Comparison of IPv4-over-IPv6 (4over6) and Dual Stack Technologies in Dynamic Configuration for IPv4/IPv6 Address

[a]Ta Te Lu, [a]Cheng Yen Wu, *[b]Wen Yen Lin,
[a]Hsin Pei Chen, [b]Kuang Po Hsueh

[a]Chien Hsin University of Science and Technology
[a]Institute of Computer Science and Engineering
[b]Vanung University
[b]Digital Multimedia Technology

[a]ttlu@uch.edu.tw, [a]johnny.wu520@gmail.com,
*[b]qqnice@mail.vnu.edu.tw, [a]hpchen@uch.edu.tw
[b]kphsueh@gmail.com

Abstract. IPv4 and IPv6 technologies face many challenges on LAN or the Internet such as transition mechanisms. The Internet Engineering Task Force (IETF) proposed a variety of solutions, e.g. Dual stack, IPv6-in-IPv4 (IPv4-IPv6), and IPv4-over-IPv6 (4over6). Clients use manual, stateful, or stateless auto configuration to get IPv6 addresses. Auto configuration with Stateful Dynamic Host Configuration Protocol for IPv6 (DHCPv6) protocol automatically configures IPv6 address through the router into the LAN, which is the best allocation choice. The DHCPv4 and DHCPv6 (DHCP 4o6) server used 4over6 and is considered to generally be the best plan.

In this paper, we set up a network communications platform and performed an effectiveness analysis comparing DHCPv4 and DHCPv6 (DHCP 4o6) servers individually with Dual Stack and 4over6 tunnel mechanisms. Experimental routing performances show that the routing path from 7 nodes with Dual Stack was better than 4over6 by 17.329%.

Key words: IPv6 transition; DHCPv6; IPv4-over-IPv6; Dual Stack

1 Introduction

In the future of network environments, IPv4-to-IPv6 or IPv6-to-IPv4 communications is an important step for Internet development. IPv6 and IPv4 environments are different and independent, and how compatible they are will influence how much time they occupy during the transition period. Presently, IP-based solutions do not deal with all these self-management demands, which leads to different approaches being adopted by different standardization bodies and even different approaches within the same

J.-S. Pan et al. (eds.), *Advances in Intelligent Information Hiding and Multimedia Signal Processing*, Smart Innovation, Systems and Technologies 63,
DOI 10.1007/978-3-319-50209-0_32

standardization bodies as systems evolve and new network architectures are developed [1]-[2]. IETF has further developed different types of IPv6 conversion techniques, including dual stack, translation, and tunneling for different IPv6 conversion scenarios. We consider IP-based communications quickly changing topologies from dynamic topological addressing auto-configuration mechanisms to be a major concern [3]. DHCP provides dynamical network configuration to hosts in an IPv4 environment. DHCP broadcasts router solicitation message through LAN to provide the address of the default router to hosts. 4over6 tunneling and dual stack technology have become a major transition scenario particularly since more and more IPv6 access networks are being deployed, while IPv4 users need to communicate with the IPv4 Internet through these IPv6 networks as shown in figure 1.

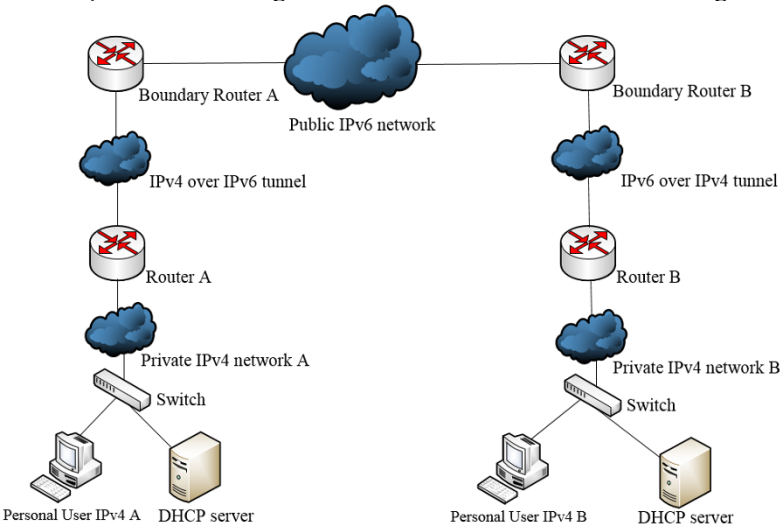

Fig. 1. IPv4-over-IPv6 transition architecture

Stateless address auto-configuration is a standard characteristic of Internet Control Message Protocol version 6 (ICMPv6) [4], permitting a router to advertise an IPv6 prefix to provide clients an individual IPv6 address. On the other hand, stateful address-auto-configuration supplies clients with IPv6 addresses from a central authority through the use of DHCPv6 (RFC 3315). DHCPv6 provides DHCPv6 DNS options when answering to requests or information-request messages. Therefore, IPv6 clients can use DHCPv6 for address distribution or stateless DHCPv6 to receive other configuration information for choosing DNS options. DHCPv6 supplies a mechanism for reconfiguring and propagating new configuration information to DHCPv6 clients when DNS information is transformed or updated. DHCPv6 allows administrators more control over address distribution than Stateless Address Auto Configuration (SLAAC) [5]. When IPv6 clients use the default DCHPv6 and as IPv4 clients use the default DHCP, the management and configuration

options provided by the protocol can be useful in extensive, complex networks. Different realms can be established to configure different addresses for different parts of the networks, as shown in figure 2.

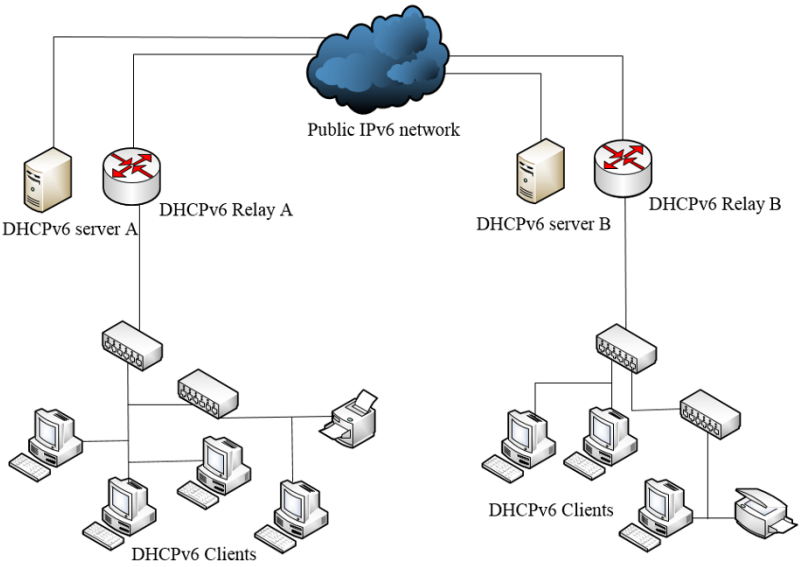

Fig. 2. DHCPv6 Architecture

DHCPv6 involves the DNS recursive name server option and the domain search list option. The DNS servers and domain names are listed in these two options in order of preference for use by the DNS resolver on the client. Therefore, the IPv6 client can choose DNS options using DHCPv6 for address distribution or stateless DHCPv6 to gain other configuration information.

2 Research Background

A Basic Bridging Broad Band (B4) element is only configured from the service provider with IPv6. As such, it can only learn the address of a DNS recursive server through DHCPv6 (or other similar methods over IPv6). As DHCPv6 only defines an option to get the IPv6 address of such a DNS recursive server, the B4 element cannot easily discover the IPv4 address of such a recursive DNS server, and as such will have to perform all DNS resolution over IPv6. The B4 element can pass this IPv6 address to downstream IPv6 nodes, but not to downstream IPv4 nodes. (Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion) [6] The DNS Recursive Name Server option provides a list of one or more IPv6 addresses of DNS recursive name servers to which a client's DNS resolver may send DNS queries. DNS servers are listed in the order of preference for use by the client resolver.

The current literature on 4over6 technology aspects, such as Lin Liu proposed

"The Research of 4over6 Transition System Deployment for IPv6 Backbone" [7], is based on the above 4over6 tunneling technology, with Provider Edge equipment (PE) being responsible for the conversion of marginal networks. As shown in figure 3, PE1 and PE2 boundary routers are mainly responsible for encapsulation, de-capsulation, and forwarding. IPv4-IPv6 transition mechanisms are separated into backbone network conversion environments and marginal network conversion environments. Backbone network conversion environment mechanisms include 6to4, NAT-PT, and SIIT. Client device router (as CE1, CE2) is responsible for marginal network conversion, and the environmental mechanisms include DS-Lite, public 4over6, lightweight 4over6, MAP, and others.

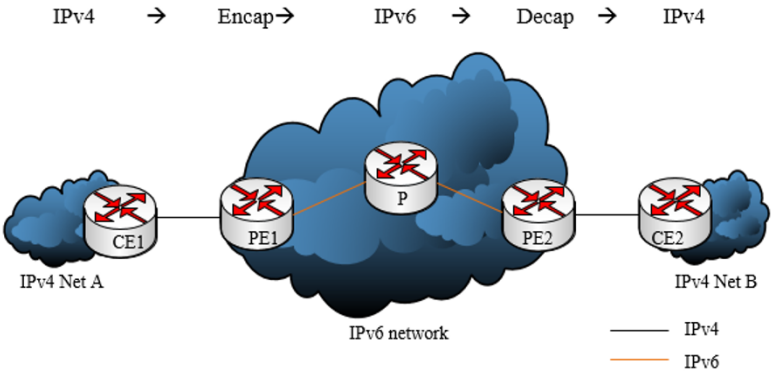

Fig. 3. 4over6 data plane

Dr. Zilong Liu proposed [8] using the lwB4 customer premises equipment (CPE) and lwAFTR the boarder router device (BR) to form a lightweight 4over6 tunnel network CERNET2 mechanism deployed in an IPv6 network environment. The new DHCP406 server respectively uses lwB4 and lwAFTR (BR) to does lease query on servers in figure 4.

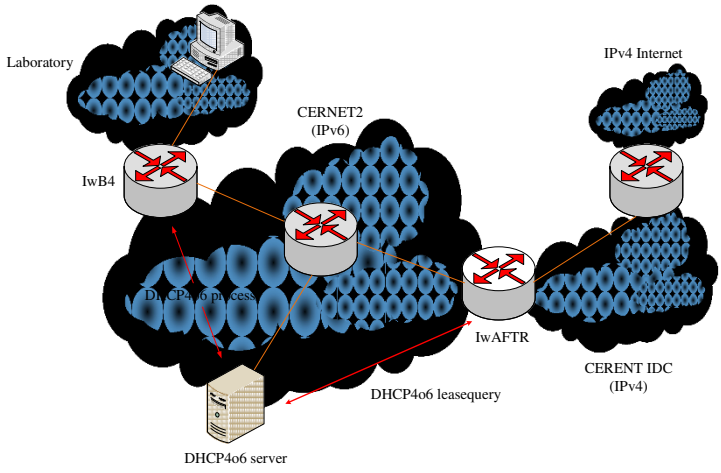

Fig. 4. Deployment in Lightweight 4over6 network at Tsinghua University

3 Tunneling and Dual Stack Routing Introduction

A. IPv4-over-IPv6 tunneling:

An IPv4-based network infrastructure will link to an IPv6 internet network in the future. IPv4 terminals connect to an IPv6 Internet network through IPv4-over-IPv6 tunneling conversion as shown in Figure 5. IPv4 packets are encapsulated into IPv6 packets in R1, and transmitted through IPv6 network links. IPv4 packets are de-capsulated from IPv6 packets in R2. Generic routing encapsulation (GRE) IPv4 tunnel supports IPv6 traffic—IPv6 traffic to carry IPv6 packets in IPv4-based network. The standard GRE tunneling technique is designed to provide secure communication between two boundary devices to implement point-to-point encapsulation scheme. C1 (e3/0 192.168.6.2/30)and R5(e3/1 192.168.6.1/30), R5(e3/0 192.168.3.2/30) and R3(e3/1 192.168.3.1/30), R3(e0/0 192.168.1.1/30) and R1(e0/0 192.168.1.2/30, tunnel 0 192.168.9.1), R2(e0/0 192.168.5.1/30, tunnel 0 192.168.9.2) and R4(e0/0 192.168.5.2/30), R4(e3/1 192.168.4.1/30) and R6(e3/0 192.168.4.2/30), R6(e3/1 192.168.7.1/30) and C2(e3/0 192.168.7.2/30) have six different local area network segment, they set routing protocol to OSPF for IPv4. R1(e0/1 2001:DB8:2:2::1/64) and R2(e0/1 2001:DB8:2:4::2/64) are boundary routers on WAN, with routing protocol set to OSPFv3 for IPv6. R1's tunnel IP is 192.168.9.1/24, the tunnel source is 2001:DB8:2:2::1, and the tunnel destination is 2001:DB8:2:4::2. R2's tunnel IP is 192.168.9.2/24, the tunnel source is 2001:db8:2:4::2, and the tunnel destination is 2001:DB8:2:2::1. When C1 transports data to C2, it must be through R5, R3, R1 by OSPF in the local area network. R1 and R2 does so by OSPFv3 [9] and 4over6 tunneling in the internet. Finally, this can be done through R2, R4, R6 by OSPF in the local area network to C2.

B. Dual stack:

Dual stack means that devices are able to run IPv4 and IPv6 in parallel in a network, so Dual stack offers a very flexible coexistence strategy. Setting Dual stack protocol in the router mode for IPv4 and IPv6, involves running IPv4 and IPv6 at the same time in Figure 6. End nodes (T1 and T2) and routers (R1, R2, R3, R4, R5, R6) run both IPv4/IPv6 protocols, and if IPv6 communication is possible, that protocol is preferred. C1 (e1/0 10.0.5.2/30, 2001:16::2/64) and R5 (e1/1 10.0.5.1/30, 2001:16::1/64), R5 (e1/0 10.0.3.2/30, 2001:14::2/64) and R3 (e1/1 10.0.3.1/30, 2001:14::1/64), R3 (e1/0 10.0.1.2/30,2001:11::2/64) and R1 (e1/0 10.0.1.1/30, 2001:11::1/64), R2 (e1/0 10.0.2.1/30, 2001:13::1/64) and R4 (e1/0 10.0.2.2/30, 2001:13::2/64), R4 (e1/1 10.0.4.1/30, 2001:15::1/64) and R6 (e1/0 10.0.4.2/30,2001:15::2/64), R6 (e1/1 10.0.6.1/30,2001:17::1/64) and C2 (e1/0 10.0.6.2/30,2001:17::2/64) have six different local area network segments, and they set routing protocol to OSPF for IPv4 and OSPFv3 for IPv6. R1 (s2/0 10.10.10.1/30, 2001:12::1/64) and R2 (s2/0 10.10.10.2/30, 2001:12::2/64) are boundary routers on WAN, and they set routing protocol to static routing for IPv4 and

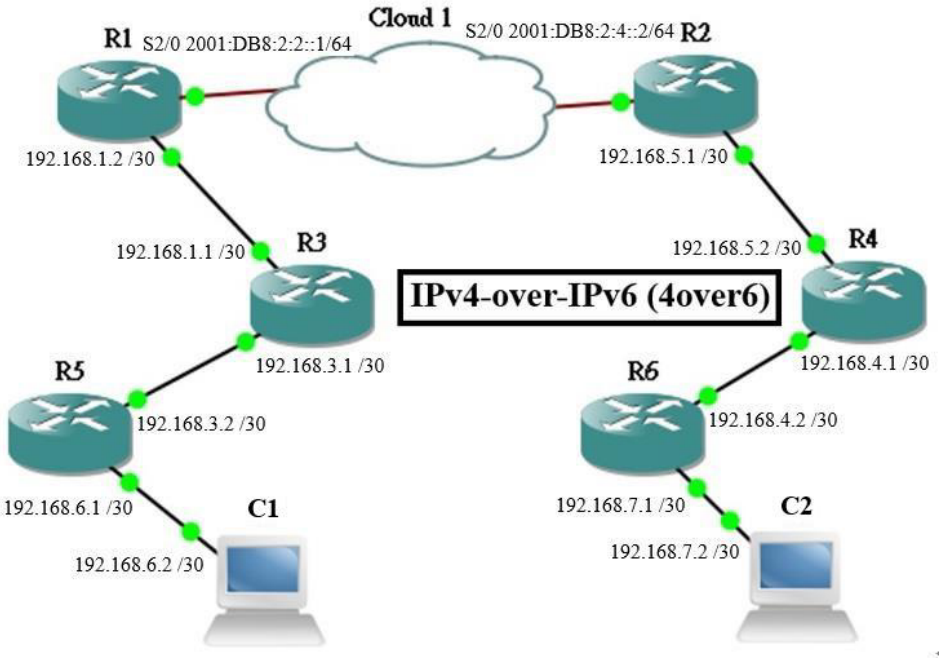

Fig. 5. IPv4 for routing communications through IPv4-over-IPv6 (4over6) architecture.

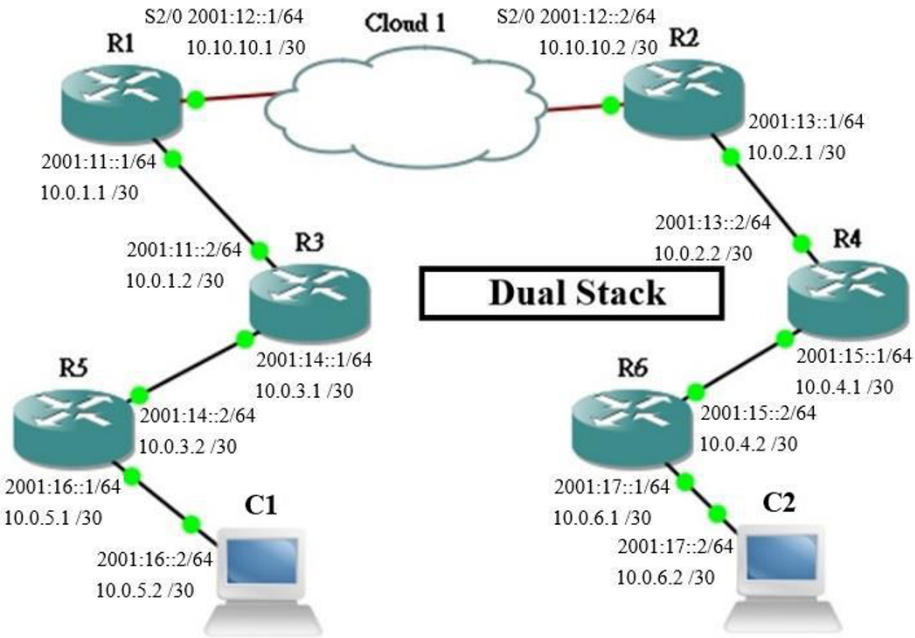

Fig. 6. IPv4 for routing communications through Dual Stack architecture.

IPv6. When C1 transports data to C2, it must be through R5, R3, R1 by OSPF for IPv4 or OSPFv3 for IPv6 in the local area network. R1, R2 does so by static routing for IPv4 and IPv6 on WAN. Finally, this can be done through R2, R4, R6 by OSPF for IPv4 or OSPFv3 for IPv6 in the local area network to C2.

Liu et al. [8] proposed a DHCPv4 server to deliver IPv4 to terminal equipment. After obtaining IPv4 address, if it needs external communication, IPv4 address will encapsulate through 4over6 tunneling server, and then afterwards convert to IPv6 external communication, as shown in figure 7.

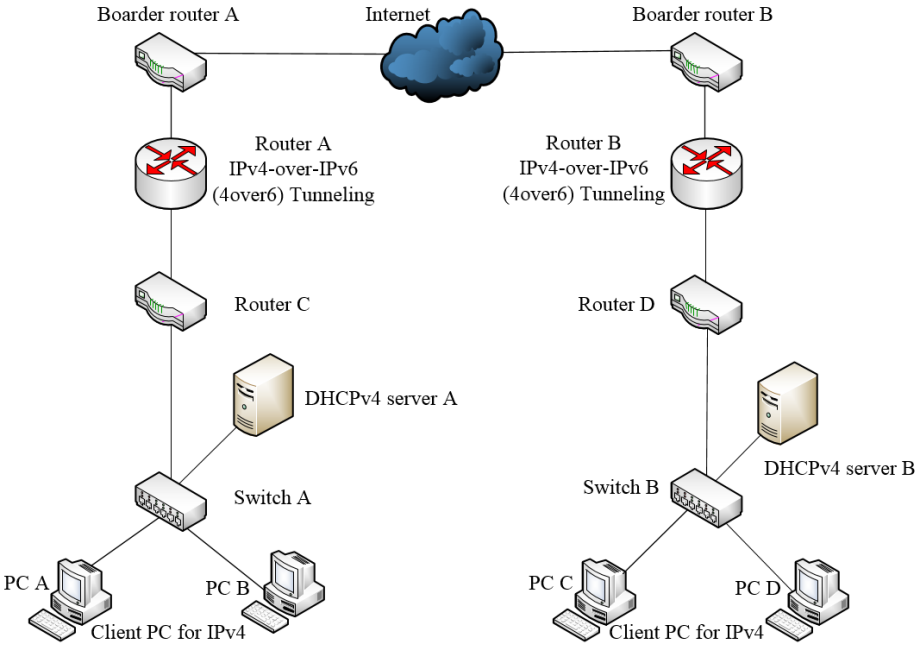

Fig. 7. IPv4-over-IPv6 tunneling architecture

This paper will present two improvement programs:

1. Remove DHCPv4 server A and DHCPv4 server B, as shown in figure 7. Router C and Router D will replace DHCPv4, as figure 8.

   It will have the following three benefits:

   A. Reduced cost: If a router is set to increase the DHCP function, enterprise

   companies do not need to provide additional servers and operating systems.

   B. Reduced information security risks: Stable routing platform that can avoid the risk of hackers attacking a DHCP server.

   C. Reduced administrator workload: Routers use a simple command-line interface and associated command set description, and engineers can reduce the workload of maintaining a DHCP server.

2. Dual stack replaces 4over6 mechanism, as shown in figure 8.

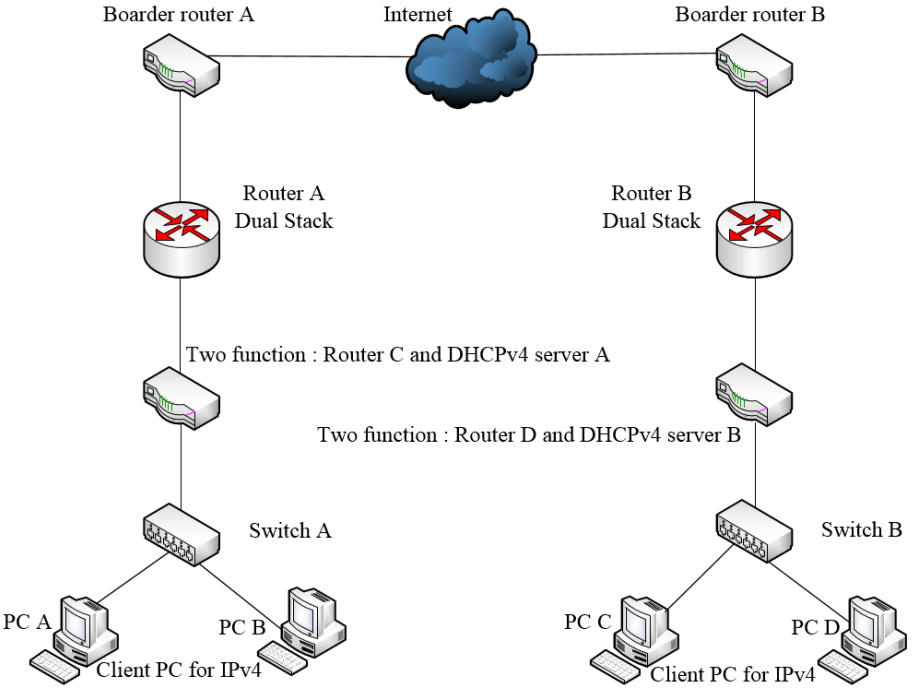

Fig. 8. Dual Stack architecture

4 Simulation and analysis

In accordance with Liu et al. [8], R1 and R2 employed 4over6 VPN routing/forwarding (VRF), R5 and R6 employed DHCPv4 functions, as shown in Fig. 5. The endpoint C1 tracks the IPv4 packets through R5 (192.168.6.1 DHCPv4 router), R3 (192.168.3.1), boundary router R1 (192.168.1.2), 4over6 tunnel from R1 to R2, boundary router R2 (192.168.9.2), R4 (192.168.5.2), R6 (192.168.4.2, DHCPv4 router), to arrive endpoint C2 (192.168.7.2). We tested tracking the route from C1 to C2 (192.168.7.2) fifty times and got an average result as shown in figures 9 and 11.

```
C1#traceroute 192.168.7.2
Type escape sequence to abort.
Tracing the route to 192.168.7.2
VRF info: (vrf in name/id, vrf out name/id)
  1 192.168.6.1 4 msec 32 msec 28 msec
  2 192.168.3.1 44 msec 72 msec 48 msec
  3 192.168.1.2 104 msec 80 msec 88 msec
  4 192.168.9.2 124 msec 120 msec 120 msec
  5 192.168.5.2 128 msec 144 msec 152 msec
  6 192.168.4.2 160 msec 144 msec 184 msec
  7 192.168.7.2 224 msec 172 msec 184 msec
```

Fig. 9. IPv4-over-IPv6 (4over6) tracking results

R1 to R6 employed Dual Stack architecture in Fig. 6. Client C1 tracks the IPv4 packets through R5 (10.0.5.1 DHCPv4 router), R3 (10.0.3.1), boundary router R1 (10.0.1.1), boundary router R2 (10.10.10.2), R4 (10.0.2.2), and R6 (10.0.4.2, DHCPv4 router) to arrive client C2 (10.0.6.2). We tracking the route from C1 (10.0.5.2) to C2 (10.0.6.2) fifty times and got an average result as shown in figure 10 and 11.

```
C1#traceroute 10.0.6.2

Type escape sequence to abort.
Tracing the route to 10.0.6.2

  1 10.0.5.1 40 msec 28 msec 4 msec
  2 10.0.3.1 76 msec 44 msec 32 msec
  3 10.0.1.1 68 msec 60 msec 64 msec
  4 10.10.10.2 92 msec 96 msec 104 msec
  5 10.0.2.2 124 msec 124 msec 120 msec
  6 10.0.4.2 188 msec 152 msec 108 msec
  7 10.0.6.2 172 msec 168 msec 144 msec
```

Fig. 10. Dual Stack tracking results

Figure 11 compares the results of Dual Stack and IPv4overIPv6 mechanisms tracked through seven nodes (from C1 to C2) of the average time for Dual Stack and IPv4overIPv6 was 95.615 msec and 112.185 msec, respectively.

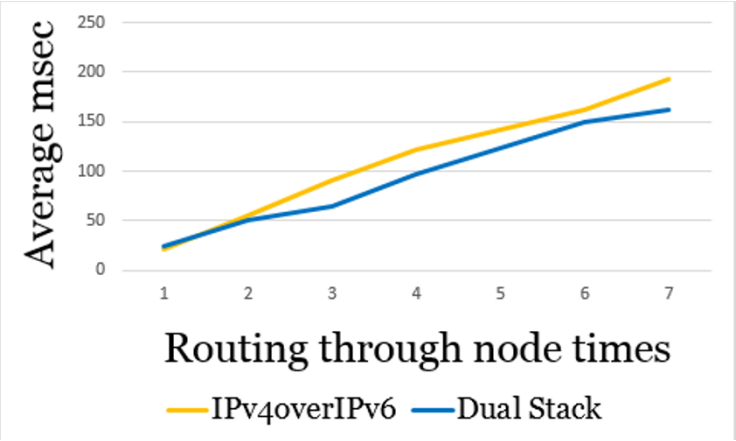

Fig. 11. Dual Stack and IPv4overIPv6 comparison of results

5 Conclusion

IPv6 and IPv4 environments are different, and are compatible for a long time during the transition period. IPv6 to IPv4 or IPv4 to IPv6 routing environments will be seen very frequently in the future.

In this paper, the performances of IPv4overIPv6 and Dual Stack tracking results are compared. The average time for Dual Stack and IPv4overIPv6 was 95.615 msec and 112.185 msec, respectively. Routing performance of Dual Stack is better than IPv4overIPv6 17.329%.

6 References

1. Cui, Y., Wu, J., Wu, P.: Public IPv4-over-IPv6 Access Network. IETF RFC 7040 (2013)
2. Bound, J., Packard, H., Ericsson, B., Lemon, V., Nominum, T., Perkins, C., Carney, M., Microsystems, S.: Dynamic Host
3. Configuration Protocol for IPv6 (DHCPv6). IETF RFC 3315 (2003)
4. Imadali, S., Vèque, V., Petrescu, A.: Analyzing Dynamic
5. IPv6 Address Auto-configuration Techniques for Group IP-Based Vehicular
6. Communications. 39th IEEE Conference on Local Computer Networks
7. Workshops (LCN Workshops), pp. 722 – 729, France (2014)
8. Conta, A., Deering, S., Gupta, M.: Internet Control Message Protocol (ICMPv6)
9. for the Internet Protocol Version 6 (IPv6) Specification. IETF RFC 4443 (2006)
10. Thomson, S., Narten, T., Jinmei, T.: IPv6 Stateless Address

Autoconfiguration.
11. IETF RFC 4862 (2007)
12. Woodyatt, J., Lee, Y., Durand, A., Droms, R.: RFC 6333 Dual-Stack Lite
12. Broadband Deployments Following IPv4 Exhaustion. IETF RFC 6333 (2011)
13. Lin, L., Cui, Y,. Sun, J., Sun, Q.: The research of 4over6 transition system deployment for IPv6 backbone. 2nd International Conference on Computer
14. Science and Network Technology (ICCSNT), pp. 912 –915, Beijing, China (2012)
15. Zilong, L., Jiang, D., Yong, C., Chaokun, Z.: Dynamic Configuration for IPv4/IPv6 Address Mapping in 4over6 Technology. 9th IEEE International Conference on Anti-counterfeiting, Security, and Identification (ASID), pp. 132 –136, Beijing, China (2015)
16. Coltun, R., Ferguson, D., Moy, J., Lindem, A.: OSPF for IPv6. IETF RFC 5340 (2008)