Analysis of BGP4 Peering Establishment Time on IPv6 Connection over 6PE and 6VPE

Irwan Piesessa [1] and Benfano Soewito [1]

[1] Computer Science Department, BINUS Graduate Program - Master of Computer Science, Bina Nusantara University, Jakarta, Indonesia

Abstract: Nowadays, because of the exhaustion of IPv4 address space, IPv6 is increasingly being used on enterprise networks. Usually, an enterprise uses an MPLS network from a Service Provider to interconnect their IPv4 network sites. Although MPLS Service Providers mostly built their MPLS backbone based on IPv4, their MPLS backbone have the capability to transport IPv6 traffic of their customers. Two methods can be used by the MPLS Service Provider to connect its customer IPv6 network, which is 6PE (IPv6 Provider Edge Routers) and 6VPE (IPv6 VPN Provider Edge Router). Enterprises generally use a BGP routing protocol to interconnect their networks, and they need to use the best method that suits their requirement from their MPLS Service Provider to transport their IPv6 traffic (including the BGP protocol). The MPLS Service Providers need to consider the advantages and disadvantages of both methods. This paper illustrates the analysis of BGP4 (current BGP version) IPv6 peering establishment time over 6PE and 6VPE methods. The MPLS Service Providers can use the analysis results of this study to determine the suited method to interconnect its customers' IPv6 networks.

Keywords: IPv6, BGP, MP-BGP, MPLS, 6PE, 6VPE.

1. Introduction

IPv4 space now is getting smaller. Even though all enterprises are using RFC 1918 Private IP Address such as 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16 prefixes for their internal networks [1] and using NAT to connect to the internet [2], the exhaustion of IPv4 is inevitable. As a solution to this problem, IPv6 is introduced and finalized in 1996 [3]. IPv6 base protocol (RFC 2460) is published in 1998 [4]. Today IPv6 is increasingly being used by enterprises or any organization.

There are several methods for an enterprise or organization that wants to do a transition from the current IPv4 toward IPv6 address. The transition methods are Tunnel Broker, 6RD, DNS64, ISATAP, Teredo, 6to4, NAT64, 464XLAT, and Dual-Stack. Another IPv6 transition methods that can be used by Multiprotocol Label Switching (MPLS) Service Provider to transport their customers IPv6 traffic are 6VPE and 6PE via MPLS network connection.

Enterprises usually use MPLS (Multi-Protocol Label Switching) connection provided by the MPLS Service Provider to interconnect their networks. Even though MPLS Service Providers are generally deployed their MPLS networks based on IPv4, it can transport IPv6 traffic of their customers as well. MPLS is very flexible [5] because it can tunnel many forms of the packet, like IPv4, IPv6, Ethernet, ATM, Frame-Relay, and Serial/PPP [6].

RFC number 4659 describes the 6VPE method. MPLS Service Provider can use IPv4 based MPLS network to provide Virtual Private Network (VPN) to transport their customer IPv6 networks. This method uses the BGP/MPLS IP VPN to support IPv6. 6VPE uses Multi-Protocol BGP (MP-BGP) for IPv6 VPN prefixes distribution over the Service Provider MPLS network [7]. A PE router establishes the MP-BGP peering to other PE routers over the VPN-IPv6 address family. In this method, the customer IPv6 CE router connects to the customer VRF interface of the MPLS Service Provider PE router.

The 6PE method is described in RFC 4798 [8]. In 6PE, the customer CE router connects to the native IPv6 or dual-stack IPv4/IPv6 interface of the PE router. The dual-stack interface is an interface that configured with the IPv4 and IPv6 addresses. The customer IPv6 network will not reside in the VPN IPv6 routing table (VRF), instead of placed in the global IPv6 routing table. Routing table lists information about neighboring nodes and determines the number of hops [9] in RIP (Routing Information Protocol), total amount of costs in OSPF (Open Shortest Path First) or list of ASN (Autonoumous System Number) and some other parameters in BGP (Border Gateway Protocol) to reach the destination node.

Like 6VPE, in the 6PE method, the PE router uses MP-BGP to distribute the customer IPv6 prefixes along with its assigned labels. But instead of uses MP-BGP VPN-IPv6 address-family peering connection, it uses an IPv6 address-family peering connection. These BGP IPv6 prefixes are propagated to it MP-BGP IPv6 address-family peer router that has the same VRF table over the MPLS network. We can see the 6VPE and 6PE network diagram in figure 1.

2. Related Works

Several studies have already been conducted to evaluate the performance of the IPv6 network and its applications. For example, Aloufi analyzed structure recommendations and message size for the IPv6 over Low Power Wireless Personal Area Networks (6LoWPAN) stack model [10]. Yang and Wu studied the Hierarchical Mobile IPv6 (HMIPv6) Binding Update message to support Call Admission Control (CAC) schemes to guarantee every service meets their Quality of Service (QoS) requirements in the mobile network of Wireless Broadband [11].

IPv4 to IPv6 transition methods also have been studied. For example, Quintero, Sans, and Gamess have studied the performance of ISATAP, 6to4, and NAT64 on several Operating Systems such as Debian, Windows 7, Windows 8, and Windows 10. For NAT64, they used two tools namely TAYGA and Jool and they measured the OWD and the TCP and UDP throughput for every transition method [12]. Repas, Farnadi, and Lencse did a study on the evaluation of free NAT64 implementations. The stability and performance of ICMP, TCP, and UDP on the NAT64 transition method were examined by used the TAYGA and PF tools [13]. Grayeli, Sarkani, and Mazzuchi analyzed the performance of the IPv6 transition mechanism (including manual tunnel, GRE, automatic IPv4-compatible tunnel, and 6to4) and compared it with 6PE, Dual-Stack, and native IPv6) over the MPLS network. The parameters that analyzed and compared were an end-to-end delay, jitter, and throughput using the OPNET simulation tool [14]. Salih, Abdalrahman, and Elsharif studied the overall network performance of the 6VPE by analyzed the round trip delay and traffic route for IPv6 connection. The overall network performance was evaluated because MPLS using labels instead of IP header to increase the level of the security of the customer's network [15]. Algabri, Alhomdy, Alselwi, Alowiri, and Sharaby have analyzed the performance of the IPv6 MPLS and MPLS VPN by sending video and audio traffic over both connections using the Opnet network simulator [16]. Al-Hamadani and Lencse reviewed the results of several papers that analyzed the performance of IPv6 transition technologies. The parameters that were compared from the papers were jitter, RTT, throughput, and packet-loss [17]. Vinodkumar, Vijayalakshmi, Kavitha, and Karthick studied the implementation of IPv6 networks for internets services and VPN in IPv6 network using MPLS [18]. Hamarsheh, Abdalaziz, and Nashwan discussed the process of the transition from IPv4 to IPv6 and the major impediments for worldwide IPv6 deployment [19].

On BGP routing protocol in terms of its implementation on the IPv6 network, several studies have been conducted. For example, Trung and Kotsis studied the development of BGP-GCR+ which is a combination between BGP routing protocol, Gravitational Cluster Routing (GCR), and IPv6 address stateless auto-configuration to enable Mobile Ad-Hoc Networks (MANET) function as a load-balancer of a transit network for the internet [20]. Zhang, Liu, and Pei observed the global routing data from RouteViews and they found the behavior of BGP AS Path Looping (either on IPv4 or IPv6) occurred and can create Multi-AS forwarding loops [21]. Jia, Luckie, Huffaker, and Elmokashfi analyzed the development of the IPv6 internet in terms of trends in the growth, structure, dynamics, and performance using historical BGP data [22].

Several studies also have been conducted to evaluate the performance of BGP in terms of establishment or convergence time. For example, Deshpande and Sikdar studied the impact of topology and the message handling procedure of BGP on its establishment/convergence time. They evaluated the convergence times of the BGP router network on the number of MRAI (Minimum Route Advertisement Interval) [23]. Bonaventure, Filsfils, and Francois studied and proposed a new BGP fast-reroute technique as routers are prepared to have a quick reaction to an interdomain link failure. The solution is to build the protection-tunnel from a BGP router to the alternative next-hop BGP router of the same destination prefix address [24]. Zhang, Massey, and Zhang examined the performance of the packet delivery of the BGP network when the destination may be disconnected from the network multiple times. On the examination, they created two metrics to measure the time interval between the perceived unreachability and the actual connectivity loss [25]. Da Silva and Mota reviewed several methods to improve the performance of the BGP inter-domain routing. Those methods can fix the problem of slow-convergence on the BGP network [26]. Devikar, Patil, and Chandraprakash summarized several approaches to improve the BGP convergence time. The approaches that were reviewed were BGP policies, fault detection, etc. [27]. Wang analyzed the convergence problem of the BGP network. MRAI (Minimum Route Advertisement Interval) that accelerates the BGP routing convergence time was evaluated in this study [28].

On IP services or dynamic routing protocol over (or combined) with the MPLS, several studies have been conducted. Katsuno, Yamazaki, Asami, and Esaki studied Layer 2 Virtual Private Wire Service over MPLS network. Theoretical study and performance testing were conducted in this study [29]. Shirazi, Asim, Irfan, and Ikram studied and proposed IP Security (IPSec) to mitigate MPLS vulnerabilities and risks [30]. Alawieh and Mouftah analyzed the performance of Multicast service over the MPLS network and compared its reliability with Protocol Independent Multicast (PIM) [31]. Al Mamun, Sheltami, Ali, and Anwar did a comparative study of the performance of the traditional dynamic routing protocols like OSPF and EIGRP, and combined those routing protocols and MPLS to achieve overall network performance improvement [32].

In our study, we compare and analyze the BGP IPv6 peering establishment time of two BGP speaker routers of an enterprise/customer over 6PE and 6VPE connection methods provided by the MPLS Service Provider. The Service Provider MPLS network is built based on IPv4. We are using BGP4 as the current BGP version.

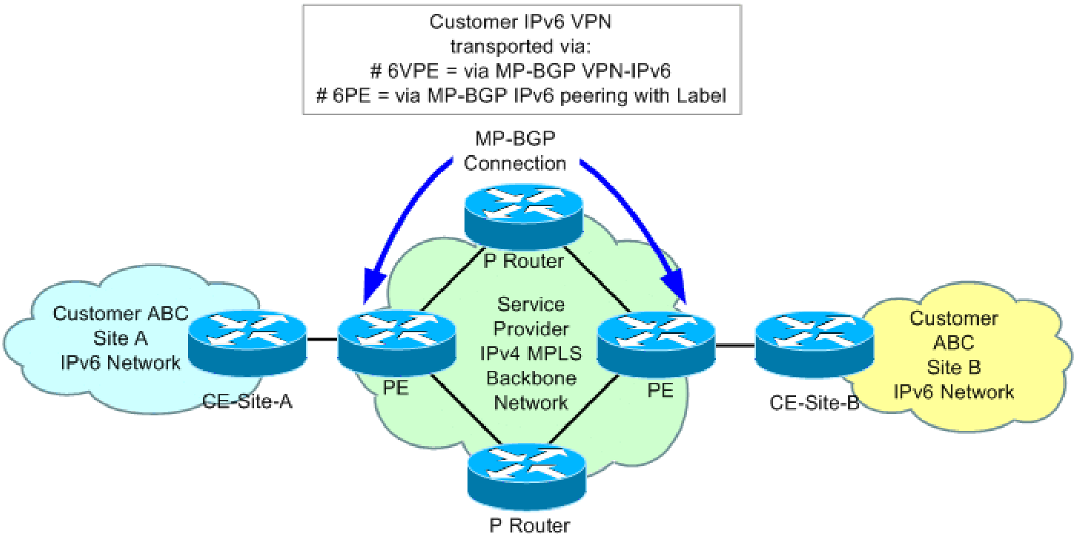


Figure 1. 6VPE and 6PE Network Diagram

3. 6VPE and 6PE Method

3.1 6VPE Method

In 6VPE, the PE router assigns a label to each customer IPv6 prefix. This IPv6 prefix along with its label propagated to other PE router that has the same customer IPv6 VRF (VPN Routing and Forwarding table) by MP-BGP over VPN-IPv6 address-family peering.

When the remote peer PE router receives the IPv6 packet from its customer network on the VPN interface, it then checks the destination address of the packet in its VPN Route Forwarding table (VRF), and lookup the label for that prefix in it VRF MP-BGP table. It also lookup the next-hop address (egress PE) label of the destination IPv6 prefix in its LFIB (Label Forwarding Information Base). The PE router then inserts both labels to the packet as an inner-label and outer-labels. PE router then forwards the IPv6 packet to the next-hop router of the outer-label.

P router will check the outer label of the packet and will do label swapping. P router will look up the LFIB table and swap the outer-label (treat it as a local label) with the outgoing-label of the egress PE router. This packet then forwarded again to the next-hop router of the outer-label. If the P router directly connected to the egress PE router and if the P router configured with PHP (Penultimate Hop Popping), then it will remove the IPv6 packet outer-label.

The egress PE router then receives the packet. If the sender P router has PHP configuration, then the IPv6 packet only has an inner-label. This inner-label is the customer IPv6 prefix label. The PE router then lookup the next-hop router of the inner-label on it LFIB and remove the inner-label. This packet then forwarded to the customer CE router where the destination IPv6 prefix is connected. We can see the example of a customer IPv6 packet that traversing the Service Provider MPLS network that utilized the 6VPE method in figure 2. In the captured packet, we can see the outer-label and inner-label.

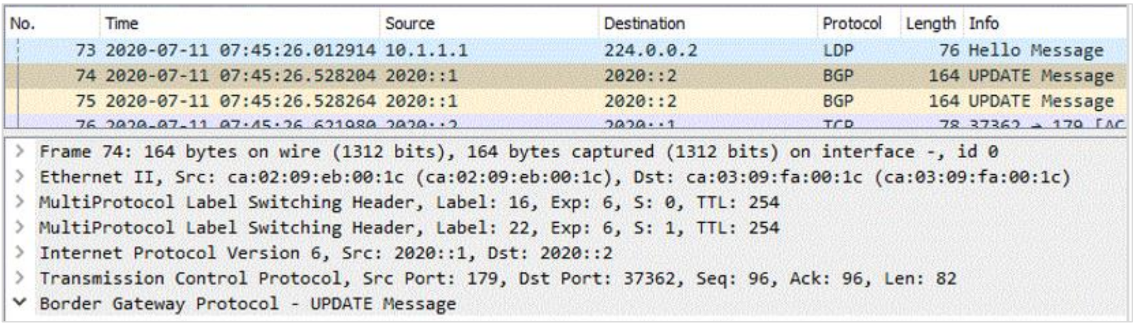
3.2 6PE Method

Like the 6VPE method, in the 6PE, the PE router assigns a label to each customer IPv6 prefix. The PE router then propagates the customer IPv6 prefixes (along with their assigned label) to the MP-BGP peer router. 6PE uses IPv6 address-family to build MP-BGP peering.

When a PE router receives an IPv6 packet on its non-MPLS interface (that connected to the customer CE router), it then checks the destination IPv6 address of the IPv6 packet in the global IPv6 routing table. If the destination IPv6 address comes from the MP-BGP IPv6 address-family peer and has a label assigned, then this label will be inserted to the packet as an inner-label.

The PE router checks the next-hop address of the destination IPv6 address (which is the egress PE). PE router then inserts the label of this egress PE to the packet as an outer-label. This packet then forwarded to the label next-hop router via a specified outgoing interface based on its LFIB table. The next process is similar to 6VPE method.

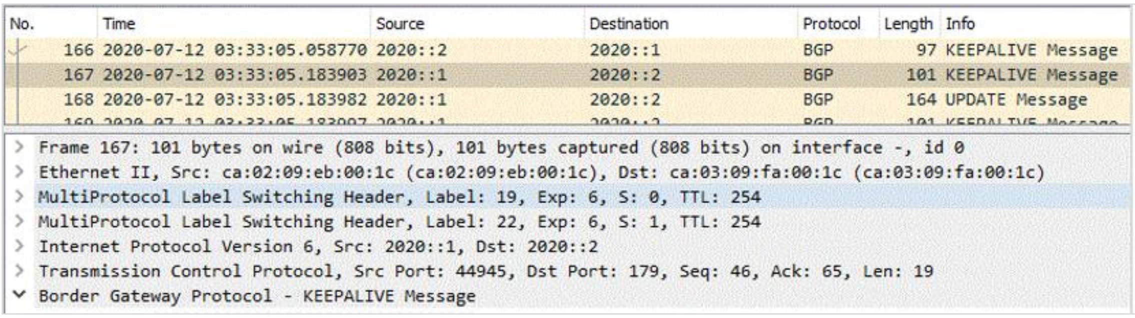
We can see the example of a customer IPv6 packet that traverses the Service Provider MPLS network that uses the 6PE method along with its outer-label and inner-label in figure 3. We also can see the comparison of the 6VPE and 6PE methods in table 1.



```
No.  Time                        Source    Destination  Protocol  Length  Info
 73  2020-07-11 07:45:26.012914  10.1.1.1  224.0.0.2    LDP       76      Hello Message
 74  2020-07-11 07:45:26.528204  2020::1   2020::2      BGP       164     UPDATE Message
 75  2020-07-11 07:45:26.528264  2020::1   2020::2      BGP       164     UPDATE Message
 76  2020-07-11 07:45:26.621980  2020::2   2020::1      TCP       78      37362 → 179 [AC

> Frame 74: 164 bytes on wire (1312 bits), 164 bytes captured (1312 bits) on interface -, id 0
> Ethernet II, Src: ca:02:09:eb:00:1c (ca:02:09:eb:00:1c), Dst: ca:03:09:fa:00:1c (ca:03:09:fa:00:1c)
> MultiProtocol Label Switching Header, Label: 16, Exp: 6, S: 0, TTL: 254
> MultiProtocol Label Switching Header, Label: 22, Exp: 6, S: 1, TTL: 254
> Internet Protocol Version 6, Src: 2020::1, Dst: 2020::2
> Transmission Control Protocol, Src Port: 179, Dst Port: 37362, Seq: 96, Ack: 96, Len: 82
˅ Border Gateway Protocol - UPDATE Message
```

Figure 2. IPv6 packet in MPLS network that uses 6VPE method



```
No.  Time                        Source    Destination  Protocol  Length  Info
166  2020-07-12 03:33:05.058770  2020::2   2020::1      BGP       97      KEEPALIVE Message
167  2020-07-12 03:33:05.183903  2020::1   2020::2      BGP       101     KEEPALIVE Message
168  2020-07-12 03:33:05.183982  2020::1   2020::2      BGP       164     UPDATE Message
169  2020-07-12 03:33:05.183997  2020::1   2020::2      BGP       101     KEEPALIVE Message

> Frame 167: 101 bytes on wire (808 bits), 101 bytes captured (808 bits) on interface -, id 0
> Ethernet II, Src: ca:02:09:eb:00:1c (ca:02:09:eb:00:1c), Dst: ca:03:09:fa:00:1c (ca:03:09:fa:00:1c)
> MultiProtocol Label Switching Header, Label: 19, Exp: 6, S: 0, TTL: 254
> MultiProtocol Label Switching Header, Label: 22, Exp: 6, S: 1, TTL: 254
> Internet Protocol Version 6, Src: 2020::1, Dst: 2020::2
> Transmission Control Protocol, Src Port: 44945, Dst Port: 179, Seq: 46, Ack: 65, Len: 19
˅ Border Gateway Protocol - KEEPALIVE Message
```

Figure 3. IPv6 packet in MPLS network that uses 6PE method

Table 1. Comparison of 6VPE and 6PE method

Router	6VPE	6PE
Interface to the CE Router	Assigned to the VRF	Assigned to the Global Routing Table
Customer IPv6 Prefix	In the VRF Table	In the Global IPv6 Routing Table
MP-BGP for BGP Peering	Yes	Yes
MP-BGP Peering between PEs	Via VPN-IPv6 Address-Family	Via IPv6 Address-Family with Label

4. BGP Peering Establishment Process

BGP (Border Gateway Protocol) is an exterior gateway routing protocol that recommended to be used by an organization that wants to connect to the Service Provider network. BGP also used by an organization to connect to its network located on different sites and different AS (Autonomous System) Number. This BGP connection, whether IPv4 or IPv6, is established over the Service Provider MPLS Network.

RFC 4271 [33] describe the process of BGP peering establishment that follows several states below:

1. BGP_Idle
2. BGP_Active
3. BGP_OpenSent
4. BGP_OpenConfirm
5. BGP_Established.

After a router runs BGP configuration, it will enter the BGP_Idle state. Once BGP peering configured, it (local router) will initiate BGP TCP Connection to the remote peer [34]. In this phase, the local router also listens for a BGP TCP initiation connection from the remote peer. If the remote peer acknowledges the TCP connection by sending the TCP packet with SYN and ACK flags, then the local router will respond with sending the response TCP packet with the ACK flag. The TCP connection established. The local router will be sending the BGP Open message to the remote peer and move to the BGP_OpenSent state.

In the BGP_OpenSent state, the local router already sent the BGP OPEN message and waiting for the OPEN message from a remote peer. After the local router receives the OPEN message from the remote peer, the local router then will compare the following parameters from both OPEN Messages:

- BGP Version.
- AS (Autonomous System) number must match with the AS number configuration for the remote peer.
- Hold time value (number of seconds that the router can wait for the KEEPALIVE or UPDATE messages from the remote peer).
- BGP Router Identifier.
- Optional Parameters (for example is security parameter) [35].

If at both routers the OPEN message matched the configured parameters, then both routers will negotiate the hold time value and will choose the lower hold time value. Then the routers will send a KEEPALIVE message and move to the OpenConfirm state. In this state, after receiving the KEEPALIVE message, both routers then move to the BGP_Established state. In the BGP_Established state, both routers send UPDATE Message that contains it BGP prefixes routes [36].

5. BGP IPv6 Peering over 6VPE and 6PE Simulation

We analyze BGP IPv6 peering establishment time between two customer CE router over Service Provider MPLS network that running 6PE and 6VPE connection method. The flowchart of the process of our study can be seen in Figure 4. We built an MPLS network of Service Provider (consists of PE and P routers), and IPv6 network sites of an enterprise (customer) on the Network Simulator. We can see the simulation network diagram in Figure 5.

The MPLS network is built based on IPv4. The PE routers have IPv6 interfaces that connected to customer CE routers. BGP IPv6 peering established between CE routers over MPLS. We can see IPv4 and IPv6 address assignment for the MPLS and customer networks in tables 2 and 3.

The MPLS network uses LDP (Label Distribution Protocol) to distribute assigned labels to other PE and P routers. PE-01 and PE-02 routers run the 6VPE connection method while PE-001 and PE-002 routers run the 6PE connection method. For the 6VPE simulation, we create VPN ABC for the customer IPv6 network. The VRF (VPN Routing and Forwarding) applied to the PE-01 and PE-02 interfaces that connected to the customer router (CE-01 and CE-02). We can see the Service Provider 6VPE and 6PE configuration parameters for the simulation network in tables 4 and 5. We also can see the LFIB table (that contains MPLS label allocation of the 6PE and 6VPE simulation networks) and the BGP routing table in figures 6, 7, 8, and 9.

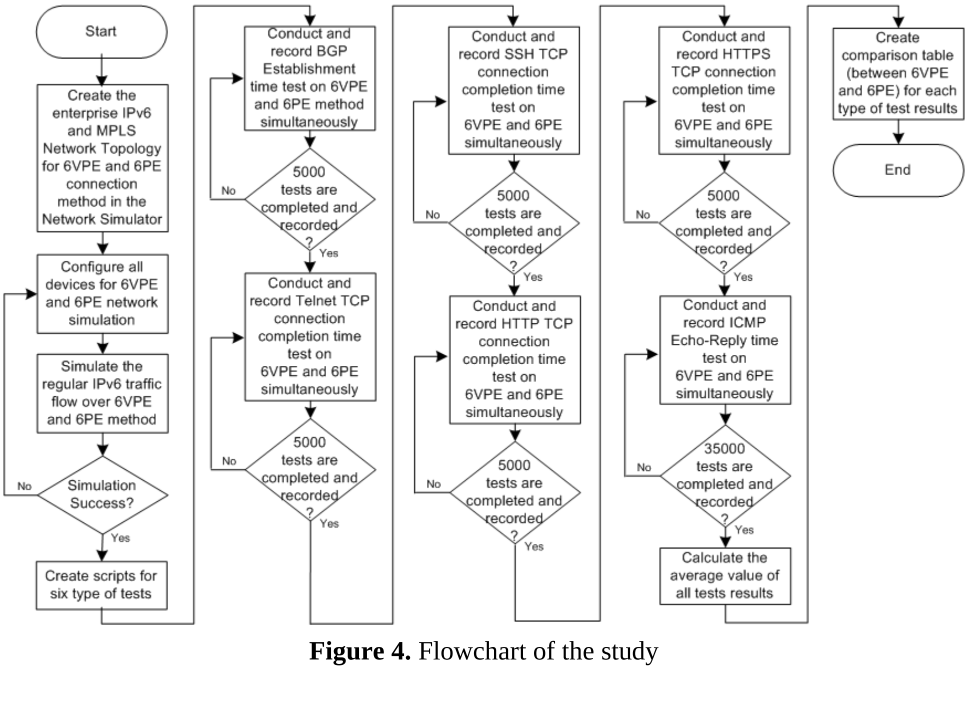

Start
Create the enterprise IPv6 and MPLS Network Topology for 6VPE and 6PE connection method in the Network Simulator
Configure all devices for 6VPE and 6PE network simulation
Simulate the regular IPv6 traffic flow over 6VPE and 6PE method
Simulation Success?
No
Yes
Create scripts for six type of tests
Conduct and record BGP Establishment time test on 6VPE and 6PE method simultaneously
5000 tests are completed and recorded ?
No
Yes
Conduct and record Telnet TCP connection completion time test on 6VPE and 6PE simultaneously
5000 tests are completed and recorded ?
No
Yes
Conduct and record SSH TCP connection completion time test on 6VPE and 6PE simultaneously
5000 tests are completed and recorded ?
No
Yes
Conduct and record HTTP TCP connection completion time test on 6VPE and 6PE simultaneously
5000 tests are completed and recorded ?
No
Yes
Conduct and record HTTPS TCP connection completion time test on 6VPE and 6PE simultaneously
5000 tests are completed and recorded ?
No
Yes
Conduct and record ICMP Echo-Reply time test on 6VPE and 6PE simultaneously
35000 tests are completed and recorded ?
No
Yes
Calculate the average value of all tests results
Create comparison table (between 6VPE and 6PE) for each type of test results
End

Figure 4. Flowchart of the study

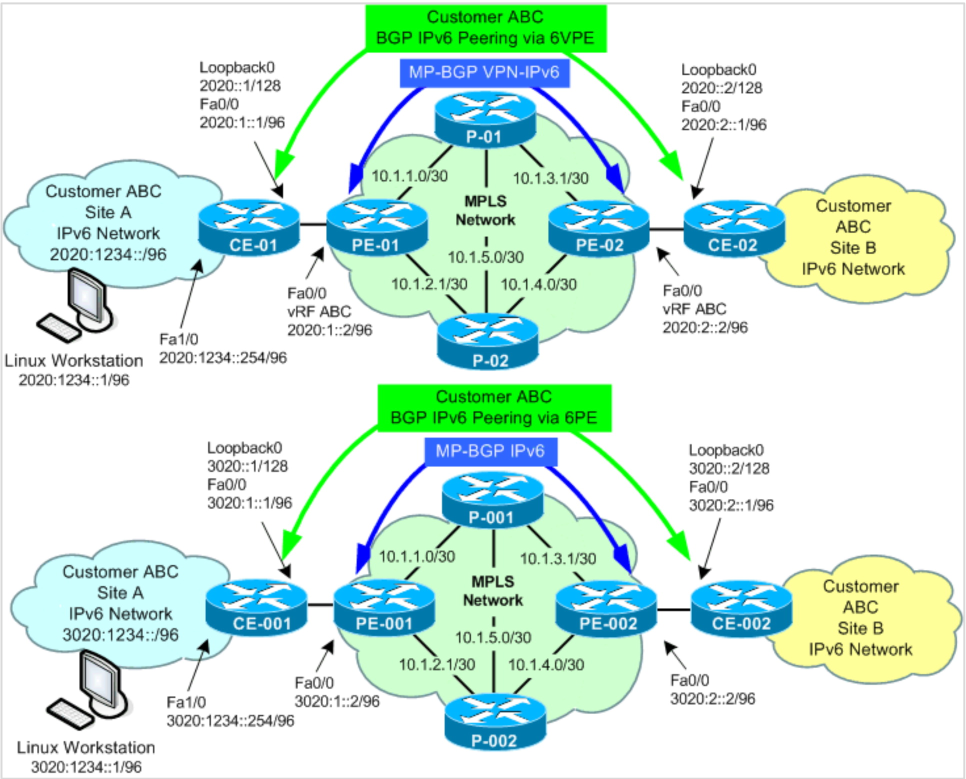


Figure 5. Network Simulation Diagram

Table 2. IPv4 and IPv6 Address Assignment for 6VPE Simulation Network

Router	Interface	IPv4 Address	IPv6 Address	Function
PE-01	FastEthernet0/0		2020:1::2/96	Connection to Customer CE-01
	FastEthernet1/0	10.1.1.1/30		Connection to Service Provider P-01
	FastEthernet1/1	10.1.2.1/30		Connection to Service Provider P-02
	Loopback0	1.1.1.1/32		MP-BGP Peering Interface to PE-02
P-01	FastEthernet0/0	10.1.5.1/30		Connection to Service Provider P-02
	FastEthernet1/0	10.1.1.2/30		Connection to Service Provider PE-01
	FastEthernet1/1	10.1.3.2/30		Connection to Service Provider PE-02
P-02	FastEthernet0/0	10.1.5.2/30		Connection to Service Provider P-01
	FastEthernet1/0	10.1.4.2/30		Connection to Service Provider PE-02
	FastEthernet1/1	10.1.2.2/30		Connection to Service Provider PE-01
PE-02	FastEthernet0/0		2020:2::2/96	Connection to Customer CE-02
	FastEthernet1/0	10.1.4.1/30		Connection to Service Provider P-02
	FastEthernet1/1	10.1.3.1/30		Connection to Service Provider P-01
	Loopback0	4.4.4.4/30		MP-BGP Peering Interface to PE-01
CE-01	FastEthernet0/0		2020:1::1/96	Connection to Service Provider PE-01
	Loopback0		2020::1/128	BGP IPv6 Peering Interface to CE-02
	FastEthernet1/0		2020:1234::254/96	LAN IPv6 Address
CE-02	FastEthernet0/0		2020:2::1/96	Connection to Service Provider PE-02
	Loopback0		2020::2/128	BGP IPv6 Peering Interface to CE-01
Linux Workstation	Eth0		2020:1234::1/96	Connection to IPv6 LAN

Table 3. IPv4 and IPv6 Address Assignment for 6PE Simulation Network

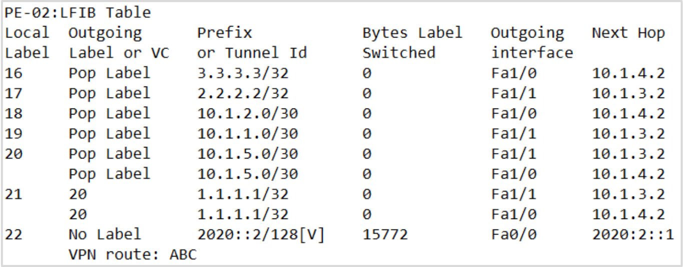
Router	Interface	IPv4 Address	IPv6 Address	Function
PE-001	FastEthernet0/0		3020:1::2/96	Connection to Customer CE-001
	FastEthernet1/0	10.1.1.1/30		Connection to Service Provider P-001
	FastEthernet1/1	10.1.2.1/30		Connection to Service Provider P-002
	Loopback0	1.1.1.1/32		MP-BGP Peering Interface to PE-002
P-001	FastEthernet0/0	10.1.5.1/30		Connection to Service Provider P-002
	FastEthernet1/0	10.1.1.2/30		Connection to Service Provider PE-001
	FastEthernet1/1	10.1.3.2/30		Connection to Service Provider PE-002
P-002	FastEthernet0/0	10.1.5.2/30		Connection to Service Provider P-001
	FastEthernet1/0	10.1.4.2/30		Connection to Service Provider PE-002
	FastEthernet1/1	10.1.2.2/30		Connection to Service Provider PE-001
PE-002	FastEthernet0/0		3020:2::2/96	Connection to Customer CE-002
	FastEthernet1/0	10.1.4.1/30		Connection to Service Provider P-002
	FastEthernet1/1	10.1.3.1/30		Connection to Service Provider P-001
	Loopback0	4.4.4.4/30		MP-BGP Peering Interface to PE-001
CE-001	FastEthernet0/0		3020:1::1/96	Connection to Service Provider PE-001
	Loopback0		3020::1/128	BGP IPv6 Peering Interface to CE-002
	FastEthernet1/0		3020:1234::254/96	LAN IPv6 Address
CE-002	FastEthernet0/0		3020:2::1/96	Connection to Service Provider PE-002
	Loopback0		3020::2/128	BGP IPv6 Peering Interface to CE-001
Linux Workstation	Eth0		3020:1234::1/96	Connection to IPv6 LAN

Table 4. 6VPE Parameters for Simulation Network

Router	Interface	VRF Name	RD	RT	Label Protocol	Function
PE-01	FastEthernet0/0	ABC	6500:100	6500:100		Connection to Customer CE-01
	FastEthernet1/0				LDP	Connection to P-01
	FastEthernet1/1				LDP	Connection to P-02
P-01	FastEthernet0/0				LDP	Connection to P-02
	FastEthernet1/0				LDP	Connection to PE-01
	FastEthernet1/1				LDP	Connection to PE-02
P-02	FastEthernet0/0				LDP	Connection to P-01
	FastEthernet1/0				LDP	Connection to PE-02
	FastEthernet1/1				LDP	Connection to PE-01
PE-02	FastEthernet0/0	ABC	6500:100	6500:100		Connection to Customer CE-02
	FastEthernet1/0				LDP	Connection to P-02
	FastEthernet1/1				LDP	Connection to P-01

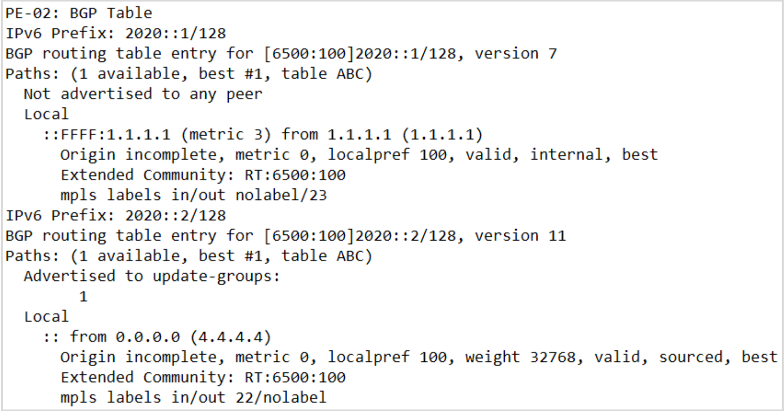
Table 5. 6PE Parameters for Simulation Network

Router	Interface	Label Protocol	Function
PE-001	FastEthernet1/0	LDP	Connection to P-001
	FastEthernet1/1	LDP	Connection to P-002
P-001	FastEthernet0/0	LDP	Connection to P-002
	FastEthernet1/0	LDP	Connection to PE-001
	FastEthernet1/1	LDP	Connection to PE-002
P-002	FastEthernet0/0	LDP	Connection to P-001
	FastEthernet1/0	LDP	Connection to PE-002
	FastEthernet1/1	LDP	Connection to PE-001
PE-02	FastEthernet1/0	LDP	Connection to P-002
	FastEthernet1/1	LDP	Connection to P-001



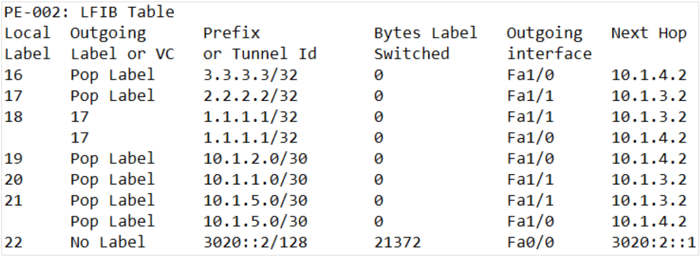
```
PE-02:LFIB Table
Local  Outgoing    Prefix           Bytes Label  Outgoing   Next Hop
Label  Label or VC or Tunnel Id     Switched     interface
16     Pop Label   3.3.3.3/32       0            Fa1/0      10.1.4.2
17     Pop Label   2.2.2.2/32       0            Fa1/1      10.1.3.2
18     Pop Label   10.1.2.0/30      0            Fa1/0      10.1.4.2
19     Pop Label   10.1.1.0/30      0            Fa1/1      10.1.3.2
20     Pop Label   10.1.5.0/30      0            Fa1/1      10.1.3.2
       Pop Label   10.1.5.0/30      0            Fa1/0      10.1.4.2
21     20          1.1.1.1/32       0            Fa1/1      10.1.3.2
       20          1.1.1.1/32       0            Fa1/0      10.1.4.2
22     No Label    2020::2/128[V]   15772        Fa0/0      2020:2::1
       VPN route: ABC
```

Figure 6. Labels information LFIB Table of PE-02 that running 6VPE configuration



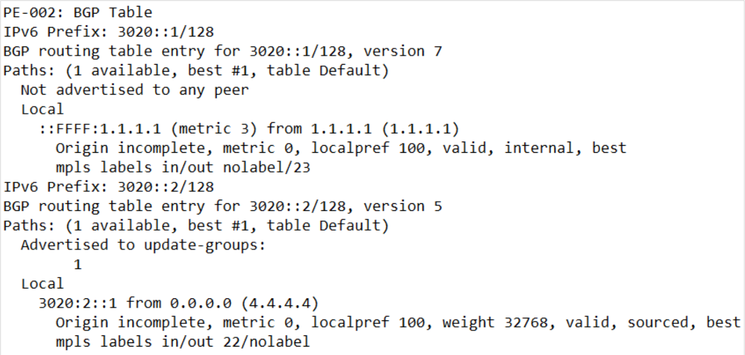
```
PE-02: BGP Table
IPv6 Prefix: 2020::1/128
BGP routing table entry for [6500:100]2020::1/128, version 7
Paths: (1 available, best #1, table ABC)
  Not advertised to any peer
  Local
    ::FFFF:1.1.1.1 (metric 3) from 1.1.1.1 (1.1.1.1)
      Origin incomplete, metric 0, localpref 100, valid, internal, best
      Extended Community: RT:6500:100
      mpls labels in/out nolabel/23
IPv6 Prefix: 2020::2/128
BGP routing table entry for [6500:100]2020::2/128, version 11
Paths: (1 available, best #1, table ABC)
  Advertised to update-groups:
        1
  Local
    :: from 0.0.0.0 (4.4.4.4)
      Origin incomplete, metric 0, localpref 100, weight 32768, valid, sourced, best
      Extended Community: RT:6500:100
      mpls labels in/out 22/nolabel
```

Figure 7. Customer BGP IPv6 Prefix on BGP Routing Table of PE-02 that running 6VPE configuration



```
PE-002: LFIB Table
Local  Outgoing    Prefix           Bytes Label  Outgoing   Next Hop
Label  Label or VC or Tunnel Id     Switched     interface
16     Pop Label   3.3.3.3/32       0            Fa1/0      10.1.4.2
17     Pop Label   2.2.2.2/32       0            Fa1/1      10.1.3.2
18     17          1.1.1.1/32       0            Fa1/1      10.1.3.2
       17          1.1.1.1/32       0            Fa1/0      10.1.4.2
19     Pop Label   10.1.2.0/30      0            Fa1/0      10.1.4.2
20     Pop Label   10.1.1.0/30      0            Fa1/1      10.1.3.2
21     Pop Label   10.1.5.0/30      0            Fa1/1      10.1.3.2
       Pop Label   10.1.5.0/30      0            Fa1/0      10.1.4.2
22     No Label    3020::2/128      21372        Fa0/0      3020:2::1
```

Figure 8. Labels information on LFIB Table of PE-02 that running 6PE configuration



```
PE-002: BGP Table
IPv6 Prefix: 3020::1/128
BGP routing table entry for 3020::1/128, version 7
Paths: (1 available, best #1, table Default)
  Not advertised to any peer
  Local
    ::FFFF:1.1.1.1 (metric 3) from 1.1.1.1 (1.1.1.1)
      Origin incomplete, metric 0, localpref 100, valid, internal, best
      mpls labels in/out nolabel/23
IPv6 Prefix: 3020::2/128
BGP routing table entry for 3020::2/128, version 5
Paths: (1 available, best #1, table Default)
  Advertised to update-groups:
        1
  Local
    3020:2::1 from 0.0.0.0 (4.4.4.4)
      Origin incomplete, metric 0, localpref 100, weight 32768, valid, sourced, best
      mpls labels in/out 22/nolabel
```

Figure 9. BGP Routing Table of PE-02 that running 6PE configuration

To ensure the fairness of the tests and the consistency of the results, we conducted 5000 tests for both connection methods (6VPE and 6PE) simultaneously (started at the same time). Each test is conducted by establishing a BGP IPv6 connection between the CE routers and deactivate the BGP peering and activate the peering again. We measure the BGP peering establishment time started from BGP_Idle state when the CE router sends TCP SYN packet to TCP port 179 and the remote peer router reply with the TCP SYN-ACK packet until both routers reach the BGP_Established state that marked with the first KEEPALIVE and UPDATE messages are sent by both routers. To measure the BGP peering establishment time, the following is the formula that we are used:

$$be = tx - ty \quad (1)$$

Where *be* is BGP peering establishment time, *tx* is the time when the TCP SYN packet sent by the BGP router and responded with the TCP ACK packet by the remote peer router, and *ty* is the time when the second UPDATE message sent by the BGP router. We did the measurement from the Wireshark capture file from each test.

To test the consistency of the BGP peering establishment measurement results, we did the following additional tests:

- Telnet IPv6 TCP connection completion time.
- SSH IPv6 TCP connection completion time.
- HTTP IPv6 TCP connection completion time.
- HTTPS IPv6 TCP connection completion time.
- ICMPv6 echo-reply time.

On Telnet, SSH, HTTP, and HTTPS IPv6 TCP connection completion time test, we measure every TCP connection (three-way handshake) completion time between the Linux workstation and either CE-02 or CE-002 on the 6PE and 6VPE method. Following is the formula for the TCP connection completion time measurement:

$$tcpt = ack - syn \quad (2)$$

Where *tcpt* is TCP connection completion time, *syn* is the time of the TCP SYN packet that sent by Linux workstation to either CE-02 or CE-002, and *ack* is the time of the TCP ACK packet that sent by Linux workstation as a response of TCP SYN-ACK packet that sent by either CE-02 or CE-002.

For ICMPv6 echo-reply time tests, we have completed the tests by sending 35,000 ICMPv6 echo packet from the Linux workstation to CE-02 over both method. Following is the formula for ICMPv6 echo-reply time measurement:

$$icmpt = ires - ireq \quad (3)$$

Where icmpt is ICMPv6 echo-reply time, ireq is the time when the ICMPv6 echo-request sent from the Linux workstation to either CE-02 or CE-002, and ires is the time when the ICMPv6 echo-reply sent by either CE-02 or CE-002 as a response packet.

5.1 Simulation Results of BGP Peering Establishment

Based on the 5000 test that we have completed on the simulation, the average BGP peering establishment time for 6VPE connection is 624 ms, and for 6PE connection is 632 ms. The comparison graph of every test result on 6VPE and 6PE shown in figure 10.

5.2 Simulation Results of Telnet TCP Connection

For Telnet TCP connection completion time tests, based on the 5000 tests that we have conducted on the simulation, the average of Telnet TCP connection completion time on 6VPE connection is 710 ms and 715 ms on 6PE connection. The comparison diagram of every test result on 6VPE and 6PE shown in figure 11.

5.3 Simulation Results of SSH TCP Connection

For SSH IPv6 TCP connection completion time, based on the 5000 test that we have conducted on the simulation, the average of SSH IPv6 TCP connection completion time on 6VPE connection is 662 ms and 669 ms on 6PE connection. The comparison diagram of every test result on 6VPE and 6PE shown in figure 12.

5.4 Simulation Results of HTTP TCP Connection

For HTTP IPv6 TCP connection completion time, based on the 5000 test that we have conducted on the simulation, the average of HTTP IPv6 TCP connection completion time on 6VPE connection is 714 ms and 718 ms on 6PE connection. The comparison diagram of every test result on 6VPE and 6PE shown in figure 13.

5.5 Simulation Results of HTTPS TCP Connection

For HTTPS IPv6 TCP connection completion time on 6VPE and 6PE connection method, based on the 5000 test that we have conducted on the simulation, the average of HTTPS IPv6 TCP connection completion time on 6VPE connection is 692 ms and 693 ms on 6PE connection. The comparison diagram of every test result on 6VPE and 6PE shown in figure 14.

5.6 Simulation Results of ICMPv6 Echo-Reply Time

On ICMPv6 echo-reply time measurement, we conducted 35,000 tests. We got the result that the average time between an ICMPv6 echo-reply packet that sent by CE-02/CE-002 to Linux workstation and an ICMPv6 echo-request on 6VPE connection is 254 ms and 256 ms on 6PE connection. The comparison diagram of every test result on 6VPE and 6PE shown in figure 15.

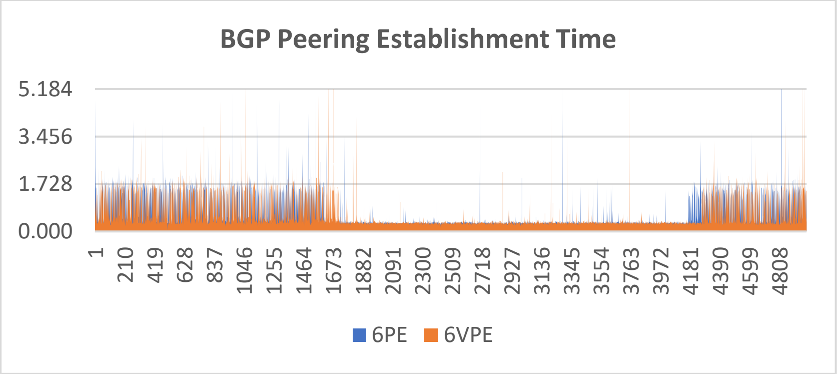


Figure 10. Comparison graph of simulation results of BGP IPv6 peering establishment time on 6VPE and 6PE

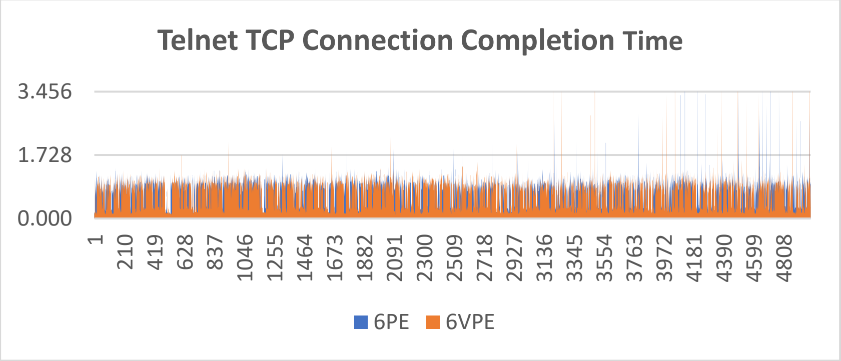


Figure 11. Comparison graph of simulation results of Telnet TCP connection completion time on 6VPE and 6PE

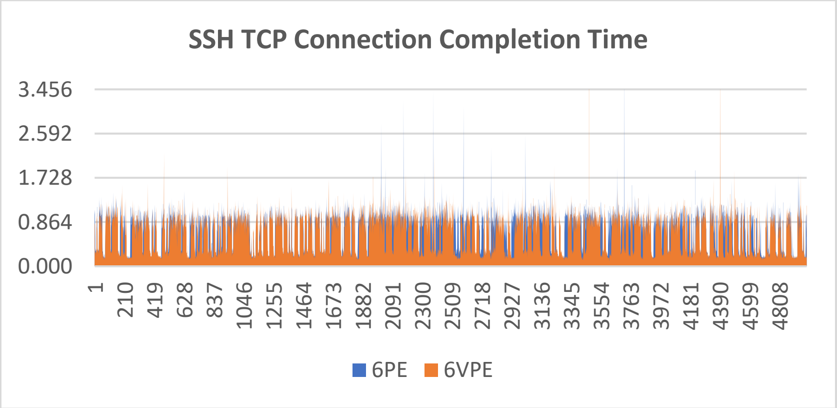


Figure 12. Comparison graph of simulation results of SSH TCP connection completion time on 6VPE and 6PE

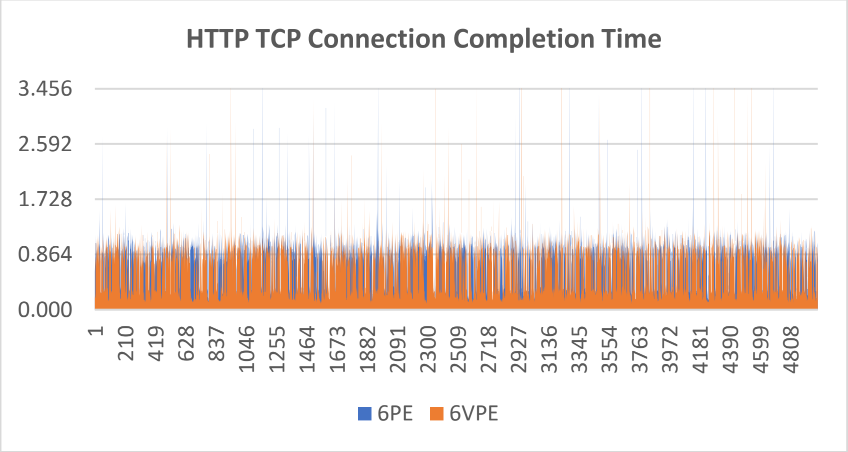


Figure 13. Comparison graph of simulation results of HTTP TCP connection completion time on 6VPE and 6PE

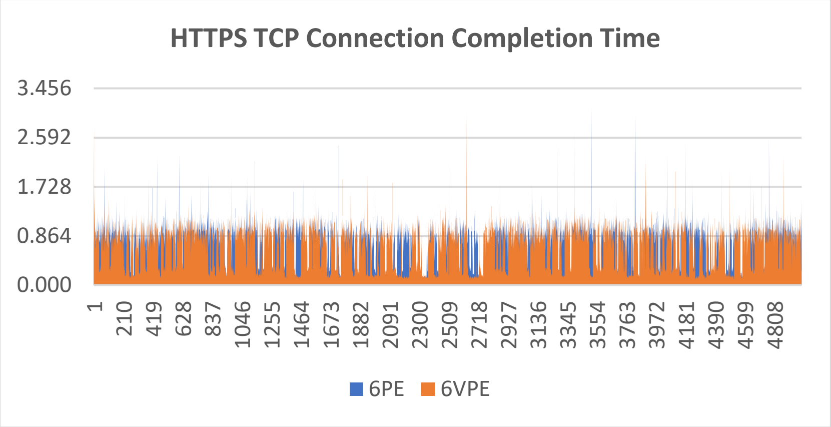


Figure 14. Comparison graph of the testing results of the HTTPS TCP connection completion time on 6VPE and 6PE

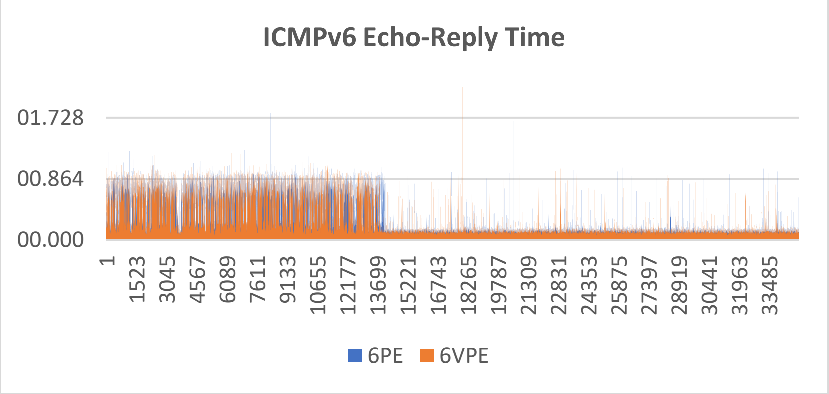


Figure 15. Comparison graph of simulation results of ICMPv6 Echo-Reply on 6VPE and 6PE

Table and graph of the comparison of simulation test results from six types of tests that are BGP IPv6 peering establishment time and five additional tests over 6PE and 6VPE connection are shown in table 6 and figure 16 (time is in millisecond).

Table 6. Comparison of Simulation Test Results

Test	6PE	6VPE	
	Time (ms)	**Time (ms)**	**% Faster than 6PE**
BGP4 IPv6 Peering Establishment	632	624	1.27%
SSH IPv6 TCP Connection	669	662	1.05%
HTTPS IPv6 TCP Connection	693	692	0.14%
HTTP IPv6 TCP Connection	718	714	0.56%
Telnet IPv6 TCP Connection	715	710	0.70%
ICMPv6 Echo-Reply Time	256	254	0.78%

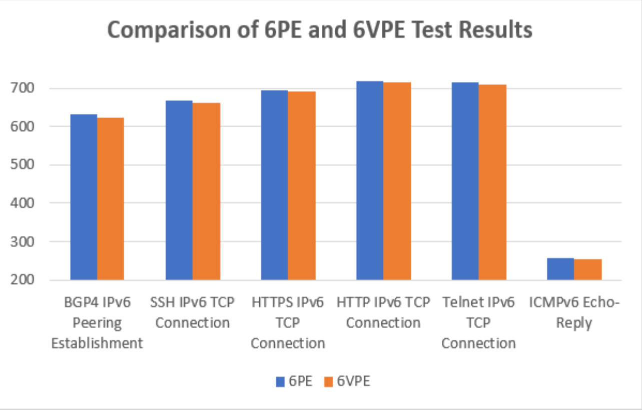


Figure 16. Comparison graph of the Test Results

6. Conclusions

We have simulated an enterprise BGP4 IPv6 peering establishment over 6PE and 6VPE connection provided by the MPLS Service Provider. We conducted 5,000 tests and measures the BGP4 IPv6 peering establishment time over both connection methods. To ensure the equality and fairness of the testing and the consistency of the test result on both connection, we did the 5,000 tests simultaneously (started at the same time). To provide comparison data for the BGP4 IPv6 peering establishment tests, we conducted 5,000 tests and measured TCP connection completion time for Telnet, SSH, HTTP, and HTTPS IPv6. We also conducted 35,000 tests for ICMPv6 echo-reply time on both methods of connection (6VPE and 6PE).

Based on the comparison table of the simulation results in table 6, we can see that all six types of tests that ran over 6VPE are consistently faster than over 6PE connection. We conclude that IPv6 traffic over 6VPE connection has lower latency than over 6PE connection.

As described earlier, on the 6VPE method, the PE router put customer IPv6 prefixes on its dedicated VRF (VPN Routing and Forwarding table), so the customer routing table separated from other customers. There are several benefits to this method, which are:

- The 6VPE connection method gives additional security to the customer. Every customer has a dedicated routing table, so every customer network is guaranteed cannot be accessed by other customers, unless there is a policy applied. In 6PE, MPLS Service Provider can prevent an IPv6 customer network accessed by other customers by deployed a BGP Policy, while in the 6VPE connection, this policy not required.

- The 6VPE connection method gives flexibility. Every customer can use overlapped IPv6 addresses/prefixes. This thing can happen because every customer has a dedicated VRF (VPN routing and forwarding table). Even depend on the requirement, a customer can have more than one VPN and VRF as well.

With the above benefits and lower latency than the 6PE connection method, we can conclude that the 6VPE connection method is the better solution for the MPLS Service Providers to transport their customer IPv6 traffic.

References

[1] Y. Rekhter, B. Moskowitz, D. Karrenberg, G. J. de Groot, and E. Lear, “RFC 1918: Address Allocation for Private Internets, https://tools.ietf.org/html/rfc1918,” Internet Engineering Task Force (IETF), 1996.

[2] K. Egevang and P. Francis, “RFC 1631: The IP Network Address Translator (NAT), https://tools.ietf.org/html/rfc1631,” Internet Engineering Task Force (IETF), 1994.

[3] L. Vegoda, “IPv6 – Successor to IPv4 Confronting Transition, https://www.iana.org/about/presentations/20110707-vegoda-ipv6.pdf,” Internet Assigned Numbers Authority, 2011.

[4] S. Deering and R. Hinden, “RFC 2460: Internet Protocol, Version 6 (IPv6) Specification, https://tools.ietf.org/html/rfc2460,” Internet Engineering Task Force (IETF), 1998.

[5] L. Mengyang, D. Yunna, and Z. Chunfei, “A WMPLS Based Multicast Mechanism in Mobile Ad hoc Network,” International Journal of Computer Network and Information Security, Vol. 3, No. 1, pp. 40-46, 2011.

[6] Cisco Systems, “Any Transport Over MPLS Data Sheet, https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/any-transport-over-multiprotocol-label-switching-atom/prod_white_paper09186a00800a8442.html,” Cisco Systems, 2008.

[7] J. De Clercq, D. Ooms, M. Carugi, and F. Le Faucheur, “RFC 4659: BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN, https://tools.ietf.org/html/rfc4659,” Internet Engineering Task Force (IETF), 2006.

[8] J. De Clercq, D. Ooms, S. Prevost, and F. Le Faucheur, “Connecting IPv6 Islands over IPv4 MPLS Using IPv6 Provider Edge Routers (6PE), https://tools.ietf.org/html/rfc4798,” Internet Engineering Task Force (IETF), 2007.

[9] N, Almrezeq, L. Almadhoor, T. Alrasheed, and A. A. Abd El-Aziz, S. Nashwan, “Design a secure IoT Architecture using Smart Wireless Networks,” International Journal of Communication Networks and Information Security (IJCNIS), Vol. 12, No. 3, pp. 401-410, 2020.

[10] K.S. Aloufi, “6LoWPAN Stack Model Configuration for IoT Streaming Data Transmission over CoAP,” International Journal of Communication Networks and Information Security (IJCNIS), Vol. 11, No. 2, pp. 304-311, 2019.

[11] S-F. Yang and J-S. Wu, “Guard Channel based Call Admission Control Schemes in Hierarchical Mobile IPv6 Networks,” International Journal of Communication Networks and Information Security (IJCNIS), Vo. 2, No. 2, pp. 68-76, 2010.

[12] A. Quintero, F. Sans, and E. Gamess, “Performance Evaluation of IPv4/IPv6 Transition Mechanisms,” International Journal of Computer Network and Information Security, Vol. 8, No. 2, pp. 1-14, 2016.

[13] S. Repas, P. Farnadi, and G. Lencse, “Performance and Stability Analysis of Free NAT64 Implementations with Different Protocols,” Acta Technica Jaurinensis, Vol. 7, No. 4, pp. 404-427, 2014.

[14] P. Grayeli, S. Sarkani, and T. Mazzuchi, “Performance Analysis of IPv6 Transition Mechanisms over MPLS,” International Journal of Communication Networks and Information Security (IJCNIS), Vol. 4, No. 2, pp. 91-103, 2012.

[15] S. Salih, A. Abdalrahman, and K. Elsharif, “Data Security vs. Overall Performance in 6VPE,” International Journal of Computing and Digital Systems (IJCDS), Vol. 7, No. 3, pp. 161-166, 2018.

[16] M. Algabri, S. Alhomdy, G. Alselwi, A. Alowiri, and N. Sharaby, “Performance Analysis of IPv6 Over MPLS & MPLS-VPN for Sana’a University,” International Journal of Innovative Science, Engineering & Technology (IJISET), Vol. 3, No. 5, pp. 165-169, 2016.

[17] A. T. H. Al-Hamadani, and G. Lencse, “Survey on the Performance Analysis of IPv6 Transition Technologies,” Acta Technica Jaurinensis, 2021.

[18] R. Vinodkumar, S. Vijayalakshmi, K. R. Kavitha, and K. Karthick, “Implementation of IPv6 Internet Service with MPLS Networks and MPLSL3VPN Service in IPv6 Networks,” International Journal of Recent Technology and Engineering, Vol. 8, No. 3, pp. 8715-8720, 2019.

[19] A. Hamarsheh, Y. Abdalaziz, and S. Nashwan, “Recent Impediments in Deploying IPv6,” Advances in Science Technology and Engineering Systems Journal, Vol. 6, No. 1, pp. 336-341, 2021.

[20] Q. Le Trung and G. Kotsis, “BGP-GCR+: An IPv6-based routing architecture for MANETs as transit networks of the internet,” International Conference on Mobile Ad-Hoc and Sensor Networks, pp. 337-350, 2005.

[21] S. Zhang, Y. Liu, and D. Pei, “A measurement study on BGP AS path looping (BAPL) behavior,” 2014 23rd International Conference on Computer Communication and Networks (ICCCN), Shanghai, China, 2014.

[22] S. Jia, M. Luckie, B. Huffaker, A. Elmokashfi, E. Aben, K. Claffy, and A. Dhamdhere, “Tracking the Deployment of IPv6: Topology, Routing and Performance,” Computer Networks, Vol. 165, 2019.

[23] S. Deshpande and B. Sikdar, "On the impact of route processing and MRAI timers on BGP convergence times," IEEE Global Telecommunications Conference, 2004. GLOBECOM '04., Dallas, USA, Vol. 2, pp. 1147-1151, 2004.

[24] O. Bonaventure, C. Filsfils and P. Francois, "Achieving Sub-50 Milliseconds Recovery Upon BGP Peering Link Failures," in IEEE/ACM Transactions on Networking, Vol. 15, No. 5, pp. 1123-1135, 2007.

[25] B. Zhang, D. Massey, and L. Zhang, "Destination Reachability and BGP Convergence Time [Border Gateway Routing Protocol]," IEEE Global Telecommunications Conference, 2004. GLOBECOM '04., Dallas, USA, Vol. 3, pp. 1383-1389, 2004.

[26] R. B. da Silva and E. S. Mota, "A Survey on Approaches to Reduce BGP Interdomain Routing Convergence Delay on the Internet," in IEEE Communications Surveys & Tutorials, Vol. 19, No. 4, pp. 2949-2984, 2017.

[27] R. N. Devikar, D. V. Patil, and V. Chandraprakash, “Study of BGP Convergence Time,” International Journal of Electrical and Computer Engineering (IJECE), Vol. 6, No. 1, pp. 413-420, 2016.

[28] B. Wang, “The research of BGP convergence time,” 2011 6th IEEE Joint International Information Technology and Artificial Intelligence Conference, Chongqing, China, pp. 354 – 357, 2011.

[29] S. Katsuno, K. Yamazaki, T. Asami, and H. Esaki, “Performance evaluation of L2 over MPLS,” Systems and Computers in Japan, Vol. 38, No. 5, pp. 59-68, 2007.

[30] S. N. Shirazi, M. Asim, M. Irfan, and N. Ikram, “MPLS unleashed: Remedy using IPSEC over MPLS VPN,” International Conference on Information Security and Assurance, pp. 241-248, 2010.

[31] B. Alawieh and H. Mouftah, “Delivering Multicast Services over MPLS Infrastructure,” 2007 12th IEEE Symposium on

Computers and Communications, Santiago, Portugal, pp. 509 – 513, 2007.

[32] A. Al Mamun, T. R. Sheltami, H. Ali, and S. Anwar, “Performance Evaluation of Routing Protocols for Video Conference over MPLS VPN Network,”. Journal of Ubiquitous Systems & Pervasive Networks, Vol. 7, No. 1, pp. 01-06, 2016.

[33] Y. Rekhter, T. Li, and S. Hares, “RFC 4271: A Border Gateway Protocol 4 (BGP-4), https://tools.ietf.org/html/rfc4271,” Internet Engineering Task Force (IETF), 2006.

[34] Cisco Systems, “IP Routing: BGP Configuration Guide, https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_bgp/configuration/xe-16/irg-xe-16-book/configuring-a-basic-bgp-network.html,” Cisco Systems, 2019.

[35] J. Doyle and J. D. Carroll, “Routing TCP/IP, Volume II: CCIE Professional Development, Second Edition,” Cisco Press, Indianapolis, USA, 2016.

[36] V. Jain and B. Edgeworth, “Troubleshooting BGP: A Practical Guide to Understanding and Troubleshooting BGP,” Cisco Press, Indianapolis, USA, 2016.