Analysis of IPv4 to IPv6 Migration Techniques in Enterprise Environments

P. Ramesh Kumar, S. Venkata Rao*

PG Scholar, Dept. of ECE, JNTU Hyderabad, Telangana, India
Lecturer, Dept. of ECE, JNTU Hyderabad, Telangana, India

ABSTRACT

Currently, the Internet world is confronting the huge issue that is exhaustion of IP addresses with the IPv4 protocol. This paper contains the imperative hypothetical ideas of new era Internet Protocol IPv6 which tackles the issue of IP tending to furthermore concentrate on IPv6 address design, directing and three mechanisms of migration from IPv4 to IPv6 system: Dual Stack, Translation and Tunneling utilizing Network Simulator as Packet tracer. This paper more accentuation on network migration from IPv4 to IPv6 which is not so distant future pattern.

INTRODUCTION

Today, with the expanding of innovation, the quantity of clients of Internet are expanding quick, thus it must need more number of IP locations in light of the fact that every gadget which utilizes web needs unique IP address. However many devices that associate through Internet are utilizing Internet Protocol rendition 4, since IPv4 has 32-bit address space, it locations and it is roughly 4 billion locations. With the expanding the innovation, PCs, as well as portable workstation, mobiles, iPod, printer, computer games, other restorative instruments, auto mobiles and other gadgets likewise utilize Internet administration. So with the restricted address space of IPv4 it resemble a weight since it has no more office to backing to give IP address to each existed gadget which is utilizations Internet. Address space of right now utilized web protocol variant 4 is excessively restricted, making it impossible to handle the new addresses. As past a few techniques were produced to conquer this address space issue to expand the eventual fate of Internet Protocol adaptation 4 (IPv4) alongside Network Address Translation (NAT), Variable Length Subnet Mask (VLSM), Classless Inter Domain Routing (CIDR) and others [1], after that, these all innovation insufficient to spare the fate of Internet Protocol form 4 (IPv4). Presently IPv4 Internet is confronting a progression of issues including address fatigue, steering versatility and broken end-to-end property. IANA (Internet Assigned Number Authority) had come up short on worldwide IPv4 address pool in Feb. 2011, while reproductions demonstrate that inside 3 years all the RIRs (Regional Internet Registries) will deplete their IPv4 address space [2]. June 6, 2012 was the chosen date by the Internet Society (ISOC) and different associations in the field as the overall dispatch of IPv6. On that day number of organizations and associations from everywhere throughout the world empowers the operations of their entries and different types of presences on the Internet with the IPv6 protocol absolutely [3].

IPV6

Internet Protocol form 6 (IPv6) is created as the cutting edge network layer protocol, to conquer the issues of IPv4 [4]. The IPv6 protocol address is 128-bit long, of 32-bit of IPv4 address. So it makes 3.4*10^38 conceivable address. This is extensive number. These new IPv6 addresses will take care of the Internet demand for the grooving future [5]. Each gadget on the web must be doled out an IP address keeping in mind the end goal to speak with different gadgets. With the regularly expanding number of new gadget being associated with the Internet, the requirement for a bigger number of locations than IPv4 can suit. IPv6 is utilizations 128-bit address permitting 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 purpose behind selection of new protocol is the development of address locations.

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 casesensitive, 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 is 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 range is 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 designated either by statically or auto designed. Address that can statically role out is utilizing identifier (ID) of manual interface or an ID of EUI-64 interface. Furthermore, it is likewise powerfully designed by utilizing stateless auto setup or by DHCPv6. Static configuration: Manually enter the IPv6 address of a node in a file or it is through any releated tools of the operating 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 fetch 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 divided 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: Using 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 fetch 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.

Directing should be possible by static steering and element directing on IPv6 protocol. Static courses are physically characterized by the chairman. Static course can be utilized as a part of that environment where system activity is unsurprising and the system outline is not all that hard. Static course can't be utilized as a part of huge, constantly changing systems since static courses can't give any activity to network changes. Most systems use dynamic courses for correspondence. If there should arise an occurrence of element steering protocols, IPv6 utilizes redesigned variants of the same directing protocol that is accessible for IPv4. The element directing protocol are Ring, OSPFv3 for IPv6, IS-IS for IPv6 and MP-BGP4 (Multiprotocol BGP) [9].

In this exploration, more fixation has been done on OSPFv3 (Open Shortest Path First) protocol. It is a connection state directing protocol and is the most generally utilized inside portal protocol (IGP), working inside a solitary self-governing framework. For IPv4, it is characterized as OSPF form 2 in RFC 2328[10] and for IPv6, it is OSPF rendition 3 in RFC 5340 [11].

C. Benefits of IPv6:

The principle advantages utilizing IPv6 protocol is its bigger location space which gives a few upgrades and hence permits extensibility, the rearranged header design, improve versatility and backing for more security [12].

MECHANISMS FOR TRANSITION

Transition from IPv4 to IPv6 system is not an overnight procedure, but rather it takes quite a while to match together. A few components have been produced that need to allow the conjunction of both the protocol and migration from current adaptation of protocol to future version of protocol. In any case, it is additionally one issue what method will be selected for the foundation of procedure to get smooth and consistent interpretation.

As IPv4 and IPv6 have diverse protocol profile, there is substantial distinction between these two protocols. Unmistakably one protocol can't discuss effectively with another protocol. A large portion of the created nations like China, USA, and Korea have moved their Network on IPV6. Govt. of India has taught to all ISPs to get prepared for relocation to IPV6 Network . Consequently it has now been the need of great importance to change over these current IPv4 systems to IPv6 system and it is likewise a blasting field in the close future. Here are a few components to move from IPv4 system to IPv6 network. As appeared in above figure, there are a few advances which can be connected for move from IPv4 to IPv6. Transition mechanisms generally come in one of the three forms: dual stack, address translation and tunnelling mechanisms.

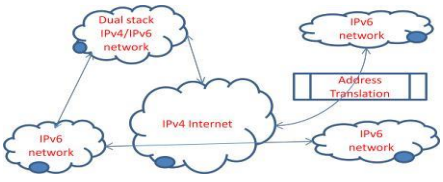

Fig. 1 transition technologies

Double stack:
In double stack system, file ought to bolster both IPv4 and IPv6 protocols. File might be outline to utilize it is possible that one or both protocol relying upon the organization circumstance. Double stack system is accounted for in RFC 4231. The double stack strategy is truly to utilize two protocol stacks which work parallel and therefore permit the gadget to capacities through either IPv4 protocol or IPv6 protocol. Double stack can be connected on both end frameworks and system gadgets. At the underlying phase of relocation from IPv4 to IPv6, double stack is utilized, yet double stack instruments don't settle without anyone else's input IPv4 and IPv6 internetworking circumstance. At the starting 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 corn that network topology requires two tables and two routing processes. [15]. Translation is necessaery for that.

Interpretation:
The objective of the interpretation is to decipher bundles with IPv6 address to those with IPv4 address. So that the IPv6 - no one but has can converse with the IPv4 - just web. This capacity is preferences in server farm arrangements in that the current IPv4 base can stay unaltered, or initially, NAT-protocol Translation (NAT-PT: RFC 2766) was proposed for this reason.

Interpretation instrument is either stateless or stateful. As stateless interpretation can prepare every change separately with no reference to already deciphered parcels; a stateful interpreter needs to keep up same type of state with interpreter to past interpretations. The interpreter must keep up a mapping between the two sorts of IP address. [p 3].

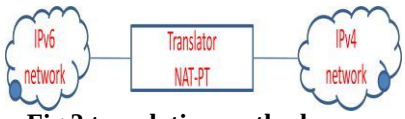

Fig.2 translation method

Translation:
The goal of the translation is to translate packets with IPv6 address to clients with IPv4 address. So that the IPv6 - only hosts can talk to the IPv4 - only internet. This capability is network written as 2002:db80:449:5a63::/64 initiates at address 2002:db80:5a63:0000:0000:0000:0000 and ends at 2001:db80:449:5a63:ffff:ffff:ffff:ffff [7]

ADVANCEMENT OF THE PROBLEM

Test system utilized for the advancement of exploration is Packet Tracer (variant 6.0.1). Parcel Tracer is a system test system of gave by CISCO that permits clients to make system topologies, arranged gadgets, embed bundles and check the correspondence join amongst gadgets and mimics a system with various visual representations. The howled system depicted the system for double stack utilizing Packet Tracer as a part of which there are double stack three switches 2811 and three non specific switches are arranged in reenactment. Figure 3 demonstrates the double stack topology in bundle tracer.

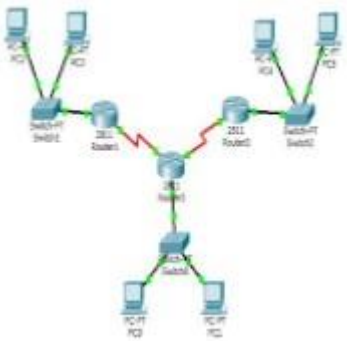

Fig. 3 Dual stack topology in the Packet Tracer simulator.

We demonstrate the procedure to design the PC0 is: First PC0 is chosen and unfurls a visual interface that has four tabs, Physical, Config, Desktop and Software/Service. In the tab Physical, there are Physical parts that could be embraced by the host like, USB hard drive, earphones, remote cards, mouthpieces and cameras. In the tab Config, there are IP locations are arranged, both of locations IPv4 and IPv6. In this issue, PC0 is chosen and the

portal addresses was characterized statically and were for IPv4 is 10.72.26.153 and that for IPv6 is fe80::20b: bedd: fedd:8301. The Fast Ethernet is statically arranged and that is 10.72.26.154/30 for IPv4 and 001:4490: d140:0:290:2bff: fe68: ea4b/64 for IPv6 and this procedure is same route rehashes for different PCs of the figure topology. In the tab Desktop, distinctive utilities are arranged, for example, a summon brief, web program, IP design, movement generator and content tool. In the summon brief, utilizing with various orders, it is anything but difficult to get data about IP locations, courses furthermore send eco kneads and checking the correspondence connection and others. See fig 4.

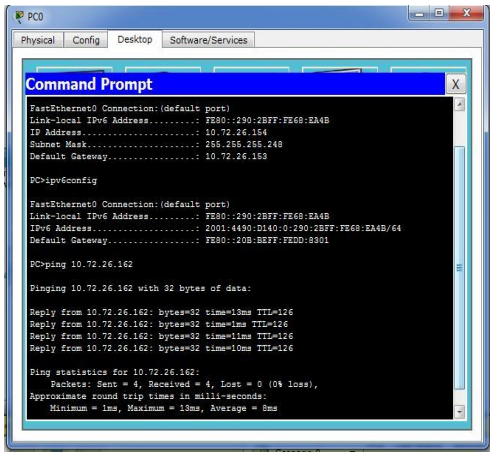

Fig 4: checking IP address and communication link in command prompt.

Design of switch: The accompanying depicts the arrangement of switch here taking switch 0 as illustration. Switch 0 is chosen and unfurls a visual interface and there are three tabs, physical, config and CLI. The physical tab is as same as depicted for host, the tab config is utilized to play out the switch essential arrangement in graphical mode and the tab CLI (Command Line Interface) is utilized for perform design with utilizing distinctive summons.

Before arrangement of the switch, it is important to have serial connection that is for correspondence between different switches, since switch 2811 have no serial interface, this was add through WIC-2T module to the opening in the switch, on the physical tab. What's more, the switch was designed utilizing CLI tab.

Arrangement of IPv4 switch R0 utilizing OSPF: The charges in CLI brief for setup of switch R0 for IPv4 system utilizing OSPF is as appeared as a part of fig 5.

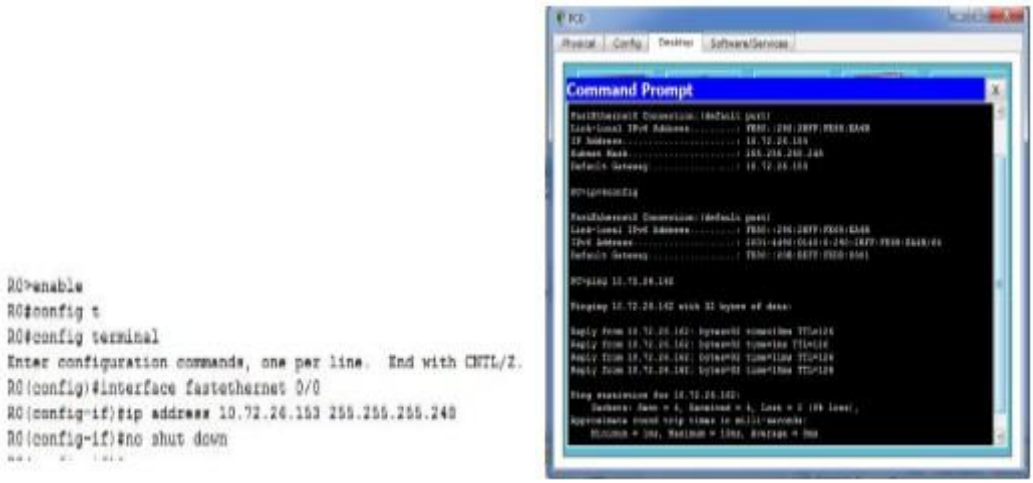

Fig 5: Configuration of Interface's IPv4

For alternate switches the same strategies are taking after as depicted previously. A few changes in serial interface 0/0/1 and in addition quick Ethernet 0/0. System for the design utilizing OSPF directing protocol is appeared in

fig 6. In our illustration issue there are consider three systems, and the methodology demonstrated is for switch 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 6: Configuration of OSPF

Setup of IPv6 and OSPF on the switch R0:
Figure 7 demonstrates the strides that are utilized to empowers the IPv6 movement sending.

```
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 7: Enabling IPv6 and OSPF

Underneath fig 7 is demonstrate that the obliged venture to empower the IPv6 protocol in the serial interface 0/0/0, the steering protocol OSPF coordinating the procedure identifier. This procedure is done same in alternate interfaces and switches for the case topology. With the whole above performed design the system that is spoken to in fig. 2 is prepared to do correspondence utilizing the double stack move system.

```
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 8: configuration of IPv6 and OSPF on the serial interface

In interpretation instrument NAT-PT Cisco IOS programming was outlined utilizing RFC 2766 and RFC 2765 as a relocation apparatus to help clients move their IPv4 systems to IPv6 systems. Utilizing a protocol interpreter amongst IPv6 and IPv4 permits direct correspondence between hosts talking an alternate system protocol. Clients can utilize either static definitions or IPv4-mapped definitions for NAT-PT operation. Illustration topology for interpretation utilizing NAT-PT switch is appeared in figure-9 beneath, where one side system is IPv4-just system and the other side system is IPv6-just system. The switch and host arrangement is as same path as portrayed for double stack instrument, just distinction in that is IPv4-just system is designed with just IPv4 locations and IPv6-just system is arranged with just IPv6 addresses. The center one switch is Network Address Translation –Protocol Translation (NAT-PT) which mapping both IPv4 and IPv6 system. Two servers are likewise portrayed in the topology in which one server is from IPv4 system side and other is from IPv6 system side.

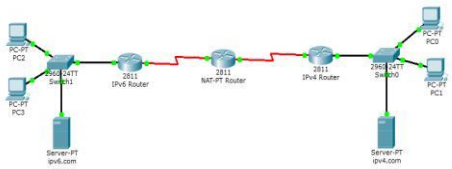

Fig 9: translation method using NAT-PT

CONFIGURATION IS DEMONSTRATED AS FOLLOWS:

IPv4 router configuration and IPv6 router configuration are similar as described above dual stack mechanism, here NATPT router configuration is describes. IPv6 network nodes communicate with IPv4 network nodes using an IPv6 mapped for 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 and enables NAT-PT on an interface are

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 convert 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. 10 Configuration of NAT-PT router for translation mechanism

The last method 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 below 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 that already 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 in between this two router and the packet is only passing through this tunnel only.

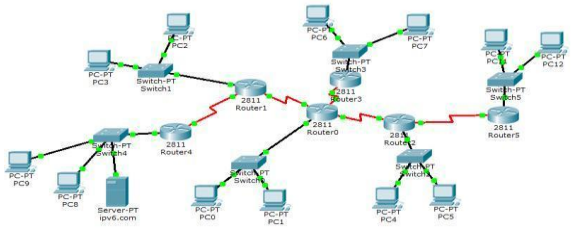

Fig. 11 tunneling mechanism in packet tracer simulator

Configuration of switch that has IPv6 delivers and needs to speak 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 12. 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.

CONCLUSION

Connectivity test successfully has been performed among IPv4 and IPv6 networks. Dual stack transition method results the communication for both the IPv4 and IPv6 protocol. In the transition mechanism , communication was possible for only IPv4 network with the only IPv6 network. In tunnelling transition mechanism, the combination of IPv6 packets with IPv4 has been successfully done. The above analysis gives the results that all three mechanisms are better according to the scope of the network; each transition mechanism can be profitable depending on situation of network. Since the Dual Stack mechanism is easy 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

routing tables to enchance 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 doble 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] Design Concept and Simulation of Migration from Present IPv4 Network to Future IPv6Network Using Three Transition Mechanisms" april 2014 Research Gate.