Sinusoida Vol: XXVI No.2, Desember 2024
p-ISSN 1411-4593, e-ISSN 2722-0222

Perancangan Jaringan VPN Dalam MPLS IP Antar Perusahaan Menggunakan Virtual Routing Forwarding Pada Router

Irmayani, Taufan Septiyanto, Fivit Marwita
Program Studi Teknik Elektro, Fakultas Teknik,
Institut Sains dan Teknologi Nasional, Jakarta 12640
E_mail: ir.irmayani@gmail.com

ABSTRAK

Jaringan *Virtual Private Network* (VPN) dalam *Multi Protocol Label Switching* (MPLS) adalah suatu bentuk komunikasi data yang menggunakan jaringan publik untuk menghubungkan dua atau lebih cabang komputer, pelanggan, secara tertutup yang dipisahkan oleh jarak. Dalam hal ini menggunakan perangkat keras *(router)* sebagai media koneksi penghubung komunikasi data tersebut. Pada tulisan ini akan dilakukan analisis model pembentukan suatu sistem jaringan VPN dalam MPLS. Perancangan dilakukan pada dua pelanggan yaitu Departemen Perhubungan (DepHub) dan Perusahaan Gas Negara (Gas). Komunikasi ini dipisahkan oleh *Virtual Routing Forwording* (VRF) dengan ditandai terbentuknya *Cloud* untuk masing-masing pelanggan sehingga terjadi pemisahan trafik yang aman untuk melakukan komunikasi data. Tahapan ini menunjukan terbentuknya sebuah VPN dalam MPLS menggunakan VRF yang akan memisahkan jalur masing-masing pelanggan dan protokol yang digunakan adalah *Open Shortest Path First* (OSPF) dan *Border Gateway Protocol* (BGP). Dalam konfigurasi jaringan VPN/MPLS ini dihasilkan model/topologi komunikasi yang terbentuk oleh Provider. Hasil yang diperoleh pada router PE1 sebagai provider menunjukkan trafik komunikasi yang ada di PE1 (Jakarta) menuju ke PE2 (Medan), atau sebaliknya dengan hasil 100 %. Nilai latancy 156 ms, average 202 ms dan maximum 248 ms untuk Customer Departemen Perhubungan. Sedangkan nilai latancy 196 ms, average 232 ms dan max 280 ms untuk Customer Perusahaan Gas Negara.

Kata Kunci: VPN, MPLS, VRF, OSPF, BGP

ABSTRACT

On network *Virtual Private Network* (VPN) in *Multi Protocol Label Switching* (MPLS) is a form of data communication using the public network to connect two or more branches of the computer, the customer, are covered that are separated by distance. In this case use the hardware (*router*) as a medium of communication connecting connection data. In this paper will be the establishment of a system analysis of the model in the MPLS VPN network. The design in done in two customers, the Departement of Transportation (Dephub) and National Gas Company (Gas). This communication Forwording separated by *Virtual Routing Forwording* (VRF) with Cloud formation is marked for each customer so that there is a separation of traffic safety to perform data communication. This stage shows the formation of an MPLS VPN using VRF that will separate the traffic of each customer (Dephub dan Gas) and the protocol used is the *Open Shortest Path First* (OSPF) and *Border Gateway Protocol* (BGP).

In the configuration of the MPLS VPN network is generated model/communication topology formed by Provider. The results obtained from the PE1 router as the provider show the communication traffic from PE1 (Jakarta) to PE2 (Medan), or vice versa, with 100% results. The latency value is 156 ms, average 202 ms, and maximum 248 ms for the Ministry of Transportation's customer. Meanwhile, the latency value is 196 ms, average 232 ms, and maximum 280 ms for the Perusahaan Gas Negara customer.

Keywords: VPN, MPLS, VRF, OSPF, BGP

1. PENDAHULUAN

Perkembangan koneksi jaringan komputer sangat pesat dan memberikan pengaruh yang cukup besar, terutama di tingkat perusahaan (corporate) yang sangat membutuhkan koneksi jaringan komputer untuk mendukung kelancaran komunikasi data. Kelancaran komunikasi data sangat ditentukan oleh baiknya suatu layanan yang disuguhkan oleh *Internet Service Provider* (ISP) pada saat ini. Kecepatan akses, keamanan, stabilitas, garansi layanan, dan pelayanan penanganan gangguan koneksi merupakan hal utama yang sangat dilirik oleh kalangan perusahaan untuk menentukan ISP yang akan dipilih. Perusahaan yang mempunyai banyak cabang sangat membutuhkan koneksi jaringan *any to any connection*, maka disinilah peranan penting dari *Virtual Private Network* (VPN) di dalam skala besar.

Dalam penelitian sebelumnya yaitu Implementasi Jaringan MPLS VPN (Studi Kasus PT Supra Primatama Nusantara BIZNET) menunjukkan proses traceroute ke router langsung menuju ke tujuan tanpa melalui beberapa router terlebih dahulu. Secara fisik untuk mencapai ke tujuan harus melewati beberapa router namun MPLS VPN langsung ke router tujuan, dengan ini dapat efektif dalam pengiriman data [3].

Untuk mendapatkan komunikasi yang cepat, aman, dan mudah diakses digunakan jaringan MPLS VPN. 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 [4] [5] [6].

Routing protokol OSPF dibagi dua daerah yaitu daerah customer dan provider. VLAN akan dikonfigu rasi melalui switch dan router CE1 agar dapat saling bertukar data ke workgroup dan lebih aman karena tidak dikirimkan secara broadcast [1] [7] [8].

Hasil pengujian pada Simulasi Multi Protocol Label Switching Virtual Private Network (MPLS VPN) Dengan Virtual Local Area Network (VLAN) Menggunakan Router Mikrotik menunjukkan bahwa MPLS VPN dengan VLAN menghasilkan bandwidth lebih kecil dibandingkan MPLS VPN non VLAN [9].

Hasil pengujian untuk faktor keamanan pada Virtual Private Network denga Secure Socket Layer untuk Pengamanan Komunikasi Video Conference, menunjukkan bahwa pengiriman informasi yang dilakukan dengan pengamanan VPN SSL tidak dapat dilihat informasi protocol seperti IP address, user ID, RTP dan SIP karena semua data telah dienkripsi dan dikapsulisasi [2].

Dalam jaringan komputer berbasis IP, Virtual Routing and Forwarding (VRF) adalah teknologi yang digunakan pada suatu router yang memungkinkan beberapa tabel routing instan dapat eksis pada suatu router dan waktu yang sama. Tabel routing instan ini bersifat independen, maka alamat IP yang sama atau yang saling bertumpang tindih dapat digunakan tanpa bertentangan satu sama lain [5].

Pengertian lain dari VRF adalah VPN Routing and Forwarding, merupakan elemen kunci dalam teknologi MPLS Cisco VPN. VRF adalah tabel routing instan yang dapat eksis dalam satu atau beberapa tabel routing disetiap service VPN pada router Provider Edge (PE).

VRF dapat diimplementasikan pada perangkat jaringan dengan tabel routing yang berbeda. Hal ini dikenal sebagai forwarding information basis (FIB), atau suatu perangkat jaringan memiliki kemampuan untuk mengkonfigurasi router virtual yang berbeda-beda. Dimana masing-masing router virtual tersebut memiliki FIB sendiri yang tidak dapat diakses oleh router virtual lain pada perangkat/router yang sama [1].

Diharapkan dengan penelitian ini, sistem akan dapat mencakup seluruh jaringan agar efisien dan aman. Perangkat yang digunakan untuk melakukan konfigu rasi adalah router Cisco, aplikasi yang dipakai dalam konfigurasi dan pengujian pada sistem jaringan VPN dalam MPLS IP menggunakan VRF di router adalah GNS3. Untuk mengetahui jalur jaringan VPN dalam MPLS IP dari 2 (dua) perusahaan yang berbeda digunakan pengalokasian Protokol VRF yang berbeda.

2. DASAR TEORI

2.1 Multi Protocol Label Switching VPN

Teknologi MPLS sudah banyak diadopsi oleh para *Service Provider* (SP) untuk diimplementasikan dengan VPN untuk menghubungkan antar cabang perusahaan.

VPN pada umumnya digunakan oleh SP untuk menggunakan infrastruktur fisik dalam mengimplemen tasikan *point-to-point link* antar cabang perusahaan. Jaringan pelanggan yang diimplementasi dengan VPN akan terdiri dari kawasan yang jelas di bawah pengawasan pelanggan tersebut dengan *customer sites* yang terhubung satu sama lain melalui jaringan SP [5].

Pada umumnya, VPN terdiri dari 2 wilayah yaitu:

1. Jaringan *Provider*, digunakan oleh SP untuk menawarkan *dedicated point-to-point link* melalui jaringannya. *Router* yang terhubung langsung dengan CE disebut dengan *Provider Edge* (PE) *router*. Selain itu juga terdapat *router* pada jaringan *backbone*-nya yang disebut dengan *Provider* (P) *router,* di sisi ini dikenal implementasi model *overlay* VPN, pada model ini *provider* menghubungkan antar cabang perusahaan dengan menggunakan jaringan pribadi yang *emulated*, *provider* tidak mencampuri proses *routing* di sisi pelanggan. *Provider* hanya bertugas untuk menyediakan layanan data dengan menggunakan *virtual point-to-point link* yang dikenal dengan istilah *Data link layer virtual circuit*.
2. Jaringan *Customer*, terdiri dari *router* pada setiap *site* pelanggan yang disebut dengan *Customer Edge* (CE) *router,* disisi ini dikenal implementasi *peer-to-peer* VPN dan dikembangkan untuk mengatasi kelemahan pada model *overlay* dan mengoptimalkan transportasi data melewati jaringan *backbone* SP. Oleh karena itu, SP juga ikut aktif dalam proses *routing* di sisi pelanggan.

2.2 Arsitektur MPLS VPN

Pada arsitektur MPLS VPN, *provider edge router* membawa informasi *routing* pelanggan dan mengoptimalkan proses *routing* pada pelanggan, sedangkan data diteruskan ke cabang-cabang pemisahan melalui jaringan *backbone* SP yang berbasiskan MPLS. Model MPLS VPN juga mencegah pengalamatan yang tumpang tindih atau o*ver lapping* [6].

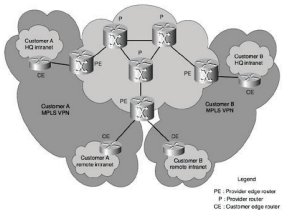
Domain jaringan MPLS VPN, seperti jaringan VPN tradisional terdiri dari jaringan *customer* dan *provider*. Model jaringan MPLS VPN mirip dengan model *peer-to-peer* VPN seperti pada gambar 1. Bagaimanapun juga, *traffic* pelanggan terisolasi pada *router* PE yang sama yang menyediakan konektivitas ke dalam jaringan SP bagi banyak pelanggan [10].

Komponen-komponen utama dalam arsitektur MPLS VPN adalah:

1. Jaringan *customer*, biasanya merupakan wilayah *customer* yang terdiri dari *router* CE.

Sinusoida Vol: XXVI No.2, Desember 2024
p-ISSN 1411-4593, e-ISSN 2722-0222

2. Jaringan *provider,* merupakan wilayah *provider* yang terdiri dari *router* PE dan P. Jaringan ini mengontrol *routing traffic* antar sisi *customer*.
3. *Router* CE, merupakan *router* yang terdapat pada jaringan *customer* yang terhubung langsung dengan jaringan SP.
4. *Router* PE, merupakan *router* yang terdapat pada jaringan *provider* yang terhubung langsung ke *router* CE.
5. *Router* P, merupakan *router* yang terdapat pada jaringan *backbone provider,* yang terhubung baik dengan *router* PE maupun sesama *router* P.



Gambar 1 Model jaringan MPLS

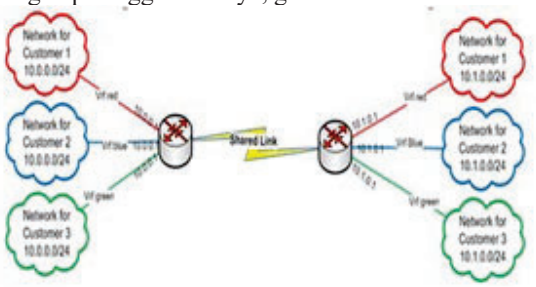
2.3 *Virtual Routing and Forwading* (VRF)

Dalam jaringan komputer berbasis IP, Virtual Routing and Forwarding (VRF) adalah teknologi yang digunakan pada suatu router dimana memungkinkan beberapa tabel routing instan dapat eksis bersamaan pada suatu router yang sama dan pada waktu yang sama pula. Karena tabel routing instan ini bersifat independen, maka alamat IP yang sama atau yang saling bertumpang tindih dapat digunakan tanpa bertentangan satu sama lain [3].

Pengertian lain dari VRF adalah VPN Routing and Forwarding, yang merupakan elemen kunci dalam teknologi MPLS Cisco VPN. Sebuah VRF adalah tabel routing instan yang dapat eksis dalam satu atau beberapa tabel routing pada setiap service VPN pada router Provider Edge (PE). Jumlah dari VRF terbatas oleh jumlah *interface* yang terdapat pada suatu *router* dan sebuah *interface* tunggal hanya bisa diasosiasikan dengan sebuah VRF [11, 15]

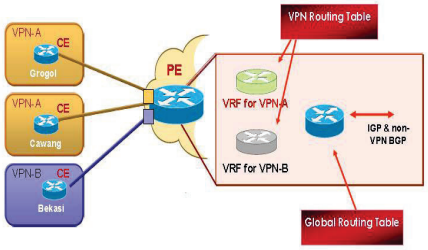
VRF biasanya sering dihubungkan dengan MPLS meskipun sebenarnya VRF bukan merupakan bagian dari MPLS, dimana di Cisco pengimplementasian VRF tanpa MPLS dikenal dengan nama VRF lite. Sedangkan saat digunakan dalam keperluan besar VRF lite tidak dapat digunakan, karena antara lain tiap instance VRF harus ada di tiap perangkat, perlu dilakukan encapsulasi (trunk di VLAN) untuk instance VRF tersebut.

Dalam jaringan data center penggunaan VRF memungkinkan adanya beberapa segmen server dengan IP network yang sama terkoneksi di satu router, sedangkan pada ISP VRF memungkinkan adanya 2 atau lebih pelanggan dengan IP network yang sama terkoneksi dalam satu router dan koneksi antar site yang diperlukan oleh satu pelanggan dapat dipisahkan dengan pelanggan lainnya, gambar 2.



Gambar 2 Topologi jaringan VRF

Pada Jaringan VPN dalam MPLS IP diperlukan VRF yang terpisah pada setiap PE, dengan menyediakan isolasi VPN dan mengizinkan overlap private ip address. VRF diasosiasikan dengan innterface / sub interface yang terhubung ke CE. PE mengelola forwading table untuk setiap site VPN. Route dalam VRF akan di distribusikan ke site yang lain, biasanya terhubung ke PE lain dari VPN yang sama seperti yang ditunjukkan pada gambar 3.



Gambar 3 Distribusi Route VRF

2.4 *Route Distinguisher* (RD) dan *Route Target* (RT)

Route Distringuisher (RD) berfungsi untuk memungkinkan memindahkan data antar kedua sisi *customer* melewati jaringan *backbone* SP. *Format* RD adalah 64-*bit unique identifier* yang digabungkan dengan 32-*bit prefix* atau rute yang diperoleh dari *router* CE, yang membentuk 96-*bit address* yang bisa dibawa melewati *router* PE pada *domain* MPLS. Oleh karena itu, sebuah RD yang unik dikonfigurasi untuk setiap VRF pada *router* PE. Pengalamatan yang dibentuk oleh 96-*bit* tersebut disebut dengan VPN *version* 4 (VPNv4) *address*.

Pengalamatan VPNv4 ditukarkan di antara *router* PE pada jaringan SP digabung dengan pengalamatan IPv4. Jika SP tidak memiliki nomor AS BGP, format pengalamatan IPv4 bisa digunakan dan jika jaringan SP memiliki nomor AS, format dari nomor AS bisa digunakan [14].

Route Targets (RT) merupakan pengenal tambahan yang digunakan pada *domain* MPLS VPN yang mengidentifikasikan keanggotan VPN dari rute-rute yang dipelajari pada sisi tersebut. RT

Sinusoida Vol: XXVI No.2, Desember 2024
p-ISSN 1411-4593, e-ISSN 2722-0222

diimplementasikan dengan cara meng-*encoding* 16-*bit* urutan teratas dari BGP *extended community* (total 64-*bit*) dengan sebuah nilai yang berhubungan dengan keanggotaan VPN pada sisi tertentu. Ketika sebuah rute VPN yang dipelajari dari sebuah *router* CE disuntikkan ke BGP VPNv4, sebuah daftar atribut-atribut *route* target *extended community* diasosiasikan dengannya. *Export route target* digunakan sebagai identifikasi dari keanggotaan VPN dan diasosiasikan ke setiap VRF. *Import route target* diasosiasikan dengan setiap VRF dan mengidentifikasi rute-rute VPNv4 yang akan diimpor ke VRF untuk *customer* tertentu. Format dari RT mirip dengan format RD. Interaksi antara nilai-nilai RT dan RD pada *domain* MPLS VPN sebagai *update* diterjemahkan sebagai sebuah *update* MP-BGP [15].

2.5 *Multi-Protocol* BGP (MP-BGP)

Protokol yang digunakan untuk menukar rute-rute VPNv4 adalah *Multiprotocol* BGP (MP-BGP). *Router* PE harus menjalankan protokol *routing* IGP untuk bertukar data sesama *router* PE, yang ada pada saat ini Cisco mendukung OSPFv2 dan IS-IS pada jaringan MPLS, MP-BGP juga bertugas untuk memberi *label* VPN, serta memungkinkan penggunaan pengalamatan VPNv4 pada lingkungan *router* MPLS VPN yang memungkinkan beberapa *customer* untuk memiliki IP address yang sama didalam satu PE.

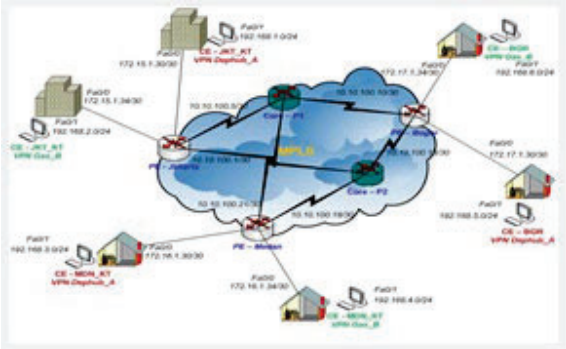
2.6 *Address Family* (AF)

Sebuah *Address Family* (AF) adalah sebuah protokol *Network Layer*. Sebuah *Address Family Identifier* (AFI) membawa sebuah identitas dari protokol *Network Layer* yang berhubungan dengan pengalamatan jaringan atribut-atribut *Multiprotocol* di BGP.

3. PERANCANGAN DAN IMPLEMENTASI

3.1 Topologi Jaringan VPN dalam MPLS IP

Dalam merancang sebuah jaringan VPN dalam MPLS IP menggunakan aplikasi GNS 3 dimana router cisco 7200 series sebagai router P (Core) dan PE, sedangkan untuk CE mengunakan cisco 3600 series. Untuk topologi konfigurasi yang akan dibuat dalam pembentukan jaringan VPN dalam MPLS IP dengan memanfaatkan VRF pada router terdapat 2 perusahaan sebagai pelanggan dari provider yaitu Dephub dan Gas. Dimana kedua perusahaan tersebut memiliki pusat cabang yaitu Jakarta dan 2 cabang Medan serta Bogor. VRF yang dipakai oleh kedua perusahaan tersebut berbeda, sebagai bukti pemisahan trafik pada jaringan VPN perusahaan dalam MPLS IP. Provider sebagai pengatur trafik koneksi antara pusat dengan cabang meneruskan komunikasi yang diinginkan customer dengan memanfaatkan router Core dan PE, ditunjukkan pada gambar 4.

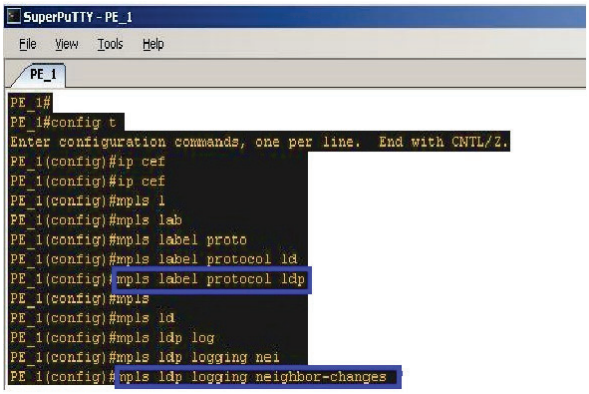


Gambar 4 Topologi Jaringan VPN-MPLS

3.2 Konfigurasi Domain MPLS Provider

Untuk melakukan konfigurasi MPLS, semua router provider dalam hal ini, P1, P2, PE1. PE2 mengunakan interface loopback0 sebagai indentitas untuk labeling distribusi protokol.

Pada gambar 5, menunjukkan *Label Distribution Protokol (LDP)*, melakukan update terhadap router Provider membentuk sebuah MPLS. Pada masing masing router Provider akan menerima update, yang berisi informasi interface loopback pada masing-masing router yang sudah menerima update dari domain MPSL. Bila router belum menerima update informasi, cek kembali routingan OSPF dan cek konfigurasi interface loopbacknya. Pastikan di interface loopback masking yang digunakan 255.255.255.255. Sesudah domain MPLS dan update routing sudah diterima masing-masing router, jalur khusus untuk setiap VPN yang menggunakan jasa provider telah terbentuk.



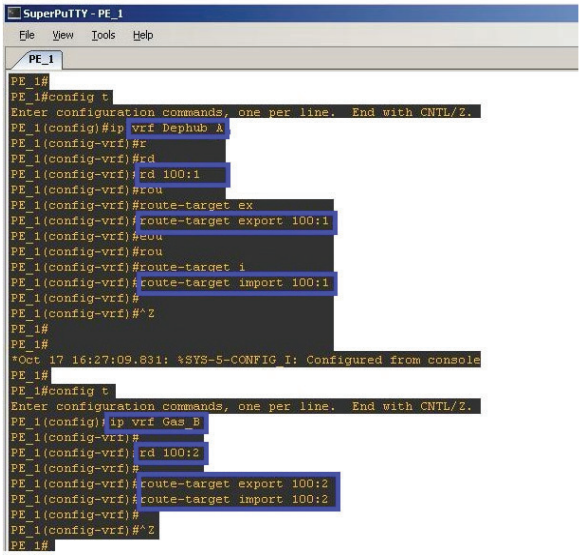
Gambar 5 Hasil konfigurasi domain MPLS

3.3 Konfigurasi VPN VRF

Dalam VPN MPLS mengunakan layer 3 untuk mendistribusikan paket ke VPN dalam jaringan MPLS. Untuk mengetahui paket dari dan ke tujuan VPN, maka jaringan MPLS memberi label distribusi setiap paket yang akan di kirim atau di terima masing-masing VPN. Pemberian label itu disebut *Virtual Routing Forwarding* atau VRF. Setiap label memiliki keunikan tertentu.

Sinusoida Vol: XXVI No.2, Desember 2024
p-ISSN 1411-4593, e-ISSN 2722-0222

Pemberian label memungkinkan paket akan sampai ke alamat tujuan tanpa mengalami kegagalan routing di provider (PE). Untuk memberikan label atau virtual routing forwarding pada masing-masing pelanggan, harus mengetahui alokasi interface di PE yang terhubung langsung (directly connected) ke router pelanggan sebelum melakukan konfigurasi di interface PE, diharuskan membuat *Route Distinguiser* (RD) dan *Target Route* masing masing VPN. Untuk menentukan hal itu, digunakan *astonomous system 100* dan untuk RD memakai nilai 1 dan 2 untuk masing-masing VPN karena hanya 2 VPN yang dibangun dalam konfigurasinya pada masing-masing PE.



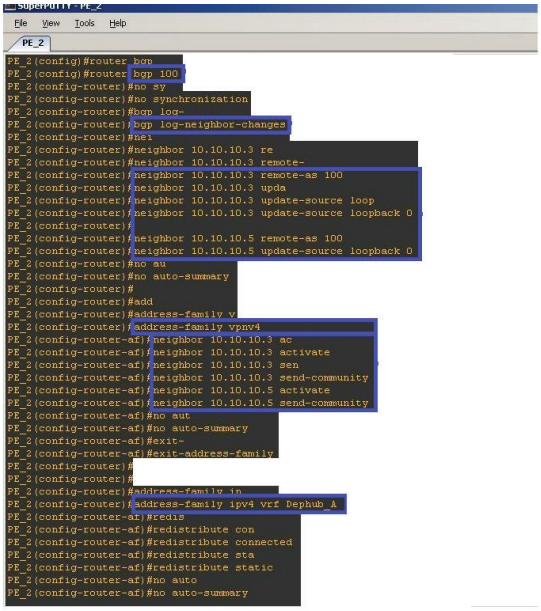
Gambar 6 Konfigurasi VRF pada PE

Pada gambar 6, menunjukkan perintah export di PE1, artinya semua routing table (atau disebut routing prefix) di router virtual vrf VPN_DEPHUB**,** jika diadvertise ke PE1, maka akan diberi tanda dengan RD (route distinghuser) 100:1. Routing prefix tersebut setelah sampai di PE2 dan PE3, akan digunakan. Tapi untuk dapat menggunakannya PE2 dan PE3 harus meng-import dulu route dengan RD 100:1 tsb. Routing untuk Customer A ditandai dengan rd 100:1 (Dephub_A), sedangkan routing untuk customer B, menggunakan rd 100:2 (untuk Gas_B). Nama Dephub_A dan Gas_B berlaku/dikenal secara local di router itu saja. Yang dipertukarkan adalah rd 100:1 dan 100:2. Nomer rd ini yang akan dipertukarkan antar PE. Setelah konfigurasi, lanjutkan konfigurasi dimasing-masing interface PE yang terhubung langsung ke interface pelanggan. Penamaan vrf berdasarkan nama pelanggan atau dengan kode tertentu dan nama vrf pelanggan satu dengan yang lainnya berbeda. Setelah melakukan konfigurasi pada masing-masing PE, kemudian melakukan ping ke IP interface palanggan. Dari router PE lakukan dengan perintah ***ping vrf Dephub_A ip*** ke interface pelanggan. Koneksi dari pelanggan ke provider (PE) sudah terbentuk untuk setiap masing-masing PE. Untuk menghubungkan VPN pelanggan dengan end pointnya, maka diperlukan routing BGP yang fungsinya membuat routing exterior dan interion pada router PE

3.4 Pengaktifan BGP Routing

Untuk dapat berkomunikasi dengan router yang lain maka diaktifkan routing BGP, dengan cara ini prefik yang dilewatkan dari VPN dapat di lewatkan dari vrf Dephub_A dan Gas_B ke masing-masing PE, yang ditunjukkan pada gambar 7.

Pada routing BGP (Border Gateway Protokol) yang dibuat, kanal trafik dan tabel routing yang di lewatkan pada masing-masing PE dan di terima juga pada vrf VPN pada PE yang lain. AS number 100 yang sebelumnya sudah ada, yaitu subtunnel untuk "melewatkan" routing table vrf Dephub_A dan vrf Gas_B. Untuk mengaktifkan gunakan command neighbor <IP_Address> activate. BGP memanfaatkan fasilitas community pada standar BGP, baik yang standard maupun extended, atau keduanya standard atau extended (both) saling dipertukarkan. Dan juga dapat dilihat apakah ada prefix yang sudah diterima oleh PE1 atau dikirimkan oleh PE1. Selanjutnya konfigurasi persiapan untuk routing prefix pada vrf Dephub_A dan vrf Gas_B. Untuk melakukan pengecekan apakah prefix Dephub_A dan Gas_B sudah di update pada masing-masing router PE, maka perintah yang digunakan adalah *sh bgp neigh.*



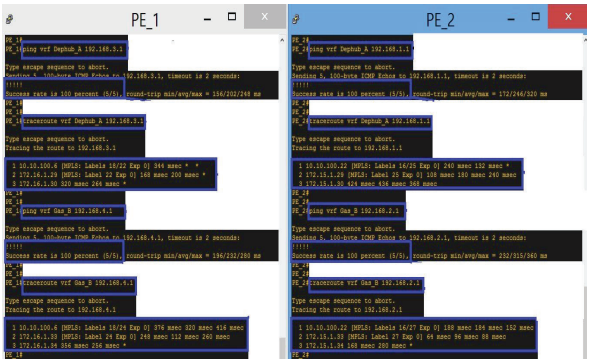
Gambar 7 Konfigurasi protokol BGP

Sinusoida Vol: XXVI No.2, Desember 2024
p-ISSN 1411-4593, e-ISSN 2722-0222

4. HASIL PENGUJIAN dan ANALISA

Hasil pengujian pembentukan VPN dalam MPLS IP, ditunjukkan dengan hasil ping dan trace route ke IP salah satu cabang VPN dengan VRF yang melewati domain MPLS tersebut gambar 8.

1. Koneksi Depatemen Perhubungan (Dephub_A) dan Perusahaan Gas Negara (Gas_B) di PE 1 (Jakarta) ke PE 2 (Medan) pada gambar 8a.
2. Metode VRF dan Update Routing pada Koneksi PE 1 ke PE 2 pada gambar 8b.



Gambar 8 Hasil pengujian pembentukan VPN

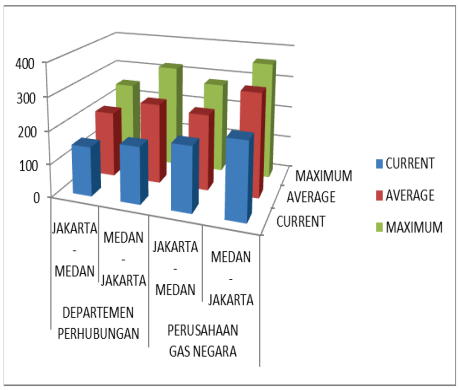
Pada Gambar 8, menunjukan hasil koneksi antar PE1 ke PE2 dalam waktu yang bersama. Pada router PE1 untuk customer Dephub_A melakukan test ping ke router cabang yang berada di PE2 dengan IP 192.168.3.1. Router PE2 untuk customer Dephub_A melakukan test Ping ke router cabang yang berada di PE1 dengan IP 192.168.1.1. Pada router PE1 dan PE2 didapat hasil ping sukses rate 100 percent yang ditandai dengan tanda **“ !!!!! ”** yang dapat diketahui koneksi antara Departemen Perhubungan lokasi Jakarta ke Medan serta sebaliknya dapat terkoneksi. Pada router PE1 dan PE2 untuk customer Dephub_A melakukan traceroute ke router cabang yang berada di PE2 dan begitupun sebaliknya. Pada router PE1 didapatkan hasil trace tersebut melewati jalur koneksi label MPLS pada IP 10.10.100.6 (router Core 1) dan 172.16.1.29 (router PE2) pada jaringan VPN yang dikelola provider. Pada router PE2 didapatkan hasil trace tersebut melewati jalur koneksi label MPLS pada IP 10.10.100.22 (router Core1) dan 172.15.1.29 (router PE2) pada jaringan VPN yang dikelola provider.

Pada router PE1 untuk customer Gas_B melakukan test ping ke router cabang yang berada di PE2 dengan IP 192.168.4.1, dan pada router PE2 untuk customer Gas_B melakukan test Ping ke router cabang yang berada di PE1 dengan IP 192.168.2.1. Pada router PE1 dan PE2 didapat hasil ping sukses rate 100 percent yang ditandai dengan tanda **“!!!!!”** yang dapat diketahui koneksi antara Perusahaan Gas Negara lokasi Jakarta ke Medan serta sebaliknya dapat terkoneksi.

Pada router PE1 dan PE2 untuk customer Gas_B melakukan traceroute ke router cabang yang berada di PE2 dan begitupun sebaliknya. Pada router PE1 didapatkan hasil trace tersebut melewati jalur koneksi label MPLS pada IP 10.10.100.6 (router Core 1) dan 172.16.1.33 (router PE2) pada jaringan VPN yang dikelola provider.

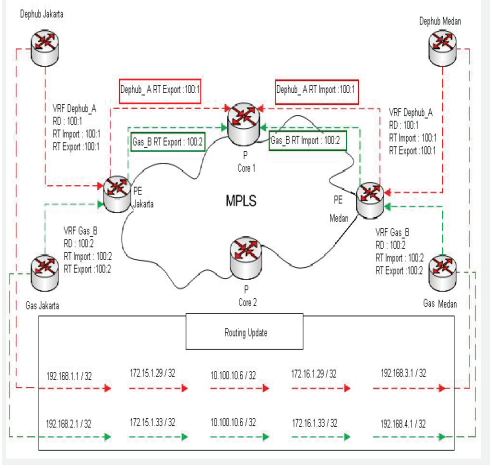
Pada router PE2 didapatkan hasil trace tersebut melewati jalur koneksi label MPLS pada IP 10.10.100.22 (router Core1) dan 172.15.1.33 (router PE2) pada jaringan VPN yang dikelola provider.

Dengan demikian didapat hasil pemisahan jalur koneksi dan pemetaan antar perusahaan antara Departemen Perhubungan dan Perusahaan Gas Negara ke masing–masing cabangnya pada router yang dikelola oleh provider. Sehingga untuk koneksi yang dikirim tidak akan bertukar dan tercampur walau dalam segment IP class yang sama.



Gambar 9 Grafik hasil pengujian latency

Pada Gambar 9, menunjukan grafik hasil latency yang terjadi saat dilakukannya pengujian jalur koneksi untuk Departemen Perhubungan dan Perusahaan Gas Negara dari Jakarta ke Medan serta sebaliknya dalam waktu yang bersama – sama. Hasil tersebut didapat dari ping yang dilakukan di dalam aplikasi GNS3 tersebut.



Gambar 10 update routing pada VRF

Sinusoida Vol: XXVI No.2, Desember 2024
p-ISSN 1411-4593, e-ISSN 2722-0222

Pada Gambar 10, menunjukan cara kerja VRF dan update routing yang terjadi pada koneksi Departemen Perhubungan dan Perusahaan Gas Negara dari PE1 ke PE2. Untuk koneksi Departemen Perhubungan Jakarta ke Medan memiliki VRF name Dephub_A dengan nilai RD dan RT (100:1) pada PE1 dan PE2. Koneksi Departemen Perhubungan dari Jakarta ke Medan melintasi jaringan VPN dalam MPLS IP. Pada router CE Jakarta dengan IP 192.168.1.1/32 dikirim ke VRF Dephub_A yang ada pada PE1 (Jakarta) dengan nilai RD (100:1) menjadi VPNv4 prefix 100:1:192.168.1.1/32. Kemudian update routing di PE1 mengirimkan vpnv4 prefix tersebut ke router P (Core) dengan routingan OSPF dan BGP. Untuk penentuan jalur router P yang akan dituju, routing BGP mengatur update informasi dan routing OSPF memilih jalur router P dengan nilai jalur terbaik dengan penilaian bandwidth, jarak dan kualitas jaringannya. Pada koneksi ini jalur P1 (core 1) yang memiliki nilai latancy current 156 ms, average 202 ms dan maximum 248 ms. Pada router PE1 IP 192.168.1.1/32 di translasikan menjadi IP 172.15.1.29/32 dengan dimasukan nilai RT export 100:1. Nilai vpnv4 prefix 100:1:172.15.1.29/32 di kirim ke router P1. Pada P1 vpnv4 prefix 172.15.1.29/32 di ubah menjadi 10.100.10.6/32. Untuk melanjutkan ke router yang dituju, router P1 menerima update info RT import 100:1 pada IP 172.16.1.29/32 dari PE2. Router P1 meneruskan paket IP tersebut ke router PE2 dengan routingan OSPF dan BGP dengan nilai vpnv4 prefix 100:1:10.100.10.6/32. Pada router PE2 vpnv4 prefix 100:1:10.100.10.6/32 di translasikan ke vpnv4 prefix 100:1:172.16.1.29/32. Saat sampai di PE2 vpnv4 prefix 100:1:172.16.1.29/32 ditranslasikan menjadi 100:1:192.168.3.1/32 setelah menerima update dari router customer Departemen Perhubungan dengan IP 192.168.3.1 dengan nilai RD 100:1, sehingga koneksi bisa berjalan sesuai dengan jalur yang telah di tentukan.

Pada koneksi Perusahaan Gas Negara Jakarta ke Medan memiliki VRF name Dephub_A dengan nilai RD dan RT (100:2) pada PE1 dan PE2. Koneksi Perusahaan Gas Negara dari Jakarta ke Medan melintasi jaringan VPN dalam MPLS IP. Pada router CE Jakarta dengan IP 192.168.2.1/32 dikirim ke VRF Gas_B yang ada pada PE1 diberikan nilai RD (100:2) menjadi vpnv4 prefix 100:2:192.168.2.1/32. Kemudian update routing di PE1 mengirimkan vpnv4 prefix tersebut ke router P dengan routingan OSPF dan BGP. Untuk penentuan jalur router P yang akan dituju, routing BGP mengatur update info dan routing OSPF memilih jalur router P dengan nilai jalur terbaik dengan penilaian bandwidth, jarak dan kualitas jaringannya. Pada koneksi ini jalur P1 yang memiliki nilai latancy current 196 ms, average 232 ms dan maximum 280 ms. Pada router PE1 IP 192.168.2.1/32 di translasikan menjadi IP 172.15.1.33/32 dengan dimasukan nilai RT export 100:2. Nilai vpnv4 prefix 100:2:172.15.1.33/32 di kirim ke router P1. Pada vpnv4 prefix 172.15.1.33/32 di ubah menjadi 10.100.10.6/32. Untuk melanjutkan ke router yang dituju, router P1 menerima update info RT import 100:2 pada IP 172.16.1.33/32 dari PE2. Router P1 meneruskan paket IP tersebut ke router PE2 dengan routingan OSPF dan BGP dengan nilai vpnv4 prefix 100:2:10.100.10.6/32. Pada router PE2 vpnv4 prefix 100:2:10.100.10.6/32 di translasikan ke vpnv4 prefix 100:2:172.16.1.33/32. Saat sampai di PE2 vpnv4 prefix 100:2:172.16.1.33/32 ditranslasikan menjadi 100:2:192.168.4.1/32 setelah menerima update dari router customer Departemen Perhubungan dengan IP 192.168.4.1 dengan nilai RD 100:2, sehingga koneksi bisa berjalan sesuai dengan jalur yang telah di tentukan.

Pada topologi jaringan yang dibuat, menunjukkan bahwa setiap perusahaan bisa terkoneksi ke cabang – cabang yang ada dilokasi tanpa harus tercampur dengan koneksi perusahaan yang ada di cloud VPN dalam MPLS IP. Adanya VRF sebagai pemisah koneksi trafik dan data suatu perusahaan dalam jaringan VPN tersebut. Pada hasil yang didapat provider selaku penyedia jaringan tersebut, membatasi dan mengatur lalulintas yang akan dilakukan oleh setiap perusahaan dari pusat Jakarta ke cabang perusahaan yang ada di Medan dan Bogor. Dalam pengaturan lalulintas tersebut, terdapat *Routing Protocols* dan *Domain MPLS* maka LDP (Label Distribution Protocol) dapat terbentuk sehingga router-router PE yang berada dibawah router-router Core tersebut saling berkomunikasi. Routing BGP dan OSPF sebagai routingan yang ada di jaringan VPN dalam MPLS IP untuk mengatur update routing dan pemilihan jalur terbaik yang akan dilewatkan.

Hasil ping yang diperoleh dari router PE1 sebagai provider menunjukan lalulintas koneksi yang ada di PE1 menuju ke PE2 dengan hasil 100 percent dan nilai latancy current 156 ms, average 202 ms dan maximum 248 ms untuk Customer Departemen Perhubungan. Sedangkan nilai latancy current 196 ms, average 232 ms dan maximum 280 ms untuk Customer Perusahaan Gas Negara. Pada hasil trace terdapat keterangan bahwa jaringan perusahaan tersebut bisa terkoneksi dengan trace route terdapat label MPLS. Dengan adanya hasil tersebut koneksi jaringan antar perusahaan dengan menggunakan VRF tidak tertukar dikarenakan setiap perusahaan memiliki VRF_name yang didalamnya terdapat nilai RD dan RT. Untuk nilai RD 100:1 dan RT 100:1 untuk Departemen Perhubungan, sedangkan untuk nilai RD 100:2 dan RT 100:2 untuk Perusahaan Gas Negara. Sehingga komunikasi jaringan yang terbentuk bisa berjalan sesuai dengan topologi yang telah dibuat.

5. SIMPULAN

Kesimpulan yang dapat diperoleh dari pembahasan adalah sebagai berikut:

1. Hasil yang diperoleh pada router PE1 sebagai provider menunjukan lalulintas koneksi yang ada di PE1 (Jakarta) menuju ke PE2 (Medan) dengan hasil 100 percent dengan nilai latancy 156 ms, average 202 ms dan maximum 248 ms untuk Customer Departemen Perhubungan. Sedangkan nilai latancy 196 ms, average 232 ms dan maximum 280 ms untuk Customer Perusahaan Gas Negara.
2. Pada koneksi VPN, hasil trace tiap-tiap PE dengan VRF_Name masing-masing nilai RD 100:1 dan RT 100:1 untuk Departemen Perhubungan, sedangkan nilai RD 100:2 dan RT 100:2 untuk Perusahaan Gas Negara dapat saling mengenal antar PE Jakarta dengan PE Medan dan PE Bogor.

DAFTAR PUSTAKA

[1] I. J. Pardede and I. Irmayani, "Implementasi Service Distribution Point Pada Jaringan MPLS Static Route Menggunakan Metode LDP Dan LSP," *Sinusoida*, vol. 26, no. 1, pp. 31–39, 2024, [Online]. Available: https://ejournal.istn.ac.id/index.php/sinusoida/article/view/2269

[2] G. Purwoko and I. Irmayani, "Implementasi Secure Socket Layer Pada Virtual Private Network Untuk Pengamanan Komunikasi Video Conference," *Sinusoida*, vol. 22, no. 2, pp. 45–57, 2020, doi: 10.37277/s.v22i2.698.

[3] Budi Sukmawan, 2022, Implementasi Jaringan MPLS VPN (Studi Kasus PT Supra Primatama Nusantara (BIZNET), AL MIKRAJ Jurnal Studi Islam dan Humaniora Vol.3 No.1 (2022) Juli–Desember 2022 hal 126–139. E-ISSN:2745-4584 https://ejournal.insuriponorogo.ac.id DOI: 10.37680/almikraj.v3i1

[4] Alexandrina, Alexandrina dan Ihsan Arief Nurhakim, Muhammad and Novel, Muhammad dan Gunar Setiadji, M.Eng, Tatang, 2013, Perancangan Jaringan Terpusat Menggunakan MPLS VPN dengan Failover Link pada CV. Rofa Food Indonesia. Jakarta: Universitas Bina Nusantara.

[5] Kristanti Novi. 2016. Simulasi Jaringan Multiprotocol Label Switching (MPLS) Menggunakan Graphical Network Simulator (GNS3). Semarang: Universitas Diponegoro.

[6] Nugroho, Kukuh. 2018. Router Cisco Implementasi MPLS VPN. Yogyakarta: Teknosain

[7] Siregar, Nur Fauzia. 2016. Perbandingan Implementasi Routing Protocol Enhanced Interior Gateway Routing Protocol (EIGRP) Dengan Open Shortest Path First (OSPF) Pada Jaringan Backbone USUNETA. Medan: Universitas Sumatera Utara

[8] Sofana, Iwan. 2017. Cisco CCNA - CCNP Routing dan Switching. Bandung: Informatika Bandung.

[9] Bertha Euginia, Theresia Ghozali, 2018, Simulasi Multi Protocol Label Switching Virtual Private Network (MPLS VPN) Dengan Virtual Local Area Network (VLAN) Menggunakan Router Mikrotik, TESLA Vol. 20 NO.2 Oktober hal 109-117

[10] Farel. A & Bruce S. Davie, 2008, MPLS Next Steps, Morgan Kaufmann.

[11] Henda, Wijaya. 2001, Cisco Router, Elek Media. Jakarta.

[12] T. Lamle, 1996, CCNA Cisco Sertified Network Associate Study Guide, Second Edition. Sybex.

[13] B. Chriss, 2000, Mastering Cisco Router, Sybex.

[14] Suryadi, M. T., 2002, TCP/IP dan Internet, Elex Media. Jakarta.

[15] Hendra Wijaya, 2001, Routing Protokol, Elex Media. Jakarta.

[16] Sukaridhoto, Sritrusta, 2016, Jaringan Komputer 1, Surabaya: Politeknik Elektronika Negeri Surabaya.

[17] Sukaridhoto, Sritrusta, 2016, Jaringan Komputer 2, Surabaya: Politeknik Elektronika Negeri Surabaya.