IlmuKomputer.Com
Ikatlah ilmu dengan menuliskannya

Positioning MPLS

Mudji Basuki
mudji@mudji.net
http://mudji.net

Lisensi Dokumen:
Copyright © 2003-2007 IlmuKomputer.Com
Seluruh dokumen di IlmuKomputer.Com dapat digunakan, dimodifikasi dan disebarkan secara bebas untuk tujuan bukan komersial (nonprofit), dengan syarat tidak menghapus atau merubah atribut penulis dan pernyataan copyright yang disertakan dalam setiap dokumen. Tidak diperbolehkan melakukan penulisan ulang,kecuali mendapatkan ijin terlebih dahulu dari IlmuKomputer.Com.

Dokumen ini berisi komponen teknologi Multi-Protocol Label Switching (MPLS), fungsi-fungsinya dan ilustrasi nilai tambah bagi Service Provider.

MPLS pada mulanya ditargetkan untuk pelanggan Service Provider; tetapi saat ini perusahaan-perusahaan sudah mulai tertarik untuk penerapan teknologi ini. Dokumen ini dapat diterapkan untuk perusahaan besar yang memiliki jaringan seperti Service Provider pada area berikut ini :

- Size/ukuran besarnya jaringan
- Menawarkan “internal services” untuk department yang berbeda dalam perusahaan

MPLS komplimen dengan teknologi IP. MPLS di desain untuk membangkitkan kecerdasan yang berhubungan dengan IP Routing, dan Paradigma Switching yang berhubungan dengan Asynchronous Transfer Mode (ATM).

MPLS terdiri dari Control Plane dan Forwarding Plane. Control Plane membuat apa yang disebut “Forwarding Table”, sementara Forwarding Plane meneruskan paket ke interface tertentu (berdasarkan Forwarding Table).

Efisien desain dari MPLS adalah menggunakan Labels untuk membungkus/encapsulate paket IP. Sebuah Forwarding Table berisi list/mengurutkan Nilai-nalai Label (Label Values), yang masing-masing berhubungan dengan penentuan “outgoing interface” untuk setiap prefix network/jaringan.

Cisco IOS Software support 2 mekanisme signalling untuk distribusi Label: Label Distribution Protocol (LDP) dan Resource Reservation Protocol/Traffic Engineering (RSVP/TE).

MPLS meliputi komponen utama sebagai berikut :

1. MPLS Virtual Private Networks (VPNs) - memberikan “MPLS-enabled IP networks” untuk koneksi Layer 3 dan Layer 2. Berisi 2 komponen utama :

1. Layer 3 VPNs - menggunakan Border Gateway Protocol.
2. Layer 2 VPNs - Any Transport over MPLS (AToM)

2. MPLS Traffic Engineering (TE) - menyediakan peningkatan utilisasi dari bandwidth jaringan yang ada dan untuk “protection services”.

3. MPLS Quality of Service (QoS) - menggunakan mekanisme IP QoS existing, dan menyediakan perlakuan istimewa untuk type trafik tertentu, berdasarkan atribut QoS (seperti MPLS EXP)

MPLS VPNs

Layer 3 VPNs

Layer 3 VPNs atau BGP VPNs, teknologi MPLS yang paling banyak digunakan. Layer 3 VPNs menggunakan “Virtual Routing instances” untuk membuat sebuah pemisahan table routing untuk tiap-tiap pelanggan/subscriber, dan menggunakan BGP untuk membentuk koneksi (peering relations) dan signal VPN-berLabel dengan masing-masing router Provider Edge (PE) yang sesuai. Hasilnya sangat scalable untuk diimplementasikan, karena router core (P) tidak memiliki informasi tentang VPNs.

BGP VPNs sangat berguna ketika pelanggan menginginkan koneksi Layer 3 (IP), dan lebih menyukai untuk membuang overhead routing ke Service Provider. Hal ini menjamin bahwa keanekaragaman interface Layer 2 dapat digunakan pada tiap sisi/side VPN. Contoh, Site A menggunakan interface Ethernet, sementara Site B menggunakan interface ATM; Site A dan Site B adalah bagian dari single VPN.

Relatif sederhana untuk penerapan “multiple topologies” dengan “router filtering”, Hub & Spoke atau Full Mesh:

- *Hub and Spoke* - “central site” dikonfigurasi untuk “learn/mempelajari” semua “routes” dari seluruh remote sites, sementara remote sites dibatasi untuk “learn/mempelajari” routes, hanya khusus dari central site.
- *Topology Full Mesh* akan menciptakan semua sites mempunyai kemampuan “learn/mempelajari” atau mengimport routes dari tiap site lainnya.

Layer 3 VPNs telah dikembangkan dalam jaringan yang mempunyai router PE sebanyak 700. Saat ini terdapat Service Provider yang memiliki sampai 500 VPNs, dengan masing-masing VPN berisi site sebanyak 1000. Banyak ragam routing protocol yang digunakan pada link akses pelanggan (yaitu link CE ke PE); Static Routes, BGP, RIP dan Open Shortest Path First (OSPF). VPNs paling banyak menggunakan Static Routes, diikuti dengan Routing BGP.

Layer 3 VPNs menawarkan kemampuan lebih, seperti Inter-AS dan Carrier Supporting Carrier (CSC). Hierarchical VPNs, memungkinkan Service Provider menyediakan koneksi melewati

"multiple administrative networks". Saat ini, penerapan awal dari fungsi seperti ini sudah tersebar luas.

Layer 2 VPNs

Layer 2 VPNs mengacu pada kemampuan dan kebutuhan dari pelanggan Service Provider untuk menyediakan Layer 2 Circuits melalui "MPLS-enabled IP backbone". Penting untuk memahami 3 komponen utama dari Layer 2 VPNs:

1. *Layer 2 Transport over over MPLS* - Layer 2 circuit - membawa data secara transparent - melalui MPLS enabled IP backbone (juga dikenal sebagai AToM).
2. *Virtual Private Wire Services* - Kemampuan untuk menambahkan signalling ke AToM, dan untuk fitur-fitur seperti auto-discovery perangkat CE.
3. *Virtual Private LAN Services* - Kemampuan menambahkan Virtual Switch Instances (VSIs) pada router PE untuk membentuk "LAN based services" melalui MPLS-enabled IP backbone.

Circuits Layer 2 yang dominan adalah Ethernet, ATM, Frame Relay, PPP, dan HDLC. AToM dan Layer 3 VPNs didasarkan pada konsep yang sama, tetapi AToM menggunakan sebuah "directed LDP session" untuk mendistribusikan Labels VC (analogy dengan BGP VPN Label). Oleh karena itu, router core tidak perlu mengetahui per-subscriber basis, hasinya sebuah architecture yang sangat "scalable".

Sebelum ada AToM, Service Provider harus membangun jaringan yang berbeda untuk menyediakan koneksi Layer 2. Contoh, Service Provider harus membangun sebuah ATM dan sebuah Frame Relay Network, hasilnya peningkatan biaya operasional dan "capital expenses". Saat ini, Layer 2 VPNs MPLS memungkinkan Service Provider untuk menggabungkan jenis jaringan yang berbeda ini, sehingga menghemat biaya operasional dan "capital expenses" secara significant.

Layer 2 VPNs dan Layer 3 VPNs dapat dikonfigurasi dalam single/satu box dan dapat difungsikan untuk meningkatkan keuntungan dari pelanggan.

Layer 2 dan Layer 3 VPNs saling melengkapi satu sama lain. Dengan berjalannya waktu, demand untuk Layer 2 VPNs bisa jadi lebih tinggi dibandingkan dengan Layer 3 VPNs.

MPLS Traffic Engineering

MPLS TE sejak awal diharapkan Service Provider sebagai teknologi yang dapat memanfaatkan bandwitdh jaringan yang tersedia secara lebih baik dengan menggunakan jalur alternatif/alternate paths (selain dari "the shortest path).
MPLS TE telah dikembangkan dengan beberapa keuntungan, termasuk Connectivity Protection menggunakan Fast ReRoute dan "Tight QoS". "Tight QoS" dihasilkan dari penggunaan MPLS TE dan mekanisme QoS secara bersamaan.

MPLS TE menggunakan IGP, IS-IS dan OSPF untuk menyebar informasi bandwidth melalui jaringan. MPLS TE juga menggunakan RSVP Extention untuk mendistribusikan label dan “constraint-based routing” untuk menghitung jalur/paths dalam jaringan. Extention ini telah didefinisikan di rfc 3209

Service Provider yang membangun MPLS cenderung untuk menerapkan “full mesh” TE Tunnels, menciptakan logical mesh, walaupun topology physical tidak full mesh. Pada situasi seperti ini, Service Provider telah memperolah tambahan 40% - 50% ketersediaan bandiwidth di jaringan. Keuntungan ini adalah penggunaan jaringan secara optimal, yang berperan penting pada penurunan “capital expenses”.

MPLS TE menyediakan Connectivity Protection menggunakan Fast ReRoute (FRR). FRR memproteksi primary tunnels menggunakan pre-provisioned backup tunnels. Jika tunnel DOWN (failure condition), dibutuhkan waktu sekitar 50 ms untuk primary tunnel “switch over” ke backup tunnel. FRR bergantung pada proteksi Layer 3, tidak seperti proteksi SONET atau SDH yang terjadi pada level interface. Oleh karena itu, Waktu restorasi bergantung pada jumlah tunel dan jumlah prefix yang di”switch-over”. Ini adalah hal penting (key issue) yang harus dipertimbangkan ketika membuat desain FRR yang optimal.

Test internal implementasi FRR Cisco telah menghasilkan performansi lebih baik dari 50 ms; walau bagaimanapun, waktu restorasi mungkin lebih tinggi, bergantung pada konfigurasi. FRR dapat digunakan untuk proteksi Links, Nodes dan seluruh LSP Path. Sebagian besar Service Provider lebih memperhatikan local failures, dan banyak ditemukan bahwa link failures lebih sering terjadi daripada node failures.

DiffServ Aware Traffic Engineering mampu menjalankan TE untuk class trafik yang berbeda. Service Provider boleh memutuskan untuk mengoperasikan TE Tunnels yang memanfaatkan “sub-pool” untuk trafik Voice. Selanjutnya, Service Provider dapat menyakinkan bahwa tunnel ini menggunakan explicit path, dimana shortest path menghasilkan delay terpendek. Selain itu, terdapat TE Tunnels yang menggunakan “global pool” untuk trafik non-voice yang bukan “delay sensitive”.

Hal ini penting untuk dicatat bahwa MPLS TE adalah fungsi dari Control Plane. Ketika solusi Virtual Leased Line (VLL) didefinisikan, mekanisme QoS yang sesuai harus dikonfigurasi (seperti Queuing atau Policing) untuk memenuhi garansi bandiwidth. Service Provider sudah mulai menawarkan jasa VLL sebagai trunk voice untuk menghubungkan Central Office termasuk PBX.

MPLS Quality of Service

MPLS QoS mempengaruhi mekanisme existing dari IP QoS DiffServ, memungkinkan mereka bekerja pada jalur/path MPLS. Extension tertentu, termasuk kemampuan untuk melakukan “set” dan “match” pada bit-bit MPLS EXP telah ditambahkan; meskipun “fundamental behavior” dari mekanisme QoS tetap tidak berubah.

MPLS secara fundamental adalah teknik “tunneling”, jadi mekanisme QoS memungkinkan untuk penerapan yang flexible dengan “tunneling” QoS pelanggan melalui policies QoS dari Service Provider.

Oleh karena itu, Service Provider seharusnya menggunakan nilai EXP 6 untuk voice, dan nilai EXP 4 dan 3 untuk trafik non-voice. Menyediakan transparent services secara simultan untuk Enterprise dengan Maps QoS sebagai berikut :

- Menggunakan Prec 3 untuk voice dan Prec 2 untuk trafik non-voice
- Menggunakan Prec 5 untuk voice dan Prec 4 untuk trafic non-voice

Penawaran service QoS pada MPLS VPN telah menjadi nilai tambah bagi Service Provider, tetapi penerapan QoS bervariasi antar customer. Beberapa customer membuat hanya 2 class of services - (voice dan non-voice), sementara lainnya membuat sebanyak 5 class :

• Best Effort Data
• Interactive Data (i.e.,Telnet)
• Mission Critical Data (ERP applications; i.e., SAP, PeopleSoft)
• Video
• Voice

Kesimpulan

MPLS sedang berkembang sebagai teknologi yang dapat diterima secara luas, dibuktikan dengan lebih dari 100 customers menerapkan Cisco MPLS. Hal ini penting untuk dicatat bahwa MPLS tidak menggantikan IP. IP Control Plane adalah komponen fundamental MPLS. Kemampuan menambahkan “ATM-like Forwarding Plane” membuatnya menarik bagi Service Provider dan Enterprises.

Service Provider bisa mendapatkan keuntungan sebesar 25% dengan menerapkan MPLS VPNs, MPLS QoS dan MPLS TE, daripada sekedar menyediakan koneksi VPNs biasa.

Kesimpulan akhir adalah, keuntungan utama bagi Service Provider dan Enterprises menerapakan MPLS-enabled IP Network adalah kemampuan menyediakan koneksi Layer 3 dan Layer 2 dan “shared services” (seperti DHCP, NAT, dll) melalui “single network”, dengan tingkat optimasi dan utilisasi yang tinggi dari bandwidth yang tersedia menggunakan TE dan QoS.

Biografi Penulis

IP Network Specialist

Pemegang sertifikasi dari Cisco sebagai Cisco Certified Academy Instructor (CCAI), Cisco Certified Network Associate (CCNA), Cisco Certified Network Professional (CCNP), Cisco Certified Internetwork Professional (CCIP), Cisco Information Security Specialist, “Securing Cisco Network Devices (SND) & Securing Networks with Cisco Routers and Switches (SNRS) for CCSP track”, Cisco Certified Internetwork Expert (CCIE,written) dan Voice over IP (VoIP) - Brainbench.