Implementation of Network Services on IPV6 Networks

Frimpong Twum
Department of Computer Science
Kwame Nkrumah University of Science and Technology,
Kumasi, Ghana.

Kwadwo Asante
Department of Computer Science
Kwame Nkrumah University of Science and Technology,
Kumasi, Ghana

Michael Asante
Department of Computer Science
Kwame Nkrumah University of Science and Technology,
Kumasi, Ghana

ABSTRACT

Internet Protocol (IP) layer also known as the network layer is responsible for sending and receiving packets in a network. This task is performed by using a uniquely identified fixed length of addresses known as IP addresses. In the IPv4 protocol, the length of addresses is 32 bits and this gives limit of addresses to 232 = 4,294,967,296. The 32 bit numeric identifier used in the IPv4 was considered enough at the early years of the creation of the internet. Various schemes such as subnetting, Variable Length subnet Mask (VLSM) and the introduction of private IP addresses in combination with Network address Translation (NAT) have been employed to delay the exhaustion of IPv4 as mobile devices increase considerably. With the increase in the world's population and the emergence of several mobile devices, it is likely that IPv4 addresses can no longer be enough even with all the interventions introduced. The only viable option is the IPV6. Since the launch of the next generation protocol (IPv6) in June 2012, various studies have been undertaken. Many network administrators, IT professional and even customers wonder what has changed and how difficult or otherwise is it to implement network services on IPv6.

This thesis seeks to bring to the fore the various works on implementation of IPv6, and also implement IPv6 networks and use it to investigate the implementation difficulties in the IPv6 connectivity and routing; transition schemes, Quality of Service (QoS), Security and other services such as Content Delivery Networks (CDN); Dynamic Host Configuration Protocol (DHCP); Transmission Control Protocol (TCP) /User Datagram Protocol (UDP); Simple Mail Transport Protocol (SMTP); Hypertext Transfer Protocol (HTTP) and Domain Name System (DNS) and compare their performances with that of IPv4.

General Terms

Internet Protocol Version 6 (IPv6), Network Services, Transition Techniques

Keywords

Internet Protocol Version 6 (IPv6), Network Services, Transition Techniques

1. INTRODUCTION

1.1 Internet Protocol Version 4 (IPv4)

32bits number is used in IPv4 addressing and it is subdivided into two parts, the network part and the host part respectively. The IPv4 addresses are divided into three classes; class A with network prefix /8 and used for large networks. Class B has a network prefix of /16 and used for medium sized networks whiles class C has a network prefix of /24 and it is used in small networks. At the early stages of the internet, allocation of addresses was unplanned, resulting in class B addresses giving to small sized companies which led to quicker depletion of the IPv4 addresses in that class. Later medium sized companies were offered several /24 addresses and this led to an increase in the Internet backbone router's routing tables [1]. Numerous methods such as Subnetting, Variable Length Subnet Mask (VLSM), Classless Inter-Domain Routing (CIDR) and Network Address Translation (NAT) have been adopted to postpone IP address space exhaustion. Conversely, the use of these methods came with a number of problems. These problems form the bases of the IPv6 address scheme, because it offers a permanent solution to these problems.

2. REVIEW OF LITERATURE

2.1 IPv6 Addressing

Made of 128bits long, the IPv6 address is divided into eight 16-bits blocks. Each block is then converted into 4-digit Hexadecimal numbers separated by colon. Types of IPv6 addresses are Multicast addresses which are used for DHCPv6, multicast applications, Router Advertisements (RA), Router Solicitations (RS) [2]. Fig 1 shows the IPv6 multicast address format.

128 Bits

8 Bits	4 Bits	4 Bits	112 Bits

Group I

Fig.1 IPv6 Multicast Address format

Anycast address: This address is also known as One to Nearest. It is no longer in use.

Unicast address: it is used to identify a single node or interface. Traffic meant for a unicast address is sent to a single interface. Fig 2 shows the global unicast address format.

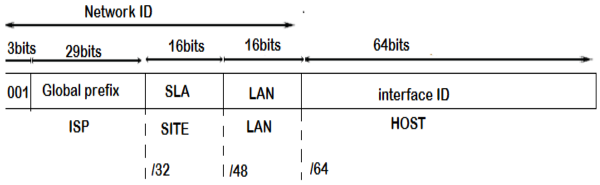

Fig 2 The global unicast address format.

The different types of unicast addressing are Global, Unique local and Link local. Only global unicast addresses are routable and reachable across the internet. Fig 3 shows the IPv6 address scope.

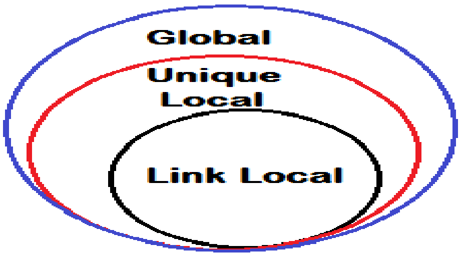

Fig. 3 IPV6 Address scopes

2.2 IPv6 Address Assignment

IPV6 devices can be assigned addresses through any of the following means:

- IPv6 Stateless Address Auto-Configuration (SLAAC) [3], which allows hosts to obtain configuration and routing parameters from an IPV6 router connected in the network through Router advertisement(RA.). it requires a public DNS server to DNS information.
- Manual Configuration - involves a network operator statically assigning IPV6 addresses to devices and interfaces.
- DHCP for IPv6 could be Stateless or Stateful. Stateless DHCPv6 is a combination of Stateless Address Auto-Configuration and (DHCPv6). The default gateway router has two configurable bits in its Router Advertisement (RA) that instruct clients either to use DHCPv6 or not**.** With the O bit set but not M in a Router Advertisement (RA), the client uses SLAAC to obtain its IPv6 address and use DHCPv6 to obtain additional information (such as Trivial File Transfer Protocol (TFTP) server address or DNS server address) [4]. Server does not keep track of the client address bindings. On the other hand, when the M bit is set, the setting of the O bit is irrelevant because the DHCPv6 server will also return "other" configuration information together with the addresses. This mechanism is known as Stateful DHCPv6 since the server keeps track of the client's address bindings [5].

2.3 IPv6 Domain Name System (DNS)

The (DNS) resolves domain names to IP addresses. An A record stores an IPV4 resolution whiles AAAA record also known as quad-A record stores IPV6 address resolutions. Usually, DNS comprises three components: The authoritative server that holds the authoritative data, the client that runs an application that needs the address for a given hostname and the intermediary server that responds to this query and acts as a proxy. A client that runs an application that needs responses normally runs a resolver, which always requests recursion. This stub resolver is configured (often through DHCP) with the IP address of the intermediary server that acknowledges this request. For reverse lookups the special domain in IPv6.ARPA is defined [6].

2.4 Internet Control Message Protocol (ICMPv6)

ICMPv6 is an integral part of IPv6 and it is carried after the basic IPv6 header information as an extension header. Every node that is to run IPv6 requires ICMPv6. It is used fundamentally to test connectivity between nodes through the ping and traceroute commands using ICMP echo request/reply [7]. It does not allow IPv6 to do any fragmentation through IPv6 process called path MTU discovery.

One new feature of ICMPv6 is Neighbor Discovery (ND) which is used to handle link- layer address of nodes determination on the local network; autoconfiguration; detecting routers and alteration of link-layer addresses. These set of functions are similar to the Address Resolution Protocol in IPv4.

2.5 IPv6 and IPv4 Compared

The main difference between IPv4 and IPv6 is the address size. IPv4 protocol has address size of 32bits which gives approximately 2^{32} = 4,294,967,296 addresses, whiles IPv6 has address size of 128bits, leading to a total of $2^{128} \approx 3.4 * 10^{38}$ addresses. Another difference worth considering is the IP header. Depending on the options preferred, the IPv4 header can range between 20 and 60 bytes whiles the IPv6 header was made a fixed size of 40 bytes [8]. Some fields, such as the identification, header checksum, header length, flags, fragment offset, specifically and the options field have been removed from the IPv6 header. With 40 bytes of fixed length and only 8 fields, new header format consume less memory. Every packet has this base header, which can be followed by an extension header defined in Next Header field. The IPv6 header is designed such that only the useful features of the IPv4 header were kept whiles the features that are not used often have been moved into optional extension headers. IPv6 packets are simpler to route though the address add more data to the packet, but the fields are fewer than IPv4 despite the fact that the address is longer. Fig 4 shows the IPv4 and IPv6 headers compared.

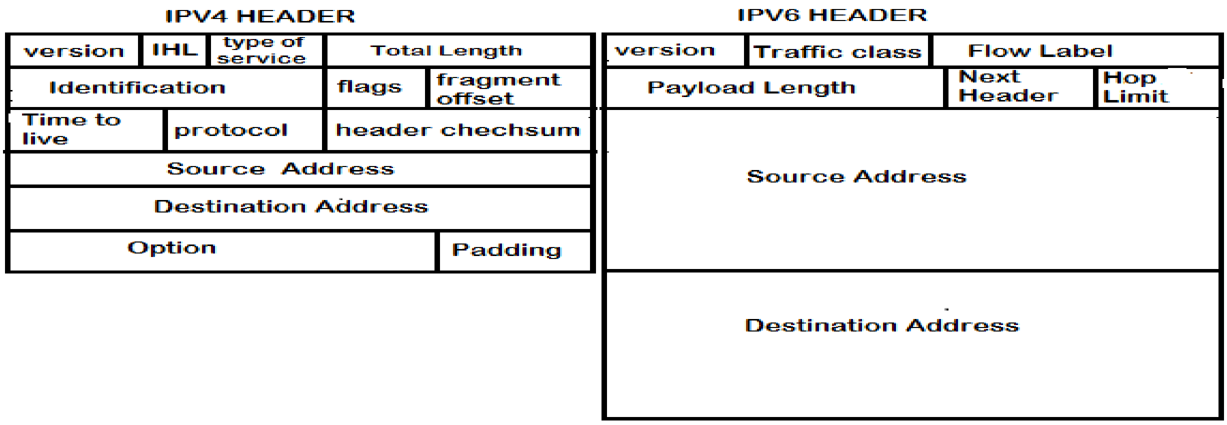

Fig. 4 IPv4 and IPv6 headers compared

IPv6 does not carry options inside the header like that of IPv4 but rather uses extension headers that are placed between IPV6 header and the next protocol header.

2.6 Routing Protocols and IPv6

Routing protocols are used by routers to forward IP packets to their correct destinations across a subnet and beyond in a network. Routing protocols in IPv6 are similar to their IPv4 equivalents, but routing updates have to carry more information since an IPv6 prefix is four times larger than an IPv4 prefix. The IPv6 routing protocols includes RIPng, EIGRPv6, OSPFv3, Integrated IS-IS, BGP-4, and MPLS. Some of which are discussed here.

2.6.1 Routing Information Protocol - New Generation (RIPng)

RIPng is an Interior Gateway Protocol (IGP) most commonly used in smaller networks. RIPng uses hop count as a routing metric. RIPng is intended to allow routers to exchange information for computing routes through an IPv6-based network [9]. RIPng is based on RIPv2 and has a maximum hop count of 15; uses split horizon, poison reverse, and other loop avoidance mechanisms, but is intended for IPv6. It is of distance vector protocol and uses the Bellman Ford algorithm to calculate the best path in a network. It still uses multicast to send its updates but uses FF02::9 for the transport address. It's counterpart IPv4 multicast address is 244.0.0.9. RIPng is a UDP-based protocol and communicates through UDP port 521 known as the RIPng port.

2.6.2 Open Short Path First (OSPFv3)

Described in [RFC 5340] OSPF is a link-state protocol based on Dijkstra's least-cost path algorithm for calculating the best paths to subnets [10]. The routers running OSPF collects Link State Advertisement (LSA) data and stores it in the Link-State Database. The Dijkstra's algorithm uses the database content to create an OSPF routing table which contains a list of the shortest possible paths to know destinations through specific router interface ports [11]. OSPFv3 uses multicast traffic to send its updates and acknowledgements with the address FF02::5 for OSPF routers and FF02::6 for OSPF-designated routers. These new addresses are the replacement for 224.0.0.5 and 224.0.0.6 respectively.

2.6.3 Boarder Gateway Protocol (BGP4)

Defined in [RFC 4271], BGP is an inter-domain routing protocol that uses the destination-based forwarding paradigm and path vector routing. It views the Internet as a collection of autonomous systems (ASs) and exchanges information between peers using TCP as underlying protocol. It maintains a database of network layer reachability information which carries the prefixes and some features associated with them, such as the mandatory NEXT_HOP attribute, hence they are still IPv4 specific [12].

2.6.4 Integrated Intermediate System Intermediate System (IS-IS)

Described in [RFC 119], IS-IS (Intermediate System - Intermediate System) was originally designed for use as a dynamic routing protocol for ISO CLNP, defined in the ISO 10589 standard and Later adapted to carry IP prefixes in addition to CLNP (known as Integrated or Dual IS-IS). It is predominantly used in ISP environment. The IS-IS protocol is one of a family of IP Routing protocols, and is an Interior Gateway Protocol (IGP) for the Internet used to distribute IP routing information throughout a single Autonomous System (AS) in an IP network[13]. ISIS has a 2 layer hierarchy; Level-2 (the backbone) and Level-1 (the areas). A router can be Level-1 (L1) router, Level-2 (L2) router or Level-1-2 (L1L2) router.

2.6.5 Multiprotocol Label Switching (MPLS)

MPLS is a scalable, protocol-independent transport. In an MPLS network, data packets are assigned labels. Packet-forwarding decisions are made solely on the contents of this label, without the need to examine the packet itself. Multi-Protocol Label Switching (MPLS) was originally presented as a way of improving the forwarding speed of routers but is now emerging as a crucial standard technology that offers new capabilities for large scale IP networks. Traffic engineering, the ability of network operators to dictate the path that traffic takes through their network, and Virtual Private Network support are examples of two key applications where MPLS is superior to any currently available IP technology [14].

2.7 IPv6 Mobility Features

Specified in [RFC 6275], IPv6 mobility offers a means for the host to roam around different links without losing any connection and its IP address. While roaming across networks, mobile IPv6 provides an IPv6 node with the ability to retain the same IPv6 address and maintain continuous link and application connectivity. In Mobile IPv6, the IPv6 address space enables Mobile IP deployment in any kind of large environment without upgrade in system infrastructure or the use of any foreign agent. Permanent IP address is assigned to each mobile node. This is known as home address and does not change along the entire network [15].

2.8 IPv6 Quality of Service (QoS)

Quality-of-S ervice (QoS) is a set of service requirements or performance guarantees to be met by the network while transporting a flow. QoS features supported for IPv6 environments include queuing, class-based packet marking; packet classification; traffic shaping; weighted random early detection (WRED), and policing of IPv6 packets. The procedure for implementing QoS in IPv6 is not different from that of IPV4. What has stimulated QoS improvements in IP networks include new types of applications such as: networked virtual environments; video distribution; VoIP; audio/video streaming; interactive gaming, e-commerce; videoconferencing; GRIDs and collaborative environments. Performance analysis are determined in terms of Bandwidth; Delay; Inter-packet Delay Variation – *Jitter* and Packet loss. The Modular Quality of Service Command line (MQC) allows you to define traffic classes, create and configure traffic policies (policy maps), and then attach those traffic policies to interfaces. Congestion can be managed by marking traffic and using it to build a policy to classify traffic on the rest of the network segments. Also congestion avoidance can be achieved by using WRED to implement RED-based drop policy on packets that are likely to overflow the limits of class- based weighted fair queuing [16].

3. METHODOLOGY

Graphic network Simulator (GNS3) was used to simulate various simple IPv6 networks which were used to implement various network services such as addressing and connectivity; routing; transition techniques mostly tunneling and dual stack; quality of service, IPSec and IPv6 for network management such as telnet, SSH, SNMP.

Address implementations included manual and DHCPv6

- Routing using static and RIPng were used to learn the routes to different networks using the topology shown by fig. 5.
- Tunneling and IPsec were implemented using the topology displayed by fig. 6.
- Datagram loss: was measured with an Iperf UDP test.
- Latency (response time or RTT): was measured with the Ping command.
- Jitter (latency variation): was measured with an Iperf UDP test.
- A tunnel broker was also set up on a on the computer to ping a dual stack websites in order to confirm the simulation results.
- A 32-bit Windows virtual Server 2003 and 2008 R2 Enterprise with service pack 1 was installed to test services DHCPv6, DNSv6 and Internet Information Server on IPv6 LAN.

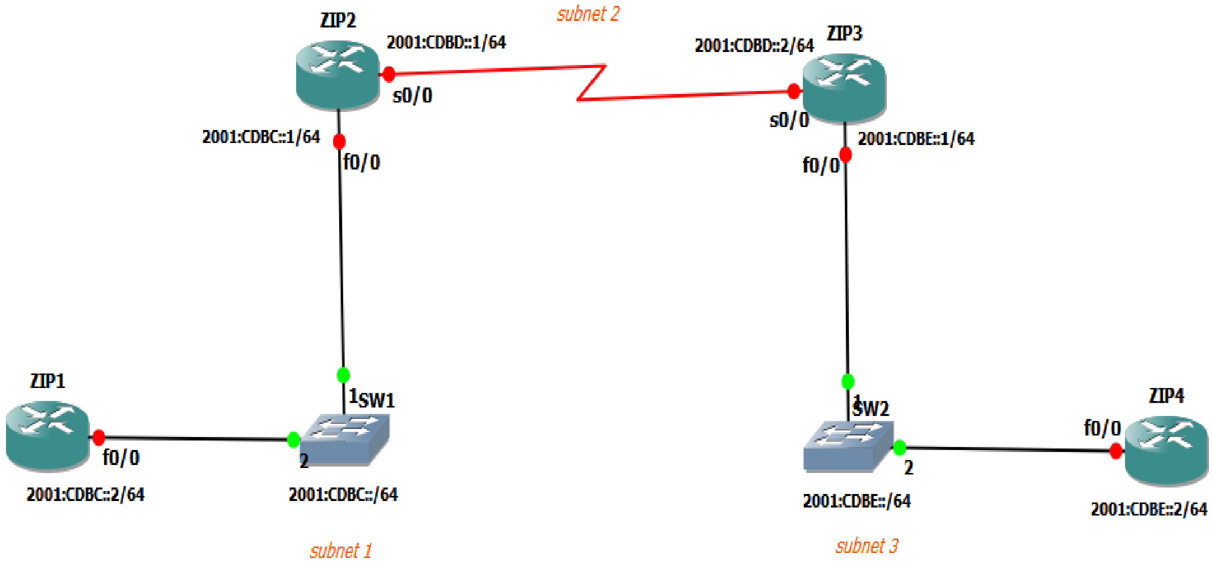

Fig. 5 Topology for testing connectivity and routing

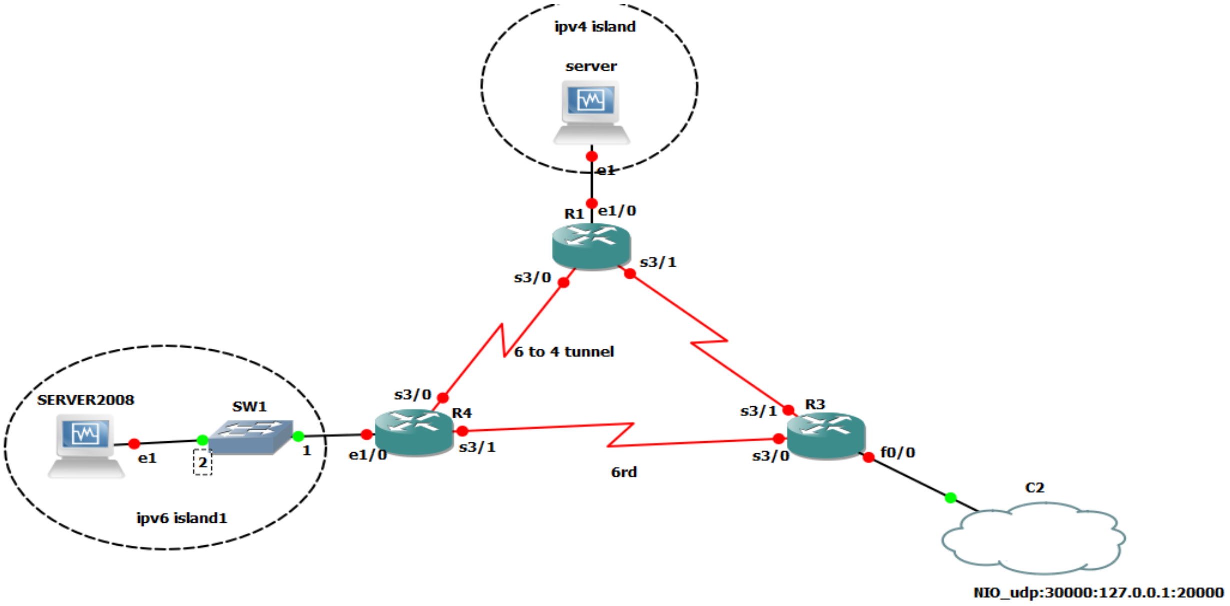

Fig. 6 Topology use for implementing tunneling, IPSEC

4. DISCUSSIONS OF RESULTS

4.1 Connectivity and Routing

After the address assignment, ICMP messages were sent within a subnet using the ping command. Datagrams were sent from ZIP1 interface fas0/0 to ZIP2 interface fas0/0 successfully. IPv6 static routes were implemented by enabling the forwarding of IPv6 unicast datagrams. However, for normal operational networks, static routing is practically impossible. RIPng was used to learn the routes to different networks.

4.2 DHCPv6

Addressing using DHCPv6 is a must for enterprise networks since manual addressing is highly prone to errors because of the address size. There are lot of similarities between DHCPv4 and DHCPv6 but also some clear differences exist. DHCP for IPv4 uses Discover/Offer/Request/Acknowledge (DORA), and DHCPv6 uses Solicit/Advertise/ Request/Reply (SARR). DHCPv4 do not have a prefix delegation but exist in DHCPv6. DHCP for IPv4 and DHCPv6 UDP port numbers are different. DHCP servers and relay agents listen on UDP port 67 and clients listen on UDP port 68, DHCPv6 clients listen on UDP port 546, DHCPv6 servers and relay agents listen on UDP port 547

4.3 Tunneling

IPv4-Compatible IPv6 tunnels, 6RD tunnels and ISATAP tunnels were implemented and tested with the 'ping' and 'show ip route' commands on router R4 of fig 6. Table 1 shows the mean and standard deviation for the data collected by Iperf measurements on bandwidth consumption for TCP and UDP for both IPv4 and IPv6

Table 1

	TCP		UDP	
Observations	30	30	30	30
	IPv4	IPv6	IPv4	IPv6
Mean Bandwidth/Mbits/sec	209.40	222.23	276.37	295.63
Standard Deviation / Mbits/sec	17.14	6.937	7.56	7.44
Skewness	-5.140	-2.592	0.710	0.443
Variance	346.250	46.512	57.300	53.565

4.4 Performance

The outcome of the ping test shows that there is no vast difference between UDP and TCP for IPv6 and IPv4. Analyses show stability in both protocols over IPv6 with fair skewness and deviation. No sensitive extreme values (outliers) were recorded for UDP or TCP for IPv6 and IPv4, but deviation was a bit high but consistent for IPv4 TCP with a deviation of 17. The bandwidth consumption for IPv6 TCP was fairly stable as indicated in table 1.

Results from the tunnel broker as indicated by table 3 shows that the Return Trip Time (RTT) for IPv6 was a little higher than that of IPv4. This might be due to the IPv6 packet not being allowed to take the optimal route to its destination due to restriction by the tunnel broker. An IPv4 packet sent from behind NAT could incur similar delay.

4.5 QoS

The QoS features for IPv6 was no different from that of IPv4. The same commands worked for both but the QoS features such as Custom queuing (CQ); Network-based application recognition (NBAR); Committed Access Rate (CAR); Compressed Real-Time Protocol (CRTP) and Priority queuing (PQ) are not supported for managing IPv6 traffic.

5. CONCLUSION

With all the test run of services, results from this study did not show much differences in terms of performance, quality of service, stability and throughput between the two protocols as shown by table 2 .

However, IPv6 has no need for NAT and has many advantages over IPv4, such as a larger address space, streamlined header and extension headers. Most services such as Content Delivery Network (CDN), DHCP, TCP/UDP, SSH, SMTP, HTTP and DNS on IPv6 networks runs smoothly just as they do on IPv4. In terms of addressing, multiple IPv6 link-local addresses on an interface are not supported.

IPv6 faces the same security treats as it predecessor IPv4 but in different forms and the solutions are not farfetched. IPSec works very efficiently with IPv6 since it is a key component of its design.

The rate of adoption for IPv6 has been slow especially in the AfriNIC and the ARINIC Regions. This study recommend to customers to demand IPv6 services from their ISPs in order to increase the adoption rate of the next generation protocol.

6. REFERENCES

[1] Fuller V. and Li T. "Classless Inter-Domain Routing (CIDR): The Internet Address Aggregation Plan " *RFC 4632,* August- 2006.

[2] Droms R "IPv6 Multicast Address Scopes" RFC-7346, [standard], August, 2014.

[3] Thomson S. and Narten T, "IPv6 Stateless Address Autoconfiguration," *Internet Request for Comments*, vol. RFC 2462 (Draft Standard), Dec. 1998.

[4] Droms R. "Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6" RFC 3736 ,[standard], April 2004

[5] Droms R, Bound J, Volz B, Lemon T, Perkins C, and Carney M, "Dynamic HostConfiguration Protocol for IPv6 (DHCPv6)," *Internet Request for Comments*, vol. RFC 3315 (Proposed Standard), Jul. 2003.

[6] Liu C. and Albitz *P. "DNS and BIND", 5th Edition,* O'Reilly Media, May 2006

[7] Hagen S, *IPv6 essentials [integrating IPv6 into your IPv4 network*. 3rdEdition, Beijing; Cambridge [Mass.]; Farnham [England]: O'Reilly, 2014

[8] Deering S and Hinden R, "Internet Protocol, Version 6 (IPv6) Specification," *InternetRequest for Comments*, vol. RFC 2460 (Draft Standard), Dec. 1998

[9] Malkin G and Minnear R, "RIPng for IPv6" RFC 2080, [Standard], January 1997

[10] Coltun R, Ferguson D, Moy J, and Lindem A, "OSPF for IPv6," *Internet Request for Comments*, vol. RFC 5340 (Proposed Standard), Jul. 2008.

[11] Kurose J. F and Ross K. W, "*Computer networking: a top-down approach"*. Boston, Mass. Pearson, 2010.

[12] Rekhter Y, Li T. and Hares S. "A Border Gateway Protocol 4 (BGP-4)," *Internet Request for Comments*, vol. RFC 4271 (Draft Standard), Jan. 2006

[13] Krilanovich M. “NETWORK FORTRAN SUBPROGRAMS”, RFC 119, April 21, 1971

[14] Kompella K. Drake J. Amante J, Henderickx W. and Yong L. “The Use of Entropy Labels in MPLS Forwarding”, RFC 6790, [Proposed Standard], November 2012.

[15] Perkins C. Johnson D. and Arkko J, “Mobility Support in IPv6”, RFC 6275 [Standard], July 2011.

[16] Rajahalme J, Conta A, Carpenter B and Deering S “IPv6 Flow Label Specification”, RFC 3697 [Standard], March 2004.

7. APPENDIX

Table 2 Ping statistics from simulated platform.

ZIP2				ZIP3				ZIP4			
Average RTT/ms		Traceroute		Average RTT/ms		Traceroute		Average RTT/ms		Trace route	
V4	V6	V4	V6	V4	V6	V4	V6	V4	V6	V4	V6
93	94	1	1	122	122	2	2	147	146	3	3
92	92	1	1	120	120	2	2	146	144	3	3
88	88	1	1	124	126	2	2	140	142	3	3
94	94	1	1	114	118	2	2	146	144	3	3
93	92	1	1	118	120	2	2	144	140	3	3
90	90	1	1	120	118	2	2	140	148	3	3
92	96	1	1	118	120	2	2	142	142	3	3
90	92	1	1	120	122	2	2	138	139	3	3
88	89	1	1	122	123	2	2	134	136	3	3
84	84	1	1	122	122	2	2	143	142	3	3
92	88	1	1	114	120	2	2	144	145	3	3
90	90	1	1	118	119	2	2	146	146	3	3
93	94	1	1	128	122	2	2	147	146	3	3
91	92	1	1	124	124	2	2	142	147	3	3
92	93	1	1	126	124	2	2	140	148	3	3

Table 3 Ping statistics from a tunnel broker.

www.lacnet.net (200.3.14.10)				www.sixxs.net (212.126.37.76)				www.google.com (74.125.136.94)			
Average RTT/ms		Traceroute		Average RTT/ms		Traceroute		Average RTT/ms		Traceroute	
IPV4	IPV6	V4	V6	IPV4	IPV6	V4	V6	IPV4	IPV6	V4	V6
397	408	17	18	182	190	12	11	293	300	14	12
394	402	17	18	180	188	12	11	292	298	14	12
392	402	17	18	184	190	12	11	291	296	14	12
394	402	17	18	184	190	12	11	290	296	14	12
393	405	17	18	181	189	12	11	291	297	14	12
390	403	17	18	180	188	12	11	292	298	14	12
392	402	17	18	179	185	12	11	292	298	14	12
390	405	17	18	180	186	12	11	293	297	14	12
388	406	17	18	182	193	12	11	294	297	14	12
384	405	17	18	180	186	12	11	293	296	14	12
392	408	17	18	181	187	12	11	294	299	14	12
390	406	17	18	178	185	12	11	291	298	14	12
391	402	17	18	178	182	12	11	293	297	14	12
392	404	17	18	179	184	12	11	292	296	14	12
392	403	17	18	176	183	12	11	294	299	14	12