Indo-Iranian Journal of Scientific Research (IIJSR)
Volume 2, Issue 1, Pages 152-156, January-March 2018

An Assessment of Quality of Service and Network Security in IP Based Communication Networks

K.Jason[1] and M.Ravikumar[2]

[1,2]*Assistant Professor, Department of CSE, JCT College of Engineering and Technology, Coimbatore, India.*

Article Received: 30 November 2017 *Article Accepted: 31 January 2018* *Article Published: 17 March 2018*

ABSTRACT

The current distribution of IPv6 in core networks of operators, its obtainability to end customers of multiple ISPs together with the availability of native access to large services like Google Access, the dispersion of IPv6 has been increased. While its deployment from the inside of the network leading to the edges is fruitful, the transition remains a matter today for numerous enterprises which see it as a monotonous and error-prone task for network administrators. In order to fill this breach and to present the essential algorithms and provide the subsidiary tools to permit this transition to become automatic. Based on the model of an IPv4 network, we design and implement an ipv6 network, thereby it supports auto configuration to the host and security is inbuilt with the protocol. An assessment of quality of service and network security in IP based communication networks has been carried out in this paper.

INTRODUCTION

Enabling the IPv6 protocol which enable the stateless auto configuration and also enables the security features which is inbuilt with IPv6 protocol. IPv4 is an abbreviation of “Internet Protocol Version Four”. It is also recognized as RFC 719. IPv4 was the fourth generation of Internet Protocol and was also the first version to be extensively deployed. The Internet Protocol sits on the third layer of the OSI network model. This is also identified as the network layer. The physical layer is the first layer in the OSI which is software based. The network layer (third layer) of the OSI model generally deals with finding, routing and switching for end to end communications that are not unswervingly connected to each other using a physical link. The security features is not in built with IPv4, ISP uses ACL, fire-wall/check point which enables the security in IPv4 network. The Internet Protocol is the most leading protocol on the Internet nowadays and commonly runs on upper layer protocols such as the Transmission Control Protocol (TCP) and the User Datagram Protocol (UDP). IP networking is a pattern of connectionless networking service (CLNS). IPv4 address consists of 32 bits, 4 bytes that are a combination between zeros and ones. The address contains two parts, the network and host address part.

Yehia et al. have planned various routing protocols and assessed them based on some performance metrics [1]. This evaluation is performed hypothetically and by using simulation. Sunjian and fang have introduced the OSPF protocol for IPv6 which is also mentioned as OSPFv3 and they primarily familiarized the knowledge of IPv6, and then implemented the OSPF over IPv6 [2]. Horenoor has introduced the implementation decision to be made when the choice is available between protocols that involve distance vector or link state or the combination of both [3]. In this paper, it is shown that OSPF definitely achieves better when compared to RIP in terms of network convergence, latency and throughput. Bahk and Zarki described about various dynamic multipath routing algorithm for networks [4]. Joseph Davies has specified detailed information for understanding IPv6 and its routing protocols [5]. The authors have made the case studies in real time about use of the dynamic routing protocols [6]. A tutorial has been entailed for simulating the wide area network using GNS-3.

The Internet Protocol version-4 (IPv4) is the fourth reconsideration in the expansion of internet protocol (IP) and the first version of the protocol to be extensively deployed. IPv4 is still by far the most extensively deployed internet layer protocol. It is basically a connectionless protocol for the use on packet switched link layer networks. It does not function on best effort delivery model, which does not guarantee delivery nor does it assure proper sequencing or avoidance of duplicate delivery.

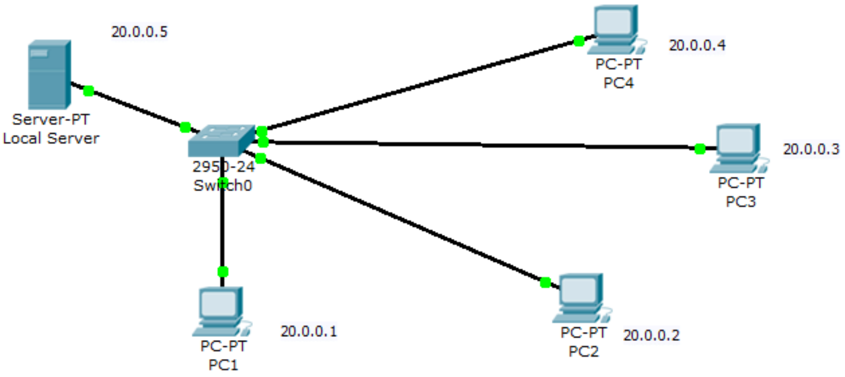

Figure 1: IPv4 Addressing Scheme

These features including data integrity are addressed by an upper layer transport protocol such as the TCP. IPv4 uses 32 bit (4 byte) addresses which limits the address space to 4294967296 (2^32) addresses. This diminishes the number of addresses that may be allocated for routing on the public internet. As addresses are assigned to the end users, IPv4 address have been developing. Network addressing changes by classful network design, classless inter-domain routing and the network address translation (NAT) have contributed to delay, significantly the inevitable exhaustion which occurred on February 3rd 2011 when IANA allocated the last five blocks to the five regional internet registries (RIRs). This restriction stimulated the development of IPv6.

THE ADDRESSING FORMAT OF IPV6

IPv6 or Internet Protocol Version-6 is the subsequent generation protocol for the Internet. It is intended to provide numerous advantages over the existing and current Internet Protocol Version4 (IPv4).

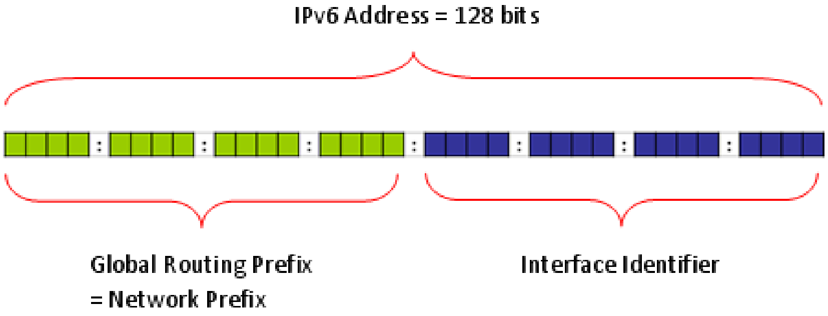

Figure 2: IPv6 Addressing Scheme

Both IPv6 and IPv4 describe network layer protocol (how the data is sent from one computer to the alternative computer over packet-switched networks such as the Internet). It is consequently also called the Next Generation Internet Protocol. Though IPv6 is the successor of IPv4, both the protocol versions will endure to be data-oriented protocols for use in Internet in the fourth coming years. IPv6 addresses the chief problem of IPv4 that is the exhaustion of addresses to link computers or host in a packet switched network. IPv6 has a very hefty address space and consists of 128 bits as compared to 32 bits in IPv4. Therefore, it is now thinkable to support 2^128 unique IP addresses, a considerable increase in number of computers that can be addressed with the aid of IPv6 addressing structure. In addition, this addressing structure will also eradicate the need of NAT (network address translation) that reasons to several networking problems.

IPv6 addresses are represented by eight groups of hexadecimal quartets detached by colons in between them. Following is an instance of a valid IPv6 address: 2001:cdba:0000:0000: 0000:0000:3257:92 address may be condensed to a single zero or altogether omitted. Consequently, the following IPv6 addresses are similar and equally valid: 2001:cdba: 0000:0000:0000:0000:3257:9652 2001:cdba:0:0:0:0:3257: 9652 2001:cdba::3257:9652

BASIC RIP CONFIGURATION

```
router> enable
router# config t
router(config)#ipv6 unicast-routing
router(config)#ipv6 router rip bsnl
router(config-rtr)#exit
router(config)#interface ethernet 0
router(config-if)# ipv6 enable
router(config-if)# ipv6 rip bsnl enable
router(config-if)# ipv6 address 2001:1111::1/56
router(config-if)# no shut
router(config-if)# exit
```

OSPF is an interior gateway protocol that routes the Internet Protocol (IP) packets exclusively within a single routing domain (autonomous system). It gathers link state information from obtainable routers and constructs a topology map of the network.

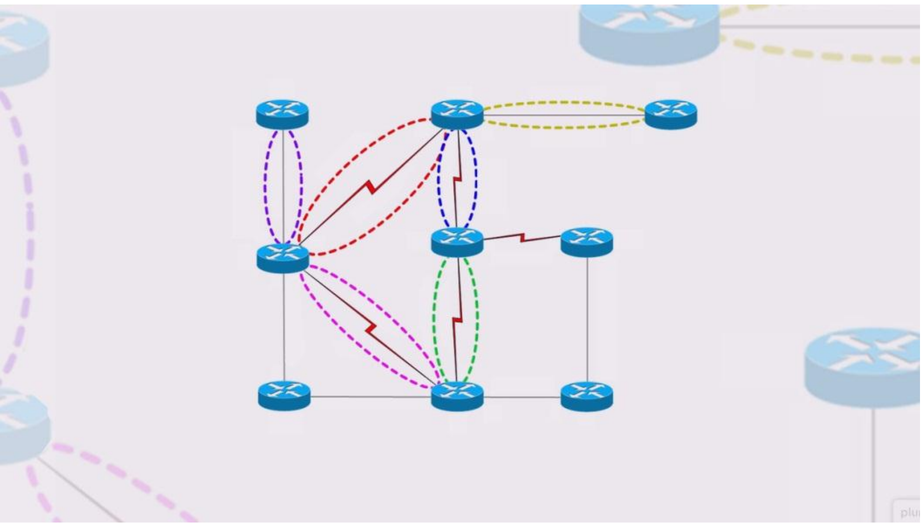

Figure 4: Implementation of OSPF

The topology regulates the routing table presented to the Internet Layer which makes routing decisions based exclusively on the destination IP address found in IP packets. OSPF was intended to support variable-length subnet masking (VLSM) or Classless Inter-Domain Routing (CIDR) addressing models. OSPF notices changes in the topology such as link failures, very rapidly and converges on a new loop-free routing arrangement within seconds. It calculates the shortest path tree for each route using a technique based on Dijkstra's algorithm which is a shortest path first algorithm.

CONCULSION AND FUTURE WORK

The experiment is manually configured, thereby it is not scalable but has a secured communication. The main objective of this research work was to realize the implementation and successful validation using the simulator. Future scope will be towards enabling the security features which is in-built with IPv6 protocol. Also deployment of IPv6 using dual stack and auto tunneling and analysing the performance using Cisco Packet Tracer will be carried out.

REFERENCES

[1] Yehia, M. A., Aziz, M. S., and Elsayed, H. A., “Analysis of IGP Routing Protocols for Real Time Applications: A comparative Study”, International Journal of Computer Applications, 2011. vol. 26, no.3, 11-17.

[2] Jian, S., and Fang, Y. Y. 2011. Research and Implement of OSPFv3 in IPv6 network, In Proceedings of the SQRWC, Conference on Cross Strait Quad-Regional Radio Science and wirelessTechnologyConference.743–746.

[3] Thorenoor S. G. 2010, “Dynamic Routing Protocol implementation decision between EIGRP, OSPF and RIP based on Technical Background Using OPNET Modeller”, In Proceedings of the ICCNT, International Conference on Computer and Network Technology. 191 –195.

[4] Bahk.S. and M. El Zarki. (1992) "A Dynamic Multi-Path Routing Algorithm for Networks," J. High Speed Networks, vol. 1, no. 3, pp. 215-36.

[5] Joseph Davies (2008), “Understanding ipv6”, second edition, Microsoft press.

[6] Kalyan, G.P.S, and Prasad, D.V.V. 2012, “Optimal selection of Dynamic Routing protocol with real time case studies”, In Proceedings of the RACSS, International Conference on Recent Advances in Computing and Software Systems. 219 – 223.