ANALISA PENGARUH FITUR BFD TERHADAP REDUNDANSI SERVIS VPN BERBASIS IP/MPLS PADA JARINGAN METRO-E PT. NETTOCYBER INDONESIA AREA MEGA KUNINGAN JAKARTA SELATAN

Latif Kamaludin, Nurwijayanti KN, ST,MT, Agus Sugiharto, ST, MT
Teknik Elektro Universitas Dirgantara Marsekal Suryadarma

ABSTRAK

Layanan jaringan khususnya jaringan Metro Ethernet pada masa dewasa ini semakin berkembang seiring dengan kebutuhan pelanggan yang sangat membutuhkan ketersedian layananan *(High Availibility)* dengan nilai *downtime* yang kecil. Untuk menunjang kebutuhan tersebut harus didukung dengan jaringan yang mempunyai redundansi, dengan adanya redundansi meminimalisasi terjadinya downtime, artinya apabila salah satu jaringan down maka akan dialihkan pada jaringan cadangan. Dalam proses pemindahan *(failover)* masih terdapat downtime pada rentang tersebut.

Untuk menanggulangi masalah tersebut maka dilakukan implementasi fitur BFD *(Bidirectional Forwarding Detection)* dengan sistem kerjanya adalah mempercepat deteksi gangguan pada jaringan sehingga pada saat terjadi gannguan, traffic jaringan akan lebih cepat dialihkan pada jaringan cadangan.

Pada penelitian yang dilakukan dapat disimpulkan bahwa implementasi jaringan dapat meningkat ketersediaan jaringan *(high availability)* hingga 0,6 persen dan meminimalisir *packet loss* pada saat *failover* dengan nilai 1 % *packet loss*

Kata kunci: Redundansi, *Bidirectional Forwarding Detection (BFD), High Availability, Failover, Packet Loss.*

I. PENDAHULUAN

1.1 Latar Belakang

Pada dewasa ini para pengguna layananan data baik dari perorangan sampai pada suatu instansi atau organisasi sangat membutuhkan kestabilan suatu koneksi jaringan yang handal untuk mendukung kegiatan maupun pekerjaan sepanjang waktu. Pada kebutuhan suatu perusahaan maupun instansi, menggunakan VPN*(Vitual Private Networks)* adalah sebuah solusi untuk menghubungkan kantor pusat dengan kantor cabang yang memiliki letak geografis yang berbeda, juga mengatasi masalah keterbatasan jaringan komunikasi data yang telah ada. VPN menawarkan jaringan *private* melalui jaringan *public* yang dapat digunakan untuk mengkoneksikan setiap kantor cabang tanpa harus membangun jaringan *physical* baru. VPN sendiri dapat diimplementasikan di berbagai jaringan salah satunya *Metro Ethernet.*

Metro Ethernet adalah *Wide Area Network* (WAN) berkelas *carrier* yang meliputi area *Metropolitan* dengan media komunikasi *Ethernet*. *Metro Ethernet* dapat menghubungkan beberapa *Local Area Network* (LAN) yang berbeda lokasi. Saat ini jaringan *Metro Ethernet* dapat memilki kapasitas *transport data* mencapai 10 Gbps. Saat ini banyak penyedia jasa layanan telekomunikasi yang menggunakan jaringan *Metro Ethernet* untuk menyediakan layanan VPN bagi *customer*yang membutuhkan jaringan *private* yang aman dan memiliki kapasitas *bandwidth* yang besar.*Metro Ethernet* mengalami perkembangan dalam mentransportasikan paket data dan menyediakan layanan VPN, yaitu dengan menerapkan teknologi *Multiprotocol Label Switching* (MPLS).MPLS memberikan optimasi routing pada komunikasi *end to endrouter* di jaringan *Metro Ethernet*.MPLS menggunakan metode *labeling* untuk pengiriman paket data sehingga paket data yang dikirimkan menjadi lebih cepat, efisien dan handal.

Pada konvergensi suatu jaringan IP/MPLS memerlukan *availability*

yang tinggi untuk memenuhi *SLA (Service-Level Agreements)* kepada pelanggan.SLA didefinisikan sebagai komitmen resmi yang berlaku antara penyedia layanan dan pelanggan. Aspek khusus dari kualitas layanan, ketersediaan, tanggung jawab yang disepakati antara penyedia layanan dan pengguna layanan. Komponen SLA yang paling umum adalah bahwa layanan harus diberikan kepada pelanggan sebagaimana disepakati dalam kontrak. Sebagai contoh, penyedia layanan Internet biasanya menyertakan perjanjian tingkat layanan sesuai persyaratan kontrak mereka dengan pelanggan untuk menentukan tingkat layanan yang dijual dalam bahasa biasa. Dalam kasus ini, SLA biasanya memiliki definisi teknis dalam waktu rata-rata antara kegagalan"*mean time between failures" (MTBF),* waktu rata-rata untuk memperbaiki atau berarti waktu untuk pemulihan"*mean time to recovery (MTTR)"*; mengidentifikasi pihak mana yang bertanggung jawab untuk melaporkan kesalahan atau membayar biaya; tanggung jawab untuk berbagai tingkat data,*downtime,throughput,latency,*dan parameter lainnya.

Kestabilan jaringan yang dirasakan oleh pelanggan akan berujung kepada penilaian terhadap suatu perusahaan penyedia jasa layanan jaringan *(Provider)*yang berujung kepada persaingan bisnis pada lingkup industri telekomunikasi tersebut. Pada sisi perusahaan penyedia jasa layanan jaringan *(Provider)* memberikan suatu kehandalan jaringan kepada pelanggan adalah suatu keharusan dan memberikan suatu redundansi jaringan adalah suatu solusi.

Pada hal ini PT. Nettocyber Indonesia (VELO Networks) sebagai salah satu *Internet Service Provider (ISP)*di Indonesia sudah memiliki jaringan *Metro Ethernet* dengan media fiber optik di area Jakarta dengan kapasitas mencapai 10 Gbps pada setiap POP *(Point of Presence)* yang mempunyai redundansi; yakni memiliki link cadangan apabila link utama mati traffic akan dialihkan ke link cadangan dengan tujuan memberikan suatu layanan yang handal dan mencapai SLA kepada pelangggan. Perlu digaris bawahi apakah redundasi yang sudah

ada yaitu reudundansi secara fisik bisa ditingkatkan dengan meningkatkan performansi protokol dan fitur jaringan. Dalam kondisi saat ini jaringan Metro-E milik PT. Nettocyber Indonesia (VELO Networks) mempunyai redundansi secara fisik maupun protokol, protokol yang digunakan adalah OSPF*(Open Shortest Path First)* fungsisnya untuk metrigger apabila salah satu link utama *failureakan failover ke* link cadangan. Protokol *OSPF (Open Shortest Path First)* yang mana protokol ini menggunakan algoritma *shortest-path-first (SPF)* (juga disebut *algoritma Dijkstra*) untuk menghitung jalur terpendek ke semua tujuan, melakukan perhitungan dengan menghitung jalur terpendek secara bertahap dan memilih kandidat terbaik dari jalur yang ada.Untuk memilih rute terbaik, parameter yang digunakan oleh OSPF adalah *cost*. Rute terbaik akan ditentukan oleh nilai *cost* terkecil. Dengan menggunakan portokol OSPF tersebut masih terdapat beberapa kekurangan yaitu beberapa parameter menunjukan adanya packet *loss, latency, dan jitter* yang cukup tinggi yang membutuhkan waktu beberapa detik pada saat proses *failover*.

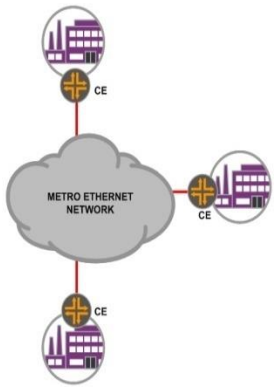
Dengan latar belakang diatas menganalisis fitur BFD *(Biderectional Forwarding Detection)* dengan sistem kerja yang sangat cepat dlama mengidentifikasi *failure* pada perangkat maupun jaringan dalam hitungan *milisecon* sehingga seharusnya proses *failover* link dapat lebih cepat dan *smooth.* Dengan kelebihan pada fitur tersebut maka *PT. Nettocyber Indonesia (VELO Networks)* sebagai penyedia jasa layanan jaringan dapat menerapkan fitur tersebut pada protokol yang digunakan dalam jaringan Metro-E , namun setiap fitur mempunyai kelebihan dan kekurangan dalam implementasinya, dalm penulisan penelitian ini akan menjawab hal tersebut.

II. LANDASAN TEORI

2.1 Metro Ethernet

Metro Ethernet umumnya didefinisikan sebagai jaringan yang menjembatani atau menggabungkan *LAN (Local Area Network)*perusahaan yang terpisah secara geografis, juga menghubungkan jaringan *WAN (Wide*

*Area Network)*atau *Backbone* yang umumnya dimiliki oleh penyedia layanan*(Provider).Metro Ethernet Networks* menyediakan layanan konektivitas di geografismetropolitan atau area perkotaan yang memanfaatkan *ethernet* sebagai protokol inti dan menggunakan kabel fiber optik sebagai infrastruktur jaringan. Dan definisi dari *ethernet* adalah sebuah teknologi komputer yang telah dibakukan oleh *IEEE (Institute of Electrical and Electronics Engineers)* dengan prinsip kerjanya mendefinisikan fungsi-fungsi yang terjadi pada lapisan fisik dan lapisan *data-link* dalam model referensi jaringan tujuh lapis *OSI* atau lebih dikenal dengan *OSI Layer* dan membentuk paket data ke dalam *frame* sebelum kemudian ditransmisikan ke media kabel. *Ethernet* dikomersialkan pada tahun 1980-an dan distandarisasikan *IEEE 802.3* pada tahun 1983.



Gambar 1. Model jaringan Metro-E sampai ke pelanggan

2.2 Biderectional Forwarding Detection (BFD)

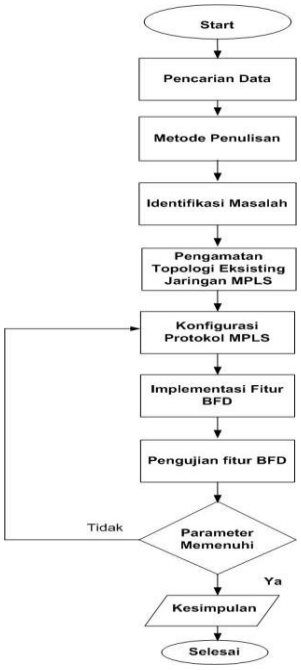
Menurunkan parameter timer pada IGP dalam hal ini adalah OSPF memang suatu solusi yang masuk akal untuk mendeteksi *failure* pada jaringan, tapi hal ini harus dibayar mahal dikarenakan akan membebani kinerja *Routing Engine* pada router sehingga menimbulkan masalah pada router. Hal ini bisa dibayangkan dengan sebuah sekenario apabila suatu jaringan mempunyai ratusan *interface* dan semuanya mengirimkan *OSPF-hello message* pasti akan memberatkan kinerja router, untuk itu menurunkan timer pada protokol OSPF bukanlah suatu solusi untuk mendeteksi link secara cepat dan efisien.

Fitur BFD adalah protokol sederhana yang dirancang untuk

melakukan satu fungsi: mendeteksi kegagalan link. BFD menyediakan mekanisme untuk memonitor link secara langsung dan memberitahukan perangkat jika berhenti menerima pesan dari tetangga di ujung link itu. Dengan BFD, tidak perlu lagi menurunkan timer pada protokol OSPF, atau bahkan membiarkannya berjalan pada pengaturan default juga dapat mengatur nilai timer yang lebih tinggi dan hampir menghilangkan masalah beban pada router yang dihasilkan dari pembuatan OSPF-Hello message.

Gambar 2. Sistem kerja *BFD (Biderectional Forwarding Detection)*

III. PENGAMATAN, KONFIGURASI PROTOKOL,IMPLEMENTASI, PENGUJIAN DAN ANALISA FITUR BFD

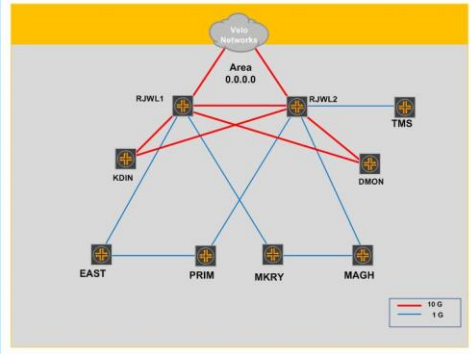


Gambar 3.*Flowchart* Metode Penelitian

3.1 Pengamatan Topologi Jaringan

Dalam melakukan melakukan pengamatan pada topologi yang ada (exisiting) maka akan dapat diketahui parameter-parameter performansi dengan malakukan simulasi sesuai dengan kondisi jaringan yang ada, pada simulasi ini akan diuji coba dari sebagian topologi yang ada pada jaringan

Metro Ethernet di PT. Nettocyber Indonesia (VELO Networks) area Mega Kuningan, dengan tujuan didapati parameter-parameter performansi servis L2VPN sebelum menggunakan fitur BFD. Berikut adalah topologi existing jaringan Metro Ethernet di PT. Nettocyber Indonesia (VELO Networks) area Mega Kuningan:



Gambar 4. Topologi Jaringan Metro-E PT. Nettocyber Indonesia (VELO Networks) Area Mega Kuningan

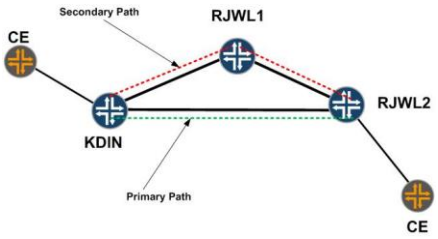
Dari gambar 4.terdapat beberapa perangkat yang terinstallasi di gedung-gedung area Mega Kuningan Jakarta Selatan, berikut nama-nama perangkat sesuai gedung yang sudah ter-install perangkat Metro Ethernet PT. Nettocyber Indonesia (VELO Networks) Area Mega Kuningan:

Tabel 1. Nama perangkat dan gedung

Nama Perangkat	**Nama Gedung**
RJWL1	Menara Rajawali
RJWL2	Menara Rajawali
KDIN	Menara Kadin
DMON	Menara Danamon
EAST	THE EAST
PRIM	Menara Prima
MKRY	Menara Karya
MAGH	Menara Anugrah

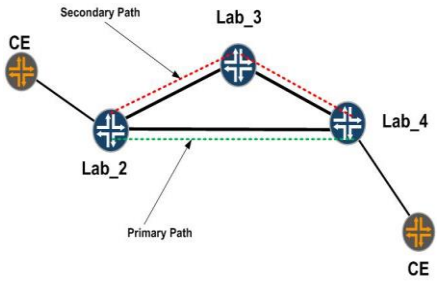
Kemudian setelah diketahui topologi *exsiting* tersebut diambil sample topologi pada area Menara Kadin, RJWL1, RJWL2 untuk dilalukan simulasi dengan tujuan didapati parameter-parameter performansi servis L2VPN dengan tidak menggunakan fitur BFD.

Berikut topologi pada area Menara Kadin, RJWL1, RJWL2:



Gambar 5. Topologi Area Menara Kadin, Menara Rajawali

Dari gambar 4.1 didapati *primary path* dari customer adalah melalui jalur RJWL2 , dan apabila link primary meuju ke RJWL2 *failure* maka akan *failover* menuju RJWL1 kemudian RJWL2 melalui *secondary path*. Pada proses failover tersebut nantinya akan diamati nilai ketersediaan jaringan *(High Availibility), packet loss,* dan *latency*pada servis L2VPN. Untuk mengetahui parameter parameter tersebut akan dilakukan simulasi sesuai dengan topologi pada *gambar 4.1 Topologi Area Menara Kadin*, Menara Rajawali. Pada topologi simulasi berdasarkan dengan gambar 4.1 yaitu topologi yang sama hanya saja akan ada perbedaan nama perangkat KDIN akan sama dengan Lab_2 berfungsi sebagai PE , RJWL1 akan sama dengan Lab_3 berfungsi sebagai P , dan RJWL2 akan sama dengan Lab_4 berfungsi sebagai PE , untuk lebih jelasnya topologi simulasi adalah sebagai berikut:



Gambar 6. Topologi lab simulasi

Simulasi yang dilakukan adalah dengan konfigurasi protokol IGP, LDP, fitur BFD, servis L2VPN dan kemudian menganalisa pengaruh fitur BFD terhadap servis L2VPN. Hal-hal tersebut akan dijelaskan secara lebih terperinci pada sub bab berikutnya.

3.2 Konfigurasi Protokol

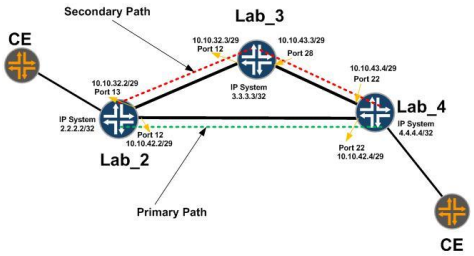
Pada simulasi untuk menganalisa pengaruh fitur BFD terhadap servis L2VPN, dibutuhkan konfigurasi pada perangkat-

perangkat sesuai dengan topologi simulasi pada gambar 4.3 Untuk melakukan konfigurasi protokol-protokol pada topologi lab simulasi pada gambar 4.3 terlebih dahulu diberikan alokasi IP address dan interface. Berikut adalah tabel alokasi IP address dan interface untuk kebutuhan tersebut.

Tabel 2. Alokasi IP address dan penamaan Interface

Nama Perangkat	IP Address	Interface Name
LAB_2	10.10.42.2/29	lab4-1/1/22
	10.10.32.2/29	lab3-1/1/12
	2.2.2.2/32	system
LAB_3	10.10.43.3/29	lab4_1/1/28
	10.10.32.3/29	lab2-1/1/13
	3.3.3.3/32	system
LAB_4	10.10.43.4/29	lab3-1/1/28
	10.10.42.4/29	lab2-1/1/12
	4.4.4.4	system

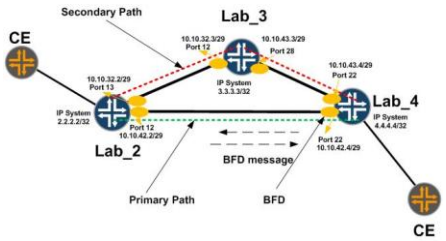
Untuk lebih memudahkan pemahaman berikut adalah alokasi IP address dan penamaan interface pada topologi lab simulasi, dan berikut gambar secara lebih detailnya;



Gambar 7. Topologi lab simulasi dan alokasi IP address

Setelah alokasi IP address dan penamaan interface ditentukan, langkah selanjutnya adalah konfigurasi pada sisi perangkat meliputi konfigurasi IP address dan interface, protokol OSPF, LDP, servis L2VPN, dan konfigurasi fitur BFD.

Konfigurasi fitur BFD diterapkan pada tiap-tiap interface dan diaktifkan pada protokol OSPF sesuai dengan kinerjanya yaitu agar dapat mendeteksi failure lebih cepat sehingga proses failover juga lebih cepat.



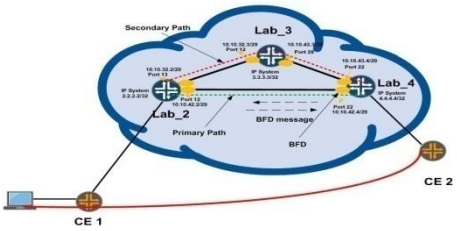
Gambar 8. Penerapan Fitur BFD

3.3 Pengujian dan Analisa Fitur BFD

Pengujian fitur BFD ini dilakukan pada sisi PE , pada sisi CE akan memonitor apakah fitur

BFD berjalan optimal pada sisi IGP sehingga mempengaruhi kualitas servis L2VPN pada sisi CE, tujuan dari pengujian ini adalah mendapat data pada saat proses failover.

Pada tahap pengujian fitur BFD dilakukan pada sisi PE yaitu dengan *shutdown* interface secara sistem dan juga *shutdown* secara fisik, pada *shutdown* secara fisik sebagai simulasi apabila *failure* disebabkan oleh perangkat fisik baik itu *port interface* maupun pada sisi kabel. Pada sisi CE1 terdapat direct koneksi pada laptop untuk memonitor dan mengamati berapa lama *downtime,* banyaknya *packet loss, latency*, dan *troughput*.

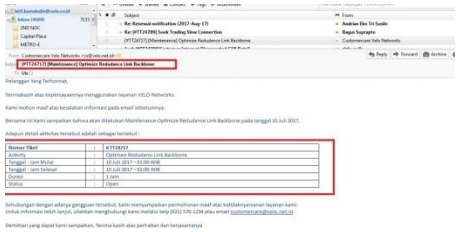


Gambar 9. Pengujian fitur BFD

Pada pengujian didapati hasil dari parameter-parameter yaitu *High Availability*, *packet loss dan latency* dengan mengimplementasi BFD maupun tidak, dibawah ini akan menjelaskan hasil pengujian dan analisa dari masing-masing parameter, yaitu:

a) High Availability

Pada pengujian *High Availibility* dilakukan pada pengujian *shutdown* sistem dan fisik dengan limitasi bandwidth 5 Mbps,10 Mbps, dan 20 Mbps dengan rentang waktu pengujian adalah 1 jam. Rentang waktu pengujian dapat disebut "*mean time between failures" (MTBF)* yang diberitahukan service provider melalui email kepada pelanggan.

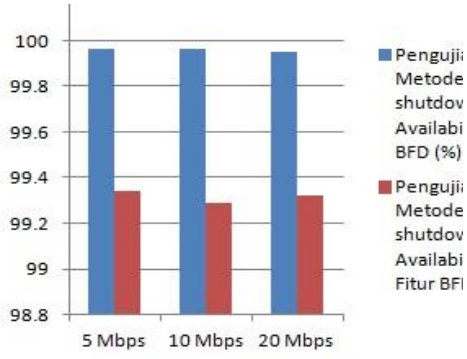


Gambar 10. Notifikasi kepada pelanggan melalui email

Dari pengujian tersebut dilakukan dengan metode shutdown sistem dan shutdown fisik, dengan mengambil parameter-parameter untuk mengetahui nilai waktu rata-

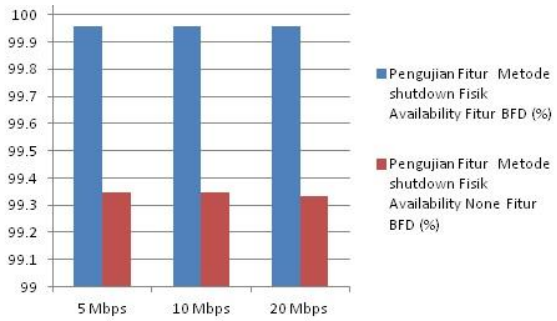
rata untuk memperbaiki atau waktu untuk pemulihan "*mean time to recovery (MTTR)"*dengan menggunakan alat ukur waktu *(stopwatch)* dan pengiriman paket ICMP menggunakan "ping time". Pengukuran MTTR dengan menghitung berapa lama durasi terjadinya downtime / paket *Request Time Out (RTO)* pada saat failover berlangsung.

Pada pengujian shutdown sistem dengan penggunaan BFD downtime termonitor durasi lebih singkat yaitu durasi minimum downtime sekitar 1,09 detik dan maksimum 1,93 detik. Sedangkan dengan tidak menggunakan fitur BFD didapati nilai minimum downtime sekitar 22,29 detik dan maksimum 27,76 detik.



Gambar 11. Availability pada pengetesan shutdown sistem

Dari perhitungan yang dilakukan pada pengujian shutdown fisik, didapati servis-servis dengan menggunakan fitur BFD memiliki angka sekitar 0,6 % lebih tinggi dibandingkan dengan servis-servis yang tidak menggunakan fitur BFD.

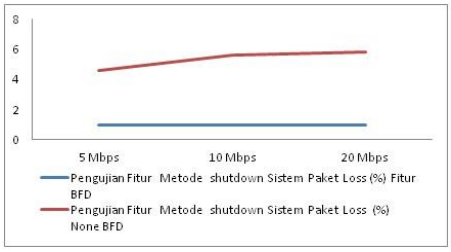


Gambar 12. Availability pada pengetesan shutdown Fisik

b) Packet Loss

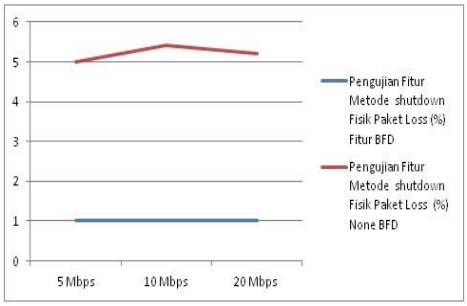
Dari hasil pengujian baik pada shutdown sistem maupun shutdown fisik dengan limitasi bandwidth pada 5 Mbps, 10 Mbps dan 20 Mbps didapati dengan menggunakan fitur BFD pada saat *failover* hanya terjadi packet loss 1% sedangkan tanpa menggunakan fitur BFD pada pengujian shutdown sistem didapati nilai minimum packet loss pada 4,6 % dan maksimum pada 5,8 %. Pengujian ini dilakukan dengan

metode pengamatan paket ICMP sebesar 56 bytes pada setiap satu paket dengan 100 kali pengiriman pada saat utilisasi traffic mencapai maksimum.



Gambar 13. Grafik packet loss pengujian shutdown sistem

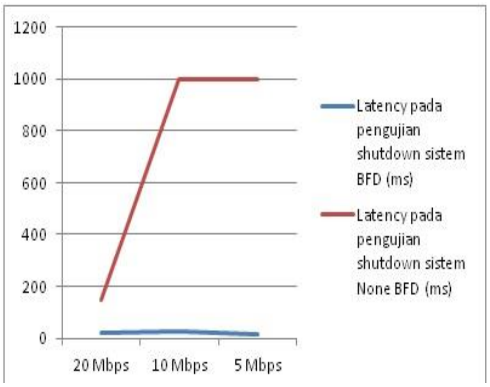
Pada pengujian *shutdown* fisik didapati nilai minimum packet loss adalah 5% dan nilai maksimum 5,4 % dengantanpa menggunakan fitur BFD, nilai paket loss tersebut jauh lebih tinggi dibandingkan dengan fitur BFD yang mampu failover dengan cepat sehingga packet loss hanya sebesar 1 %.



Gambar 14. Grafik packet loss pengujian shutdown fisik

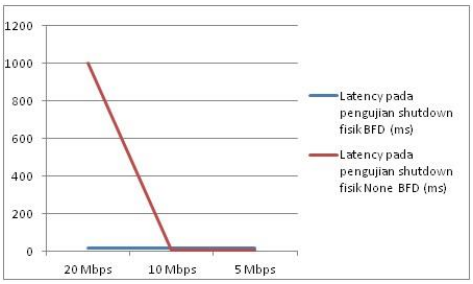
c) Latency

Pada pengujian shutdown sistem dan fisik didapati latency proses failover berlansung, hasil tersebut pada penggunaan fitur BFD maupun tanpa menggunaan fitur BFD. Pada pengujian shutdown sistem dengan mengguankan fitur BFD didapati nilai minimum latency sekitar 13 ms dan nilai maksimum pada 26 ms, sedangkan tanpa fitur BFD didapati nilai minimum latency sekitar 148 ms dan nilai maksimum 1000 ms. Berikut adalah tabel dan grafik hasil pengujian dan analisa latency dengan shutdown sistem.



Gambar 15. Grafik latency pengujian shutdown sistem

Pada pengujian shutdown fisik, latency dengan penggunaan fitur BFD didapati nilai minimum sekitar 15 ms dan nilai maksimum 18 ms. Hasil tersebut cukup jauh berbeda dengan hasil dari pengujian latency tanpa menggunakan fitur BFD , yaitu didapati nilai minimum sekitar 3 ms dan nilai maksimum 1002 ms. Dari hasil tersebut fitur BFD tidak berpengaruh signifikan pada latency setelah proses failover berlangsung. Berikut tabel dan grafik pada pengujian latency dengan shutdown fisik.



Gambar 16. Grafik latency pengujian shutdown fisik

IV. KESIMPULAN

Dalam penelitian ini dapat disimpulkan bahwa penggunaan fitur BFD (Bidirectional Forwarding detection) pada jaringan Metro Ethernet PT. NETTOCYBER INDONESIA (VELO NETWORKS) di area Mega Kuningan, Jakarta Selatan memiliki keuntungan dalam performansi dan redundasi yaitu:

1) Dengan menggunakan fitur BFD meningkatkan high availability hingga 0,6 % dibandingkan dengan tidak menggunakan fitur BFD.
2) Dengan menggunakan fitur BFD paket loss hanya 1 % pada saat terjadi *failover*dibandingkan dengan tidak menggunakan fitur BFD yang terdapat hingga 5,8 % paket loss.
3) Pada pengujian shutdown sistem dan fisik didapati latency proses failover yang tidak stabil pada servis L2VPN tanpa menggunakan fitur BFD, dengan nilai minimum 3 ms dan nilai maksimum mencapai 1002 ms.

V. DAFTAR PUSTAKA

1. Ivan Pepelnjak CCIE #1354, Jim Guichard CCIE #2069, MPLS and

VPN Architectures, CCIP™ Edition ,2002
2. Martin Brown, Nick Ryce, Day One: Routing The Internet Protocol,Juniper Netwokrs, 2015
3. Paresh Khatri, MPLS-based Metro Ethernet Networks A Tutorial, Alcatel Lucent, 2013
4. Sam Halabi, OSPF Design Guide,Cisco System , 1996
5. Thomas M. Thomas II,OSPF Network Design Solutions Second Edition,2003
6. Juniper Networks, JNCIS-SP Study Guide—Part 2, 2013
7. Juniper Networks, JNCIS-SP Study Guide—Part 3, 2013
8. https://id.wikipedia.org/wiki/Ethernet , 13 Mei 2017
9. https://www.beritateknologi.com/mengenal-lebih-dalam-tentang-kabel-fiber-optik, 13 Mei 2017
10. https://jarkomindonesia.wordpress.com/2013/02/25/mpls-basic-ldp, 13 Mei 2017
11. https://tools.ietf.org/html/rfc2544 , 13 Mei 2017
12. https://www.juniper.net/documentation/en_US/junos/topics/concept/bfd-understanding-qfx-series.html, 20 Mei 2017
13. https://en.wikipedia.org/wiki/High_availability, 2 Juni 2017