# A Simulation Analysis of Latency and Packet Loss on Virtual Private Network through Multi Virtual Routing and Forwarding

Rissal Efendi
STMIK PROVISI
Semarang, Indonesia

## ABSTRACT

MPLS is a network management system used to manage and monitor VPN services on the Service Provider (SP). MPLS VPN enables SP to provide intranet and extranet VPN services. MPLS VPN is a solution to keep the SP fixed network scalability, because SP can design, specify, and manage all VPN services on the terms of the contract that has been agreed with each customer. VRF is a major element of the MPLS VPN technology. VRF only are the PE routers only. VRF routing table are independent on the PE router. VRF contains routes available to reach the network sites that exist across the property of their respective VPN. This papers research the latency and the packet loss in network combining VPN MPLS and VRF.

## Keywords

Virtual Private Network, Multi Protocol Layer Switch, Virtual Routing and Forwarding.

## 1. INTRODUCTION

VPN (Virtual Private Network) is a technology to connect two or more local networks of different locations across the public network (the Internet) is encrypted. Therefore many SP (Service Provider) to provide VPN services to meet the needs of its customers, to connect the local network from the center with branches in some areas while in the SP range, so customers do not need to build an independent infrastructure to connect centers with a branch network, simply by subscribing to a VPN service on the selected SP. VPN technology continues to evolve to provide benefits to the SP and the customer. The technology that is now being implemented by the SP is Layer 3 MPLS VPN, the VPN service delivery across MPLS networks owned by SP. Layer 3 MPLS VPN SP makes it easy to develop its network, because if the customer increases, configuration and setup is done on the physical connection between the customer's enterprise network with the device in front of him and will not affect other customers. Then, when viewed from a business standpoint SP, Layer 3 MPLS VPN technology also provides an advantage because SP is possible to make every customers different virtual paths, and can serve a lot of customers in virtually all PE routers (Provider Edge), so no need to buy a router to PE serve one customer. Virtual Services was created by Cisco as the Multi-VRF (Virtual Routing Forwarding) is a service or feature on a Cisco router to make a VPN routing in Layer 3 MPLS VPN network. And able to perform Overlapping IP address that allows two different VPN interconnected despite having the exact same IP address so it will not conflict SP IP address on the network. Moreover it can be made virtual routing table at router PE (Provider Edge). Where the router belongs to SP that deal directly with the customer's routers have multiple routing tables that serve to direct the VPN each other despite having the same IP address on the gateway side of a client.

## 2. Virtual Private Network (VPN)

VPN (Virtual Private Network) is a logical connection that connects two points via the public network. Logical connection can be a layer 2 or layer 3 in the OSI Layer base. Likewise with VPN technology can be classified on the Layer 2 VPN or Layer 3 VPN. In concept, both Layer 2 VPN or Layer 3 VPN is the same, each adding "delivery header" in the data packets towards the destination address. For Layer 2 VPN, delivery is in Layer 2 header. As for the Layer 3, delivery is on the Layer 3 header. ATM and Frame Relay is an example of a Layer 2 VPN. GRE, L2TP, MPLS and IPSec are examples of Layer 3 VPN. Now many kinds of modern services-based VPN IP address of the VPN replaces traditional ATM or Frame Relay offered by the SP [1]. Starting from the "do-it-yourself IPSec-over-internet" that offer MPLS VPNs, pseudo wire (VPWS) to VPLS services. Details of the implementation of these services and the protocol used (MPLS, AToM, L2TPv3, etc.) It must be considered by the designers of the network. It is important to understand the key concepts of the network needed to be made, the interaction between the routers and switches on the network, the impact of what would happen to the company, whether the network is reliable and always available services [2].

There are three main categories of VPN services (Figure 1):

- Layer-2 VPN services, where data transport ¬ SP offers end-to-end Layer-2 customers proprietary network. L2VPN classic Services (Frame Relay and ATM) has been replaced with point-to-point (VPWS) or multipoint (VPLS)-based Ethernet.
- Layer-3 VPN services, where the SP took over responsibility for routing IP core enterprise network.
- Remote Access VPN service, where SP concentrates on communication access remote devices (e.g. mobile phone connection) to get sent to a concentration point on the tip of the enterprise network.

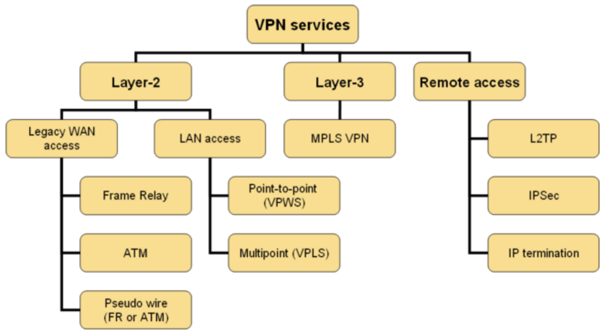

**Fig 1: Type of VPN Services**

## 3. Multiprotocol Label Switching (MPLS)

MPLS (Multi Protocol Label Switching) technology is the delivery of packets on a high-speed backbone network that incorporates some of the advantages of circuit-switched communication systems and packet-switched so as to produce a better performance than the normal IP routing. Routing protocol is in the network layer in the OSI Layer, while MPLS is between the second and third layer, so MPLS is often said to be in Layer 2.5 for MPLS combines switching techniques in routing at layer two to layer three [3].

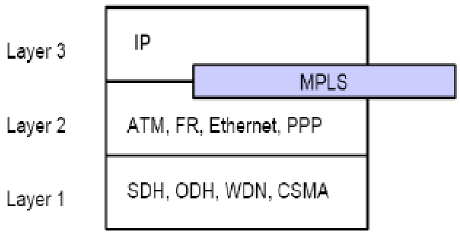

**Fig 2: Location of MPLS in OSI Layer**

MPLS consists of four major components, such as Label Edge Router (LER), Label Switched Router (LSR), MPLS Labels and Label Distribution Protocol (LDP). Figure 3 gives an illustration of these important components.

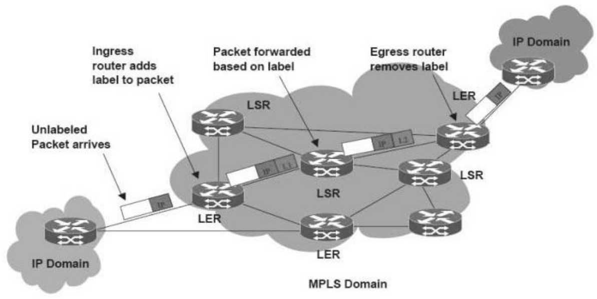
Ingress router adds label to packet
Packet forwarded based on label
Egress router removes label
IP Domain
LER
LSR
Unlabeled Packet arrives
LSR
LSR
LER
LER
IP Domain
MPLS Domain

**Fig 3: Components of MPLS**

### 3.1 Label Edge Router (LER)

Routers placed on the border of the MPLS network. Routers is assigned MPLS label on each packet of data to be transmitted through Switched Label Router (LSR). There are two types of LER, namely [4]:

- Ingress Router is a router (LER), which regulates data traffic when going into the MPLS domain.

- Egress Router is a router (LER), which regulates the data traffic as it leaves the MPLS domain.

### 3.2 Label Switched Router (LSR)

Routers in the MPLS network are assigned to forward (forwarding) data packets based on the label that has been inserted by the LER on the package. LSR is divided into two types, such as:

- Upstream LSR is the sender of data.

- Downstream LSR is the recipient of the data LSR tasked to perform the following tasks:

  - Aggregate, removes the label and do the processing network layer
  - Pop, remove the label and transmit the payload.
  - Push, which transmits the label by providing a set of new labels
  - Swap replace the label with a new label value
  - Un-Tag, which remove the label and forwards the packet to the destination hop.

### 3.3 Label

A label is attached to a particular value by LER to each data packet enters the MPLS network. MPLS labels are used for identification at the local switching MPLS network. These labels carry additional information that is useful in the process of switching, but does not contain the information the network layer protocol in the packet. For each point-to-point connection LSR interface, label value must be unique, but for a different value of LSR interface.

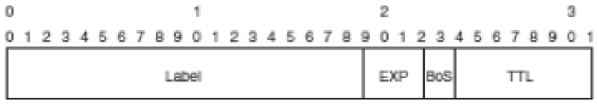

**Fig 4 : MPLS Labels**

MPLS label consists of four parts as shown in Fig. 4, the following explanation:

- 20-bit "Label" is the main bits of the MPLS label that contains a unique value in each local and LSR

- Subsequent 3-bit field called experimental (EXP), which is a field that is used to provide class of service (CoS)

- 1-bit bottom of stack indicator (BOS), served to indicate whether this is the last label in the header of a packet or not because MPLS allows the attachment of multiple labels simultaneously in the header of a data packet. A value of "1" is given as a sign of the last data packet.

- 8-bit Time to Live (TTL) which acts as the TTL in the IP header to be passed down in value every hop.

## 4. MPLS VPN

MPLS is a network management system used to manage and monitor VPN services on the Service Provider (SP). MPLS VPN enables SP to provide intranet and extranet VPN services. MPLS VPN is a solution weeks to keep the SP fixed network scalability, because SP can design, specify, and manage all VPN services on the terms of the contract that has been agreed with each customer. Advantages that can be gained by implementing Cisco MPLS VPN is a simplification of the provision of services (simplified provisioning). Underwriting services (service assurance), and ease the process of calculating the bill (billing processes), so the cost in the development and operation of the VPN can be reduced. MPLS VPN focuses on the link between the Provider's Edge router (PE) and Customer's Edge router (CE). CE router is connected directly to the PE router so that the encapsulated data traffic to be sent to the CE routers others. CE router VPN routes notify to all devices on the network are connected to the customer's order. MPLS VPN consists of several sites that are interconnected with MPLS provider core network [5]. At each site there are one or more CE routers that are connected to one or multiple PE routers. PE routers use the Border Gateway Protocol-Multiprotocol (MP-BGP) to dynamically communicate between PE routers. All IP addresses used in the VPN network must be exclusive and different IP addresses owned by the core network owned by SP. Each CE router must be able to send data packets to the PE router directly opposite. Therefore, the IP addresses that exist on the PE routers may not have the same IP address the customer's VPN.

## 4.1 Forms of Customer and Provider Networks

Seen from the point of view of the customer (customer), all internal routers they seem to communicate directly with the CE routers from one site to another site through a VPN that is set by the Service Provider (SP) as shown in Figure 5

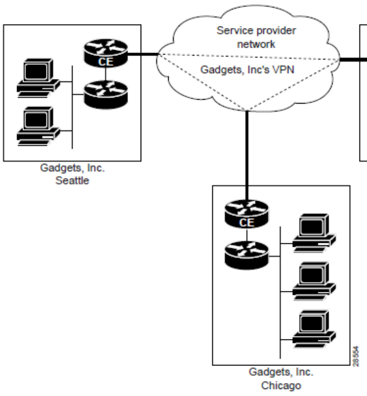

**Fig 5: The Network View of customer**

The view shows a simple computer network from the customer side is an advantage of the technology to implement VPN. The customers can communicate directly with all the sites that they have a private or local though in reality through public network infrastructure that also boarded by other customers.

While the shape of the SP network is different, as Figure 6 illustrates the two different customers, where each customer has one or more VPNs.

At the end of the SP network placed Provider Edge Routers (PES). In the SP network was also installed in addition to PE routers is required (usually called a P router) is responsible for managing communications PE routers using MP-protocol BGP (Border Gateway Protocol-Multiprotocol). Can be seen in the above network model, the SP only provide service between the PE routers the CE routers. PE routers must be able to run several different routing tables are named with a VPN Routing and Forwarding Tables (VRFs). VRF contains routes which should be passed to lead directly to site VPN. PE routers exchange VPN-IPv4 update through MP-iBGP sessions. More updates contains addresses and VPN-IPv4 labels. PE routers determine where to route data packets must first traverse the SP. IP address of the PE routers is called the host routes that lead to the Core Interior Gateway Protocol.

The advantages of implementing MPLS-VPN include:

- Capable of speeds present in the network that are needed in the IP address-based services, including the speed of data exchange intranets, extranets, voice, multimedia, and network commerce.
- Privacy and security equal to Layer-2 VPN to tighten the distribution of VPN routes, meaning only certain routers that are part of a VPN [3].
- A seamless connection to the customer's intranet
- Scalability of the network is very high, even capable of handling thousands of sites and hundreds of thousands of VPN
- VPN management easy and fast to create a new VPN
- High Scalability to support connection-any-to-any, so the network intranets and extranets can be extended.

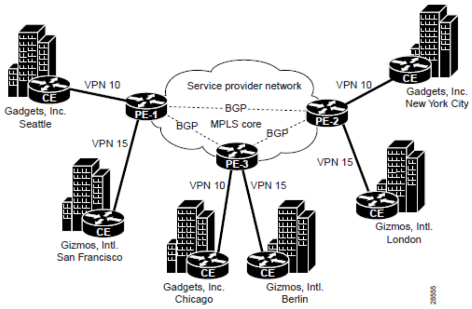

**Fig 6: The Network View of Service Provider**

## 4.2 Character MPLS VPN

The character of MPLS VPN technologies are as follows:

- MPLS-based VPN focused on OSI Layer 3 and peer-based model, so it has high scalability, easy to build, and easy-to has managed than conventional VPNs. Moreover, the additional value in applying MPLS VPN is easy to implement various services of data, voice, and multimedia in it, as backbone SP is able to recognize each MPLS VPN as a secure network and a connectionless IP network
- MPLS VPN to separate network traffic using a unique routing table, called Virtual Routing Forwarding Tables (VRFs) to each customer's VPN network so that each user on a VPN cannot see traffic outside VPN network. Separation of network traffic occurs without tunneling or encryption processes, because it is built directly into the network
- MPLS VPNs use Multiprotocol Border Gateway Protocol (MP-BGP) prefix-prefix to encode IPv4 addresses to the customer's VPN-IPv4 NLRI (Network Layer Reachability Information) which has a unique or different from one another. NLRI shows the destination address in MP-BGP, so NLRI can be considered "one routing unit." NLRI prefix derived from tissue that is inserted in the BGP4 routing updates.
- MPLS VPN has Extended MP-BGP community used to manage the distribution of data on customer routers.

- Each route known to the customer's network, interspersed with MPLS label, which was added by the PE router. The label serves to direct packets to the CE router is on the opposite side. Then when a data packet forwarded to the SP network backbone, two labels are used. Label the first duty to send data packets to the PE router across; then label the latter governs how the relevant PE routers transmit data packets.
- Each link between the PE and CE routers using standard IP forwarding. Since each PE router has multiple VPN routing and multiple VRF, each PE router work with any router CE with each forwarding table that contains a set of routes within the scope of the relevant CE router.

## 5. Virtual Routing and Forwarding

VRF is a major element of the MPLS VPN technology. VRF only are the PE routers only. VRF routing table are independent on the PE router. VRF contains routes available to reach the network sites that exist across the property of their respective VPN. A VRF is always associated with the following elements [6]:

- IP routing table
- Derived forwarding table, a technology-based Cisco Express Forwarding (CEF)
- Interface anywhere using the derived forwarding table
- Routing protocols and routing peers that inject information into the VRF

Each PE router can have one or more VRF. So since the beginning of MPLS VPN is programmed to determine a data packet that has a destination address to be sent to the relevant VRF only, not to the other VRF. Because routing on the PE router must be independent or separate between the customer VPN, each VPN must have a routing table of each as in figure 7 The interface on the PE router that leads to the CE router can only handle one VRF only so that each data packet received in the VRF is not identified as ambiguous, but it is directed by the VRF [7].

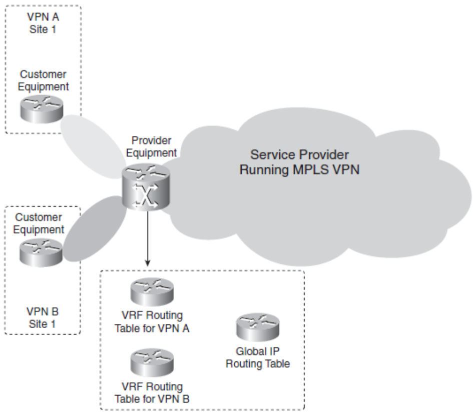

**Fig 7: Illustration of VRF on the PE router**

The main function of the Multi-VRF (Virtual Routing Forwarding) is implementing several independent routing table in a router without disrupting the performance of MPLS VPN. Each VRF and global routing tables has directives and their functions. Application of VRF on the enterprise network, the global routing table can be used to support the functioning of the regular network paths and create VPN networks that are riding to run concurrently.

## 6. System Performance

Cisco Multi-VRF is a technology or features available in Cisco network MPLS Layer 3 VPN that separate routing tables or routing information per customer, so that each customer has their own path and separate from other customer lines. Because each customer's VPN should have its own track, then the router PE (Provider Edge) VRF table must have as many subscribers. In this study, PE1 and PE2 are configured to deliver (forwarding) packets for each customer, which vpnTI and vpnDKV. How to work on the network VRF SP (Service Provider) can be seen in Figure 8.

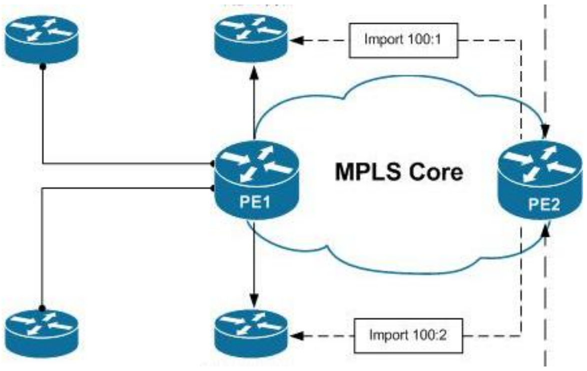

**Fig 8: Layer 3 MPLS VPN Topology Design**

### 6.1 Route Distinguisher

Prefix-prefix VPN across the MPLS VPN network using Multiprotocol Core delivered BGP (MP-BGP). When the MP-BGP prefix source IPv4 in the network Service Provider (SP) is required concepts Route distinguisher (RD), which serves to mark each customer and make every customer a unique prefix by adding the value of RD. Because every customer is different prefix after being given the RD, the IP addresses overlap can be done without an interruption in the SP network. For example, the results of the prefix 192.168.10.1/24 vpnDKV already owned the inserted RD 100:1 is 100:1:192.168.10.1 / 24. IPv4 prefix was inserted called the RD vpnv4 prefix. When vpnTI and vpnDKV have the same IP address in the local network and sends them into the IPv4 prefix SP network will not be a problem. Because after a prefix-IPv4 prefix PE1 enters the RD inserted into vpnv4 prefix corresponding topology. As evidence, vpnv4 prefix is owned vpnDKV 100:1:192.168.10.1 / 24 and vpnv4 prefix is owned vpnTI 100:2:192.168.10.1 / 24, so despite having the same IP address, the SP core network still think differently.

### 6.2 Route Target (RT)

RD only serves as a marker vpnv4 prefix, but the Route Target serves to control the data communication between VPN sites to each other. RT is a BGP extended community that directs which path should be used for import (import) and export (export) MP-BGP into the VRF should be. In Figure 8, has a value vpnDKV and vpnTI RT RT Import and Export are different in PE1 router. Export surgery means adding BGP RT extended community into vpnv4 routes sent from the VRF into MP-BGP. RT surgery means VRF Import routes received from MP-BGP vpnv4 then matched to the value of RT or BGP extended community that is in the VRF to be accepted. If the RT values match, the vpnv4 prefix is converted into IPv4 prefix and inserted into the VRF routing table, but if the value of RT does not match with those of VRF, the vpnv4 prefix is discarded (dropped). In Figure 8 indicated that the RT control vpnv4 prefix of each customer towards PE2 PE1 keep separate track so that virtually even through the same physical media.

### 6.3 Packet Forwarding

In this section, explain how IP packet across the MPLS VPN network owned by SP from CE1 go to CE2. Because the SP network using MPLS technology, the LDP (Label Distribution Protocol) must already exist in the PE1, P, and PE2. Value LDP on the router PE1, P, and PE2 can be seen in the source code MPLS forwarding table below.

**Table 1 MPLS forwarding table on PE1**

```
Local  Outgoing    Prefix            Bytes tag  Outgoing   Next Hop
tag    tag or VC   or Tunnel Id      switched   interface
16     Pop tag     192.168.3.0/24    0          Se0/3/0    192.168.2.2
17     Pop tag     192.168.100.2/32  0          Se0/3/0    192.168.2.2
18     17          192.168.100.3/32  0          Se0/3/0    192.168.2.2
19     Aggregate   192.168.1.0/24[V] 10400
20     Untagged    202.147.192.1/32[V]   \
                                     11400      Fa0/1      192.168.1.1
21     Aggregate   192.168.6.0/24[V] 10400
22     Untagged    202.147.192.1/32[V]   \
                                     11400      Fa0/0      192.168.6.1
```

Table 1 is the result of the # show mpls forwarding table on PE1. It shows the value of the label (tag) and treatment (Pop, Aggregate, untagged) provided by MPLS to every packet of data coming out of the next hop PE1 and where the data packets are transmitted.

**Table 2 MPLS forwarding table on P**

```
P#show mpls forwarding-table
Local  Outgoing    Prefix            Bytes tag  Outgoing   Next Hop
tag    tag or VC   or Tunnel Id      switched   interface
16     Pop tag     192.168.100.1/32  56964      Se0/2/0    192.168.2.1
17     Pop tag     192.168.100.3/32  56586      Se0/2/1    192.168.3.2
```

It shows that the P router only has two values MPLS label. Label (tag) 16 given (Pop tag) to the data packet with the prefix 192.168.100.1/32 (PE1) to be sent to the next hop through 192.168.2.1 Serial0/2/0. Label 17 is given to the data packet with the prefix 192.168.100.3/32 (PE2) to be sent to the next hop through 192.168.3.2 Serial0/2/1.

**Table 3 MPLS forwarding table on PE2**

```
PE2#show mpls forwarding-table
Local  Outgoing    Prefix            Bytes tag  Outgoing   Next Hop
tag    tag or VC   or Tunnel Id      switched   interface
16     Pop tag     192.168.2.0/24    0          Se0/3/0    192.168.3.1
17     16          192.168.100.1/32  0          Se0/3/0    192.168.3.1
18     Pop tag     192.168.100.2/32  0          Se0/3/0    192.168.3.1
19     Aggregate   192.168.4.0/24[V] 10400
20     Untagged    202.147.192.2/32[V]   \
                                     11400      Fa0/0      192.168.4.2
21     Aggregate   192.168.5.0/24[V] 10400
22     Untagged    202.147.192.2/32[V]   \
                                     11400      Fa0/1      192.168.5.2
23     16          192.168.1.0/24[V] 0          Se0/3/0    192.168.3.1
24     16          202.147.192.1/32[V]   \
                                     0          Se0/3/0    192.168.3.1
```

Table 3 is result of # show mpls forwarding table on PE2. Forwarding table on PE2 has the same meaning as the Forwarding table that exist in the router PE1 and P, just have a different next hop.

As an explanation of MPLS forwarding label, then take a sample of what happens when an IP packet of CE1_VPN_TI across MPLS VPN-A-B toward CE2_VPN_TI can be seen in Figure 9.

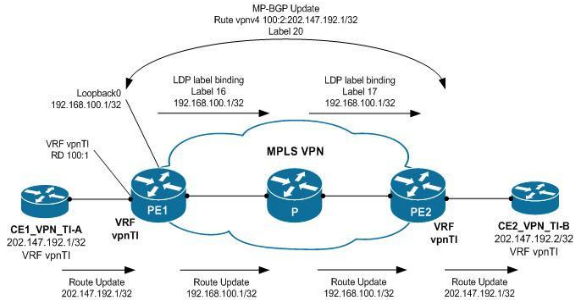

**Fig 9: The Process of IP Packets Across the MPLS VPN**

IP packets from the 202.147.192.1/32 CE1_VPN_TI sent to the VRF-A's in PE1 vpnTI. PE1 receives IPv4 prefix then redistribute to the MP-BGP, given the RD 100:2 and label 20 that turned into a vpnv4 prefix 100:2:202.147.192.1 / 32. Then the existing BGP at ingress PE, PE1 sends in this vpnv4 prefix to the router P with label 16. Then the P routers forward the vpnv4 prefix to PE2 with label 17. After vpnv4 prefix received by PE2, PE2 remove the value labels and RD so that vpnv4 prefix is converted into IPv4 prefix 202.147.192.1/32 to further put in vpnTI VRF routing table.

### 6.4 Analysis of Jitter

Jitter is the variation in delay caused by the long queue of data packets reassembles the data packets when the shipment arrives at the final destination. Basically, if the jitter value is increasing the speed of the network will be noticeably slower. Jitter is divided into four categories based on the value, including the excellent jitter values> 75ms. Good with jitter values between 75ms to 125ms. Average jitter value between 75ms to 125ms. Poor with jitter values between 125ms to 225ms.

In MPLS VPN networks that have been implemented, the method used to measure the jitter value of each VPN is using "IP SLAs ICMP Path Jitter" on each CE router VPN. IP SLAs ICMP Path Jitter is the operation of the CISO IOS to measure jitter value of each point, measure packet loss and delay measure.

**Table 4 IP SLA *Path Jitter* on CE2_VPN_TI-B**

```
ip sla monitor 1
 type pathJitter dest-ipaddr 202.147.192.1 source-ipaddr 202.147.192.2 num-packets 20
 request-data-size 32
 timeout 1000
  tag COBA vpnTI
 frequency 20
ip sla monitor schedule 1 life forever start-time now
```

Table 3 shows the result of the configuration of IP SLA monitor 1 to monitor the Path Jitter from 202.147.192.1 202.147.192.2 to get the number of packets as many as 20 packets. The size of each packet is 32 bytes with timeout rule of 1.000ms. Transmission of data packets is done continuously with a frequency of every 20 seconds. Results from Path Jitter can be seen with the command # show ip sla monitor statistics 1. Results of IP SLA monitor will appear in the form of statistics such as the Table 3.

**Table 5 Path Jitter Statistic**

```
CE2_VPN_TI-B#show ip sla moni stat
Round trip time (RTT)   Index 1
        Latest RTT: 80 ms
Latest operation start time: *00:11:55.751 UTC Fri Mar 1 2002
Latest operation return code: OK

---- Path Jitter Statistics ----

Hop IP 192.168.5.1:
Round Trip Time milliseconds:
        Latest RTT: 18 ms
        Number of RTT: 20
        RTT Min/Avg/Max: 7/18/39 ms
Jitter time milliseconds:
        Number of jitter: 14
        Jitter Min/Avg/Max: 3/14/32 ms
Packet Values:
        Packet Loss (Timeouts): 0
        Out of Sequence: 0
        Discarded Samples: 0

Hop IP 192.168.6.1:
Round Trip Time milliseconds:
        Latest RTT: 80 ms
        Number of RTT: 20
        RTT Min/Avg/Max: 51/80/136 ms
Jitter time milliseconds:
        Number of jitter: 19
        Jitter Min/Avg/Max: 1/18/49 ms
Packet Values:
        Packet Loss (Timeouts): 0
        Out of Sequence: 0
        Discarded Samples: 0
Operation time to live: Forever
```

Table 5 shows the result of the Path Jitter of CE2_VPN_TI-B toward CE2_VPN_TI-A. Be seen, only two hop that emerged is 192.168.5.1 and 192.168.6.1 as the IP address in the MPLS Service Provider Cloud is in Layer 3, while the IP SLAs ICMP Path Jitter running in Layer 2. Based on the value of jitter are obtained, the first hop is 14ms jitter values means in the category of excellent. In the second hop jitter values obtained are in the category of 19ms means excellent. IP SLAs ICMP Path Jitter will be activated on the router CE1_VPN_DKV CE1_VPN_DKV-A to-B without IPsec tunneling, CE1_VPN_TI-B toward CE1_VPN_TI-A without IPsec tunneling, and CE1_VPN_TI-B toward CE1_VPN_TI-A to enable IPsec tunneling. Jitter values are recorded in Table 6. shows the jitter value of each VPN. When IPsec tunneling is not enabled, both VPN has excellent jitter category. But when IPsec tunneling enabled jitter value increases dramatically up in the category of Poor.

**Table 6 Jitter on each Host**

| ***Hostname*** | ***Jitter on 1st Hop*** | ***Jitter on 2nd Hop*** | **Category** |
|---|---|---|---|
| CE1_VPN_<br>DKV-A | 18ms | 46ms | *Excellent* |
| CE1_VPN_<br>TI-B | 14ms | 19ms | *Excellent* |
| CE1_VPN_<br>DKV-A<br>with IPsec | - | - | - |
| CE1_VPN_<br>TI-B<br>with IPsec | - | 221ms | *Poor* |

## 6.5 Analysis of Packet Loss

Packet loss is failure in transmitting data packets. The more the number of packet loss, it will cause problems in the network. Packet Loss is divided into four categories based on the value of the percentage of packets that failed to be sent. The first category is excellent with 0% packet loss, both are Good with a percentage between 0% to 3% packet loss, the third is the Average with a percentage between 3% to 15% packet loss, the fourth is the Poor with a percentage of 15% to 25% packet loss. The results of monitoring packet loss take place during transmission of data from the router towards CE1_VPN_DKV CE1_VPN_DKV-A-B without IPsec tunneling, CE1_VPN_TI-B toward CE1_VPN_TI-A without IPsec tunneling, and CE1_VPN_TI-B toward CE1_VPN_TI-A to enable IPsec tunneling recorded in Table 7

**Table 7 Packet Loss on each Host**

| ***Hostname*** | ***Packet Loss*** | **Category** |
|---|---|---|
| CE1_VPN_DKV-A | 0% | *Excellent* |
| CE1_VPN_TI-B | 0% | *Excellent* |
| CE1_VPN_DKV-A with IPsec | - | - |
| CE1_VPN_TI-B with Ipsec | 1% | *Excellent* |

Table 7 shows the percentage of packet loss of each VPN. IPsec is not activated at the time, and vpnDKV vpnTI have no packet loss, and in the category of Excellent. When IPsec is enabled, vpnTI having 1% packet loss is there are two data packets that fail decrypted, but the percentage of packet loss is only 1% then the entry in the category of Excellent.

## 7. CONCLUSION

Based on the research and testing that has been done on the simulation, then some conclusions can be drawn as follows that by using Multi-VRF run in a Layer 3 MPLS VPN network it will be more secure because it has independent routing table. Encryption and encapsulation process in VPN do not increase the latency of data transmission. Besides that, the transmitted packet is also not lost significantly.

1. Based on the analysis of latency and packet loss percentage has satisfactory performance.

## 8. REFERENCES

[1] Pepelnjak, Ivan., 2010., *Understanding Modern* VPN *Service Offerings.*

[2] Cisco *Systems.*, 2007., *Cisco VPN Solutions Center : MPLS Selection User Guide.*

[3] Seno, Rahardianto., 2010., Perancangan dan Penerapan Teknologi *Multi Protocol Label Switching* Pada Jaringan Telekomunikasi Indosat

[4] Cisco *Systems.*, 2008., *Cisco IOS IP SLA Configuration Guide Release 12.4*

[5] Pultz, Richard., 2004., *Analysis of MPLS-Based IP VPN Security: Comparison to Traditional L2VPNs such as ATM and Frame Relay, and Deployment Guidelines*.

[6] Bollapragada, Vijay., 2005., *IPsec VPN Design*., Khalid, Mohhamed., Wainner, Scott.

[7] Fitzgerald, Denis., 2012., *Business Data Communications & Networking 11th Edition.*

[8] Ghein, Luc De., 2007., MPLS *Fundamentals.*

[9] Osborne, Simha., 2002., *Traffic Engineering with MPLS.*