

## Implementasi *Service Distribution Point* Pada Jaringan MPLS *Static Route* Menggunakan Metode LDP Dan LSP

Irmayani; Ivan Josua Pardede  
Program Studi Teknik Elektro, Fakultas Teknik,  
Institut Sains dan Teknologi Nasional, Jakarta  
e\_mail: [ir.irmayani@gmail.com](mailto:ir.irmayani@gmail.com)

### Abstrak

VPLS merupakan salah satu teknologi MPLS yang dapat menghubungkan beberapa kawasan geografi yang terpisah dengan mengemulasikan *bridging domain*. Pelanggan yang memiliki layanan VPLS akan memiliki segmen *Local Area Network* yang sama, walaupun secara geografis kondisinya berjauhan. Dalam kasus, beberapa pelanggan membutuhkan kualitas layanan yang baik. Pelanggan menginginkan agar koneksi ke tujuan tidak lambat dan terputus. Maka dibutuhkan suatu sistem redundansi agar jalur komunikasi tidak terputus dan dibutuhkan juga suatu sistem agar trafik tidak hanya dalam satu jalur saja. Untuk mengatasi permasalahan tersebut dibutuhkan metode LDP dan LSP yang diterapkan pada VPLS. Dengan metode tersebut dapat diterapkan sistem redundansi, ketika jalur utama mati maka trafik berpindah ke jalur backup. selain itu, adanya metode LSP, trafik pelanggan dapat dipisah dengan pelanggan lainnya yang melalui jalur LDP sehingga tidak akan menumpuk pada satu jalur saja. Pengujian SDP dengan metode LDP dan LSP ini diukur dengan dua cara. Pertama mengirimkan trafik ke host tujuan sehingga dapat dilihat bahwa trafik menggunakan LSP dapat terpisah dari trafik yang menggunakan LDP. Kedua ialah melakukan redundansi. Hasil pengujian menunjukkan bahwa dengan menggunakan kedua metode tersebut dapat diterapkan sistem redundansi ketika jalur utama terputus dan bekerja dengan baik dalam membagi trafik dan jalur yang dapat dipakai *customer*. Dengan demikian SDP dengan metode LDP dan LSP dapat di implementasikan pada jaringan MPLS.

Kata kunci : MPLS, VPLS, SDP, LSP, LDP

### Abstract

*VPLS MPLS technology is one that can connect multiple separate geographic region to emulate bridging domain. Customers with VPLS services will have the same Local Area Network segment, even though they are geographically far apart. In cases where multiple customers require good service quality, customers want the connection to the destination to be fast and uninterrupted. Therefore, a redundancy system is needed to ensure that the communication path does not break, and a system is also required to prevent traffic from using only a single path. To address these issues, the LDP and LSP methods are applied to VPLS. With these methods, a redundant system can be implemented, where if the primary path fails, traffic will switch to the backup path. Additionally, with the LSP method, customer traffic can be separated from other customers' traffic using the LDP path, ensuring that it does not congest a single route. The SDP testing with the LDP and LSP methods is measured in two ways. First, traffic is sent to the destination host to observe that traffic using LSP is separated from traffic using LDP. Second, redundancy is tested. The test results show that by using both methods, a redundancy system can be applied when the primary path is interrupted and works well in dividing traffic and channels that can be used by customers. Thus, SDP with the LDP and LSP methods can be implemented in MPLS networks.*

*Keywords: MPLS, VPLS, SDP, LSP, LDP*

### 1. PENDAHULUAN

Jaringan Metro *Ethernet* merupakan salah satu bridge dari suatu jaringan yang dapat menghubungkan LAN dengan WAN maupun ke area *backbone network*. Umumnya hal tersebut terdapat pada jaringan *Service provider*. Salah satu perangkat yang dapat mendukung jaringan metro *ethernet* tersebut adalah Alcatel Lucent. Beberapa layanan yang terdapat pada Alcatel lucent, seperti *Virtual Private LAN Service* (VPLS) dan *Virtual Private Routed Network* (VPRN). VPLS atau yang dikenal dengan *Transparent LAN Service* atau E-LAN *Service* adalah teknologi *layer dua* yang bersifat *multipoint to multipoint* VPN dan dapat menyambungkan antara beberapa site

dalam *single bridge domain* (SBD) dengan menggunakan jaringan IP/MPLS. VPLS dapat menghubungkan beberapa kawasan yang ter pisah secara geografi dengan mengemulasi kan *bridging domain*. Pelanggan yang memiliki layanan VPLS akan memiliki segmen *Local Area Network* yang sama, walaupun secara geografis kondisinya berjauhan. VPRN merupakan VPN *Routing and Forwarding* yang menjadi kunci di teknologi MPLS. ISP biasanya menggunakan VPRN untuk memisahkan VPN untuk pelanggannya. Pada kedua arsitektur tersebut terdapat 2 komponen yang bisa dimasukkan, yaitu SAP dan SDP. Salah satu komponen tersebut yaitu *Service Access Point* (SAP), merupakan suatu

layanan yang dapat menghubungkan akses (jaringan non VPLS) dan jaringan MPLS. Pada SAP inilah pelanggan terdistribusikan. Sedangkan SDP bertugas untuk mengalirkan paket trafik dari pelanggan ke pelanggan lainnya. SDP dapat mengirimkan paket trafik dari jaringan yang berbeda.

Pada penelitian sebelumnya yaitu Analisis Perbandingan Kinerja Multiprotocol Label Switching dengan Mekanisme Label Distribution Protocol dan Traffic Engineering menunjukkan bahwa MPLS-TE memiliki kinerja yang lebih baik karena pengiriman dilakukan menggunakan rute eksplisit dalam tunnel sehingga tidak perlu mencari designated router seperti pada MPLS LDP yang akan melakukan pencarian best path saat terjadinya percabangan. Penggunaan rute cadangan juga membantu MPLS-TE untuk mempersingkat waktu convergence saat terjadinya kegagalan dalam pengiriman [1].

Hasil dari penelitian Pemanfaatan Protokol LDP over RSVP Dengan Metode Routing IS- IS Pada Jaringan MPLS Untuk Mengoptimalkan KQI menunjukkan bahwa protocol LDP over RSVP terbukti dapat mengatasi terjadinya degradasi KQI throughput & delay yang disebabkan oleh link kongesti pada jaringan backbone NGN [2].

Pelanggan membutuhkan kualitas layanan yang baik. Availabilitas suatu jaringan merupakan salah satu hal penting yang harus diperhatikan. Oleh karena itu, *availability link* adalah hal yang sangat penting karena berkaitan dengan keseterediaan sebuah layanan dari suatu *provider*. Pelanggan menginginkan agar koneksi ke tujuan tidak lambat dan terputus. Maka dibutuhkan suatu sistem redundansi agar komunikasi tidak terputus dan dibutuhkan juga suatu sistem agar trafik tidak hanya dalam satu jalur saja. Untuk itu dengan metode LDP dan LSP diharapkan dapat mengatasi permasalahan. Dengan metode tersebut dapat diterapkan sistem redundansi ketika jalur utama mati sehingga trafik berpindah ke jalur backup. Selain itu, adanya metode LSP, trafik pelanggan dapat dipisah dengan pelanggan lainnya melalui jalur LDP sehingga tidak akan menumpuk pada satu jalur saja.

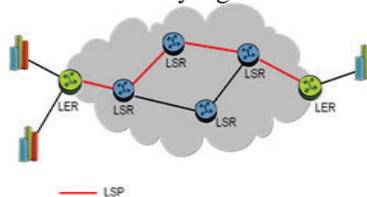
Konfigurasi dan topologi dasar jaringan yang disimulasikan adalah konfigurasi *Metro Ethernet* untuk layanan jaringan seluler milik PT. Indosat. Parameter yang diamati hanya di sisi perangkat *router* yaitu 7x50 Alcatel Lucent. Parameter yang diuji hanya redundansi dan pembagian trafik.

## 2. DESKRIPSI PEMBAHASAN

### 2.1 Multi Protocol Label Switching (MPLS)

MPLS adalah suatu metode *forwarding* (meneruskan data melalui suatu jaringan dengan menggunakan informasi dalam label yang dilekatkan pada IP), sehingga memungkinkan *router* untuk meneruskan paket dengan hanya melihat label dari paket itu, tidak perlu melihat IP address tujuannya. Hasil pengujian data pada Virtual Private Network MPLS dengan Secure Socket Layer untuk Pengamanan Komunikasi Video Conference, menunjukkan bahwa pengiriman informasi yang dilakukan dengan pengamanan VPN SSL tidak dapat dilihat informasi protocol seperti IP address, user ID, RTP dan SIP karena semua data telah dienkripsi dan dikapsulisasi [3]. Konsep dasar MPLS adalah teknik peletakan label dalam setiap paket yang dikirim dalam jaringan. MPLS bekerja dengan cara melabeli paket-paket data untuk memuat rute dan prioritas pengiriman paket tersebut. Label tersebut akan memuat informasi penting yang berhubungan dengan informasi routing suatu paket. Teknik pelabelan ini biasa disebut dengan label *switching*. Tiap paket hanya dianalisa sekali di dalam *router*, dimana paket tersebut masuk ke dalam jaringan MPLS untuk pertama kali [4].

Gambar 1 menunjukkan *router* yang bertindak sebagai Label Edge Router (LER) mengkoneksikan semua jaringan diluar MPLS domain. Untuk dapat berkomunikasi dengan LER yang lain, *router* terkoneksi dengan *router* yang bertindak sebagai LSR untuk *forwarding* MPLS *router* LER yang akan dikoneksikan.



Gambar 1 Terminologi dari MPLS [4].

Proses utama dari Label Switching meliputi proses *forwarding* atau pengiriman paket dan proses kontrol. Dalam proses ini *router* akan menggunakan informasi label untuk melakukan pengiriman paket. Ketika sebuah *router* yang digunakan sebagai LSR menerima sebuah paket berlabel, maka label tersebut akan digunakan sebagai sebuah indeks *Label Forwarding Information Base* (LFIB). Masing-masing entry dari LFIB ini terdiri dari sebuah *incoming label* dan sub entry lainnya yang meliputi *outgoing label*, *outgoing interface* dan *outgoing link level information*.

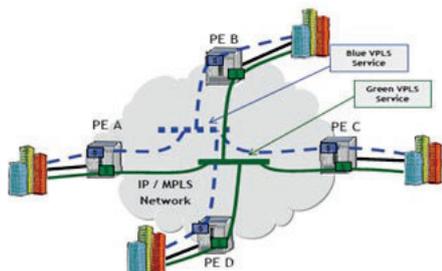
Proses pengiriman sebuah paket pada MPLS berbasis pada teknik penggantian label atau *label swapping*. Jadi dalam setiap sub entry

tersebut, LSR akan mengganti *incoming label* dengan sebuah *outgoing label* dan mengirimkan paket tersebut keluar setelah melewati sebuah *outgoing interface* yang sesuai dengan *outgoing link level information*.

## 2.2 Virtual Private LAN Service (VPLS)

VPLS (Virtual Private LAN Service) merupakan salah satu layanan yang dapat digunakan pada jaringan IP/MPLS *Metro Ethernet*. VPLS adalah suatu layanan multipoint layer 2 (gambar 2) yang memungkinkan beberapa lokasi pelanggan dapat terhubung dalam domain tunggal yang terkandung dalam jaringan IP/ MPLS. VPLS menggunakan IP Tunnel sebagai protokol yang digunakan dalam jaringan. Pada pandangan pelanggan seolah-olah semua site terkoneksi pada satu VLAN. Penyedia layanan dapat menggunakan infrastruktur IP/MPLS untuk menyediakan berbagai jenis layanan [5].

Pada gambar 2 dijelaskan suatu pelanggan terkoneksi dengan pelanggan lainnya di *router* berbeda menggunakan VPLS, pelanggan yang terhubung dengan pelanggan lainnya harus mempunyai ID yang sama supaya pelanggan tersebut mempunyai identitas sendiri dari VPLS pelanggan lain di *router* tersebut, dan trafik juga dipisah berdasarkan identitas tersebut.



Gambar 2 Layanan Ethernet multipoint layer 2 (VPLS) [5]

Dalam gambar 2, pelanggan PE A terkoneksi dengan PE B, C dan D. Keempat pelanggan tersebut terkoneksi dengan ID yang sama yaitu "green VPLS Service".

Karena VPLS mengemulasi layanan *switched ethernet*, *forwarding* alamat MAC Database (FDB) harus dikelola oleh setiap VPLS. Ketika frame *unicast* dengan alamat sumber yang tidak diketahui tiba pada SAP atau SDP, VPLS mempelajari alamat, dengan cara yang sama bahwa *ethernet switch* mempelajari alamat MAC pada *port*-nya. VPLS FDB mengaitkan alamat MAC dengan SAP dan SDP.

Pada saat *frame ethernet* tiba pada SAP atau SDP, *lookup* dilakukan di FDB untuk alamat tujuan. Jika ada entri untuk alamat, *frame* diteruskan ke SAP sesuai atau SDP. Jika tidak ada entri untuk alamat, *frame* membanjiri semua SAP lainnya dan SDP, yang mana sangat

mirip dengan *flooding frame* yang tidak diketahui pada *ethernet switch*.

## 2.3 VPRN (Virtual Private Routed Network)

Setiap Virtual Private Routed Network (VPRN) terdiri dari satu set lokasi pelanggan terhubung ke satu atau lebih *router* PE. Setiap *router* PE terkait memantau IP forwarding table terpisah untuk setiap VPRN. Selain itu, *router* PE bertukar informasi routing dikonfigurasi atau belajar dari semua situs pelanggan melalui MP-BGP peering. Setiap rute yang dipertukarkan melalui protokol MP-BGP termasuk rute *distinguisher* (RD), yang mengidentifikasi asosiasi VPRN.

Penyedia layanan (ISP) menggunakan *routing* untuk bertukar dari VPN khususnya rute antara *router* PE yang melekat pada VPN tsb. Hal ini dilakukan dengan cara yang memastikan bahwa rute dari VPN yang berbeda tetap berbeda dan terpisah, bahkan jika dua VPN memiliki ruang alamat yang tumpang tindih. Dalam VPN tertentu, *router* PE mendistribusikan informasi rute dari dan ke *router* CE. Karena *router* CE tidak mengintip satu sama lain, tidak ada overlay terlihat dengan algoritma *routing* VPN [6].

Setiap VPRN terdiri dari satu set lokasi pengguna terhubung ke satu atau lebih penyedia *router*. Setiap asosiasi menyediakan *router* terpisah IP *forwarding table* untuk setiap VPRN. Pengguna dapat mengatur IP sendiri dan memilih preferensi sendiri untuk protokol *routing*. Jaringan penyedia memiliki infrastruktur bersama, menawarkan layanan untuk beberapa pengguna, memisahkan *routing* dan *forwarding* paket masing-masing pengguna. Setiap pengguna *router* menjadi rekan *routing router* penyedia yang langsung terhubung, tidak *peer to peer* ke pengguna lain. Selain itu, penyedia dapat menawarkan berbagai layanan IP-enabled kepada penggunanya. Sebuah *router* pengguna menyediakan *router* penyedia dengan informasi *routing* untuk jaringan pribadi pengguna. Terlepas dari *routing* dipertukarkan antara pengguna dan penyedia *router*, menyediakan infrastruktur ditetapkan sedemikian rupa sudut pandang dari *router* pengguna, yang langsung terhubung pada lapisan 3. Penyedia layanan dapat menggunakan kembali infrastruktur IP/MPLS untuk menawarkan beberapa layanan kepada setiap pengguna.

## 2.4 Routed Virtual Private LAN Services (RVPLS)

VPLS Routed (R-VPLS) memungkinkan VPLS dapat berkomunikasi dengan *Integrated Edge Services* (IES) atau antarmuka VPRN. Host dalam subnet yang sama berkomunikasi

langsung satu sama lain tanpa perlu *router*, tetapi setiap komunikasi dengan host di luar subnet membutuhkan routing. Dengan VPLS routed, dapat menggunakan bridging untuk tujuan lokal bila memungkinkan dan routing untuk tujuan non-lokal yang tidak dapat dicapai secara langsung. R-VPLS dapat dibandingkan dengan Switch LAN Ethernet dan *Router*. Ketika IP tujuan tidak lokal, metro akan mencoba untuk rute trafik melalui antarmuka VPRN/IES berdasarkan tabel forwarding IP, sementara trafik lokal diaktifkan dan diteruskan berdasarkan tabel VPLS forwarding. Fungsi Routed VPLS menyediakan platform metro dengan kemampuan untuk komunikasi internal, contoh menghubungkan VPLS ke antarmuka L3 VPRN/IES IP, untuk menghindari kebutuhan untuk koneksi fisik [6].

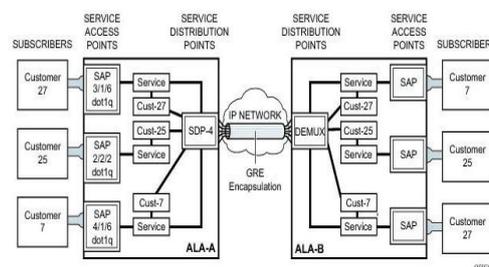
**2.5 Service Access Point (SAP)**

SAP adalah entitas logis yang berfungsi sebagai titik pengguna untuk akses ke layanan. Setiap layanan pengguna dikonfigurasi dengan setidaknya satu SAP. SAP berfungsi sebagai antarmuka antara jaringan penyedia layanan dan pengguna akhir. Dalam beberapa kasus, SAP bisa juga dikaitkan dengan port PW (Pseudowire)/PW SAP. Pseudowire adalah sebuah teknik yang digunakan untuk membawa jenis layanan (seperti Ethernet, TDM, atau bahkan saluran suara) melalui jaringan MPLS dengan cara "meniru" layanan tersebut di atas jaringan IP/MPLS. Dengan kata lain, pseudowire memungkinkan transportasi layanan layer 2 (misalnya Ethernet) melalui jaringan layer 3 (IP/MPLS) dengan menjamin bahwa data di antaranya dapat berjalan secara transparan seperti jika berada pada jaringan layer 2 biasa. PW SAP berfungsi untuk menghubungkan antarmuka yang digunakan dalam pseudowire ini dengan sistem manajemen yang lebih luas, seperti Enhanced Service Management (ESM). Jenis enkapsulasi yang digunakan bergantung pada jenis port atau saluran dan pada kemampuan perangkat downstream (perangkat yang menerima data) yang terhubung. Contoh jenis enkapsulasi yang disebutkan adalah IEEE 802.1Q (atau dot1q), yang digunakan untuk mengenkapsulasi frame Ethernet dengan tag VLAN untuk membedakan trafik antar layanan yang berbeda [7]. Sebuah SAP dibuat pada port atau saluran tertentu dengan mengidentifikasi layanan dengan ID enkapsulasi tertentu.

**2.6 Service Distribution Point (SDP)**

SDP mengidentifikasi endpoint dari sebuah tunnel namun tidak directional. Secara umum lebih, SDP mengacu terowongan layanan itu sendiri. SDP berakhir pada farend router lain,

yang bertanggung jawab untuk mengarahkan aliran paket ke egress layanan SAP pada perangkat. Ketika sebuah SDP terikat ke layanan, layanan ini disebut sebagai layanan terdistribusi. Sebuah layanan terdistribusi terdiri dari konfigurasi dengan setidaknya satu SAP pada node lokal, SAP pada node jauh, dan SDP mengikat yang mengikat layanan ke layanan tunnel. Untuk mengkonfigurasi layanan dari router-A ke router-B, SDP ID pada router-A harus ditentukan selama pembuatan layanan untuk mengikat layanan ke tunnel (SDP). Jika tidak, lalu lintas layanan tidak diarahkan ke farend dan perangkat tujuan tidak dapat berpartisipasi dalam layanan (tidak ada layanan). Untuk mengkonfigurasi layanan yang terdistribusi dari router-B ke router-A, SDP ID di sisi router-B harus ditentukan [7].



Gambar 3 Proses Komunikasi SDP [7]

Pada gambar 3 menunjukkan proses komunikasi SDP untuk menghubungkan antara *Service* dengan *Service* lainnya. *Service* SAP di-binding kedalam *Service* MPLS. Layanan tersebut dapat terkoneksi dengan layanan lainnya menggunakan SDP sebagai tunnelnya.

SDP memiliki nilai implisit Maximum Transmission Unit (MTU) karena layanan dilakukan melalui tunnel enkapsulasi, dan SDP berfungsi sebagai pintu masuk ke tunnel tersebut. MTU dapat dikonfigurasi (dalam oktet), di mana frame yang ditransmisikan tidak boleh lebih besar dari nilai MTU. Dengan MPLS, MTU pada port jaringan memungkinkan penambahan label untuk transmisi jaringan MPLS. Frame Ethernet yang dikirim dari port jaringan menuju jaringan inti MPLS (atau router P) dapat memiliki ukuran lebih besar untuk menyertakan label MPLS tanpa perlu memfragmentasi frame yang besar.

**2.7 Static Route**

Ruting statik dikonfigurasi oleh administrator dan tidak menggunakan dynamic protokol routing. Ketika ada perubahan dalam jaringan, atau kegagalan terjadi antara dua node didefinisikan statis, trafik tidak akan dialihkan. Apa pun yang akan melewati jalur tersebut akan terkena dan harus menunggu untuk perbaikan kegagalan tersebut. Untuk routing static

diperbarui oleh administrator. Sebagai perbandingan, rute dinamis dibuat dari pertukaran data antara router yang menggunakan protokol routing umum. rute dinamis otomatis berubah karena perubahan topologi.

**2.8 Label Distribution Protocol (LDP).**

LDP merupakan suatu prosedur yang digunakan untuk menginformasikan ikatan label yang telah dibuat dari satu LSR ke LSR lainnya dalam satu jaringan MPLS. Dalam arsitektur jaringan MPLS, sebuah LSR yang merupakan tujuan atau hop selanjutnya akan mengirimkan informasi tentang ikatan sebuah label ke LSR yang sebelumnya mengirimkan pesan untuk mengikat label tersebut bagi rute pakatnya [8]. Teknik ini biasa disebut distribusi label downstream on demand.

LDP adalah protokol standar pada setiap LSR untuk saling bertukar informasi label dan menyimpannya ke dalam LIB (Label Information Base) masing-masing. Setelah itu, informasi label dalam LIB diakses ke dalam data plane untuk ditawarkan pada fungsionalitas MPLS untuk menambahkan label ke dalam FIB untuk menghubungkan ke next hop, hasil dari penggabungan antara LIB dan FIB adalah LFIB yang berisi nomor label, alamat tujuan, outgoing interface (exit interface) dan next hop [9].

**2.9 Label Switched Path (LSP)**

Network MPLS terdiri atas sirkit yang disebut label-switched path (LSP), yang menghubungkan titik-titik yang disebut label-switched router (LSR). Setiap LSP dikaitkan dengan sebuah forwarding equivalence class (FEC), yang merupakan kumpulan paket yang menerima perlakuan forwarding yang sama di sebuah LSR. FEC diidentifikasi dengan pemasangan label. Untuk membentuk LSP, diperlukan suatu protokol persinyalan. Protokol ini menentukan forwarding berdasarkan label pada paket. Label yang pendek dan berukuran tetap mempercepat proses forwarding dan mempertinggi fleksibilitas pemilihan path. Hasilnya adalah network datagram yang bersifat lebih connection-oriented [8].

**2.10 Open Shortest Path First (OSPF)**

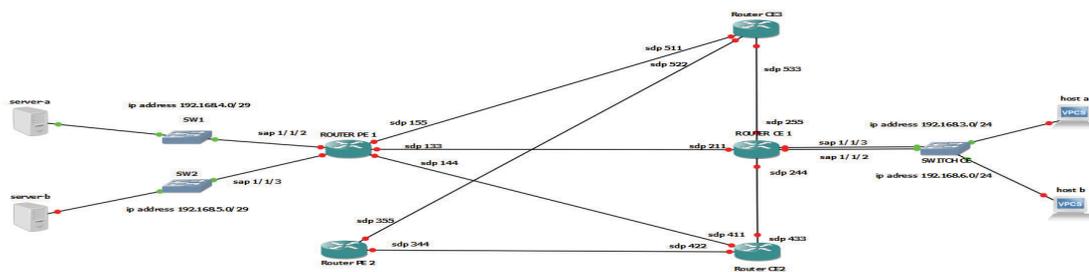
Open Shortest Path First adalah protokol routing otomatis (Dynamic Routing) yang mampu menjaga, mengatur dan mendistribusikan informasi routing antar jaringan mengikuti setiap perubahan jaringan secara dinamis. Pada OSPF dikenal sebuah istilah *Autonomous System* (AS) yaitu sebuah gabungan dari beberapa jaringan yang sama sifat routingnya dan memiliki kesamaan metode serta policy pengaturan jaringan, yang semuanya dapat dikendalikan oleh network administrator. Dan kebanyakan fitur ini digunakan untuk manajemen dalam skala jaringan yang sangat besar. Oleh karena itu untuk mempermudah penambahan informasi routing dan meminimalisir kesalahan distribusi informasi routing, maka OSPF bisa menjadi sebuah solusi [10], [11].

OSPF termasuk di dalam kategori IGP (Interior Gateway Protocol) yang memiliki kemampuan Link-State dan Algoritma Dijkstra yang jauh lebih efisien dibandingkan protokol IGP yang lain. Prinsip kerja dari OSPF adalah Setiap *router* membuat Link State Packet (LSP), setiap *router* menghitung jalur terpendek (Shortest Path) ke semua neighbour berdasarkan cost routing. LSP akan didistribusikan oleh DR ke *router* neighbour lain dalam 1 area sehingga semua *router* neighbour akan melakukan perhitungan ulang jalur terpendek.

**3. PERANCANGAN DAN IMPLEMENTASI**

**3.1 Rancangan Sistem**

Topologi jaringan MPLS yang disimulasi terdiri dari 5 *router*. Dalam jaringan ini, menggunakan topologi jaringan yang berisi *router* R1 dan R2 serta 3 *router* CE. Selain itu terdapat server dan host yang akan dihubungkan melalui *router* tersebut. Agar setiap *router* saling terhubung, maka konfigurasi pada setiap *router* harus benar. Topologi jaringan dapat dilihat pada gambar 4.



Gambar 4 Topologi Jaringan

Pada jaringan ini terdapat beberapa layanan MPLS, yaitu layanan VPLS dan VPRN. Layanan VPLS merupakan layanan didalam MPLS yang menjalankan sistem layer 2 switch ethernet. Setiap *router* mempunyai ID *Service* VPLS yang sama. Selain itu VPLS mempunyai SDP yang diinputkan kedalam *Service* tersebut. SDP berfungsi sebagai jalur atau tunnel yang akan dilalui trafik servis dari *router* ke *router* lainnya. SDP dapat berfungsi menjadi redundan jika link ke arah tujuan mati maka jalur kearah tujuan akan berpindah sesuai path selanjutnya yang sudah ditentukan.

Selain VPLS, terdapat layanan VPRN yang merupakan sebuah koneksi sendiri melalui jaringan public. Fungsi dari VPRN bertujuan sebagai IP forwarding, dimana informasi routing *Service* host dan server lainnya akan didistribusikan melalui *Service* ini. Interface didalam VPRN adalah interface RVPLS dan interface jaringan non MPLS.

Interface RVPLS digunakan sebagai komunikasi antar VPLS antar *router* agar dapat terkoneksi dengan perangkat diluar layanan di *router* lainnya. Sementara interface ke arah jaringan non MPLS digunakan untuk mengkoneksikan perangkat yang masuk kedalam jaringan MPLS. didalam interface ini terdapat SAP. SAP pada interface ini merupakan port logik yang mengkoneksikan perangkat seperti server dan host untuk dapat berkomunikasi didalam layanan MPLS.

Pada layanan MPLS agar *customer* untuk saling terkoneksi dengan *customer* lainnya, maka dibuat SDP agar *customer* dapat mengirim dan menerima trafik dari *customer* lainnya. SDP merupakan sebuah tunnel yang dapat membawa beberapa jaringan dari *customer* yang berbeda. Dalam prosesnya komunikasinya, SDP dapat berkomunikasi mengikuti koneksi antar *router* yang secara langsung ataupun tidak langsung. Koneksi *router* secara langsung, yaitu koneksi *direct* antara kedua *router*. Lalu koneksi secara tidak langsung, ketika *router* tidak mempunyai koneksi *direct* ke *router* tujuan namun *router* asal mempunyai koneksi ke *router* lain. *Router* lain tersebut mempunyai koneksi ke *router* tujuan.

Ada 2 metode melakukan koneksi antar SDP. Metode yang pertama ialah dengan menggunakan LDP (Label Distribution Point). Dengan menggunakan LDP, komunikasi SDP mengikuti jalur yang primary yang sudah ditentukan oleh kondisi jalur pada OSPF *router*. Didalam protocol OSPF terdapat metric yang bertujuan memutuskan jalur mana yang lebih diutamakan. Metric yang terkecil akan dipilih sebagai jalur utama. Jika terdapat link putus, maka rute SDP pun berubah mengikuti jalur yang lainnya secara otomatis. Namun pada permasalahannya jika trafik tersebut hanya mengalir ke salah satu path saja, akan timbul permasalahan. Beberapa contoh kasus yang terjadi adalah congestion dan hal tersebut akan mengganggu *customer*. Untuk mengatasi problem tersebut maka dipakai metode LSP agar dapat memisahkan trafik dari *customer* dengan *customer* lainnya. Metode LSP ialah jalur statik. dimana jalur kearah tujuan dapat ditentukan sendiri. Ada 2 Parameter pemilihan jalur LSP.

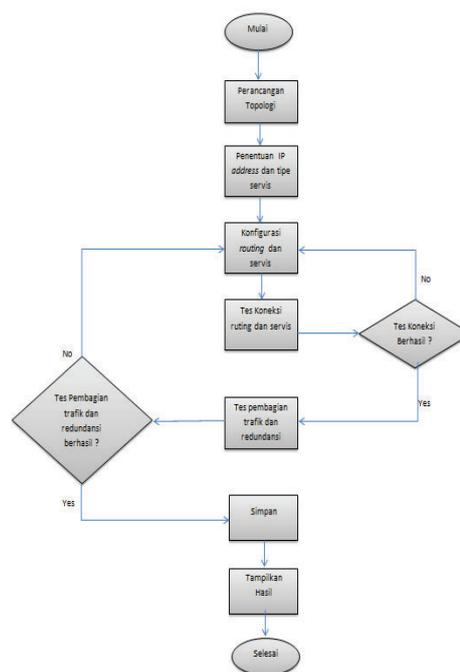
1. Jalur yang akan dilalui di cek terlebih dahulu utilitas trafik ke *router* yang akan dilalui tidak tinggi dan tidak terdapat packet loss dan *router* yang dilalui tidak bermasalah perangkat-nya.
2. Jalur yang dilalui harus dicek terlebih dahulu apakah kapasitas port tersebut mencukupi. Sebagai contoh trafik tujuan ialah 3Gb dengan kapasitas port 10Gb. Maka jalur yang akan dilalui harus dapat memenuhi kapasitas tersebut.

### 3.2. Implementasi metode LDP dan LSP

Pada layanan MPLS agar pelanggan dapat saling terkoneksi dengan pelanggan lainnya, maka dibuat SDP agar dapat mengirim dan menerima trafik dari pelanggan lainnya. SDP merupakan sebuah tunnel yang dapat membawa beberapa jaringan dari *customer* yang berbeda. Dalam proses komunikasinya, SDP dapat berkomunikasi mengikuti koneksi antar *router* yang secara langsung ataupun tidak langsung. Koneksi *router* secara langsung, yaitu koneksi *direct* antara kedua *router*. Lalu koneksi secara tidak langsung, ketika *router* tidak mempunyai koneksi *direct* ke *router* tujuan namun *router* asal mempunyai koneksi ke *router* lain. *Router* lain tersebut mempunyai koneksi ke *router* tujuan. Ada 2 metode koneksi yang digunakan antar SDP. Metode yang pertama ialah dengan menggunakan LDP. Dengan menggunakan

LDP, komunikasi SDP mengikuti jalur yang primary yang sudah ditentukan oleh kondisi jalur pada OSPF router. Didalam protocol OSPF terdapat metric yang bertujuan memutuskan jalur mana yang lebih diutamakan. Metric yang terkecil akan dipilih sebagai jalur utama. Jika terdapat link putus, maka rute SDP pun berubah mengikuti jalur yang lainnya secara otomatis. Namun pada permasalahannya jika trafik tersebut hanya mengalir ke salah satu path saja, akan timbul permasalahan. Beberapa contoh kasus yang terjadi adalah congestion dan hal tersebut akan mengganggu pelanggan. Untuk mengatasi problem tersebut maka dipakai metode LSP agar dapat memisahkan trafik dari customer dengan customer lainnya. Metode LSP ialah jalur statik, dimana jalur kearah tujuan dapat ditentukan sendiri.

Implementasi dilakukan melalui beberapa proses agar simulasi dapat berjalan dengan baik. Proses perancangan meliputi beberapa tahap (gambar 5). Tahapan pertama melakukan perancangan topologi. Perancangan topologi meliputi perangkat yang digunakan, topologi jaringan. Lalu pada tahapan yang kedua dilakukan penentuan jumlah network dan service yang dipakai. Dalam tahapan ini, ditentukan IP address dan jenis layanan Service yang digunakan. Tahapan ketiga, terdapat tahapan konfigurasi routing protocol dan service. Dimana pada tahapan ini dilakukan proses perutingan agar router dapat terkoneksi dengan router yang lain. Kemudian dilakukan konfigurasi layanan MPLS meliputi tipe Service VPLS, VPRN sebagai jalur host ke arah host lain atau server. Selanjutnya pada pengujian akan diuji terlebih dahulu koneksi ruting dan servis sebelum memulai tahapan pengujian. Pada tahapan terakhir dilakukan pengujian pembagian trafik, dengan menggunakan LSP. Didalam LSP akan disetting beberapa opsi path yang akan dilalui. Disini akan di cek trafik pada jalur yang menggunakan LDP dan jalur dengan LSP akan terpisah. Kemudian dilakukan pengujian redundansinya dengan metode LDP dan LSP, ketika jalur putus maka trafik akan berpindah ke jalur berikutnya. Diagram alur dapat dilihat pada gambar 5.



Gambar 5 Diagram alur Implementasi

#### 4. PENGUJIAN DAN ANALISA

##### 4.1 Pengujian Server ke customer

Pengujian pertama ialah melakukan verifikasi ruting server dan customer. Dalam hal ini untuk melihat router sudah dapat terjangkau/terkoneksi. Pada tabel 1 menunjukkan bahwa interface customer pada router R1 dan R3 sudah terkoneksi.

Tabel 1 verifikasi Ping Service R1 ke R3

```

A:Router-R1# show router 32225 route-table
=====
Route Table (Service: 32225)
=====
Dest Prefix[Flags]                               Type  Proto  Age      Pref
  Next Hop[Interface Name]                       Metric
-----
22.22.22.0/29                                     Local  Local  00h19m11s  0
  service_customer_abc
33.33.33.0/29                                     Local  Local  00h18m57s  0
  service_customer_bca
192.168.3.0/24                                    Remote Static  00h19m11s  5
  22.22.22.2
192.168.4.0/29                                     Local  Local  00h28m41s  0
  server_abc
192.168.5.0/29                                     Local  Local  00h28m41s  0
  server_bca
192.168.6.0/24                                    Remote Static  00h18m58s  5
  33.33.33.2
-----

A:Router-R1# ping router 32225 192.168.4.3
PING 192.168.4.3 56 data bytes
64 bytes from 192.168.4.3: icmp_seq=1 ttl=128 time=5.58ms.
64 bytes from 192.168.4.3: icmp_seq=2 ttl=128 time=1.68ms.
64 bytes from 192.168.4.3: icmp_seq=3 ttl=128 time=1.89ms.
64 bytes from 192.168.4.3: icmp_seq=4 ttl=128 time=2.73ms.
64 bytes from 192.168.4.3: icmp_seq=5 ttl=128 time=5.93ms.
---- 192.168.4.3 PING Statistics ----
5 packets transmitted, 5 packets received, 0.00% packet loss
round-trip min = 1.68ms, avg = 3.56ms, max = 5.93ms, stddev = 1.83ms
A:Router-R1# ping router 32225 192.168.5.3
PING 192.168.5.3 56 data bytes
64 bytes from 192.168.5.3: icmp_seq=1 ttl=128 time=5.58ms.
64 bytes from 192.168.5.3: icmp_seq=2 ttl=128 time=1.68ms.
64 bytes from 192.168.5.3: icmp_seq=3 ttl=128 time=1.89ms.
64 bytes from 192.168.5.3: icmp_seq=4 ttl=128 time=2.73ms.
64 bytes from 192.168.5.3: icmp_seq=5 ttl=128 time=5.93ms.
---- 192.168.5.3 PING Statistics ----
  
```

## 4.2 Pengujian Pembagian Trafik

Pada pengujian berikutnya trafik kembali dikirim sesuai tujuannya. *Service customer* ABC menggunakan SDP dengan metode LDP sedangkan BCA menggunakan SDP dengan metode LSP. Hasil pengujian menunjukan trafik *customer* BCA melewati jalur berbeda dengan *customer* ABC. Jalur *customer* BCA melewati *router* R4, ditunjukkan pada tabel 2.

Tabel 2 Hasil uji Trafik customer ABC & BCA

```
Ai:Router-R1# show router interface
=====
Interface Table (Router: Base)
=====
Interface-Name      Adm      Opr (v4/v6)  Mode      Port/SapId  PfxState
-----
system              Up       Up/--        Network   system      n/a
1.1.1.1/32          Up       Up/--        Network   1/1/1       n/a
to_router_R3        Up       Up/--        Network   1/1/1       n/a
to_router_R4        Up       Up/--        Network   1/1/5       n/a
to_router_R5        Up       Up/--        Network   1/1/4       n/a
to_router_R5        Up       Up/--        Network   1/1/4       n/a
to_router_R5        Up       Up/--        Network   1/1/4       n/a
-----
Interfaces : 4
=====
Ai:Router-R1# monitor port 1/1/1 rate interval 3 repeat 3 | match %
=====
Utilization (% of port capacity) 0,04
Utilization (% of port capacity) 0,04
Utilization (% of port capacity) 0,04
=====
Ai:Router-R1# monitor port 1/1/5 rate interval 3 repeat 3 | match %
=====
Utilization (% of port capacity) ~0,02
Utilization (% of port capacity) ~0,02
Utilization (% of port capacity) ~0,02
=====
```

## 4.3 Pengujian Redundansi

### 4.3.1 Pengujian Redundansi metode LDP

Pada pengujian ini, kedua *customer* memakai LDP sebagai tipe tunelnya. Trafik dari kedua server ditujukan kearah masing-masing *customer*. dari hasil pengecekan terlihat trafik kedua *customer* masih berada dalam satu jalur yang sama. Sesuai dengan metode, LDP mengikuti jalur terbaik sesuai path OSPF yang sudah ditentukan sebelumnya. Pada tabel 3 dapat dilihat jalur terbaik (best path) adalah interface *direct* langsung ke antara kedua *router*.

Tabel 3 OSPF pada router R3

```
Ai:router-R3> config>router>ospf# info
-----
router-id 3.3.3.3
area 0.0.0.0
interface "system"
no shutdown
exit
interface "to_router_R4"
interface-type point-to-point
metric 10000
authentication-type message-digest
message-digest-key 1 md5
"/j1R8sNuqKaQcPxEKz55xW9/PV5bsZbUw.Hk4Dr22qp3VaUMbG3k" hash2
no shutdown
exit
interface "to_router_R5"
interface-type point-to-point
metric 1000
authentication-type message-digest
message-digest-key 1 md5
"/j1R8sNuqKaQcPxEKz55xW9/PV5bsZbUw.Hk4Dr22qp3VaUMbG3k" hash2
no shutdown
exit
interface "to_router_R1"
interface-type point-to-point
authentication-type message-digest
message-digest-key 1 md5
"/j1R8sNuqKaQcPxEKz55xW9/PV5bsZbUw.Hk4Dr22qp3VaUMbG3k" hash2
no shutdown
exit
no shutdown
exit
no shutdown
-----
```

Interface dari *router* R1 akan dishtutdown ke *router* R3. Pilihan jalur terbaik (best path) yang bisa dilalui adalah melewati *router* R5. Hasil pengujian ditunjukkan pada tabel 4, *router* R1 dan *router* R3 mengirim dan menerima trafik dari *router* R5.

Tabel 4 Hasil uji Trafik R1 ke R3 melalui R5

```
Ai:Router-R1# show router interface
=====
Interface Table (Router: Base)
=====
Interface-Name      Adm      Opr (v4/v6)  Mode      Port/SapId  PfxState
-----
system              Up       Up/--        Network   system      n/a
1.1.1.1/32          Up       Up/--        Network   1/1/1       n/a
to_router_R3        Up       Down/--      Network   1/1/1       n/a
to_router_R4        Up       Up/--        Network   1/1/5       n/a
to_router_R5        Up       Up/--        Network   1/1/4       n/a
to_router_R5        Up       Up/--        Network   1/1/4       n/a
-----
Interfaces : 4
=====
Ai:Router-R1# monitor port 1/1/4 rate interval 3 repeat 3 | match %
=====
Utilization (% of port capacity) 0,06
Utilization (% of port capacity) 0,06
Utilization (% of port capacity) 0,06
=====
```

### 4.3.2 Pengujian Redundansi metode LSP

Pengujian redundansi menggunakan LSP, membutuhkan jalur standby untuk redundansi. Pada tabel 5 menunjukkan jalur yang tersedia.

Tabel 5 Jalur LSP router R1 ke R3

```
Ai:Router-R1# show router mpls lsp to-R3 path
=====
HPLS LSP to-R3 Path
=====
LSP Name      : to-R3          To          : 3.3.3.3
Admin State   : Up                Oper State  : Up
Path Name     Next Hop           Type        Out I/F  Adm  Opr
-----
to_R3         10.10.1.2         Standby     1/1/1   Up   Up
to_R3_via_R4 10.10.1.30        Primary     1/1/5   Up   Up
to_R3_via_R5 10.10.1.21        Standby     1/1/4   Up   Up
=====
Ai:Router-R1# show router mpls lsp path to_R3_via_R4
=====
VPLS LSP to_R3_via_R4 Path
=====
No Matching Entries Found
=====
Ai:Router-R1# show router mpls path "to_R3_via_R4"
=====
VPLS Path: to_R3_via_R4
=====
Path Name     Adm  Hop Index  IP Address  Strict/Loose
-----
to_R3_via_R4  Up   1          10.10.1.30  Strict
to_R3_via_R4  Up   2          10.10.1.13  Strict
=====
Total Paths : 1
=====
Ai:Router-R1# show router mpls path "to_R3_via_R5"
=====
HPLS Path: to_R3_via_R5
=====
Path Name     Adm  Hop Index  IP Address  Strict/Loose
-----
to_R3_via_R5  Up   1          10.10.1.21  Strict
to_R3_via_R5  Up   2          10.10.1.26  Strict
=====
Total Paths : 1
=====
```

Hasil pengujian untuk perpindahan jalur ini ditunjukkan pada table 6. Dalam proses pengujian akan dishtutdown port kearah *router* R4. Dari hasil tersebut trafik *router* R1 dan *router* R3 berpindah ke *router* R5.

Tabel 6 Hasil uji Trafik R1 berpindah ke R5.

```
Ai:Router-R1# show router interface
=====
Interface Table (Router: Base)
=====
Interface-Name      Adm      Opr (v4/v6)  Mode      Port/SapId  PfxState
-----
system              Up       Up/--        Network   system      n/a
1.1.1.1/32          Up       Up/--        Network   1/1/1       n/a
to_router_R3        Up       Up/--        Network   1/1/1       n/a
to_router_R4        Up       Down/--      Network   1/1/5       n/a
to_router_R5        Up       Up/--        Network   1/1/4       n/a
to_router_R5        Up       Up/--        Network   1/1/4       n/a
-----
Interfaces : 4
=====
Ai:Router-R1# show router mpls lsp path
=====
HPLS LSP Path
=====
LSP Name      : to-R3          To          : 3.3.3.3
Admin State   : Up                Oper State  : Up
Path Name     Next Hop           Type        Out I/F  Adm  Opr
-----
to_R3         10.10.1.2         Standby     1/1/1   Up   Up
to_R3_via_R4  n/a              Primary     n/a     Up   Dwn
to_R3_via_R5  10.10.1.21        Standby     1/1/4   Up   Up
to_R3_via_R5R2 n/a              Standby     n/a     Up   Dwn
=====
Ai:Router-R1# monitor port 1/1/4 rate interval 3 repeat 3 | match %
=====
Utilization (% of port capacity) ~0,00
Utilization (% of port capacity) ~0,00
Utilization (% of port capacity) ~0,00
=====
```

## 5. SIMPULAN

Berdasarkan hasil pengujian dan pembahasan yang sudah dilakukan, dapat disimpulkan bahwa:

1. Implementasi *Service Distribution Point* pada jalur ruting statik jaringan MPLS dengan metode LDP dan LSP dalam pengujian redundansi dengan kedua metode tersebut dapat berjalan dengan baik. Metode LDP dapat menjalankan sistem redundansi sesuai jalur OSPF. Sementara LSP dapat menjalankan sistem redundansi sesuai prioritas path yang sudah ditentukan.
2. Metode LDP dan LSP dapat berjalan dengan baik dalam membagi trafik dan jalur yang dapat dipakai *customer* dimana trafik *customer* tidak hanya melewati satu jalur saja namun dapat dipisah trafik *customer* lainnya untuk melewati jalur yang lain sehingga tidak menumpuk pada satu jalur saja.

## DAFTAR PUSTAKA

- [1] Yani, Rahmat, Trisnawan, Primantara Hari, Fauzi, Mochammad Ali, 2019, Analisis Perbandingan Kinerja Multiprotocol Label Switching dengan Mekanisme Label Distribution Protocol dan Traffic Engineering, Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer, e-ISSN: 2548-964X, Vol. 3, No. 5, Mei 2019, hlm. 5077-5085, <http://j-ptiik.ub.ac.id>
- [2] Hamdani, Mohammad dan Ocktavianti, Firda, 2019, Pemanfaatan Protokol LDP over RSVP Dengan Metode Routing IS-IS Pada Jaringan MPLS Untuk Mengoptimalkan KQI, Jurnal Sainstech, ISSN: 1410-7104 Vol.29, No.2, Juli 2019, hal 29-36, <https://doi.org/10.37277/stch.v29i2.335>
- [3] Gesang Purwoko, Irmayani, 2020, Implementasi Secure Socket Layer Pada Virtual Private Network untuk Pengamanan Komunikasi Video Conference, Jurnal Sinusoida Vol.22 No.2, April 2020, hal 45-57, DOI: <https://doi.org/10.37277/s.v22i2.698>
- [4] Pardila, Meydita, Alyaidrus, Mudrik, 2015, Studi Analisa Transfer Rate Multiprotocol Label Switching (MPLS) Pada Media Akses Wireless dan Wireline di PT. BANK COMMONWEALTH (PTBC), Jurnal Teknologi Elektro, Vol.6 No.2 Mei 2015, Jakarta: ISSN: 2086-9479.
- [5] Xu, Zhuo., 2013, Designing and Implementing IP/MPLS-Based Ethernet Layer 2 VPRN Services: An Advanced Guided for VPLS and VLL, Alcatel Lucent: California.
- [6] Warnock, G., Nathoo, A., 2011, Alcatel-Lucent Multiprotocol Label Switching (MPLS), Alcatel Lucent: California.
- [7] Warnock, G., Nathoo, A., 2011, Alcatel-Lucent Service Architecture, Alcatel Lucent: California.
- [8] Bhandure, Madhulika, 2013, Comparative Analysis of MPLS and Non MPLS Network. IJERA: Mumbai
- [9] Garg, S., Chaudhary, A., 2017, A Study of Performance Analysis of Signaling Protocols in MPLS. IEEE-CICT 2017.
- [10] Warnock, G., Nathoo, A., 2011, *Alcatel-Lucent Network Routing Specialist II (NRS II)*, Alcatel Lucent: California.
- [11] Hundley, Kent., 2011, *Alcatel-Lucent Scalable IP Network Self-Study*, Alcatel Lucent: California.