FOUNDRY NETWORKS

VPNs de Camada 2 e 3 usando MPLS

Agenda

- Objetivos
- Introdução
- VPNs de Camada 3
- VPNs de Camada 2
- Conexões Ponto- a- Ponto
- Conexões Ponto- Multiponto
- Camada 2 ou Camada 3?
- Conclusões

FOUNDRY NETWORKS

Objetivos

- Apresentar os conceitos básicos que envolvem a criação de VPNs de Camada 2 e 3 usando MPLS
- Avaliar os prós e contras de abordagens de Camada 2 e Camada 3 para implantação de VPNs usando MPLS.

FOUNDRY NETWORKS

Introdução

- A tecnologia MPLS está recebendo muita atenção dos provedores de serviço nos últimos anos. Originalmente ela foi usada para Engenharia de Tráfego.
- Atualmente, MPLS está sendo usado também para implantação de VPNs. Numa mesma rede MPLS podem ser criadas várias **Virtual Private Networks (VPNs),** que permitem o compartilhamento de um mesmo backbone com total segregação de tráfego entre clientes diferentes.
- Os provedores de serviço têm duas alternativas:
  - Criar VPNs com serviços de Camada 3
  - Criar VPNs com serviços de Camada 2

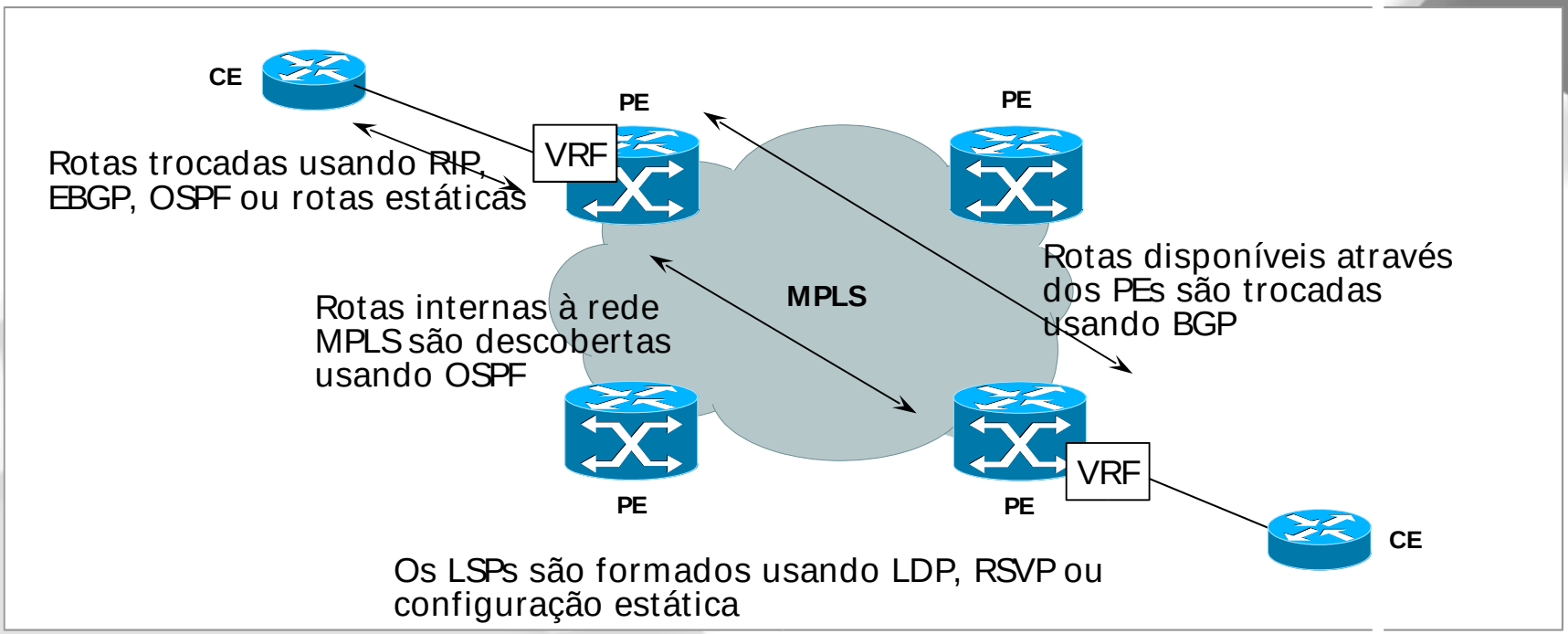
FOUNDRY NETWORKS

VPNs de Camada 3

- O padrão “de fato” para montagem de VPNs de Camada 3 com MPLS está descrito na RFC 2547. Uma nova versão, chamada **RFC 2547bis** ou BGP/MPLS, já está sendo usada por diversos fabricantes.
- Esse método usa tabelas de roteamento IP (baseadas em endereços IP de destino) para enviar o tráfego através da rede da operadora usando um LSP (Label Switched Path).
- São definidos quatro componentes básicos:
  - Customer Edge Router **(CE)**
  - Provider Edge Router **(PE)**
  - Virtual Routing and Forwarding Table **(VRF)**
  - Provider MPLS Domain, formado por Provider Routers **(P)**

FOUNDRY NETWORKS

Componentes de uma VPN de Camada 3



- Os roteadores CE oferecem conectividade com as redes dos clientes e com os PEs. As redes do cliente são divulgadas para o PE usando usando RIP, OSPF, BGP ou rotas estáticas.
- Na rede MPLS cada PE se comunica com os demais PEs da mesma VPN usando IBGP e extensões de MBGP. Um PE que recebe um pacote de um CE é chamado **Ingress LER**. Um PE que transmite um pacote para um CE é chamado **Egress LER**.
- Os PEs contém VRFs para cada VPN. Essas tabelas contém todas as rotas entre o PE e o CE e os LSPs para cada PE que faz parte da mesma VPN.
- As entradas dessas tabelas são propagadas para todos os PEs da mesma VPN, mas nunca para os roteadores (P), porque eles não precisam dessa informação, já que usam apenas LSPs para fazer comutação do tráfego.

Mecanismos Utilizados - VRFs

- VPNs de Camada 3 usando MPLS possuem duas importantes características:
  - Suporte para endereços públicos únicos do lado do cliente, e também endereços privados não-únicos, permitindo sobreposição de endereços.
  - Suporte para sobreposição de VPNs, onde um site pode pertencer a mais de uma VPN.
- Para permitir sobreposição (ou repetição) de endereços, são criadas múltiplas tabelas de roteamento nos roteadores PEs. Essas tabelas são chamadas **VRFs (VPN Routing and Forwarding tables)** e mantém isoladas as redes de cada VPN.
- Para cada VPN existente em um PE corresponde uma VRF, mesmo que essa VPN esteja distribuída em vários sites diferentes.

FOUNDRY NETWORKS

Mecanismos Utilizados – Route Distinguisher

- Uma implicação da sobreposição de rotas é que um PE que recebe atualizações de seus vizinhos via BGP poderá receber rotas conflitantes ou repetidas, que pertencem a VPNs diferentes.
- Para identificar rotas pertencentes a VPNs diferentes (e evitar que BGP selecione uma e descarte as outras), um atributo chamado **Router Distinguiser (RD)**, usando 8 octetos, é prefixado a cada rota anunciada.
- O resultado é um endereço de 12 octetos (4 para o endereço IP e 8 para o RD) que cria uma nova família de endereços, chamada **VPN-IPv4**. Esses prefixos são transportados pelo protocolo MBGP.
- Os roteadores que recebem esse endereço usa o campo RD para distinguir uma VPN da outra.
- Ao anunciar uma rota VPN- IPv4, um PE também inclui um label representando essa rota na mensagem BGP, e ajusta o parâmetro BGP NEXT_HOP igual ao seu próprio endereço.
- Como a rede do provedor é inteira MPLS, cada roteador PE pode alcançar qualquer outro roteador PE através de um LSP. Os LSPs podem ser criados por LDP ou RSVP/ TE.

FOUNDRY NETWORKS

Relação entre VRFs e RDs

- Os RDs servem apenas para diferenciar rotas entre VPNs diferentes. Eles não influenciam na distribuição das rotas.
- Um **RD fica associado a um VRF**, de forma que todos os prefixos anunciados por essa VRF vão usar esse RD.
- Faz sentido configurar o mesmo RD para VRFs pertencentes à mesma VPN. Normalmente, cada VPN terá um RD único.
- Isso não significa que VRFs de sites que pertencem a várias VPNs possuem vários RDs. As VRFs desses sites continuam tendo um único RD.

FOUNDRY NETWORKS

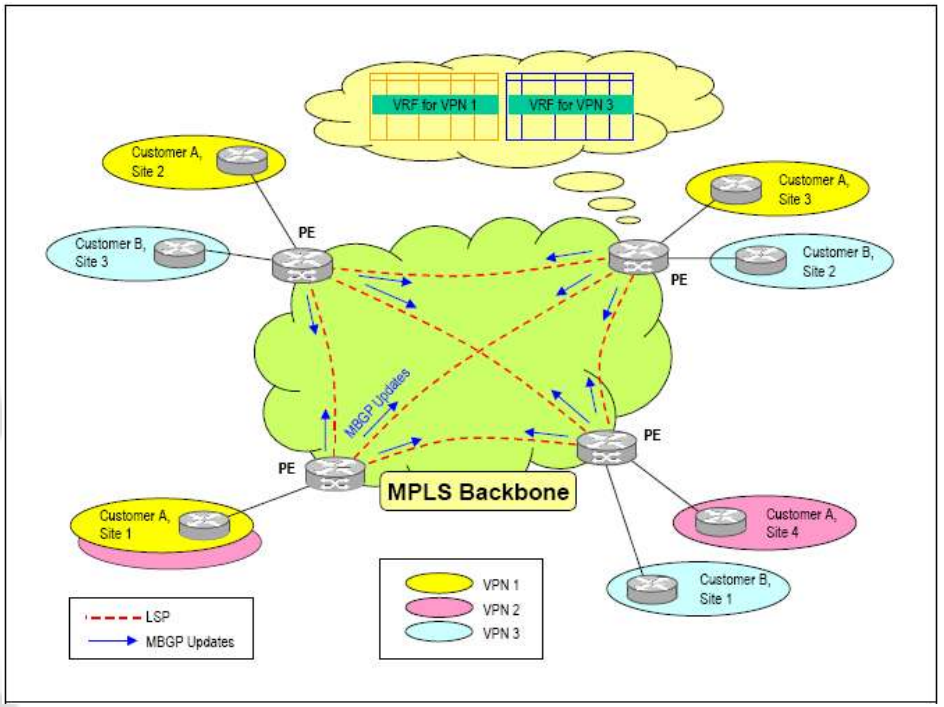
Mecanismos Utilizados – Route Target

- Para separar o tráfego de sites que participam de várias VPNs, evitando que um PE aceite rotas de VPNs que ele não transporta são usados atributos de comunidades estendidas de BGP.
- O atributo **Route Target** é incluído com cada rota anunciada para indicar a VPN à qual essa rota pertence.
- Cada VPN recebe um valor único para Route Target.
- Quando um roteador PE recebe um anúncio de rota com esse atributo, ele verifica se a VPN correspondente faz parte do grupo de VPNs com as quais ele trabalha. Caso afirmativo, a rota é aceita; caso negativo a rota é descartada.
- Isso evita que todos os PEs trabalhem com todas as rotas de todas as VPNs existentes na operadora, fato que poderia causar problemas de escalabilidade.

FOUNDRY NETWORKS

Combinando RDs e Route Targets

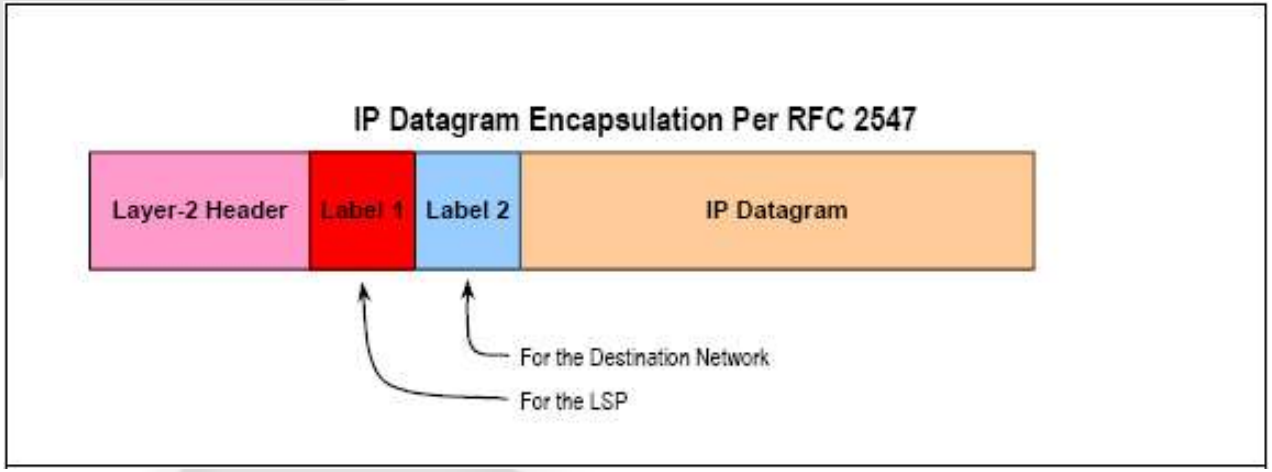
- Tomemos o exemplo de um cliente que usa uma VPN para acessar sua Intranet e outra para a Extranet, cada uma com um conjunto de rotas diferentes.
- Na figura ao lado, o cliente A, no site 1, trabalha na VPN1 e na VPN2.
- As rotas para esse site são anunciadas pelo roteador PE usando um único RD, porém com dois Route Target diferentes: um para VPN1 e outro para VPN2.
- Esse PE vai aceitar rotas de outros PEs apenas se os prefixos recebidos fizerem parte da VPN1 e VPN2.



FOUNDRY NETWORKS

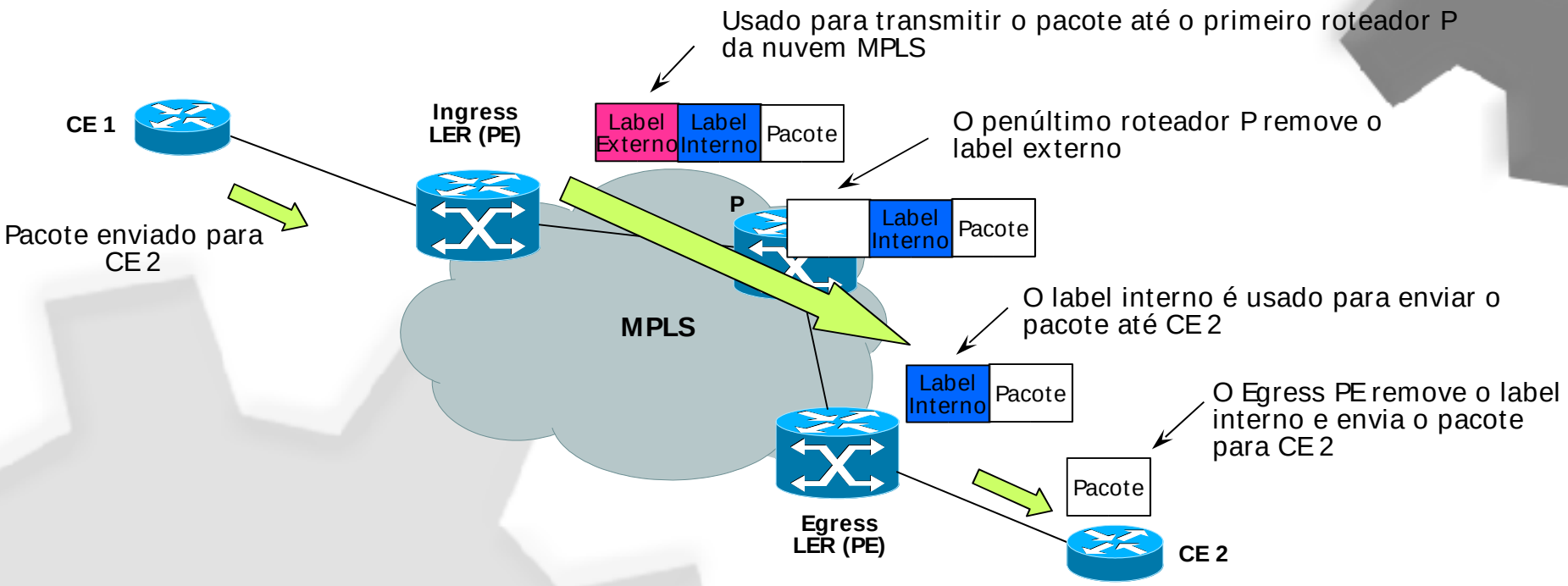
Labels em VPNs de Camada 3

- Quando um PE recebe um pacote com destino para um site remoto, ele insere **dois labels** no pacote.
- O label mais externo é para o LSP que conduz até o BGP NEXT_HOP.
- O label mais interno está associado com o destino final, e foi aprendido com uma mensagem BGP recebidas de um peer.



FOUNDRY NETWORKS

Mecanismo de Transporte



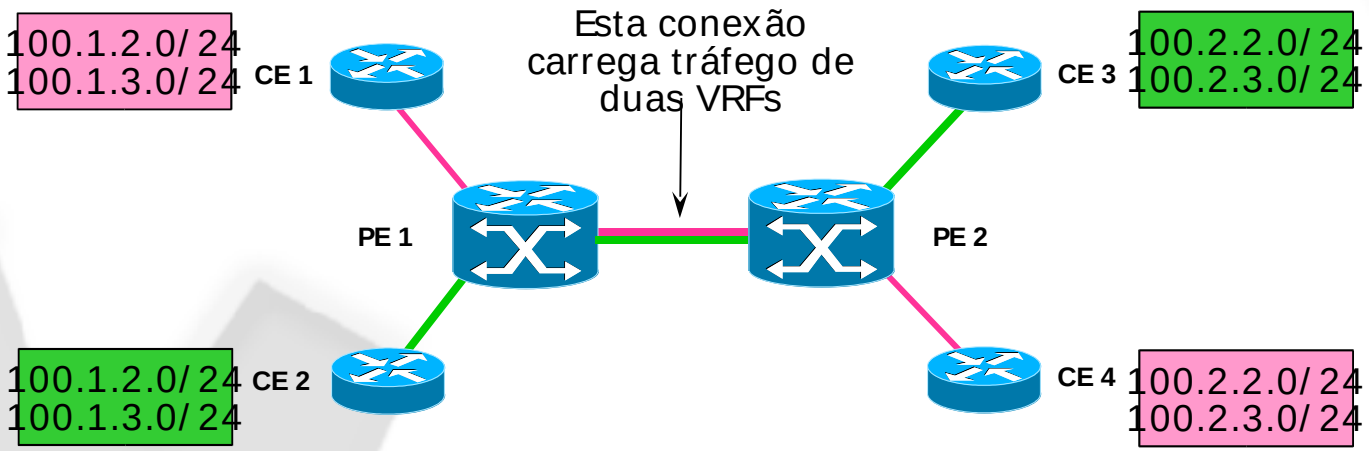
- Quando um pacote é transmitido de um CE para um Ingress PE, esse PE adiciona o Label Interno, obtido do Egress PE através do anúncio de rotas com IBGP, e adiciona o Label Externo, obtido do LSP que conduz ao Egress PE.
- O pacote é comutado pelos roteadores P usando apenas o Label Externo.
- O penúltimo roteador P remove o Label Externo e envia o pacote ao Egress PE.
- O Egress PE usa o Label Interno para identificar o CE para onde o pacote deve ser transmitido. Ele remove o Label Interno e transmite o pacote para o CE.

VRFs sem MPLS

- Na prática, VRF permite que o roteador seja dividido em “roteadores virtuais”, cada um com seu próprio conjunto de interfaces, tabelas de roteamento e comutação.
- Isso permite que um provedor de serviços usando a RFC 2547bis suporte duas ou mais VPNs com endereçamento IP repetido na mesma interface ou roteador.
- Uma variação dessa tecnologia, chamada Multi-VRF ou VRF-Lite, utiliza VRFs sem usar MPLS.
- Multi-VRF utiliza portas de entrada para distinguir as rotas de VPNs diferentes a forma tabelas de comutação virtuais associando uma ou mais interfaces de Camada 3 para cada VRF. Essas interfaces podem ser físicas ou virtuais.

FOUNDRY NETWORKS

Exemplo usando Multi- VRF



- Os roteadores CE 1 e CE 4 são CEs para a VPN “Rosa” e os roteadores CE 2 e CE 4 são CEs para a VPN “Verde”. Os CEs precisam rodar RIP, OSPF, BGP ou simplesmente rotas estáticas.
- Os dois PEs suportam VRF, e precisam estar conectados em Camada 3, seja diretamente ou através de switches.
- As duas VPNs são formadas por VRF com exatamente as mesmas redes.
- Para garantir isolamento entre rotas de VPNs diferentes, cada VRF é configurado com um RD diferente.

FOUNDRY NETWORKS

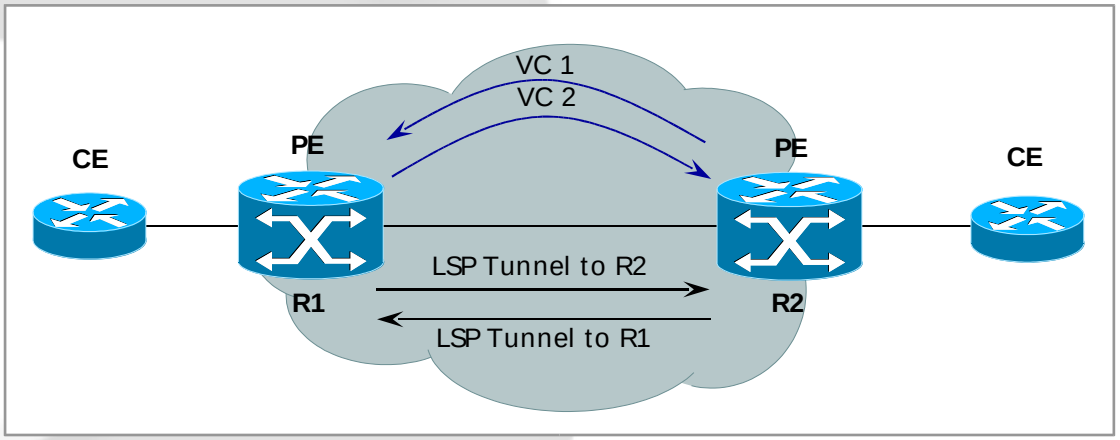
VPNs de Camada 2

- VPNs de Camada 2 permitem maior separação lógica entre a rede da operadora e a rede do usuário, isto é, não existe troca de rotas entre os PEs e CEs.
- VPNs de Camada 2 usando MPLS oferecem serviços de transporte de frames de um site para outro, de forma totalmente transparente e independente dos protocolos de Camada 3. Dessa forma, a operadora pode transportar IPv4, IPv6, IPX, DECNet, OSI, etc.
- Há dois métodos de conexão:
  - Conexão Ponto-a-Ponto
  - Conexão Ponto-Multiponto

FOUNDRY NETWORKS

Conexões Ponto- a- Ponto

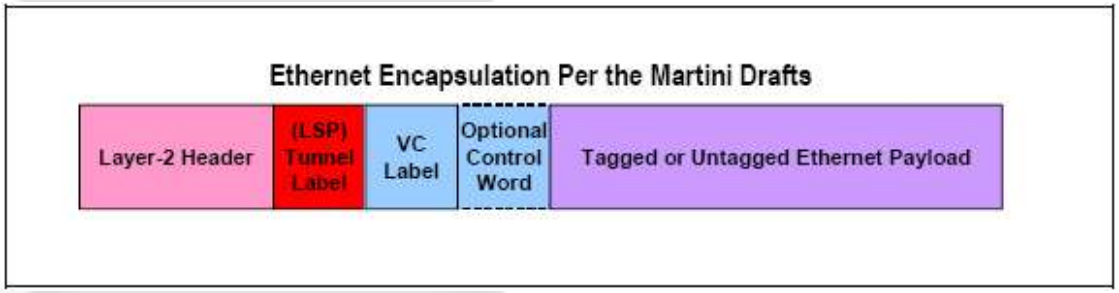
- Os padrões “de fato” para estabelecimento de conexões ponto- a- ponto estão definidos por dois drafts:
  - draft- martini- l2circuit- trans- mpls
  - draft- martini- l2circuit- encap- mpls
- Esses drafts apresentam o conceito de Circuitos Virtuais **(VCs).**
- Um LSP funciona como um túnel transportando vários VCs, enquanto que o VC efetivamente é o circuito que transporta os frames do usuário.



FOUNDRY NETWORKS

Tunel Label e VC Label

- Na verdade, o VC é outro LSP dentro do LSP original. O LSP de túnel faz a conexão entre dois PEs e o VC carrega os frames de um único usuário.
- Os VCs são uni-direcionais. É necessário um par de VCs para comunicação bi-direcional.
- De novo encontramos um frame contendo dois labels:
  - Um label associado ao túnel que conduz ao PE destino (**Tunnel label**)
  - Um label associado ao VC que contém os frames do usuário e conduz ao site associado ao PE destino (**VC label**)



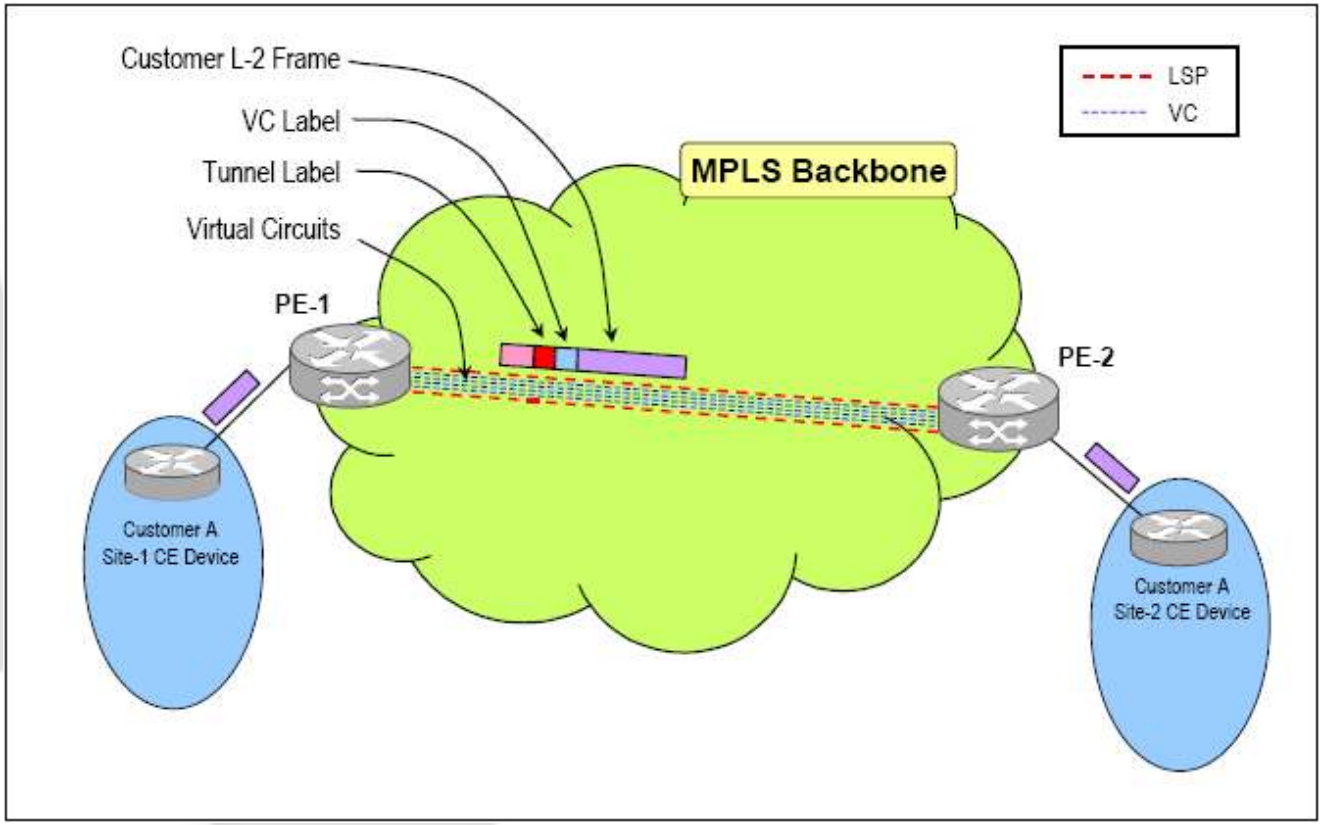
FOUNDRY NETWORKS

Mecanismo de Transporte

- Os LSPs de túnel entre os roteadores PE podem ser criados usando RSVP/ TE ou LDP. Já os LSPs de VCs sempre são criados usando- se LDP.
- Na borda da rede da operadora o roteador PE encapsula os frames do usuário, adiciona o label de VC e o label de túnel e envia o frame pelo LSP de túnel.
- Na outra ponta do LSP de túnel, o PE receptor retira o label de túnel, determina a porta de usuário para enviar o frame com base no label de VC, extrai o frame de Camada 2 original e o envia pela porta determinada.

FOUNDRY NETWORKS

Exemplo de VPN Ponto- a- Ponto



- Usando conexões ponto- a- ponto uma operadora pode oferecer serviços similares a linhas privadas ou PVCs de Frame Relay, em uma rede IP com interfaces PoS, Gig e 10 Gig

FOUNDRY NETWORKS

Conexão Ponto- Multiponto

- O objetivo é transportar frames de Camada 2 através de uma rede MPLS para múltiplos sites que compõe uma mesma VPN.
- Para uso mais eficiente da banda da operadora, o frame deve ser enviado apenas para o PE que está diretamente conectado ao site de destino, ao invés de ser transmitido para todos os PEs do backbone.
- Isso é conseguido comutando- se os frames com base no endereço MAC de destino.
- A forma popular para implementar essa solução é chamada Virtual Private LAN Service (VPLS).
- Essa tecnologia está descrita no documento “draft- lasserre- vkompellappvpn- vpls”.

FOUNDRY NETWORKS

Mecanismos Utilizados – VPN ID

- VPLS cria uma malha completa de VCs (para cada sentido de tráfego) entre os PEs que estão conectados aos sites que fazem parte da VPN.
- As VPNs dos clientes são identificadas com um **VPN ID** único, formado por 32 bits. Existem propostas para expandir esse identificador para 56 ou 64 bits e para criar um serviço de resolução de nomes entre strings de texto e os números de VPN.
- Notem que VPLS, mesmo sendo um serviço de Camada 2, não utiliza VLAN IDs para identificar a qual VPN pertence um determinado frame. Só os labels associados aos frames possuem significado para comutação através do backbone.
- Portanto, a limitação de 4095 VLANs existente em IEEE 802.1Q não se aplica a VPNs usando VPLS.

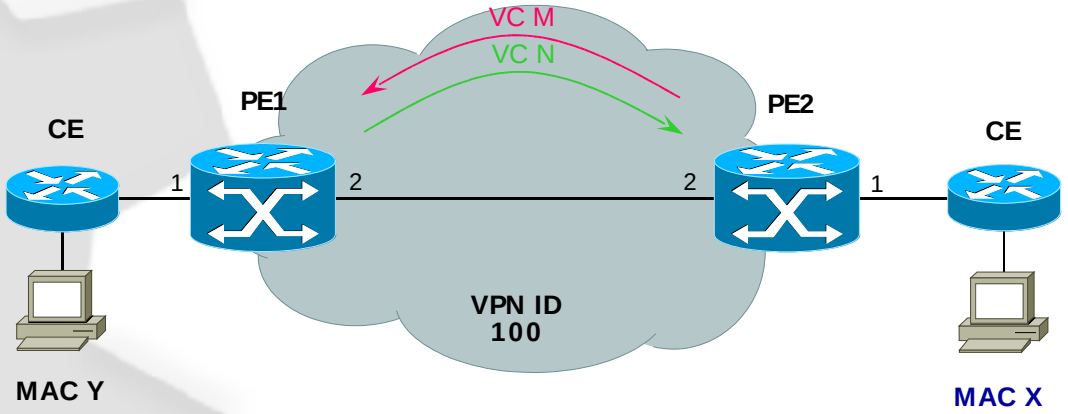
FOUNDRY NETWORKS

Mecanismo de Transporte

- Um PE mantém uma tabela separada, chamada **Virtual Forwarding Instance (VFI)**, para cada VPN que ele possui.
- Os roteadores do tipo PE aprendem endereços MAC do mesmo jeito que switches convencionais, exceto pelo fato que os frames são recebidos através de VCs e não portas físicas.
- Por exemplo, se o PE1 recebe um frame com endereço de origem **MAC X** sobre o **VC M**, ele cria uma entrada na sua tabela de endereços MAC que associa o endereço **MAC X** com o **VC N**, que é o outro VC na direção oposta de M.

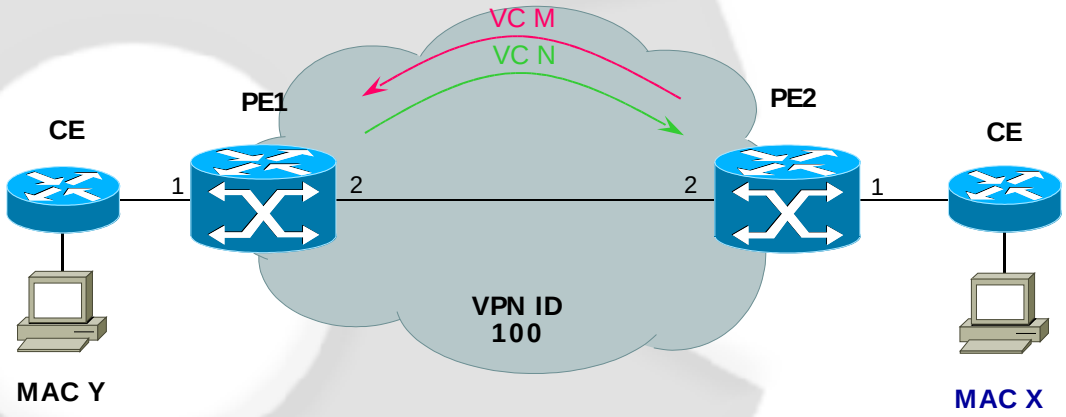
Virtual Forwarding Table para PE1

VPN ID	MAC	VC	Porta
100	X	N	- - -
100	Y	- - - - -	1



Mecanismo de Transporte

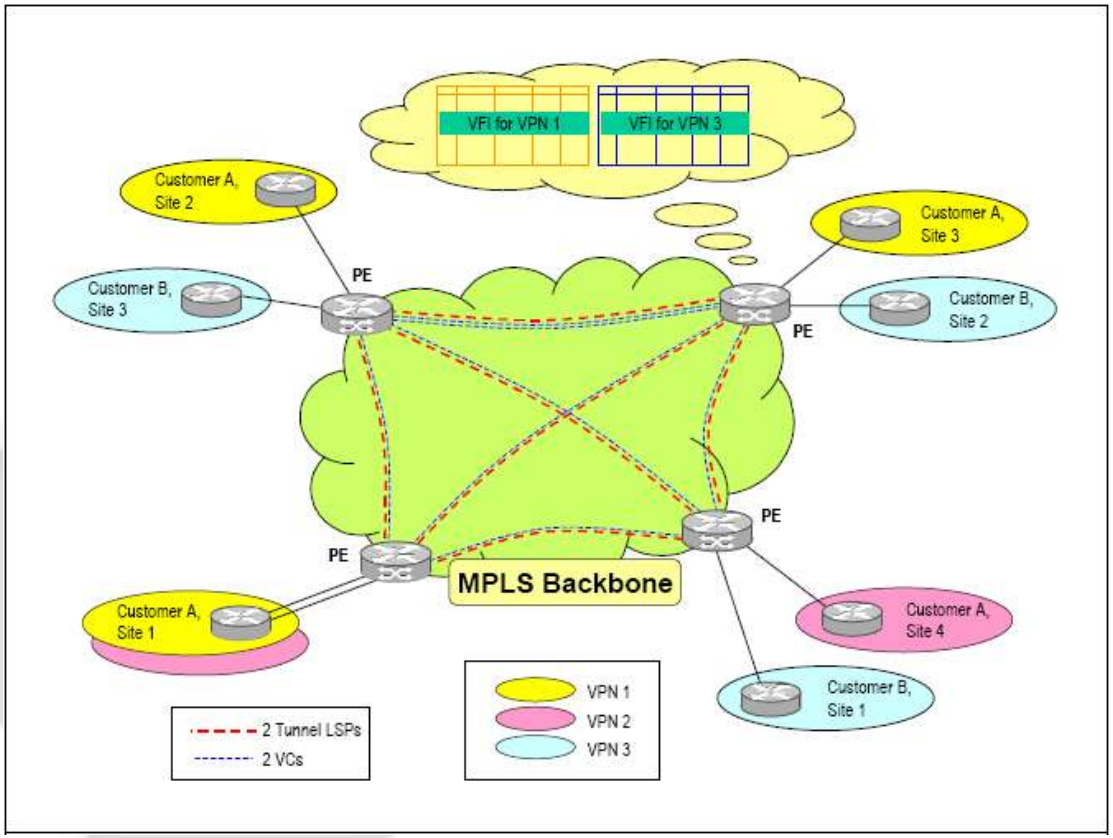
- Quando PE1 recebe um frame de um usuário diretamente conectado para o destino **X**, ele consulta a tabela de endereços e encontra a associação com o **VC N**. Assim, ele encapsula o frame e o envia pelo **VC N**.
- Se PE2 recebe um frame com destino Y, que não aparece na sua tabela de endereços, ele transmite o frame para todos os VCs da VPN. Quando chegar uma resposta com endereço de origem Y, ele cria uma entrada apontando para o VC onde Y reside.



Virtual Forwarding Table para PE2

VPN ID	MAC	VC	Porta
100	Y	M	- - -
100	X	- - - -	1

Exemplo de VPN Ponto- Multiponto



- Um PE aprende apenas os endereços MAC das VPNS que ele possui.
- Um roteador do tipo P (não está exibido – está dentro da nuvem MPLS) nunca aprende endereços MAC; eles apenas fazem comutação baseada em labels.

FOUNDRY NETWORKS

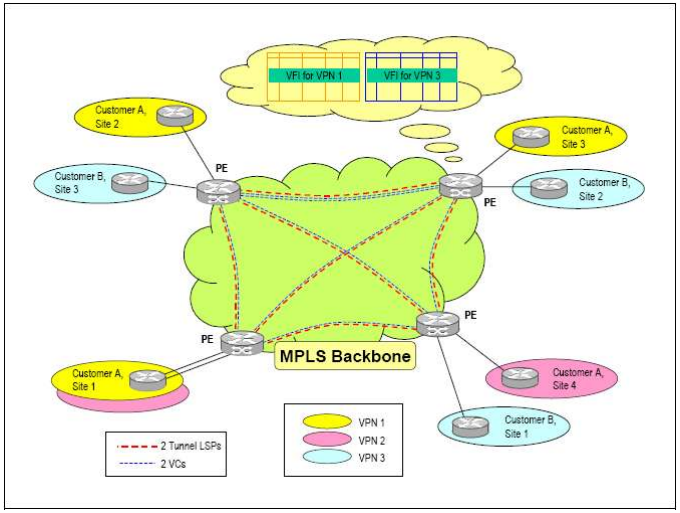
VPLS não Usa Spanning Tree

- Diferente dos switches convencionais, roteadores PE não precisam rodar Spanning Tree para implementar uma rede redundante sem loops.
- Como VPLS está baseado em MPLS, VPLS utiliza os mecanismos de proteção e recuperação existentes em MPLS.
- Além disso, como VPLS utiliza uma malha completa de VCs entre os PEs de uma VPN (um PE se conecta a qualquer outro usando apenas 1 hop), VPLS pode utilizar uma regra do tipo "split horizon" para transporta frames:
  - Se um frame de um cliente é recebido por um VC em uma VPN, esse frame só pode ser transmitido para um cliente diretamente conectado, e não de volta para a mesma VPN (usando outro VC).
- Essa regra e a malha completa de VCs permite montar redes sem loops sem usar Spanning Tree.

FOUNDRY NETWORKS

Redes Sobrepostas

- Na figura abaixo, o cliente A do site 1 participa da VPN 1 e VPN 2. Para separar o tráfego de cada VPN, o sites dos clientes podem ser conectados a portas diferentes do roteador PE, uma para cada VPN.
- Como alternativa, o tráfego pertencente às duas VPNs pode ser multiplexado sobre a mesma conexão física usando-se dois VLAN IDs diferentes. Também podem ser usados IEEE 802.1Q com VLAN aggregation para aumentar a escalabilidade das VLANs e evitar que o tag da operadora coincida com o tag do usuário.
- Ao contrário das VPNs de Camada 3, o trabalho de controlar as rotas que são anunciadas em cada VPN permanecem como responsabilidade do cliente, já que os roteadores PE não lidam com rotas.



FOUNDRY NETWORKS

Configuração Básica

- Criando uma instância de VPLS

```
PE1(config)# router mpls
PE1(config-mpls)# vpls TESTE 40000
PE1(config-mpls-vpls-TESTE)#
```

- Os demais PEs da mesma VPN devem ser configurados com o mesmo VPN ID

- Criando a malha de PEs

```
PE1(config-mpls-vpls-TESTE)# vpls-peer 192.168.2.100 192.168.2.101
```

- A malha de VCs vai ser formada entre os peers usando o protocolo LDP

- Fazendo a associação de portas físicas

```
PE1(config-mpls-vpls-TESTE)# vlan 200
PE1(config-mpls-vpls-TESTE-vlan-200)# tagged e 3/11
PE1(config-mpls-vpls-TESTE-vlan-200)# untagged e 2/1
```

FOUNDRY NETWORKS

Exibindo as VPNs

- Exibindo um sumário das instâncias de VPLS

```
PE1# show mpls vpls summary
Virtual Private LAN Service summary:
    Total VPLS configured: 1, maximum number of VPLS: 2048
    Total VPLS peers configured: 3, total peers operational: 3
    VC label allocation range size: 32
    Maximum VPLS mac entries allowed: 8192, currently installed: 200
```

- Exibindo detalhes de uma instância de VPLS

```
PE1# show mpls vpls TESTE detail
VPLS TESTE, Id 100, Max mac entries: 2048
    Total vlans: 1, Tagged ports: 1 (1 Up), Untagged ports 1 (1 Up)
      Vlan 200
        Tagged: ethe 3/11
        Untagged: ethe 2/1
    Total VC labels allocated: 32 (983040-983071)
    Total VPLS peers: 2 (2 Operational)
    Peer address: 192.168.2.100, State: Operational, Uptime: 28 min
    Tnnl: tnl0(1025), LDP session: Up, Local VC lbl: 983040, Remote VC lbl: 983041
    Peer address: 192.168.2.101, State: Operational, Uptime: 27 min
    Tnnl: tnl0(1026), LDP session: Up, Local VC lbl: 983042, Remote VC lbl: 983043
```

FOUNDRY NETWORKS

Exibindo as Tabelas

- Exibindo uma VFI

```
PE1# show mac vpls TESTE

Total VPLS mac entries in the table: 10 (Local: 5, Remote: 5)

MAC Address           L/R    VC      Port     VLAN/Peer
============      ===    ==      ====     =========
0016.0100.1501     R      983072   5/1      192.168.2.100
0016.0100.1502     R      983045   5/1      192.168.2.100
0016.0100.1503     R      983054   5/1      192.168.2.100
0016.0100.1504     L      ------   2/1      200
0016.0100.1601     L      ------   3/11     200
0016.0100.1602     R      983076   5/1      192.168.2.100
0016.0100.1603     R      983088   5/1      192.168.2.100
0016.0100.1604     L      ------   2/1      200
0016.0100.1605     L      ------   3/11     200
0016.0100.1606     L      ------   2/1      200
```

FOUNDRY NETWORKS

Camada 2 ou Camada 3?

- Vários aspectos devem ser observados para uma decisão sobre o tipo de VPN a ser usado:
  - Tipo de tráfego suportado;
  - Formas de conexão;
  - Escalabilidade;
  - Complexidade na implantação;
  - Complexidade no provisionamento dos serviços;
  - Complexidade do gerenciamento e manutenção;
  - Custos da implantação;
  - Custos do gerenciamento e manutenção.
- Esses aspectos serão analisados a seguir.

FOUNDRY NETWORKS

Tipos de Tráfego Suportado

- Obviamente, VPNs de Camada 3 suportam apenas tráfego IP. VPNs de Camada 2 suportam qualquer protocolo: IPv4, IPv6, IPX, DECNet, OSI, etc.
- Muitas empresas ainda usam outros protocolos além de IP, portanto VPNs de Camada 2 são uma opção mais interessante.
- Outro motivo para usar VPNs de Camada 2 é o suporte para IPv6. As VPNs de Camada 3 por enquanto suportam apenas IPv4. Serão necessárias modificações nos padrões e possivelmente atualização de hardware para os roteadores PE suportarem VPN-IPv6.

FOUNDRY NETWORKS

Formas de Conexão

- Existem várias topologias possíveis de conexão:
  - 1. Ponto-a-ponto
  - 2. Estrela
  - 3. Malha parcial
  - 4. Malha completa
  - 5. VPNs sobrepostas
- Uma VPN de Camada 3 funciona bem nos cenários 1, 4 e 5, permitindo acesso transparente aos roteadores CE.
- Uma VPN de Camada 2 funciona bem nos cenários 1, 2, 3 e 4. Nos cenários 2 e 3 é mais fácil usar VCs em Camada 2 do que controlar rotas com BGP em Camada 3.
- O cenário 5 também é viável usando Camada 2, mas requer mais configurações no CE onde ocorre sobreposição: ele terá que controlar quais rotas são anunciadas em cada VPN, por isso essa forma não é tão transparente como em Camada 3.

FOUNDRY NETWORKS

Escalabilidade

- Há semelhanças na escalabilidade de VPNs de Camada 2 e Camada 3. Um limitante para ambas soluções é o número máximo de LSPs e/ou VCs suportados em um LSR.
- Outro fator limitante é o tamanho máximo do arquivo de configuração que pode ser armazenado em um roteador PE, visto que o arquivo de configuração conterá informação sobre todas as VPNs dos clientes:
  - Em Camada 3 o arquivo contém definições de VRFs, RDs, comunidades estendidas e políticas de BGP.
  - Em Camada 2 o arquivo contém definições de VPN IDs, VCs com cada PE remoto e portas físicas associadas a cada VPN. Usar serviços de auto-discovery permite diminuir bastante o tamanho do arquivo de configuração.
- Em Camada 3, outro limitante é o número de rotas que pode ser armazenada em cada PE, porque cada VPN (ou VRF) terá seu próprio conjunto de rotas. Usar sumarização de rotas alivia esse prolema.
- Em Camada 2, outro limitante é o número de entradas nas tabelas de endereços em cada PE. Isso pode ser aliviado limitando-se o número de endereços MAC admitidos em cada VPN.

FOUNDRY NETWORKS

Implantação

- A implantação de uma solução de Camada 3 requer LSRs de alto desempenho capazes de manipular múltiplas tabelas de roteamento e comutação na borda de rede. Ela também exige o uso de BGP peering entre esses roteadores. Se o provedor já usa BGP extensivamente, uma VPN de Camada 3 faz bastante sentido.
- Em uma implantação de Camada 2 os roteadores PE podem ser mais simples, porque não é necessário estabelecer sessões BGP entre os peers. Essa é uma boa solução para provedores que não utilizam BGP maciçamente.
- Em qualquer caso, devem ser configurados os LSPs entre os PEs para o transporte dos dados de um PE para outro.

FOUNDRY NETWORKS

Provisionamento

- Para uma solução de Camada 3, o provisionamento de serviço vai exigir desenhar toda a topologia de roteamento requerida pelo cliente. Isso implica definir a relação de VPNs com os VRFs, (um VRF por VPN ou uma VRF para várias VPNs) configurar cada VRF contendo os conjuntos de rotas de cada VPN, os valores para RD e Route Target para cada VPN e finalmente todas as regras de BGP que irão compor as VRFs de cada VPN.
- Provisionar uma solução de VPN em Camada 2 é mais simples. Cada PE de uma VPN necessita estabelecer VCs com os demais PEs da mesma VPN. A seguir, as portas físicas dos PEs são mapeadas para a VPN desejada. Já estão disponíveis protocolos de auto- discovery que tornam o trabalho de configuração manual dos VCs desnecessário.

FOUNDRY NETWORKS

Gerenciamento

- Gerenciar uma VPN de Camada 3 é mais complicado, porque a maior parte do trabalho de configuração e troubleshooting envolve lidar com as sessões de BGP e políticas de distribuição de rotas. Além disso, cada VPN corresponde a um VRF com sua própria tabela de roteamento e políticas de BGP individuais, ao invés de uma única tabela e políticas globais. Os arquivos de configuração ficam bastante grandes, o que dificulta a procura de erros na configuração.
- Uma solução de Camada 2 é mais simples porque o provedor não precisa lidar com as rotas dos clientes nem controlar sua distribuição. Como não é necessário usar BGP, as tarefas de gerenciamento e troubleshooting ficam muito mais simples. As atividades que sobram são a configuração dos VCs que constituem a VPN e as portas associadas à VPN, além da monitoração das tabelas de endereços MAC e VCs para cada VPN (VFIs).

FOUNDRY NETWORKS

Custos

- Normalmente uma solução de Camada 3 será mais custosa que uma solução de Camada 2, devido ao fato que os equipamentos que suportam VPNs de Camada 3 são mais sofisticados e potentes.
- Da mesma forma, os custos de implantação, gerenciamento e manutenção são maiores para uma VPN de Camada 3, pelas mesmas razões apresentadas no slide anterior.

FOUNDRY NETWORKS

Conclusões

- Uma VPN de Camada 3 suporta apenas IP com roteamento, suportando múltiplas VPNs usando políticas de rotas definidas por BGP.
- Soluções de Camada 2 são uma abordagem mais nova para criação de VPNs. Ela oferece uma solução de comutação de frames de Camada 2, o que torna a VPN transparente para qualquer protocolo de Camada 3. São usados circuitos virtuais para criação das múltiplas VPNs.
- A escolha de uma ou outra abordagem deve considerar os pontos fortes e fracos de cada alternativa, os requisitos atuais e futuros do serviço a ser implantado, a infra-estrutura existente e os custos envolvidos.

FOUNDRY NETWORKS

Referências

- White Paper “IP/MPLS-Based VPNs Layer-3 vs Layer-2 http://www.foundrynet.com/solutions/appNotes/MPLS_L3vsL2.htm