IPv4 & IPv6 COMPARISON,TRANSITION TECHNOLOGIES & CONFIGURING IPv6 OVER IPv4 TUNNELING

Dr J Sebastian Nixon
Department of CS & IT
CNCS, Wolaita Sodo University
Federal Democratic Republic of Ethiopia

Dr A Francis Saviour Devaraj
Department of CS & IT
CNCS, Wolaita Sodo University
Federal Democratic Republic of Ethiopia

Abstract— **The telecom and hand held smart devices (mobile, tablets) companies around the globe have made a revolution in making Internet available to common man in a much affordable cost. Luring the public with new technologies available at an ease has contributed to scalability of users on the Internet. This has challenged the current Internet Protocol IPv4 in terms of address space. This paved the way for IPv6. The exhaustion of IPv4 address space increases pressure on network operators to implement IPv6. So, in future it may become mandatory for all internet users to migrate from IPv4 to IPv6. In this paper we deliberate about various aspects of IPv4 & IPv6, Transition Technologies from IPv4 to IPv6, GRE (Generic Routing Encapsulation) and a demonstration of how tunneling configuration of IPv6 over IP4 is done in routers using GNS3, & wireshark.**

Keywords: ***IPv4, IPv6, Transition, tunneling***

I. INTRODUCTION

An **Internet Protocol** address (**IP** address) is a unique numerical label assigned to each device like computer, printer, hand held device like tab, mobile etc.. participating on a computer network that uses the **Internet Protocol** for communication. IP was the connectionless datagram service in the original *Transmission Control Program* introduced by Vint Cerf and Bob Kahn in 1974, the other being the connection-oriented Transmission Control Protocol (TCP). The Internet protocol suite is therefore often referred to as TCP/IP.

In 1991, the IETF decided that the current version of IP, called IPv4, had outlived its design. The problem of the limited IPv4 addresses could be solved in different alternative technologies like sub netting, Network Addresses Translation (NAT) & Classless Inter-Domain Routing (CIDR) but they may be the temporary solution they will no longer be able to handle the fast growth of Internet.

Version 5 of the IP family was an experimental protocol developed in the 1980s. IPv5 (also called the Internet Stream Protocol) was never widely deployed. Since the number 5 was already allocated, this number was not considered for the successor to IPv4. Several proposals were suggested as the IPv4 successor and each was assigned a number. In the end, it happened that the one with version number 6 was selected. **[1]**

The new version of IP called either IPng (Next Generation) or IPv6 (IPversion 6) was the result of a long and tumultuous process which came to a head in 1994, when the IETF gave a clear direction for IPv6. IPv6 is designed to solve the problems of IPv4. [2]. IPv6 is not entirely different from IPv4. Whatever is available in IPv4 also exists in IPv6.
The differences between IPv6 and IPv4 can be classified in five major areas:

1. Addressing and routing
2. Security
3. Network Address Translation
4. Administrative workload
5. Support for mobile devices.

II. INTERNET PROTOCOL VERSION 4 (IPv4)

Internet Protocol version 4 (IPv4) is the fourth version of the Internet Protocol (IP) and it is the first version of the protocol to be widely deployed. IPv4 is still by far the most widely deployed Internet Layer protocol. It uses a 32 bit addressing and allows for 4,294,967,296 unique addresses [3]. Even though the name seems to imply that it's the fourth generation of the key Internet Protocol, version 4 of IP was the first that was widely used in modern TCP/IP. It provides the basic datagram delivery capabilities upon which all of TCP/IP functions and it has proven its quality in use over a period of more than two decades.

III. INTERNET PROTOCOL VERSION 6 (IPv6)

Internet Protocol version 6 (IPv6) is a version of the Internet Protocol (IP) intended to succeed IPv4. IPv6 is proposed by IETF to provide the Internet with larger address space and better performance [4]. It provides a very large address space. It has a very simplified header. After full implementation of IPv6, every host can directly reach other hosts of course with limitations like firewall, organizations policy etc.. Makes inter segment communication possible because it supports both stateful and stateless auto configuration mode of its host devices. High-bandwidth multimedia and fault tolerance applications are the focus of the major goal of IPv6. IPv6 also defines a new kind of service called **"anycast".** Another aspect of VPNs built into IPv6 is **QoS** (Quality of Service). IPv6 builds-in and requires these protocols, which will mean that secure networks will be easier to build and deploy in an IPv6 world. Find below is table that compares IPv4 & IPv6.

Table 1: Comparison of IPv4 & IPv6

Feature	IPv4	IPv6
Address	32 bit length.	128 bit length.
Address representation	Binary numbers represented in decimals.	Binary numbers represented in hexadecimals.
IPSec	Optional.	Inbuilt support.
Fragmentation	Done by sender and forwarding routers.	Done only by sender.
Packet flow identification	Not available	Available within the IPv6 header.
Checksum	Available	Not Available
Options field	Available.	Not Available
Address **R**esolution **P**rotocol (ARP)	Available	Replaced with a function of **N**eighbor **D**iscovery **P**rotocol (NDP).
Internet **G**roup **M**anagement **P**rotocol (IGMP)	Available	Replaced with **M**ulticast **L**istener **D**iscovery (MLD) messages.
Broadcast	Available.	Not available
Configuration of addresses	Manual.	Auto-configuration.

IV. WHY IPv6 ?

The growth of internet with its need for more addresses is a main factor driving the need for a new version of the Internet Protocol. According to the estimation currently more than 100 million computers are connected to the Internet. Well, it's is not exactly known when the Internet run out of addresses. Many of the devices such as phones, automobiles will require connection to the internet which implies it will require unique address that is IP address. This creates the demand for more IP addresses. To overcome different problems related to the Internet, it was suggested the necessity to move from version 4 to version 6 of the Internet Protocol. These are some limitations of IPv4 which force the need of IPv6 [5]. In the recent years, huge amount of work has been done on the protocol design [6], connection and routing mechanism [7], [8], [9], and transition mechanisms [10], [11] of IPv6

V. IPv6 TRANSITION TECHNOLOGIES

There are mainly three kinds of techniques: [12] :
1. Dual-stack network
2. Tunneling
3. Translation

1. **Dual-Stack Network:** - Dual-stack IPv4 and IPv6 dual stack network shared / dedicated link is a transition technology that work in tandem. The diagram is given in Figure 1.

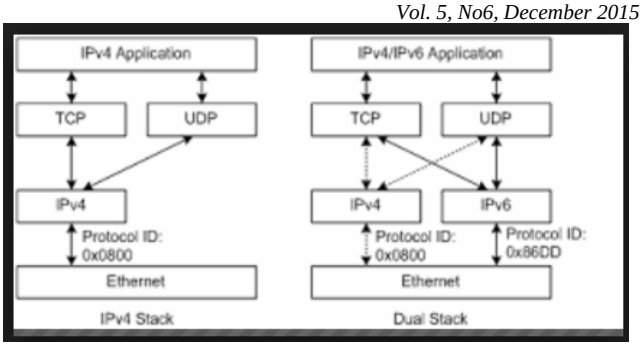


Figure 1: Dual stack architecture

2. **Translation: - A**ddress **F**amily **T**ranslation (AFT) / simply translation facilitates communication between IPv6-only and IPv4-only hosts and networks.
3. **Tunneling Techniques-** IPv6 is encapsulated in the header of IPv4 and forwarded over the infrastructure of IPv4. Transition mechanisms that allow IPv6 hosts to communicate via intervening IPv4 networks is also known as **tunneling**. In [13], the authors discuss the IPv6-in-IPv4 tunnel discovery issues, and propose a set of techniques to infer tunnels. The tunnel architecture is furnished in Figure 2.

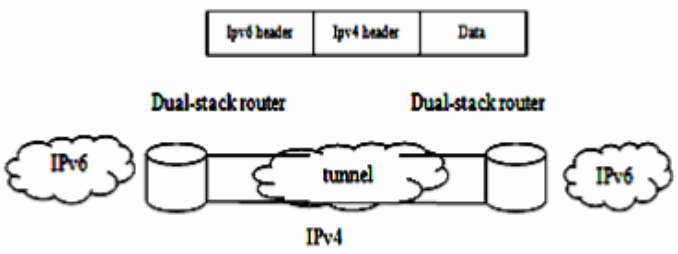


Figure 2: Tunnel architecture

There are two types of tunneling techniques are available:
i. Configured / Static
ii. Automatic / Dynamic.

i. Configured / Static: Configured tunneling is typically used when sites or hosts exchange traffic regularly. It is also used when only a few sites need to be connected. Configured tunneling also offers the advantage of enabling hosts in IPv6 sites to use native IPv6 addresses rather than IPv4-IPv6 address constructs.

ii. Automatic / Dynamic : Automatic tunneling is a transition scheme that requires an IPv4 address for each host. This enables a node to establish a tunnel without configuration. Automatic tunnels are created when required and eliminated when no longer needed. These include IPv4-compatible IPv6 addresses, the "6to4" transition mechanism (6to4) and **I**ntra-**S**ite **A**utomatic **T**unnel **A**ddressing **P**rotocol (**ISATAP**).

VI.CONFIGURATION OF IPv6 OVER IPv4

In this section, we have elaborated the static configuration of IPv6 over IPv4 tunneling with a sample network topology as given below:

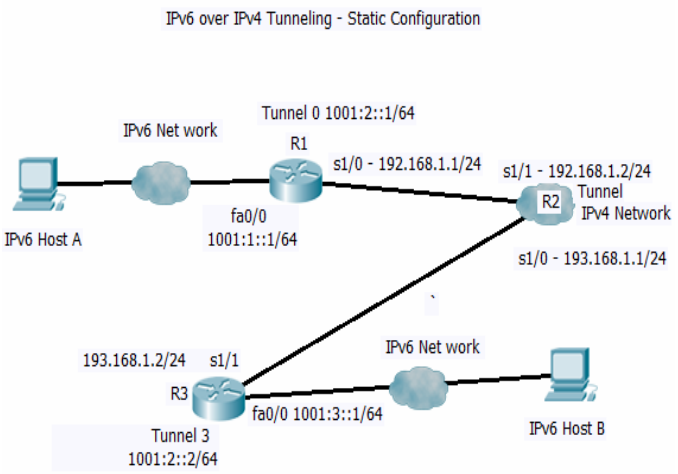


Figure 3: topology diagram

R1 – Configuration	R2- Configuration
R1#configure terminal R1(config)# interface fa0/0 R1(config-if)# ipv6 address 1001:1::1/64 R1(config-if)#no shutdown R1(config-if)#exit R1(config)#interface s1/0 R1(config-if)#ip address 192.168.1.1 255.255.255.0 R1(config-if)#no shutdown R1(config-if)#encapsulation hdlc R1(config-if)#clockrate 64000 R1(config-if)#exit R1(config)#	R2#configure terminal R2(config)#interface s1/1 R2(config-if)#ip address 192.168.1.2 255.255.255.0 R2(config-if)#no shutdown R2(config-if)#encapsulation hdlc R2(config-if)#exit R2(config)# R2(config)#interface s1/0 R2(config-if)#ip address 193.168.1.1 255.255.255.0 R2(config-if)#no shutdown R2(config-if)#encapsulation hdlc R2(config-if)#clockrate 64000 R2(config-if)#exit

R3 – Configuration
R3(config)#interface s1/1 R3(config-if)#ip address 193.168.1.2 255.255.255.0 R3(config-if)#no shutdown R3(config-if)#encapsulation hdlc R3(config-if)#exit R3(config)# R3(config)# interface fa0/0 R3(config-if)# ipv6 address 1001:3::1/64 R3(config-if)#no shutdown R3(config-if)#exit

Tunnel 0 – Configuration on R1
R1#configure terminal R1(config)#no ip routing R1(config)# ip routing R1(config)#no ipv6 unicast-routing R1(config)# ipv6 unicast-routing R1(config)# int tunnel 0 R1(config-if)#ipv6 address 1001:2::1/64 R1(config-if)#no shutdown R1(config-if)#tunnel source s1/0 R1(config-if)#tunnel destination 193.168.1.2 R1(config-if)#tunnel mode ipv6ip R1(config-if)#ip route 0.0.0.0 0.0.0.0 s1/0 R1(config-if)#ipv6 route 1001:3::/64 tunnel 0 R1(config-if)#exit **Tunnel 0 – Configuration on R2** R2#configure terminal R2(config)#no ip routing R2(config)# ip routing
Tunnel 3 – Configuration on R3
R3#configure terminal R3(config)#no ip routing R3(config)# ip routing R3(config)#no ipv6 unicast-routing R3(config)# ipv6 unicast-routing R3(config)# int tunnel 3 R3(config-if)#ipv6 address 1001:2::2/64 R3(config-if)#no shutdown R3(config-if)#tunnel source s1/1 R3(config-if)#tunnel destination 192.168.1.1 R3(config-if)#tunnel mode ipv6ip R3(config-if)#ip route 0.0.0.0 0.0.0.0 s1/1 R3(config-if)#ipv6 route 1001:1::/64 tunnel 3 R3(config-if)#exit

VII GRE [GENERIC ROUTING ENCAPSULATION] TUNNELING

The GRE IPv6 Tunnels feature enables the delivery of packets from other protocols through an IPv6 network and allows the routing of IPv6 packets between private networks across public networks with globally routed IPv6 addresses[14]. GRE is a unicast protocol that offers the advantages of encapsulating broadcast and multicast traffic or other non-IP protocols and of being **protected by IPsec**. For point-to-point GRE tunnels, each tunnel interface requires a tunnel

- **Source IPv6 address**
- **Tunnel destination IPv6 address** when being configured.

All packets are encapsulated with an **outer router's IPv6 header and a GRE header**.

Intermediate **S**ystem to **I**ntermediate **S**ystem **(IS-IS):-** is a routing protocol designed to move information efficiently within a computer network, a group of physically connected computers or similar devices. It accomplishes this

by determining the best route for datagram through a packet-switched network. It is one of the families of IP Routing protocols and is an **I**nterior **G**ateway **P**rotocol (**IGP**) for the Internet, used to distribute IP routing information throughout a single **A**utonomous **S**ystem (**AS**) in an IP network.

In the case of Manual Tunnel IPv4 encapsulates the IPv6 packet directly for tunneling across the IPv4 cloud. Whereas in **GRE Tunnel**, it takes the IPv6 packet and encapsulates it using the standard IPv4 GRE tunnel. Its mainly used within integrated IS-IS and IPv6 tunnel environments. If we plan to send both IS-IS traffic and IPv6 traffic over the tunnel, we need the protocol field of the GRE header that allows identification of the passenger protocol.

The following configuration shall be done in outer routers R1 & R3 to perform the same

GRE Configuration for R1	GRE Configuration for R3
R1(config)#ipv6 unicast-routing	R3(config)#ipv6 unicast-routing
R1(config)#interface loopback 0	R3(config)#interface loopback 0
R1(config-if)#ipv6 rip RIPNG enable	R3(config-if)#ipv6 rip RIPNG enable
R1(config-if)#exit	R3(config-if)#exit
R1(config)#interface tunnel 0	R3(config)#interface tunnel x
R1(configif)#ipv6 address 1001:2::1/64	R3(configif)#ipv6 address 1001:2::2/64
R1(config-if)#tunnel source fa0/0	R3(config-if)#tunnel source fa0/0
R1(config-if)#tunnel destination 193.168.1.2	R3(config-if)#tunnel destination 192.168.1.1
R1(config-if)#tunnel mode gre ip	R3(config-if)#tunnel mode gre ip
R1(config-if)#ipv6 rip RIPNG enable	R3(config-if)#ipv6 rip RIPNG enable
R1(config-if)#end	R3(config-if)#end

GRE TUNNEL PROTECTION [IPSEC]

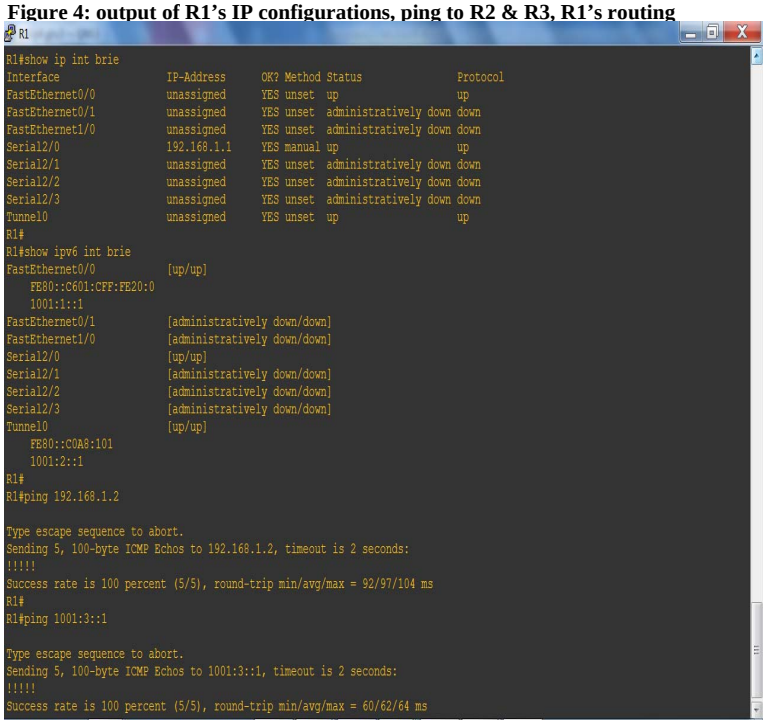
GRE tunnel protection IPsec allows devices to work as security gateways, establish IPsec tunnels between other security gateway devices and provide crypto IPsec protection for traffic from internal networks when the traffic is sent across the public IPv6 Internet. The GRE IPv6 tunnel protection functionality is similar to the security gateway model that uses GRE IPv4 tunnel protection. By adding the following commands in the router configuration we can enable the IPsec.

crypto ipsec profile ipsec-profile
set transform-set ipsec-profile
tunnel protection ipsec profile ipsec-profile

VIII.SCREEN SHOTS

In this section we have furnished the screen shots from GNS3 and wireshark.

Figure 4: output of R1's IP configurations, ping to R2 & R3, R1's routing



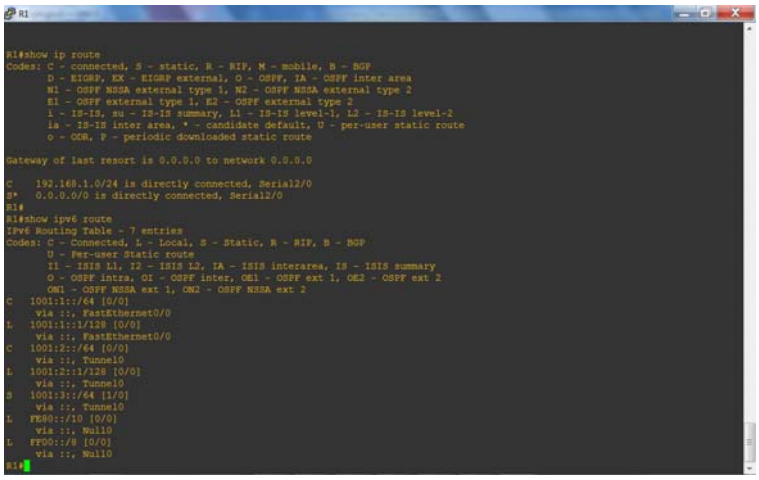


Figure 5: output of R2's IP configurations, ping to R1 & R3, R2's routing

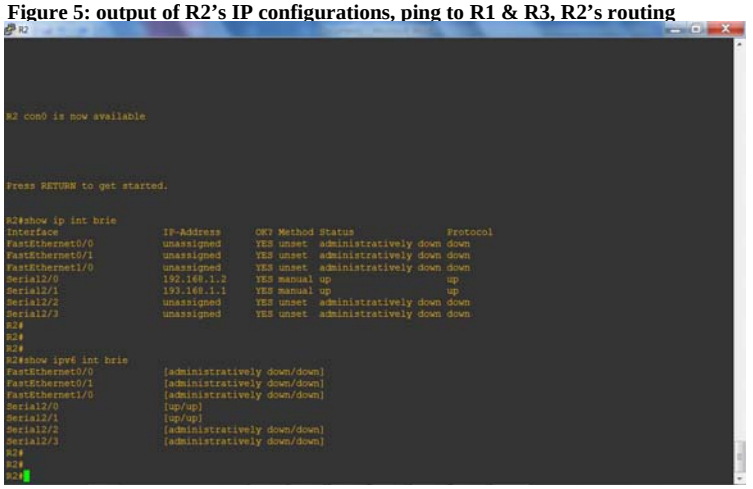


Figure 5: (contd..)

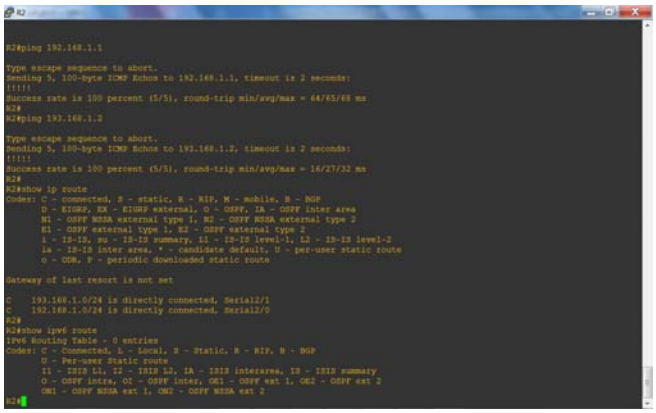
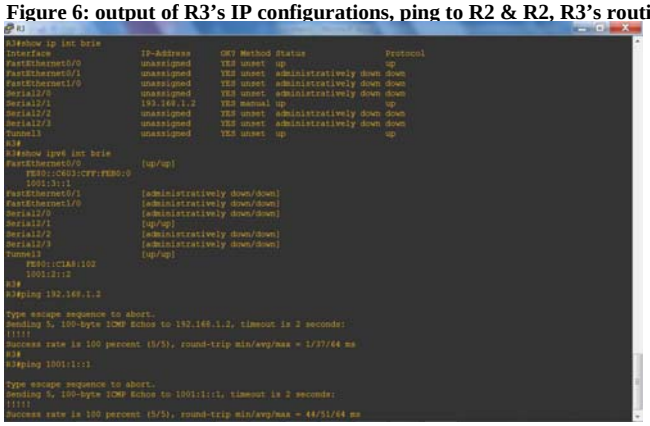


Figure 6: output of R3's IP configurations, ping to R2 & R2, R3's routing



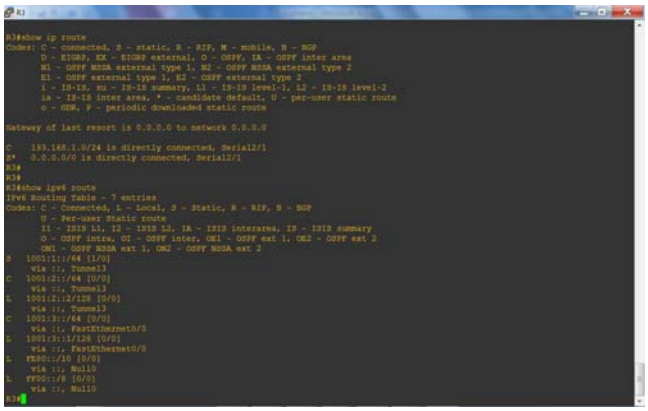
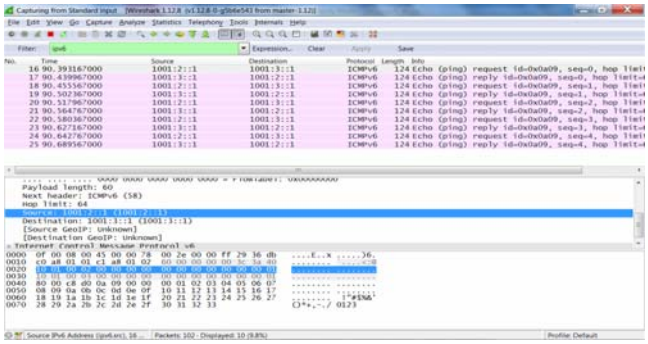


Figure 7: Output of data capture through wireshark - communication between R1 & R3 through R2



CONCLUSION

In this paper we have discussed about IPv4, reasons why we need IPv6, brief about IPv6, comparison between IPv4 & IPv6, transition techniques, tunneling in IPv6, GRE and configuration of IPv6 over IPv4 methods using GNS3& wireshark. In future a model network would be taken to study the performance of network using IPv6.

REFERENCES

[1] http://www.internetsociety.org
[2]"IPv6Headers",Online: http://www.cu.IPv6tf.org/literatura/chap3.pdf, chapter 3, pp. 40-55, Des 12 1997.
[3] S. Deering, R. Hinden, Internet Protocol Version 6 (RFC2460), 1998
[4]. S. Bradner and A. Mankin: IP: Next Generation (IPng) White Paper Solicitation. RFC 1550, Dec. 1993
[5] Importance and Benefits of IPV6 over IPV4 (International Journal of Scientific and Research
Publications, Volume 2, Issue 12, December 2012)
[6] S. Deering and R. Hinden: Internet Protocol, version 6 (IPv6) Specification. RFC 2460, Dec.1998
[7] R. Rockell and R. Fink: 6Bone Backbone Routing Guidelines. RFC2772, Feb. 2000
[8] B. Carpenter and K. Moore: Connection of IPv6 Domains via IPv4 Clouds. RFC 3056, Feb.2001
[9] A. Durand, P. Fasano, I. Guardini, and D. Lento: IPv6 Tunnel Broker. RFC 3053, Jan. 2001
[10] R. Gilligan and E. Nordmark: Transition Mechanisms for IPv6 Hosts and Routers. RFC 2893,Aug. 2000
[11] Ioan Raicu and Sherali Zeadally: Evaluating IPv4 to IPv6 Transition Mechanisms, IEEE International Conference on Telecommunications 2003, ICT'2003, Tahiti Papeete, French Polynesia, Feb. 2003
[12] A. Dhamdhere, M. Luckie, B. Huffaker, k. claffy, A. Elmokashfi, and E. Aben, "Measuring the Deployment of IPv6: Topology, Routing and Performance", in Internet Measurement Conference (IMC), Nov 2012.
[13] L. Colitti, G. D. Battista, and M. Patrignani: IPv6-in-IPv4 tunnel discovery: methods and experimental results. IEEE Transactions on Network and Service Management, vol. 1, no.1. April. 2004.
[14]. Interface and Hardware Component Configuration Guide, Cisco IOS XE Release 3S

AUTHORS PROFILE

Dr. J Sebastian Nixon is a professor, department of CS & IT, CNCS, Wolaita Sodo University, Federal Democratic Republic of Ethiopia. He is a Microsoft Certified Sysem Engineer (MCSE). He is specialized in network security. He has around 19 plus years of teaching experience. He is a life member in CSI, ISOC & CRSI.

Dr. A Francis Saviour Devaraj is a professor, department of CS & IT, CNCS, Wolaita Sodo University, Federal Democratic Republic of Ethiopia. He is a Cisco Certified Network Associate (CCNA). He is specialized in informationsecurity. He has around 15 plus years of teaching experience. He is a life member in CSI, ISOC, CRSI & ISTE.