
IMPLEMENTASI JARINGAN MPLS VPN (STUDI KASUS PT SUPRA PRIMATAMA NUSANTARA (BIZNET))

Budi Sukmawan

Teknik Informatika, STMIK Dharma Negara Bandung; Indonesia
correspondence e-mail*, budskman@gmail.com

Submitted:

Revised: 2022/08/14; Accepted: 2022/09/17; Published: 2022/10/20

Abstract

Multiprotocol Label Switching-Virtual Private Network (MPLS VPN) dapat didefinisikan sebagai penggabungan dari teknologi Virtual Private Network (VPN) dengan teknologi Multiprotocol Label Switching (MPLS) dimana teknologi VPN dibangun di atas jaringan yang menggunakan teknologi MPLS. MPLS adalah teknologi penyampaian paket pada jaringan inti atau backbone berkecepatan tinggi. Asas kerjanya menggabungkan beberapa kelebihan dari sistem komunikasi circuit-switched dan packet-switched pada IP yang melahirkan teknologi yang baik dari keduanya. Multiprotocol Label Switching-Virtual Private Network (MPLS-VPN) dapat didefinisikan sebagai penggabungan dari teknologi Virtual Private Network (VPN) dengan teknologi Multiprotocol Label Switching (MPLS) dimana teknologi VPN dibangun di atas jaringan yang menggunakan teknologi MPLS

Keywords

Multiprotocol Label Switching, Virtual Private Network



© 2022 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution 4.0 International (CC BY SA) license, <https://creativecommons.org/licenses/by-sa/4.0/>.

PENDAHULUAN

Seiring berkembangnya zaman, perkembangan teknologi khususnya informasi dan komunikasi akan membantu kemajuan dari suatu perusahaan yang menggunakannya, dengan adanya jaringan komputer penyebaran informasi antara titik satu ke titik lainnya menjadi lebih mudah. Perusahaan yang mempunyai banyak cabang dapat melakukan pertukaran data dan informasi secara cepat dan optimal.¹ Penggunaan teknologi yang tepat akan membuat perusahaan menjadi lebih efisien dan juga fleksibel dalam melakukan pertukaran data dan informasi.

Pembangunan suatu jaringan yang bersifat private yang digunakan untuk menghubungkan antar cabang melalui suatu link berkecepatan tinggi dimana keterbatasan tempat bukan menjadi penghalang untuk dapat saling terhubung. Metode MPLS VPN diharapkan mampu memberikan solusi terhadap masalah ini, karena MPLS VPN memberikan layanan VPN (Virtual Private network) yang melintasi jaringan MPLS. MPLS VPN Memudahkan pembangun untuk mengembangkan jaringannya karena jika ada penambahan, konfigurasi dan pengaturan cukup dilakukan di koneksi fisik antar pengguna dengan perangkat jaringan yang ada di depannya dan tidak akan

¹ Kristanti Novi. 2016. Simulasi Jaringan Multiprotocol Label Switching (MPLS) Menggunakan Graphical Network Simulator (GNS3). Semarang: Universitas Diponegoro.

mempengaruhi pengguna lainnya. Teknologi MPLS VPN juga memberikan keuntungan karena pembangun dimungkinkan membuat tiap jalur penggunaanya berbeda secara Virtual serta dapat melayani banyak Pengguna secara Virtual di router PE (Provider Edge), sehingga tidak perlu membeli satu router PE tambahan.

Layanan Virtual disebut dengan Multi-VRF (Virtual Routing Forwarding) yaitu sebuah layanan atau fitur router untuk melakukan overlap alamat IP pada jaringan yang memungkinkan dua VPN berbeda untuk saling berhubungan meskipun memiliki alamat IP yang sama persis sehingga tidak akan terjadi konflik alamat IP pada jaringan, selain itu dapat dibuat routing table yang Virtual pada router PE. Router yang berhubungan langsung dengan router milik pengguna memiliki beberapa routing table yang berfungsi untuk mengarahkan VPN satu dengan yang lain meskipun alamat IP yang sama pada sisi gateway milik pengguna.

Sisi provider internet, MPLS merupakan solusi yang baik karena fleksibel dan skalabel. Fleksibel karena seluruh pelanggan dapat menggunakan perangkat dan konfigurasi perangkat lunak yang sejenis untuk bermacam-macam jenis layanan premium seperti VoIP, Internet, Intranet, Extranet, dan VPN-dial. Semua layanan dapat diaktifkan hanya dengan perubahan parameter di konfigurasi perangkat lunaknya.

METODE

Tahap awal ini dilakukan analisa kebutuhan, analisa permasalahan yang muncul, analisis keinginan pengguna, dan analisis topologi jaringan yang sudah ada saat ini. Metode yang biasa digunakan pada tahap ini diantaranya: Wawancara, dilakukan dengan pihak terkait melibatkan dari struktur manajemen atas sampai ke tingkat bawah/operator agar mendapatkan data yang konkrit dan lengkap. Kasus di Computer Engineering biasanya melakukan brainstorming dari pihak vendor untuk solusi yang ditawarkan, karena setiap mempunyai karakteristik yang berbeda.

Survey langsung ke lapangan, pada tahap analisis juga biasanya dilakukan survey langsung ke lapangan untuk mendapatkan hasil sesungguhnya dan gambaran seutuhnya sebelum masuk ke tahap desain. Survey biasa dilengkapi dengan alat ukur seperti GPS dan alat lain sesuai kebutuhan untuk mengetahui detail yang dilakukan.

Membaca manual atau blueprint dokumentasi, pada analisis awal ini juga dilakukan dengan mencari informasi dari manual-manual atau blueprint dokumentasi yang mungkin pernah dibuat sebelumnya. Hal itu menjadi keharusan dalam setiap pengembangan suatu sistem dokumentasi menjadi pendukung akhir dari pengembangan tersebut, dalam proyek jaringan dokumentasi menjadi syarat mutlak setelah sistem selesai dibangun.

Menelaah setiap data yang didapat dari data-data sebelumnya, maka perlu dilakukan analisis data tersebut untuk masuk ke tahap berikutnya.

Tahap design ini akan membuat gambar desain topologi jaringan interkoneksi yang akan

dibangun dengan gambar ini diharapkan dapat memberikan gambaran seutuhnya dari kebutuhan yang ada. Desain bisa berupa desain struktur topologi, desain akses data, desain layout perkabelan, dan sebagainya yang akan memberikan gambaran jelas tentang proyek yang akan dibangun. Biasanya hasil dari design berupa: Gambar-gambar topologi (server farm, firewall, datacenter, storages, lastmiles, perkabelan, titik akses dan sebagainya). Gambar-gambar detail estimasi kebutuhan yang ada.

Simulation Prototype

Pekerja jaringan akan membuat prototype dalam bentuk simulasi dengan bantuan tools khusus di bidang network seperti Boson, Packet Tracert, Netsim, dan sebagainya. Hal ini dimaksudkan untuk melihat kinerja awal dari jaringan yang akan dibangun dan sebagai bahan presentasi dan sharing dengan tim lainnya. Namun karena keterbatasan perangkat lunak simulasi ini, banyak para pekerja jaringan yang hanya menggunakan alat bantu tools Visio untuk membangun topologi yang akan didesain.

Implementation

Tahapan ini akan memakan waktu lebih lama dari tahapan sebelumnya. Dalam implementasi pekerja jaringan akan menerapkan semua yang telah direncanakan dan didesain sebelumnya. Implementasi merupakan tahapan yang sangat menentukan dari berhasil atau gagalnya proyek yang akan dibangun dan ditahap inilah team work akan diuji di lapangan untuk menyelesaikan masalah teknis dan non teknis. Masalah-masalah yang sering muncul pada tahapan ini, diantaranya:

- a. Jadwal yang tidak tepat karena faktor-faktor penghambat.
- b. Masalah dana dan perubahan kebijakan.
- c. Team work yang tidak solid.
- d. Peralatan pendukung dari vendor makanya dibutuhkan manajemen proyek dan manajemen resiko untuk meminimalkan sekecil mungkin hambatan-hambatan yang ada.

Implementasi tahapan monitoring merupakan tahapan yang penting, agar jaringan komputer dan komunikasi dapat berjalan sesuai dengan keinginan dan tujuan awal dari user pada tahap awal analisis, maka perlu dilakukan kegiatan monitoring. Monitoring bisa berupa melakukan pengamatan pada: Infrastruktur hardware dengan mengamati kondisi reliability atau kehandalan sistem yang telah dibangun (reliability = performance+availability+security). Memperhatikan jalannya paket data di jaringan (pewaktuan, latency, peektime, troughput).

Metode yang digunakan untuk mengamati kondisi jaringan dan komunikasi secara umum secara terpusat atau tersebar. Pendekatan yang paling sering dilakukan adalah pendekatan Network Management. Pendekatan ini banyak digunakan di jaringan lokal dan tersebar dapat dimonitor secara utuh.

Level manajemen atau pengaturan, salah satu yang menjadi perhatian khusus adalah masalah kebijakan (policy). Kebijakan perlu dibuat untuk membuat atau mengatur agar sistem yang telah dibangun dan berjalan dengan baik dapat berlangsung lama dan unsur reliability terjaga. Policy akan sangat tergantung dengan kebijakan level management dan strategi bisnis perusahaan tersebut. IT sebisa mungkin harus dapat mendukung atau alignment dengan strategi bisnis Perusahaan.

HASIL DAN PEMBAHASAN

Jaringan Komputer

Jaringan komputer adalah hubungan antara dua atau lebih sistem komputer melalui media komunikasi untuk melakukan komunikasi data satu dengan yang lainnya. Manfaat utama dari terbentuknya jaringan komputer adalah:

1. Dapat saling berbagi (sharing) sumber daya peralatan (devices) secara bersama seperti harddisk, printer, modem, dan lain sebagainya. Demikian dengan hal tersebut terjadi peningkatan efisiensi waktu dalam operasi dan biaya pembelian hardware.
2. Dapat saling berbagi (sharing) penggunaan file yang ada pada server atau pada masing-masing workstation.
3. Aplikasi dapat dipakai bersama-sama (multiuser).
4. Akses ke jaringan memakai nama, kata sandi, dan pengaturan hak untuk data-data rahasia, sehingga masing-masing pengguna memiliki otorisasi.
5. Komunikasi antar pemakai melalui email atau LAN Conference.
6. Pengontrolan para pemakai ataupun pemakaian data secara terpusat dan oleh orang-orang tertentu, sehingga meningkatkan keamanan dan dapat melakukan pendelegasian pekerjaan yang sesuai.
7. Mudah dalam melakukan backup data, karena manajemen yang tersentralisasi.
8. Tidak tergantung kepada orang yang menyimpan data (apabila orangnya tidak ada) karena penyimpanan data tersentralisasi.
9. Data yang selalu up to date karena server senantiasa memutakhirkan data begitu ada input (data

entry) diterima.

10. Seorang supervisor/administrator dapat melakukan pengontrolan pemakai berdasarkan waktu akses, tempat akses, kapasitas pemakaian harddisk, mendeteksi pemakai yang tidak berhak, monitor pekerjaan setiap pemakai.²

Multiprotocol Label Switching (MPLS)

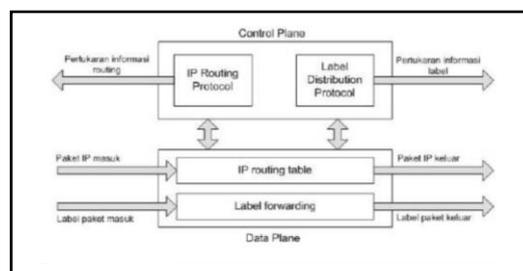
MPLS adalah teknologi arsitektur network dimana paket disampaikan pada jaringan backbone berkecepatan tinggi. Asas kerjanya menggabungkan beberapa kelebihan dari sistem komunikasi circuit-switched dan packet-switched. Sebelumnya, paket diteruskan dengan protokol routing seperti OSPF, S-IS, BGP atau EGP.

Protokol routing berada pada lapisan network dalam system OSI, sedangkan MPLS berada di antara lapisan kedua dan ketiga. Prinsip kerja MPLS ialah menggabungkan kecepatan switching pada data link layer dengan kemampuan routing dan skalabilitas pada layer network. Cara kerjanya adalah dengan menyelipkan label di antara header data link layer dan network layer pada paket yang diteruskan. Label dihasilkan oleh Label-Switching Router dimana bertindak sebagai penghubung jaringan MPLS dengan jaringan luar. Label berisi informasi tujuan node selanjutnya kemana paket harus dikirim. Kemudian paket diteruskan ke node berikutnya, di node ini label paket akan dilepas dan diberi label yang baru yang berisi tujuan berikutnya. Paket-paket diteruskan dalam path yang disebut LSP (Label Switching Path).³ (Sukaridhoto, 2014:27)

Arsitektur MPLS

MPLS node mempunyai dua bidang arsitektural seperti gambar di bawah ini, yaitu MPLS control plane dan MPLS forwarding plane.

Figure 1. Control Plane dan Data Plane



² Kristanti Novi. 2016. Simulasi Jaringan Multiprotocol Label Switching (MPLS) Menggunakan Graphical Network Simulator (GNS3). Semarang: Universitas Diponegoro.

³ Nugroho, Kuku. 2018. Router Cisco Implementasi MPLS VPN. Yogyakarta: Teknosain

Fungsionalitas MPLS dibagi menjadi dua bagian utama blok arsitektur, yaitu:

- a. Control Plane – Bertanggung jawab dalam hal yang berhubungan dengan pengidentifikasian kemampuan untuk mencapai tujuan. Oleh karena itu, control plane terdiri dari semua informasi pada Network layer. Contoh fungsi control plane adalah pertukaran informasi protokol routing, seperti OSPF dan BGP. Selain itu, semua fungsi yang berhubungan dengan pertukaran label antara router tetangga.
- b. Forwarding Plane – Forwarding plane biasa di sebut juga dengan data plane, bertugas untuk meneruskan paket-paket data. paket-paket di sini bisa berarti paket IP network layer atau labeled IP paket. Informasi pada data plane, seperti label value adalah berasal dari control plane. Pertukaran informasi antara router tetangga akan memetakan jaringan tujuan ke label pada control plane, yang akan digunakan untuk meneruskan data plane labeled paket.

Komponen dalam MPLS

Teknologi MPLS terdapat beberapa komponen di dalamnya, yaitu:

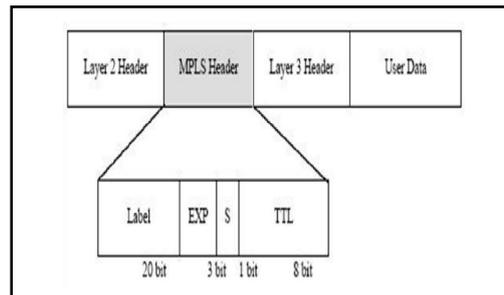
- a. Label Switched Path (LSP): Merupakan jalur yang melalui satu atau serangkaian LSR dimana paket diteruskan oleh label swapping dari satu MPLS node ke MPLS node yang lain.
- b. Label Switching Router (LSR): MPLS node yang mampu meneruskan paket-paket Network layer.
- c. Forwarding Equivalent Class (FEC): Merupakan sekumpulan paket-paket yang akan mendapatkan perlakuan forwarding yang sama (melewati jalur yang sama). MPLS Egress Node: MPLS node yang mengatur trafik saat meninggalkan MPLS domain.
- d. MPLS Ingress Node: MPLS node yang mengatur trafik saat akan memasuki MPLS domain.
- e. MPLS Label: merupakan label yang ditempatkan sebagai MPLS header.
- f. MPLS Node: node yang menjalankan MPLS. MPLS node ini sebagai control protocol yang akan meneruskan paket berdasarkan label.

MPLS Label

MPLS hanya melakukan enkapsulasi paket IP dengan menempelkan header MPLS pada suatu paket. Header MPLS terdiri dari 32-bit data, termasuk 20-bit label, 3-bit eksperimen, 1-bit identifikasi stack, serta 8-bit TTL. Label adalah bagian dari header, memiliki panjang yang bersifat tetap dan merupakan satu-satunya tanda identifikasi paket. Label digunakan untuk proses forwarding.⁴

Figure 2. Format MPLS header packet

⁴ Siregar, Nur Fauzia. 2016. Perbandingan Implementasi Routing Protocol Enhanced Interior Gateway Routing Protocol (EIGRP) Dengan Open Shortest Path First (OSPF) Pada Jaringan Backbone USUNET.A. Medan: Universitas Sumatera Utara



Gambar diatas merupakan gambar format MPLS header paket dengan rincian sebagai berikut. Label Value (LABEL) merupakan field yang terdiri dari 20-bit yang merupakan nilai dari label tersebut. Experimental Use (EXP) secara teknis field ini digunakan untuk keperluan eksperimen. Field ini dapat digunakan untuk menunjukkan prioritas data pada FEC yang telah diberi label. Bottom of Stack (STACK) Pada sebuah paket terdapat kemungkinan untuk menggunakan lebih dari satu label. Field ini digunakan untuk mengetahui label stack yang paling bawah. Label yang paling bawah dalam stack memiliki nilai bit 1 sedangkan yang lain diberi nilai bit 0. Hal ini sangat diperlukan pada proses label stacking. Time to Live (TTL) field ini biasanya merupakan hasil salinan dari IP TTL header. Nilai bit TTL akan berkurang 1 setiap paket melewati hop untuk menghindari terjadinya packet storms.

MPLS Virtual Private Network (MPLS VPN)

MPLS VPN merupakan sebuah konsep dalam membangun jaringan private dimana infrastruktur jaringan public-nya menggunakan teknologi MPLS. Biasanya konsep jaringan public yang menggunakan teknologi MPLS adalah jaringan yang digunakan oleh Service Provider (SP).⁵

Teknologi MPLS sudah banyak diadopsi oleh para SP untuk diimplementasikan dengan VPN untuk menghubungkan antar cabang perusahaan, berikut ini akan dijelaskan sedikit pondasi dan menunjukkan bagaimana cara untuk menyediakan layanan VPN ke pelanggan.

Kategori VPN

VPN pada umumnya digunakan oleh SP untuk menggunakan infrastruktur fisik dalam mengimplementasikan 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. Biaya pengimplementasikan tergantung pada jumlah site yang akan dihubungkan dan umumnya, VPN

⁵ 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.

terdiri dari 2 wilayah yaitu: 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.

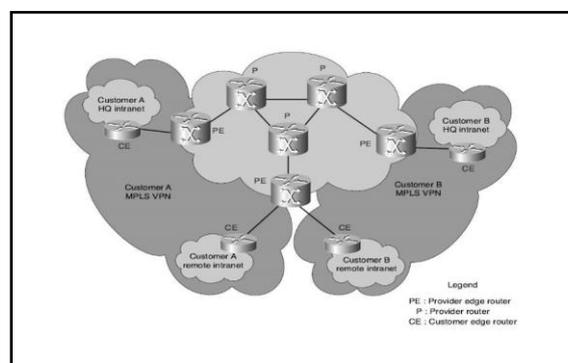
Jaringan Customer, terdiri dari router pada setiap site pelanggan yang disebut dengan Customer Edge (CE) router, disini ini dikenal implementasi peer-to-peer VPN dan dikembangkan untuk mengatasi kelemahan pada model overlay serta mengoptimalkan transportasi data melewati jaringan backbone SP. SP juga ikut aktif dalam proses routing di sisi pelanggan.

Arsitektur MPLS VPN

Arsitektur pada 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 over lapping.

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, bagaimanapun traffic pelanggan terisolasi pada router PE yang sama yang menyediakan konektivitas ke dalam jaringan SP bagi banyak pelanggan.

Figure 3. MPLS VPN



Komponen-komponen utama dalam arsitektur MPLS VPN adalah:

1. Jaringan customer, biasanya merupakan wilayah kekuasaan customer yang terdiri dari router CE.
2. Jaringan provider, merupakan wilayah kekuasaan 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.

Model Routing pada Jaringan MPLS VPN

Implementasi dari MPLS VPN sangatlah mirip dengan implementasi model peer-to-peer VPN karena pada router CE, hanya update data yang diteruskan ke router PE. Router CE tidak perlu dikonfigurasi sebagai router MPLS untuk menjadi bagian dari domain MPLS VPN. Router CE hanyalah routing protokol yang memungkinkannya untuk menukar informasi routing antara router CE dengan router PE.⁶

Implementasi MPLS VPN, pada router PE berfungsi banyak hal. Pertama, router PE harus bisa mengisolasi traffic customer jika terdapat lebih dari satu customer yang terhubung ke router PE. Routing bisa melewati jaringan backbone SP karena menggunakan proses routing yang terdapat pada global routing table. Router P menyediakan label switching antar router PE dan tidak mengetahui ada rute-rute VPN. Router CE pada jaringan customer tidak perlu mengetahui informasi tentang router P dan oleh sebab itu, topologi bagian dalam jaringan SP tidak terlihat bagi customer.

Router PE hanya bertugas dalam label switching paket dan mereka tidak membawa rute-rute VPN. Router PE menukar rute-rute IP dengan router CE menggunakan konteks routing protokol secara individual sehingga memungkinkan jaringan melayani banyak VPN customer, multiprotocol BGP (MP-BGP) harus dikonfigurasi pada router PE untuk membawa rute-rute customer.

⁶Supriyanto. 2013. Jaringan Dasar 1. Jakarta. Kementerian Pendidikan dan Kebudayaan.

Virtual Routing and Forwarding (VRF)

Pengisolasian pelanggan dilakukan oleh router PE dengan menggunakan label Virtual Routing and Forwarding (VRF). Intinya ini sama dengan menggunakan beberapa router untuk menangani pelanggan-pelanggan yang terhubung ke jaringan provider.⁷ Fungsi dari table VRF mirip dengan table routing global, kecuali bahwa table VRF berisi semua rute yang menuju ke VPN khusus. Jumlah dari VRF terbatas oleh jumlah interface yang terdapat pada suatu router dan sebuah interface tunggal hanya bisa diasosiasikan dengan sebuah VRF.

Route Distinguisher (RD) dan Route Target (RT)

Route Distinguisher (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. 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. SP tidak memiliki nomor AS BGP, format pengalamatan IPv4 bisa digunakan dan jika jaringan SP memiliki nomor AS, format dari nomor AS bisa digunakan.⁸

Route Targets (RT) merupakan pengenalan tambahan yang digunakan pada domain MPLS VPN yang mengidentifikasi keanggotaan VPN dari rute-rute yang dipelajari pada sisi tersebut. RT 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.

⁷ Sukaridhoto, Sritrusta. 2016 Jaringan Komputer 2. Surabaya: Politeknik Elektronika Negeri Surabaya

⁸ Sukaridhoto, Sritrusta. 2016 Jaringan Komputer 1. Surabaya: Politeknik Elektronika Negeri Surabaya.

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.⁹

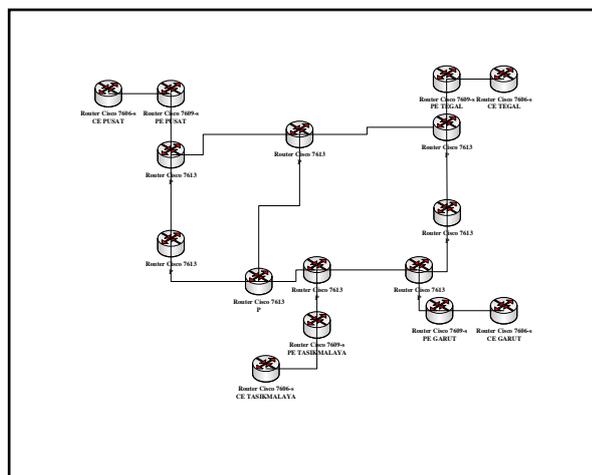
Address Family (AF)

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.

Perancangan Sistem

Setelah melakukan analisis, tahap kedua yang dilakukan oleh peneliti berpedoman pada NDLC adalah tahap perancangan. Adapun tools yang digunakan dalam melakukan perancangan desain topologi yaitu menggunakan Microsoft Visio.¹⁰ Berikut adalah gambar desain Simulasi jaringan MPLS VPN Biznet.

Figure 4. Topologi MPLS VPN

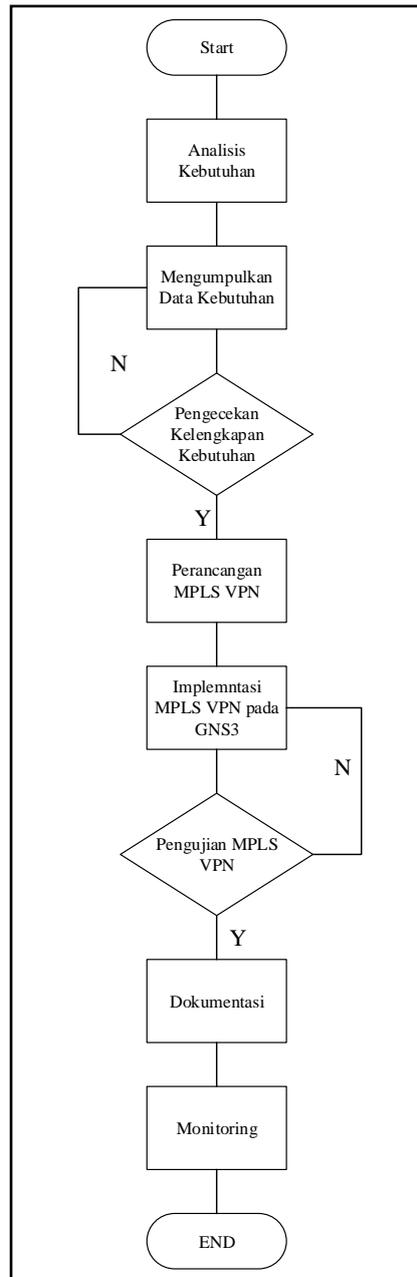


⁹ Alexandrina, Alexandrina dan Ihsan Arief Nurhakim, Muhammad and Novel, Muhammad dan Gunar Setiadji, M.Eng, Tatang 2013. Perancangan Jaringan Terpusat Menggunakan MPLS VPN dengan Failover Link pada CV. Rofa Food Indonesia. Jakarta: Universitas Bina Nusantara.

¹⁰ Sofana, Iwan. 2017. Cisco CCNA - CCNP Routing dan Switching. Bandung: Informatika Bandung.

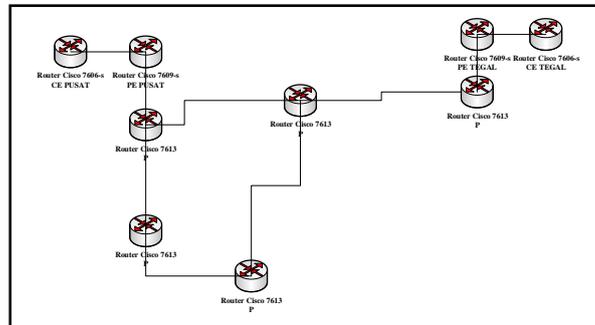
Tahap perancangan pengembangan penulis menggunakan Flowchart sebagai berikut:

Figure 5. Flow Chart Pengembangan Jaringan MPLS



Kondisi Sebelum ada penambahan cabang di jaringan MPLS VPN, penulis mendapat gambaran bahwa topologi yang digunakan adalah sebagai berikut:

Figure 6. Topologi sebelum ada penambahan cabang



Implementasi yang dilakukan menggunakan perangkat yang sudah direncanakan pada bab sebelumnya. implementasi dilakukan dengan beberapa tahapan yaitu, konfigurasi router, membuat web login akses dan tes MPLS VPN dengan tools yaitu Ping dan Tracert menggunakan virtual GNS3.

KESIMPULAN

Berdasarkan hasil yang telah penulis uraikan pada bab sebelumnya, maka penulis dapat mengambil kesimpulan sebagai berikut: Beberapa kantor cabang dapat terhubung dengan kantor pusat yang berada di berbagai tempat dengan menggunakan jaringan MPLS VPN. Setiap ada penambahan jaringan di kantor cabang dapat meminimalisir pengeluaran untuk membangun sebuah jaringan dengan memakai jaringan MPLS VPN, karena jika ada penambahan hanya menambah satu perangkat setelah router PE dengan begitu akan lebih efisien saat ada penambahan. Manajemen user hanya bisa edit username di phpmyadmin, untuk mengurangi resiko penyalahgunaan dari pihak yang tidak bertanggung jawab.

Server akan lebih aman dikarenakan adanya web login pada akses server. User dibatasi hanya akses website untuk masuk ke dalam server. Proses traceroute ke router tujuan 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.

REFERENCES

- 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.
- Kristanti Novi. 2016. Simulasi Jaringan Multiprotocol Label Switching (MPLS) Menggunakan Graphical Network Simulator (GNS3). Semarang: Universitas Diponegoro.
- Nugroho, Kukuh. 2018. Router Cisco Implementasi MPLS VPN. Yogyakarta: Teknosain
- 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
- Sofana, Iwan. 2017. Cisco CCNA - CCNP Routing dan Switching. Bandung: Informatika Bandung.
- Sukaridhoto, Sritrusta. 2016 Jaringan Komputer 1. Surabaya: Politeknik Elektronika Negeri Surabaya
- Sukaridhoto, Sritrusta. 2016 Jaringan Komputer 2. Surabaya: Politeknik Elektronika Negeri Surabaya
- Supriyanto. 2013. Jaringan Dasar 1. Jakarta. Kementerian Pendidikan dan Kebudayaan.