

Simulasi Multi Protocol Label Switching Virtual Private Network (MPLS VPN) Dengan Virtual Local Area Network (VLAN) Menggunakan Router MIKROTIK

Bertha Euginia¹, Theresia Ghozali¹

ABSTRACT: Abstract MPLS VPN with VLAN network is used to get fast, secure, and easily accessible communication. MPLS network will send packet data with label in header to the destination and VPN will limit the user who can access the network by VRF configuration. Routing protocol OSPF will divide to two areas, customer area and provider area. VLAN will be configured in switch and router CE1 so they can exchange data to workgroup and it will be safe because it is not broadcasted. MPLS VPN with VLAN simulation using Mikrotik router board and switch by measuring bandwidth. The result show that MPLS VPN with VLAN using less bandwidth than MPLS VPN.

KEYWORDS: OSPF, mikrotik, MPLS, VLAN, VPN

ABSTRAK: Untuk mendapatkan komunikasi yang cepat, aman, dan mudah diakses digunakan jaringan MPLS VPN menggunakan VLAN. Jaringan MPLS akan mengirimkan paket sesuai dengan label yang ada pada header paket ke tujuan yang diinginkan dan VPN akan membatasi siapa pengguna yang berhak mengakses jaringan menggunakan konfigurasi VRF. Routing protokol OSPF dibagi dua daerah yaitu daerah *customer* dan *provider*. VLAN akan dikonfigurasi melalui switch dan router CE1 agar dapat saling bertukar data ke *workgroup* dan lebih aman karena tidak dikirimkan secara *broadcast*. Hasil pengujian menunjukkan bahwa MPLS VPN dengan VLAN menghasilkan *bandwidth* lebih kecil dibandingkan MPLS VPN tanpa VLAN.

KATA KUNCI: OSPF, mikrotik, MPLS, VLAN, VPN

PENDAHULUAN

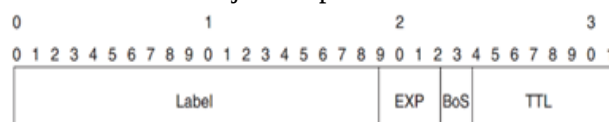
Di zaman seperti ini banyak orang dan perusahaan yang membutuhkan komunikasi yang lancar, aman, dan mudah diakses. Misalnya komunikasi dalam suatu perusahaan. Suatu perusahaan besar yang memiliki beberapa cabang perusahaan dapat berkomunikasi dengan baik dengan cara membangun jaringan komunikasi menggunakan *switching* dan *routing* serta harus memiliki jaringan yang aman agar tidak mudah diakses oleh pihak yang tidak bertanggungjawab.

Upaya yang dilakukan untuk membangun jaringan yang baik dan aman adalah dengan membuat *Virtual Private Network* (VPN) melalui jaringan Multi Protocol Label Switching (MPLS). Melalui VPN, dapat mempermudah pengguna karena dapat mengakses dan menggunakan jaringan pada perusahaan dimana saja selama terhubung dengan internet dan penggunaan *bandwidth* yang rata. Selain menggunakan VPN, untuk mempermudah perusahaan yang memiliki banyak divisi maka suatu perusahaan memerlukan suatu jaringan *Virtual Local Area Network* (VLAN). VLAN dapat berfungsi untuk menghubungkan beberapa cabang menjadi *workgroup* atau suatu grup kecil sehingga dapat berkomunikasi dengan divisi lain dengan lancar, mudah, dan murah. Dengan VLAN dapat membuat penggunaan *bandwidth* menjadi efisien sehingga dapat menghindari *bandwidth storm*. Satu divisi perusahaan dengan divisi perusahaan lain tentu ada beberapa data yang bersifat rahasia dan tidak dapat dikirimkan secara *broadcast* ke seluruh divisi. Oleh karena itu, pada jaringan ini diperlukan MPLS dan VLAN agar dapat menentukan rute mana yang ingin dilewati, rute mana yang cepat untuk mengirimkan suatu informasi dan *workgroup* mana yang ingin kita kirimkan informasinya.

MULTI PROTOCOL LABEL SWITCHING (MPLS)

Multiprotocol Label Switching (MPLS) adalah teknologi penyampaian paket pada jaringan dengan cepat yang menggabungkan kelebihan dari sistem komunikasi circuit-switched dan packet-switched. Kelebihan circuit-switched adalah menentukan jalur berdasarkan label yang ada pada paket, sedangkan kelebihan packet-switched adalah memungkinkan jalur dapat dipakai oleh user lain[2]. MPLS dapat mengirimkan data dengan cepat, karena pada MPLS memberi label pada header paket. Label tersebut akan memuat informasi penting yang berhubungan dengan informasi routing sebuah paket.

Prinsip kerja MPLS adalah pemberian label pada setiap paket yang ingin diteruskan ke tujuan. Pemberian label dilakukan untuk menentukan jalur pengiriman ke tujuan dan prioritas paket mana yang harus dikirim dahulu. Pemberian label dilakukan dengan menyelipkan label di antara header layer 2 dan layer 3 pada paket yang diteruskan. Struktur label MPLS ditunjukkan pada Gambar 1.



■ Gambar 1 Struktur Label MPLS [1]

¹ Program Studi Teknik Elektro Universitas Katolik Atma Jaya

Label MPLS terdiri dari 32 bit data dengan 20 bit pertama untuk nomor label, 3 bit untuk *experimental* (EXP), 1 bit untuk *Bottom of Stack* (BoS), dan 8 bit untuk *Time To Live* (TTL). Bit EXP berisi informasi kelas layanan. Bit pada BoS digunakan untuk mengetahui apakah terdapat label lain dalam suatu paket. Jika label BoS bernilai 1, maka terdapat lebih dari satu label pada paket, sedangkan jika BoS bernilai 0, maka hanya ada satu label pada paket. Bit TTL berisi informasi umur paket dan berapa kali paket dapat diteruskan. Bit TTL akan berkurang satu setiap paket melalui hop untuk menghindari terjadinya paket *storms*. Paket *storms* adalah paket yang tidak dapat diteruskan dan terjebak dalam *loop*, sehingga dapat menyebabkan kelebihan paket yang dikirim dan akhirnya paket akan *crash* atau tidak berhasil terkirim ke tujuan.

Berikut adalah komponen MPLS yang dapat dilihat pada Gambar 2, yaitu:

1. *Label Switched Path* (LSP)

Label MPLS terdiri dari 32 bit data dengan 20 bit pertama untuk nomor label, 3 bit untuk *experimental* (EXP), 1 bit untuk *Bottom of Stack* (BoS), dan 8 bit untuk *Time To Live* (TTL). Bit EXP berisi informasi kelas layanan. Bit pada BoS digunakan untuk mengetahui apakah terdapat label lain dalam suatu paket. Jika label BoS bernilai 1, maka terdapat lebih dari satu label pada paket, sedangkan jika BoS bernilai 0, maka hanya ada satu label pada paket. Bit TTL berisi informasi umur paket dan berapa kali paket dapat diteruskan. Bit TTL akan berkurang satu setiap paket melalui hop untuk menghindari terjadinya paket *storms*. Paket *storms* adalah paket yang tidak dapat diteruskan dan terjebak dalam *loop*, sehingga dapat menyebabkan kelebihan paket yang dikirim dan akhirnya paket akan *crash* atau tidak berhasil terkirim ke tujuan.

2. *Label Switching Router* (LSR)

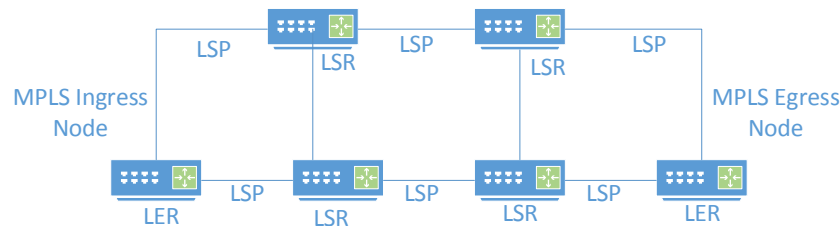
Label Switching Router (LSR) merupakan MPLS *node* yang mampu meneruskan paket-paket *layer 3*

3. *Label Edge Router* (LER)

Label Edge Router (LER) merupakan MPLS *node* yang menghubungkan sebuah MPLS domain dengan *node* yang berada di luar MPLS domain

4. *Label Distribution Protocol* (LDP)

Label Distribution Protocol (LDP) berfungsi untuk mendistribusikan informasi yang ada pada label ke setiap LSR pada jaringan MPLS. Selain itu, LDP juga melakukan penempatan label awal (*initial label*) dan mengambil label MPLS dari paket (*popped label*).



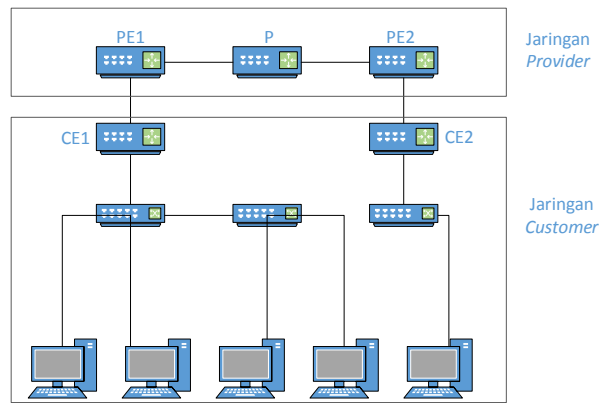
■ Gambar 2 Komponen MPLS.

MULTI PROTOCOL LABEL SWITCHING VIRTUAL PRIVATE NETWORK

Virtual Private Network (VPN) adalah sebuah jaringan komputer dimana koneksi antar perangkatnya (*node*) memanfaatkan jaringan publik sehingga yang diperlukan hanyalah koneksi internet di masing-masing *site*. Meskipun VPN menggunakan jaringan publik, keamanan dan kerahasiaan antar pengguna VPN dapat tetap terjaga karena VPN membentuk jalur *virtual* khusus yang hanya bisa diakses oleh pengguna VPN.

MPLS VPN merupakan jaringan VPN berbasis MPLS dimana komunikasi antar pengguna menjadi lebih aman meskipun menggunakan jaringan publik. Jaringan MPLS VPN dibagi menjadi empat jenis perangkat seperti Gambar 3, yaitu:

1. Perangkat *Customer* yaitu perangkat pada jaringan yang berhubungan langsung dengan pengguna jaringan.
2. Perangkat *Customer Edge* (CE) yaitu perangkat yang terletak di paling luar jaringan *customer* yang berhubungan langsung dengan perangkat *Provider Edge* (PE) untuk meneruskan setiap paket yang dikirim untuk *customer*.
3. Perangkat *Provider Edge* (PE) yaitu perangkat yang terletak di paling luar jaringan *provider*. Perangkat PE berfungsi untuk melakukan pemberian label paket, pertukaran informasi antar protokol *routing*, menerjemahkan informasi *routing* dari perangkat *customer edge* menjadi informasi VPNv4 *route* dan sebagai pembatas antara protokol *routing* pada *customer* dan *provider*.
4. Perangkat *Provider* yaitu perangkat yang terletak di pusat jaringan *provider* yang berfungsi untuk melakukan proses *switching* dan meneruskan paket MPLS menuju perangkat PE tujuan. [10]



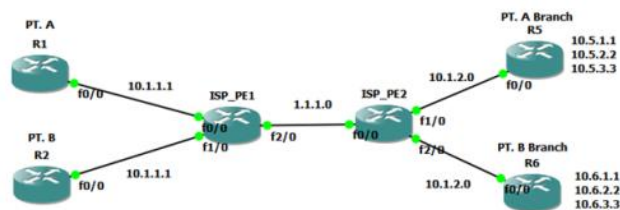
■ Gambar 3 Jaringan MPLS VPN

Cara kerja MPLS adalah memberikan label pada *header* paket. Label MPLS berisi jalur yang akan ditempuh paket untuk sampai ke tujuan. Label yang berada pada ujung jaringan MPLS disebut *Label Edge Router* (LER). Label ini berguna untuk mencatat dan menganalisa paket sebelum masuk ke MPLS.

Setiap paket yang sudah diberi label akan masuk ke router berikutnya. Pada router *provider edge* (*hop*) akan dilihat informasi yang dibawa oleh paket mengenai *hop* berikutnya dan mengganti label paket (*swap*) dengan label baru yang ada pada router *provider edge*. Paket yang telah diberi label baru akan diteruskan ditujukan berdasarkan informasi *routing* dari router *customer edge*. Setelah sampai pada router *customer edge* tujuan akhir jaringan MPLS, label yang telah diteruskan dari *provider edge* akan dilepaskan dari *header* paket (*pop*).

VIRTUAL ROUTING FORWARDING

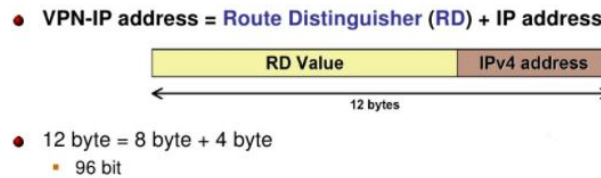
Virtual Routing and Forwarding (VRF) adalah teknologi yang memungkinkan beberapa tabel *routing* berjalan bersamaan pada suatu *router* dan pada waktu yang sama. Gambar 4 memperlihatkan jaringan VRF. Pada router *Provider Edge* (PE) harus dikonfigurasi terlebih dahulu menggunakan VRF agar dapat membentuk VPN. Alamat IP dari perangkat *customer* dan *Customer Edge* (CE) dicatat pada VRF. Setiap VRF memiliki data paket yang disimpan pada *IP routing table* untuk mencegah paket luar yang masuk ke dalam VPN dan mencegah paket didalam VPN yang akan diteruskan keluar dari VPN. [6].



■ Gambar 4 Jaringan VRF [5].

Komponen utama untuk dapat membentuk VRF adalah:

1. *Route distinguisher* membuat alamat IPv4 terdiri dari 32 bit menjadi 96 bit *unique address*. Format *route distinguisher* adalah *autonomous system number:arbitrary number* atau *IP address:arbitrary number*. Sebagai contoh, alamat IP tujuan adalah 192.168.10.0 dengan nomor *autonomous system* 100 dan jalur VPN 1. Setelah ditambahkan *route distinguisher*, alamat IP tujuan akan dikenali oleh jaringan sebagai 100:1 atau 192.168.10.0:1. Paket IP yang telah ditambahkan *route distinguisher* akan menjadi paket VPN-IPv4. Alamat VPN-IPv4 ini yang akan digunakan oleh MP BGP untuk meneruskan paket melalui MPLS.
2. *Route target* digunakan untuk menentukan *route* yang akan diimpor ke dalam VRF dan menentukan *route* yang akan diekspor dari VRF. Penambahan *route target* pada *route distinguisher* dilakukan saat terdapat *customer* yang memiliki dua atau lebih VPN. Sebagai contoh, *route target-export* 100:1 menandakan bahwa *routing* VRF akan diberikan kepada VRF dengan *route distinguisher* 100:1. Sedangkan, *route-target import* 100:1 menandakan bahwa VRF akan mengambil informasi *routing* dari VRF dengan *route distinguisher* 100:1. Dengan penggunaan *route target*, jaringan VPN hanya akan dapat diakses oleh VRF yang telah dikonfigurasi pada *router*. Gambar 5 menunjukkan bentuk alamat VPNv4.



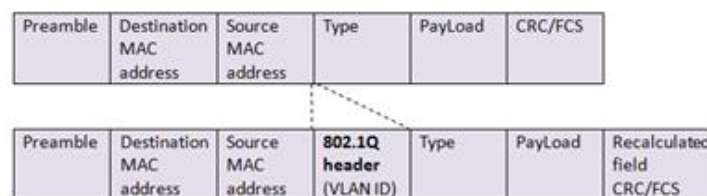
■ Gambar 5 Bentuk alamat VPNv4.

BORDER GATEWAY PROTOCOL

Border Gateway Protocol (BGP) adalah salah satu jenis *routing protocol* yang berfungsi untuk mempertukarkan informasi antar *Autonomous System* (AS). *Autonomous System* (AS) adalah kumpulan dari jaringan-jaringan dalam satu administrasi yang mempunyai strategi *routing* bersama. BGP diperlukan untuk menerjemahkan alamat yang VPNv4 yang telah dirubah oleh VRF untuk membangun jaringan VPN dan BGP digunakan oleh router PE agar dapat terhubung dengan router P.

VIRTUAL LOCAL AREA NETWORK

Virtual Local Area Network (VLAN) merupakan sekelompok perangkat pada satu *Local Area Network* (LAN) atau lebih yang dikonfigurasi (menggunakan perangkat lunak pengelolaan) sehingga dapat berkomunikasi seperti halnya bila perangkat tersebut terhubung ke jalur yang sama, walaupun sebenarnya perangkat tersebut berada pada sejumlah segmen LAN yang berbeda. VLAN berada pada *layer* kedua pada OSI *seven layer*. Protokol umum yang paling sering digunakan adalah IEEE 802.1Q. 802.1Q berfungsi untuk membentuk jalur agar satu VLAN dengan VLAN lain dapat saling berkomunikasi[3]. Gambar 6 menunjukkan penambahan *header* untuk VLAN.

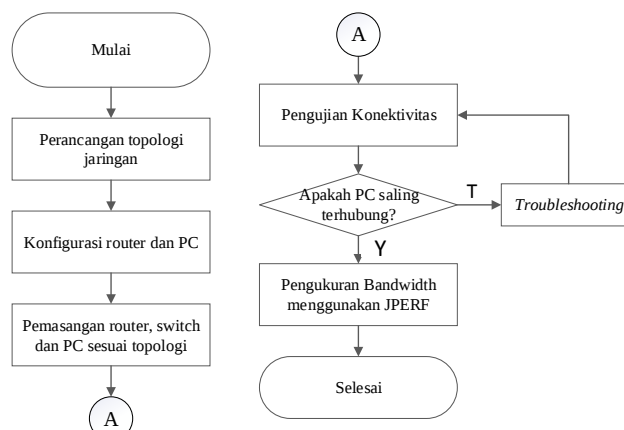


■ Gambar 6 Penambahan *header* untuk *Virtual Local Area Network* (VLAN) [9]

VLAN dibagi menjadi 3 metode dalam penggunaannya, yaitu menggunakan *port*, *MAC address*, dan *IP address*. Semua informasi yang mengandung penandaan/pengalamatan suatu VLAN (*tagging*) disimpan pada suatu *database*. Jika VLAN yang akan digunakan menggunakan metode *port*, maka VLAN akan mengindikasikan semua *port* yang digunakan ke dalam *database*. Switch atau *bridge* bertugas untuk bertanggung jawab menyimpan semua informasi *port* dalam *database* dan konfigurasi. [2]

KONSEP PERANCANGAN

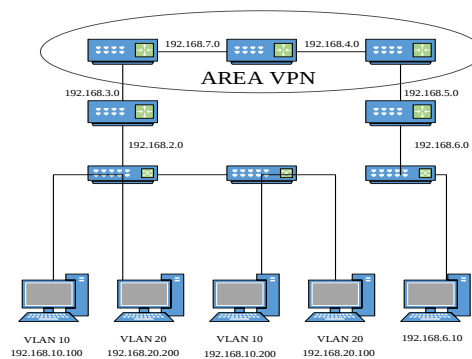
Berikut adalah konsep perancangan berupa bagan alir perancangan simulasi MPLS VPN dengan VLAN pada Gambar 7



■ Gambar 7 Bagan Alir Perancangan.

PERANCANGAN JARINGAN SIMULASI

Perancangan simulasi jaringan *Multi Protocol Label Switching Virtual Private Network* (MPLS VPN) dengan *Virtual Local Area Network* (VLAN) akan dibagi 2 bagian yaitu area VPN dan VLAN. MPLS dan BGP akan dilakukan pada router *provider* dan router *provider edge*. Pada simulasi ini akan disimulasikan pada satu perusahaan A yang memiliki dua divisi yaitu VLAN. Topologi jaringan MPLS VPN dengan VLAN dapat dilihat pada Gambar 8.



■ Gambar 8 Topologi jaringan MPLS VPN dengan VLAN.

Pengaturan alamat IP address pada masing-masing router dan PC dapat dilihat pada Tabel 1 dan Tabel 2.

■ Tabel 1 Alamat IP masing-masing router

Router	Ethernet 1	Ethernet 2	Ethernet 3	Loopback
CE1	192.168.2.6/24	192.168.3.5/24	-	-
PE 1	192.168.3.4/24	192.168.7.7/24	-	192.168.10.5
P	192.168.7.8/24	192.168.4.8/24	-	192.168.10.6
PE2	192.168.4.7/24	192.168.5.6/24	-	192.168.10.7
CE2	192.168.5.5/24	-	192.168.6.15	-

■ Tabel 2 Alamat IP masing-masing PC

VLAN	PC	IP Address	Subnet Mask	Default Gateway
10	PC 1	192.168.10.100	255.255.255.0	192.168.10.1
	PC 2	192.168.20.200	255.255.255.0	192.168.20.1
20	PC 3	192.168.10.200	255.255.255.0	192.168.10.1
	PC 4	192.168.20.100	255.255.255.0	192.168.20.1
-	PC 5	192.168.6.10	255.255.255.0	192.168.6.15

Pemberian alamat IP address pada setiap router menggunakan Winbox. Contoh pemberian alamat pada router CE1.

PENGUJIAN KONEKTIVITAS

Pada saat ditambahkan router CE yang lain pada router PE1 dan diuji konektivitasnya, tidak dapat saling terhubung, hal ini disebabkan karena pada router PE1 sudah dibatasi user mana yang dapat masuk ke dalam daerah VPN. Pengujian antar VLAN 10 dan VLAN 10 dengan CE2 berhasil terhubung terbukti menghasilkan 0% loss, sehingga antar VLAN 10 dengan CE2 dapat saling bertukar data. Berikutnya adalah pengujian konektivitas antar VLAN 20 dan VLAN 20 dengan CE2, pada pengujian ini juga menghasilkan 0% loss, sehingga antar VLAN 20 dengan CE2 dapat saling bertukar data. Pengujian konektivitas antar VLAN juga saling terhubung karena adanya tag 802.1Q. Hasil pengujian konektivitas VLAN dapat dilihat pada Tabel 3.

■ Tabel 3 Pengujian konektivitas

VLAN	Alamat IP asal	Alamat IP tujuan	Keterangan
10	192.168.10.100	192.168.6.10	berhasil
		192.168.10.200	berhasil
		192.168.20.200	berhasil
		192.168.20.100	berhasil
	192.168.10.200	192.168.6.10	berhasil
		192.168.10.100	berhasil
		192.168.20.200	berhasil
		192.168.20.100	berhasil
20	192.168.20.200	192.168.6.10	berhasil
		192.168.10.100	berhasil
		192.168.10.200	berhasil
		192.168.20.100	berhasil
	192.168.20.100	192.168.6.10	berhasil
		192.168.10.100	berhasil
		192.168.10.200	berhasil
		192.168.20.200	berhasil

PENGUJIAN ROUTING TABLE

Pengujian ini menunjukkan informasi yang berisi IP *address* tujuan. Tabel ini berfungsi agar *router* dapat menentukan jalur mana yang tercepat untuk mengirimkan data dan bekerja secara dinamik dengan selalu memperbarui tabel *routing* sehingga jika terjadi suatu kerusakan disalah satu jalur dapat tetap mengirimkan data melalui jalur lain tanpa harus merubah topologi dan konfigurasi. Gambar 9, 10 dan 11 adalah hasil simulasi dari *router* PE dan P.

	Dst. Address	Gateway	Distance	Routing Mark
DAo	192.168.2.0/24	192.168.3.5 on vrf1 reachable ether1	110	vrf1
DAC	192.168.3.0/24	ether1 reachable	0	vrf1
DAo	192.168.4.0/24	192.168.7.8 reachable ether2	110	
DAb	192.168.5.0/24	192.168.10.7 recursive via 192.168.7.8 ether2	200	vrf1
DAb	192.168.6.0/24	192.168.10.7 recursive via 192.168.7.8 ether2	200	vrf1
DAC	192.168.7.0/24	ether2 reachable	0	
DAo	192.168.10.0/...	192.168.3.5 on vrf1 reachable ether1	110	vrf1
DAC	192.168.10.5	loopback2 reachable	0	
AS	192.168.10.6	192.168.7.8 reachable ether2	1	
Do	192.168.10.6	192.168.7.8 reachable ether2	110	
AS	192.168.10.7	192.168.7.8 reachable ether2	1	
Do	192.168.10.7	192.168.7.8 reachable ether2	110	
DAo	192.168.20.0/...	192.168.3.5 on vrf1 reachable ether1	110	vrf1

■ Gambar 9 Tabel *Routing* pada *router* PE1

	Dst. Address	Gateway	Distance	Routing Mark
DAC	192.168.2.0/24	ether2 reachable	0	
DAC	192.168.3.0/24	ether1 reachable	0	
AS	192.168.10.5	192.168.7.7 reachable ether1	1	
Do	192.168.10.5	192.168.7.7 reachable ether1	110	
DAC	192.168.10.6	loopback3 reachable	0	
AS	192.168.10.7	192.168.4.7 reachable ether2	1	
Do	192.168.10.7	192.168.4.7 reachable ether2	110	

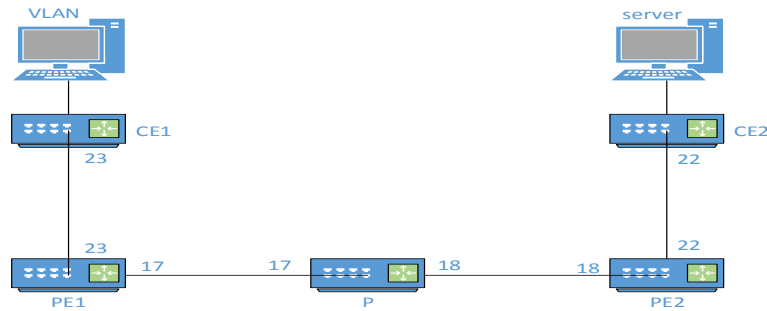
■ Gambar 10 Tabel *Routing* pada *router* P.

	Dst. Address	Gateway	Distance	Routing Mark
DAb	192.168.2.0/24	192.168.10.5 recursive via 192.168.4.8 ether1	200	vrf1
DAb	192.168.3.0/24	192.168.10.5 recursive via 192.168.4.8 ether1	200	vrf1
DAC	192.168.4.0/24	ether1 reachable	0	
DAC	192.168.5.0/24	ether2 reachable	0	vrf1
DAo	192.168.6.0/24	192.168.5.5 on vrf1 reachable ether2	110	vrf1
DAo	192.168.7.0/24	192.168.4.8 reachable ether1	110	
AS	192.168.10.5	192.168.4.8 reachable ether1	1	
Do	192.168.10.5	192.168.4.8 reachable ether1	110	
AS	192.168.10.6	192.168.4.8 reachable ether1	1	
Do	192.168.10.6	192.168.4.8 reachable ether1	110	
DAC	192.168.10.7	loopback4 reachable	0	

■ Gambar 11 Tabel *Routing* pada *router* PE2.

PENGUJIAN LABEL MPLS

Proses pelabelan MPLS pada Gambar 12 menunjukkan pengiriman paket dari salah satu VLAN ke *server*. Pada paket yang diteruskan, *router* akan menyisipkan label pada *interface* yang masuk maupun yang keluar dari *router*. Saat paket masuk ke CE1, paket disisipkan dengan label 23 menuju PE1. Setelah paket sampai di *router* PE1, label 23 dilepaskan dan diganti dengan label baru yaitu label 17. Setelah diganti, label akan menuju ke *router* P. Pada *router* P, label 17 akan diganti menjadi label 18 dan menuju ke *router* PE2. Pada saat sampai di *router* PE2, label 18 akan diganti menjadi label 22 dan menuju *router* CE2. Pada saat sampai di *router* CE2 label 22 akan dilepaskan dan paket diteruskan dan menuju ke *server*. Proses pelabelan dapat dilihat pada Tabel 4.



■ Gambar 12 Pelabelan MPLS

■ Tabel 4 Proses pelabelan MPLS

Router	In label	Out label	Action
CE1	Ether 1, -	Ether 2, 23	Push
PE1	Ether 1, 23	Ether 2, 17	Swap
P	Ether 1, 17	Ether 2, 18	Swap
PE2	Ether 1, 18	Ether 2, 22	Swap
CE2	Ether 1, 22	Ether 2, -	Pop

Pelabelan yang dilakukan MPLS diberikan kepada *customer edge* yang ingin mengirimkan paket melalui *provider edge*. Gambar 13, 14 dan 15 adalah hasil pelabelan MPLS pada router PE dan P

MPLS							
LDP Interface		LDP Neighbor	Accept Filter	Advertise Filter	Forwarding Table	MPLS Interface	Local Bindings
In Label	Out Labels	Interface	Nexthop	Destination	Bytes	Packets	
expl-null					0	0	
17	16	ether2	192.168.7.8	192.168.10.6	0	0	
18		ether2	192.168.7.8	192.168.10.7	0	0	
19		ether2	192.168.7.8	192.168.4.0/24	0	0	
23				192.168.3.0/24@main	0	0	
27				192.168.2.0/24@main	0	0	
28				192.168.20.0/24@main	0	0	
29				192.168.10.0/24@main	0	0	

■ Gambar 13 Label MPLS pada router PE1.

MPLS							
LDP Interface		LDP Neighbor	Accept Filter	Advertise Filter	Forwarding Table	MPLS Interface	Local Bindings
In Label	Out Labels	Interface	Nexthop	Destination	Bytes	Packets	
expl-null					0	0	
17		ether2	192.168.4.7	192.168.10.7	0	0	
18		ether1	192.168.7.7	192.168.10.5	0	0	

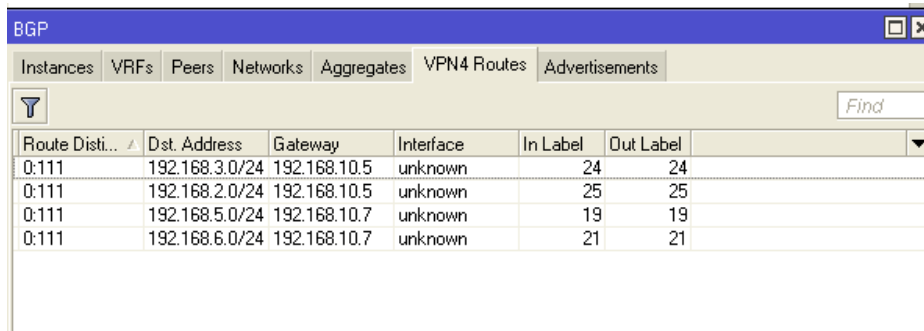
■ Gambar 14 Label MPLS pada router P.

MPLS							
LDP Neighbor		Accept Filter	Advertise Filter	Forwarding Table	MPLS Interface	Local Bindings	Remote Bindings
In Label	Out Labels	Interface	Nexthop	Destination	Bytes	Packets	
expl-null					0	0	
17	18	ether1	192.168.4.8	192.168.10.5	0	0	
18		ether1	192.168.4.8	192.168.10.6	0	0	
20		ether1	192.168.4.8	192.168.7.0/24	0	0	
22				192.168.5.0/24@main	0	0	

■ Gambar 15 Label MPLS pada router PE2.

PENGUJIAN BGP

BGP akan memberikan alamat *prefix* pada *customer edge* agar *customer edge* dapat masuk dan dapat terhubung dengan *provider edge*. Gambar 16 adalah hasil pengujian pada router P.

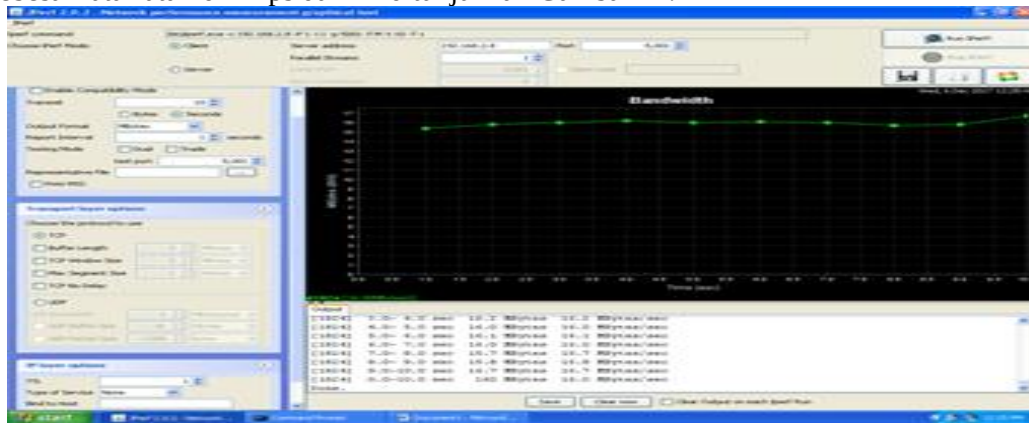


Route Dist...	Dst. Address	Gateway	Interface	In Label	Out Label
0:111	192.168.3.0/24	192.168.10.5	unknown	24	24
0:111	192.168.2.0/24	192.168.10.5	unknown	25	25
0:111	192.168.5.0/24	192.168.10.7	unknown	19	19
0:111	192.168.6.0/24	192.168.10.7	unknown	21	21

■ Gambar 16. Pelabelan VPN4 pada router P

PENGUJIAN MPLS TANPA VLAN

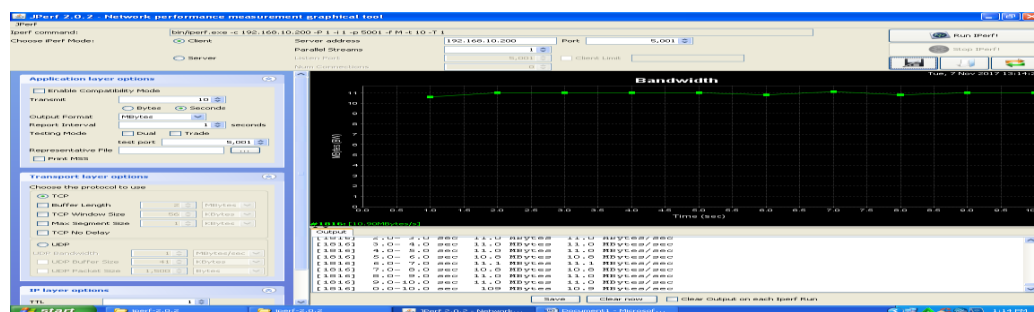
Pada pengujian CE1 tidak menjadi VLAN dan sebagai *client* dengan CE2 sebagai *server* menghasilkan *bandwidth* sebesar rata-rata 16 MBps dan ini ditunjukkan Gambar 17.



■ Gambar 17 Pengujian MPLS tanpa VLAN antara CE2 dengan CE1

PENGUJIAN MPLS DENGAN VLAN

Pada pengujian VLAN 20 sebagai *client* dengan CE2 sebagai *server* menghasilkan *bandwidth* sebesar rata-rata 11 MBps seperti yang diperlihatkan Gambar 18.



■ Gambar 18 Pengujian MPLS dengan VLAN antara CE2 dengan VLAN 10 (PC2) .

KESIMPULAN

1. Jaringan MPLS VPN dengan VLAN aman karena terdapat jaringan VPN yang hanya dapat terhubung dengan *customer edge* tertentu dan jaringan VLAN aman karena dapat memilih VLAN mana yang akan menerima data tanpa perlu mengirim secara *broadcast*.
2. Pengukuran *bandwidth* MPLS menggunakan VLAN lebih kecil daripada dengan MPLS tanpa menggunakan VLAN, hal ini karena pada saat menggunakan VLAN *bandwidth* yang digunakan akan terbagi sesuai dengan kebutuhan setiap PC, sedangkan pada saat tanpa VLAN *bandwidth* yang digunakan tidak terbagi dan mengirim data secara *broadcast*.
3. Hasil simulasi menunjukkan VLAN yang berada pada beda VLAN dapat saling berkomunikasi karena adanya *tag 802.1Q* dan terhubung dengan *router*

DAFTAR PUSTAKA

- [1] Allour. 2011. *Multi Protocol Label Switching (MPLS)*, (online) (<https://aloriadi.wordpress.com/2011/12/02/multyprotocol-label-switching-mpls/>), diakses, 30 November 2017)
- [2] David. 2016. *Multi Protocol Label Switching – Traffic Engineering menggunakan Router Mikrotik*. Skripsi. Jakarta: Program Sarjana Universitas Katolik Indonesia Atma Jaya.
- [3] Kun, A. 2009. *Konsep VLAN*, (online) (<https://pekoktenan.wordpress.com/2009/03/23/konsep-vlan/comment-page-2/>), diakses 29 November 2017)
- [4] Musajid, A. 2015. *Jaringan Virtual Mikrotik, Cisco, dan Juniper dengan GNS3*. Jakarta: Jasakom.
- [5] Rahman, M. 2013. *VRF (VPN Routing Forwarding) Configuration*, (online) (<https://belajarcomputernetwork.com/2013/10/07/vrf-virtual-routing-forwarding-configuration/>), diakses 29 November 2017)
- [6] Ridwan. 2011. *Virtual Routing and Forwarding (VRF)*, (online) (<https://ridwannm.wordpress.com/2011/02/12/virtual-routing-and-forwarding-vrf/>), diakses 29 November 2017)
- [7] Sofana, I. 2012. *CISCO CCNP dan Jaringan Komputer Materi Route, Switch, Troubleshooting*. Bandung: Informatika Bandung.
- [8] Triana, J. 2016. *Simulasi Multi Protocol Label Switching Virtual Private Network (MPLS VPN) dengan Router Mikrotik*. Skripsi. Jakarta: Program Sarjana Universitas Katolik Indonesia Atma Jaya.
- [9] Wiki. Tanpa Tahun. *Manual:Interface/VLAN*, (online) (<https://wiki.mikrotik.com/wiki/Manual:Interface/VLAN>), diakses 1 Desember 2017).
- [10] Wiki. Tanpa Tahun. *SwOS*, (online) (<https://wiki.mikrotik.com/wiki/SwOS>), diakses 4 Desember 2017)