ANALISIS PERBANDINGAN LABEL DISTRIBUTION PROTOCOL (LDP) DAN TRAFFIC ENGINEERING (TE) PADA JARINGAN BACKBONE MPLS DI PT IFORTE SOLUSI INFOTEK

Dody Frianto, Desi Ramayanti
Teknik Informatika, Universitas Dian Nusantara
Jl. Tj. Duren Barat. 2 No.1, RT.1/RW.5, Tj. Duren Utara,
Kec. Grogol petamburan, Kota Jakarta Barat, Daerah Khusus Ibukota Jakarta 11470
411201034@mahasiswa.undira.ac.id

ABSTRAK

Multi-Protocol Label Switching (MPLS) adalah teknologi untuk jaringan *backbone* yang memadukan kecepatan *switching layer* 2 dengan kemampuan *routing layer* 3. Penelitian ini mengevaluasi MPLS LDP dan MPLS TE yang digunakan oleh iForte untuk meningkatkan efisiensi pengalihan lalu lintas, pengendalian *bandwidth*, dan prioritas layanan. MPLS LDP menggunakan oleh *Routing Information Base* (RIB) untuk distribusi *label* berdasarkan *cost* terendah antar *node*, sementara MPLS TE mengelola dengan LSP berdasarkan kriteria khusus seperti performansi, efisiensi *bandwidth*, dan *Quality of Service* (QoS). Hasil pengujian menunjukkan MPLS TE lebih unggul dalam *round trip, failover*, dan *packet loss rate*, menunjukkan respons jaringan yang lebih responsif. MPLS TE juga potensial meningkatkan efisiensi *bandwidth* melalui LSP yang lebih efektif, meskipun kompleksitas implementasi dan manajemen perlu dipertimbangkan. Secara skalabilitas, MPLS TE mendukung pertumbuhan jaringan tanpa mengorbankan kualitas layanan. Pemilihan antara MPLS LDP dan MPLS TE harus disesuaikan dengan kebutuhan jaringan dan tujuan bisnis, dengan fokus pada peningkatan QoS dan efisiensi operasional. Rekomendasi untuk penelitian ini mencakup eksplorasi lebih lanjut terhadap faktor-faktor yang mempengaruhi kinerja kedua protokol dalam skenario jaringan yang kompleks dan bervariasi, untuk memberikan wawasan mendalam tentang penerapan MPLS dalam teknik *traffic engineering* dan dampak positifnya terhadap peningkatan kinerja jaringan secara keseluruhan.

Kata kunci : *MPLS, LDP, traffic engineering, round trip, failover time, packet loss rate*

1. PENDAHULUAN

PT iForte Solusi Infotek adalah salah satu perusahaan telekomunikasi di Indonesia yang sudah memiliki jaringan tetap tertutup dan lisensi sebagai *Internet Service Provider* (ISP) dengan berbagai layanan, yang salah satunya adalah layanan MPLS VPN (*Multiprotocol Label Switching Virtual Private Network*) [1]. iForte telah mencapai efisiensi tinggi dalam pengalihan lalu lintas serta kontrol yang lebih baik terhadap arah dan kapasitas *bandwidth*. Layanan MPLS VPN yang disediakan memungkinkan penyebaran jaringan *virtual* pada *layer* 2 (L2VPN) dan *layer* 3 (L3VPN), yang secara signifikan meningkatkan fleksibilitas, efisiensi dan skalabilitas jaringan untuk memenuhi kebutuhan pelanggan yang beragam [2].

Dengan demikian, MPLS menjadi alternatif menarik bagi pelanggan dengan harga layanan yang semakin terjangkau. Selain itu, layanan MPLS juga memungkinkan pemberian prioritas layanan yang berbeda sesuai dengan kebutuhan, menjadikannya solusi yang komprehensif dan efektif dalam dunia telekomunikasi. Dalam MPLS, mekanisme *routing* protokol untuk distribusi *label* terbagi menjadi dua jenis utama, yaitu *Label Distribution Protocol* (LDP) dan *Traffic Engineering* (TE). LDP adalah protokol *routing* utama yang digunakan untuk menginformasikan ikatan *label* yang telah dibuat dari satu *node* ke *node* lain dalam jaringan MPLS. Dalam arsitektur jaringan MPLS, LDP digunakan untuk mendistribusikan ikatan *label* dari satu *Label Switching Router* (LSR) ke LSR lainnya [3]. Proses ini dilakukan dengan cara LSR tujuan atau *hop* berikutnya mengirimkan informasi ikatan *label* ke LSR sebelumnya, yang kemudian akan mengikat *label* untuk rute paketnya. LDP membuat *label* dan mentransmisikannya berdasarkan biaya (*cost*) terendah yang ditentukan oleh *Routing Information Base* (RIB) [4].

Sementara itu, MPLS *Traffic Engineering* (TE) memiliki kemampuan lebih dalam mengatur arah lalu lintas jaringan, mengatur kapasitas *bandwidth*, memberikan prioritas yang berbeda untuk setiap layanan, salah satunya mencegah *congestion traffic* pada jalur LDP. MPLS TE menetapkan jalur pengalihan *label* rute *(Label Switched Path* atau LSP) berbasis batasan dan mentransmisikan lalu lintas secara transparan melaluinya. Jalur LSP dapat dikontrol berdasarkan batasan tertentu, dan hubungan di sepanjang jalur tersebut menyediakan *bandwidth* yang cukup untuk lalu lintas layanan. LSP dengan prioritas lebih tinggi dapat mengakses *bandwidth* jika sumber daya mencukupi, sedangkan LSP dengan prioritas lebih rendah akan memenuhi kebutuhan layanan dengan prioritas lebih rendah. Selain itu, MPLS TE memungkinkan administrator jaringan untuk menyebarkan LSP, yang memungkinkan mereka untuk mengalokasikan sumber daya jaringan

dengan tepat dan meminimalkan tekanan pada jaringan [5]. Dengan menggunakan *Fast Reroute* (FRR) dan jalur cadangan, MPLS TE dapat memberikan perlindungan yang lebih baik saat LSP gagal atau *node* jaringan mengalami kemacetan [6].

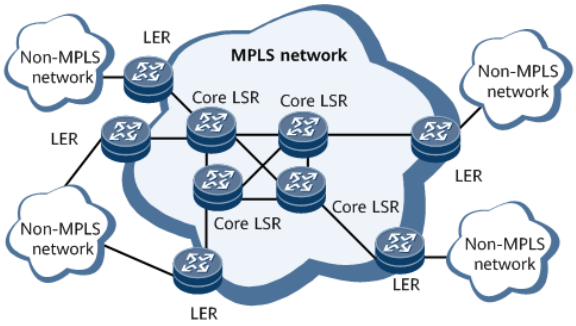
Dalam jaringan *backbone MPLS*, terutama yang menggunakan kabel serat optik, menjaga kualitas layanan menjadi sangat penting untuk memastikan *Service Level Agreement* (SLA) tetap optimal, terutama saat menghadapi masalah seperti *fiber cut*, *degraded*. atau *asymmetric traffic*. Dalam prosesnya, MPLS LDP akan terus melakukan distribusi *label* dengan memanfaatkan informasi yang dikumpulkan oleh *routing protocol* untuk menentukan jalur yang tepat untuk setiap *label* MPLS melalui (*best path*) berdasarkan perhitungan *cost* terendah yang diperoleh dari RIB (*Routing Information Base*) [4]. Bahkan jika *segment* yang dilaluinya mengalami penurunan kualitas atau *asymmetric traffic* yang pastinya akan mengakibatkan layanan menjadi *intermittent*, *high latency* atau *low speed access*. Sementara itu, MPLS TE, dengan kemampuannya dalam melakukan rekayasa lalu lintas, memungkinkan pengalihan *traffic* ke jalur yang *available* atau telah ditentukan sebelumnya. Hal ini membantu meningkatkan kualitas layanan dengan menghindari *segment* yang mengalami masalah atau mengalihkan *traffic* jika diperlukan.

Dengan membandingkan MPLS LDP dan MPLS TE, penelitian ini memberikan justifikasi penting bagi perusahaan untuk memilih protokol yang tepat berdasarkan kebutuhan spesifik mereka dalam hal *Quality of Service (QoS)*, efisiensi penggunaan *bandwidth*, skalabilitas, kompleksitas implementasi dan manajemen. Dengan memahami perbedaan antara MPLS LDP dan MPLS TE, perusahaan dapat membuat keputusan yang lebih tepat dalam merancang dan mengelola jaringan MPLS mereka, meningkatkan kualitas layanan bagi pelanggan, dan mengoptimalkan penggunaan sumber daya jaringan untuk meningkatkan efisiensi operasional.

2. TINJAUAN PUSTAKA

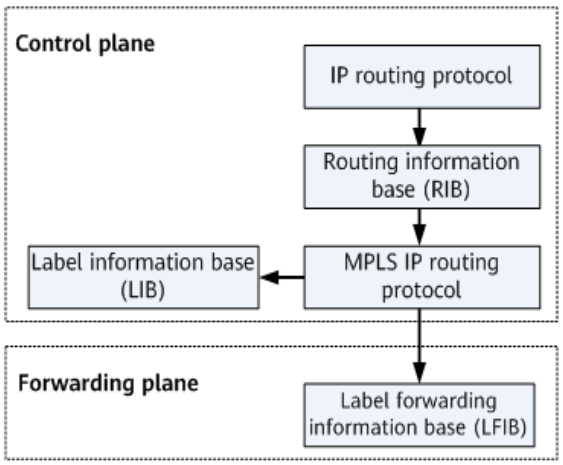
2.1. MPLS

Multi-Protocol Label Switching (MPLS) adalah teknologi pengiriman paket jaringan *backbone* berkecepatan tinggi yang menggabungkan kecepatan *switching* pada *layer* 2 dengan kemampuan *routing* pada *layer* 3 [4]. Sederhananya cara kerja MPLS adalah dengan menyisipkan *label* di antara *header layer* 2 dan 3 pada paket yang diteruskan. *Label-label* ini melekat pada paket-paket, memungkinkan *router* untuk membuat keputusan pengalihan berdasarkan *label-label* tersebut daripada *header* IP [7]. Paket-paket pada MPLS diteruskan dengan protokol *routing* seperti OSPF, IS-IS, BGP atau EGP. Protokol *routing* berada pada *layer* 3 (*network*), sedangkan MPLS berada di *layer* 2-3 [8]. Ketika paket-paket IP memasuki jaringan MPLS, LER masuk menganalisis paket-paket tersebut dan menambahkan *label-label* yang sesuai. Semua LSR di jaringan MPLS meneruskan paket-paket berdasarkan *label-label* tersebut. Saat paket-paket IP meninggalkan jaringan MPLS, LER keluar menghapus *label-label* tersebut. Sebuah jalur di mana paket-paket IP dikirimkan melalui jaringan MPLS disebut sebagai *Label Switched Path* (LSP).



Gambar 1. Struktur jaringan MPLS

LSP adalah jalur unidireksional yang diikuti oleh paket-paket data. *Node* di awal LSP adalah *ingress*, dan node di ujung LSP adalah *egress*. Node di antara *ingress* dan *egress* disebut *transit*. LSP hanya memiliki satu *ingress* dan satu *egress*, namun dapat memiliki nol, satu, atau beberapa *node transit*. Paket-paket MPLS dikirimkan dari *ingress* ke *egress*, dengan *ingress* sebagai sumber untuk *transit*, *transit* sebagai tujuan untuk *ingress* dan sumber untuk *egress*, serta *egress* sebagai tujuan untuk *transit* [4].



Gambar 2. Arsitektur MPLS

Arsitektur MPLS memiliki bagian-bagian sebagai berikut.

a. *Control Plane*, berfungsi menghasilkan dan memelihara informasi *routing* dan *label*, yang terdiri dari :
   - *Routing Information Base* (RIB), dihasilkan oleh protokol *routing* IP dan digunakan untuk memilih rute.
   - *Label Distribution Protocol* (LDP), mengalokasikan *label*, membuat *Label Information Base* (LIB), dan membentuk serta membongkar LSP.

- *Label Information Base* (LIB), dihasilkan oleh LDP dan digunakan untuk mengelola *label* [4].

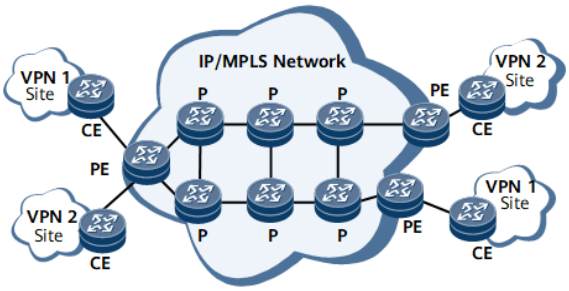
b. *Forwarding plane (Data Plane)*, berfungsi meneruskan paket IP dan paket MPLS yang terdiri dari :
   - *Forwarding Information Base* (FIB), dihasilkan berdasarkan informasi *routing* yang diperoleh dari RIB dan digunakan untuk meneruskan paket IP biasa.
   - *Label Forwarding Information Base* (LFIB), dibuat oleh LDP pada sebuah LSR dan digunakan untuk meneruskan paket MPLS [4].

2.2. RSVP Signaling

Resource Reservation Protocol (RSVP) adalah protokol sinyal yang menangani alokasi *bandwidth* dan teknik lalu lintas sejati di seluruh jaringan MPLS. Seperti LDP, RSVP menggunakan pesan penemuan dan iklan untuk pertukaran informasi jalur LSP antara semua *host*. Namun, RSVP juga mencakup serangkaian fitur yang mengontrol aliran lalu lintas melalui jaringan MPLS. Sedangkan LDP terbatas pada menggunakan jalur terpendek IGP yang dikonfigurasi sebagai jalur transit melalui jaringan, RSVP menggunakan kombinasi algoritma *Constrained Shortest Path First* (CSPF) dan *Explicit Route Objects* (EROs) untuk menentukan bagaimana lalu lintas diarahkan melalui jaringan [9].

Sesi RSVP dasar dibangun dengan cara yang sama dengan pembangunan sesi LDP. Dengan mengkonfigurasi MPLS dan RSVP pada antarmuka transit yang sesuai, Anda memungkinkan pertukaran paket RSVP dan pembangunan LSP. Namun, RSVP juga memungkinkan konfigurasi otentikasi tautan, jalur LSP *explicit*, dan pewarnaan tautan [9].

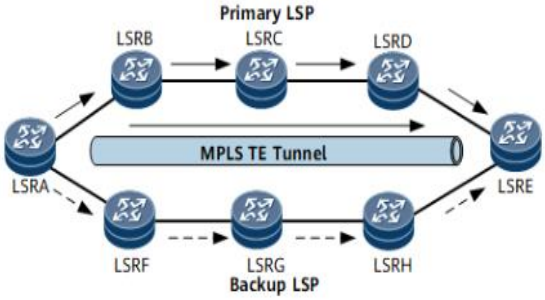
2.3. MPLS LDP



Gambar 3. MPLS LDP

Label Distribution Protocol (LDP) dalam MPLS berfungsi untuk menyebarkan informasi yang terdapat dalam *label* ke setiap *Label Switching Router* (LSR) dalam jaringan MPLS. Selain itu, LDP juga bertanggung jawab untuk menetapkan *label* awal (*initial label*) dan menghapus *label* MPLS dari paket (*popped label*) [10]. LDP mengklasifikasikan *forwarding equivalence classes* (FECs), mendistribusikan *label*, serta mendirikan dan memelihara *label switched paths* (LSPs). LDP mendefinisikan pesan-pesan yang digunakan dalam proses distribusi *label* serta prosedur-prosedur untuk memproses pesan-pesan tersebut [11]. MPLS sangat skalabel karena memungkinkan penggunaan beberapa *label* dalam sebuah paket dan memiliki *plane* penerusan yang berorientasi pada koneksi. Skalabilitas ini memungkinkan jaringan MPLS/IP untuk menyediakan berbagai layanan. *Label Switch Router* (LSRs) pada jaringan MPLS menggunakan LDP untuk memetakan informasi *routing layer* 3 ke jalur *switch layer* 2, dan mendirikan LSPs pada lapisan jaringan. LDP banyak digunakan untuk menyediakan layanan VPN karena penerapannya yang sederhana dan konfigurasinya, kemampuannya untuk mendirikan LSPs secara dinamis berdasarkan informasi *routing*, serta dukungannya terhadap jumlah LSP yang besar [3].

2.4. MPLS TE



Gambar 4. MPLS TE

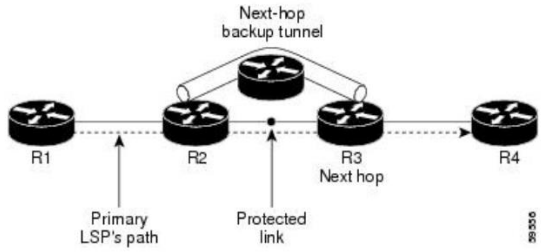
Pada jaringan IP tradisional, *node* memilih jalur terpendek sebagai rute menuju tujuan tanpa memperhatikan faktor-faktor lain seperti *bandwidth* [12]. Mekanisme *routing* ini dapat menyebabkan *congestion traffic* pada *shortest path* (jalur terpendek) dan menyia-nyiakan sumber daya pada jalur lain yang tersedia. MPLS *Traffic Engineering* dapat mencegah *congestion traffic* yang disebabkan oleh alokasi sumber daya yang tidak merata dengan mengalokasikan sebagian *traffic* ke *path* yang tidak digunakan. MPLS dapat membentuk topologi *virtual* di atas topologi fisik dan memetakan lalu lintas ke topologi *virtual* tersebut. MPLS TE sepenuhnya memanfaatkan sumber daya jaringan dan menyediakan jaminan *bandwidth* dan QoS tanpa perlu melakukan *upgrade hardware*. Hal ini secara signifikan mengurangi biaya implementasi jaringan. MPLS TE mudah untuk diterapkan dan dipelihara karena diimplementasikan berdasarkan MPLS. Selain itu, MPLS TE menyediakan berbagai mekanisme keandalan untuk memastikan keandalan jaringan dan perangkat [5].

2.5. Fast Reroute

Fast Reroute (FRR) adalah mekanisme yang melindungi MPLS TE LSP dari kegagalan tautan dan *node* dengan memperbaiki LSP secara lokal di titik kegagalan. Mekanisme ini memungkinkan data tetap mengalir sementara *router* di ujung utama berusaha membangun LSP baru untuk menggantikan yang

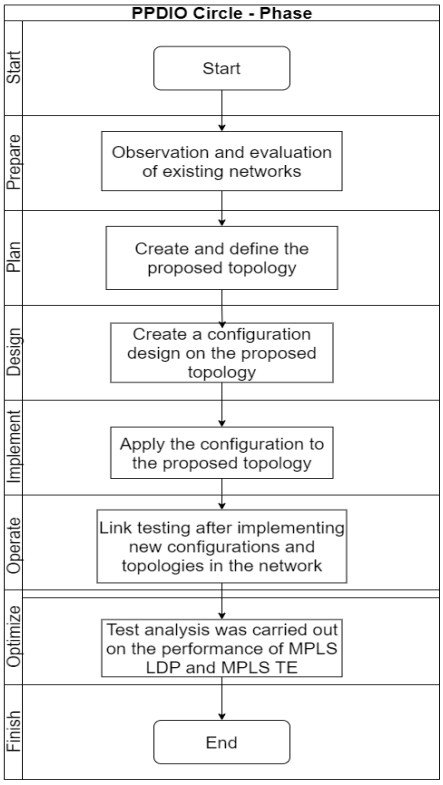
gagal. FRR memperbaiki LSP yang dilindungi dengan mengalihkan jalur melalui terowongan cadangan yang melewati tautan atau *node* yang bermasalah [12].

Fast Reroute (FRR) adalah mekanisme krusial dalam MPLS TE yang secara otomatis mengalihkan lalu lintas ke jalur sekunder jika terjadi kegagalan pada jalur utama (*primary tunnel*). FRR menggunakan dua jalur : *primary tunnel* untuk lalu lintas normal dan *secondary tunnel* sebagai cadangan untuk menghindari kehilangan paket. Tujuannya adalah memulihkan lalu lintas dengan cepat untuk mengurangi dampak kehilangan paket, yang khususnya kritis untuk aplikasi seperti suara dan video yang memerlukan QoS tinggi. Dibandingkan dengan algoritma *routing* tradisional seperti SPF yang lambat dalam menghitung ulang jalur setelah kegagalan, FRR menawarkan perlindungan instan terhadap kegagalan link atau *node* dalam jaringan MPLS [13].



Gambar 5. Fast Reroute

3. METODE PENELITIAN



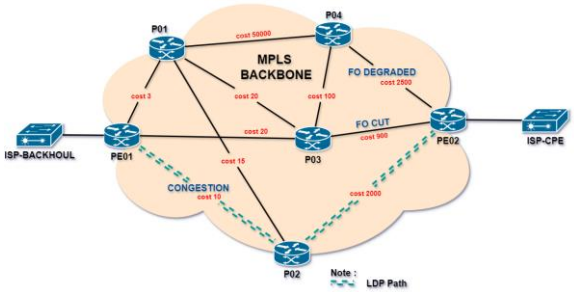
Gambar 6. Metode PPDIOO

Penelitian ini menggunakan metode PPDIOO (*Prepare, Plan, Design, Implement, Operate, Optimize*), yang merupakan pendekatan siklus hidup untuk mengelola dan mengembangkan jaringan [14]. Berikut adalah tahapan PPDIOO seperti yang ditunjukkan pada Gambar 6.

3.1. Prepare

Pada tahap ini, peneliti menentukan parameter yang akan digunakan untuk mengevaluasi kinerja link jaringan yang sudah ada. Ini termasuk parameter *bandwidth*, round *trip (latency)*, dan *route path*.

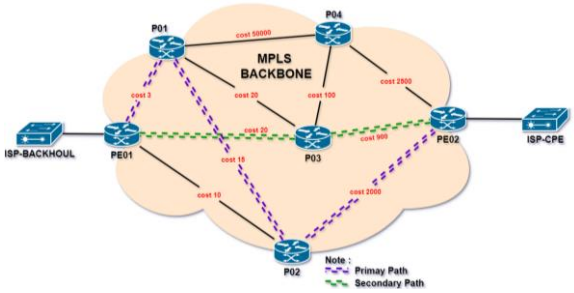
Gambar 7 menunjukkan topologi MPLS eksisting yang digunakan untuk mengirimkan *label* dari PE01 ke PE02 menggunakan metode MPLS LDP. Jalur yang digunakan ditentukan berdasarkan akumulasi nilai *cost* terendah yang dihitung oleh *routing protocol* (IS-IS), yang dianggap sebagai *bestpath*. Jalur ini ditunjukkan dengan garis putus-putus berwarna biru yang saat ini terjadi *congestion traffic* pada segmen PE01 - P02 akibat adanya masalah berupa *fiber optic cut* pada segmen P03 - PE02 dan *fiber optic degraded* pada segmen P04 - PE02 yang menyebabkan service melalui PE01 - P02 mengalami *intermittent* atau *high latency*. Karena hal tersebut, perlu dilakukan upaya preventif untuk mengembalikan layanan ke kondisi normal dengan melakukan *traffic engineering* pada jaringan *backbone* MPLS.



Gambar 7. Topologi MPLS LDP

3.2. Plan

Pada tahap ini, peneliti membuat rancangan topologi untuk menerapkan MPLS TE pada jaringan *backbone*. Rancangan ini mencakup penentuan lokasi *node*, dan jalur yang mana saja yang akan dilakukan *traffic engineering*. Setiap *node* ditentukan berdasarkan kebutuhan jaringan, memastikan bahwa setiap elemen dalam topologi dapat berkomunikasi secara efektif dan efisien.



Gambar 8. Topologi MPLS TE

3.3. Design

Fokus bagian ini adalah menentukan jalur atau *path* mana saja yang akan digunakan saat menerapkan MPLS TE pada jaringan *backbone* dengan membuat *explicit path primary & secondary* yang bertujuan untuk meningkatkan keandalan dan kualitas layanan. *Secondary path* berfungsi sebagai jalur cadangan yang memastikan kontinuitas layanan saat *primary path* gagal, serta mengoptimalkan kinerja dan manajemen bandwidth untuk menghindari kemacetan jaringan Berikut adalah rancangan IP *address* untuk explicith path yang akan digunakan sebagai *primary path* dan jalur *secondary path*.

Tabel 1. Explicit Path (Primary Path)

PE01 - Explicit Path	PE02 - Explicit Path
[P01] - 10.172.151.102	[P02] - 10.172.150.57
[P02] - 10.172.232.18	[P01] - 10.172.232.17
[PE02] - 10.172.150.58	[PE01] - 10.172.151.101

Tabel 1 menunjukkan jalur utama (*primary path*) atau *hop* yang akan digunakan dalam proses transmisi dari PE01 ke PE02 dan sebaliknya.

Tabel 2. Explicit Path (Secondary Path)

PE01 - Explicit Path	PE02 - Explicit Path
[P03] -10.172.150.242	[P03] - 10.172.150.246
[PE02] - 10.172.150.245	[PE01] - 10.172.150.241

Tabel 2 menunjukkan jalur cadangan (*secondary path*) atau *hop* yang akan digunakan dalam proses transmisi dari PE01 ke PE02 dan sebaliknya.

3.4. Implement

Pada bagian ini, peneliti menerapkan konfigurasi pada perangkat MPLS sesuai dengan topologi jaringan yang telah ditetapkan sebelumnya.

3.5. Konfigurasi *Explicit Path*

Explicit path merupakan sebuah mekanisme dalam jaringan MPLS yang memungkinkan pengguna untuk menentukan jalur tertentu yang harus dilewati oleh paket-paket dalam jaringan. Dengan menggunakan jalur *explicit*, konfigurasi harus dilakukan pada kedua ujung jalur, yaitu pada *router* pengirim *(ingress)* dan *router* penerima *(egress)*, sehingga memastikan paket-paket data diarahkan sesuai dengan rute yang telah ditentukan secara statis. Mekanisme ini memberikan kontrol lebih besar terhadap pengelolaan lalu lintas jaringan, memungkinkan optimasi jalur untuk menghindari kemacetan dan meningkatkan efisiensi jaringan.

```
<PE01-                >display explicit-path EP-IDC3DC-KLDRDC-VIA-TBET
Path Name :     EP-IDC3DC-KLDRDC-VIA-TBET     Path Status :  Enabled
 1          10.172.151.102     Strict     Include
 2          10.172.232.18      Strict     Include
 3          10.172.150.58      Strict     Include
<PE01-                >display explicit-path EP-IDC3DC-KLDRDC-VIA-DPLU
Path Name :     EP-IDC3DC-KLDRDC-VIA-DPLU     Path Status :  Enabled
 1          10.172.150.242     Strict     Include
 2          10.172.150.245     Strict     Include
<PE02-                >display explicit-path EP-IDC3DC-KLDRDC-VIA-TBET
Path Name :     EP-IDC3DC-KLDRDC-VIA-TBET     Path Status :  Enabled
 1          10.172.150.57      Strict     Include
 2          10.172.232.17      Strict     Include
 3          10.172.151.101     Strict     Include
<PE02-                >display explicit-path EP-IDC3DC-KLDRDC-VIA-DPLU
Path Name :     EP-IDC3DC-KLDRDC-VIA-DPLU     Path Status :  Enabled
 1          10.172.150.246     Strict     Include
 2          10.172.150.241     Strict     Include
```

Gambar 9. Konfigurasi explicit path

3.6. Konfigurasi *Tunneling*

Interface tunnel memungkinkan untuk menentukan *explicit path* yang akan digunakan untuk mengarahkan trafik serta memungkinkan pengalihan trafik secara cepat ke jalur alternatif jika terjadi kegagalan pada jalur utama (*Fast Reroute*).

```
<PE01-                >dis curr int tun 328
#
interface Tunnel328
 description EP-KLDR-IDC3D-VIA-TBET-DPLU
 ip address unnumbered interface LoopBack0
 tunnel-protocol mpls te
 destination 10.131.223.23
 mpls te record-route label
 mpls te priority 1
 mpls te backup ordinary best-effort
 mpls te backup hot-standby
 mpls te reoptimization
 mpls te reserved-for-binding
 statistic enable
 mpls te tunnel-id 328
 mpls te path explicit-path IDC3DC-KLDRDC-VIA-TBET
 mpls te path explicit-path IDC3DC-KLDRDC-VIA-DPLU secondary
#
return
<PE02-                >dis curr int tun328
#
interface Tunnel328
 description EP-KLDR-IDC3D-VIA-TBET-DPLU
 ip address unnumbered interface LoopBack0
 tunnel-protocol mpls te
 destination 10.131.200.27
 mpls te record-route label
 mpls te priority 1
 mpls te backup ordinary best-effort
 mpls te backup hot-standby
 mpls te reoptimization
 mpls te reserved-for-binding
 statistic enable
 mpls te tunnel-id 328
 mpls te path explicit-path IDC3DC-KLDRDC-VIA-TBET
 mpls te path explicit-path IDC3DC-KLDRDC-VIA-DPLU secondary
#
return
```

Gambar 10. Konfigurasi interface tunnel

3.7. Konfigurasi *Tunnel Policy*

Tunnel-policy ini berfungsi untuk menetapkan cara arus lalu lintas menuju tujuan tertentu melalui *interface tunnel* yang telah ditetapkan sebelumnya. Ini memungkinkan kontrol yang lebih tepat dalam mengatur rute data untuk memaksimalkan efisiensi dan keandalan jaringan, terutama dalam menghadapi kebutuhan pengalihan trafik dalam kondisi darurat atau optimalisasi jalur untuk memenuhi persyaratan khusus jaringan.

```
<PE01-                >dis curr | b tunnel-policy
Info: It will take a long time if the content you search is too much or
long, you can press CTRL_C to break.
tunnel-policy TP-KLDR-IDC3D-VIA-TBET-DPLU
 tunnel binding destination 10.131.223.23 te Tunnel328 down-switch
#
<PE02-                >dis curr | b tunnel-policy
Info: It will take a long time if the content you search is too much or
long, you can press CTRL_C to break.
tunnel-policy TP-KLDR-IDC3D-VIA-TBET-DPLU
 tunnel binding destination 10.131.200.27 te Tunnel328 down-switch
#
```

Gambar 11. Konfigurasi tunnel-policy

3.8. Konfigurasi VSI (*Virtual Switch Instance*)

```
<PE01-                >dis c c vsi VPLS-VIA-MPLS-TE
#
vsi VPLS-VIA-MPLS-TE
 pwsignal ldp
  vsi-id 9
  peer 10.131.223.23 tnl-policy TP-KLDR-IDC3D-VIA-TBET-DPLU
#
return
<PE02-                >dis c c vsi VPLS-VIA-MPLS-TE
#
vsi VPLS-VIA-MPLS-TE
 pwsignal ldp
  vsi-id 9
  peer 10.131.200.27 tnl-policy TP-KLDR-IDC3D-VIA-TBET-DPLU
#
return
```

Gambar 12. Konfigurasi VSI

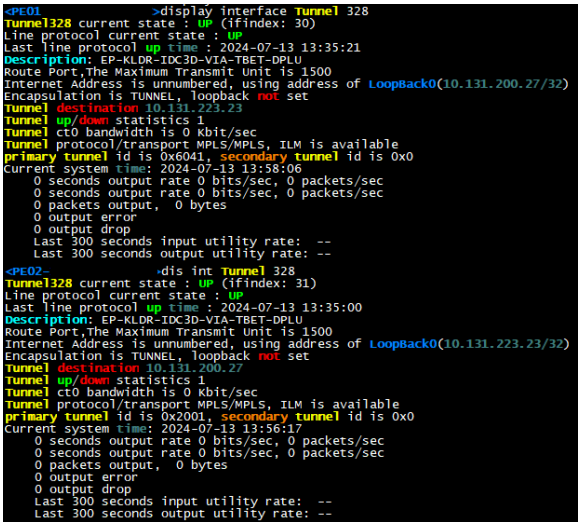
VSI merupakan entitas di jaringan MPLS yang memungkinkan berbagai layanan dan aliran lalu lintas dikategorikan dan diatur secara terpisah. Dalam tahap

ini akan dilakukan modifikasi peering supaya VSI yang akan dilakukan MPLS TE bisa melalui *path* yang telah ditentukan pada *tunnel-policy* sebelumnya.

3.9. Operate

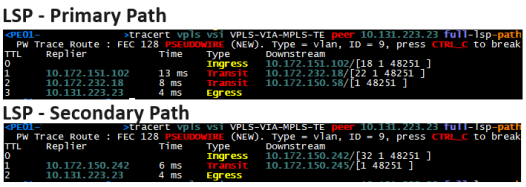
Sebelum melanjutkan dengan uji coba lebih lanjut, penting untuk memastikan bahwa konfigurasi MPLS TE telah berjalan dengan baik melalui beberapa langkah verifikasi berikut :

a. Status *interface tunnel* UP, menunjukkan bahwa *interface port* pada perangkat jaringan aktif dan siap untuk mengirim dan menerima data, menunjukkan tidak ada masalah pada tingkat fisik atau koneksi.



Gambar 13. Status interface tunnel

b. Jalur LSP *(Label Switched Path) primary* dan *secondary path* telah sesuai dengan *path explicit* yang telah ditentukan. Jalur LSP ini mengarahkan lalu lintas jaringan sesuai dengan kebijakan tertentu untuk meningkatkan efisiensi rute atau kualitas layanan.



Gambar 14. LSP path MPLS TE

Untuk mengevaluasi kinerja jaringan, pengujian dilakukan dengan skenario pengujian mencakup :

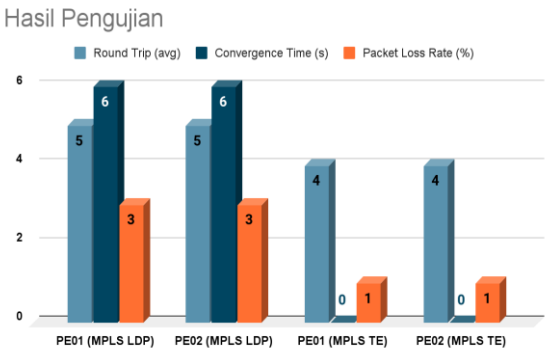
a. *Round trip*, melakukan ICMP *ping* dari PE01 ke PE02 sebanyak 100 kali dalam keadaan normal menggunakan MPLS LDP dan MPLS TE untuk mengukur waktu perjalanan bolak-balik.
b. *Failover time*, melakukan *shutdown* pada salah satu port segmen MPLS *backbone* untuk mengukur waktu yang diperlukan saat terjadi perubahan topologi.
c. *Packet loss rate*, melakukan ICMP *ping* dari PE01 ke PE02 sebanyak 100 kali dilakukan secara bersamaan dengan terputusnya salah satu segmen pada MPLS *backbone* untuk mengukur tingkat kehilangan paket selama proses transmisi

3.10. Optimize

Melakukan analisis perbandingan kinerja LDP dan MPLS TE pada jaringan *backbone* adalah langkah terakhir dalam penelitian ini. Peneliti akan menganalisis data yang dikumpulkan selama pengujian, yang meliputi berbagai metrik kinerja seperti *round trip*, *failover time* dan *packet loss rate*. Hasil analisis ini bukan hanya untuk membandingkan performa kedua teknologi tersebut, tetapi juga untuk memberikan rekomendasi yang dapat meningkatkan efektivitas dan efisiensi operasional jaringan, sesuai dengan kebutuhan spesifik perusahaan atau penyedia layanan jaringan.

4. HASIL DAN PEMBAHASAN

Dalam pengujian ini, penulis tidak melakukan shutdown port pada jaringan nyata untuk menghindari *impact service* terhadap layanan yang sedang berjalan. Sebagai gantinya, penulis melakukan simulasi dengan mengikuti kondisi sebenarnya untuk mengevaluasi operasional saat menggunakan MPLS LDP dan MPLS TE. Data yang dikumpulkan dari serangkaian pengujian mengungkapkan perbedaan signifikan dalam respons dan stabilitas antara dua mekanisme MPLS, yaitu MPLS LDP dan MPLS TE.



Gambar 15. Hasil pengujian

Tabel 3. Hasil pengujian link

Keterangan		Round Trip	Failover Time	Packet Loss Rate
MPLS LDP	PE01	round-trip min/avg/max = 3/5/12 ms	6s	3.00% packet loss
	PE02	round-trip min/avg/max = 3/5/16 ms	6s	3.00% packet loss
MPLS TE	PE01	round-trip min/avg/max = 2/4/9 ms	0s	1.00% packet loss
	PE02	round-trip min/avg/max = 2/4/13 ms	0s	1.00% packet loss

Hasil dari skenario pengujian di atas dapat diuraikan sebagai berikut :

a. *Round Trip Time*
   - MPLS LDP menunjukkan rata-rata waktu *round trip* sebesar 5 ms untuk pengujian dari PE01 ke PE02 dan sebaliknya.
   - MPLS TE menunjukkan rata-rata waktu *round trip* sebesar 4 ms untuk pengujian yang sama, menunjukkan *latency* yang lebih rendah dibandingkan MPLS LDP.
   - *Ini* menunjukkan bahwa MPLS TE mampu memberikan *latency* yang lebih rendah, yang sangat krusial untuk aplikasi yang memerlukan kecepatan tinggi dan respon *real-time*.

b. *Failover Time*
   - *MPLS* LDP memerlukan waktu *failover* selama 6 detik untuk melakukan *switching* dari *primary path* ke *secondary path*, yang dipengaruhi oleh akumulasi *cost* dari *routing protocol* (IS-IS).
   - *MPLS* TE hanya memerlukan waktu *failover* selama 0 detik karena *path* sudah terdefinisi sebelumnya, menunjukkan keunggulan dalam kecepatan *switching*.
   - *Kecepatan switching* yang lebih cepat ini meningkatkan keandalan jaringan, mengurangi *downtime*, dan memastikan kontinuitas layanan.

c. *Packet Loss Rate*
   - *Dengan* MPLS LDP, terjadi kehilangan paket sebesar 3% (3 paket dari 100 paket) selama proses *switching* path akibat salah satu segmen sedang mengalami *down* atau *failure path*.
   - *MPLS* TE menunjukkan tingkat kehilangan paket sebesar 1% (1 paket dari 100 paket) dalam kondisi yang sama, menunjukkan stabilitas performa yang lebih tinggi.
   - *Penurunan* tingkat kehilangan paket ini mencerminkan kestabilan dan kehandalan yang lebih tinggi dari MPLS TE dalam menghadapi gangguan jaringan.

Di samping hasil uji tersebut, efisiensi penggunaan *bandwidth* dari MPLS TE terbukti lebih efektif dengan menggunakan teknik *traffic engineering* yang adaptif. Ini memungkinkan manajemen sumber daya jaringan yang efisien, mengurangi pemborosan *bandwidth*, dan optimal dalam memanfaatkan kapasitas jaringan sesuai dengan fluktuasi trafik yang terjadi.

Dalam hal skalabilitas, MPLS TE juga unggul dengan kemampuannya untuk mengatur jalur secara fleksibel dan efisien, menanggapi pertumbuhan jaringan yang cepat dan integrasi dengan *node* baru tanpa mengorbankan kualitas layanan atau stabilitas operasional. Namun implementasi dan manajemen MPLS TE membutuhkan tingkat kompleksitas yang lebih tinggi dibandingkan MPLS LDP, karena melibatkan konfigurasi *explicit path* dan pengelolaan *traffic engineering* yang memerlukan pemahaman teknis yang mendalam dan manajemen yang baik.

Secara keseluruhan, hasil pengujian ini menggambarkan bahwa MPLS TE memberikan alternatif yang lebih kuat untuk aplikasi dan infrastruktur jaringan yang memerlukan respons cepat, keandalan tinggi, dan penggunaan sumber daya yang efisien, meskipun dengan tingkat kompleksitas implementasi yang lebih tinggi.

5. KESIMPULAN DAN SARAN

Berdasarkan perbandingan performansi jaringan antara MPLS LDP dan MPLS TE, MPLS TE menunjukkan keunggulan dalam beberapa aspek. MPLS TE menawarkan waktu *round trip* yang lebih singkat (avg 4ms), *failover time* yang lebih cepat (0s), dan *packet loss rate* yang lebih rendah (1 dari 100 paket atau sebesar 1%) dibandingkan MPLS LDP. Hal ini menunjukkan bahwa MPLS TE juga berpotensi meningkatkan efisiensi *bandwidth* melalui pengaturan *path* yang lebih efektif. Namun, kompleksitas implementasi dan manajemen MPLS TE perlu dipertimbangkan. Dalam skalabilitas, MPLS TE mendukung pertumbuhan jaringan tanpa mengorbankan kualitas layanan. Pemilihan antara MPLS LDP dan MPLS TE harus sesuai dengan kebutuhan jaringan dan tujuan bisnis, fokus pada peningkatan QoS dan efisiensi operasional. Saran untuk penelitian ini adalah untuk melanjutkan eksplorasi dan analisis lebih lanjut terhadap faktor-faktor yang mempengaruhi kinerja MPLS TE dan MPLS LDP dalam skenario jaringan yang lebih kompleks dan beragam. Dengan demikian, penelitian ini dapat memberikan wawasan yang lebih mendalam tentang penerapan MPLS dalam konteks *traffic engineering* dan kontribusi potensialnya terhadap peningkatan kinerja jaringan secara keseluruhan.

DAFTAR PUSTAKA

[1] About Us," *PT iForte Solusi Infotek*. https://www.iforte.id/company/about-us (accessed May 21, 2024).

[2] I. Rozali, "Studi Empiris Perbaikan Quality Of Service dengan DiffServ dan MPLS pada Jaringan IP," *Seminar Nasional Aplikasi Teknologi Informasi (SNATI)*, p., Jan. 2005.

[3] https://support.huawei.com/enterprise/en/doc/EDOC1100138150/bcd405be/overview-of-mpls-ldp (accessed May 21, 2024).

[4] https://support.huawei.com/enterprise/en/doc/EDOC1100138150/7c5ca4fb/basic-mpls-architecture (accessed May 21, 2024).

[5] https://support.huawei.com/enterprise/en/doc/EDOC1100270080/1c528a01/overview-of-mpls-te (accessed May 21, 2024).

[6] "MPLS Traffic Engineering (TE) - Fast Reroute (FRR) Link and Node Protection [Support]," *Cisco*. https://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_te_frr_node_prot_external_

docbase_0900e4b1805dfeff_4container_external_docbase_0900e4b1814cdd7b.html (accessed May 21, 2024).

[7] I. Nurhaida, D. Ramayanti, and I. Nur, "Performance Comparison based on Open Shortest Path First (OSPF) Routing Algorithm for IP Internet Networks," *Communications on Applied Electronics*, vol. 7, no. 31, pp. 12–25, Sep. 2019, doi: 10.5120/cae2019652838.

[8] "Multi-protocol Label Switching (MPLS) untuk jaringan," *BINUS UNIVERSITY*, Dec. 23, 2019. https://binus.ac.id/bandung/2019/12/multi-protocol-label-switching-mpls-untuk-jaringan/ (accessed May 21, 2024).

[9] *Juniper Networks*. https://www.juniper.net/documentation/us/en/software/junos/mpls/topics/topic-map/rsvp-overview.html (accessed May 21, 2024).

[10] B. Euginia and T. Ghozali, "Simulasi Multi Protocol Label Switching Virtual Private Network (MPLS VPN) Dengan Virtual Local Area Network (VLAN) Menggunakan Router MIKROTIK," *TESLA: Jurnal Teknik Elektro*, vol. 20, no. 2, p. 109, Feb. 2019, doi: 10.24912/tesla.v20i2.2987.

[11] R. Y. H. T. A. Fauzi, "Analisis Perbandingan Kinerja Multiprotocol Label Switching dengan Mekanisme Label Distribution Protocol dan Traffic Engineering".

[12] "MPLS Traffic Engineering Fast Reroute -- Link Protection," *Cisco*. http://www.cisco.com/en/US/docs/ios/12_0st/12_0st10/feature/guide/fastrout.html (accessed Jul. 01, 2024).

[13] M. Khan, "MPLS Traffic Engineering in ISP Network," *International Journal of Computer Applications*, vol. 59, no. 4, pp. 23–32, Dec. 2012, doi: 10.5120/9536-3972.

[14] "PPDIOO Lifecycle Approach to Network Design and Implementation > Analyzing the Cisco Enterprise Campus Architecture," *Cisco Press*. https://www.ciscopress.com/articles/article.asp?p=1608131&seqNum=3 (accessed Jul. 01, 2024).