



**Analisa Redundansi Servis VPN Berbasis IP/MPLS Pada Jaringan Metro Ethernet
Menggunakan Fitur BFD**

TUGAS AKHIR

Irawan Febriyanto
41514320012

**PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS MERCU BUANA
JAKARTA
2018**



**Analisa Redundansi Servis VPN Berbasis IP/MPLS Pada Jaringan Metro Ethernet
Menggunakan Fitur BFD**

Tugas Akhir

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

Oleh:
Irawan Febriyanto
41514320012

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS MERCU BUANA

JAKARTA

2018

MERCU BUANA

LEMBAR PERNYATAAN ORISINALITAS

Yang bertanda tangan dibawah ini:

NIM : 41514320012

Nama : Irawan Febriyanto

Judul Tugas Akhir : Analisa Redundansi Servis VPN Berbasis IP/MPLS Pada Jaringan Metro Ethernet Menggunakan Fitur BFD

Menyatakan bahwa Laporan Tugas Akhir saya adalah hasil karya sendiri dan bukan plagiat. Apabila ternyata ditemukan didalam laporan Tugas Akhir saya terdapat unsur plagiat, maka saya siap untuk mendapatkan sanksi akademik yang terkait dengan hal tersebut.

Jakarta, 26 Desember 2018



Irawan Febriyanto

UNIVERSITAS
MERCU BUANA

SURAT PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR

Sebagai mahasiswa Universitas Mercu Buana, saya yang bertanda tangan di bawah ini :

Nama Mahasiswa : Irawan Febriyanto
NIM : 41514320012
Judul Tugas Akhir : Analisa Redundansi Servis VPN Berbasis IP/MPLS
Pada Jaringan Metro Ethernet Menggunakan Fitur
BFD

Dengan ini memberikan izin dan menyetujui untuk memberikan kepada Universitas Mercu Buana **Hak Bebas Royalti Noneksklusif** (*None-exclusive Royalty Free Right*) atas karya ilmiah saya yang berjudul diatas beserta perangkat yang ada (jika diperlukan).

Dengan Hak Bebas Royalti/Noneksklusif ini Universitas Mercu Buana berhak menyimpan, mengalihmedia/formatkan, mengelola dalam bentuk pangkalan data (*database*), merawat dan mempublikasikan tugas akhir saya.

Selain itu, demi pengembangan ilmu pengetahuan di lingkungan Universitas Mercu Buana, saya memberikan izin kepada Peneliti di Lab Riset Fakultas Ilmu Komputer, Universitas Mercu Buana untuk menggunakan dan mengembangkan hasil riset yang ada dalam tugas akhir untuk kepentingan riset dan publikasi selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Jakarta, 26 Desember 2018



Irawan Febriyanto

SURAT PERNYATAAN LUARAN TUGAS AKHIR

Sebagai mahasiswa Universitas Mercu Buana, saya yang bertanda tangan di bawah ini :

Nama Mahasiswa : Irawan Febriyanto
 NIM : 41514320012
 Judul Tugas Akhir : Analisa Redundansi Servis VPN Berbasis IP/MPLS Pada Jaringan Metro Ethernet Menggunakan Fitur BFD

Menyatakan bahwa Luaran Tugas Akhir saya adalah sebagai berikut :

No	Luaran	Jenis	Status
1	Publikasi Ilmiah	Jurnal Nasional Tidak Terakreditasi	Diajukan
		Jurnal Nasional Terakreditasi	
		Jurnal International Tidak Bereputasi	Diterima
		Jurnal International Bereputasi	
	Disubmit/dipublikasikan di :	Nama Jurnal : International Journal of Computer Applications ISSN : 0975 – 8887	V
2	Kertas Kerja, Merupakan material hasil penelitian sebagai kelengkapan Artikel Jurnal. Terdiri dari (minimal 4)	Literatur Review	[V]
		Hasil analisa & perancangan aplikasi	[V]
		Source code	[V]
		Data set	[]
		Tahapan eksperimen	[V]
		Hasil eksperimen seluruhnya	[V]
3	HAKI Disubmit / Terdaftar	HKI	Diajukan
		Paten	Tercatat
		No & Tanggal Permohonan	
		No & Tanggal Pencatatan	

Demikian pernyataan ini saya buat dengan sebenarnya.

Jakarta, 26 Desember 2018


 Irawan Febriyanto


LEMBAR PERSETUJUAN

Nama Mahasiswa : Irawan Febriyanto
NIM : 41514320012
Judul Tugas Akhir : Analisa Redundansi Servis VPN Berbasis IP/MPLS
Pada Jaringan Metro Ethernet Menggunakan Fitur
BFD

Tugas Akhir ini telah diperiksa dan disetujui

Jakarta, 26 Desember 2018

Menyetujui,



(Sri Dianing Asri, S.T., M.Kom)

Dosen Pembimbing

UNIVERSITAS
MERCU BUANA

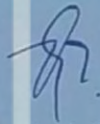
LEMBAR PERSETUJUAN

Nama Mahasiswa : Irawan Febriyanto
NIM : 41514320012
Judul Tugas Akhir : Analisa Redundansi Servis VPN Berbasis IP/MPLS
Pada Jaringan Metro Ethernet Menggunakan Fitur
BFD

Tugas Akhir ini telah diperiksa dan disetujui

Jakarta, 26 Desember 2018

Menyetujui,



(Sri Dianing Asri, S.T., M.Kom)
Dosen Pembimbing

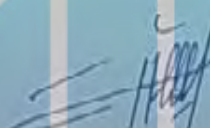
UNIVERSITAS
MERCU BUANA

LEMBAR PERSETUJUAN PENGUJI


NIM : 41514320012
Nama : Irawan Febriyanto
Judul Tugas Akhir : Analisa Redundansi Servis VPN Berbasis IP/MPLS
Pada Jaringan Metro Ethernet Menggunakan Fitur
BFD

Tugas Akhir ini telah diperiksa dan disidangkan sebagai salah satu persyaratan untuk memperoleh gelar Sarjana pada Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Mercu Buana.

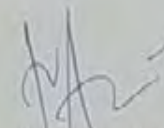
Jakarta, 22 Januari 2019



(Diky Firdaus, S.Kom, MM)
Ketua Penguji



(Umniy Salamah, MMSI)
Anggota Penguji 1



(Nur Ani, MMSI)
Anggota Penguji 2

UNIVERSITAS
MERCU BUANA

LEMBAR PENGESAHAN

NIM : 41514320012
Nama : Irawan Febriyanto
Judul Tugas Akhir : Analisa Redundansi Servis VPN Berbasis IP/MPLS Pada Jaringan Metro Ethernet Menggunakan Fitur BFD

Tugas Akhir ini telah diperiksa dan disidangkan sebagai salah satu persyaratan untuk memperoleh gelar Sarjana pada Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Mercu Buana.

Jakarta, 22 Januari 2019

Menyetujui,



(Sri Dianing Asri, ST, M.Kom)
Dosen Pembimbing

Mengetahui,

UNIVERSITAS

(Diky Firdaus, S.Kom, MM)

Koord. Tugas Akhir Teknik Informatika

(Desi Ramayanti, S.Kom, MT)

Ka. Prodi Teknik Informatika

MERCU BUANA

ABSTRAK

Nama : Irawan Febriyanto
NIM : 41514320012
Pembimbing TA : Sri Dianing Asri, S.T, M.Kom
Judul : Analisa Redundansi Servis VPN Berbasis IP/MPLS
Pada Jaringan Metro Ethernet Menggunakan Fitur
BFD

Dalam operasionalnya setiap perusahaan yang memiliki beberapa cabang, diharuskan untuk dapat saling berkomunikasi dengan kantor pusat dan juga kantor cabang lainnya. Dikarenakan setiap data transaksi yang harus diketahui oleh kantor pusat dan ada data yang kantor cabang harus bisa mendapatkannya dari kantor pusat. Namun data yang ditransaksikan tersebut harus dijaga kerahasiaannya. Untuk dapat mengkomunikasikan data tersebut antar kantor harus bisa saling terkoneksi, dengan kebutuhan akan kerahasiaan data yang sangat tinggi maka VPN (Virtual Private Network) adalah salah satu solusi untuk menghubungkan setiap kantor dan menjaga kerahasiaan data yang ditransaksikan. PT NettoCyber Indonesia adalah sebuah perusahaan penyedia layanan internet yang bisa memberikan layanan VPN untuk customer yang memiliki kantor cabang yang harus saling terhubung. Dengan menggunakan jaringan Metro Ethernet yang berbasis IP/MPLS PT NettoCyber Indonesia bisa menjamin tingkat ketersediaan yang tinggi di dalam SLA (Service Level Agreement). Demi menjaga SLA dengan customer maka setiap jaringan Metro Ethernet memiliki redundansi. Dimana jika salah satu backbone link bermasalah maka akan segera pindah ke backbone lainnya yang available dengan proses failover yang tidak memakan waktu lama. Sehingga bisa menjaga High Availability kepada customer yang sangat membutuhkan koneksi stabil dalam operasionalnya. karena pada customer yang membutuhkan high availability biasanya memiliki transaksi data yang sangat banyak dan cepat

Kata kunci:

VPN, Metro Ethernet, Redundansi, Failover

UNIVERSITAS
MERCU BUANA

ABSTRACT

Name : Irawan Febriyanto
Student Number : 41514320012
Counsellor : Sri Dianing Asri, S.T, M.Kom
Title : Redundancy Analysis VPN Service IP/MPLS Based
on Metro Ethernet Network Using BFD Feature

In daily operations company that has some of the branch offices, required to communicate with and other offices as well. Because every data transaction that must be known by the headquarters and branch office data there should get it from headquarters. But the data are transacted must be kept confidential. To communicate such data between Office must be interconnected with the need for confidentiality of data is very high, then the VPN (Virtual Private Network) is one of the solutions for connecting each Office and keep confidentiality of data is transacted. PT NettoCyber Indonesia is a major internet service provider that can provide VPN service for customers that have branch offices should be connected. By using Metro Ethernet networks IP/MPLS-based PT NettoCyber Indonesia can guarantee high availability in an SLA (Service Level Agreement). For maintaining the SLA with the customer then any Metro Ethernet networks have redundancy. Where if one backbone links are problem, it will soon be moved to other backbone available with failover process doesn't take a long time. So that it can keep the High Availability to customer a very stable connection in its operational needs. Because on a customer who requires high availability typically have transaction data very much and fast.

Key words:

VPN, Metro Ethernet, Redundansi, Failover

UNIVERSITAS
MERCU BUANA

KATA PENGANTAR

Puji syukur kita panjatkan Allah SWT atas rahmat dan karunia-Nya sehingga penulis dapat menyelesaikan tugas akhir ini.

Penulis menyadari bahwa tanpa dukungan dan bimbingan dari berbagai pihak. Kiranya penulisan akan mengalami kesulitan dalam penyusunan tugas akhir ini tanpa bimbingan dan dukungan maka penulis akan mengalami kesulitan dalam penulisan tugas akhir ini. Oleh karena itu, penulis mengucapkan terima kasih kepada:

1. Allah SWT yang telah memberikan segala rahmat dan karunia-Nya sehingga penulisa bisa menyelesaikan tugas akhir ini
2. Kedua orang tua yang turut membantu dalam hal moral maupun doa agar penulis mendapatkan kelancaran dalam penulisan tugas akhir
3. Ibu Sri Dianing Asri, S.T, M.Kom, Selaku Dosen Pembimbing dan Pengampu matakuliah Metodologi Penelitian Teknik Informatika
4. Desi Ramayanti, MT, Selaku Ketua Program Studi Teknik Informatika Universitas Mercu Buana
5. Serta berbagai pihak yang tidak dapat disebutkan satu persatu, yang telah memberikan dukungan moral dan doa kepada penulis

Adapun kiranya dalam penulisan ini kiranya masih banyak kekurangan dan jauh dari kata sempurna. Untuk itu penulis menghaturkan permohonan maaf apabila terdapat kesalahan dalam penulisan tugas akhir ini

Akhir kata, penulis berharap penulisan ini bisa menjadi bahan acuan untuk penulisan tugas akhir maupun makalah dikemudian hari

Jakarta, 26 Desember 2018
Penulis



DAFTAR ISI

HALAMAN SAMPUL.....	i
HALAMAN JUDUL	i
LEMBAR PERNYATAAN ORISINALITAS.....	ii
SURAT PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR.....	iii
SURAT PERNYATAAN LUARAN TUGAS AKHIR	iv
LEMBAR PERSETUJUAN.....	v
LEMBAR PERSETUJUAN PENGUJI	vi
LEMBAR PENGESAHAN	vii
ABSTRAK	viii
ABSTRACT.....	ix
KATA PENGANTAR.....	x
DAFTAR ISI.....	xi
NASKAH JURNAL	1
1. INTRODUCTION	1
2. IMPLEMENTATION.....	2
2.1 Configuration	3
3. TESTING, RESULT And ANALYSIS	3
3.1 High Availability	3
3.1.1 BFD Feature Using System Shutdown	4
3.1.2 BFD Feature Using Physic Shutdown	5
3.2 Packet Loss	6
3.3 Latency.....	8
4. CONCLUSION.....	8
5. REFERENCES	9
KERTAS KERJA.....	10
BAGIAN 1. LITERATUR REVIEW	11
1.1 Metro Ethernet	11
1.2 Kabel Fiber Optic.....	11
1.3 Virtual Private Networks	12
1.4 MPLS (Multiprotocol Label Switching).....	13

1.5	Open Shortest Path First (OSPF)	15
1.6	Bidirectional Forwarding Detection (BFD)	15
1.7	Parameter Performansi Layanan L2VPN Berbasis MPLS	17
1.7.1	Throughput	17
1.7.2	Packet Loss	17
1.7.3	Latency	18
1.7.4	Jitter	18
1.7.5	Availability	19
2	Penelitian Terkait	19
BAGIAN 2 ANALISIS DAN PERANCANGAN.....		21
2.1	Pengamatan Topologi Jaringan	21
2.2	Konfigurasi Protocol	24
2.3	Implementasi BFD	26
BAGIAN 3 SOURCE CODE		27
3.1	Konfigurasi IP Address dan Interfaces	27
3.2	Konfigurasi L2VPN Service	28
3.3	Konfigurasi Protocol MPLS	30
3.4	Konfigurasi OSPF	33
3.5	Konfigurasi BFD.....	35
BAGIAN 4 TAHAPAN EKSPERIMEN		39
4.1	Pencarian Data	39
4.2	Identifikasi Masalah	39
4.3	Perencanaan Topologi Jaringan MPLS	39
4.4	Konfigurasi Protokol MPLS	40
4.5	Implementasi BFD	40
4.6	Pengujian Fitur BFD	40
4.7	Analisa Fitur BFD	40
BAGIAN 5 HASIL SEMUA EKSPERIMEN.....		41
5.1	High Availability	41
5.1.1	Pengujaan Shutdown Sistem.....	41
5.1.1.1	Limitasi Bandwidth 5 Mbps	42
5.1.1.2	Limitasi Bandwidth 10 Mbps	45
5.1.1.3	Limitasi Bandiwdth 20 Mbps	48
5.1.1.4	Limitasi Bandwidth 5 Mbps	50
5.1.1.5	Limitasi Bandwidth 10 Mbps	53
5.1.1.6	Limitasi Bandwidth 20 Mbps	56
5.1.2	Pengujian Shutdown Fisik	58
5.1.2.1	Limitasi Bandwidth 5 Mbps	58

5.1.2.2	Limitasi Bandwidth 10 Mbps	61
5.1.2.3	Limitasi Bandwidth 20 Mbps	63
5.1.2.4	Limitasi Bandwidth 5 Mbps	65
5.1.2.5	Limitasi Bandwidth 10 Mbps	68
5.1.2.6	Limitasi Bandwidth 20 Mbps	71
5.2	Packet Loss	74
5.2.1	Shutdown Sistem	74
5.2.1.1	Menggunakan Fitur BFD	75
5.2.1.2	Tanpa Menggunakan Fitur BFD	76
5.2.2	Shutdown Fisik	78
5.2.2.1	Menggunakan Fitur BFD	78
5.2.2.2	Tanpa Menggunakan Fitur BFD	79
5.3	Latency	81
5.3.1	Shutdown Sistem	82
5.3.2	Shutdown Fisik	82
5.4	Kesimpulan	83



Redundancy Analysis VPN Service IP/MPLS Based on Metro Ethernet Network Using BFD Feature

Sri Dianing Asri, S.T, M.Kom Mercu Buana
University Jakarta, Indonesia
dianing.asri@mercubuana.ac.id

Irawan Febriyanto Mercu Buana
University Depok, Indonesia
Irawanfebriy19@gmail.com

ABSTRACT

In daily operations company that has some of the branch offices, required to communicate with and other offices as well. Because every data transaction that must be known by the headquarters and branch office data there should get it from headquarters. But the data are transacted must be kept confidential. To communicate such data between Office must be interconnected with the need for confidentiality of data is very high, then the VPN (Virtual Private Network) is one of the solutions for connecting each Office and keep confidentiality of data is transacted. PT NettoCyber Indonesia is a major internet service provider that can provide VPN service for customers that have branch offices should be connected. By using Metro Ethernet networks IP/MPLS-based PT NettoCyber Indonesia can guarantee high availability in an SLA (Service Level Agreement). For maintaining the SLA with the customer then any Metro Ethernet networks have redundancy. Where if one backbone links are problem, it will soon be moved to other backbone available with failover process doesn't take a long time. So that it can keep the High Availability to customer.

Keywords

VPN, Metro Ethernet, Redundancy, Failover

1. INTRODUCTION

Nowadays use of data requires a stable reliable stability network connection and high availability to support work activities all the time.

In a company or other institution that has many branches office, which requires head office direct connect to branch office mostly use VPN (Virtual Private Networks) connection to run data communications inter office. VPN provide a solution private network through public network that can connect any office without have to build a physical networks. And the requirements of any ICT (Information and Communication Technologies) system regarding data protection and information security are constantly increasing[1]. VPN technology is present as one of solution to secure data transferred through the internet network. This technology allows data to be sent in the form encrypted and can only be read when it has been decrypted so that it cannot be easily controlled by a third party. Data security and the closure of data transmission from unauthorized access to transmission on the internet are the main standards in VPN[2]. VPN can be implemented on a various types of networks, Metro Ethernet is one of them.

Metro Ethernet is Wide Area Network (WAN) carrier class covering Metropolitan Area with Ethernet for communication media. Metro Ethernet can connect some Local Area Network (LAN) in different location with data capacity transport up to 10 Gb/s. In transporting data and VPN services, Metro Ethernet progression by applying Multiprotocol Label Switching (MPLS). MPLS provide routing optimization on end to end in Metro Ethernet network. With labeling method MPLS can provide data transfer be faster, efficient and powerful. MPLS is a label that was created to be used communication between routers so that the router can build label-to-label mapping independently. The label is placed on an IP package, which is possible router to continue communication by looking at the label and not the destination IP address. The package is forwarded by the label and switch without process by IP switching. MPLS labels are used to forward packages and no longer Destination IP address have caused the popularity of MPLS. Benefits-like this as better integration than IP on ATM and MPLS popular virtual private or VPN networks[3]. MPLS is an advanced forwarding scheme. It extends routing with respect to packet forwarding and path controlling[4]. MPLS technology offers more flexibility by placing labels on IP packets and using label switched paths (LSPs) to transmit packets through the network[5]. MPLS has an architecture, which supports its functions. In this paper, the MPLS architecture is divides into three parts: MPLS Definition, MPLS header, and MPLS signaling protocols[6]. The Internet Engineering Task Force (IETF) standardizes a solution such as Multiprotocol Label Switching (MPLS) as an expansion of VPN tp increase the performance of forwarding and traffic engineering intelligence on packet based network[7]

On the convergence of a IP/MPLS networks requires high availability to fulfill SLA (Service Level Agreement) for customers. On this matter NettoCyber Indonesia Company as a Internet Service Provide (ISP) already have Metro Ethernet network with fiber optic media with 10 Gb/s on every POP (Point of Presence) which redundancy to purpose provide high SLA to customers. Fiber optic systems are used worldwide for broadband networks. It is a method of transmitting information from one place to another by using light pulses through an optical fiber. Its main benefits are low loss, higher data rates, can be used up to large distances, used in light prone areas, no crosstalk, higher reliability etc[8]

Current conditions on NettoCyber Indonesia Company has physic and protocol redundancy, protocol used is OSPF (Open Shortest Path First) with function triggered if one of link failure will failover to other link[9]. Failover is the technique of applying some path to reach the goal. There are two links, namundalam normal circumstances there is only one link that was used in the other is used in as a backup when the main

link link interrupted[10]. Within OSPF protocol deployment still found deficiency. In several parameters shows packet loss, latency and jitter high enough which need a few seconds on failover process. OSPF is a link state protocol which is created due to requirements such as software or hardware independencies, the need for the dynamic algorithms, the ability to use other cost metrics to determine the optimal route, the need for service quality support, load balancing, the need for hierarchical routing, increased security level, Support for tunnel creation mechanism[11]. From that found, will analyzed BFD (Bidirectional Forwarding Detection) with very quick system failure identifying on device or networks only milliseconds. So failover process faster and smoother. Bidirectional Forwarding Detection (BFD) is a network protocol used to detect faults between two forwarding engines. BFD provides low-overhead, low-latency detection of faults even on physical media that don't support failure detection of any kind, such as ethernet, virtual circuits, tunnels and MPLS LSPs[12]. BFD provides low-overhead, short-duration detection of failures in the path between adjacent forwarding engines, including the interfaces, data links, and to the extent possible the forwarding engines themselves. BFD has already been deployed in the MPLS-based networks and demonstrated to be in effect[12]. Of these advantages NettoCyber Indonesia Company applying that feature on protocol used in Metro Ethernet networks.

2. IMPLEMENTATION

BFD (Bidirectional Forwarding Detection) feature is a simple mechanism that is designed to detection failure on the network. In principle it works, BFD form grooves Exchange communication by sending Hello packets with the specified interval, the failure on the device when the device is detected the neighboring routing stops receiving a reply Hello packet after interval for BFD are determined and started working with various network environment and topology, BFD provides faster detection. With the advantages of the BFD allows when applying at the interface of the device that is running routing protocol IGP that support performance-based MPLS L2VPN services.

In observations on existing topology then it will be known performance parameters by making simulations according to the conditions of existing networks. In this simulation will be tested from most existing topology on Metro Ethernet network at PT. NettoCyber Indonesia (VELO Networks) Mega Kuningan area, with purpose of found parameters before using the L2VPN services performance features of BFD. Below are the existing Ethernet Metro network topology at PT. NettoCyber Indonesia (VELO Networks) area of Mega Kuningan :

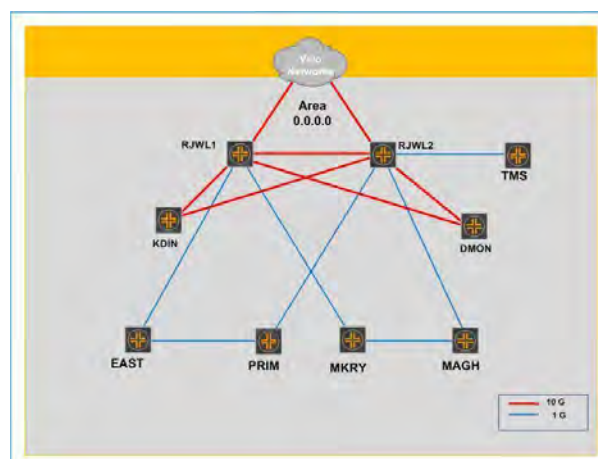


Fig 1: Metro E Network Topology NettoCyber Indonesia Company on Mega Kuningan Area

On Fig 1 contained some devices installed on buildings in Mega Kuningan Area South Jakarta. Below Table 1 show devices name and buildings:

Table 1. Device Name and Building Name

Device Name	Building Name
RJWL1	Menara Rajawali
RJWL2	Menara Rajawali
KDIN	Menara Kadin
DMON	Menara Danamon
EAST	THE EAST
PRIM	Menara Prima
MKRY	Menara Karya
MAGH	Menara Anugerah

After known that existing topology choose sample topology on area KDIN, RJWL1, RJWL2 for simulation with purposed to get parameters about performance L2VPN by not using BFD feature. Topology on that area:

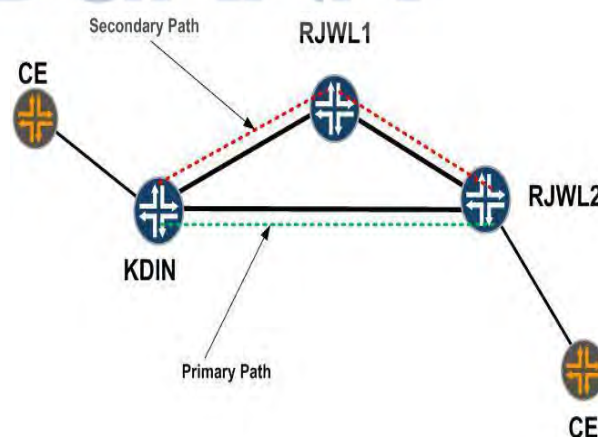


Fig 2: Topology on KDIN, RJWL1 and RJWL2 Area

From Fig 2 found primary path customer through RJWL2 line and when primary link to RJWL2 failure so will failover to

RJWL1 previously then to RJWL2 through secondary path. On that failover process will be observed result of network availability, packet loss and latency on L2VPN Services.

To know that parameters will simulated according topology on Fig 2 however device name changed to Lab_2 for KDIN as PE, Lab_3 for RJWL1 as P and Lab_4 for RJWL2 as PE.

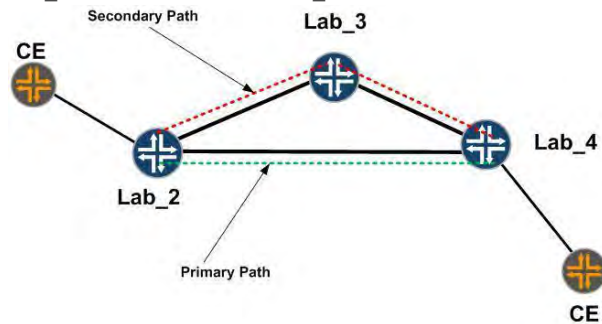


Fig 3: Simulation Lab Topology

Simulation will adjust configuration IGP Protocol, LDP, BFD Feature, L2VPN Service and analyze BFD Feature impact toward L2VPN Services.

2.1 CONFIGURATION

Simulation impact on BFD feature towards L2VPN services, requires configuration on devices suitable with simulation topology in Fig 3. Before simulation protocol configuration on that topology, the first to do is assign IP address and interfaces allocation. Below table for that IP address and interface requires:

Table 2. IP address and Interfaces Allocation

Device Name	IP Address	Interface Name	Port
LAB_2	10.10.42.2/29	lab4-1/1/22	12
	10.10.32.2/29	lab4-1/1/12	13
	2.2.2.2/32	system	
LAB_3	10.10.43.3/29	lab4-1/1/28	28
	10.10.32.3/29	lab4-1/1/13	12
	3.3.3.3/32	system	
LAB_4	10.10.43.4/29	lab4-1/1/28	28
	10.10.42.4/29	lab4-1/1/28	22
	4.4.4.4/32	system	

To make it easier comprehension of IP address and interfaces allocation on simulation lab topology. Fig 4 will explain in more detail about simulation lab topology with using IP address and interfaces allocation

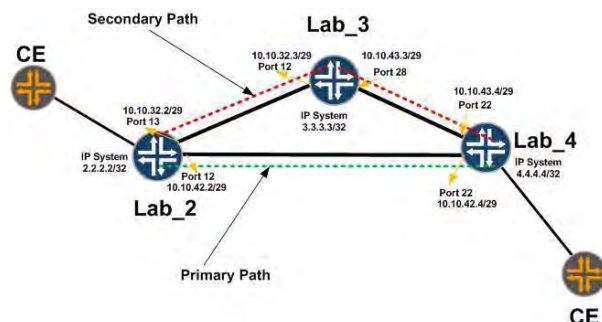


Fig 4: IP address and Interfaces Name Allocation

After IP address and interfaces name allocation defined, next step is configuration on devices involves IP address and interfaces, OSPF protocol, LDP, L2VPN services and BFD feature. When all configuration ready, BFD feature applied each interfaces and activated on OSPF protocol. According to purpose in order failure detection and failover process faster. Fig 5 show simulation lab topology after all configuration ready and running well.

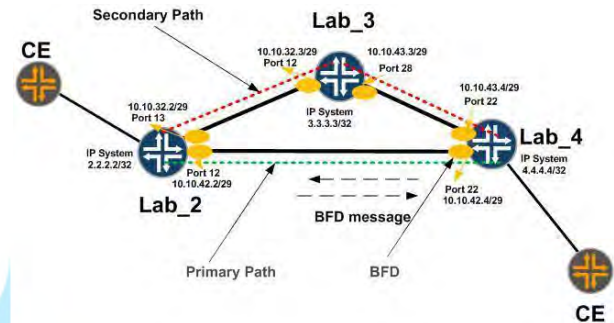


Fig 5: Simulation Lab Topology with All Configuration Running

3. Testing, Result and Analysis

BFD feature testing on PE, while CE will monitor whether BFD feature running well in IGP so affect to L2VPN services quality on CE with purpose to get data and information when failover process from primary path to secondary path.

Phase testing BFD feature in PE namely shutdown interfaces by system and physically. Physical shutdown simulated when failure caused physical device like interfaces port or cables.

In CE1 side there is notebook direct against CE1 devices to observe and monitor downtime, packet loss, latency and throughput.

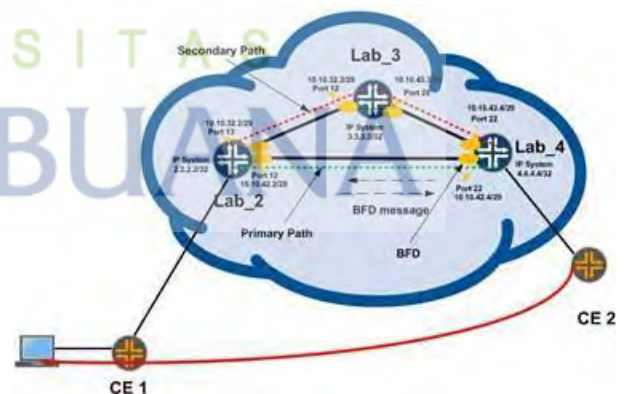


Fig 6: Implement and Testing BFD Feature

Based on testing on simulation topology found result parameters as High Availability, packet loss and latency by implement BFD feature and didn't use BFD feature. And below will explain detail result and analysis on each parameters

3.1 High Availability

High availability result obtained by system and physic shutdown using bandwidth limitation 5 Mbps, 10 Mbps and

20 Mbps in time range 1 hour. That range time can describe with *Mean Time Between Failures (MTBF)*.

System and physic shutdown method by taking parameters to find out average time value recovery or *Mean Time To Recovery (MTTR)*. Stopwatch used as time measuring device and ping time as ICMP delivery packet. MTTR measurement by counting downtime duration or Request Time Out (RTO) packet when failover process. Mathematically availability calculation can be calculated using formula

$$\text{Availability} = \frac{\text{MTTF}}{\text{MTTF} + \text{MTTR}} \times 100\%$$

3.1.1 BFD Feature Using System Shutdown

Below testing result downtime duration on BFD feature using system shutdown method with bandwidth 5 Mbps, 10 Mbps and 20 Mbps. Testing repeat until 5 times explain on Fig 7 – Fig 9 and Table 3 – Table 5

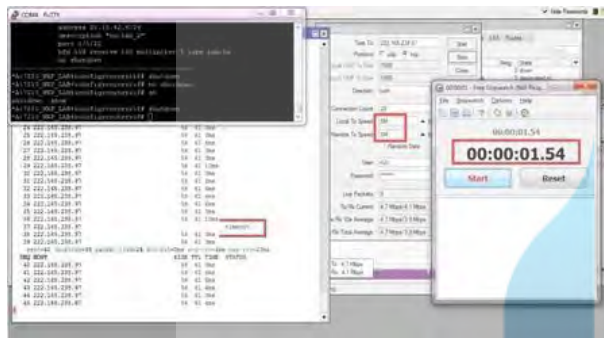


Fig 7: Result BFD Feature System Shutdown Bandwidth 5 Mbps

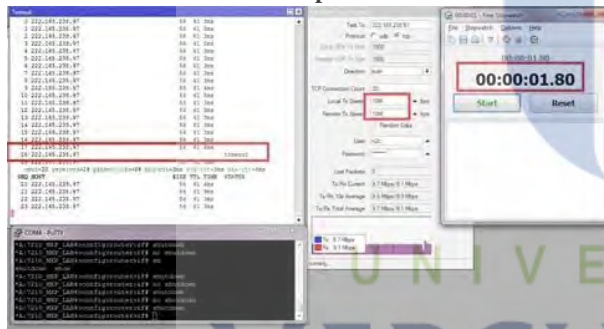


Fig 8: Result BFD Feature System Shutdown Bandwidth 10 Mbps

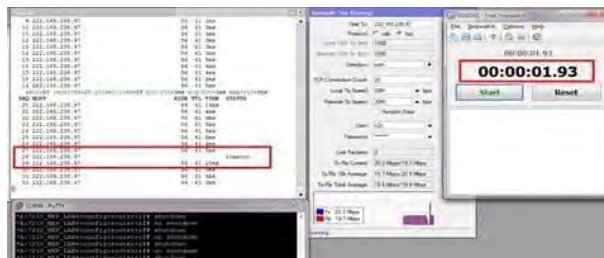


Fig 9: Result BFD Feature System Shutdown Bandwidth 20 Mbps

Table 3. Availability Service BFD Feature System Shutdown Bandwidth 5 Mbps

Result	Bandwidth	MTTF (Second)	MTTR (Second)
First	5 Mbps	3600	1.54

Second	5 Mbps	3600	1.42
Third	5 Mbps	3600	1.16
Fourth	5 Mbps	3600	1.22
Fifth	5 Mbps	3600	1.15
Average			1.298

Table 4. Availability Service BFD Feature System Shutdown Bandwidth 10 Mbps

Result	Bandwidth	MTTF (Second)	MTTR (Second)
First	10 Mbps	3600	1.17
Second	10 Mbps	3600	1.22
Third	10 Mbps	3600	1.25
Fourth	10 Mbps	3600	1.8
Fifth	10 Mbps	3600	1.09
Average			1.306

Table 5. Availability Service BFD Feature System Shutdown Bandwidth 20 Mbps

Result	Bandwidth	MTTF (Second)	MTTR (Second)
First	20 Mbps	3600	1.93
Second	20 Mbps	3600	1.81
Third	20 Mbps	3600	1.29
Fourth	20 Mbps	3600	1.86
Fifth	20 Mbps	3600	1.97
Average			1.772

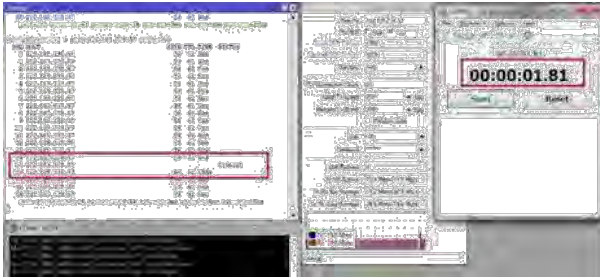
Based on testing result bandwidth 5 Mbps BFD Feature using shutdown system. Failover process test show availability can reach 99,9639%, bandwidth 10 Mbps 99,9637% and 99,950% in 20 Mbps bandwidth, obtain from formula:

$$\text{Availability} = \frac{3600}{3600 + 1.298} \times 100\% = 99,9639\% \text{ (5 Mbps)}$$

$$\text{Availability} = \frac{3600}{3600 + 1.306} \times 100\% = 99,9637\% \text{ (10 Mbps)}$$

$$\text{Availability} = \frac{3600}{3600 + 1.772} \times 100\% = 99,950\% \text{ (20 Mbps)}$$

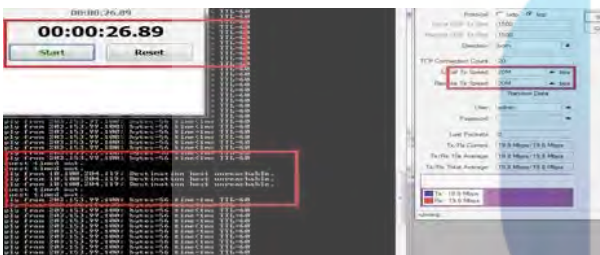
Further after testing and get result downtime duration failover test using BFD feature on system shutdown. Next action test for downtime duration failover test didn't use BFD feature but still system shutdown method and repeat until 5 times. Below Fig 10 – Fig 12 and Table 6 – Table 8 will explain the detail and different result if compare with BFD feature.



**Fig 10: Result Non BFD Feature System Shutdown
Bandwidth 5 Mbps**



**Fig 11: Result Non BFD Feature System Shutdown
Bandwidth 10 Mbps**



**Fig 12: Result Non BFD Feature System Shutdown
Bandwidth 20 Mbps**

**Table 6. Availability Service BFD Feature System
Shutdown Bandwidth 5 Mbps**

Result	Bandwidth	MTTF (Second)	MTTR (Second)
First	5 Mbps	3600	24.56
Second	5 Mbps	3600	24.79
Third	5 Mbps	3600	22.29
Fourth	5 Mbps	3600	22.29
Fifth	5 Mbps	3600	24.92
Average			23.774

**Table 7. Availability Service BFD Feature System
Shutdown Bandwidth 5 Mbps**

Result	Bandwidth	MTTF (Second)	MTTR (Second)
First	10 Mbps	3600	23.7
Second	10 Mbps	3600	27.76
Third	10 Mbps	3600	23.73
Fourth	10 Mbps	3600	24.33
Fifth	10 Mbps	3600	25.08
Average			25.72

**Table 8. Availability Service BFD Feature System
Shutdown Bandwidth 20 Mbps**

Result	Bandwidth	MTTF	MTTR
--------	-----------	------	------

		(Second)	(Second)
First	10 Mbps	3600	24.06
Second	10 Mbps	3600	23.96
Third	10 Mbps	3600	26.89
Fourth	10 Mbps	3600	25.31
Fifth	10 Mbps	3600	22.33
Average			24.51

Based on result seen that didn't use BFD feature availability cant optimal although downtime duration on failover process under 1 minutes but impact to customer who requires high availability connection. In bandwidth 5 Mbps availability reach 99,343%, 10 Mbps 99,290% and 20 Mbps 99,323%.

$$\text{Availability} = \frac{3600}{3600 + 23.774} \times 100\% = 99,343\% \text{ (5 Mbps)}$$

$$\text{Availability} = \frac{3600}{3600 + 25.72} \times 100\% = 99,290\% \text{ (10 Mbps)}$$

$$\text{Availability} = \frac{3600}{3600 + 24.51} \times 100\% = 99,323\% \text{ (20 Mbps)}$$

3.1.2 BFD Feature Using Physic Shutdown

Testing BFD feature using physical shutdown on failover process to obtain result downtime duration almost the same process but the difference is unplug cable on device interface for this testing. So directly see the result of BFD feature and non BFD feature with Physic Shutdown

**Table 9. Availability Service BFD Feature Physical
Shutdown Bandwidth 5 Mbps**

Result	Bandwidth	MTTF (Second)	MTTR (Second)
First	5 Mbps	3600	1.47
Second	5 Mbps	3600	1.83
Third	5 Mbps	3600	1.25
Fourth	5 Mbps	3600	1.62
Fifth	5 Mbps	3600	1.61
Average			1.556

$$\text{Availability} = \frac{3600}{3600 + 1.556} \times 100\% = 99,956\%$$

**Table 10. Availability Service BFD Feature Physical
Shutdown Bandwidth 10 Mbps**

Result	Bandwidth	MTTF (Second)	MTTR (Second)
First	10 Mbps	3600	1.5
Second	10 Mbps	3600	1.66
Third	10 Mbps	3600	1.79
Fourth	10 Mbps	3600	1.43
Fifth	10 Mbps	3600	1.71
Average			1.618

$$\text{Availability} = \frac{3600}{3600 + 1.618} \times 100\% = 99,955\%$$

Table 11. Availability Service BFD Feature Physical Shutdown Bandwidth 20 Mbps

Result	Bandwidth	MTTF (Second)	MTTR (Second)
First	20 Mbps	3600	1.72
Second	20 Mbps	3600	1.31
Third	20 Mbps	3600	1.64
Fourth	20 Mbps	3600	1.95
Fifth	20 Mbps	3600	1.47
Average			1.62

$$\text{Availability} = \frac{3600}{3600 + 1.62} \times 100\% = 99,955\%$$

After get result of BFD feature on physical shutdown. Next step is test and result non BFD feature on physical shutdown. That data and information explain on Table 12 – Table 14

Table 12. Availability Service Non BFD Feature System Shutdown Bandwidth 5 Mbps

Result	Bandwidth	MTTF (Second)	MTTR (Second)
First	5 Mbps	3600	22.5
Second	5 Mbps	3600	23.22
Third	5 Mbps	3600	23.3
Fourth	5 Mbps	3600	24.6
Fifth	5 Mbps	3600	23.95
Average			23.514

$$\text{Availability} = \frac{3600}{3600 + 23.514} \times 100\% = 99,346\%$$

Table 13. Availability Service Non BFD Feature System Shutdown Bandwidth 10 Mbps

Result	Bandwidth	MTTF (Second)	MTTR (Second)
First	10 Mbps	3600	24.14
Second	10 Mbps	3600	22.74
Third	10 Mbps	3600	23.52
Fourth	10 Mbps	3600	23.76
Fifth	10 Mbps	3600	23.73
Average			23.578

$$\text{Availability} = \frac{3600}{3600 + 23.578} \times 100\% = 99,345\%$$

Table 14. Availability Service Non BFD Feature System Shutdown Bandwidth 20 Mbps

Result	Bandwidth	MTTF (Second)	MTTR (Second)
First	20 Mbps	3600	26.02
Second	20 Mbps	3600	24.14
Third	20 Mbps	3600	23.57

Fourth	20 Mbps	3600	23.08
Fifth	20 Mbps	3600	22.74
Average			23.91

$$\text{Availability} = \frac{3600}{3600 + 23.91} \times 100\% = 99,335\%$$

On testing the system shutdown with the use of BFD monitored duration shorter downtimes i.e. Duration minimum downtime of about 1.09 seconds and a maximum of 1.97 seconds. Whereas by not using BFD found minimum downtime of about 22.29 seconds and a maximum of 27.76 seconds. And from calculations made on testing the physical shutdown, found services-services by using the features of the BFD has roughly 0.6% higher compared to services-services that do not use the BFD.

3.2 Packet Loss

The test results either on the system shutdown or shutdown with the physical limitations of bandwidth at 5 Mbps, 10 Mbps, and 20 Mbps is found by using the features of the BFD on when failover occurs only packet loss 1% whereas without using BFD in system shutdown test found the minimum packet loss at 4.6% and 5.8% at the maximum. This testing is by the method of observation of the ICMP packet of 56 bytes on any one package with 100 times the delivery on time of traffic utilization reaches a maximum

Mathematically packet loss can counting by formula. To know packet loss BFD feature on system shutdown show in below table

Table 15. Packet Loss Services 5 Mbps BFD Feature System Shutdown

Result	Bandwidth	Packet Send (Bytes)	Packet Receive (Bytes)	Packet Loss
First	5 Mbps	5600	5544	1%
Second	5 Mbps	5600	5544	1%
Third	5 Mbps	5600	5544	1%
Fourth	5 Mbps	5600	5544	1%
Fifth	5 Mbps	5600	5544	1%
Average				1%

$$\text{Paket Loss} = \frac{5600 - 5544 \times 100\%}{5600} = 1\%$$

Table 16. Packet Loss Services 10 Mbps BFD Feature System Shutdown

Result	Bandwidth	Packet Send (Bytes)	Packet Receive (Bytes)	Packet Loss
First	10 Mbps	5600	5544	1%
Second	10 Mbps	5600	5544	1%
Third	10 Mbps	5600	5544	1%
Fourth	10 Mbps	5600	5544	1%
Fifth	10 Mbps	5600	5544	1%
Average				1%

$$\text{Paket Loss} = \frac{5600 - 5544 \times 100\%}{5600} = 1\%$$

Table 17. Packet Loss Services 20 Mbps BFD Feature System Shutdown

Result	Bandwidth	Packet Send (Bytes)	Packet Receive (Bytes)	Packet Loss
First	20 Mbps	5600	5544	1%
Second	20 Mbps	5600	5544	1%
Third	20 Mbps	5600	5544	1%
Fourth	20 Mbps	5600	5544	1%
Fifth	20 Mbps	5600	5544	1%
Average				1%

$$\text{Paket Loss} = \frac{5600 - 5544 \times 100\%}{5600} = 1\%$$

The values derived from mathematical calculations packet loss by didn't using BFD on testing system shutdown, below

Table 18. Packet Loss Services 5 Mbps Non BFD Feature System Shutdown

Result	Bandwidth	Packet Send (Bytes)	Packet Receive (Bytes)	Packet Loss
First	5 Mbps	5600	5320	1%
Second	5 Mbps	5600	5320	1%
Third	5 Mbps	5600	5377	1%
Fourth	5 Mbps	5600	5377	1%
Fifth	5 Mbps	5600	5320	1%
Average		5600	5342.8	4.6%

$$\text{Paket Loss} = \frac{5600 - 5342.8 \times 100\%}{5600} = 4.6\%$$

Table 19. Packet Loss Services 10 Mbps Non BFD Feature System Shutdown

Result	Bandwidth	Packet Send (Bytes)	Packet Receive (Bytes)	Packet Loss
First	10 Mbps	5600	5376	1%
Second	10 Mbps	5600	5208	1%
Third	10 Mbps	5600	5208	1%
Fourth	10 Mbps	5600	5320	1%
Fifth	10 Mbps	5600	5320	1%
Average		5600	5286.4	5.6%

$$\text{Paket Loss} = \frac{5600 - 5286.4 \times 100\%}{5600} = 5.6\%$$

Table 19. Packet Loss Services 20 Mbps Non BFD Feature System Shutdown

Result	Bandwidth	Packet Send (Bytes)	Packet Receive (Bytes)	Packet Loss
First	20 Mbps	5600	5208	1%
Second	20 Mbps	5600	5320	1%

Third	20 Mbps	5600	5208	1%
Fourth	20 Mbps	5600	5320	1%
Fifth	20 Mbps	5600	5320	1%
Average		5600	5275.2	5.8%

$$\text{Paket Loss} = \frac{5600 - 5275.2 \times 100\%}{5600} = 5.8\%$$

On testing the physical shutdown found minimum packet loss is 5% and 5.4% with maximum values without using BFD, value packet loss that much higher compared to the BFD feature to failover quickly so that packet loss only 1%. Seen on Fig 13 manual testing shutdown physic by unplug fiber optic cable on device interface LAB_2, LAB_3 and LAB_4.



Fig 13: Unplug Fiber Optic Cable on Device Interfaces

Further testing physic shutdown finish by unplug cable repeated until 5 times. Packet loss detail when failover process in 5, 10 and 20 Mbps bandwidth using BFD Feature explain on following table

Table 20. Packet Loss Services 5 Mbps BFD Feature Physical Shutdown

Result	Bandwidth	Packet Send (Bytes)	Packet Receive (Bytes)	Packet Loss
First	5 Mbps	5600	5544	1%
Second	5 Mbps	5600	5544	1%
Third	5 Mbps	5600	5544	1%
Fourth	5 Mbps	5600	5544	1%
Fifth	5 Mbps	5600	5544	1%
Average				1%

$$\text{Paket Loss} = \frac{5600 - 5544 \times 100\%}{5600} = 1\%$$

Table 21. Packet Loss Services 10 Mbps BFD Feature Physical Shutdown

Result	Bandwidth	Packet Send (Bytes)	Packet Receive (Bytes)	Packet Loss
First	10 Mbps	5600	5544	1%
Second	10 Mbps	5600	5544	1%
Third	10 Mbps	5600	5544	1%
Fourth	10 Mbps	5600	5544	1%

Fifth	10 Mbps	5600	5544	1%
Average				1%

$$\text{Paket Loss} = \frac{5600 - 5544 \times 100\%}{5600} = 1\%$$

Table 22. Packet Loss Services 10 Mbps BFD Feature Physical Shutdown

Result	Bandwidth	Packet Send (Bytes)	Packet Receive (Bytes)	Packet Loss
First	20 Mbps	5600	5544	1%
Second	20 Mbps	5600	5544	1%
Third	20 Mbps	5600	5544	1%
Fourth	20 Mbps	5600	5544	1%
Fifth	20 Mbps	5600	5544	1%
Average				1%

$$\text{Paket Loss} = \frac{5600 - 5544 \times 100\%}{5600} = 1\%$$

When physical shutdown finish on device interfaces using BFD feature. Next step is to compare physical shutdown devices interfaces by didn't use BFD feature to get values of packet loss. The comparison show on following table

Table 23. Packet Loss Services 5 Mbps Non BFD Feature Physical Shutdown

Result	Bandwidth	Packet Send (Bytes)	Packet Receive (Bytes)	Packet Loss
First	5 Mbps	5600	5264	6%
Second	5 Mbps	5600	5320	5%
Third	5 Mbps	5600	5320	5%
Fourth	5 Mbps	5600	5320	5%
Fifth	5 Mbps	5600	5320	5%
Average		5600	5308.8	5%

$$\text{Paket Loss} = \frac{5600 - 5308.8 \times 100\%}{5600} = 5\%$$

Table 24. Packet Loss Services 10 Mbps Non BFD Feature Physical Shutdown

Result	Bandwidth	Packet Send (Bytes)	Packet Receive (Bytes)	Packet Loss
First	10 Mbps	5600	5320	5%
Second	10 Mbps	5600	5208	7%
Third	10 Mbps	5600	5320	5%
Fourth	10 Mbps	5600	5320	5%
Fifth	10 Mbps	5600	5320	5%
Average		5600	5297.6	5.4%

$$\text{Paket Loss} = \frac{5600 - 5297.6 \times 100\%}{5600} = 5.4\%$$

Table 25. Packet Loss Services 10 Mbps Non BFD Feature Physical Shutdown

Result	Bandwidth	Packet Send (Bytes)	Packet Receive (Bytes)	Packet Loss
First	20 Mbps	5600	5264	6%
Second	20 Mbps	5600	5432	3%
Third	20 Mbps	5600	5320	5%
Fourth	20 Mbps	5600	5208	7%
Fifth	20 Mbps	5600	5377	4%
Average		5600	5320.2	5.2%

$$\text{Paket Loss} = \frac{5600 - 5320.2 \times 100\%}{5600} = 5.2\%$$

3.3 Latency

After all process system and physical shutdown finished, found latency when failover process. The result maintained its position of using BFD feature and without BFD feature. System shutdown using BFD feature found latency minimum approximately 13 ms and maximum 26 ms. Whereas without BFD feature get the value of latency minimum approximately 148 ms and 1000 ms maximum latency. Show on following table

Table 25. Latency Result by System shutdown

Bandwidth	BFD (ms)	Non BFD (ms)
5 Mbps	13	148
10 Mbps	26	1000
20 Mbps	18	1000

On testing the physical shutdown, latency with the use of BFD feature found the minimum value about 15 ms and maximum value 18 ms. the Results are pretty much different from the results of testing the latency without using BFD feature, that found the minimum value about 3 ms and a maximum value of 1002 ms. From those results do not affect significant BFD feature on latency after the failover occurs.

Table 25. Latency Result by Physical shutdown

Bandwidth	BFD (ms)	Non BFD (ms)
5 Mbps	18	6
10 Mbps	16	3
20 Mbps	15	1002

4. CONCLUSION

In this research can concluded that use of BFD feature on Metro Ethernet network with L2VPN services on NettoCyber Indonesia Company influential profitable in performances and redundancy by result all of testing explain that:

BFD feature implementation running well on Metro Ethernet network with L2VPN services so can provide to customer better than before using BFD feature

By using BFD feature increased availability services compared without using BFD feature. It almost

significant for customer who requires high availability of services

When failover process using BFD feature on system shutdown and physical shutdown found packet loss only 1% without BFD feature can reach 5,8% and stable latency using BFD feature, but unstable without BFD feature until 1000 ms

BFD feature implementation quite significant when failover process, especially when one of the link problem and failover in customer rush/offices hour to other link not too affected critically and still delivered high availability services.

no. 1, pp. 30–39, 2016.

- [11] M. Reza, M. Naderi, and R. Javidan, “A New Architecture to Improve Multimedia QoS over Software Defined Networks,” *Int. J. Comput. Appl.*, vol. 179, no. 23, pp. 14–19, 2018.
- [12] H. R. Arkian, R. E. Atani, A. Pourkhalili, and S. Kamali, “A stable clustering scheme based on adaptive multiple metric in vehicular Ad-hoc Networks,” *J. Inf. Sci. Eng.*, vol. 31, no. 2, pp. 361–386, 2015.

5. REFERENCES

- [1] N. Stoianov, M. Urueña, M. Niemiec, P. Machnik, and G. Maestro, “Integrated security infrastructures for law enforcement agencies,” *Multimed. Tools Appl.*, vol. 74, no. 12, pp. 4453–4468, 2015.
- [2] 林伸行,
“病院・介護施設におけるノロウイルス感染症の
拡大防止対策を
目的とした吐物の飛散状況に関する研究 No
Title,” *感染症誌*, vol. 91, no. 2, pp. 399–404, 2017.
- [3] B. Nugraha, T. Elektro, and T. Elektro, “Jurnal
Teknologi Elektro , Universitas Mercu Buana ISSN :
2086 - 9479 ANALISA PERBANDINGAN PERFORMA
TEKNOLOGI MPLS-TP (MULTIPROTOCOL LABEL
SWITCHING - TRANSPORT PROFILE) DENGAN
TOPOLOGI RING DAN POINT-TO-POINT,” vol. 8, no. 2,
pp. 138–144, 2017.
- [4] X. Xiao, A. Hannan, B. Bailey, and L. M. Ni,
“Traffic engineering with MPLS in the Internet,”
IEEE Netw., vol. 14, no. 2, pp. 28–33, 2000.
- [5] K. Stefan and A. Binzenh, “MPLS Traffic
Engineering in OSPF Networks - A combined
approach.”
- [6] A. S. G. Allah and N. M. El-shennawy, “Admission
Control Algorithm for MPLS-TE Networks,” vol.
160, no. 5, pp. 11–16, 2017.
- [7] D. J. Casa *et al.*, “In Pr es s,” *Lung*, vol. 47, no. 1,
pp. 1–23, 2011.
- [8] A. Parmar, “Study of Inter-Satellite Optical Wireless
Communication System with different Modulation
Techniques,” vol. 182, no. 6, pp. 24–28, 2018.
- [9] B. Rifai and E. Supriyanto, “Management System
Failover Dengan Routing Dinamis Open Shortest
Path First Dan Border Gateway Protocol,” *JITK
(Jurnal Ilmu Pengetah. Dan Teknol. Komputer)*, vol.
3, no. 1, pp. 39–46, 2017.
- [10] B. Yuliadi and A. Nugroho, “Rancangan Disaster
Recovery Pada Instansi Pendidikan Studi Kasus
Universitas Mercu Buana,” *J. Tek. Inform.*, vol. 9,



**Analisa Redundansi Servis VPN Berbasis IP/MPLS Pada Jaringan Metro Ethernet
Menggunakan Fitur BFD**

Tugas Akhir

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

Oleh:
Irawan Febriyanto
41514320012

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS MERCU BUANA

JAKARTA

2018

MERCU BUANA

LEMBAR PERNYATAAN ORISINALITAS

Yang bertanda tangan dibawah ini:

NIM : 41514320012

Nama : Irawan Febriyanto

Judul Tugas Akhir : Analisa Redundansi Servis VPN Berbasis IP/MPLS Pada Jaringan Metro Ethernet Menggunakan Fitur BFD

Menyatakan bahwa Laporan Tugas Akhir saya adalah hasil karya sendiri dan bukan plagiat. Apabila ternyata ditemukan didalam laporan Tugas Akhir saya terdapat unsur plagiat, maka saya siap untuk mendapatkan sanksi akademik yang terkait dengan hal tersebut.

Jakarta, 26 Desember 2018



Irawan Febriyanto

UNIVERSITAS
MERCU BUANA

SURAT PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR

Sebagai mahasiswa Universitas Mercu Buana, saya yang bertanda tangan di bawah ini :

Nama Mahasiswa : Irawan Febriyanto
NIM : 41514320012
Judul Tugas Akhir : Analisa Redundansi Servis VPN Berbasis IP/MPLS
Pada Jaringan Metro Ethernet Menggunakan Fitur
BFD

Dengan ini memberikan izin dan menyetujui untuk memberikan kepada Universitas Mercu Buana **Hak Bebas Royalti Noneksklusif** (*None-exclusive Royalty Free Right*) atas karya ilmiah saya yang berjudul diatas beserta perangkat yang ada (jika diperlukan).

Dengan Hak Bebas Royalti/Noneksklusif ini Universitas Mercu Buana berhak menyimpan, mengalihmedia/formatkan, mengelola dalam bentuk pangkalan data (*database*), merawat dan mempublikasikan tugas akhir saya.

Selain itu, demi pengembangan ilmu pengetahuan di lingkungan Universitas Mercu Buana, saya memberikan izin kepada Peneliti di Lab Riset Fakultas Ilmu Komputer, Universitas Mercu Buana untuk menggunakan dan mengembangkan hasil riset yang ada dalam tugas akhir untuk kepentingan riset dan publikasi selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Jakarta, 26 Desember 2018



Irawan Febriyanto

SURAT PERNYATAAN LUARAN TUGAS AKHIR

Sebagai mahasiswa Universitas Mercu Buana, saya yang bertanda tangan di bawah ini :

Nama Mahasiswa : Irawan Febriyanto
 NIM : 41514320012
 Judul Tugas Akhir : Analisa Redundansi Servis VPN Berbasis IP/MPLS Pada Jaringan Metro Ethernet Menggunakan Fitur BFD

Menyatakan bahwa Luaran Tugas Akhir saya adalah sebagai berikut :

No	Luaran	Jenis		Status	
1	Publikasi Ilmiah	Jurnal Nasional Tidak Terakreditasi		Diajukan	
		Jurnal Nasional Terakreditasi			
		Jurnal International Tidak Bereputasi		Diterima	V
		Jurnal International Bereputasi			
	Disubmit/dipublikasikan di :	Nama Jurnal	: International Journal of Computer Applications		
	ISSN	: 0975 – 8887			
2	Kertas Kerja, Merupakan material hasil penelitian sebagai kelengkapan Artikel Jurnal. Terdiri dari (minimal 4)	Literatur Review			[V]
		Hasil analisa & perancangan aplikasi			[V]
		Source code			[V]
		Data set			[]
		Tahapan eksperimen			[V]
		Hasil eksperimen seluruhnya			[V]
3	HAKI Disubmit / Terdaftar	HKI			Diajukan
		Paten			Tercatat
		No & Tanggal Permohonan	:		
		No & Tanggal Pencatatan	:		

Demikian pernyataan ini saya buat dengan sebenarnya.

Jakarta, 26 Desember 2018


 Irawan Febriyanto


LEMBAR PERSETUJUAN

Nama Mahasiswa : Irawan Febriyanto
NIM : 41514320012
Judul Tugas Akhir : Analisa Redundansi Servis VPN Berbasis IP/MPLS
Pada Jaringan Metro Ethernet Menggunakan Fitur
BFD

Tugas Akhir ini telah diperiksa dan disetujui

Jakarta, 26 Desember 2018

Menyetujui,



(Sri Dianing Asri, S.T., M.Kom)
Dosen Pembimbing

UNIVERSITAS
MERCU BUANA

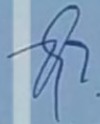
LEMBAR PERSETUJUAN

Nama Mahasiswa : Irawan Febriyanto
NIM : 41514320012
Judul Tugas Akhir : Analisa Redundansi Servis VPN Berbasis IP/MPLS
Pada Jaringan Metro Ethernet Menggunakan Fitur
BFD

Tugas Akhir ini telah diperiksa dan disetujui

Jakarta, 26 Desember 2018

Menyetujui,



(Sri Dianing Asri, S.T., M.Kom)
Dosen Pembimbing

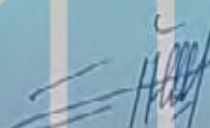
UNIVERSITAS
MERCU BUANA

LEMBAR PERSETUJUAN PENGUJI


NIM : 41514320012
Nama : Irawan Febriyanto
Judul Tugas Akhir : Analisa Redundansi Servis VPN Berbasis IP/MPLS
Pada Jaringan Metro Ethernet Menggunakan Fitur
BFD

Tugas Akhir ini telah diperiksa dan disidangkan sebagai salah satu persyaratan untuk memperoleh gelar Sarjana pada Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Mercu Buana.

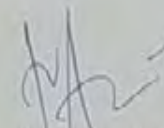
Jakarta, 22 Januari 2019



(Diky Firdaus, S.Kom, MM)
Ketua Penguji



(Umniy Salamah, MMSI)
Anggota Penguji 1



(Nur Ani, MMSI)
Anggota Penguji 2

UNIVERSITAS
MERCU BUANA

LEMBAR PENGESAHAN

NIM : 41514320012
Nama : Irawan Febriyanto
Judul Tugas Akhir : Analisa Redundansi Servis VPN Berbasis IP/MPLS Pada Jaringan Metro Ethernet Menggunakan Fitur BFD

Tugas Akhir ini telah diperiksa dan disidangkan sebagai salah satu persyaratan untuk memperoleh gelar Sarjana pada Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Mercu Buana.

Jakarta, 22 Januari 2019

Menyetujui,



(Sri Dianing Asri, ST, M.Kom)
Dosen Pembimbing

Mengetahui,

UNIVERSITAS

(Diky Firdaus, S.Kom, MM)

Koord. Tugas Akhir Teknik Informatika

(Desi Ramayanti, S.Kom, MT)

Ka. Prodi Teknik Informatika

MERCU BUANA

ABSTRAK

Nama : Irawan Febriyanto
NIM : 41514320012
Pembimbing TA : Sri Dianing Asri, S.T, M.Kom
Judul : Analisa Redundansi Servis VPN Berbasis IP/MPLS
Pada Jaringan Metro Ethernet Menggunakan Fitur
BFD

Dalam operasionalnya setiap perusahaan yang memiliki beberapa cabang, diharuskan untuk dapat saling berkomunikasi dengan kantor pusat dan juga kantor cabang lainnya. Dikarenakan setiap data transaksi yang harus diketahui oleh kantor pusat dan ada data yang kantor cabang harus bisa mendapatkannya dari kantor pusat. Namun data yang ditransaksikan tersebut harus dijaga kerahasiaannya. Untuk dapat mengkomunikasikan data tersebut antar kantor harus bisa saling terkoneksi, dengan kebutuhan akan kerahasiaan data yang sangat tinggi maka VPN (Virtual Private Network) adalah salah satu solusi untuk menghubungkan setiap kantor dan menjaga kerahasiaan data yang ditransaksikan. PT NettoCyber Indonesia adalah sebuah perusahaan penyedia layanan internet yang bisa memberikan layanan VPN untuk customer yang memiliki kantor cabang yang harus saling terhubung. Dengan menggunakan jaringan Metro Ethernet yang berbasis IP/MPLS PT NettoCyber Indonesia bisa menjamin tingkat ketersediaan yang tinggi di dalam SLA (Service Level Agreement). Demi menjaga SLA dengan customer maka setiap jaringan Metro Ethernet memiliki redundansi. Dimana jika salah satu backbone link bermasalah maka akan segera pindah ke backbone lainnya yang available dengan proses failover yang tidak memakan waktu lama. Sehingga bisa menjaga High Availability kepada customer yang sangat membutuhkan koneksi stabil dalam operasionalnya. karena pada customer yang membutuhkan high availability biasanya memiliki transaksi data yang sangat banyak dan cepat

Kata kunci:

VPN, Metro Ethernet, Redundansi, Failover

UNIVERSITAS
MERCU BUANA

ABSTRACT

Name : Irawan Febriyanto
Student Number : 41514320012
Counsellor : Sri Dianing Asri, S.T, M.Kom
Title : Redundancy Analysis VPN Service IP/MPLS Based
on Metro Ethernet Network Using BFD Feature

In daily operations company that has some of the branch offices, required to communicate with and other offices as well. Because every data transaction that must be known by the headquarters and branch office data there should get it from headquarters. But the data are transacted must be kept confidential. To communicate such data between Office must be interconnected with the need for confidentiality of data is very high, then the VPN (Virtual Private Network) is one of the solutions for connecting each Office and keep confidentiality of data is transacted. PT NettoCyber Indonesia is a major internet service provider that can provide VPN service for customers that have branch offices should be connected. By using Metro Ethernet networks IP/MPLS-based PT NettoCyber Indonesia can guarantee high availability in an SLA (Service Level Agreement). For maintaining the SLA with the customer then any Metro Ethernet networks have redundancy. Where if one backbone links are problem, it will soon be moved to other backbone available with failover process doesn't take a long time. So that it can keep the High Availability to customer a very stable connection in its operational needs. Because on a customer who requires high availability typically have transaction data very much and fast.

Key words:

VPN, Metro Ethernet, Redundansi, Failover

UNIVERSITAS
MERCU BUANA

KATA PENGANTAR

Puji syukur kita panjatkan Allah SWT atas rahmat dan karunia-Nya sehingga penulis dapat menyelesaikan tugas akhir ini.

Penulis menyadari bahwa tanpa dukungan dan bimbingan dari berbagai pihak. Kiranya penulisan akan mengalami kesulitan dalam penyusunan tugas akhir ini tanpa bimbingan dan dukungan maka penulis akan mengalami kesulitan dalam penulisan tugas akhir ini. Oleh karena itu, penulis mengucapkan terima kasih kepada:

1. Allah SWT yang telah memberikan segala rahmat dan karunia-Nya sehingga penulisa bisa menyelesaikan tugas akhir ini
2. Kedua orang tua yang turut membantu dalam hal moral maupun doa agar penulis mendapatkan kelancaran dalam penulisan tugas akhir
3. Ibu Sri Dianing Asri, S.T, M.Kom, Selaku Dosen Pembimbing dan Pengampu matakuliah Metodologi Penelitian Teknik Informatika
4. Desi Ramayanti, MT, Selaku Ketua Program Studi Teknik Informatika Universitas Mercu Buana
5. Serta berbagai pihak yang tidak dapat disebutkan satu persatu, yang telah memberikan dukungan moral dan doa kepada penulis

Adapun kiranya dalam penulisan ini kiranya masih banyak kekurangan dan jauh dari kata sempurna. Untuk itu penulis menghaturkan permohonan maaf apabila terdapat kesalahan dalam penulisan tugas akhir ini

Akhir kata, penulis berharap penulisan ini bisa menjadi bahan acuan untuk penulisan tugas akhir maupun makalah dikemudian hari

Jakarta, 26 Desember 2018
Penulis



DAFTAR ISI

HALAMAN SAMPUL.....	i
HALAMAN JUDUL	i
LEMBAR PERNYATAAN ORISINALITAS.....	ii
SURAT PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR.....	iii
SURAT PERNYATAAN LUARAN TUGAS AKHIR	iv
LEMBAR PERSETUJUAN.....	v
LEMBAR PERSETUJUAN PENGUJI	vi
LEMBAR PENGESAHAN	vii
ABSTRAK	viii
ABSTRACT.....	ix
KATA PENGANTAR.....	x
DAFTAR ISI.....	xi
NASKAH JURNAL	1
1. INTRODUCTION	1
2. IMPLEMENTATION.....	2
2.1 Configuration	3
3. TESTING, RESULT And ANALYSIS	3
3.1 High Availability	3
3.1.1 BFD Feature Using System Shutdown	4
3.1.2 BFD Feature Using Physic Shutdown	5
3.2 Packet Loss	6
3.3 Latency.....	8
4. CONCLUSION.....	8
5. REFERENCES	9
KERTAS KERJA.....	10
BAGIAN 1. LITERATUR REVIEW	11
1.1 Metro Ethernet	11
1.2 Kabel Fiber Optic.....	11
1.3 Virtual Private Networks	12
1.4 MPLS (Multiprotocol Label Switching).....	13

1.5	Open Shortest Path First (OSPF)	15
1.6	Bidirectional Forwarding Detection (BFD)	15
1.7	Parameter Performansi Layanan L2VPN Berbasis MPLS	17
1.7.1	Throughput	17
1.7.2	Packet Loss	17
1.7.3	Latency	18
1.7.4	Jitter	18
1.7.5	Availability	19
2	Penelitian Terkait	19
BAGIAN 2 ANALISIS DAN PERANCANGAN.....		21
2.1	Pengamatan Topologi Jaringan	21
2.2	Konfigurasi Protocol	24
2.3	Implementasi BFD	26
BAGIAN 3 SOURCE CODE		27
3.1	Konfigurasi IP Address dan Interfaces	27
3.2	Konfigurasi L2VPN Service	28
3.3	Konfigurasi Protocol MPLS	30
3.4	Konfigurasi OSPF	33
3.5	Konfigurasi BFD.....	35
BAGIAN 4 TAHAPAN EKSPERIMEN		39
4.1	Pencarian Data	39
4.2	Identifikasi Masalah	39
4.3	Perencanaan Topologi Jaringan MPLS	39
4.4	Konfigurasi Protokol MPLS	40
4.5	Implementasi BFD	40
4.6	Pengujian Fitur BFD	40
4.7	Analisa Fitur BFD	40
BAGIAN 5 HASIL SEMUA EKSPERIMEN.....		41
5.1	High Availability	41
5.1.1	Pengujaan Shutdown Sistem.....	41
5.1.1.1	Limitasi Bandwidth 5 Mbps	42
5.1.1.2	Limitasi Bandwidth 10 Mbps	45
5.1.1.3	Limitasi Bandiwdth 20 Mbps	48
5.1.1.4	Limitasi Bandwidth 5 Mbps	50
5.1.1.5	Limitasi Bandwidth 10 Mbps	53
5.1.1.6	Limitasi Bandwidth 20 Mbps	56
5.1.2	Pengujian Shutdown Fisik	58
5.1.2.1	Limitasi Bandwidth 5 Mbps	58

5.1.2.2	Limitasi Bandwidth 10 Mbps	61
5.1.2.3	Limitasi Bandwidth 20 Mbps	63
5.1.2.4	Limitasi Bandwidth 5 Mbps	65
5.1.2.5	Limitasi Bandwidth 10 Mbps	68
5.1.2.6	Limitasi Bandwidth 20 Mbps	71
5.2	Packet Loss	74
5.2.1	Shutdown Sistem	74
5.2.1.1	Menggunakan Fitur BFD	75
5.2.1.2	Tanpa Menggunakan Fitur BFD	76
5.2.2	Shutdown Fisik	78
5.2.2.1	Menggunakan Fitur BFD	78
5.2.2.2	Tanpa Menggunakan Fitur BFD	79
5.3	Latency	81
5.3.1	Shutdown Sistem	82
5.3.2	Shutdown Fisik	82
5.4	Kesimpulan	83



Redundancy Analysis VPN Service IP/MPLS Based on Metro Ethernet Network Using BFD Feature

Sri Dianing Asri, S.T, M.Kom Mercu Buana
University Jakarta, Indonesia
dianing.asri@mercubuana.ac.id

Irawan Febriyanto Mercu Buana
University Depok, Indonesia
Irawanfebriy19@gmail.com

ABSTRACT

In daily operations company that has some of the branch offices, required to communicate with and other offices as well. Because every data transaction that must be known by the headquarters and branch office data there should get it from headquarters. But the data are transacted must be kept confidential. To communicate such data between Office must be interconnected with the need for confidentiality of data is very high, then the VPN (Virtual Private Network) is one of the solutions for connecting each Office and keep confidentiality of data is transacted. PT NettoCyber Indonesia is a major internet service provider that can provide VPN service for customers that have branch offices should be connected. By using Metro Ethernet networks IP/MPLS-based PT NettoCyber Indonesia can guarantee high availability in an SLA (Service Level Agreement). For maintaining the SLA with the customer then any Metro Ethernet networks have redundancy. Where if one backbone links are problem, it will soon be moved to other backbone available with failover process doesn't take a long time. So that it can keep the High Availability to customer.

Keywords

VPN, Metro Ethernet, Redundancy, Failover

1. INTRODUCTION

Nowadays use of data requires a stable reliable stability network connection and high availability to support work activities all the time.

In a company or other institution that has many branches office, which requires head office direct connect to branch office mostly use VPN (Virtual Private Networks) connection to run data communications inter office. VPN provide a solution private network through public network that can connect any office without have to build a physical networks. And the requirements of any ICT (Information and Communication Technologies) system regarding data protection and information security are constantly increasing[1]. VPN technology is present as one of solution to secure data transferred through the internet network. This technology allows data to be sent in the form encrypted and can only be read when it has been decrypted so that it cannot be easily controlled by a third party. Data security and the closure of data transmission from unauthorized access to transmission on the internet are the main standards in VPN[2]. VPN can be implemented on a various types of networks, Metro Ethernet is one of them.

Metro Ethernet is Wide Area Network (WAN) carrier class covering Metropolitan Area with Ethernet for communication media. Metro Ethernet can connect some Local Area Network (LAN) in different location with data capacity transport up to 10 Gb/s. In transporting data and VPN services, Metro Ethernet progression by applying Multiprotocol Label Switching (MPLS). MPLS provide routing optimization on end to end in Metro Ethernet network. With labeling method MPLS can provide data transfer be faster, efficient and powerful. MPLS is a label that was created to be used communication between routers so that the router can build label-to-label mapping independently. The label is placed on an IP package, which is possible router to continue communication by looking at the label and not the destination IP address. The package is forwarded by the label and switch without process by IP switching. MPLS labels are used to forward packages and no longer Destination IP address have caused the popularity of MPLS. Benefits-like this as better integration than IP on ATM and MPLS popular virtual private or VPN networks[3]. MPLS is an advanced forwarding scheme. It extends routing with respect to packet forwarding and path controlling[4]. MPLS technology offers more flexibility by placing labels on IP packets and using label switched paths (LSPs) to transmit packets through the network[5]. MPLS has an architecture, which supports its functions. In this paper, the MPLS architecture is divides into three parts: MPLS Definition, MPLS header, and MPLS signaling protocols[6]. The Internet Engineering Task Force (IETF) standardizes a solution such as Multiprotocol Label Switching (MPLS) as an expansion of VPN tp increase the performance of forwarding and traffic engineering intelligence on packet based network[7]

On the convergence of a IP/MPLS networks requires high availability to fulfill SLA (Service Level Agreement) for customers. On this matter NettoCyber Indonesia Company as a Internet Service Provide (ISP) already have Metro Ethernet network with fiber optic media with 10 Gb/s on every POP (Point of Presence) which redundancy to purpose provide high SLA to customers. Fiber optic systems are used worldwide for broadband networks. It is a method of transmitting information from one place to another by using light pulses through an optical fiber. Its main benefits are low loss, higher data rates, can be used up to large distances, used in light prone areas, no crosstalk, higher reliability etc[8]

Current conditions on NettoCyber Indonesia Company has physic and protocol redundancy, protocol used is OSPF (Open Shortest Path First) with function triggered if one of link failure will failover to other link[9]. Failover is the technique of applying some path to reach the goal. There are two links, namundalam normal circumstances there is only one link that was used in the other is used in as a backup when the main

link link interrupted[10]. Within OSPF protocol deployment still found deficiency. In several parameters shows packet loss, latency and jitter high enough which need a few seconds on failover process. OSPF is a link state protocol which is created due to requirements such as software or hardware independencies, the need for the dynamic algorithms, the ability to use other cost metrics to determine the optimal route, the need for service quality support, load balancing, the need for hierarchical routing, increased security level, Support for tunnel creation mechanism[11]. From that found, will analyzed BFD (Bidirectional Forwarding Detection) with very quick system failure identifying on device or networks only milliseconds. So failover process faster and smoother. Bidirectional Forwarding Detection (BFD) is a network protocol used to detect faults between two forwarding engines. BFD provides low-overhead, low-latency detection of faults even on physical media that don't support failure detection of any kind, such as ethernet, virtual circuits, tunnels and MPLS LSPs[12]. BFD provides low-overhead, short-duration detection of failures in the path between adjacent forwarding engines, including the interfaces, data links, and to the extent possible the forwarding engines themselves. BFD has already been deployed in the MPLS-based networks and demonstrated to be in effect[12]. Of these advantages NettoCyber Indonesia Company applying that feature on protocol used in Metro Ethernet networks.

2. IMPLEMENTATION

BFD (Bidirectional Forwarding Detection) feature is a simple mechanism that is designed to detection failure on the network. In principle it works, BFD form grooves Exchange communication by sending Hello packets with the specified interval, the failure on the device when the device is detected the neighboring routing stops receiving a reply Hello packet after interval for BFD are determined and started working with various network environment and topology, BFD provides faster detection. With the advantages of the BFD allows when applying at the interface of the device that is running routing protocol IGP that support performance-based MPLS L2VPN services.

In observations on existing topology then it will be known performance parameters by making simulations according to the conditions of existing networks. In this simulation will be tested from most existing topology on Metro Ethernet network at PT. NettoCyber Indonesia (VELO Networks) Mega Kuningan area, with purpose of found parameters before using the L2VPN services performance features of BFD. Below are the existing Ethernet Metro network topology at PT. NettoCyber Indonesia (VELO Networks) area of Mega Kuningan :

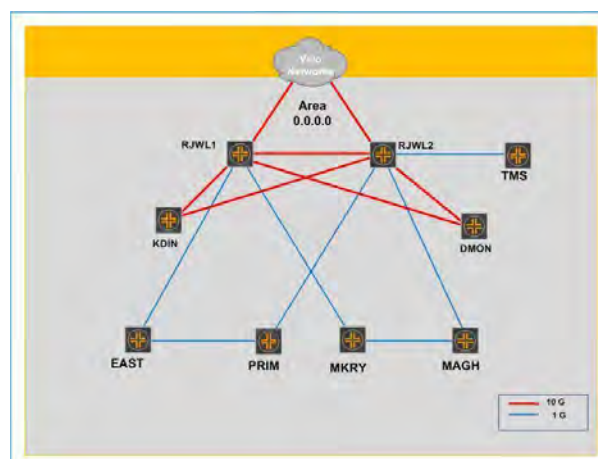


Fig 1: Metro E Network Topology NettoCyber Indonesia Company on Mega Kuningan Area

On Fig 1 contained some devices installed on buildings in Mega Kuningan Area South Jakarta. Below Table 1 show devices name and buildings:

Table 1. Device Name and Building Name

Device Name	Building Name
RJWL1	Menara Rajawali
RJWL2	Menara Rajawali
KDIN	Menara Kadin
DMON	Menara Danamon
EAST	THE EAST
PRIM	Menara Prima
MKRY	Menara Karya
MAGH	Menara Anugerah

After known that existing topology choose sample topology on area KDIN, RJWL1, RJWL2 for simulation with purposed to get parameters about performance L2VPN by not using BFD feature. Topology on that area:

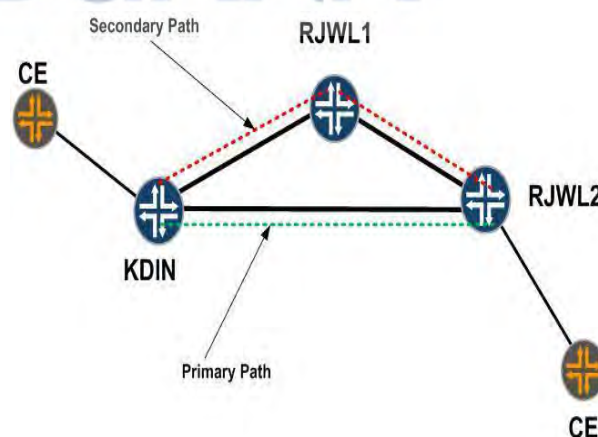


Fig 2: Topology on KDIN, RJWL1 and RJWL2 Area

From Fig 2 found primary path customer through RJWL2 line and when primary link to RJWL2 failure so will failover to

RJWL1 previously then to RJWL2 through secondary path. On that failover process will be observed result of network availability, packet loss and latency on L2VPN Services.

To know that parameters will simulated according topology on Fig 2 however device name changed to Lab_2 for KDIN as PE, Lab_3 for RJWL1 as P and Lab_4 for RJWL2 as PE.

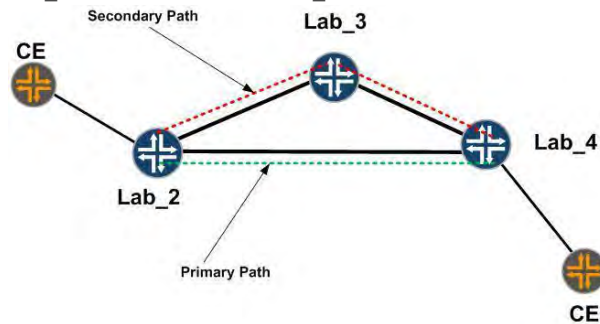


Fig 3: Simulation Lab Topology

Simulation will adjust configuration IGP Protocol, LDP, BFD Feature, L2VPN Service and analyze BFD Feature impact toward L2VPN Services.

2.1 CONFIGURATION

Simulation impact on BFD feature towards L2VPN services, requires configuration on devices suitable with simulation topology in Fig 3. Before simulation protocol configuration on that topology, the first to do is assign IP address and interfaces allocation. Below table for that IP address and interface requires:

Table 2. IP address and Interfaces Allocation

Device Name	IP Address	Interface Name	Port
LAB_2	10.10.42.2/29	lab4-1/1/22	12
	10.10.32.2/29	lab4-1/1/12	13
	2.2.2.2/32	system	
LAB_3	10.10.43.3/29	lab4-1/1/28	28
	10.10.32.3/29	lab4-1/1/13	12
	3.3.3.3/32	system	
LAB_4	10.10.43.4/29	lab4-1/1/28	28
	10.10.42.4/29	lab4-1/1/28	22
	4.4.4.4/32	system	

To make it easier comprehension of IP address and interfaces allocation on simulation lab topology. Fig 4 will explain in more detail about simulation lab topology with using IP address and interfaces allocation

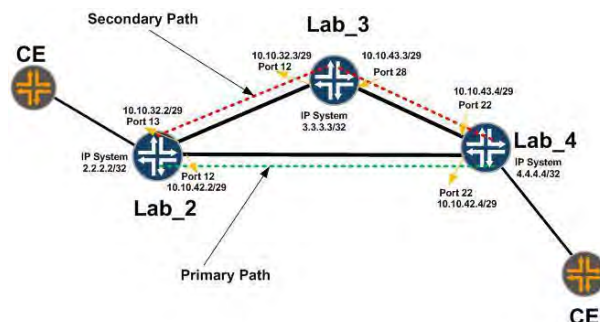


Fig 4: IP address and Interfaces Name Allocation

After IP address and interfaces name allocation defined, next step is configuration on devices involves IP address and interfaces, OSPF protocol, LDP, L2VPN services and BFD feature. When all configuration ready, BFD feature applied each interfaces and activated on OSPF protocol. According to purpose in order failure detection and failover process faster. Fig 5 show simulation lab topology after all configuration ready and running well.

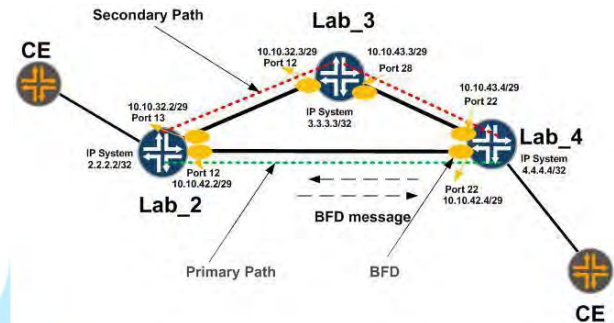


Fig 5: Simulation Lab Topology with All Configuration Running

3. Testing, Result and Analysis

BFD feature testing on PE, while CE will monitor whether BFD feature running well in IGP so affect to L2VPN services quality on CE with purpose to get data and information when failover process from primary path to secondary path.

Phase testing BFD feature in PE namely shutdown interfaces by system and physically. Physical shutdown simulated when failure caused physical device like interfaces port or cables.

In CE1 side there is notebook direct against CE1 devices to observe and monitor downtime, packet loss, latency and throughput.

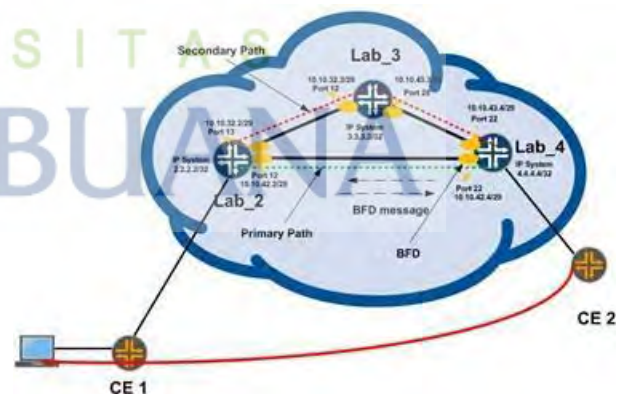


Fig 6: Implement and Testing BFD Feature

Based on testing on simulation topology found result parameters as High Availability, packet loss and latency by implement BFD feature and didn't use BFD feature. And below will explain detail result and analysis on each parameters

3.1 High Availability

High availability result obtained by system and physic shutdown using bandwidth limitation 5 Mbps, 10 Mbps and

20 Mbps in time range 1 hour. That range time can describe with *Mean Time Between Failures (MTBF)*.

System and physic shutdown method by taking parameters to find out average time value recovery or *Mean Time To Recovery (MTTR)*. Stopwatch used as time measuring device and ping time as ICMP delivery packet. MTTR measurement by counting downtime duration or Request Time Out (RTO) packet when failover process. Mathematically availability calculation can be calculated using formula

$$\text{Availability} = \frac{\text{MTTF}}{\text{MTTF} + \text{MTTR}} \times 100\%$$

3.1.1 BFD Feature Using System Shutdown

Below testing result downtime duration on BFD feature using system shutdown method with bandwidth 5 Mbps, 10 Mbps and 20 Mbps. Testing repeat until 5 times explain on Fig 7 – Fig 9 and Table 3 – Table 5

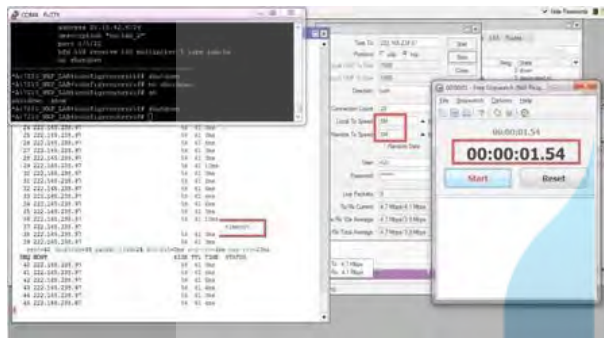


Fig 7: Result BFD Feature System Shutdown Bandwidth 5 Mbps

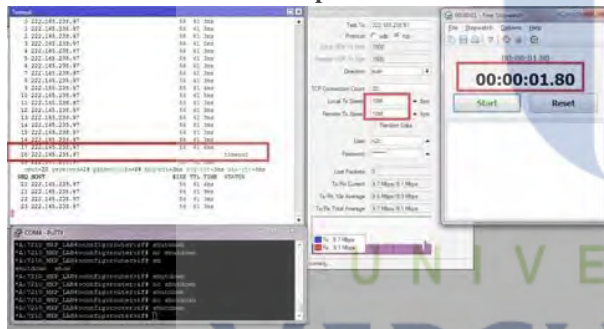


Fig 8: Result BFD Feature System Shutdown Bandwidth 10 Mbps

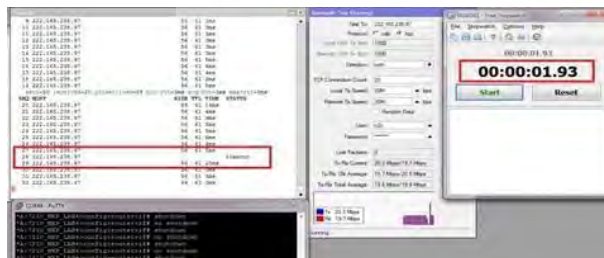


Fig 9: Result BFD Feature System Shutdown Bandwidth 20 Mbps

Table 3. Availability Service BFD Feature System Shutdown Bandwidth 5 Mbps

Result	Bandwidth	MTTF (Second)	MTTR (Second)
First	5 Mbps	3600	1.54

Second	5 Mbps	3600	1.42
Third	5 Mbps	3600	1.16
Fourth	5 Mbps	3600	1.22
Fifth	5 Mbps	3600	1.15
Average			1.298

Table 4. Availability Service BFD Feature System Shutdown Bandwidth 10 Mbps

Result	Bandwidth	MTTF (Second)	MTTR (Second)
First	10 Mbps	3600	1.17
Second	10 Mbps	3600	1.22
Third	10 Mbps	3600	1.25
Fourth	10 Mbps	3600	1.8
Fifth	10 Mbps	3600	1.09
Average			1.306

Table 5. Availability Service BFD Feature System Shutdown Bandwidth 20 Mbps

Result	Bandwidth	MTTF (Second)	MTTR (Second)
First	20 Mbps	3600	1.93
Second	20 Mbps	3600	1.81
Third	20 Mbps	3600	1.29
Fourth	20 Mbps	3600	1.86
Fifth	20 Mbps	3600	1.97
Average			1.772

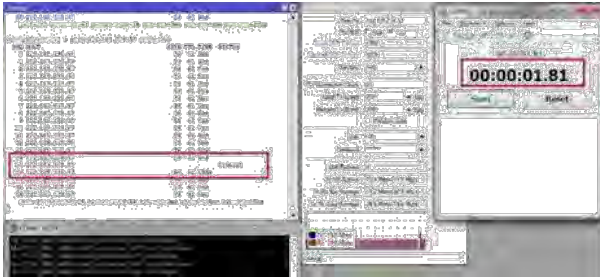
Based on testing result bandwidth 5 Mbps BFD Feature using shutdown system. Failover process test show availability can reach 99,9639%, bandwidth 10 Mbps 99,9637% and 99,950% in 20 Mbps bandwidth, obtain from formula:

$$\text{Availability} = \frac{3600}{3600 + 1.298} \times 100\% = 99,9639\% \text{ (5 Mbps)}$$

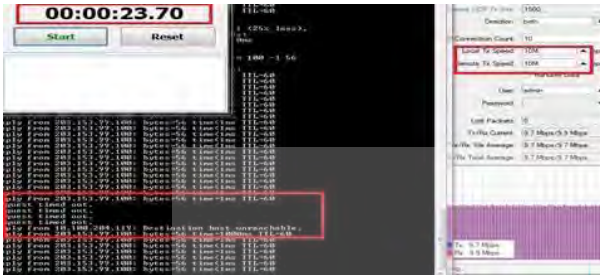
$$\text{Availability} = \frac{3600}{3600 + 1.306} \times 100\% = 99,9637\% \text{ (10 Mbps)}$$

$$\text{Availability} = \frac{3600}{3600 + 1.772} \times 100\% = 99,950\% \text{ (20 Mbps)}$$

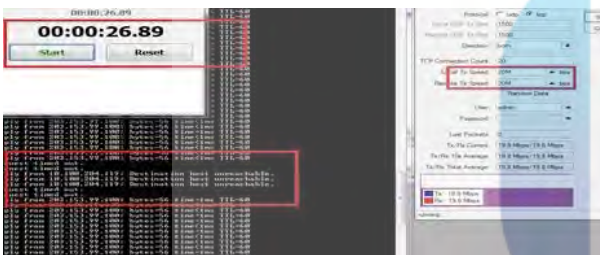
Further after testing and get result downtime duration failover test using BFD feature on system shutdown. Next action test for downtime duration failover test didn't use BFD feature but still system shutdown method and repeat until 5 times. Below Fig 10 – Fig 12 and Table 6 – Table 8 will explain the detail and different result if compare with BFD feature.



**Fig 10: Result Non BFD Feature System Shutdown
Bandwidth 5 Mbps**



**Fig 11: Result Non BFD Feature System Shutdown
Bandwidth 10 Mbps**



**Fig 12: Result Non BFD Feature System Shutdown
Bandwidth 20 Mbps**

**Table 6. Availability Service BFD Feature System
Shutdown Bandwidth 5 Mbps**

Result	Bandwidth	MTTF (Second)	MTTR (Second)
First	5 Mbps	3600	24.56
Second	5 Mbps	3600	24.79
Third	5 Mbps	3600	22.29
Fourth	5 Mbps	3600	22.29
Fifth	5 Mbps	3600	24.92
Average			23.774

**Table 7. Availability Service BFD Feature System
Shutdown Bandwidth 5 Mbps**

Result	Bandwidth	MTTF (Second)	MTTR (Second)
First	10 Mbps	3600	23.7
Second	10 Mbps	3600	27.76
Third	10 Mbps	3600	23.73
Fourth	10 Mbps	3600	24.33
Fifth	10 Mbps	3600	25.08
Average			25.72

**Table 8. Availability Service BFD Feature System
Shutdown Bandwidth 20 Mbps**

Result	Bandwidth	MTTF	MTTR
--------	-----------	------	------

		(Second)	(Second)
First	10 Mbps	3600	24.06
Second	10 Mbps	3600	23.96
Third	10 Mbps	3600	26.89
Fourth	10 Mbps	3600	25.31
Fifth	10 Mbps	3600	22.33
Average			24.51

Based on result seen that didn't use BFD feature availability cant optimal although downtime duration on failover process under 1 minutes but impact to customer who requires high availability connection. In bandwidth 5 Mbps availability reach 99,343%, 10 Mbps 99,290% and 20 Mbps 99,323%.

$$\text{Availability} = \frac{3600}{3600 + 23.774} \times 100\% = 99,343\% \text{ (5 Mbps)}$$

$$\text{Availability} = \frac{3600}{3600 + 25.72} \times 100\% = 99,290\% \text{ (10 Mbps)}$$

$$\text{Availability} = \frac{3600}{3600 + 24.51} \times 100\% = 99,323\% \text{ (20 Mbps)}$$

3.1.2 BFD Feature Using Physic Shutdown

Testing BFD feature using physical shutdown on failover process to obtain result downtime duration almost the same process but the difference is unplug cable on device interface for this testing. So directly see the result of BFD feature and non BFD feature with Physic Shutdown

**Table 9. Availability Service BFD Feature Physical
Shutdown Bandwidth 5 Mbps**

Result	Bandwidth	MTTF (Second)	MTTR (Second)
First	5 Mbps	3600	1.47
Second	5 Mbps	3600	1.83
Third	5 Mbps	3600	1.25
Fourth	5 Mbps	3600	1.62
Fifth	5 Mbps	3600	1.61
Average			1.556

$$\text{Availability} = \frac{3600}{3600 + 1.556} \times 100\% = 99,956\%$$

**Table 10. Availability Service BFD Feature Physical
Shutdown Bandwidth 10 Mbps**

Result	Bandwidth	MTTF (Second)	MTTR (Second)
First	10 Mbps	3600	1.5
Second	10 Mbps	3600	1.66
Third	10 Mbps	3600	1.79
Fourth	10 Mbps	3600	1.43
Fifth	10 Mbps	3600	1.71
Average			1.618

$$\text{Availability} = \frac{3600}{3600 + 1.618} \times 100\% = 99,955\%$$

Table 11. Availability Service BFD Feature Physical Shutdown Bandwidth 20 Mbps

Result	Bandwidth	MTTF (Second)	MTTR (Second)
First	20 Mbps	3600	1.72
Second	20 Mbps	3600	1.31
Third	20 Mbps	3600	1.64
Fourth	20 Mbps	3600	1.95
Fifth	20 Mbps	3600	1.47
Average			1.62

$$\text{Availability} = \frac{3600}{3600 + 1.62} \times 100\% = 99,955\%$$

After get result of BFD feature on physical shutdown. Next step is test and result non BFD feature on physical shutdown. That data and information explain on Table 12 – Table 14

Table 12. Availability Service Non BFD Feature System Shutdown Bandwidth 5 Mbps

Result	Bandwidth	MTTF (Second)	MTTR (Second)
First	5 Mbps	3600	22.5
Second	5 Mbps	3600	23.22
Third	5 Mbps	3600	23.3
Fourth	5 Mbps	3600	24.6
Fifth	5 Mbps	3600	23.95
Average			23.514

$$\text{Availability} = \frac{3600}{3600 + 23.514} \times 100\% = 99,346\%$$

Table 13. Availability Service Non BFD Feature System Shutdown Bandwidth 10 Mbps

Result	Bandwidth	MTTF (Second)	MTTR (Second)
First	10 Mbps	3600	24.14
Second	10 Mbps	3600	22.74
Third	10 Mbps	3600	23.52
Fourth	10 Mbps	3600	23.76
Fifth	10 Mbps	3600	23.73
Average			23.578

$$\text{Availability} = \frac{3600}{3600 + 23.578} \times 100\% = 99,345\%$$

Table 14. Availability Service Non BFD Feature System Shutdown Bandwidth 20 Mbps

Result	Bandwidth	MTTF (Second)	MTTR (Second)
First	20 Mbps	3600	26.02
Second	20 Mbps	3600	24.14
Third	20 Mbps	3600	23.57

Fourth	20 Mbps	3600	23.08
Fifth	20 Mbps	3600	22.74
Average			23.91

$$\text{Availability} = \frac{3600}{3600 + 23.91} \times 100\% = 99,335\%$$

On testing the system shutdown with the use of BFD monitored duration shorter downtimes i.e. Duration minimum downtime of about 1.09 seconds and a maximum of 1.97 seconds. Whereas by not using BFD found minimum downtime of about 22.29 seconds and a maximum of 27.76 seconds. And from calculations made on testing the physical shutdown, found services-services by using the features of the BFD has roughly 0.6% higher compared to services-services that do not use the BFD.

3.2 Packet Loss

The test results either on the system shutdown or shutdown with the physical limitations of bandwidth at 5 Mbps, 10 Mbps, and 20 Mbps is found by using the features of the BFD on when failover occurs only packet loss 1% whereas without using BFD in system shutdown test found the minimum packet loss at 4.6% and 5.8% at the maximum. This testing is by the method of observation of the ICMP packet of 56 bytes on any one package with 100 times the delivery on time of traffic utilization reaches a maximum

Mathematically packet loss can counting by formula. To know packet loss BFD feature on system shutdown show in below table

Table 15. Packet Loss Services 5 Mbps BFD Feature System Shutdown

Result	Bandwidth	Packet Send (Bytes)	Packet Receive (Bytes)	Packet Loss
First	5 Mbps	5600	5544	1%
Second	5 Mbps	5600	5544	1%
Third	5 Mbps	5600	5544	1%
Fourth	5 Mbps	5600	5544	1%
Fifth	5 Mbps	5600	5544	1%
Average				1%

$$\text{Paket Loss} = \frac{5600 - 5544 \times 100\%}{5600} = 1\%$$

Table 16. Packet Loss Services 10 Mbps BFD Feature System Shutdown

Result	Bandwidth	Packet Send (Bytes)	Packet Receive (Bytes)	Packet Loss
First	10 Mbps	5600	5544	1%
Second	10 Mbps	5600	5544	1%
Third	10 Mbps	5600	5544	1%
Fourth	10 Mbps	5600	5544	1%
Fifth	10 Mbps	5600	5544	1%
Average				1%

$$\text{Paket Loss} = \frac{5600 - 5544 \times 100\%}{5600} = 1\%$$

Table 17. Packet Loss Services 20 Mbps BFD Feature System Shutdown

Result	Bandwidth	Packet Send (Bytes)	Packet Receive (Bytes)	Packet Loss
First	20 Mbps	5600	5544	1%
Second	20 Mbps	5600	5544	1%
Third	20 Mbps	5600	5544	1%
Fourth	20 Mbps	5600	5544	1%
Fifth	20 Mbps	5600	5544	1%
Average				1%

$$\text{Paket Loss} = \frac{5600 - 5544 \times 100\%}{5600} = 1\%$$

The values derived from mathematical calculations packet loss by didn't using BFD on testing system shutdown, below

Table 18. Packet Loss Services 5 Mbps Non BFD Feature System Shutdown

Result	Bandwidth	Packet Send (Bytes)	Packet Receive (Bytes)	Packet Loss
First	5 Mbps	5600	5320	1%
Second	5 Mbps	5600	5320	1%
Third	5 Mbps	5600	5377	1%
Fourth	5 Mbps	5600	5377	1%
Fifth	5 Mbps	5600	5320	1%
Average		5600	5342.8	4.6%

$$\text{Paket Loss} = \frac{5600 - 5342.8 \times 100\%}{5600} = 4.6\%$$

Table 19. Packet Loss Services 10 Mbps Non BFD Feature System Shutdown

Result	Bandwidth	Packet Send (Bytes)	Packet Receive (Bytes)	Packet Loss
First	10 Mbps	5600	5376	1%
Second	10 Mbps	5600	5208	1%
Third	10 Mbps	5600	5208	1%
Fourth	10 Mbps	5600	5320	1%
Fifth	10 Mbps	5600	5320	1%
Average		5600	5286.4	5.6%

$$\text{Paket Loss} = \frac{5600 - 5286.4 \times 100\%}{5600} = 5.6\%$$

Table 19. Packet Loss Services 20 Mbps Non BFD Feature System Shutdown

Result	Bandwidth	Packet Send (Bytes)	Packet Receive (Bytes)	Packet Loss
First	20 Mbps	5600	5208	1%
Second	20 Mbps	5600	5320	1%

Third	20 Mbps	5600	5208	1%
Fourth	20 Mbps	5600	5320	1%
Fifth	20 Mbps	5600	5320	1%
Average		5600	5275.2	5.8%

$$\text{Paket Loss} = \frac{5600 - 5275.2 \times 100\%}{5600} = 5.8\%$$

On testing the physical shutdown found minimum packet loss is 5% and 5.4% with maximum values without using BFD, value packet loss that much higher compared to the BFD feature to failover quickly so that packet loss only 1%. Seen on Fig 13 manual testing shutdown physic by unplug fiber optic cable on device interface LAB_2, LAB_3 and LAB_4.



Fig 13: Unplug Fiber Optic Cable on Device Interfaces

Further testing physic shutdown finish by unplug cable repeated until 5 times. Packet loss detail when failover process in 5, 10 and 20 Mbps bandwidth using BFD Feature explain on following table

Table 20. Packet Loss Services 5 Mbps BFD Feature Physical Shutdown

Result	Bandwidth	Packet Send (Bytes)	Packet Receive (Bytes)	Packet Loss
First	5 Mbps	5600	5544	1%
Second	5 Mbps	5600	5544	1%
Third	5 Mbps	5600	5544	1%
Fourth	5 Mbps	5600	5544	1%
Fifth	5 Mbps	5600	5544	1%
Average				1%

$$\text{Paket Loss} = \frac{5600 - 5544 \times 100\%}{5600} = 1\%$$

Table 21. Packet Loss Services 10 Mbps BFD Feature Physical Shutdown

Result	Bandwidth	Packet Send (Bytes)	Packet Receive (Bytes)	Packet Loss
First	10 Mbps	5600	5544	1%
Second	10 Mbps	5600	5544	1%
Third	10 Mbps	5600	5544	1%
Fourth	10 Mbps	5600	5544	1%

Fifth	10 Mbps	5600	5544	1%
Average				1%

$$\text{Paket Loss} = \frac{5600 - 5544 \times 100\%}{5600} = 1\%$$

Table 22. Packet Loss Services 10 Mbps BFD Feature Physical Shutdown

Result	Bandwidth	Packet Send (Bytes)	Packet Receive (Bytes)	Packet Loss
First	20 Mbps	5600	5544	1%
Second	20 Mbps	5600	5544	1%
Third	20 Mbps	5600	5544	1%
Fourth	20 Mbps	5600	5544	1%
Fifth	20 Mbps	5600	5544	1%
Average				1%

$$\text{Paket Loss} = \frac{5600 - 5544 \times 100\%}{5600} = 1\%$$

When physical shutdown finish on device interfaces using BFD feature. Next step is to compare physical shutdown devices interfaces by didn't use BFD feature to get values of packet loss. The comparison show on following table

Table 23. Packet Loss Services 5 Mbps Non BFD Feature Physical Shutdown

Result	Bandwidth	Packet Send (Bytes)	Packet Receive (Bytes)	Packet Loss
First	5 Mbps	5600	5264	6%
Second	5 Mbps	5600	5320	5%
Third	5 Mbps	5600	5320	5%
Fourth	5 Mbps	5600	5320	5%
Fifth	5 Mbps	5600	5320	5%
Average		5600	5308.8	5%

$$\text{Paket Loss} = \frac{5600 - 5308.8 \times 100\%}{5600} = 5\%$$

Table 24. Packet Loss Services 10 Mbps Non BFD Feature Physical Shutdown

Result	Bandwidth	Packet Send (Bytes)	Packet Receive (Bytes)	Packet Loss
First	10 Mbps	5600	5320	5%
Second	10 Mbps	5600	5208	7%
Third	10 Mbps	5600	5320	5%
Fourth	10 Mbps	5600	5320	5%
Fifth	10 Mbps	5600	5320	5%
Average		5600	5297.6	5.4%

$$\text{Paket Loss} = \frac{5600 - 5297.6 \times 100\%}{5600} = 5.4\%$$

Table 25. Packet Loss Services 10 Mbps Non BFD Feature Physical Shutdown

Result	Bandwidth	Packet Send (Bytes)	Packet Receive (Bytes)	Packet Loss
First	20 Mbps	5600	5264	6%
Second	20 Mbps	5600	5432	3%
Third	20 Mbps	5600	5320	5%
Fourth	20 Mbps	5600	5208	7%
Fifth	20 Mbps	5600	5377	4%
Average		5600	5320.2	5.2%

$$\text{Paket Loss} = \frac{5600 - 5320.2 \times 100\%}{5600} = 5.2\%$$

3.3 Latency

After all process system and physical shutdown finished, found latency when failover process. The result maintained its position of using BFD feature and without BFD feature. System shutdown using BFD feature found latency minimum approximately 13 ms and maximum 26 ms. Whereas without BFD feature get the value of latency minimum approximately 148 ms and 1000 ms maximum latency. Show on following table

Table 25. Latency Result by System shutdown

Bandwidth	BFD (ms)	Non BFD (ms)
5 Mbps	13	148
10 Mbps	26	1000
20 Mbps	18	1000

On testing the physical shutdown, latency with the use of BFD feature found the minimum value about 15 ms and maximum value 18 ms. the Results are pretty much different from the results of testing the latency without using BFD feature, that found the minimum value about 3 ms and a maximum value of 1002 ms. From those results do not affect significant BFD feature on latency after the failover occurs.

Table 25. Latency Result by Physical shutdown

Bandwidth	BFD (ms)	Non BFD (ms)
5 Mbps	18	6
10 Mbps	16	3
20 Mbps	15	1002

4. CONCLUSION

In this research can concluded that use of BFD feature on Metro Ethernet network with L2VPN services on NettoCyber Indonesia Company influential profitable in performances and redundancy by result all of testing explain that:

BFD feature implementation running well on Metro Ethernet network with L2VPN services so can provide to customer better than before using BFD feature

By using BFD feature increased availability services compared without using BFD feature. It almost

significant for customer who requires high availability of services

When failover process using BFD feature on system shutdown and physical shutdown found packet loss only 1% without BFD feature can reach 5,8% and stable latency using BFD feature, but unstable without BFD feature until 1000 ms

BFD feature implementation quite significant when failover process, especially when one of the link problem and failover in customer rush/offices hour to other link not too affected critically and still delivered high availability services.

no. 1, pp. 30–39, 2016.

- [11] M. Reza, M. Naderi, and R. Javidan, “A New Architecture to Improve Multimedia QoS over Software Defined Networks,” *Int. J. Comput. Appl.*, vol. 179, no. 23, pp. 14–19, 2018.
- [12] H. R. Arkian, R. E. Atani, A. Pourkhalili, and S. Kamali, “A stable clustering scheme based on adaptive multiple metric in vehicular Ad-hoc Networks,” *J. Inf. Sci. Eng.*, vol. 31, no. 2, pp. 361–386, 2015.

5. REFERENCES

- [1] N. Stoianov, M. Urueña, M. Niemiec, P. Machnik, and G. Maestro, “Integrated security infrastructures for law enforcement agencies,” *Multimed. Tools Appl.*, vol. 74, no. 12, pp. 4453–4468, 2015.
- [2] 林伸行,
“病院・介護施設におけるノロウイルス感染症の
拡大防止対策を
目的とした吐物の飛散状況に関する研究 No
Title,” *感染症誌*, vol. 91, no. 2, pp. 399–404, 2017.
- [3] B. Nugraha, T. Elektro, and T. Elektro, “Jurnal
Teknologi Elektro , Universitas Mercu Buana ISSN :
2086 - 9479 ANALISA PERBANDINGAN PERFORMA
TEKNOLOGI MPLS-TP (MULTIPROTOCOL LABEL
SWITCHING - TRANSPORT PROFILE) DENGAN
TOPOLOGI RING DAN POINT-TO-POINT,” vol. 8, no. 2,
pp. 138–144, 2017.
- [4] X. Xiao, A. Hannan, B. Bailey, and L. M. Ni,
“Traffic engineering with MPLS in the Internet,”
IEEE Netw., vol. 14, no. 2, pp. 28–33, 2000.
- [5] K. Stefan and A. Binzenh, “MPLS Traffic
Engineering in OSPF Networks - A combined
approach.”
- [6] A. S. G. Allah and N. M. El-shennawy, “Admission
Control Algorithm for MPLS-TE Networks,” vol.
160, no. 5, pp. 11–16, 2017.
- [7] D. J. Casa *et al.*, “In Pr es s,” *Lung*, vol. 47, no. 1,
pp. 1–23, 2011.
- [8] A. Parmar, “Study of Inter-Satellite Optical Wireless
Communication System with different Modulation
Techniques,” vol. 182, no. 6, pp. 24–28, 2018.
- [9] B. Rifai and E. Supriyanto, “Management System
Failover Dengan Routing Dinamis Open Shortest
Path First Dan Border Gateway Protocol,” *JITK
(Jurnal Ilmu Pengetah. Dan Teknol. Komputer)*, vol.
3, no. 1, pp. 39–46, 2017.
- [10] B. Yuliadi and A. Nugroho, “Rancangan Disaster
Recovery Pada Instansi Pendidikan Studi Kasus
Universitas Mercu Buana,” *J. Tek. Inform.*, vol. 9,

KERTAS KERJA

Ringkasan

Kertas kerja merupakan material kelengkapan artikel jurnal dengan judul yang telah dipaparkan di atas. Kertas kerja berisi semua material hasil penelitian Tugas Akhir yang tidak dimuat/atau disertakan di artikel jurnal. Di dalam kertas kerja ini disajikan :

- A. literature review yang digunakan oleh penulis sebagai bahan acuan dalam penelitian.
- B. Analisa dan perancangan desain topologi jaringan yang dibangun.
- C. Source code dari konfigurasi dalam jaringan yang dibangun
- D. Tahapan – tahapan yang dilakukan oleh penulis dalam penelitian.
- E. Hasil dari penelitian secara keseluruhan

