

Peningkatan Konektifitas Service VPLS Redundant Path Dengan Rapid Spanning Tree Protocol

Fikri Iqromuddin¹, Novi Dian Nathasia², Iskandar Fitri³

¹fikri1892@gmail.com, ²novidian@civitas.unas.ac.id, ³tektel2001@yahoo.com

^{1,2,3}Fakultas Teknologi Komunikasi dan Informatika, Universitas Nasional

Abstract— *Virtual Private LAN Service is already very popular among the enterprise industry which is a point to point network or multipoint to multipoint I2VPN service, VPLS provides transparent bridge between customers connected to geographically dispersed locations delivered via MPLS backbone by utilizing features such as MPLS Fast reroute and traffic engineering. Redundant paths can be applied to the VPLS service on the access side and backbone to maintain link performance that aims to minimize down time during network fails on the VPLS service. In this research, the implementation of redundant path using RSTP to prevent forwarding loop switching network in VPLS service to protect end-to-end data traffic with VPLS mesh-pseudowire and spoke-pseudowire with RSTP is the most optimal result compared to STP and build reliable network System with high performance for use in modern industry.*

Keyword — *MPLS, Pseudowire, RSTP, Redundant, VPLS*

Intisari— *Virtual Private LAN Service sudah sangat populer di kalangan industri enterprise yang merupakan jaringan point to point atau multipoint to multipoint I2VPN service, VPLS menyediakan transparan bridge antara customer yang terkoneksi dengan lokasi terpisah secara geografis yang di deliver melalui MPLS backbone dengan memanfaatkan feature seperti MPLS fast reroute dan traffic engineering. Redundant path dapat di terapkan pada service VPLS di sisi akses maupun backbone untuk menjaga performa link yang bertujuan untuk meminimalisir down time saat network fail pada service VPLS. Dalam penelitian ini di implementasikan redundant path menggunakan RSTP guna mencegah forwarding loop switching network pada service VPLS agar terlindungnya traffic data secara end to end dengan hasil VPLS mesh-pseudowire dan spoke-pseudowire dengan RSTP merupakan hasil yang paling optimal dibandingkan dengan STP dan terbentuk reliable network system dengan high performance untuk di gunakan pada modern industri.*

Kata Kunci — *MPLS, Pseudowire, RSTP, Redundant, VPLS*

I. PENDAHULUAN

Seiring dengan meningkatnya kebutuhan industri enterprise, maka dibutuhkan teknologi canggih untuk memenuhi segala kebutuhan tersebut, tantangan bagi penyedia layanan adalah meningkatkan performa *network* dan inovatif untuk memenuhi kebutuhan kritis ini. Industri enterprise membutuhkan koneksi antar site dengan kriteria *high bandwidth, plug and play* dan *simple service peering*. Dalam rangka *improve availability*, perlu di perhatikan *failure* yang terjadi pada *network* yang mengakibatkan menurunnya *network availability*. Dengan segala kebutuhan ini layanan VPLS merupakan salah satu solusi

tersebut. *Virtual Private LAN Service (VPLS)* mengkoneksikan *point to point* atau *multipoint to multipoint Ethernet bridging via IP/MPLS backbone*, semua *customer* yang terhubung dalam VPLS yang sama menjadi *segment LAN* yang sama terlepas dari lokasi yang berbeda. VPLS memanfaatkan segala keuntungan dari MPLS infrastruktur, seperti *traffic engineering* pada *transport tunnel, tunnel resilient feature, convergensi backbone* untuk *multiple service*, namun VPLS service perlu di proteksi secara *end to end* untuk menghindari segala macam *network fail*.

II. PENELITIAN TERKAIT

Pada penelitian sebelumnya yaitu penerapan *spanning tree* pada VPLS yang di bagi menjadi dua yaitu *customer associated* dan *provider associated* pada *flat* desain VPLS [1] dengan hasil *spanning tree* dapat *transmitted broadcast frames* melalui VPLS *network* tanpa mengirim *broadcast storm* dan dapat mengurangi waktu konvergensi pada *segment network provider* maupun *customer*. Pada VPLS *flat* desain, fungsi $n(n-1)/2$ *mesh-pseudowire* harus di terapkan pada VPLS dimana *n* adalah member PE router yang berpartisipasi pada *service VPLS*. VPLS *flat* desain menggunakan *mesh-pseudowire* untuk koneksi antar PE, pengurangan jumlah *mesh-pseudowire* dapat mengakibatkan *loss* koneksi dengan masalah *data plane* maupun *control plane* untuk skala *network* yang luas. Dimana akan banyaknya *packet* untuk di *replicate* dan pengelolaan *pseudowire* pada *service VPLS*.

VPLS *interoperability* dengan CE *bridge* di bagi dua kategori yaitu *mandatory* dan *optional* [2], kategori *mandatory* yaitu memastikan pengopreasian VPLS yang tepat dengan CE *bridge* dalam kasus ketika *attachment circuit* menggunakan VLAN maka PE perlu menyesuaikan dengan perangkat CE seperti penyesuaian *protocol spanning tree*. Sedangkan *optional* yaitu penyediaan tambahan *operational* dalam rangka *improvement* dan *efficiency VPLS* seperti *redundancy* dalam kasus melindungi *primary PE fails* agar *reroute* ke *backup PE*.

Peneliti sebelumnya juga sudah membahas tentang *three-rings redundancy* industri Ethernet menggunakan RSTP [3], dengan hasil terbentuk *network system* yang benar-benar handal dan *real time performance* dengan sedikit *packet loss*.

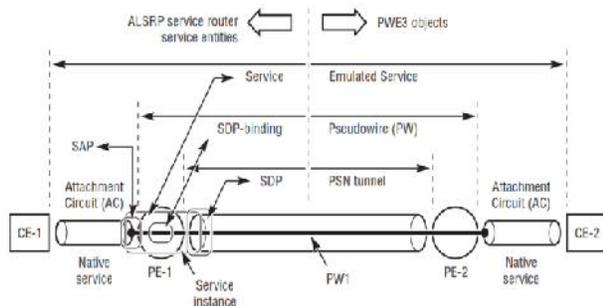
Awal mulanya, IETF membagi dua standar pengembangan VPLS *network* dengan *signaling Border Gateway Protocol (BGP)* [4] dan *signaling Label Distribution Protocol (LDP)* [5] berdasarkan arsitektur ini perlu di terapkan mekanisme *failure handling* dalam VPLS untuk meningkatkan *availability*. Pada kedua standar VPLS ini di jelaskan keuntungan pada mekanisme VPLS yang ada dari sisi kemudahan dan efisiensi dalam menyediakan *service VPLS* pada [6]. Berdasarkan *control plane* skalabilitas, tantangan besar dengan LDP VPLS adalah pengelolaan *full mesh targeted LDP session* dimana dalam BGP VPLS dapat mengatasi masalah ini dengan *route reflection*.

Pada penelitian ini akan di buat desain *VPLS redundant path* dengan *LDP signaling* pada *pseudowire* dan *redundant* di sisi akses sebagai kategori *optional* dari *VPLS interoperability*. Bagaimanapun, *redundancy path* dapat menyebabkan *forwarding loop* yang akan menjadi masalah serius seperti *broadcast storm*, *multiple frame transmission* dan ketidakstabilan *database MAC (Media Acces Control) address*. Untuk mengatasi masalah ini *Rapid Spanning Tree Protocol (RSTP)* dapat di gunakan untuk mengontrol data *traffic* dan pemanfaatan *failure handling* pada *switching segment* untuk meningkatkan *availability network*. Tujuan dari penulisan penelitian ini diantaranya adalah sebagai berikut :

1. Membuktikan tidak terjadinya *forwarding loop* pada network *VPLS* dengan topologi yang di buat.
2. Meminimalisir *down time* ketika terjadi *network fail* pada jaringan *VPLS redundant path* di sisi akses maupun *backbone network RSTP*.

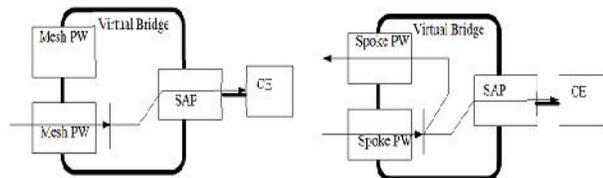
III. METODE PENELITIAN

Dalam penelitian ini akan di implementasikan *redundant path* pada *service VPLS* dengan Alcatel lucent sebagai perangkat *network backbone* dan cisco sebagai perangkat akses dengan variasi *Rapid Per-Vlan Spanning Tree Protocol* yang di simulasikan dalam *GNS3*. Implementasi *multi vendor* ini menjadi penting karena *survey* pada *real network* beroperasi dengan *multi vendor*.



Gambar 1, Perbandingan Service Model ALSRP Dengan PWE3 Model

Gambar 1 di atas merupakan referensi model *PWE3 (Pseudo Wire Emulation Edge-to-Edge)* dengan *ALSRP (Alcatel-Lucent Service Router Portfolio)* [7], model di atas merupakan keperluan dalam penyediaan *pseudowire emulation* untuk Ethernet yang menunjukkan *point to point service*. Arsitektur ini di terapkan juga pada *multipoint service* seperti *VPLS*.



Gambar 2, Ilustrasi Perbandingan Forwarding Mesh PW dan Spoke PW

ALSRP mengidentifikasi *service* dengan *service-ID*, model *service* menggunakan *logical service entity* untuk membangun *service* dengan atribut *Service Acces Point (SAP)*, *Service Distribution Path (SDP)*, *SDP-binding*. *ALSRP* membagi 2 tipe *pseudowire (PW)* yaitu *spoke* dan *mesh*.

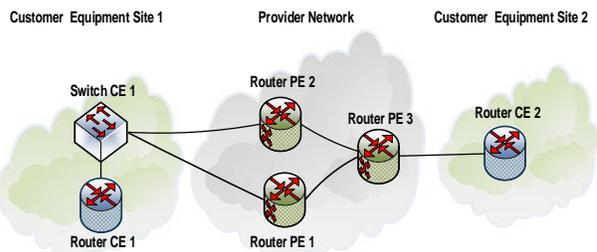
Gambar 2 merupakan Ilustrasi *forwarding packet* yang di terima dari *pseudowire*, *mesh- pseudowire* pada *VPLS* selalu *loop-free* ini dikarenakan *mesh- pseudowire* mematuhi aturan *split-horizon* ketika *forwarding traffic* antar *PE* yang bunyinya “do not relay traffic among mesh-pseudowire” yang bermaksud *split-horizon* melarang pengiriman *traffic* dari *mesh-pseudowire* ke sesama *mesh-pseudowire* dalam *service* yang sama.

Selain *mesh-pseudowire*, *VPLS* dapat menggunakan *spoke-pseudowire* sebagai solusi dari skalabilitas *VPLS* untuk koneksi antar *PE*, namun tipe *pseudowire* ini memungkinkan terjadinya masalah seperti *forwarding loop* dalam *VPLS* karena *spoke-pseudowire* tidak mematuhi aturan *split- horizon*. *Spoke-pseudowire* membolehkan pertukaran *traffic* ke semua *forwarding entity* dalam *service (mesh- pseudowire, spoke-pseudowire dan SAP)*. Maka pada *redundant spoke-pseudowire* perlu di terapkan *STP* untuk menghindari *forwarding loop* dan dapat juga di gunakan sebagai *alternate forwarding*.

A. Pertimbangan VPLS STP dengan Redundant Path

STP dalam *VPLS* di bedakan menjadi 2 istilah yaitu *transparan mode* dan *participant mode*. Dalam *transparan mode*, *STP* dalam status *shutdown* pada *VPLS*, *VPLS flood BPDU* yang di terima dari node lainnya namun tidak memproses *BPDU* tersebut. *VPLS* memperlakukan *STP BPDU* yang di terima sama seperti data *frame* lainnya yaitu *replicate BPDU* dan *flood* ke semua *pseudowire (mesh, spoke)* sama halnya dengan *BUM (broadcast, unicast, multicast) traffic*.

Dalam *participant mode*, *STP protocol enable* dalam *VPLS* dan memproses *BPDU packet* yang di terima dari node lain untuk memastikan tidak terdapat *forwarding loop*. *VPLS* mengkonsumsi dan menghasilkan *BPDU* untuk menentukan *root bridge*, *root port* dan *designated port*.



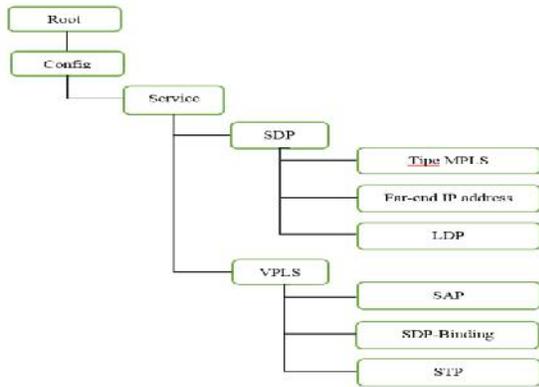
Gambar 3, Ilustrasi Service VPLS Redundant Path

Terlihat dari gambar merupakan jaringan *VPLS point to point*, tiga router *PE* sebagai jaringan *backbone*, *switch* sebagai jaringan akses, *redundant* di terapkan di sisi akses dengan variasi *Rapid-PVST+* dan juga *backbone* dengan *redundant pseudowire*. Dalam kategori *mandatory, mode Rapid-PVST+* memungkinkan untuk setiap *VLAN* yang ada pada *switch* maupun node *PE* memiliki *private spanning tree* masing-masing dimana penukaran *BPDU* hanya berlangsung pada *port grup vlan* dan *service VPLS* yang di ditetapkan. *STP* menggunakan variasi *BPDU* dengan *protocol multicast grup MAC address* dari *01-80-2c-xx-xx-xx*, beberapa *propriety STP* implementasinya menggunakan *MAC address* lain untuk *BPDU* destinasi *MAC address*. Dalam *participation mode* perlu di perhatikan *STP* kompatibel dengan perangkat node lain yang terkoneksi dengan *VPLS*. *VPLS ALSRP* kompetibel dengan beberapa variasi *STP* seperti *RSTP*, *Comp-dot1w*, *STP* dan Cisco *PVST+*. Pentingnya memperhatikan *STP* kompetibel

karena ketika terjadi perubahan topologi yang di sebabkan *link fail STP* tidak akan beroperasi. *STP* antar node mungkin akan memilih *forwarding* dan *blocking port* yang berbeda.

B. Tahap Konfigurasi Desain

Konfigurasi desain *VPLS Redundant Path* dengan penerapan *RSTP* ini di simulasikan pada *simulator GNS3*.

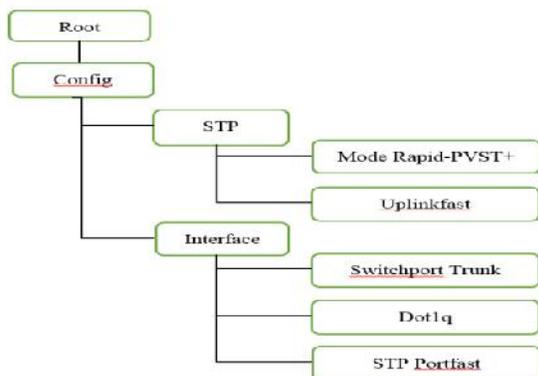


Gambar 4, Step Konfigurasi Service Pada PE

SDP merupakan *logical service direct* untuk mengkoneksikan antar node *PE* melewati *service tunnel*. *SDP* pada setiap *PE* menggunakan *MPLS Transport tunnel* untuk *transport traffic service VPLS* pada *network backbone* antar *PE*. Behubung *SDP* bersifat *unidireksional* maka *PE local* dan *remote* harus dibuat *SDP* agar terbentuk koneksi *bidireksional*. *SDP* ini menggunakan *LDP* untuk mendistribusikan informasi *router-id* untuk mencapai router *PE* lain dengan *label binding*. Pada *service VPLS* yang di simulasikan ini menggunakan *LDP-signaled* untuk membawa *traffic* melewati *MPLS tunnel*. *Targeted-LDP (TLDP)* di gunakan untuk memberikan sinyal status *pseudowire*.

Konfigurasi *Service VPLS* pada setiap member *PE* perlu di masukan *logical SAP* dan *SDP-Binding*, dalam simulasi ini di terapkan *SAP encapsulasi dot1q* untuk *forwarding packet* ke *customer site* dan *mesh SDP-binding/pseudowire* untuk *forwarding traffic* melewati *network backbone*.

Pada gambar 5 terlihat step konfigurasi pada switch, dengan topologi *redundant link* ini data *traffic* di kontrol oleh *RSTP* pada switch yang saling bertukar *BPDU* dengan *VPLS* untuk memastikan hanya satu *link active forwarding*.



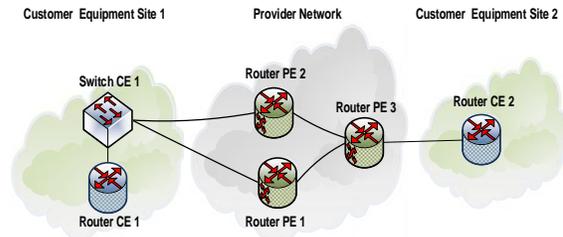
Gambar 5, Step Konfigurasi Pada Switch CE

BPDU ini berisikan *root-id*, *root path cost*, *bridge identifier (bridge-id)* dan *port identifier (port-id)*. *Ip address* di setting

point to point antar router *CE*. Sebagai perspektif *user/customer* segment *layer 3* hanya ada pada *end user* atau *segment customer* sendiri dan di sisi *VPLS/backbone provider* hanya menyediakan segment *layer 2* untuk *transport data frame*.

IV. HASIL DAN PEMBAHASAN

Berdasarkan desain *VPLS network* yang di simulasikan dengan *GNS3* di lakukan pengujian *availability network* dengan parameter *packet send*, *packet receive*, *packet loss* dan *durasi down time network* secara *real time*, hal ini untuk membuktikan peningkatan konektifitas *service VPLS redundant path* dengan *RSTP* sebagai *failure handling* pada *network*.



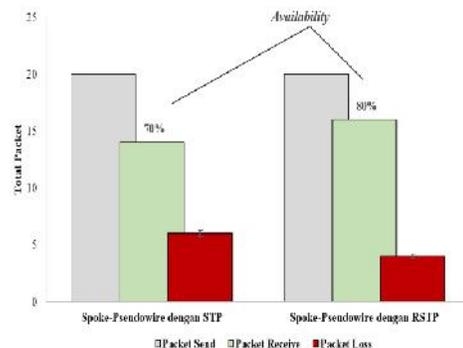
Gambar 6, Desain Redundant Path Pada Service VPLS

Konfigurasi tipe *pseudowire* pada *VPLS* di terapkan *mesh* dan *spoke* untuk membandingkan kualitas *network* dan perbandingan mekanisme pencegahan *loop STP* dan *RSTP* untuk *failure handling*, pada *spoke-pseudowire* diharuskan pemilihan *transparan* dan *participant mode* pada setiap *VPLS* karena perancangan yang tidak tepat akan mengakibatkan *forwarding loop* pada *VPLS*.

A. Hasil Pengujian Redundant Spoke Pseudowire VPLS

Hasil pengujian ini di dapat dengan cara *ICMP ping real time* dan mematikan *link* berdasarkan kemungkinan *network fail*.

Pengamatan ini di uji dengan pengiriman *20 packet* pada *network*, hasil pengujian ini menggunakan *VPLS redundant spoke-pseudowire* dengan membandingkan penerapan *STP* dan *RSTP*. *Spoke-pseudowire* melakukan pertukaran *traffic* ke semua *forwarding entity* dalam *service (mesh-pseudowire, spoke-pseudowire dan SAP)* dan membentuk *multi bridge network* sehingga dapat membentuk *loop forwarding*.



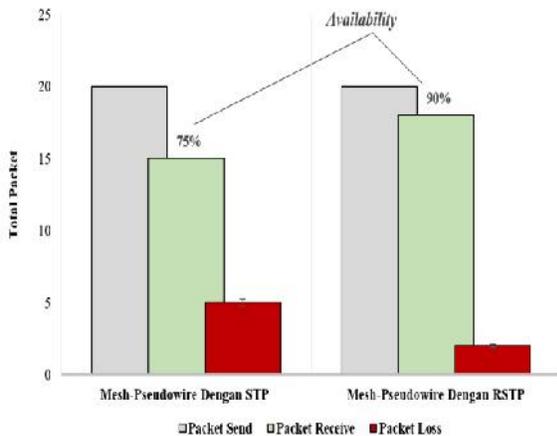
Gambar 7, Grafik Pengamatan Availability VPLS Spoke Pseudowire

Dalam desain ini mekanisme pencegahan *loop* berhasil membuat *single spoke-pseudowire* dalam status

backup/discard, *backup spoke-pseudowire* berubah menjadi *forwarding* hanya ketika *active spoke-pseudowire* down. Dengan ini *redundant pseudowire* akan beroperasi dengan baik dan tidak membentuk *forwarding loop* dan di dapat hasil *availability* dengan *RSTP* 80% dimana hasil ini dapat mempercepat waktu *konvergensi network* di bandingkan dengan *STP* yang di dapat hasil 70%.

B. Hasil Pengujian Redundant Mesh Pseudowire VPLS

Metode pengujian ini sama dengan *redundant spoke pseudowire VPLS* sebelumnya, yaitu *ICMP ping real time* dan mematikan *link* berdasarkan kemungkinan *network fail*.

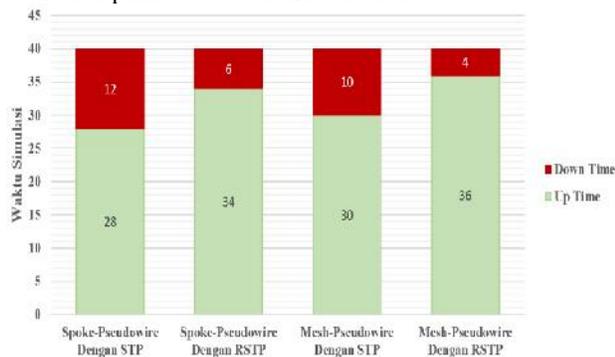


Gambar 8, Grafik Pengamatan Availability VPLS Mesh-Pseudowire

Hasil pengujian ini menggunakan *VPLS redundant mesh-pseudowire, mesh-pseudowire* pada *VPLS* selalu *loop-free* dalam *forwarding traffic* antar node dikarenakan aturan *split-horizon* maka mekanisme pencegahan *loop* ini hanya beroperasi pada *interface* akses *VPLS* kearah *customer*. Maka di dapat hasil *mesh-pseudowire* membentuk *single bridge* pada *network* dan tidak membuat *forwarding loop*, berdasarkan pengamatan *konvergensi RSTP* di dapat *availability network* 90% dimana ini mengindikasikan performa lebih tinggi di bandingkan *STP* yang hanya mendapat 75%.

C. Durasi Down Time Network

Dari pengujian yang di lakukan sebelumnya di dapat durasi *down time* pada *network* secara *real time*.



Gambar 9, Grafik Pengamatan Durasi Down Time Pada Network

Grafik di atas menampilkan durasi *down time* dan *up time* pada *network* ketika *network fail*, satuan waktunya detik. Berdasarkan hasil ini penerapan *VPLS mesh-pseudowire* dengan *RSTP* mengalami durasi *down* lebih sedikit dibandingkan dengan *VPLS spoke-pseudowire RSTP, spoke-pseudowire STP* dan *mesh-pseudowire STP*. Hal ini di karenakan mekanisme pencegahan *loop* dengan perbandingan *BPDU* hanya beroperasi pada akses *link VPLS* kearah *customer*. Sedangkan penerapan *VPLS spoke-pseudowire* dengan *STP* mengalami *down time* paling lama yaitu 12 detik dari 40 detik pengamatan. Durasi *down time redundant VPLS mesh-pseudowire* 6 detik dan *spoke-pseudowire* 4 detik dengan *RSTP* merupakan hasil yang paling optimal, hal ini di buktikan dengan *availability network* yang lebih tinggi di bandingkan dengan *STP*.

IV. KESIMPULAN

Berhubung kebutuhan *industry enterprise* saat ini semakin meningkat maka di perlukan *IT infrastruktur* dengan performa tinggi dan handal, dengan inovasi dari *service VPLS* melalui *MPLS pseudowire L2 ethernet bridging* untuk menyediakan koneksi *customer* yang terpisah secara geografis dan implementasi *RSTP* pada *redundant link* di sisi akses maupun *backbone* dapat memberikan solusi dari kebutuhan tersebut. *RSTP* digunakan untuk mencegah *forwarding loop* pada *redundant path*, sehingga hanya satu *link active* dalam *status forwarding*. Dari hasil simulasi *VPLS redundant link mesh-pseudowire* dan *spoke-pseudowire* dengan *RSTP* membuktikan bahwa performa *network* terjaga secara *end to end* karena hanya memakan sedikit *down time* dibandingkan dengan *STP* saat mengembalikan ke status *forwarding* dari *discard* sehingga *data frame* yang di kirim antar *CE* akan terjaga dan tercapainya *SLA* antara *customer* dan *ISP*.

V. DAFTAR PUSTAKA

- [1] Madhusanka Liyanage, Mika Ylianttila, Andrei Gurtov, "A Novel Distributed Spanning Tree Protocol for Provider Provisioned VPLS Networks," IEEE ICC, 2014
- [2] A. Sajjasi, Ed., F. Brockners, D. Mohan, Ed., Y. Serbest, "Virtual Private LAN Service (VPLS) Interoperability with Customer Edge (CE) Bridges", IETF RFC 6246, Juni 2011
- [3] Guitang Wang, Jun Liu, Liming Wu, Huan Yao, "Three-rings Redundancy Industrial Ethernet based on RSTP", International Conference on Signal Processing Systems, 2009
- [4] K. Kompella, Ed, Y. Rekhter, ed, "Virtual Private LAN Service (VPLS) Using BGP for Auto-Discovery and Signaling", IETF RFC 4761, Januari 2007
- [5] M. Lasserre, ed, V. Kompella, ed, "Virtual Private LAN Service (VPLS) Using Label Distribution Protocol (LDP) Signaling", IETF RFC 4762, Januari 2007
- [6] R. Gu, J. Dong, M. Chen, Q. Zeng, "Analysis of Virtual Private LAN Service (VPLS) Deployment", Huawei Technologists China Telecom, Maret 2011
- [7] Zhuo (Frank) Xu, "Designing and Implementing IP/MPLS-Based Ethernet Layer 2 VPN Service", Wiley Publishing, Inc., Indianapolis, Indiana, 2010
- [8] R. Mohtasin, P.W.C. Prasad, Abeer Alsadoon, G. Zajko, A. Elchouemi, Ashutosh Kumar Singh, "Development of a Virtualized Networking Lab using GNS3 and VMware Workstation", IEEE WiSPNET 2016 conference, 2016