DAFTAR ISTILAH

D	
Delay	Waktu yang dibutuhkan sebuah paket menempuh perjalanan dari pengirim ke penerima
J	
Jitter	Variasi Delay
P	
Packet Loss	Persentase dari paket yang hilang dari paket yang dikirim
T	
Throughput	kemampuan sebenarnya suatu jaringan dalam melakukan pengiriman data

.

BAB I
PENDAHULUAN

1.1 Latar Belakang

Industri penyedia layanan internet atau *Internet Service Provider* pada umumnya banyak menggunakan teknologi *Ethernet* dalam akses dari *core network* untuk sampai kepada pelanggan. Teknologi ini digunakan karena memiliki kestabilan yang lebih kuat dibanding dengan *wireless.*Teknologi *Ethernet* yang cukup banyak digunakan saat ini adalah koneksi *Ethernet* dengan *standard* IEEE 802.1ad karena dapat menyediakan pengiriman paket yang cepat. Untuk metode yang digunakan adalah layer 2 *tunneling*. Koneksi ini dianggap kurang baik terhadap performansi jaringan.

Pada tugas akhir ini akan dilakukan studi kasus pada Laboratorium Kalibrasi tentang bagaimana pengaruh penggunaan *Vlan stacking* pada QoS dari layanan pada jaringan simulasi tersebut.

Pada penelitian yang dilakukan Chunming Liu dan Bryan Fleming [1], telah dilakukan penggunaan metode *Vlan stacking* untuk performansi didalam suatu jaringan. Namun pada penelitian tersebut tidak membandingkan antara *single* & *double* VLAN. Sehingga penelitian akan dilanjutkan di dalam jaringan *Ethernet*.

1.2 Penelitian Terkait

Pada penelitian sebelumnya [1] telah dilakukan penggunaan *vlan stacking* sebagai metode layer 2 *tunneling*. namun pada metode tersebut belum digunakan scenario perbandingan antara *single* dan *double* vlan pada jaringan. Serta belum dilakukan analisis terkait dengan QoS.

1.3 Perumusan Masalah

Berdasarkan deskripsi latar belakang dan penelitian terkait, maka dapat dirumuskan beberapa masalah di tugas akhir ini yaitu :

1. Perancangan dan implementasi pada metode VLAN *Stacking* untuk performansi pada jaringan simulasi.

2. Mengukur dan menganalisis QoS *standard* ITU dengan 3 parameter yaitu *Delay*, *Throughput*, dan *Jitter* pada jaringan berdasarkan tiga scenario pengujian yaitu hanya menggunakan CVLAN, menggunakan SVLAN dan menggunakan *Double* VLAN untuk analisis kemampuan VLAN *Stacking* dalam performansi jaringan.

1.4 Tujuan Penelitian

1. Implementasi jaringan dengan *Single* & *Double* VLAN
2. Menganilis performansi jaringan *single* & *double* VLAN berdasarkan parameter *throughput*, *delay*, *jitter* dan *packet loss*.

1.5 Batasan Masalah

1. Pada tugas akhir ini dilakukan pengamatan pada performansi jaringan saja, tidak berkaitan dengan keamanan jaringan.
2. Topologi jaringan yang digunakan adalah point-to-point untuk semua skenario.
3. Skenario yang dibuat menggunakan empat segmen yang berbeda sehingga setiap klien hanya dapat berkomunikasi dengan satu server saja

1.6 Sistematika Penulisan

Adapun sistematika penulisan pada tugas akhir ini sebagai berikut.

BAB I PENDAHULUAN

Bab ini menjelaskan mengenai latar belakang, rumusan masalah, batasan masalah, tujuan, metodologi penelitian, dan sistematika penulisan tugas akhir ini

BAB II DASAR TEORI

Bab ini menjelaskan berbagai dasar teori yang mendasari penulisan tugas akhir ini.

BAB III PERANCANGAN DAN IMPLEMENTASI

Pada bab ini akan dibahas bagaimana model simulasi yang akan dibuat, cara kerja sistem, diagram alir dari proses kerja sistem, dan hasil keluaran sistem.

BAB IV PENGUJIAN SISTEM DAN ANALISIS HASIL

Pada Bab ini akan dilakukan implementasi perancangan jaringan simulasi dan dilakukan anilisis terhadap simulasinya

BAB V KESIMPULAN DAN SARAN

Bab ini akan menguraikan kesimpulan dari hasil penelitian Tugas Akhir ini dan saran untuk pengembangan lebih lanjut.

1.7 Metodologi Penelitian

Metode yang dilakukan dalam penyusunan tugas akhir ini adalah sebagai berikut

1. Studi literatur

a. Mempelajari mengenai prinsip dan cara kerja *VLAN Stacking*
b. Mempelajari dari jurnal dan buku mengenai *Provider Bridge*.
c. Diskusi dan konsultasi dengan Dosen dan Mahasiswa sertaPembimbing dari Laboratorium Kalibrasi

2. Implementasi Sistem

a. Merancang arsitektur jaringan simulasi yang akan digunakan
b. Mengimplementasikan jaringan simulasi yang sudah dirancang
c. Mengimplementasikan metode *Vlan stacking* pada jaringan simulasi

3. Simulasi Sistem

a. Melakukan simulasi trafik antara pelanggan dengan penyedia layanan
b. Melakukan pengukuran secara *troughput*, *delay* dan *jitter* pada trafik dari sisi penyedia layanan.

4. Analisis Kerja Sistem

Menganilisis hasil dari simulasi yang telah dilakukan

BAB II
DASAR TEORI

2.1 Evolusi Standar Ethernet menuju 802.1ad

Perkembangan *Ethernet* telah didorong oleh kebutuhan untuk menyediakan *set* standar layanan *Ethernet* yang dapat didefinisikan dan mudah dibangun. *Ethernet* bermula sebagai media bersama tunggal. Telah terjadi evolusi progresif interkoneksi dan *forwarding*, dengan repeater pertama kali berkembang menjadi hub, dan kemudian berkembang menjadi bridge dengan peningkatan yang progresif dalama skala dan efisiensi [2]

Bridging Ethernet, sering kali disebut bridging yang transparan, adalah suatu mekanisme yang bertanggung jawab untuk menyampaikan dan mereplikasi *frame Ethernet* dalam sebuah jaringan *Ethernet* [2].

2.1.1 VIRTUAL LAN (IEEE 802.1Q)

Dalam beberapa tahun terakhir penggunaan *Ethernet* menemukan jalan melalui jaringan operator untuk menyediakan layanan *point-to-point* dan VLAN. Kesederhanaan dan efisiensi biaya perlengkapan *Ethernet* menjadikan sesuatu yang menarik, tapi berdasarkan kebutuhan, jaringan memerlukan kapabilitas *Ethernet* yang mudah untuk diperpanjang [2].

VLAN pertama kali dikenalkan pada pertengahan tahun 1990 yang secara logika berkonsentrasi pada topologi *bridged* jaringan fisik. *Id* VLAN (VID) adalah sebuah bagian dalam *header Ethernet* yang memilliki 12 bit, melewati 4096 VLAN. Ada sebuah konsep mengaktifkan topologi VLAN untuk mengatur *port bridge* membagi VLAN tersebut. Kemudian ada juga konsep penyedia layanan dengan VLAN menjadi antarmuka *port*. Inilah alasan bahwa VLAN dalam sebuah *interface* atau sirkuit *point-to-point* memiliki kemudahan sebagai pengenal kanal untuk layanan *multiplexing*. [2]

Dalam *switching Ethernet*, suatu konsep topologi aktif VLAN sangat berguna untuk membatasi domain *broadcast* dan kontrol LAN. Dengan membuat VLAN dan memasukkan *port* ke VLAN, sesuatu yang menarik terbentuk. Banyak VLAN dijalankan secara paralel. Sebagai VLAN yang telah terbentuk, *quality of*

service (QoS) juga perlu diperhatikan.setelah perkembangan yang terjadi, Sebuah *tag header* dibuat untuk memperpanjang *frame Ethernet*. *Header* Q-Tag membawa ID VLAN, dan juga mengandung prioritas layanan [2]

2.1.2 PROVIDER BRIDGE (IEEE 802.1AD)

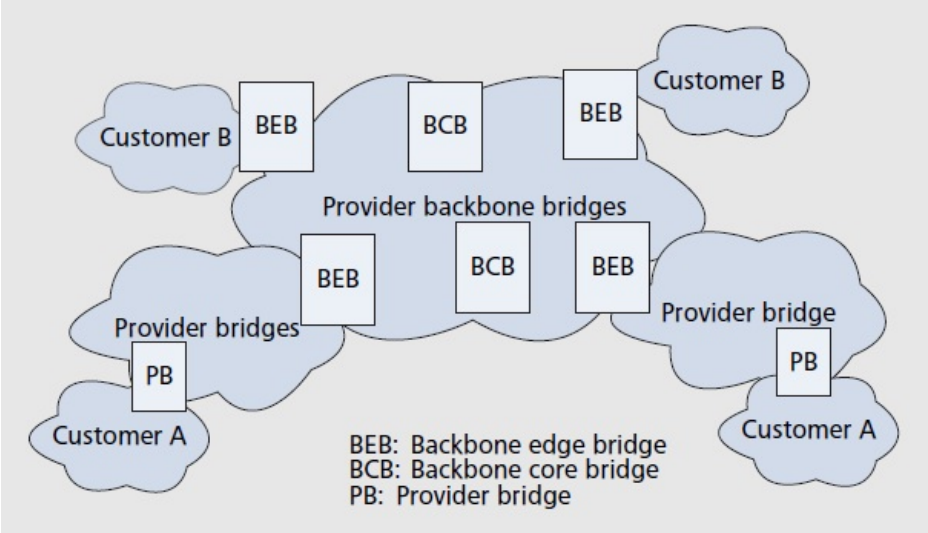
Secara fisik kabel *Ethernet* memiliki batasan dalam mengaplikasikan *Ethernet* di lingkup operator. Operator biasanya membuat teknologi *Ethernet* terkoneksi langsung ke jaringan mereka. Hal ini menyebabkan konflik untuk penggunaan VLAN, sebagaimana dipergunakan oleh dua penyedia layanan dan pelanggan *enterprise*. [2]

Penyedia layananan mulai menawarkan layanan pada layer 2 antara daerah pelanggan. Layanan layer 2 ini, dicari oleh pelanggan sebagai *media sharing* sebuah LAN atau VLAN. Kenyataan peng implementasian Operator pertama kali berdasarkan teknologi lain seperti *asynchronous transfer mode* (ATM) dan terakhir *virtual private* LAN *service* (VPLS). Pelanggan juga menggunakan VLAN mereka untuk QoS dan memudahkan managemen layer 2. Ketika operator menawarkan sebuah layanan VLAN kepada pelanggan, operator akan mempunyai tambahan perlengkapan VLAN pelanggan. [2].

Situasi ini memberikan beberapa solusi yang disetujui untuk melayani berbagai kebutuhan pelanggan. Solusi yang tersedia adalah untuk membagai Q-TAG, yang bernama *header* Q-in-Q. Membagi VLAN untuk membedakan *Customer* VLAN (CVLAN) dari *Service* VLAN (SVLAN) memberikan jaringan operator untuk membuat ruang VLAN operator ketika membawa jaringan VLAN pelanggan lain secara jelas. terdapat 2 aspek penting disini, pertama, ada mekanisme untuk menggabungkan VLAN pelanggan dalam VLAN operator. Kedua, ada kebutuhan untuk meyediakan VLAN operator [2].

802.1Q memiliki bidang 12-bit VLAN ID, yang memiliki batas teoritis 2^12=4096 *tags*. Dengan pertumbuhan jaringan, keterbatasan ini menjadi lebih penting. Sebuah frame *double-tag* memiliki keterbatasan teoritis 4096x4096= 16777216, cukup untuk mengakomodasi pertumbuhan jaringan untuk beberapa tahun kedepan. Sebuah tumpukan *tag* menciptakan mekanisme untuk *Internet Service Provider* untuk merangkum trafik pelanggan dengan *tag* tunggal, frame

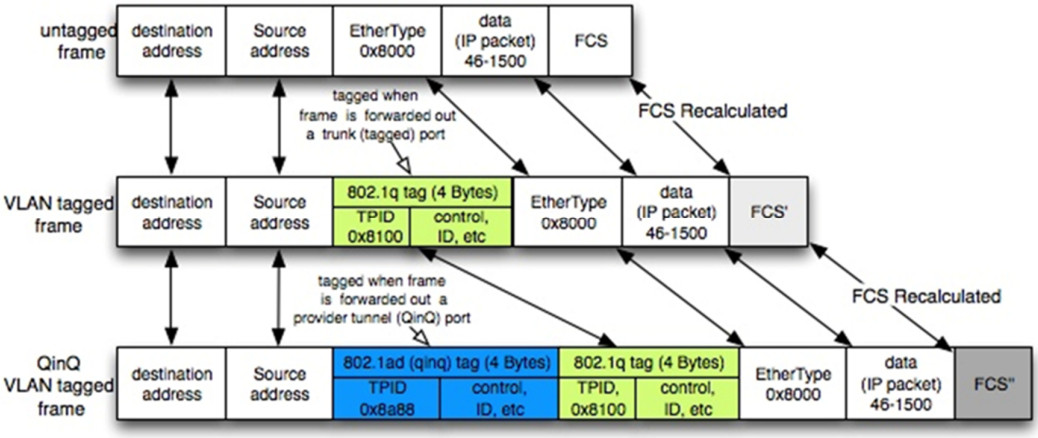
akhir menjadi sebuah frame QinQ. *Outer tag* digunakan untuk mengidentifikasi dan memisahkan trafik dari pelanggan yang berbeda dan *inner tag* diawetkan dari frame aslinya.



Gambar 2.1 *Provider backbone bridge hierarchy* [2]

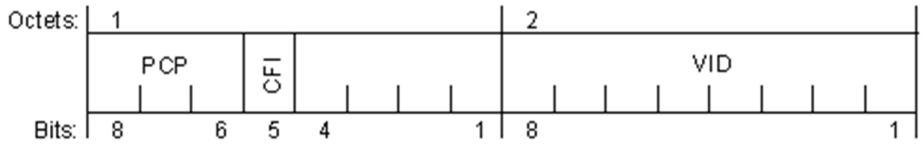
2.1.2.1 Frame Format

Untagged frame adalah frame asli dari sebuah protokol *Ethernet* dengan identitas *ethertype* 0x8000. Penambahan header dengan panjang 4 byte membuat *ethertype* frame asli berubah menjadi 0x8100. *Header* kedua ditambahkan dengan *ethertype* 0x88A8 secara *default* [3].



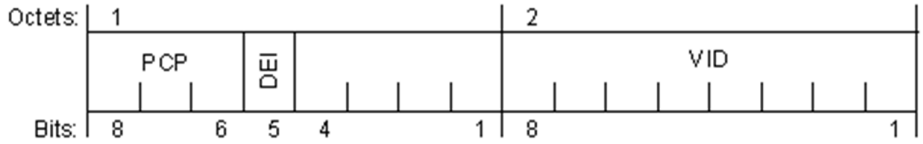
Gambar 2.2 Format Frame

a. CVLAN Tag



Gambar 2.3 C-TAG *Format* [7]

b. SVLAN Tag



Gambar 2.4 S-TAG *Format* [7]

2.2 Quality of Service

QoS adalah parameter yang menunjukkan kemampuan suatu jaringan untuk menyediakan layanan pada berbagai *platform* teknologi. QoS tidak diperoleh langsung dari infrastruktur yang ada, melainkan diperoleh dengan mengimplementasikannya pada jaringan yang bersangkutan. Parameter QoS yang digunakan untuk mengetahui kualitas dari suatu layanan yaitu:

1. Throughput

didefinisikan sebagai kemampuan sebenarnya suatu jaringan dalam melakukan pengiriman data.

$$throughput = \frac{\text{Jumlah data yang diterima}}{\text{waktu perngiriman data}}$$

2. End to End Delay

Delay yang didefinisikan sebagai waktu yang dibutuhkan sebuah paket untuk sampai pada satu titik dari titik asal. Pengukuran dari *end-to-end* delay bergantung kepada komponen seperti waktu propagasi, waktu transmisi, waktu antrian dan waktu proses.

Delay propagasi atau *propagation delay* adalah waktu yang diperlukan oleh suatu informasi untuk melintasi suatu line dengan jarak tertentu. *Propagation delay* ditentukan oleh jarak dan kecepatan cahaya. Waktu transmisi atau

transmission delay adalah waktu yang diperlukan oleh sebuah paket data untuk melintasi suatu media. Transmission delay dipengaruhi oleh kecepatan media besar paket data. Processing delay adalah waktu yang diperlukan network untuk memproses data real menjadi bit bit data yang akan dikirimkan. Queing delay adalah waktu yang diperlukan oleh sebuah paket dalam suatu antrian.

$$delay \text{ rata} - \text{rata} = \frac{\text{total delay}}{\text{total paket yang diterima}}$$

3. Jitter

Jitter dapat didefinisikan sebagai variasi dari delay *end-to-end* yang di akibatkan oleh panjang antrian dalam suatu pengolahan data dan reassemble paket-paket data di akhir pengiriman akibat kegagalan sebelumnya.

4. Packet loss

Didefinisikan sebagai persentase dari paket yang hilang dari paket yang dikirim.

$$packet\ loss = \frac{\text{paket data yang dikirim} - \text{paket data yang diterima}}{\text{paket data yang dikirim}} \text{x100\%}$$

2.3 Virtual Private Network (VPN)

Virtual Private Network (VPN) adalah sebuah jaringan komputer dimana koneksi antar nodenya memanfaatkan jaringan publik (internet/WAN) karena mungkin dalam kondisi atau kasus tertentu tidak memungkinkan untuk membangun infrastruktur sendiri. Ketika mengkoneksikan VPN, interkoneksi antar node seperti memiliki jaringan yang independen yang sebenarnya dibuatkan koneksi atau jalur khusus melewati jaringan publik.

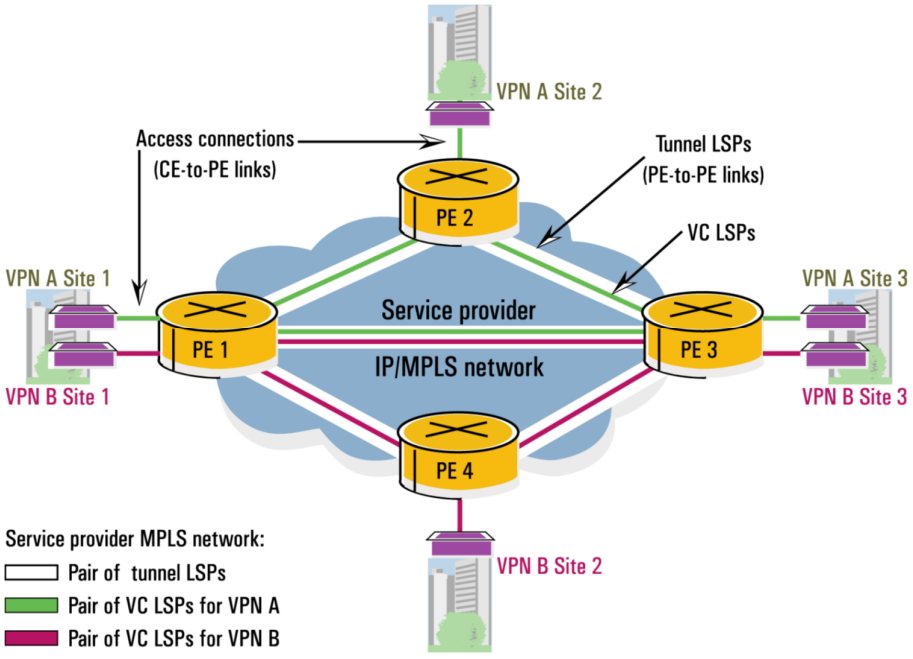
Pada implementasinya, VPN biasanya digunakan untuk membuat komunikasi yang bersifat *secure* melalui jaringan internet, tetapi VPN tidak harus menggunakan standar keamanan yang baku seperti autentikasi atau enkrispsi. VPN biasanya digunakan oleh perusahaan yang membutuhkan ruang sendiri di internet. Misalnya komunitas bisnis yang memerlukan keamanan jaringan sendiri di internet

melakukan berbagai kegiatan dalam lingkungannya sendiri. VPN bisa diimplementasikan di jaringan yang melewati multi hop (*routed network*) ataupun jaringan yang ruang lingkupnya masih dalam satu switch (*bridge network*).

Penggunaan VPN bisa menggunakan suatu perangkat khusus produksi vendor tertentu yang dibuat untuk proses komunikasi lewat internet, seperti produk dari vendor Cisco, Nortel, Linksys, dll. Sistem tersebut juga disebut *hardware based*, sedangkan sistem yang menggunakan perangkat lunak sebagai sistem utamanya sering disebut sebagai *software based*. Contoh aplikasi yang digunakan untuk membangun VPN adalah: OpenVPN, UltraVPN, CyberGhost, Tor VPN, AceVPN, Safe VPN, dll.

2.3.1 Virtual Private LAN Service (VPLS)

VPLS, yang dikenal juga sebagai Transparent LAN Service (TLS) atau E-LAN service, adalah multipoint VPN layer 2 yang mengijinkan banyak daerah untuk dihubungkan dalam satu *single bridge* domain yang sama melalui jaringan IP/MPLS. Semua daerah *client* dalam VPLS instance dapat seolah-olah berada pada satu jaringan LAN yang sama walaupun sebenarnya terpisah secara geografis. VPLS menggunakan *interface Ethernet* ke client-nya [4].



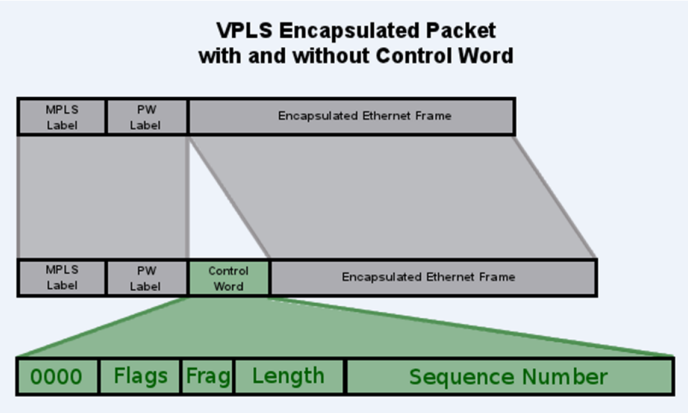
Gambar 2.5 VPLS *Reference Model* [8]

Jaringan VPLS terdiri dari Customer Edge (CE), Provider Edge (PE), dan jaringan MPLS sebagai *core network*-nya:[4]

a. Perangkat CE merupakan sebuah router atau switch yang terletak pada sisi *client*, dapat dimiliki maupun di *manage* oleh *client* ataupun dimiliki dan juga di-manage oleh *service provider*. Perangkat CE terhubung ke PE melalui sebuah Attachment Circuit (AC). Dalam kasus VPLS, diasumsikan bahwa *interface* antara CE dan PE adalah *Ethernet.*

b. Perangkat PE merupakan dimana kecerdasan VPN berada, dimana VPLS dimulai dan diakhiri, dan dimana semua *tunnel* yang dibutuhkan dibentuk untuk menghubungkan semua PE. Karena VPLS merupakan layanan *Ethernet* layer 2, PE harus memiliki kemampuan untuk pembacaan Media Access Control (MAC).

c. *Core network* IP/MPLS menginterkoneksikan setiap PE. Sebenarnya *core* IP/MPLS tidak benar-benar berpartisipasi dalam fungsi VPN. Trafik secara *simple* di-switch berdasarkan MPLS label.

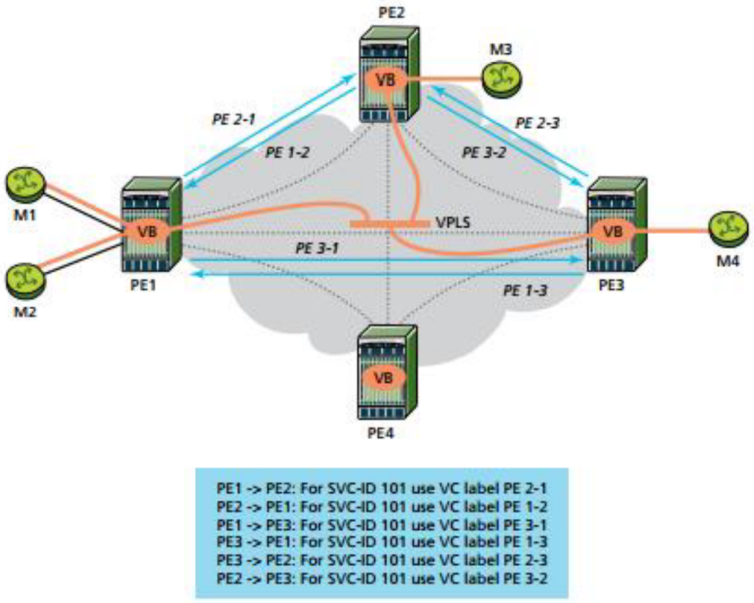


Gambar 2.6 Format Paket VPLS [5]

2.3.1.1 Cara kerja VPLS

Diasumsikan bahwa ada *full mesh* antara empat PE yang terhubung ke jaringan MPLS. Sebagai contoh, sebuah VPLS instance diidentifikasi oleh Service-identifier 101 (Svc-id 101) harus dibuat antara PE1, PE2, dan PE3. PE4 tidak ikut berpartisipasi dalam VPLS *instance* ini. Asumsikan bahwa konfigurasi ini ditentukan dengan menggunakan mekanisme *auto-discovery* yang tidak ditentukan. M1, M2, M3, dan M4 adalah *end-station* yang terdapat pada lokasi client yang

berbeda dan AC mereka ke perangkat PE masing-masing telah dikonfigurasi dalam PE yang tergabung dalam VPLS *instance*, Svc-id 101.[4]



Gambar 2.7 PW *Signaling* [4]

a. Pembentukan PW

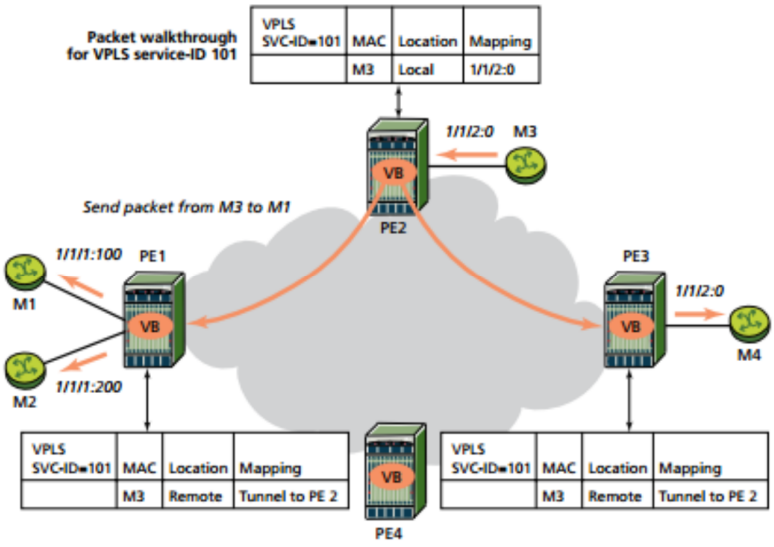
Tiga PW perlu dibuat, masing-masing terdiri dari sepasang LSP searah atau VC. Untuk pensinyalan VC label antara PE, setiap PE memulai sesi *targeted* LDP ke PE *peer* dan berkomunikasi dengan PE *peer* dimana VC label digunakan ketika mengirim paket untuk VPLS yang dipertimbangkan. Spesifik VPLS *instance* diidentifikasi pada pertukaran pensinyalan menggunakan sebuah *service identifier* sebagai contoh Svc-101. Dalam contoh berikut, PE1 mengindikasikan ke PE2 “Jika Anda memiliki trafik untuk dikirim kepada saya untuk Svc-id 101, gunakan VC label PE2-1 pada enkapsulasi paket”. Demikian juga, PE2 mengindikasikan ke PE1 ”Jika Anda memiliki trafik untuk dikirim kepada saya untuk Svc-id 101, gunakan VC label PE1-2 pada enkapsulasi paket”. Melalui cara ini, PW pertama dibuat.[4]

b. MAC learning dan paket forwarding

Setelah VPLS *instance* dengan Svc-id 101 telah dibuat, paket pertama dapat dikirim dan proses MAC *learning* dimulai. Asumsikan M3 sedang

mengirimkan sebuah paket ke PE2 yang ditujukan untuk M1 (M3 dan M1 diidentifikasi dengan alamat MAC yang unik), seperti yang ditunjukkan pada gambar di bawah ini:[4]

- PE2 menerima paket dan mempelajari (dari alamat MAC sumber) bahwa M3 dapat dicapai pada port local 1/1/2:0, dia menyimpan informasi ini pada FIB untuk Svc-id 101.
- PE2 belum mengetahui alamat MAC tujuan M1, sehingga dia membanjiri paket ke PE1 dengan VC label PE2-1 (pada MPLS outer tunnel yang sesuai) dan PE3 dengan VC label PE2-3 (pada MPLS outer tunnel yang sesuai). Format paket ditunjukkan pada gambar.
- PE1 belajar dari VC label PE2-1 bahwa M3 berada di belakang PE2, dia menyimpan informasi ini pada FIB untuk Svc-id 101.
- PE3 belajar dari VC label PE2-3 bahwa M3 berada di belakang PE2, dia menyimpan informasi ini pada FIB untuk Svc-id 101.
- PE1 mencopot label PE2-1, tidak tahu tujuan M1 dan membanjiri paket pada port 1/1/1:100 dan 1/1/1:200.
- PE3 mencopot label PE2-3, tidak tahu tujuan M1 dan mengirim paket ke port 1/1/2:0.
- M1 menerima paket.



Gambar 2.8 VPLS *Learning* [4]

Ketika M1 menerima paket dari M3, dia menjawab dengan sebuah paket ke M3.

- PE1 menerima paket dari M1 dan mempelajari bahwa M1 berada pada local port 1/1/1:100. Dia menyimpan informasi ini pada FIB untuk Svc-id 101.
- PE1 sudah mengetahui bahwa M3 dapat dicapai melalui PE2 dan karena itu hanya mengirimkan paket ke PE2 menggunakan label VC PE1-2.
- PE2 menerima paket untuk M3. Dia mengetahui bahwa M3 dicapai pada port 1/1/2:0.
- M3 menerima paket.

2.3.1.1 Enkapsulasi Ethernet

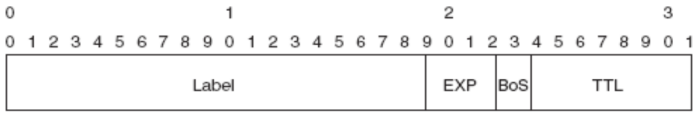
Berikut ini adalah tiga jenis enkapsulasi yang digunakan di dalam *port* akses *ethernet.*

1. Null
   Id enkapsulasi dibuat sama dengan 0
2. Dot1q
   Memiliki nilai dari 0 sampai 4096
3. Qinq
   Memiliki dua taq. Setiap taq mempunyai nilai dari 0 sampai 4096

2.3.2 Multi Protcocol Label Switching (MPLS)

Multi Protocol Label Switching (MPLS) adalah suatu metode *forwarding* (meneruskan data melalui suatu jaringan dengan menggunakan informasi dalam label yang dilekatkan pada paket IP), sehingga memungkinkan router untuk meneruskan paket dengan hanya melihat label dari paket itu, tidak perlu melihat alamat IP tujuannya. [9]

Format *header* MPLS:



Gambar 2.9 Format MPLS *Header* [9]