ARTIGO Nº 11

TIPOS DE VPN PARA TRANSPORTE DE ETHERNET (EVPNs)

1 - OBJETIVO

O objetivo do presente artigo é o de apresentar os fundamentos das tecnologias de VPN (Virtual Private Networks) utilizadas para o transporte de Ethernet, ou seja, das EVPNs (*Ethernet VPNs*).

Redes virtuais são redes que compartilham uma rede física, identificadas por alguma forma própria de identificação, sendo utilizadas por um grupo de usuários para isso autorizados. Para esses usuários, tudo se passa com se estivessem em uma rede física própria.

Como cada uma dessas redes virtuais são de uso privativo de um tipo de entidade, elas são referidas como redes virtuais privativas (VPNs). Uma EVPN é uma VPN que transporta tráfego Ethernet.

Ressaltamos que, embora existam os diversos tipos de EVPN que abordaremos neste artigo, as *BGP MPLS-Based EVPNs,* que constituem um desses tipos, é referido na literatura, inclusive nos textos de RFCs, como EVPN.

2 – INTRODUÇÂO

As redes Ethernet, que a princípio se resumiam em LANs Ethernet, operando apenas em âmbito local, passaram a operar também como redes (LANs) Bridged Ethernet, ou redes (LANs) Switched Ethernet (*Ethernet Bridged LANs ou Ethernet Switched LANs*), a partir da emissão do padrão IEEE 802.1D (cuja última versão data de 2004). Passaremos a nos referirmos a essas redes como redes Bridged Ethernet.

Posteriormente, foi publicado o padrão IEEE 802.1Q (cuja última versão data de 2014), que introduziu o conceito de VLAN (*Virtual LAN*), dando início ao estabelecimento de EVPNs. VLANS são EVPNs identificadas por meio de VLAN IDs (*VLAN Identifiers*), também referidos como VIDs.

Tanto as redes Bridged Ethernet IEEE 802.1D-2004, quanto as redes Bridged Ethernet IEEE 802.1Q-2014, operam com *LAN Bridging* baseada em *Spanning Trees*.

Observamos que continuamos a denominar as redes bridged Ethernet na versão inicial do padrão IEEE 802.1Q como redes 802.1Q, embora a última versão do padrão IEEE 802.1Q, de 2014, tenha passado a incluir outros tipos de EVPN, como o PB e o PBB, que serão vistos adiante neste artigo.

Spanning Trees são árvores lógicas constituídas sobre redes Bridged Ethernet físicas com redundância de links, de modo a possibilitar a condução do tráfego de dados sem a ocorrência de loops.

A definição de VLANs possibilitou, dentre outros aprimoramentos, a constituição de MSTPs (*Multiple Spanning Trees*), que são árvores múltiplas dedicadas a cada uma das VLANs ou a determinados subgrupos de VLANs. Dessa forma, reduz-se significantemente o tráfego de overhead do algoritmo *Spanning Tree* assim como as distâncias percorridas por quadros de dados unicast com endereços MAC de destino aprendidos.

Citamos também a filtragem do tráfego de dados proporcionado pelo protocolo MVRP (Multiple VLAN Registration Protocol), que limita a condução de tráfego de uma dada VLAN em uma Spanning Tree, apenas por portas de bridge registradas para essa VLAN.

As redes 802.1Q, por sua reduzida escalabilidade (uma única instância de serviço com 4096 VLAN IDs), restringem-se normalmente ao atendimento de um único usuário. Devido à enorme aceitação dessas redes, por sua simplicidade e por baixo custo, formou-se um número elevado de sites Ethernet, dispersos principalmente pelos grandes centros.

Constatou-se então a necessidade de constituição de redes de provedores de maior escalabilidade, sob a forma de EVPNS, com o propósito de interligar esses sites Ethernet de usuário.

As redes IEEE 802.1Q, além de não possuírem escalabilidade suficiente para esse propósito, apresenta coincidência total entre os endereços MAC de usuários e os endereços MAC do provedor, o que representa uma outra limitação.

Foram então definidas várias alternativas de EVPN de provedores, baseadas em diferentes tecnologias de rede de transporte, que apresentam a seguinte classificação geral:

- EVPNs de provedor com transporte por Ethernet;

- EVPNs de provedor com transporte por camada 3;

- EVPNs de provedor com transporte por MPLS;

- *Carrier Ethernet.*

Registramos a existência de tecnologias para o transport6e Ethernet sobre redes modo circuito, como SDH, OTN, WDM ou mesmo as próprias fibras ópticas. Tais tecnologias, genericamente referidas EoSDH, EoOTN, etc.

Com esse propósito, são utilizados o protocolo LAPS (*link Access Procedure – SDH*), especificamente para SDH, e protocolo GFP (*Generic Framing Procedure*), aplicável

indistintamente para SDH, OTN, WDM e fibras ópticas, além de outras tecnologias estranhas ao Ethernet.

Não incluímos essas tecnologias em nosso artigo, por se tratar de formas de transporte de Ethernet transparentes a VLANs ou a qua6lquer outra forma de identificação de instâncias de serviço, não caracterizando assim a operação por EVPNs.

3 – EVPNs de PROVEDOR com TRANSPORTE por ETHERNET

As EVPNs de Provedor com transporte por Ethernet foram definidas em dois diferentes paradigmas:

- *LAN Bridging* com *Spanning Trees*;

- *LAN Bridging* com IS-IS (*Intermediate System-to-Intermediate System*).

3.1 – LAN Bridging com Spanning Trees

esse paradigma, as EVPNs de provedor operam da mesma forma que as redes IEEE 802.1D-2004 e IEEE 802.1Q-2014 iniciais, onde o tráfego unicast e as inundações da rede ocorrem dentro de *Spanning Trees*.

Foram definidos dois tipos de VLANs de provedor pelo IEEE:

- PB (*Provider Bridging*);

- PBB (*Provider Backbone Bridging*).

O PB e o PBB foram inicialmente especificados em padrões do IEEE próprios, mas hoje se encontram-se incorporados ao padrão IEEE 802.1Q-2014.

3.1.1 – PB (*Provider Bridging*)

O PB foi inicialmente especificado no padrão IEEE 802.1ad, hoje obsoletado, sendo a sua especificação incorporada ao padrão IEEE 802.1Q-2014, nas Seções 15 e 16.

No PB, a rede do provedor encapsula os quadros MAC dos usuários apenas por um *VLAN-Tag*, referido como *S-Tag* (*Service Tag*), no interior do qual se encontram os 4096 S-VIDs identificadores das S-VLANs. Por essa razão, o PB é também denominado *Q-in-Q Bridging.*

Como se observa na Figura 1, o *S-Tag* foi inserido entre o endereço MAC de origem (MAC SA) e o *C-Tag* (*customer tag*).

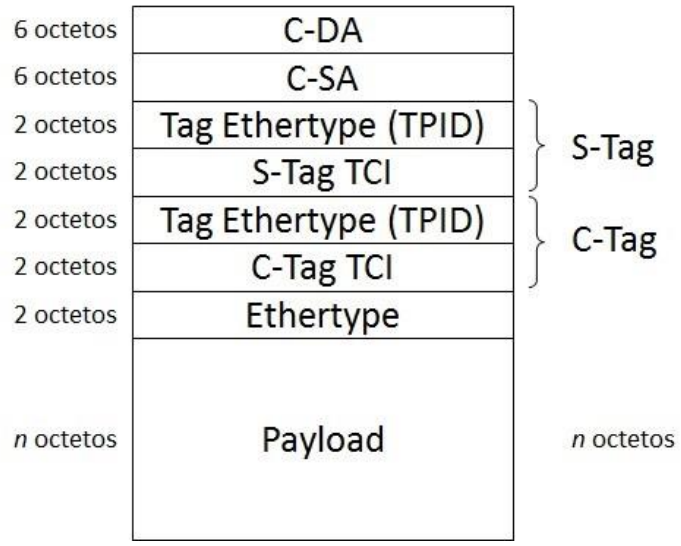


Figura 1 – Formato básico de um quadro PB.

Nessa figura, o campo *Tag Ethertype* (TPID), com dois octetos, identifica o *S-Tag*, com o valor hexadecimal 0x88A8. O campo *S-Tag TCI* (*Tag Control Information*), também com dois octetos, contém o S-VID (12 bits), além do PCP (*Priority Code Point*), com três bits e do bit DEI (*Drop Elegible Indicator*).

Lembramos que a cada uma das 4096 instâncias de serviço (representadas pelos 4096 S-VIDs) pode transportar teoricamente até 4096 VLANs.

Os quadros de usuário envelopados por um *S-Tag* podem pertencer a uma única C-VLAN (*Customer VLAN*), a um conjunto de C-VLANs identificadas (podendo consistir inclusive na totalidade de C-VLANs), o que representa o acesso *VLAN-based,* ou à totalidade de C-VLANs não identificadas, o que representa o acesso *port-based*.

Como se conclui do parágrafo anterior, o PB, embora seja uma forma de constituição de redes virtuais, admite o acesso *port-based,* o que descaracteriza *a* virtualização do serviço. O mesmo ocorre com o PBB.

Como as bridges no interior de uma rede PB, referida como PBN (*PB Network*), são transparentes aos *C-Tags*, o domínio broadcasting (domínio de inundação) de uma S-VLAN é delimitado pelo S-VID.

3.1.2 – PBB (Provider Backbone Bridging)

O PBB foi definido com o propósito de eliminar as limitações básicas do PB, que são a promiscuidade entre os endereços do provedor e dos usuários e a reduzida escalabilidade.

Para eliminar a primeira dessas limitações, o PBB passou a envelopar os quadros de usuário não apenas por um *VLAN-Tag*, mas por um cabeçalho MAC completo, referido como cabeçalho B-MAC (*Backbone MAC*). Por essa razão, o PBB é também referido como *MAC-in-MAC Bridging*, ou simplesmente *MAC-in-MAC*.

Dessa forma, o PBB passou a contar com os endereços B-MAC de origem (B-SA) e B-MAC de destino (B-DA), além do *B-Tag*. O *B-Tag* opera da mesma forma que o *S-Tag* no PB, existindo então as B-VLANS e os B-VIDs.

Quando da aprendizagem de endereços MAC de usuário (endereços U-MAC), os PEs da PBBN (*PBB Network*) aprendem também a associação entre o endereço U-MAC aprendido e o correspondente endereço B-MAC. Dessa forma, um PE de origem fica habilitado a montar o quadro MAC completo para transmissão na PBBN.

Para a solução da segunda limitação do PB, que diz respeito à sua reduzida escalabilidade, foi acrescido no PBB um novo *tag*, referido como I-TAG (*Instance Tag*), sobreposto ao *B-Tag,* destinado exclusivamente à multiplexação estatística do B-VID de forma a ampliar o número de instancias de serviço, e consequentemente ampliar a escalabilidade.

Não existem consequentemente as I-VLANs.

Como existem 4096 instâncias de serviço providas por B-VIDs, e como cada B-VID passa a corresponder a 4096 I-SIDs (*Instance Service Identifiers*), o PBB é capaz de oferecer o limite teórico máximo superior a 16 milhões de instâncias de serviço (de I-SIDs). Lembramos que cada I-SID é capaz de transportar teoricamente até 4096 VLANs.

O PBB pode atender diretamente os usuários, ou o atendimento ocorre com a intermediação de PBNs. Nesse último caso, a escalabilidade da rede é ampliada teoricamente 4096 vezes.

A Figura 2 exibe o formato completo de um quadro de dados PBB.

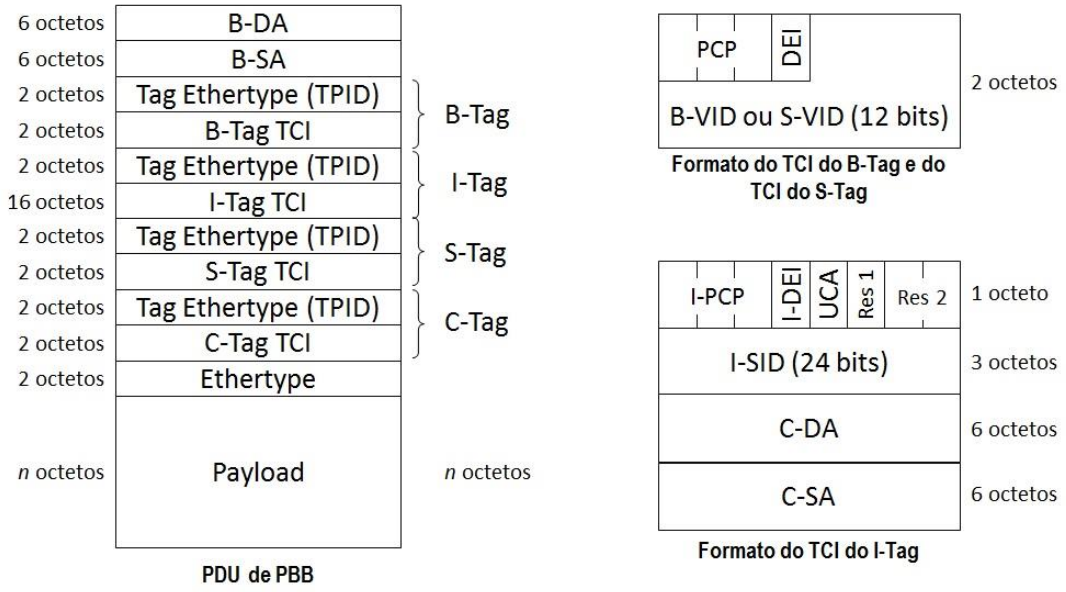


Figura 2 – Formato de um quadro PBB.

Constata-se nessa figura a utilização de PBN intermediando o acesso dos usuários à PBBN.

Registramos que o valor 0x88A8 aplica-se tanto para o S-Tag TPID quanto para o B-Tag TPID.

A Figura 3 ilustra um exemplo de PBBN, onde se constata o uso de PB.

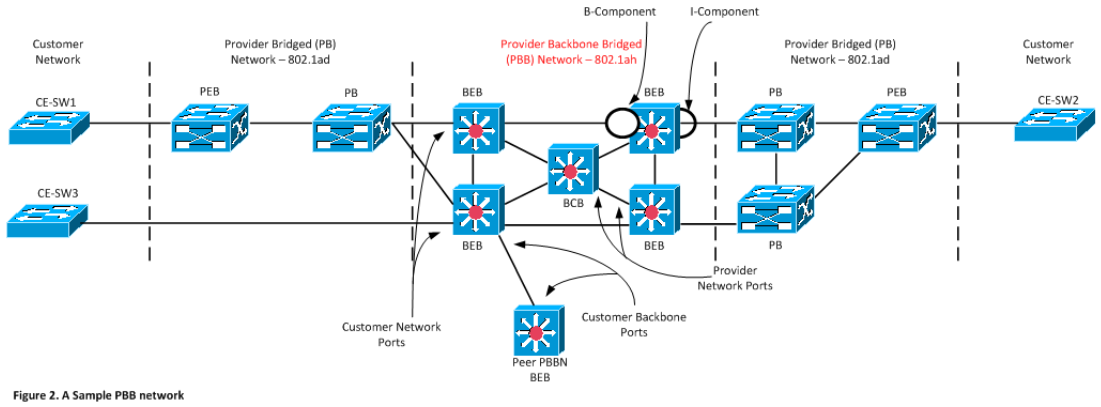


Figura 3 – Exemplo de PBBN com o uso de PB.

Como no caso do PB, o PBB oferece acessos *port-based,* além dos acessos *VLAN-based.*

3.2 – LAN Bridging com IS-IS

Conforme palavras de Radia Perlman, a própria criadora do mecanismo *Spanning Trees*, esse mecanismo representa uma baixa eficiência no uso dos recursos das redes Ethernet que o utiliza. Ironicamente, foi também Radia Perlman quem também criou uma das alternativas de solução que evita a utilização de *Spanning Trees,* a tecnologia TRILL (*Transparent Interconnection of Lots of Links*), além de ter criado o protocolo IS-IS, que se constitui na base das alternativas ao uso de *Spanning Trees*, ou seja, o SPB (*Shortest Path Bridging*) e o TRILL.

O IS-IS (*Intermediate Systems -to- Intermediate Systems*), definido no padrão ISO/IEC 10589 e referendado na RFC 1195 (*Use of OSI IS-IS protocol for Routing In TCP/IP and Dual Environments*), é um protocolo de roteamento *link-state* equivalente ao OSPF, sendo ambos utilizados no processo de roteamento intra-AS do TCP/IP, ou seja, no roteamento IGP do TCP/IP.

Para possibilitar roteamento *link-state* IS-IS em diferentes tecnologias de rede de camada 2, como por exemplo redes Ethernet, foi emitida a RFC 6165 (*Extensions to IS-IS for Layer-2 Systems*), definindo extensões do IS-IS cm esse propósito.

3.2.1 – SPB (Shortest Path Bridging)

O SPB foi definido inicialmente no padrão IEEE 802.1aq (*Shortest Path Bridging*), sendo a sua definição posteriormente incorporada ao padrão IEEE 802.1Q-2014, cláusulas 27 e 28.

Foram especificados dois modos de operação para o SPB:

- SPBV (SPB-VID);

- SPBM (SPB-MAC).

O SPBV e o SPBM eram referidos inicialmente como SPB e SPBB (*Shortest Path Backbone Bridging*), respectivamente. A sigla SPB passou a referir-se ao SPB como um todo na nova terminologia.

O SPBV e o SPBM adotam planos de dados próprios, mas utilizam no plano de controle um único conjunto de extensões do protocolo IS-IS, extensões essas referidas como protocolo ISIS-SPB. O ISIS-SPB foi definido na RFC 6329 (*IS-IS Extensions Supporting IEEE 802.1aq Shortest Path Bridging*).

O plano de dados do SPBV tem como base o encapsulamento utilizado no plano de dados do PB. As bases de dados de filtragem são calculadas e instaladas para VIDs unidirecionais, referidos como SPVIDs (*Shortest Path VIDs*).

Como no SPBV (diferentemente do SPBM) as rotas utilizadas pelo ISIS-SPB não constam dos quadros de dados enviados nas redes, ocorre a aprendizagem de endereços MAC das estações finais em todas as bridges da rede SPBV (como nas redes PB).

O SPBM, por sua vez, tem o seu plano de dados baseado no plano de dados do PBB, sendo a sua utilização indicada para aplicações onde é requerido o completo isolamento entre os endereços da rede e os endereços dos usuários e/ou maior escalabilidade.

A transmissão de quadros de dados no SPBM requer a associação entre os endereços MAC da estação final de destino e o endereço MAC da bridge de borda da rede SPBM, referida como BEB (*Backbone Edge Bridge*). Os endereços MAC das BEBs são referidos como endereços B-MAC (*Backbone MAC Addresses*), como no PBB.

As associações entre endereços mencionada no parágrafo anterior ficam registradas na BEB de origem quando da transmissão de um quadro de dados. Como no PBB, é desnecessária a aprendizagem de endereços MAC de estações Ethernet finais pelas bridges no interior da rede SPBM, bridges essas referidas como BCBs (*Backbone Core Bridges*).

3.2.2 – TRILL (Transparent Interconnection of Lots of Links)

O TRILL representa uma iniciativa do IETF na mesma linha do SPB definido no padrão IEEE 802.1Q-2014, onde a extensão do IS-IS para redes de camada 2 é utilizado para roteamento.

O TRILL possui, contudo, uma amplitude operacional mais ampla que o SPB, podendo ser utilizada não só Ethernet, mas também outros protocolos, como o PPP e PWs, por exemplo, na interligação de RBridges, o que justifica o termo “transparente” em sua denominação.

Para a definição do TRILL, foram emitidas diversas RFCs, dentre as quais destacamos as seguintes:

- RFC 5556 (*Transparent Interconnection of Lots of Links (TRILL): Problem and Applicability Statement*);

- RFC 6325 (*Routing Bridges (RBridges): Base Protocol Specification*);

- RFC 7172 (*TRILL: Fine-Grained Labeling*);

- RFC 7357 (*TRILL: End Station Address Distribution Information (ESADI) Protocol*).

O TRILL, que possibilita a transmissão de tráfego multicast/broadcast em adição ao tráfego unicast, utiliza um novo tipo específico de bridge, referido como *RBridges* (*Routing Bridges*).

Os quadros MAC nativos recebidos são encapsulados na *RBridge* de ingresso pelo *TRILL header,* transmitidos na rede TRILL com base em roteamento IS-IS, e desencapsulados na *RBridge* de egresso.

A estrutura dos quadros de dados do TRILL encontra-se na Figura 4.

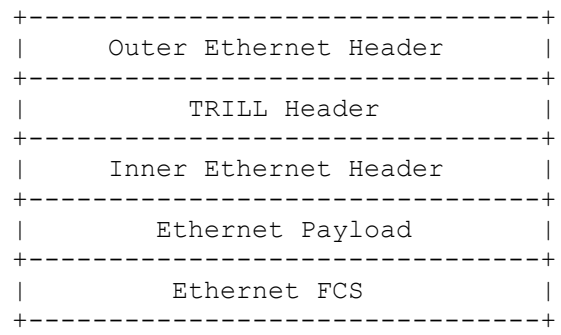


Figura 4 – Estrutura dos quadros de dados do TRILL.

Verifica-se, nessa figura, o envelopamento do quadro Ethernet nativo (*Inner Ethernet*) pelo *TRILL header*, que por sua vez encontra-se encapsulado pelo *outer header* (que pode ser Ethernet, PPP, PW ou mesmo outros).

Foram definidos dois tipos de serviço no TRILL:

- VL (*VLAN-Labeled*) TRILL;

- FGL (*Fine-Grained Label*) TRILL.

No VL TRILL, um quadro de dados Ethernet MAC nativo, com o seu *VLAN-Tag*, é envelopado em um quadro de dados do TRILL sem que se acrescente qualquer tipo de *VLAN -Tag.* Dessa forma, os únicos labels disponíveis para uso são os 4096 VLAN-IDs do quadro MAC Ethernet nativo (*Inner Ethernet)*.

Essa escala de VLAN-IDs, que equivale à escala das redes IEEE 802.1Q-2014 iniciais, foi considerada insuficiente para o atendimento de aplicações de maior vulto. Definiu-se então o FGL TRILL, na RFC 7172, que, como o PB e o SPBV, oferecem 4096 instâncias de serviço, cada uma delas podendo mapear teoricamente até 4096 VLAN IDs.

Um FGL resulta da inclusão de um segundo *VLAN-Tag* no quadro de dados do TRILL, quando do ingresso do respectivo quadro de dados MAC nativo na rede TRILL. Essa inclusão ocorre na parte superior do cabeçalho MAC nativo, envelopando o VLAN-Tag nativo. Por essa razão, o *VLAN-Tag* incluído é referido, na estrutura do quadro de dados do FGL TRILL, como a *Inner.Label High Part*. O *VLAN-Tag* nativo, por sua vez, passa a ser denominado *Inner.Label Low Part.*

Registramos, por fim, o uso do protocolo ESADI (*End Station Address Distribution Information Protocol (ESADI) Protocol*). O ESADI representa o uso antecipado de uma concepção que veio a ser adotada nas *Virtual Extensible LANs* (VXLANs) e nas *BGP MPLS-Based EVPNs,* concepção essa que consiste na definição dos caminhos direcionados para quadros Ethernet unicast no plano de controle.

Como sabemos, isso ocorre tradicionalmente por aprendizagem de endereços MAC no plano de dados, o que resulta em elevado desperdício de recursos de redes Ethernet.

4 – VXLAN (VIRTUAL EXTENSIBLE LAN)

VXLAN representa a única tecnologia de constituição de EVPNs com transporte por camada 3 apresentada neste artigo. VXLAN é um exemplo de rede em overlay com encapsulamento por UDP, sendo outros exemplos o protocolo LISP (*Locator/ID Separation Protocol*), definido na RFC 6830, e a tecnologia OTV (*Overlay Transport Virtualization*), ainda em fase de padronização no IETF.

VXLAN, definida na RFC 7348 (*Virtual eXtensible Local Area Network (VXLAN): A Framework for Overlaying Virtualized Layer 2 Networks over Layer 3 Networks*), é uma tecnologia de overlay concebida para o provimento de serviços de conectividade de camada 2 e de camada 3 sobre uma rede IP genérica.

A virtualização de servidores em *Data Centers* (DCs) tem causado uma crescente disponibilização de VMs (*Virtual Machines*) com endereços MAC próprios, o que se reflete na constituição de um número elevado de VLANs, ultrapassando a sua escala de 4096 segmentos. Esse problema acentua-se pelo uso dos *Data Centers* por múltiplas entidades (*tenants*).

O tráfego de quadros Ethernet ocorre não só entre DCs, mas também no interior de grandes DCs.

Para aliviar essa situação, os administradores de rede têm optado pelo uso compartilhado de redes físicas mediante virtualização. Esses administradores estão no momento optando por redes IP na interconexão das redes físicas, para obter maior eficiência no uso da rede proporcionada pela transmissão multicaminhos (*multipath*) que caracteriza a disponibilidade de ECMP em redes IP.

Ademais, as redes IP proveêm escalabilidade, desempenho e recuperação de falhas de forma aprimorada.

VXLAN é um exemplo de compartilhamento de uma rede IP por redes de camada 2 virtuais. Embora definida dessa forma ampla, VXLAN é geralmente utilizada como uma

rede *MAC-in-UDP,* onde quadros MAC Ethernet de dados originais (*inner Ethernet*) são envelopados sucessivamente por um cabeçalho VXLAN (8 bytes), um cabeçalho UDP (8 bytes), um cabeçalho IP (20 bytes) e um cabeçalho MAC da *outer Ethernet* (14 bytes).

O quadro de dados assim formado é eventualmente referido como quadro VXLAN IP UDP, e o seu formato encontra-se representado na Figura 5.

Cabeçalho Ethernet Externo
Cabeçalho IP Externo
Cabeçalho UDP Externo
Cabeçalho VXLAN
Quadro Ethernet Original

Figura 5 – Formato do quadro VXLAN IP UDP.

VXLAN opera como uma aplicação do IP, com UDP, cujo *Port Number* default é igual a 4789.

O cabeçalho Ethernet externo (*outer Ethernet)* objetiva transportar os pacotes IP entre os pontos de terminação de ingresso e de egresso no túnel virtual constituído na rede VXLAN, representando assim uma sub-rede IP no domínio VXLAN.

Esses pontos de terminação são referidos como VTEPs (*Virtual Tunnel Endpoints*). Os VTEPs representam bridges Ethernet virtuais que interfaceiam, de um lado, a rede Ethernet transportada, e do outro lado, a rede IP transportadora.

Os quadros MAC Ethernet originais são envelopados pelos VTEPs de ingresso e desenvelopados pelos VTEPs de egresso.

A Figura 6 exibe a configuração básica de uma rede VXLAN.

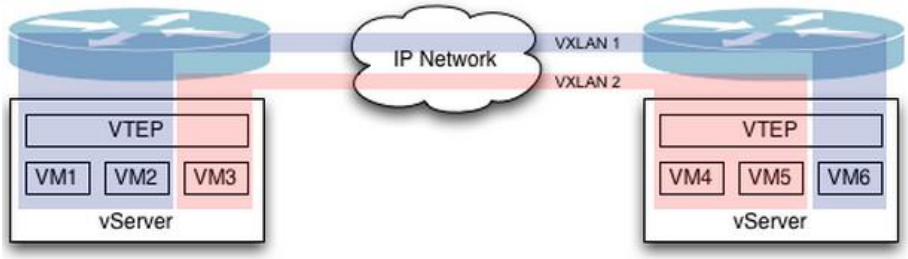


Figura 6 – Configuração básica de uma rede VXLAN.

Observa-se nessa figura a utilização de duas VXLANs (VXLAN 1 e VXLAN 2).

No cabeçalho VXLAN encontra-se um campo referido como VNID (*Virtual Network Identifier*), que identificam as instâncias virtuais de serviço das VXLANs. Essas instâncias se serviço são denominadas VNIs (*Virtual Network Instances*).

A Figura 7 representa o formato do cabeçalho VXLAN.

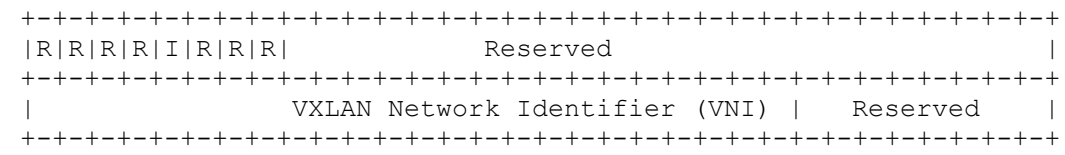


Figura 7 – Formato do cabeçalho VXLAN.

O campo VNID possui 24 bits, o que representa a elevada escalabilidade de cerca de 16,7 milhões de VNIs em uma rede VXLAN.

Dos oito bits *flags* disponíveis, apenas o quinto bit (bit I) é atualmente utilizado. O valor 1 nesse bit indica tratar-se de um VNID válido. Os demais bits estão reservados.

Diferentemente de outras tecnologias de EVPN, como por exemplo PB e PBB, as instâncias da rede *underlay* (rede IP, no caso de VXLAN) não são multiplexadas estatisticamente pelas VLANs. Ocorre em VXLAN, diferentemente, o mapeamento um para um entre VLAN IDs e VNIDs. O aumento de escala decorre do maior número de VNIDs.

Em sua fase inicial, quando definida apenas na RFC 7348, VXLAN utiliza aprendizagem da associação entre endereços MAC de estações finais (possivelmente VMs) e endereços IP de VTEPs, no plano de dados, no que se denomina modelo "*flood-and-learning*". Isso significa que a aprendizagem fica na dependência da ocasionalidade de ocorrência de transmissão de tráfego de dados pela estação final que se deseja alcançar.

Posteriormente, passou-se a utilizar o protocolo de controle MP-BGP EVPN com essa finalidade, com base na RFC 7342. Dessa forma, o plano de controle e o plano de dados foram separados, tanto para a camada 2 quanto para a camada 3. Isso reduz a carga de tráfego de overhead resultante da frequente ocorrência de inundação da rede para quadros de dados unicast com endereços de destino desconhecidos, antes existente.

5 – EVPNs com TRANSPORTE por MPLS

MPLS é uma tecnologia ampla de redes comutadas modo pacote, por oferecer diferentes opções de serviço de rede (MPLS baseado em LDP, MPLS-TE e MPLS-TP) e diferentes opções de aplicações (MPLS Público, BGP MPLS/IP VPNs, VPWS, VPLS, IPLS, e mais recentemente *BGP MPLS-Based EVPNs*).

As aplicações do MPLS podem ser classificadas de acordo com os tipos de rede interconectadas. Assim, por exemplo, o MPLS Público e as BGP MPLS/IP VPNs destinam-se à interconexão de redes IP.

Por sua vez, o VPLS e as *BGP MPLS-Based EVPNS* dedicam-se à interligação de redes Ethernet, em configuração ponto a ponto ou multiponto. O VPWS atende a uma multiplicidade de redes, apenas em configuração ponto a ponto, dente as quais as redes

Frame Relay, ATM e Ethernet. Em resumo, redes Ethernet podem ser interligadas, utilizando MPLS, por VPWS, VPLS e *BGP MPLS-Based EVPNS.*

As *BGP MPLS-Based EVPNs*, daqui para frente referidas apenas como EVPNs, foram definidas em decorrência de limitações apresentadas pelo VPLS.

5.1 – Embasamento para VPWS e VPLS

Nesse ponto, o leitor interessado pode consultar o livro TCP/IP sobre MPLS de minha autoria, que se encontra disponível para acesso gratuito no portal WirelessBrasil.com.br, onde se encontram descrições detalhadas do VPWS e VPLS.

A RFC 3985 (*Pseudowire Emulation Edge-to-Edge (PWE 3) Architecture*) descreve a arquitetura PWE 3 para a emulação de PWs (*pseudowire*) para o transporte de quadros de dados de diferentes tipos de rede, tais como ATM, Frame Relay, Bridged Ethernet e SDH, por exemplo. Esse transporte ocorre sobre redes PSN (*Packet Switching Networks*), tendo como PSN redes IP e redes MPLS.

PWs são mecanismos que transportam os elementos essenciais de um serviço emulado, de PE para um outro PE (PW ponto a ponto) ou para outros PEs (PWs ponto a multiponto). Uma função primordial de PWs é a de poder multiplexar estatisticamente os túneis da PSN (*PSN tunnels*) que os transportam.

A Figura 8 exibe a representação da arquitetura PWE 6.

Payload
Encapsulamento (Opcional)
Demultiplexador PW
Convergência na PSN (opcional)
PSN
Enlace de Dados
Camada Física

Figura 8 – Arquitetura PWE 3.

Para o caso particular em que a PSN é uma rede MPLS, foi emitida a RFC 4447 (*Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP)*). Essa RFC especifica um protocolo básico para o estabelecimento e a manutenção de PWs de qualquer tipo, como VPWS PWs e VPLS PWs, para a transmissão em quadros MPLS por túneis de PSN, protocolo esse que representa extensões do MPLS LDP (*Label Distribution Protocol*).

No contexto da RFC 4447, o demultiplexador da Figura 3 anterior é um label MPLS obrigatoriamente no formato genérico, denominado *PW label*, e os PWs são mapeados em LSPs. A PSN é representada por um label de túnel LSP, e os campos opcionais não são normalmente utilizados.

Resulta, nos termos da RFC 4447, a arquitetura PWE 3 simplificada da Figura 9, que é utilizada no plano de dados do VPWS e do VPLS.

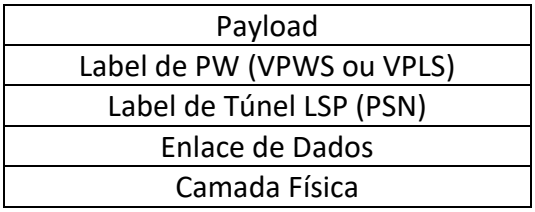


Figura 9 – Arquitetura PWE 3 utilizada no plano de dados do VPWS ou do VPLS.

Para a definição de métodos específicos para o transporte de Ethernet sobre redes MPLS foi emitida a RFC 4448 (*Encapsulation Methods for Transport of Ethernet over MPLS Networks*).

A RFC 4448 habilita provedores de serviço a prestar os diferentes serviços Ethernet sobre os diferentes tipos de PW em redes MPLS existentes. Essa RFC define o uso de *Attachment Circuits* (ACs) e de acesso no *Ethernet Tagged Mode* e acesso no *Ethernet Raw Mode*.

Um *Attachment Circuit* é um canal, físico ou virtual (lógico), entre um CE (*Customer Edge Equipment*) e o respectivo PE, que se destina à associação entre um site da rede do usuário (rede Ethernet, por exemplo) e um dado PW na rede MPLS.

No acesso *Ethernet Tagged Mode*, aqui referido simplesmente como acesso *Tagged Mode,* também denominado acesso *VLAN-Based,* um PW é definido especificamente para um agrupamento identificado de *VLAN IDs*, agrupamento esse constituído por um, por alguns ou pela totalidade de *VLAN IDs* da rede do usuário.

No *Tagged Mode*, os ACs são virtuais no interior do AC físico, sendo o AC destinado especificamente ao mapeamento em dado PW, definido para o mesmo agrupamento de *VLAN IDs* correspondente a esse PW.

No acesso *Raw Mode,* também referido como acesso *Port-Based,* os *VLAN IDs* não são considerados, tanto no AC quanto no PW utilizados. O AC é físico, correspondendo integralmente ao link CE/PE.

Finalmente, vamos mencionar nesta introdução ao VPWS e ao VPLS, a RFC 4664 (*Framework for Layer 2 Virtual Private Networks (L2 VPNs)*). Essa RFC introduz os conceitos de VPWS, VPLS e IPLS, e define o embasamento conceitual aplicável a essas aplicações do MPLS.

A RFC 4664 estabelece o conceito de *forwarder,* como sendo o processo encarregado do mapeamento entre ACs e PWs. Como veremos adiante com mais clareza, o *forwarder* no VPWS é um ponto de conexão, enquanto no VPLS é um switch Ethernet virtual referido como VSI (*Virtual Switching Instance*).

É importante observar que os *forwarders* de qualquer tipo se localizam nos PEs da rede MPLS.

5.2 – VPWS

VPWS é um tipo de L2VPN onde um *forwarder* (um ponto de terminação, no caso) mapeia exatamente uma terminação de um AC em exatamente um PW, estando a outra terminação desse AC conectada a um dado CE que representa um site da rede do usuário.

VPWS pode funcionar sobre diferentes tipos de PSN. Nos limitaremos neste artigo ao MPLS VPWS, ao qual nos referiremos apenas como VPWS.

Como cada PW (MPLS PW, a rigor) encontra-se mapeado em um dado LSP, fica então estabelecido, no VPWS, um circuito virtual entre um par de CEs para cada AC (físico ou virtual) existente nesses CEs.

Em consequência, um quadro de dados do usuário transmitido pelo CE de origem por um dado AC, alcançará inexoravelmente o CE de destino, pelo correspondente AC de destino. Essa transmissão entre o par de CEs ocorre sem a necessidade de qualquer procedimento de descoberta ou de aprendizagem de endereços na PSN de transporte.

Para o encapsulamento de quadros Ethernet sobre MPLS, inclusive no caso particular do VPWS, utiliza-se a RFC 4448. São aplicáveis o acesso *Tagged-Mode* (*VLAN-Based*) e o acesso *Raw-Mode* (*Port-Based*) no VPWS.

Na sinalização para a constituição de VPWS PWs utiliza-se a RFC 4447, sem a necessidade de qualquer alteração ou extensão. Como veremos a seguir, para a constituição de VPLS PWs foi necessária a definição de extensões à RFC 4447.

5.3 – VPLS

VPLS possibilita a emulação de múltiplas redes bridged Ethernet privativas virtuais, ou seja, de EVPNs, pela rede MPLS. Essas EVPNs são referidas como VPLS VPNs. As bridges virtuais configuradas para cada uma das VPLS VPNs são referidas como VSIs (*Virtual Switching Instances*), e a interconexão de VSIs ocorre por meio de VPN PWs (*pseudowires*).

A topologia *full-mesh* é tipicamente utilizada em VPLS VPNs. Nesse caso, a prevenção de loops na VPN ocorre pelo mecanismo *Split-Horizon*, sendo dispensável, portanto, o uso de *Spanning Trees*.

5.3.1 – Sinalização no VPLS

As VSIs de uma VPLS VPN são definidas no interior dos PEs determinados pelo usuário contratante da VPLS VPN, sendo configurado um identificador de cada VPLS VPN (*VPN-Id*) em cada um desses PEs e na VSI definida para a VPLS VPN no PE.

Cada VSI de uma dada VPLS VPN atribui e distribui, mediante o uso de um protocolo de sinalização, um valor de *PW label* (label MPLS no formato genérico), destinado a

identificar os quadros de dados dessa VPLS VPN que serão recebidos por essa VSI. O valor de *PW label* distribuído por uma VSI fica registrado nessa própria VSI e no PE que a contém.

Cada uma das demais VSIs da VPLS VPN registra o valor de *PW label* recebido, com base no *VPN-Id* também presente nos quadros de sinalização. Os valores de *VPN-Id* identificam as VPNs no plano de controle.

O procedimento acima deve ser repetido, em cada uma das VPLS VPNs, para todas as VSIs que a compõem, o que, ao fim, provê bidirecionalidade na comunicação das VPLS VPNs.

Da mesma forma que no caso dos *VPWS labels*, os *PW labels* (*VPLS labels*) irão constituir os *bottom labels* dos quadros de dados das respectivas *VPLS VPNs*, sendo envelopados pelos labels de túnel LSP (*top labels*) da rede MPLS transportadora. Os *bottom labels* são visíveis apenas para os PEs envolvidos.

Diferentemente do VPWS, que utiliza apenas um protocolo de sinalização para a constituição de PWs (RFC 4447, baseada em extensões do LDP), o VPLS dispõe de dois protocolos com esse propósito, um definido na RFC 4761 (*VPLS Using BGP for Auto-Discovery and Signaling*) e o outro na RFC 4762 (*VPLS Using LDP Signaling*).

A RFC 4761 representa uma extensão do protocolo MP-BGP (*Multi-Protocol BGP*), definido na RFC 4760 (*Multiprotocol Extensions for BGP-4*), utilizada para *auto-discovery* de PEs e sinalização no VPLS.

A RFC 4762, que representa extensões da RFC 4447 para o VPLS, restringe-se à sinalização para a constituição de PWs no VPLS, não abrangendo, portanto, auto-descobrimento de PEs.

5.3.2 – Associação entre ACs e VSIs

Em cada PE participante de uma VPLS VPN, os ACs são associados à respectiva VSI. A forma pela qual os ACs são associados a uma VSI depende da implementação. Pode ocorrer a associação de apenas um AC em uma VSI, a associação de parte ou da totalidade dos ACs de uma porta do PE (relativos a um único CE) em uma VSI ou mesmo a associação de ACs de diferentes portas do PE em uma VSI.

No acesso *Raw Mode*, um AC é identificado pela respectiva porta de PE. No acesso *Tagged Mode*, um AC é identificado pela respectiva porta de PE e por VLAN ID a ele associado.

A Figura 10 exibe uma configuração de uma VPLS VPN onde uma das VSIs mapeia ACs de duas portas do PE.

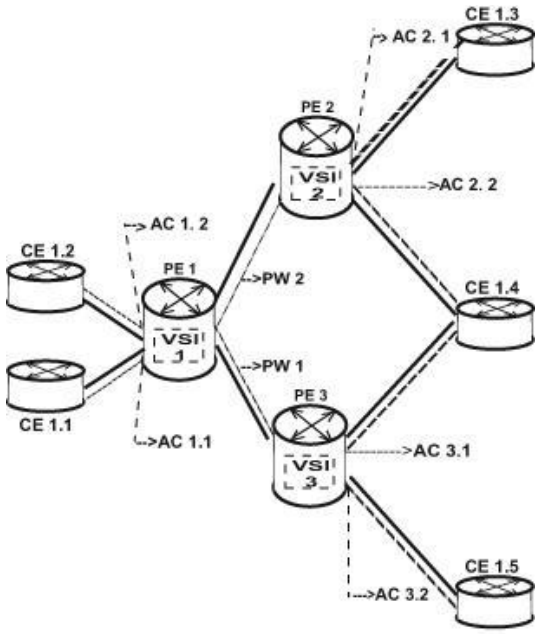


Figura 10 – Configuração de VPLS VPN.

Como se observa na figura, à VSI 1 (no PE 1) encontram-se mapeados o AC 1.1, relativo ao CE 1.1, e o AC 1.2, relativo ao CE 1.2.

Na VSI 1, o AC 1.1 foi associado ao PW 1, que conecta a VSI 1 à VSI 3, enquanto o AC 1.2 foi associado ao PW 2, que conecta a VSI 1 à VSI 2. O tráfego entre os CE 1.1/CE 1.2 e o CE 1.4 pode transitar alternativamente via VSI 2 ou via VSI 3, estando uma dessas vias ativa e a outra como backup.

5.3.3 – Transmissão de Tráfego

Quando da fase de transmissão de tráfego de dados em uma VPLS VPN, um quadro transmitido por um CE em um dado AC, será enviado, no PE, para a correspondente VSI.

De posse desse quadro de dados, a VSI verifica se se trata de um quadro unicast com endereço MAC conhecido. Se não for o caso, quando então se trata de um quadro referido na literatura com quadro BUM (*Broadcast, Unknown MAC Address, Multicast*), a VSI replica o quadro para todos os LSPs associados à VPLS VPN, incluindo os correspondentes *PW labels*.

Cada um dos PEs receptores verifica se possui uma VSI associada ao valor de *PW label* do quadro. Os PEs que não possuem uma VSI nessa condição, descartam o quadro sumariamente.

Caso contrário, cada PE receptor encaminha, com base no valor de *PW label*, o quadro para a correspondente VSI, que o reencaminha para o respectivo CE (ou CEs), por meio do correspondente AC.

Se existirem múltiplos CEs conectados, o quadro será enviado para o devido CE se o PE tenha aprendido o endereço MAC de destino. Se não, o quadro será enviado para todos os CEs.

Como regra, esses CEs inundam os respectivos sites Ethernet com quadros recebidos nessa condição, o que representa um considerável desperdício de rede, característico das redes Ethernet tradicionais.

Na hipótese do parágrafo anterior, as VSIs receptoras aproveitam as informações contidas no quadro, para fins de aprendizagem. Diferentemente de outras opções tradicionais de rede Ethernet, que aprendem apenas a associação do endereço MAC de origem do quadro com a porta física de entrada, as VSIs aprendem esse endereço MAC e também o valor do *PW label* contido no quadro, e os associam.

Assim, caso uma VSI receba um quadro unicast com endereço MAC de destino aprendido, a VSI obtém o valor de *PW label* associado a esse endereço MAC. Dessa forma, a VSI é capaz de enviar o quadro direcionadamente para o PE de destino pelo devido LSP.

Na hipótese do parágrafo anterior, a inundação ou não do site Ethernet de destino com o quadro, dependerá de ter havido ou não a aprendizagem do endereço MAC de destino nesse site.

5.4 – BGP MPLS-Based EVPNs

A padronização das *BGP MPLS-Based EVPNs,* ou seja, de EVPN, teve início com a emissão da RFC 7209 (*Requirements for Ethernet VPN (EVPN)*). Foi posteriormente publicada a RFC 7432 (*BGP MPLS-Based Ethernet VPN*), em fevereiro de 2015, com o propósito de descrever os procedimentos para EVPN.

Foram então emitidas, adicionalmente, as RFCs abaixo relacionadas, definindo aspectos específicos das EVPNs:

- RFC 8214 (*Virtual Private Wire Service Support in Ethernet VPN*);

- RFC 8317 (*Ethernet-Tree (E-Tree) Support in Ethernet VPN (EVPN) and Provider Backbone Bridging EVPN (PBB-EVPN)*);

- RFC 8388 (*Usage and Applicability of BGP MPLS-Based Ethernet VPN*).

Paralelamente aos esforços do IETF, o BBF (*Broadband Forum*) passou a emitir *Technical Reports* (TRs) relativos a EVPN, destacando-se o TR 350 (*Ethernet Services Using BGP MPLS Based Ethernet VPNs (EVPN)*).

5.4.1 – Definições em EVPN

EVPN é uma solução que, como o VPLS, provê serviços Ethernet multiponto sobre redes MPLS. EVPN, no entanto, foi definido como uma nova alternativa que elimina algumas limitações do VPLS. Tais limitações representam importantes considerações para a implementação de *Data Centers* (DCs).

EVPN estabelece uma base comum para os serviços *E-Line, E-LAN* e *E-Tree*, providos por *Carrier Ethernet*.

Da mesma forma que o VPWS e o VPLS, EVPN pode ser prestado sobre diferentes tipos de PSN. A padronização básica dessas redes, contudo, restringe-se ao suporte do uso do MPLS como PSN, o mesmo ocorrendo com o presente artigo.

EVPN requer extensões dos protocolos do IP/MPLS existentes, conforme a RFC 7432. Adicionalmente a essas extensões, EVPN utiliza diversas partes da tecnologia MPLS atual.

EVPN utiliza o MP-BGP (*Multiprotocol BGP*), definido na RFC 4760, entre PEs para a distribuição de rotas MAC e possibilita o controle apurado dessa distribuição.

Uma *EVPN Instance* (EVI), ou seja, uma Instância EVPN, é uma instância de EVPN que engloba CEs conectados aos PEs que participam dessa EVPN, juntamente com esses PEs. Um CE pode ser um host, um roteador ou um switch Ethernet. Podem existir múltiplas Instâncias EVPN na rede do provedor.

Se um CE se conecta a múltiplos PEs (*multihoming*), o conjunto de links utilizados constitui um *Ethernet Segment* (ES), ou seja, um Segmento Ethernet. Cada ES é identificado por um *Ethernet Segment Identifier* (ESI).

A Figura 11 apresenta a configuração básica de uma rede EVPN.

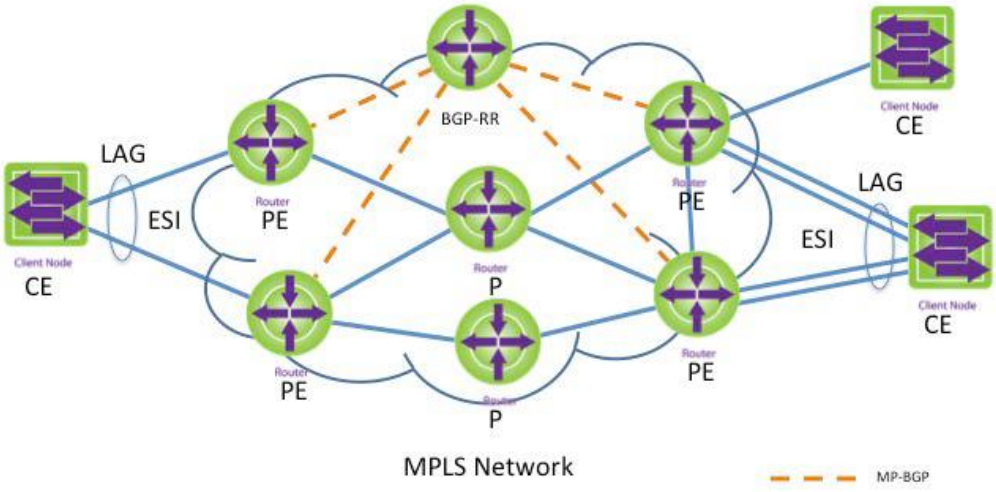


Figura 11 – Configuração básica de uma rede EVPN.

Nessa figura, verifica-se a presença de dois CEs, estando cada um deles conectado a dois PEs por meio dos respectivos ESs, sendo os ESs constituidos por LAGs (*Link Aggregation Groups*). Um terceiro CE encontra-se conectado a um dos PEs em comum com um dos outros PEs.

Constata-se também nessa figura a utilização de um BGP RR (*BGP Route Reflector*) em um dos PEs que suportam o MP-BGP.

As ESIs encontram-se no interior dos PEs, não aparecendo, portanto, na figura.

Além de prestar serviços Ethernet nativamente e de dar suporte a serviços *Carrier Ethernet* (vide TR-350), EVPN pode ser utilizada para suportar o VPWS em redes MPLS/IP, nos termos da RFC 8214.

EVPN provê ao VPWS as seguintes capacidades:

- *Multihoming* no modo um-ativo e no modo todos-ativos, com balanceamento de carga de tráfego baseado em fluxo;

- Eliminação da necessidade de sinalização para a constituição de PWs;

- Convergência rápida em caso de falha em links ou em nós.

5.4.2 – Requisitos Atendidos

EVPN oferece soluções que atendem requisitos estabelecidos na RFC 7209, ao contrário do VPLS, que não satisfaz esses requisitos.

Dentre tais requisitos, podem ser mencionados os seguintes:

- *Multi-homing* (conexão de um CE a múltiplos PEs) no modo transmissão todos-ativos (*all active forwarding*), quando o CE pode transmitir simultaneamente para todos os PEs;

- Balanceamento de carga (*load balancing*) de tráfego de CE para CE;

- Aprendizagem de endereços MAC unicast de estações finais no plano de controle;

- Otimização de multicast, para o suporte eficiente de aplicações P2MP e MP2MP nativamente. O VPLS suporta apenas aplicações P2MP nativamente;

- Simplicidade de provisionamento;

- Balanceamento de carga de tráfego baseado em fluxo (*flow-based load balancing*);

- *Multipathing;*

- Convergência rápida para minimizar tempos de interrupções e perdas de quadros;

- Mobilidade de endereços MAC para o suporte de serviços na nuvem.

5.4.2.1 – Multi-Homing e Balanceamento de Carga de Tráfego

Devido ao rápido crescimento de tráfego, a conexão de um CE a múltiplos PEs no modo um-ativo (ativo/standby) pode ser ineficiente. EVPN suporta esse tipo de *multihoming* no modo um-ativo assim como no modo todos-ativos com balanceamento de carga de tráfego.

O VPLS, no entanto, suporta apenas o modo um-ativo, o que obviamente dificulta a ocorrência de tráfego mais intenso envolvendo o CE.

O modo todos-ativos possibilita, a EVPN, melhor balanceamento de carga de tráfego entre PEs pares, comparativamente ao VPLS.

Adicionalmente, EVPN possibilita balanceamento de carga de tráfego através sa

5.4.2.2 – Aprendizagem de Endereços MAC Unicast

Os PEs transmitem os quadros de dados que recebem com base nos respectivos endereços MAC de destino. Para que um quadro de dados não seja transmitido como um quadro BUM, é necessário que se trate de um quadro unicast com endereço de destino aprendido.

A RFC 7432 divide a aprendizagem de endereços MAC em aprendizagem local e aprendizagem remota.

Na aprendizagem local, um PE aprende os endereços MAC unicast nos quadros enviados pelos CEs a ele conectado.

Na aprendizagem remota, um dado PE aprende os endereços MAC unicast que pertencem aos CEs conectados a outros PEs ou os endereços MAC de estações que se encontram além desses CEs.

Em EVPN, a aprendizagem remota de endereços MAC unicast ocorre no plano de controle, enquanto a aprendizagem local ocorre no plano de dados.

Aprendizagem no plano de controle elimina a necessidade de inundações desnecessárias da rede para quadros unicast, por não depender da ocasionalidade do tráfego de dados. Permite também a aplicação de políticas, sendo possível a escolha do que se aprende e de quem aprende.

No VPLS, tanto a aprendizagem local quanto a aprendizagem remota ocorrem no plano de dados. A aprendizagem remota no plano de dados representa um elevado nível de desperdício de recursos da rede, pela frequente ocorrência de inundações da rede. De fato, a ocasionalidade de ocorrência de tráfego de dados não permite frequência na aprendizagem, que se verifica de forma aleatória.

5.4.3 – Tipos de Interface de Serviço em EVPN

Em EVPN, são utilizados os seguintes tipos de interface de serviço:

- Interface de serviço *VLAN-Based*;

- Interface de serviço *VLAN Bundle*;

- Interface de serviço *Port-Based VLAN Bundle*;

- Interface de serviço *VLAN-Aware Bundle*;

- Interface de serviço *Port-Based VLAN-Aware Bundle.*

Com a interface de serviço *VLAN-Based*, uma EVI consiste em apenas um único domínio broadcast, ou seja, em uma única VLAN.

Com a interface de serviço *VLAN Bundle*, uma EVI corresponde a múltiplos domínios broadcast, ou seja, a múltiplas VLANs. Em outras palavras, existe um mapeamento muitos-para-um entre VLANs e uma MAC-VRF, sendo que uma MAC-VRF consiste em uma única tabela bridge. Não ocorre translação de valores de VLAN ID nesse tipo de interface.

Existe um caso especial de interface *VLAN Bundle* em que que todas as VLANs na porta são parte do mesmo serviço e mapeiam no mesmo agregado (*bundle*). Essa opção é referida como interface *Port-Based VLAN Bundle.*

Com a interface de serviço *VLAN-Aware Bundle*, uma EVI consiste em múltiplos domínios broadcast (múltiplas VLANs), como em interfaces de serviço *VLAN Bundle,* sendo que nas interfaces de serviço *VLAN-Aware Bundle* cada VLAN possui a sua própria tabela bridge

Como no caso das interfaces *VLAN Bundle*, as interfaces *VLAN-Aware Bundle* possuem uma opção *port-based*, referida como interfaces de serviço *Port-Based VLAN-Aware Bundle*.

5.4.4 – Funcionamento de EVPN

Em EVPN, os PEs são interconectados por LSPs MPLS, como em qualquer outra aplicação do MPLS, o que provê os benefícios da tecnologia empregada. No caso do MPLS-TE, as facilidades de engenharia de tráfego podem ser utilizadas por EVPN.

Em EVPN, os PEs divulgam, pelo MP-BGP, os endereços MAC aprendidos a partir dos CEs a eles conectados, juntamente com um label MPLS, para os outros PEs. Dessa forma, ocorre a aprendizagem dos endereços MAC divulgados, no plano de controle portanto.

O funcionamento de EVPN é bastante similar ao das BGP MPLS IP VPNs, ressalvando-se que o seu propósito é o de interconectar sites Ethernet. Uma instância EVPN adquire um *Route Distinguisher* (RD) que é único por MAC-VRF (*MAC VPN Routing and Forwarding*). Adquire também um ou mais *Route Targets* RTs), que são globalmente únicos.

A RFC 7432 define, para o MP-BGP, uma nova NLRI (*Network Layer Reachability Information*), denominada EVPN NLRI. O formato da EVPN NLRI encontra-se na Figura 12.

Tipo de Rota (1 octeto)
Comprimento (1 octeto)
Informações Específicas do Tipo de Rota (variável)

Figura 12 - Formato da EVPN NLRI.

Foram definidos, para a EVPN NLRI, quatro tipos de rota. A codificação desses quatro tipos de rota inicia-se pela indicação do RD que identifica a ESI no plano de controle.

No plano de dados, uma ESI é identificada pelo respectivo label MPLS. Os valores desse label MPLS são também distribuídos na EVPN NLRI, nos tipos de rota aplicáveis.

Um CE conecta-se a uma MAC-VRF, em um PE, por uma interface Ethernet que pode ser configurada para um ou mais VLAN IDs. Em alguns cenários é garantida a unicidade de VLAN IDs entre todas as instâncias EVPN. Isso significa que todas os pontos de conexão para uma dada instância EVPN utilizam o mesmo VLAN ID, que não pode ser utilizado por nenhuma outra instância EVPN. A RFC 7432 refere-se a esse caso como EVPN com VLAN Único (*Unique VLAN EVPN*).

7 - CARRIER ETHERNET

Carrier Ethernet representa um novo paradigma de rede, que proporciona unificação, por generalização, na prestação de serviços de transmissão de Ethernet sobre uma diversidade de redes de transporte. Dentre essas redes, podem ser citadas as redes MPLS (VPWS e VPLS), PB, PBB, SDH, OTN, dentre outras.

A prestação unificada de serviços Ethernet sobre redes de transporte é obtida por meio de um elevado nível de abstração, obtido mediante a criação de um envoltório Ethernet em torno dessas redes, tornando-as opacas para os usuários, que julgam utilizar serviços de uma rede Ethernet.

A Figura 13 exibe a arquitetura de redes Carrier Ethernet, onde fica evidenciada a descrição dos parágrafos anteriores.

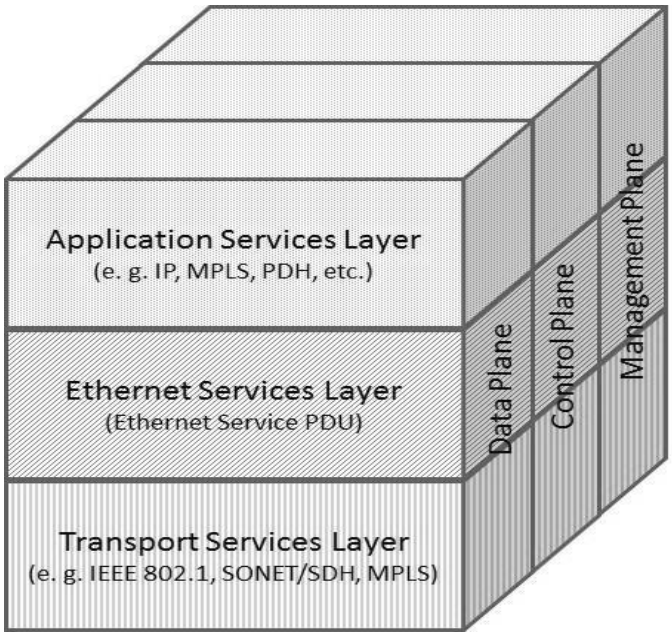


Figura 13 - Arquitetura de redes Carrier Ethernet.

Como se observa na figura, existem três camadas em *Carrier Ethernet:*

- Camada de serviços de transporte (*TRAN Layer*);

- Camada de serviços Ethernet (*ETH Layer*);

- Camada de serviços de aplicação (*APP Layer*).

A *ETH Layer*, que representa a essência de *Carrier Ethernet*, consiste em uma malha constituida por UNIs (*User Network Interfaces*) Ethernet, que envolve qualquer uma das redes que compõem a *TRAN Layer*, oferecendo às redes dos usuários uma interface Ethernet única.

Na visão dos usuários, o que existe são serviços *Carrier Ethernet* específicos, e não a gama variada de serviços que seria oferecida pelas diferentes redes de transporte.

Carrier Ethernet está sendo especificada pelo MEF (*Metro Ethernet Forum*), mediante a emissão de um número considerável de padrões MEF até o momento.

Os serviços *Carrier Ethernet* são prestados por meio de conexões Ethernet virtuais fim a fim entre as UNIs, referidas como EVCs (*Ethernet Virtual Connections*).

7.1 – EVCs e OVCs

Em redes constituídas por uma única CEN (*Carrier Ethernet Network*), as EVCs interconetam diretamente duas ou mais de duas UNIs, sem qualquer envolvimento de unidades de interfaceamento intermediárias, como mostra a Figura 14.

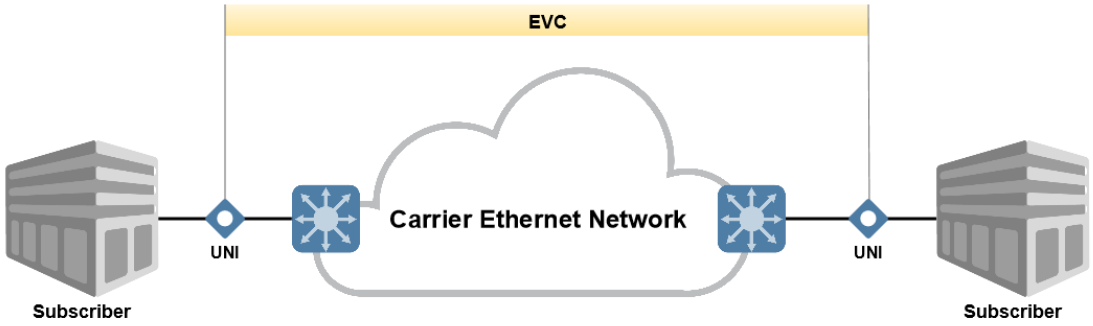


Figura 14 – EVC em rede Carrier Ethernet constituída por uma única CEN.

Em redes *Carrier Ethernet* constituídas por múltiplas CENs (redes *Multi-CEN*), contudo**,** uma EVC é composta por segmentos existentes nessas CENs, que são conjuntamente concatenados para formar a EVC. Esses segmentos são referidos como OVCs (*Operator Virtual Connections*).

OVC é uma conexão Ethernet virtual fim a fim entre uma ou mais de uma UNI e uma única entidade de interfaceamento intermediária, referida como ENNI (*External Network-to-Network Interface*). Uma ENNI é uma interface que representa a fronteira entre duas CENs de operador que são operadas como domínios administrativos distintos.

Cada associação de uma OVC e uma ENNI é denominada um Ponto de Terminação de OVC.

As EVCs e as OVCs podem ser dos seguintes tipos:

- EVCs ou OVCs ponto a ponto;

- EVCs ou OVCs multiponto a multiponto;

- EVCs ou OVCs multiponto com raiz (*rooted multipoint*).

As EVCs/OVCs multiponto a multiponto e as EVCs/OVCs multiponto com raiz, em conjunto, são denominadas EVCs/OVCs multiponto.

A Figura 14 anterior é um exemplo de EVC ponto a ponto.

A Figura 15 mostra uma rede Carrier Ethernet *multi-CEN*, onde se verifica a existência de quatro OVCs ponto a ponto.

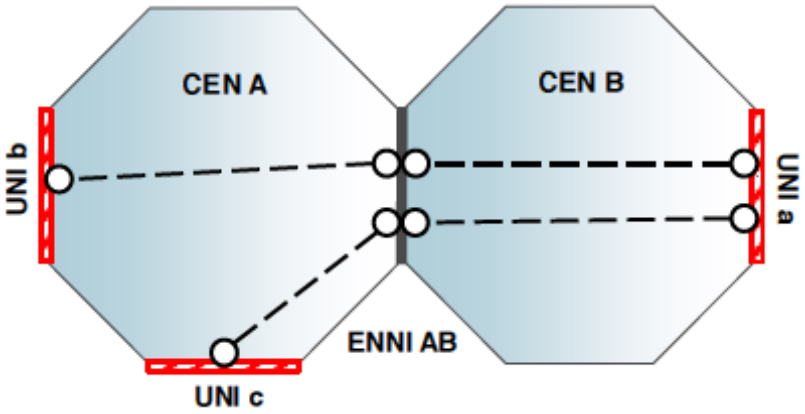
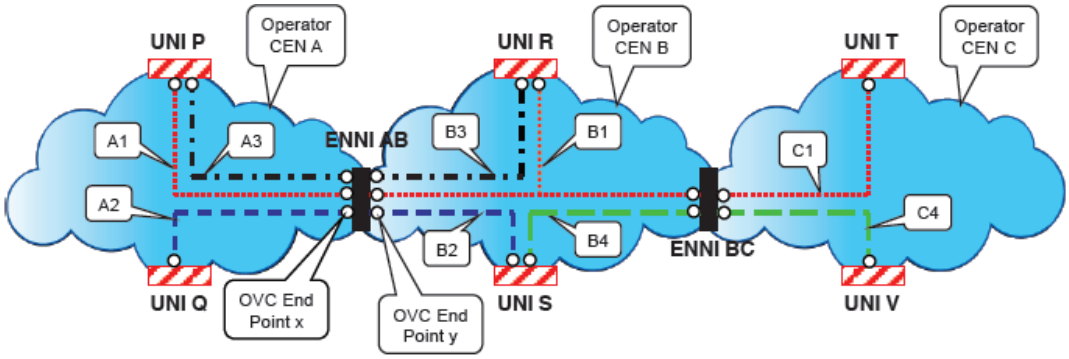


Figura 15 – Rede Carrier Ethernet multi-CEN com quatro OVCs.

Nessa figura, estão configuradas duas EVCs ponto a ponto, ambas terminando na UNI **a.** Cada uma dessas EVCs é constituida por duas OVCs ponto a ponto localizadas em CENs distintas.

A Figura 16 representa uma configuração de rede onde existem quatro EVCs: uma EVC multiponto a multiponto (EVC 1) e três EVCs ponto a ponto (EVC 2, EVC 3 e EVC 4).



EVC	UNIs	OVCs
1	UNI P, UNI R, UNI T	A1, B1, C1
2	UNI Q, UNI S	A2, B2
3	UNI P, UNI R	A3, B3
4	UNI S, UNI V	B4, C4

Figura 16 – EVCs e OVCs de diferentes tipos.

A EVC 1 e a EVC 3, por compartilharem a UNI e por ser a EVC 1 uma EVC multiponto a multiponto, constituem, em conjunto, um exemplo de serviço EVP-LAN com utilização de Multiplexação de Serviços. Esses conceitos serão vistos nos próximos subitens deste artigo.

Para que uma EVC seja uma EVC multiponto, basta que uma OVC dela participante seja uma OVC multiponto. É o que evidencia a existência da OVC multiponto ENNI AB/UNI R/ENNI BC como parte da EVC 1, o que torna a EVC 1 uma EVC multiponto.

O mapa na parte inferior da Figura 16 anterior mostra as UNIs e as OVCs que constituem cada uma das quatro EVCs exibidas.

7.2 – Conceitos Fundamentais

Vamos considerar os seguintes conceitos fundamentais em *Carrier Ethernet*:

- Acesso *VLAN-Based* e acesso *Port-Based*;

- Multiplexação de Serviços;

- Agrupamento (*Bundling*);

- Agrupamento Todos em Um (*All-to-One Bundling*). VLAN-Based

Os conceitos de acesso *VLAN-Based* e de acesso *Port-Based* foram já vistos anteriormente neste artigo, quando da abordagem de outras tecnologias de EVPN.

Em suma, no acesso *VLAN-Based* os VLAN IDs são considerados, enquanto no acesso *Port-Based* os VLAN IDs atravessam a rede transparentemente, sem qualquer consideração dos VLAN IDs.

Na Multiplexação de Serviços, uma UNI é multiplexada estatisticamente por duas ou mais EVCs. Não importa se essas EVCs terminam em uma outra UNI ou se terminam em mais de uma UNI. Esse conceito será ilustrado no próximo subitem.

Ocorre Agrupamento (*Bundling*) quando uma EVC é multiplexada estatisticamente por um conjunto de dois ou mais VLAN IDs do site do usuário identificados. Esse conjunto pode consistir inclusive da totalidade de VLAN IDs no acesso físico ao PE, desde que a totalidade de VLAN IDs seja considerada.

No Agrupamento Todos-em-Um (*All-to-One Bundling*), a totalidade dos VLAN IDs no acesso físico ao PE são aceitos transparentemente na EVC, sem a necessidade de qualquer forma de identificação. Há uma associação biunívoca entre Agrupamento Todos-em-Um e acesso *Raw Mode*.

7.3 – Serviços Carrier Ethernet

O MEF define, em *Carrier Ethernet*, serviços Ethernet de EVC e serviços Ethernet de OVC. Nos limitaremos neste artigo aos serviços Ethernet de EVC, ressalvando que os serviços Ethernet de OVC são estruturados de forma análoga aos serviços Ethernet de EVC.

Nesse ponto, informamos ao leitor que o livro de minha autoria (em co-autoria) Carrier Ethernet – Padrões do MEF, Serviços e Aplicações está disponível, para acesso gratuito, em meu site no portal Wirelessbrasil.com.br.

Os serviços Ethernet em *Carrier Ethernet* classificam-se quanto ao tipo de acesso e quanto ao tipo de EVC.

Quanto ao tipo de acesso existem os seguintes tipos de serviço Ethernet de EVC:

- Serviços EP (*Ethernet Private*), associados ao acesso *Raw Mode*;

- Serviços EVP (*Ethernet Virtual Private*), associados ao acesso *Tagged Mode*.

Em decorrência da associação entre acesso *Raw Mode* e Agrupamento Todos-em-Um, resulta que nos serviços EP ocorre sempre Agrupamento Todos-em-Um.

Nos serviços EVP podem ocorrer as seguintes combinações:

- Apenas Multiplexação de Serviços;

- Apenas Agrupamento;

- Multiplexação de Serviços e Agrupamento;

- Nem Multiplexação de Serviços nem Agrupamento;

- Jamais Agrupamento Todos-em-Um.

Quanto aos tipos de EVC, os serviços de EVC podem ser do tipo *E-Line* (EVCs ponto a ponto), do tipo *E-LAN* (EVCs multiponto a multiponto) e do tipo *E-Tree* (EVCs multiponto com raiz).

Considerando-se essas duas formas de classificação, a totalidade de serviços Ethernet de EVC encontra-se relacionada na Figura 17.

Service Type	Port-Based (All to One Bundling)	VLAN-Based (EVC identified by VLAN ID)
E-Line (Point-to-Point EVC)	Ethernet Private Line (EPL)	Ethernet Virtual Private Line (EVPL)
E-LAN (Multipoint-to-Multipoint EVC)	Ethernet Private LAN (EP-LAN)	Ethernet Virtual Private LAN (EVP-LAN)
E-Tree (Rooted-Multipoint EVC)	Ethernet Private Tree (EP-Tree)	Ethernet Virtual Private Tree (EVP-Tree)

Figura 17 – Serviços Ethernet de EVC.

Ilustraremos os serviços Ethernet de EVC com dois exemplos.

A Figura 18 mostra uma configuração de rede com um exemplo de serviço EVPL.

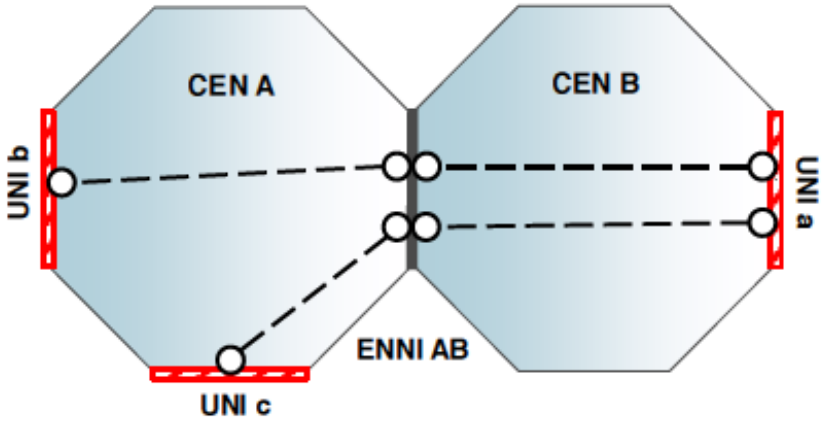


Figura 18 – Exemplo de serviço EVPL.

Nessa figura, a Multiplexação de Serviços na UNI **a** é condição suficiente (mas não necessária) para definir o serviço como virtual, no caso o serviço EVPL.

A figura 19 exibe uma configuração de rede com um exemplo envolvendo o serviço *VP-LAN* e o serviço *EVP-Tree*.

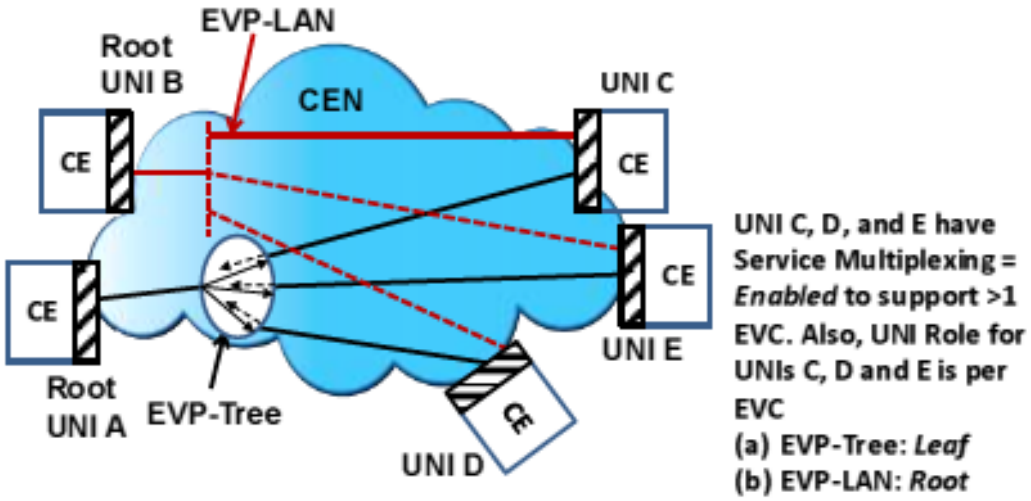


Figura 19 – Serviço EVP-LAN e serviço EVP-Tree.

Nessa figura, existe um serviço *EVP-Tree*, o qual possui duas UNIs raiz (UNI A e UNI B) e três UNIs folha (UNI C, UNI D e UNI E), conforme as linhas tracejadas.

Existe também um serviço EVP-LAN coexistindo nessa rede, conforme as linhas cheias.

O fato de tratar-se de rede com serviços EVP evidencia-se pela ocorrência de Multiplexação de Serviços nas UNI C, UNI D e UNI E.

Esse exemplo mostra também que o papel desempenhado por uma UNI depende da EVC. Nesse caso, as UNI C, UNI D e UNI são folhas para as EVCs em linhas tracejadas (EVP-Tree) e são raízes para as EVCs em linhas cheias (EVP-LAN). É preciso lembrar que em EVP-LANs todas as UNIs são raizes.

++++++++++++++