MPLS

Mapa Mental - Aplicações Baseadas no MPLS e seus Respectivos Componentes
Leonardo Furtado

Principais Componentes das Soluções MPLS

MPLS Label Switching

- Control Plane
  - Router ID
  - Label Switching Protocol (LDP)
  - Label Information Base (LIB)
  - Estruturas de dados de Protocolos de Roteamento (ex: LSDB)
  - Routing Information Base (RIB, ou Tabela de Roteamento)
- Data Plane
  - Forwarding Information Base (FIB)
  - Label Forwarding Information Base (LFIB)
  - Adjacency Table (ADJ)
- Configuração do MPLS LDP para um Cenário "Frame-Mode" típico
  - Habilitar globalmente o protocolo LDP
  - Configurar o Router ID usando como referência o endereço IPv4 da interface Loopback "principal" do equipamento
  - Configurar o LDP para alocar labels somente para prefixos /32 (host-routes)
  - Configurar o Anúncio Condicional de Labels se necessário para o projeto
  - Habilitar o protocolo LDP somente nas interfaces PE --> P e P-P
  - Ajustar o MTU das interfaces para acomodar pelo menos um stack com 3 labels (1512 bytes) ou adotando 9000 bytes para o backbone
  - Configurar o Jumbo Frame para SWITCHES na LAN que estiverem transportando o tráfego entre dois neighbors LDP
  - Ajustar os timers do protocolo LDP de forma consistente na rede, caso isto se faça necessário
  - Desabilitar a propagação de TTL para o tráfego de trânsito, e manter habilitado para o tráfego local
  - Configurar o Implicit Null global, condicional, ou seletivo (rotas "non-Egress"), caso exigido para o projeto
  - Configurar o sincronismo entre IGP e LDP, se desejado
  - Configurar o Entropy Label (RFC 6790) para implementar Entropy Label Capability (ELC) e o uso de Entropy Label Indicator (ELI)/Entropy Label(EL) para implementar hashing mais eficiente visando o balanceamento de carga sobre links físicos de eventuais Layer 2 EtherCahannel do backbone MPLS

MPLS Layer 3 VPN (L3VPN)

- Control Plane
  - Protocolo de Roteamento entre PE e CE (IGP ou BGP)
  - Protocolo MP-BGP entre roteadores PE
  - Família de Endereços VPNv4 e VPNv6
  - Route Distinguisher (RD)
  - Route Target (RT), um atributo BGP (Extended Community RT)
  - Virtual Forwarding and Routing (VRF)
  - Os mesmos componentes de Control Plane do MPLS Label Switching
  - MP-BGP para Label Exchange (para projetos CoC ou Unified MPLS
  - Atributos adicionais (ex: Site of Origin (SoO), dentre outros)
- Data Plane
  - Forwarding Information Base (FIB)
  - Label Forwarding Information Base (LFIB)
  - Adjacency Table (ADJ)
- Configuração de uma L3VPN típica
  - Configurar uma VRF para cada cliente
    - Determinar o Route Distinguisher (RD) globalmente (Cisco IOS) ou no processo BGP (IOS XR)
    - Determinar os Route Targets (RT) conforme o tipo de VPN desejado / a ser estabelecida
      - Simple Vpn
      - Overlapping VPN
      - Central Services VPN
      - Managed Services VPN
      - Internet as a VPN
      - Ou uma combinação de tipos de VPN
    - Posicionar a interface L3 do cliente (física, subinterface, SVI/VLAN, BVI, Bundle-Ethernet...) para a VRF desejada
    - Configurar regras de importação de rotas com Import Map, e exportação de rotas com Export Map para fins de estabelecer VPNs mais complexas, tais como Serviços Gerenciados em combinação com Overlapping VPNs
    - Definir os limites de rotas permitidas na tabela de roteamento da VRF
  - Configurar o MP-BGP para suportar a família de endereços VPNv4 ou VPNv6
    - Informar a VRF do cliente e configurar a redistribuição do protocolo IGP do cliente nesta VRF, por cliente, abaixo da configuração do protocolo BGP
    - No caso de projetos com protocolo BGP para o roteamento PE-CE, definir na VRF do cliente os parâmetros para a sessão EBGP com o CPE do cliente (neighbor, remote-as, local-as (se exigido), policy IN e OUT, máximo de prefixos recebidos, etc.)
      - Se exigido, configurar o Allow-As In ou o AS Override, em combinação com o Site of Origin (SoO)
    - Configurar a alocação de Labels por VRF
    - Habilitar a família de endereços VPNv4 e VPNv6
      - Configurar o neighbor-group ou peer-group para as sessões IBGP entre os roteadores MP-BGP do backbone, usando a Loopback como source, Next Hop Self, Route Reflectors e/ou Confederations onde aplicáveis, etc.
  - Configuração do Protocolo de Roteamento PE-CE
    - Promover a redistribuição mútua entre o protocolo IGP e o BGP, dentro das respectivas VRFs de clientes
      - Protocolos de roteamento RIPv2 e EIGRP obrigatoriamente exigem o fornecimento de uma Seed Metric durante a redistribuição
      - Protocolo de roteamento OSPF não redistribui rotas BGP como LSA Type 5
      - Algumas L3VPNs com OSPF podem exigir a configuração de Sham-Links
      - Atenção quanto as questões de escalabilidade com processos OSPF no roteador PE
    - Em cenários Carrier Supporting Carrier (CsC) o "CE" é o PE de outra operadora. Neste caso, dos métodos possíveis, o MPLS é indicado. Recomenda-se configurar o BGP para a troca de Labels entre as duas Operadoras

MPLS Layer 2 VPN (L2VPN)

- Control Plane
  - Os mesmos componentes de Control Plane do MPLS Label Switching
  - Bridge Domains
  - Virtual Forwarding Instance (VFI)
  - Xconnect para EFPs locais
  - Ethernet Flow Point (EFP)
  - Ethernet Virtual Circuit (EVC)
  - MST AG ou PVST AG (PVRSTAG)
  - Layer 2 Protocol Tunneling (L2TP), peer, forward ou tunnel
  - Flow-Aware Transport Pseudowire (FAT-PW)
- Data Plane
  - Forwarding Information Base (FIB)
  - Label Forwarding Information Base (LFIB)
  - Adjacency Table (ADJ)
- Configuração de uma L2VPN típica
  - Definir o tipo de VPN a ser constituída
    - Point-to-Point
    - Point-to-Multipoint
    - Mesh e PBB
  - Definir os Attachment Circuits (AC) e Ethernet Flow Point (EFP) de cada VPN a ser estabelecida, geralmente um EFP + um cliente ou um serviço distinto por cliente
  - Definir o Ethernet Virtual Circuit (EVC) para a VPN, consolidando a interface Layer 2 e a Routed Interface de acordo, podendo ser em regime point-to-point, ou multipoint através de uma Bridge Domain para separação da VLAN de seu domínio de broadcast, e consolidação de múltiplas VLANs para o mesmo domínio de broadcast em cenários específicos
  - Definir Templates type pseudowire ou pseudowire-classes para definir características específicas para a L2VPN, incluindo tipo e encapsulamento, VC type, MTU, preferred-path e outros
  - Definir propriedades adicionais tais como protocolos de controle que deverão ser suportados, limitação de endereços MAC, Split Horizon Groups (SHGs) para L2VPN multiponto, etc.
  - Definir se deverá haver Flow-Aware Transport Pseudowire (FAT-PW) para fornecer hashing para balanceamento de tráfego em port-channels (EtherChannel) em L2 ao longo do backbone MPLS

MPLS Traffic Engineering (TE)

- Control Plane
  - Os mesmos componentes de Control Plane do MPLS Label Switching
  - Traffic Tunnels
    - Atributos
      - Traffic Parameter
        - Tailend Ldp
        - Bandwidth
      - Generic Path Selection
        - Static
        - Dynamic
      - Resource Class Affinity
        - Reoptimize, Do Not Reoptimize
      - Adaptability
      - Priority and Pre-emption
        - Setup Priority
        - Hold Priority
      - Resilience
        - Reroute, Do Not Reroute, Reroute qualquer Carretel Value
  - Network e Link Attributes
    - Maximum Bandwidth
    - Maximum Reservable Bandwidth
    - Link Affinity String / Link Resource Class
    - Constraint-based Specific Metric
  - Constrained-Based Path Computation (CSPF) ou Path Calculation (PCALC)
    - Constraint-Based Routing (CBR)
      - Dynamic
      - Static
      - Link Resource Attributes
      - Traffic Tunnel Attributes
    - MPLS TE para OSPF / ISIS
      - Router ID
      - Area
  - Protocolo IGP (OSPF ou ISIS)
  - Resource Reservation Protocol (RSVP)
    - Global Pool
    - Subpool
  - Link-level Call Admission Control (LCAC)
    - Auto Bandwidth
    - Interação com RSVP
  - Modificações da Tabela de Conexão
    - Static Routing
    - Policy Routing (PBR)
    - Forwarding Adjacency
    - Autoroute
- Data Plane
  - Forwarding Information Base (FIB)
  - Label Forwarding Information Base (LFIB)
  - Adjacency Table (ADJ)

MPLS QoS

- Control Plane
  - Os mesmos componentes de Control Plane do MPLS Label Switching
  - DiffServ-Aware TE
    - Em conjunto com o MPLS-TE
  - Marking (DiffServ)
    - Uniform Mode
    - Pipe Mode
    - Short Pipe Mode
- Data Plane
  - Forwarding Information Base (FIB)
  - Label Forwarding Information Base (LFIB)
  - Adjacency Table (ADJ)

MPLS-TP

- Arquitetura PWE3 Pseudowire
- Control Plane: static ou dynamic Generalized MPLS (G-MPLS)
- Generic Associated Channel (G-ACH)
- Generic Alert Label (GAL)

Aplicações MPLS

MPLS Label Switching

- Comutação de pacotes é feita baseada em instruções contidas em "labels", sem utilização do cabeçalho IP (IP Header)
  - Menos instruções para trabalhar, operações mais simplificadas no Data Plane
  - Penultimate Hop Popping (PHP), que é habilitado por default, realiza o "pop" do Label no penúltimo salto da saída do domínio MPLS, preservando os recursos do último salto, que por sua vez só realiza uma simples consulta na FIB. O Egress LER anuncia um label "implicit-null" (valor 3) para o penúltimo salto, indicando que esta ação de PHP é desejada para aquele LSP
    - Pode ser desabilitado com Explicit-Null (valor 0)
- Computacionalmente mais eficiente que "IP routing" tradicional, menos instruções para processar; ações de Data Plane são mais simples (push, swap, pop de labels), logo, "throughput" mais favorável
- Projetada para aumentar a taxa de desempenho de backbones com suporte a múltiplos protocolos, embora hoje consideremos somente o protocolo IP
  - A operação com labels é menos computacionalmente intensa do que o "path determination" e "packet switching" (incluindo "packet rewrite") executados na operação IP routing tradicional
  - Este "desempenho maior" perdeu um pouco de relevância em função das ações de Data Plane nos roteadores mais sofisticados, as quais são executadas integralmente em hardware especializado e dedicado (ex: prefix lookup, packet rewrite, ACL, QoS, NetFlow), tanto para "ingress" quanto para "egress"
    - Plataformas como Network Processor Unit (NP) do ASR 9000, ou Packet Switching Engine (PSE) do CRS-1/3/X, Policy Feature Card 4 (PFC4) do Catalyst 6500, Cisco QuantumFlow Processor (QFP) do ASR 1000, para exemplificar algumas destas arquiteturas, podem realizar o processamento de pacotes de entrada (ingress) e de saída (egress) integralmente em hardware altamente especializado, independente do pacote possuir label ou não, e considerando múltiplas ações (ACL, QoS, NetFlow, etc.)
- Funciona como o alicerce para as demais aplicações suportadas pelo MPLS (ex: L3VPN, AToM, MPLS TE)

MPLS Layer 3 VPNs (L3VPN)

- Tecnologia de implementação de redes privativas para fins de segregação de tráfego de controle e de dados entre clientes sobre uma mesma infraestrutura física.
- Aproveita a arquitetura do MPLS Label Switching para o transporte de pacotes de múltiplos clientes sobre uma infraestrutura comum.
- Promove a virtualização do Control Plane e Data Plane por intermédio da tecnologia **Virtual Routing and Forwarding** (VRF), o que permite a completa segregação de clientes atendidos pelo mesmo roteador de agregação ("PE router") e a separação do tráfego de cliente sobre os mesmos enlaces de rede.
  - Por exemplo, permite faixas de endereços IP "conflitantes" de clientes distintos a coexistir sobre a mesma infraestrutura
- Combina os benefícios providos por redes Overlay VPN (ex: ATM e Frame Relay) e Peer-to-Peer (IP routing), maximizando o "melhor dos dois mundos" ao mesmo tempo em que evitando-se as deficiências e limitações de cada caso.
  - Mais simples
  - Mais flexível
  - Maior escalabilidade
  - Melhor gerenciamento
  - Melhores níveis de serviço
- Tipos de VPN comumente empregadas para serviços com Clientes
  - Simple VPN
  - Overlapping VPN
  - Central Services VPN
  - Managed Services VPN
  - Internet as a VPN Service
- Cenários Adicionais de VPN
  - **Carrier Supporting Carrier** (CsC), primariamente direcionado para trânsito entre Operadoras, e através do conceito de "VPNs sobre VPNs"
  - **6VPE** para transporte de prefixos IPv6 em VPN de clientes sobre backbone MPLS ainda operando somente com IPv4 (ou seja, sem dual-stack)
  - **Seamless MPLS**, também conhecido por **Unified MPLS**, tem como principal proposta a escalabilidade massiva de redes MPLS.A proposta é criar diversos domínios IGP + LDP confinados e interconectar estes domínios com o BGP em operação por Labels.Por exemplo, a redistribuição de IGPs é bastante indesejada no backbone das operadoras mas ao mesmo tempo se isto não for feito, não será possível estabelecer LSPs fim-a-fim. O objetivo do Unified MPLS é viabilizar o LSP fim a fim em redes muito grandes, no entanto sem exigir redistribuição entre protocolos de roteamento IGP.

MPLS Layer 2 VPNs (L2VPN)

- Primariamente, uma tecnologia de extensão de LANs e emulação de serviços Ethernet sobre uma infraestrutura puramente IP/MPLS. Implementa os chados "pseudowires"
- Tradicionalmente conhecido por **Any Transport over MPLS** (AToM) para os serviços Ethernet over MPLS (EoMPLS), Frame Relay over MPLS (FRoMPLS), PPP over MPLS (PPPoMPLS), etc.
- Diversas tecnologias associadas aos cenários de L2VPN possuem soluções mapeadas e compatíveis, com reconhecimento na indústria
  - Na terminologia do Metro Ethernet Forum: **E-Line** (para um EVC ponto-a-ponto), **E-LAN** (para um EVC ponto-multiponto), **E-Tree** (para um Rooted-multipoint EVC)
  - Na Terminologia do IETF (MPLS):**Virtual Private Wire Service** (VPWS), para serviços ponto-a-ponto; **Virtual Private LAN Services** (VPLS), para serviços Multiponto
  - Na Terminologia da Cisco: **Ethernet Wire Service** (EWS), para serviços ponto-a-ponto em QinQ e 802.1ad; **Ethernet Relay Service**, para serviços ponto-a-ponto com 802.1Q ; **Ethernet Multipoint Service** (EMS), para serviços multiponto com QinQ e .1ad ; **Ethernet Relay Multipoint Service** (ERMS), para serviços multiponto com .1Q
- Elimina as deficiências associadas com topologias de Camada 2 no backbone, pois, ao implementar IP/MPLS somente para o backbone, eliminamos as deficiências de tecnologias tais como o protocolo Spanning Tree, prevenção de loops, e distribuição de carga ("load balancing")
  - Roteamento IP converge bem mais eficientemente que L2/STP, é muito mais seguro e imune a loops que protocolos de resiliência tais como REP, possui melhores capacidades de balanceamento de tráfego
  - Roteamento IP permite realizar load balancing de forma muito mais eficiente e funcional que a segregação de domínios Layer 2 que posicionam Root Bridges em pontos distintos no backbone

MPLS Traffic Engineering (TE)

- Roteamento IP nativo possui limitações, já que os pacotes são inspecionados salto a salto, o endereço IP de destino contido nos cabeçalho IP é verificado, uma rota correspondente (a mais específica) é escolhida; a interface associada à rota é utilizada como saída, o cabeçalho IP é reescrito (TTL e CRC), e ocorre então a reescrita do novo cabeçalho de Camada 2 correspondente às instruções desta interface.
- Este comportamento "per hop behavior", salto a salto, introduz alguns desafios e limitações que são nativos do protocolo IP
  - Havendo múltiplos caminhos para um determinado destino, o caminho de menor custo será sempre utilizado, e independente da carga que é oferecida sobre este (melhor) caminho ou caminho de menor custo.
  - O fato é que entre poderá sempre haver mais de um caminho para se chegar a um determinado destino. Às vezes mais de dois caminhos.
  - O melhor caminho será sempre utilizado e mesmo assim poderá não possuir os recursos para acomodar toda a carga de tráfego que é lançado sobre ele.
  - Consequentemente, o caminho fica sobrecarregado enquanto as demais alternativas ficam bastante ociosas. E o efeito chamado "**the flah problem**".
- Tecnologia que permite manipular o tráfego no backbone sem que seja necessário alterar métricas dos protocolos de roteamento e interfaces, ou implementar quaisquer políticas de roteamento no Core.
  - É possível selecionar exatamente quais tipos de tráfego serão mapeados para os túneis de TE, podendo ser destinos específicos, todas as rotas atrás do Tailend do túnel, ou por condições mais granulares via políticas de roteamento (RPL)
- Possui ferramentas adicionais como atrativos extras, tais como reconvergência de alta performance com até 50 ms de recuperação de falhas de links e roteadores no backbone; tecnologia **Fast Reroute** (FRR)
  - Em muitos casos, a Operadora está mais interessada no FRR em si do que na própria capacidade de manipular o tráfego no backbone.
- O **Preferred Path** do MPLS L2VPN funciona em combinação com túneis de Engenharia de Tráfego do MPLS TE
  - Isto permite fazer a engenharia de tráfego de L2PVNs específicas para sanear o gargalo de redes para clientes ou serviços específicos.

MPLS QoS

- Tecnologia que permite estabelecer níveis de serviço mais atraentes para a Operadora, aproveitando-se de todas as ferramentas do DiffServ. E visando implementar níveis de serviço distintos para clientes e aplicações específicas.
- Essencialmente significa estabelecer **Forwarding Equivalence Classes** (FECs) com tratamentos diferenciados através do backbone MPLS
- Não executa o chamado "hard QoS", pois isto é função das ferramentas funcionais do domínio DiffServ (congestion management, congestion avoidance, policing, shaping, LFI, etc.). Ao invés disto, o MPLS QoS funciona somente no aspecto Control Plane, e usa os mecanismos configurados nos roteadores (as ferramentas do DiffServ) para executar as ações sobre os pacotes em suas respectivas FECs.
- Uma das ferramentas do MPLS QoS inclui o chamado "**DS-TE**" ou **DiffServ Aware Traffic Engineering**. Com esta ferramenta, é possível estabelecer uma FEC exclusiva utilizando-se um subpool da reserva de banda de interfaces - em nível Control Plane apenas - permitindo o gerenciamento da reserva e controle de admissão de túneis para tráfego de maior prioridade e sensíveis aos efeitos de latência e jitter (ex: VoIP). Esta FEC não disputaria recursos de banda com outras FECs que compartilham a banda, em suas respectivas prioridades, no pool global das interfaces do backbone MPLS TE.
- Outras ferramentas incluem estratégias bem inteligentes de marcação e remarcação dos pacotes em suas respectivas classes de tráfego de clientes, devidamente mapeadas para classes de tráfego da Operadora, possibilitanto manipular bem as questões de prioridade. Exemplos aqui: **Uniform Mode**, **Pipe Mode**, **Short Pipe Mode**.

MPLS Transport Profile (TP)

- É uma variação do protocolo MPLS usada em redes baseadas em pacotes, sendo uma padronização de especificações regidas pelo IETF para incorporar facilidades das arquiteturas IETF MPLS e PWE3 para suportar e acomodar capacidades de redes de transportes.
- A questão é que as redes estão sendo completamente migradas para infraestruturas de comutação baseadas em pacote mas que, ao mesmo tempo, ainda há muitos componentes de infraestruturas baseadas em tecnologias TDM, tais como DSL/DSLAMs, E1 PDH, SDH, etc. A proposta do MPLS-TP é fornecer uma versão simplificada do MPLS para redes de transporte com algumas das funções nativas do MPLS, tais como PHP, LSP, ECMP, etc. O MPLS-TP não requer capacidades de Control Plane de MPLS, e isto permite o estabelecimento do plano de gerenciamento para a definição manual de LSPs. Em adição, as suas capacidades de OAM funcionam sem qualquer dependência de mecanismos de protocolo IP.

ALGUNS COMANDOS DE VERIFICAÇÃO E TROUBLESHOOTING DE BACKBONES MPLS

VERIFICAÇÃO DO OSPF
```
show ip ospf interface brief
show ip ospf neighbor
show ip ospf database
show ip ospf
show ip protocols
show ip route ospf
show ip cef
```
VERIFICAÇÃO DO LDP
```
show mpls interfaces
show mpls ldp discovery
show mpls ldp neighbor
show mpls ldp bindings
show mpls forwarding-table
```
VERIFICAÇÃO DO L2VPN
```
show xconnect name CLIENTE-XPTO detail
show mpls l2transport vc VLANID detail
show bridge-domain ID show ethernet service instance id ID interface INTERFACE detail
show l2vpn vfi name CLIENTE-XPTO
show l2vpn service name CLIENTE-XPTO
show l2vpn bridge-domain bd-name NOME detail (IOS XR)
show l2vpn forwarding bridge-domain mac-address location (IOS XR)
```
VERIFICAÇÃO DO MPLS TE
```
show mpls traffic-eng tunnels
show mpls traffic-eng topology
show mpls traffic-eng forwarding
show mpls traffic-eng tunnels protection
show mpls traffic-eng fast-reroute database
show mpls traffic-eng link-management admission-control
show mpls traffic-eng autoroute
show ip rsvp interface
show ip rsvp neighbor
show ip rsvp reservation
```