless auto configuration, in which each router broadcasts information of the network including the prefix assigned to each of its interfaces. With the obtained information in this broadcasting, the end systems create a unique address concatenating the prefix with the ID in EUI-64 interface format. The "stateless" name comes from that no device keeps track of the assigned IP addresses [14]. The other method is with DHCPv6, its operation is similar to the traditional DHCP, hosts obtain its interface address, information and configuration parameters from a server [15].

2.3 Advantages of using IPv6

Among the main advantages of using the IPv6 protocol are: improved IP address (a bigger address space offer several enhancements), the simplified header (better efficiency on routing to performance scalability and forwarding speed), enhanced mobility and security (ensure that abides standards functionality of mobile IP and IP security) [11].

III. Routing

Routing on IPv6 can be done through the use of static routes and dynamic routing protocols. Static routes are manually defined by the administrator so the router learns about a remote network, are usually used when the routing is from a network to a single connection network; a single connection network is a network accessible by only one route [15].

In regards to dynamic routing protocols, IPv6 uses updated versions of the same routing protocols available for IPv4; among the most important ones are: RIPng, EIGRP for IPv6, IS-IS for IPv6, MP-BGP4 (Multi Protocol BGP) and OSPFv3 [14].

Open Shortest Path First (OSPF) is a routing protocol for Internet Protocol (IP) networks. It uses a link state routing algorithm and falls into the group of interior routing protocols, operating within a single autonomous system (AS). It is defined as OSPF Version 2 in RFC 2328 (1998) for IPv4. The updates for IPv6 are specified as OSPF Version 3 in RFC 5340 (2008).

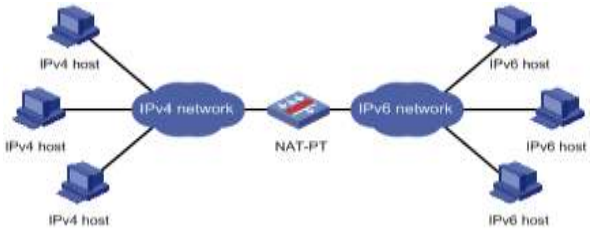
IV. Transition Mechanisms

As seen in recent years transition from IPv4 to IPv6 has not been an immediate process but they had to coexist together for several years, thus mechanisms has been developed that have allowed the coexistence and migration from one protocol to another; there are several mechanisms but in this work there are only mentioned two, since those are the used to perform the tests.

Dual stack: This mechanism implements both protocols on each node in the network; IPv4 and IPv6, each node with dual stack in the network will have two addresses, one for IPv4 and other for IPv6. This procedure is easy to implement and is widely supported; however it has the disadvantage that the network topology requires two tables and two routing processes [17].

Tunneling: On using tunneling, the routers that execute IPv4 and IPv6 at the same time encapsulate IPv6 traffic inside IPv4 packets. The origin of the IPv4 is the own local router, and the destination will be the router at the end of the tunnel. When the destination router receives the IPv4 packet, decapsulates it and send forwards the IPv6 traffic that was encapsulated. This tunneling system is effective although increases the MTU since it consumes 20 bytes with each IPv4 header on the intermediate links and is also difficult the resolution and tracking of problems [14].

NAT-PT: In computer networking, network address translation (NAT) provides a method of modifying network address information in Internet Protocol (IP) datagram packet headers while they are in transit across a traffic routing device for the purpose of remapping one IP address space into another. The term NAT44 is sometimes used to more specifically indicate mapping between two IPv4 addresses; this is the typical case while IPv4 carries the majority of traffic on the Internet. NAT64 refers to the mapping of an IPv4 address to an IPv6 address, or vice versa.



There are different types of NAT they are:

Static NAT: This type of NAT converts the IPv6 address into IPv4 and vice versa to perform the routing. In this type of routing the no. of IP addresses required is more when compared to the other type of NAT as it requires IP addresses for all components.

Dynamic NAT: Puts a dynamic mapping between an internal private address and a public address. This also creates a one-to-one relationship on a first-come-first-served basis. The public address that is used by private devices can change over time and cannot be trusted. This would allow systems out, when you are not concerned with outside devices trying to connect in, as with the previous web server example.

V. CISCO PACKET TRACER

Cisco Packet Tracer is a network simulation program that allows students to experiment with network behavior and ask "what if" questions. As an integral part of the Networking Academy comprehensive learning experience, Packet Tracer provides simulation, visualization, authoring, assessment, and collaboration capabilities and facilitates the teaching and learning of complex technology concepts. The current version of Packet Tracer supports an array of simulated Application Layer protocols, as well as basic routing with RIP, OSPF, and EIGRP, to the extents required by the current CCNA curriculum. While Packet Tracer aims to provide a realistic simulation of functional networks.

5.1.Implementation of Translator strategy using Static NAT:

Figure shows the change in the router"s mode from user to global configuration and the assignment of the name "R1".

```
R1#enable
R1#configure terminal
Enter configuration commands,
R1(config)#hostname R1
R1(config)#
```

Fig.. Modification of the router‟s name.

Configuration of IPv4:

The configuration of the remaining interfaces on the router R1 is similar to the above with the only difference that in the serial interface 0/0/1 as well as in the fastEthernet one 0/0.

```
R1(config)#
R1(config)#interface serial 0/0/0
R1(config-if)#ip address 200.125.15.1 255.255.255.0
R1(config-if)#clock rate 64000
R1(config-if)#no shutdown
```

Fig. Configuration of interfaces IPv4.

Configuration of IPv6:

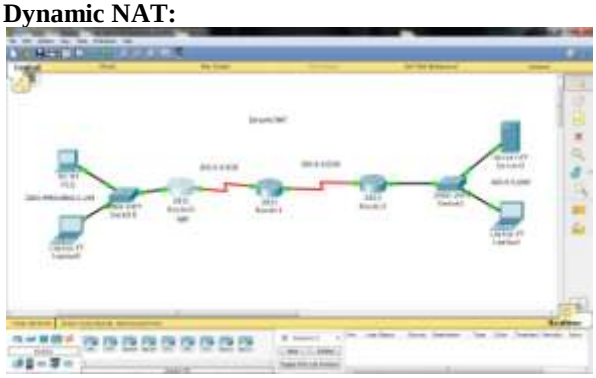
```
R1(config)#
R1(config)#ipv6 unicast-routing
R1(config)#ipv6 router rip cisco
```

Fig Configuration of interfaces IPv6

Ping Information:

Pinging 200.4.6.2 with 32 bytes of data:
Reply from 200.4.6.2: bytes=32 time=15ms TTL=125
Reply from 200.4.6.2: bytes=32 time=11ms TTL=125
Reply from 200.4.6.2: bytes=32 time=11ms TTL=125
Reply from 200.4.6.2: bytes=32 time=11ms TTL=125
Ping statistics for 200.4.6.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 11ms, Maximum = 15ms, Average = 12ms
Pinging 2001:4490:D960:FF::5 with 32 bytes of data:
Reply from 2001:4490:D960:FF::5: bytes=32 time=15ms TTL=125
Reply from 2001:4490:D960:FF::5: bytes=32 time=11ms TTL=125
Reply from 2001:4490:D960:FF::5: bytes=32 time=11ms TTL=125
Reply from 2001:4490:D960:FF::5: bytes=32 time=11ms TTL=125
Ping statistics for 2001:4490:D960:FF::5:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 11ms, Maximum = 15ms, Average = 12ms

5.2.Implementation of Translator strategy using Dynamic NAT:



Pinging:

Pinging 2001::C804:503 with 32 bytes of data:
Reply from 2001::C804:503: bytes=32 time=11ms TTL=125
Reply from 2001::C804:503: bytes=32 time=11ms TTL=125
Reply from 2001::C804:503: bytes=32 time=11ms TTL=125
Reply from 2001::C804:503: bytes=32 time=14ms TTL=125
Ping statistics for 2001::C804:503:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 11ms, Maximum = 14ms, Average = 11ms
Pinging 2001::C804:502 with 32 bytes of data:
Reply from 2001::C804:502: bytes=32 time=10ms TTL=125
Reply from 2001::C804:502: bytes=32 time=14ms TTL=125
Reply from 2001::C804:502: bytes=32 time=14ms TTL=125
Reply from 2001::C804:502: bytes=32 time=11ms TTL=125
Ping statistics for 2001::C804:502:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 10ms, Maximum = 14ms, Average = 12ms

VI. Conclusion

It was observed that packets has been transferred successfully from IPv4 network devices to IPv6 network devices. The NAT-PT transition mechanism is more advanced when compared to Dual stack and Tunneling transition mechanisms because the dual stack and tunneling have their own disadvantages. Our future scope is to implement this NAT-PT transition mechanism in hardware equipment.

References:

[1]. H. Houassi, A. Bilami, IP address lookup for Internet routers using cache routing table, International Journal of Computer Science

Issues, Vol. 7, No 8, 2010.
[2]. B. Luis, Crece la potencia de la Red, El Informador, 2004, México.
[3]. M. Francisco, Planificación y Administración de Redes, Ra-Ma, 2010.
[4]. Nueva era en Internet: Se terminó el stock central de direcciones IPv4 de Internet, 2011, http://lacnic.net/sp/, última consulta 6 Junio de 2012.
[5]. Lanzamiento Mundial de IPv6 2012, http://www.isocmex.org.mx/ipv6_2012.html , última consulta 7 Junio de 2012.
[6]. IPv6 México, http://www.ipv6.unam.mx/, última consulta 7 Junio de 2012.
[7]. F. Azael, IPv6 ¡toda una realidad! 2005, http://www.enterate.unam.mx/Articulos/2005/enero/ipvseis. htm, última consulta 7 agosto de 2012.
[8]. A. Abu, Comparison study between IPV4 & IPV6, International Journal of Computer Science Issues, Vol. 9, No 1, 2012.
[9]. IPv6 la transición necesaria, Computerworld, 2004, http://www.idg.es/computerworld/articulo.asp?id=154237, última consulta 28 Julio de 2012.
[10]. D. Yezid, et al, Prueba de conectividad y tiempo de respuesta del protocolo IPv6 en redes LAN, Redalyc, No. 011, 2002, pp. 55 – 68.
[11]. V. Bob, et al, Acceso a la Wan, Guía de Estudio de CCNA Exploratión, Cisco Press, 2009.
[12]. H. Silvia, IPv6 Essentials, O"Reilly, 2006.
[13]. J. Felipe, Estudio e Implementación de una Red IPv6 en la UTFSM, Título De Ingeniero Civil Telemático, Universidad Técnica Federico Santa María, Valparaíso Chile, 2009.
[14]. A. Ernesto, B. Enrique, Redes Cisco CCNP a fondo, Guía de estudio para profesionales, Alfaomega, 2010.
[15]. C. Mariano, et al, El protocolo IPv6, Departamento de electrónica Facultad de Ciencias Exactas, Ingeniería y Agrimensura, Universidad Nacional del Rosario, 2006.
[16]. O. Wendell, CCNA ICND2. Guía Oficial para el Examen de Certificación, Cisco Press, 2008.
[17]. A. Oscar, Migración del protocolo IPv4 a IPv6, ContactoS 79, 2011, pp. 55 - 60.

 Dr.K.R.R.Mohan Rao Completed Ph.D in 2012. Presently working as professor at K L university in ECE department. His research interest Sensor networks. His having 24 years teaching experience and 5 years research experience. Published two text books in networking and having 5 scopus index journals and 20 international journals

 Mounisha Peduru is pursuing her B. Tech in Electronics and Communication Engineering from K L University. She is member of IETE. She is getting specialization in Networking. Her interested areas include Wireless sensor networks and Information theory and coding. As a part of our project we done this work.

 P.P.V.K.RaghuRam is pursuing his B.Tech in Electronics and Communication Engineering from K L University. He is member of IETE. He is getting specialization in Networking . His interested area include Computer Networks. As a part of our project we done this work.

 Shanmukharjuna Reddy Bade is pursuing his B.Tech in Electronics and Communication Engineering from K L University. He is member of IETE. He is getting specialization in Networking . His interested areas include Wireless Sensor Networks and Network Security. As a part of our project we done this work.

 Bulusu devi sowjanya is pursuing his B.Tech in Electronics and Communication Engineering from K L University. He is member of IETE. He is getting specialization in Networking . His interested areas include Wireless Sensor Networks and Network Security. As a part of our project we done this work.

 D.Sai Teja is pursuing his B.Tech in Electronics and Communication Engineering from K L University. He is member of IETE. He is getting specialization in Networking . His interested area include Computer Networks. As a part of our project we done this work.

.