BAB II
TINJAUAN PUSTAKA

2.1 Routing

John Gage, chief researcher dari *Sun Microsystems* (1984:6) mengatakan *routing protocol* menjelaskan bagaimana *router* yang ada saling berkomunikasi satu dengan yang lain dan digunakan untuk memelihara / mengupdate isi dari *routing table*. Macam - macam Routing: (Juni Agustino, 2013)

1. Static Routing

Static routing ini merupakan cara paling simple untuk mengisi *routing table* yang ada di router , tapi dengan menggunakan *static routing* ini biasa nya di gunakan pada jaringan – jaringan yang kecil di mana hanya ada beberapa ip yang harus di masukan ke dalam *routing table.*

2. Dynamic Routing

Dynamic Routing adalah fungsi dari *routing protocol* yang saling berkomunikasi untuk melakukan *update* pada *routing table*, berbeda dengan *static routing* di mana admin harus secara manual memasukan *routing table*, dengan menggunakan *dynamic routing* ini admin tidak perlu untuk mengupdate jika terjadi perubahan dalam *routing table*, karena dalam *dynamic routing* ini dapat melakukan *periodic update*. Oleh sebab itu *dynamic routing* ini biasa di gunakan untuk jaringan yang kompleks.

Yang termasuk Dynamic Routing adalah:

1. RIP (*Routing Information Protocol).*

RIP adalah *routing protocol dynamic* yang menggunakan algoritma *distance vector*, di mana RIP menggunakan protocol UDP untuk mengirimkan informasi routing atas router. Protocol RIP ini menggunakan perhitungan *Hop-Count* sebagai *routing metric*.

2. IGRP (*Interior Gateway Routing Protocol*).

IGRP adalah routing protocol yang diciptakan untuk menutupi kekurangan dari RIP, di mana dalam protocol IGRP ini menggunakan *Autonomous System* (AS) yang dapat menentukan routing berdasarkan system interior atau exterior. *Administrative Distance* untuk IGRP adalah 100.

3. EIGRP (*Enhanced Interior Gateway Routing Protocol*).

EIGRP adalah *routing protocol* yang biasa di sebut sebagai *proprietary protocol*. Dimana EIGRP ini merupakan pengembangan dari protocol IGRP, dan EIGRP menggunakan *Diffusing Update Algorithm* (DUAL) dengan bertukar informasi "*Hello Packet*" untuk memastikan keberadaan router yang ada di sekitar nya.

4. OSPF (*Open Shortest Path First*).

OSPF merupakan *routing protocol* yang hanya dapat bekerja di dalam jaringan internal suatu organisasi atau perusahaan tertentu. Selain itu OSPF merupakan protocol yang dapat di gunakan di perangkat manapun yang compatible dengan protocol ini. OSPF merupakan *routing protocol* yang menggunakan konsep hirarki, yang arti nya OSPF membagi – bagi jaringan menjadi beberapa tingkatan.

5. BGP (*Border Gateway Protocol*)

BGP adalah sebuah *system* antar *Autonomous Routing Protocol*, pada umum nya BGP ini digunakan untuk pertukaran informasi routing untuk internet dan merupakan protocol yang digunakan antar penyedia layanan internet (ISP).

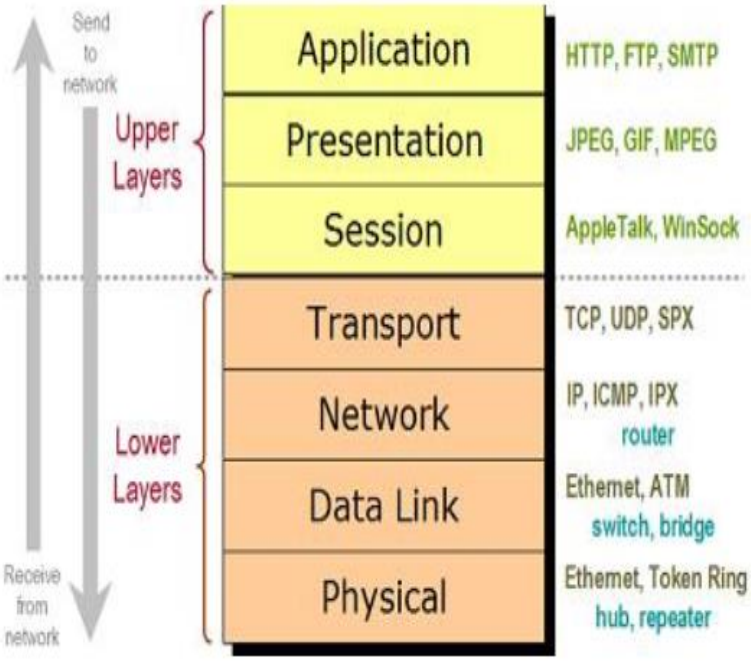
2.2 Jaringan OSI Layer

Model OSI menerapkan konsep yang dikenal dengan enkapsulasi. Enkapsulasi adalah metode membungkus data dari satu lapisan model OSI dalam struktur data baru sehingga setiap lapisan model OSI hanya akan melihat

dan berurusan dengan formasi yang dibutuhkan untuk dengan benar menangani dan memberikan data pada jaringan komputer. (A. Sujana, 2014)

Model Referensi OSI didasarkan pada prinsip - prinsip sebagai berikut:

a. Setiap lapisan memiliki fungsi yang dapat didefinisikan .
b. Batas-batas lapisan telah dirancang untuk mengurangi arus informasi dalam antarmuka.
c. Ketika tingkat tambahan abstraksi diperlukan, maka lapisan selanjutnya akan dibuat dan
d. Setiap lapisan memiliki fungsi protokol standar internasional



Gambar 2.1 Protokol OSI Layer

2.2.1 Application Layer

"*Layer* ke-7 dari model *network* OSI, menyediakan layanan-layanan untuk prosedur-prosedur aplikasi (seperti *electronic mail* atau *transfer file)* yang berada

diluar model OSI. Layer ini memilih dan menentukan ketersediaan dari *partner* komunikasi dan juga sumber daya yang diperlukan untuk membuat koneksi, mengkoordinasi aplikasi-aplikasi yang berpasangan, dan membentuk sebuah kesepakatan terhadap prosedur-prosedur untuk mengendalikan integritas data dan *error recovery*" (Todd Lamle, 2005)

- HTTP (*Hyper Text Transfer Protocol*)

  Protokol yang dipergunakan untuk mentransfer dokumen dan web dalam sebuah *web browser*, melalui www. HTTP juga merupakan protokol yang meminta dan menjawab antar klien dan server.

- FTP (*File Transfer Protokol*)

  Protokol internet yang berjalam dalam *layer* aplikasi yang merupakan standar untuk mentransfer file komputer antar mesin-mesin dalam sebuat jaringan internet.

- NFS (*Network File System*)

  Jaringan protokol yang memungkinkan pengguna di klien komputer untuk menngakses file melalui jaringan dengan cara yang sama dengan bagaiman penyimpanan lokal yang diaksesnya.

- DNS (*Domain Name System*)

  Protokol yang digunakkan untuk memberikan suatu nama *domain* pada sebuah alamat IP agar lebih mudah diingat.

- POP3 (*Post Office Protocol*)

  Protokol yang digunakan untuk mengambil *mail* dari suatu *mail transfer agent* yang akhirnya *mail* tersebut akan di *download* kedalam jaringan local.

- MIME (*Multipurpose Internet Mail Exension*)

  Protokol yang digunakan untuk mengirim *file binary* dalam bentuk teks.

- SMB (*Server Messange Block*)

  Protokol yang digunakan untuk mentransfer server-server file ke DOS dan Windows.

- NNTP (*Network News Transfer Protocol*)

  Protokol yang digunakan untuk menerima dan mengirim newsgroup.

- DHCP (*Dynamic Configuration Protocol*)

  Layanan yang memberikan no IP kepada komputer yang meminta nya secara otomatis.

2.2.2 Presentation Layer

"*Layer* 6 dari model referensi OSI, mendefenisikan bagaimana data di-*format*, dinyatakan, di-*encode*, dan diubah untuk digunakan oleh *software* pada layer aplikasi'.

- TELNET

  Protokol yang digunakan untuk akses remote masuk ke suatu host, data berjalan secara lain teks.

- SMTP (*Simple Mail Transfer Protocol*)

  Salah satu protokol yang biasa digunakan dalam pengiriman *e-mail* di internet atau untuk mengirimkan data dari komputer pengirim *e-mail* ke *server e-mail* penerima.

- SNMP (*Simple Network Management Protocol*)

  Protokol yang digunakan dalam suatu manajemen jaringan.

2.2.3 Session Layer

"*Layer* 5 dari model referensi model OSI, bertanggung jawab untuk membuat, mengelola, dan mengakhiri *session-session* antara aplikasi-aplikasi dan mengawasi pertukaran data antara *entitas-entitas layer presentation*".

- NETBIOS

  Berfungsi sebagai penyiaran pesan maksud nya memungkinkan user mengirim pesan tunggal secara serempak ke komputer lain yang terkoneksi. NETBEUI (NETBIOS *Extended User Interface*) Berfungsi sama dengat NETBIOS hanya sedikit di kembangkan lagi dengan menambahkan fungsi yang memungkinkan bekerja dengan beragam perangkat keras dan perangkat lunak.

- ADSP (*AppleTalk Data Stream Protocol*)

  Protokol ini berfungsi memantau aliran data diantara dua komputer dan untuk memeriksa aliran data tersebut tidak terputus.

- SPDU (*Session Protokol Data Unit*)

  Berfungsi mendukung hubungan antara dua *session service user*.

2.2.4 Transport Layer

"*Layer* 4 dari model referensi OSI, digunakan untuk komunikasi yang dapat diandalkan antara *node-node* akhir melalui network. *Layer transport* menyediakan mekanisme yang digunakan untuk membuat, memelihara, dan mengakhiri rangkaian-rangkaian virtual, mengangkut deteksi kesalahan dan *recovery*, dan mengendalikan aliran informasi".

- TCP (*Transmission Control Protocol*)

  Protokol yang menyediakan layanan penuh lapisan transport untuk aplikasi.

- UDP (*User Datagram Protocol*)

  Protokol *connectionless* dan *proses-to-procces* yang hanya menambahkan alamat port, *cheksum error control* dan panjang informasi data pada layer di atasnya.

2.2.5 Network Layer

”Dalam model referensi OSI, merupakan *layer* ke-3 – *layer* dimana *routing* diimplementasikan, mengaktifkan koneksi-koneksi dan pemilihan jalur antara dua sistem akhir”.

- IP (*Internetworking Protocol)*

  Mekanisme transmisi yang digunakan untuk menstransportasikan data dalam-dalam paket yang disebut datagram.

- ARP (*Address Resulotion Protocol*)

  Protokol yang digunakan untuk mengetahui alamat IP berdasarkan alamat fisik dari sebuah komputer.

- RARP (*Reverse Address Resulotion Protocol*)

  Protokol yang digunakan untuk mengetahui alamat fisik melalui IP komputer.

- ICMP (*Internet Control Message Protocol*)

  Mekanisme yang digunakan oleh sejumlah host untuk mengirim notifikasi datagram yang mengalami masalah pada hostnya.

- IGMP (*Internet Group Message Protocol*)

  Protokol yang digunakan untuk memberi fasilitas message yang simultan kepada group penerima.

2.2.6 Data Link Layer

"*Layer* 2 dari model referensi OSI, ia memastikan transmisi data yang bisa dipercaya melalui sebuah *link* fisikal dan terutama berkaitan dengan pengalamatan fisikal, disiplin *line*, topologi *network*, pemberitahuan *error*, pengiriman *frame* yang berurutan, dan *flow control*. IEEE membagi lebih lanjut layer ini menjadi *sublayer* MAC dan *sublayer* LLC. Juga dikenal sebagai *link layer*".

- PPP (*Point to Point Protocol*)

  Protokol yang digunakan untuk point to point pada suatu jaringan.

- SLIP (*Serial Line Internet Protocol*)

  Protokol yang digunakan untuk menyambung serial.

2.2.7 Physical Layer

"*Layer* terendah – *layer* 1 – dalam model referensi OSI, bertanggung jawab untuk mengubah *frame-frame* data dari *layer Data Link* (layer-2) menjadi sinyal-sinyal listrik. Protokol-protokol dan standar-standar *layer Physical* mendefenisikan, sebagai contoh, jenis kabel dan konektor yang digunakan, termasuk pemilihan *pin* dan skema *encoding* untuk pensinyalan nilai 0 dan 1".

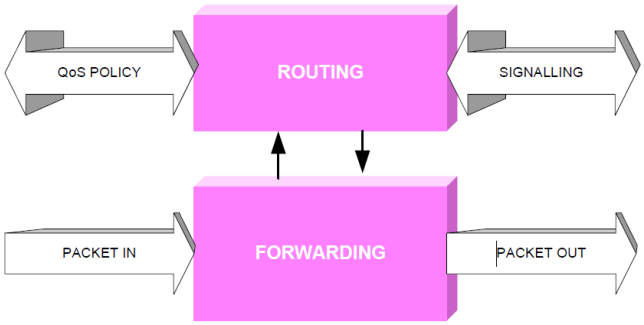
2.3 *Multi Protocol Label Switching* (MPLS)

"MPLS, *multi-protocol label switching*, adalah arsitektur *network* yang didefinisikan oleh IETF untuk memadukan mekanisme label *swapping* di layer 2 dengan *routing* di layer 3 untuk mempercepat pengiriman paket. Arsitektur MPLS dipaparkan dalam RFC-3031", (Rosen, 2001).

MPLS merupakan mekanisme *forwarding* dimana paket di-*forward*-kan berdasarkan label. Label dapat direlasikan dengan alamat tujuan IP (seperti *traditional IP forwarding*) atau direlasikan dengan parameter lain seperti QoS atau alamat pengirim IP. MPLS juga didesain untuk mendukung mekanisme *forwarding* protokol-protokol lain. (Hadi Kristianta, 2013)

2.3.1 Arsitektur MPLS

MPLS, *multi-protocol label switching*, adalah arsitektur *network* yang didefinisikan oleh IETF untuk memadukan mekanisme label *swapping* di layer 2 dengan *routing* di *layer* 3 untuk mempercepat pengiriman paket.



Gambar 2.2 Arsitektur MPLS

Arsitektur MPLS terdiri dari dua bagian utama, yaitu *control plane* dan *data plane*.

1. *Control plane* adalah tempat informasi *routing* dan informasi kontrol lainnya, seperti *label binding*, dipertukarkan antara *label switch router* (LSR). MPLS adalah sebuah protokol dimana pertukaran informasi kontrol

terjadi sebelum paket data pertama bisa diteruskan. Pengelompokan paket IP yang diberi perlakuan sama disebut sebagai *Forwarding Equivalence Class* (FEC). Biasanya FEC dikelompokan berdasarkan alamat *network layer* tujuan. Selain itu juga bisa berdasarkan IP ToSbits, IP protokol ID, *port number* dan lainnya. Proses klasifikasi ini hanya dilakukan pada *ingress*.

2. *Data Plane*, adalah tempat dimana terjadinya penerusan paket data. Pada MPLS-*based forwarding*, ada tiga proses utama dalam meneruskan paket yaitu, *label pushing*, *label swapping* dan *label popping*.
   a. *Label Pushing* : adalah proses menambahkan label pada data paket sesuai FEC-nya.
   b. *Label Swapping* : adalah proses mengganti label paket data yang masuk dan menggantinya dengan label paket keluar untuk diteruskan ke *interface* yang sesuai.
   c. *Label Popping* : adalah proses pelucutan label pada paket ketika paket sampai pada akhir dari jaringan MPLS.

Network MPLS terdiri atas sirkit yang disebut *label-switched path* (LSP), yang menghubungkan titik-titik yang disebut *label-switched router* (LSR). LSR pertama dan terakhir disebut *ingress* dan *egress*. Setiap LSP dikaitkan dengan sebuah *forwarding equivalence class* (FEC), yang merupakan kumpulan paket yang menerima perlakukan *forwarding* yang sama di sebuah LSR. FEC diidentifikasikan dengan pemasangan label.

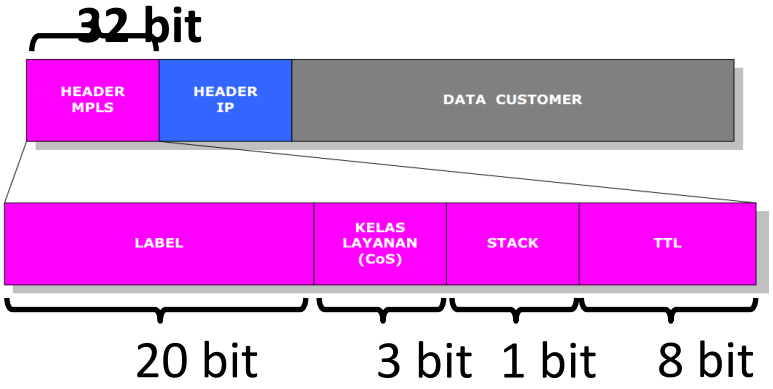
Untuk membentuk LSP, diperlukan suatu protokol persinyalan. Protokol ini menentukan *forwarding* berdasarkan *label* pada paket. Label yang pendek dan berukuran tetap mempercepat proses *forwarding* dan mempertinggi fleksibilitas pemilihan *path*. Hasilnya adalah network *datagram* yang bersifat lebih *connection-oriented*.

Komponen MPLS :

a. *Label Switched Path* (LSP): Merupakan jalur yang melalui satu atau serangkaian LSR dimana paket diteruskan oleh *label swapping* dari satu MPLS *node* ke MPLS *node* yang lain.
b. *Label Switching Router*: MPLS node yang mampu meneruskan paket-paket layer-3.
c. MPLS *Edge Node* atau *Label Edge Router* (LER): MPLS *node* yang menghubungkan sebuah MPLS *domain* dengan *node* yang berada diluar MPLS *domain.*
d. MPLS *Egress Node*: MPLS *node* yang mengatur trafik saat meninggalkan MPLS *domain*
e. MPLS *ingress Node*: MPLS *node* yang mengatur trafik saat akan memasuki MPLS *domain.*
f. MPLS *label*: merupakan label yang ditempatkan sebagai MPLS *header*.
g. MPLS *node*: *node* yang menjalankan MPLS. MPLS *node* ini sebagai *control* protokol yang akan meneruskan paket berdasarkan label.

2.3.2 Enkapsulasi Paket

MPLS melakukan enkapsulasi paket IP dengan memasang header MPLS sebesar 32 bit, seperti pada gambar.



Gambar 2.3 Header MPLS

MPLS *header* meliputi:

a). 20 *bit label value*

Suatu bidang label yang berisi nilai yang nyata dari MPLS label (label dari paket)

b). 3 *bit field* CoS

Class of Service, suatu bidang yang digunakan untuk mempengaruhi antrian paket data dan algoritma paket data yang tidak diperlukan.

c). 1 *bit bottom of stack flag*

Suatu bidang yang mendukung hirarki label *stack*. Jika 1 bit di-set, maka ini menandakan label yang sekarang adalah label yang terakhir.

d). 8 *bit* TTL *field*

Time to live, untuk 8 bit yang bekerja.

Teknologi ATM dan frame relay bersifat *connection-oriented*: setiap *virtual circuit* harus di-*set-up* dengan protokol persinyalan sebelum transmisi. IP bersifat *connectionless*: protokol *routing* menentukan arah pengiriman paket dengan bertukar info routing. MPLS mewakili konvergensi kedua pendekatan ini. Topologi jaringan *backbone* yang kini digunakan PT. Telkom Palembang yaitu jaringan MPLS. Seperti yang dijelaskan sebelumnya pada landasan teori, yakni MPLS adalah teknologi penyampaian paket pada jaringan *backbone* kecepatan tinggi. Sebelumnya, paket-paket diteruskan oleh *routing protocol* seperti OSPF, BGP, atau EGP. Dimana *routing protocol* tersebut berada pada layer 3 sistem OSI, sedangkan MPLS berada di antara layer 2 dan 3.

Jaringan MPLS dapat dikatakan sebagai sebuah bentuk penggabungan antara kelebihan dari ATM (*layer* 2) dan kelebihan IP (*layer* 3), dimana ATM memiliki kelebihan QoS dan *security* yang tinggi tapi tidak fleksibel dimanajemen *bandwith* atau pemborosan *bandwith*, sedangkan IP mempunyai QoS yang sensitif dan *security* yang rendah tapi fleksibilitas *bandwith* tinggi. Dari analisa diatas yang mendasari penerapan teknologi MPLS pada jaringan *backbone* PT. Telkom. Penerapan teknologi MPLS dapat dilakukan tanpa mengubah struktur dan konfigurasi pisik jaringan yang sudah ada sebelumnya.

2.4 Traffic Engineering

Traffic Engineering adalah proses pemilihan saluran data traffic untuk menyeimbangkan beban trafik pada berbagai jalur dan titik dalam network. Tujuan akhirnya adalah memungkinkan operasional network yang andal dan efisien, sekaligus mengoptimalkan penggunaan sumber daya dan performansi trafik.

Traffic Engineering sangat penting bagi para penyedia jasa layanan dan Internet Service Provider. Seperti backbone yang mendukung penggunaan transmisi yang sangat tinggi sehingga jaringan harus tahan banting agar dapat menahan link atau node yang mengalami kegagalan. Traffic Engineering MPLS menyediakan pendekatan yang terintegrasi dalam layer 3, yang fungsinya mengoptimalkan routing IP traffic.

2.5 Manfaat Traffic Engineering

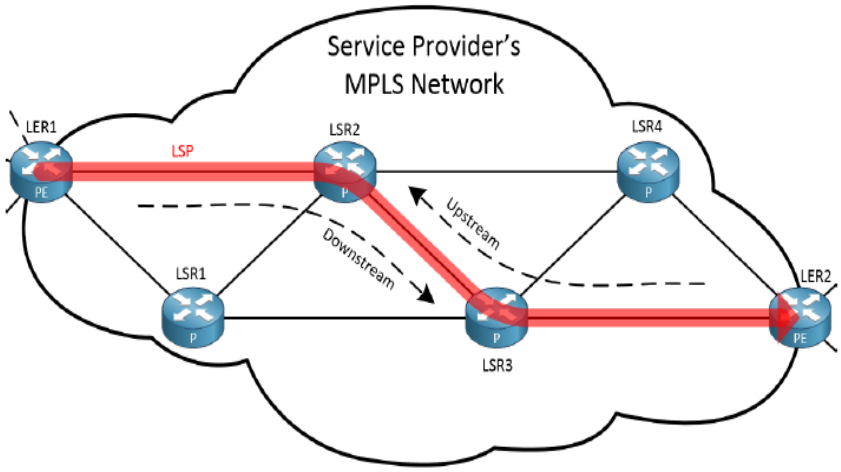
Traffic Engineering menawarkan 2 manfaat di dua bidang utama yaitu:

1. Investasi infrastruktur jaringan backbone yang lebih tinggi. Secara khusus, rute terbaik ditentukan dengan mempertimbangkan kendala jaringan backbone dan total trafik.
2. Pengurangan biaya operasi. Biaya berkurang karena proses yang penting menjadi otomatis.

2.6 *Label Switched Path* (LSP)

LSP adalah jalur satu arah yang dibentuk didalam jaringan MPLS antara dua node. Dengan kata lain, sebuah LSP adalah urutan dari LSR yang mana meneruskan label paket dari *Forwarding Equivalence Class* (FEC) tertentu. Node yang memulai sebuah LSP disebut head end dari LSP atau memiliki akronim ingress LSP, juga ke node dimana LSP dihentikan menjadi menjadi rujukan sebagai tail end dari LSP atau dengan kata lain egress LSP. Pengetahuan tentang label yang mana seharusnya digunakan untuk downstream node adalah masalah

dari control plane dimana label yang mengikat menjadi tertukar antara node dengan bantuan dari salah satu Label Distribution Protocol.



Gambar 2.4 Label Switched Path

(Sumber: Michal Aron, 2014)

2.7 Circuit Emulation Service

Circuit Emulation Service (CES) adalah teknologi telekomunikasi yang digunakan untuk mengirimkan informasi melalui jaringan data Asynchronous, seperti Ethernet atau MPLS.

Gambar 2.5 Circuit Emulation Service

Pada CES, terdapat port-port yang biasanya digunakan untuk menghubungkan antara jaringan satu dengan lainnya. Seperti pada gambar CES diatas, untuk pembacaan port (misalnya port 2/1/1 self-modul-port), 2 adalah self. Dari 4 self, untuk self pertama yaitu deretan paling atas. Self kedua dibawahnya dan seterusnya. Untuk 1 yaitu modul. Karena self kedua berarti dia berada dibarisan no 2 sebelah kiri. Untuk 1 terakhir yaitu port. Bisa dilihat pada modul 2 hanya terdapat 1 port sehingga disebut 1.

2.8 RSVP-TE

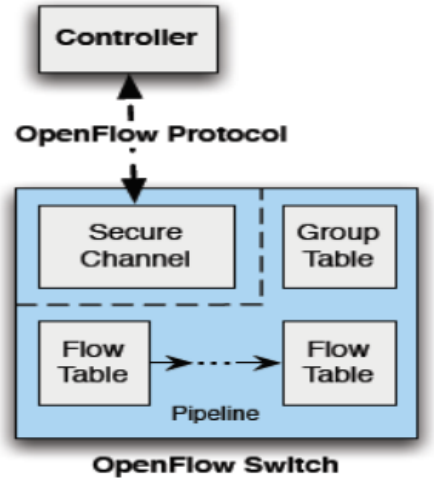
Ada dua standardisasi protokol untuk memanage alur MPLS yaitu :

1. CR-LDP (*Constraint-based Routing Label Distribution Protocol*)
2. RSVP-TE, suatu perluasan protocol RSVP untuk *traffic* rancang-bangun.

Resource Reservation protocol (RSVP) adalah protokol kontrol *internet* seperti ICMP yang beroperasi pada *transport layer* tetapi tidak berpartisipasi dalam transmisi data. RSVP-TE adalah ekstensi dari RSVP yang mendukung pendistribusian label dan memungkinkan informasi reservasi sumber daya dikirimkan dengan label *binding* (Anthony Andry, 2012:2). Pada MPLS-TE, RSVP-TE bekerja sebagai protokol *signaling* pada pembuatan LSP *Tunnel*.

2.9 OpenFlow

Openflow adalah sebuah standar terbuka yang memungkinkan peneliti untuk menjalankan eksperimen protokol dalam jaringan yang biasa kita pakai sehari-hari (Anthony Andry, 2012:2). Pada *router* klasik, *data path* dan kontrol *path* terletak dalam perangkat yang sama. Tetapi pada *Openflow switch* kedua fungsi ini dipisahkan, bagian data *path* tetap berada dalam *switch*, sementara control *path* dipindahkan ke *controller* yang terpisah. *Openflow switch* dan *controller* tersebut berkomunikasi menggunakan protokol *OpenFlow*, yang berisi *message-message* yang sudah terdefinisi sebelumnya.



Gambar 2.6 Arsitektur Openflow

Data path dari *openflow switch* memperlihatkan "*clean flow table abstraction*" dimana setiap *flow entri* terdiri dari satu set *packet field* untuk dicocokan, *counters* untuk menyimpan *flow* statistik dan sebuah aksi yang akan diberikan ketika terjadi kecocokan paket dengan *field* tersebut. Ketika *switch* menerima paket yang tidak didefinisikan dalam *flow entri*, *switch* tersebut akan mem-*forward* informasi tentang paket tersebut ke *controller*, kemudian *controller* akan memutuskan bagaimana untuk memproses paket tersebut. Paket dapat didrop atau controllerdapat menginstall *flow entri* pada *switch*, sehingga *switch* bisa menangani paket-paket yang sama selanjutnya.