SR. ANTONIO MARCOS MOREIRAS: Muito bom dia para todo mundo. Estamos aqui hoje no que é o último dia da semana de capacitação on-line do NIC.br. Pois é, pessoal, tudo que é bom tem um final. Espero que vocês tenham realmente achado boa a semana inteira, mas ainda tem hoje para aproveitar. E hoje a gente tem a participação da Juniper, com o Eduardo Haro, que vai falar sobre a evolução da tecnologia de transporte Layer 2, vai falar de Ethernet VPN, EVPN. Quem que já usa EVPN aí no seu provedor? Posta aí no chat para a gente, para a gente ter uma ideia de quem já está usando essa tecnologia, ou quem pretende usar, coloquem aí nos comentários, já para o Eduardo também já ter uma ideia de quem já está familiarizado com essa tecnologia ou não.

Lembrando a vocês que, como no restante da semana, nós vamos fornecer certificados de participação para quem estiver aqui acompanhando ao vivo. E esses certificados de participação estão disponíveis apenas até às 14 horas. É necessário você fazer a inscrição no nosso sistema de cursos e eventos do NIC.br, como se você fosse fazer um curso, tal, não precisa fazer inscrição para participar aqui, não precisa, você está vendo aqui pelo YouTube ou está assistindo pelo Facebook, é só participar e aprender. Mas caso você precise do certificado, queira o certificado, faça a inscrição até às 14 horas impreterivelmente. Não venha depois falar para a gente: "Ah, mas eu estava acompanhando no celular, não consegui ver o link, tal". A gente não consegue abrir uma exceção e emitir o certificado de uma outra forma. É um jeito da gente ver quem está acompanhando aqui on-line: "Mas, Moreiras. Eu estou no celular, não consigo fazer isso agora". Tá bom, tem até às 14 horas para você arrumar um computador, ir lá, ver lá o histórico do chat, e pegar esse link, e fazer a inscrição, certo? Faça isso, por favor. Ajuda a gente a te ajudar também e emitir esse certificado direitinho.

Como nos demais dias, a gente pediu o favor para o Eduardo para que ele gravasse em vídeo a parte principal da explicação, a parte principal do curso aqui. Hoje é um curso mais... ele não tem a parte prática, como teve ontem e anteontem, não tem o laboratório para vocês fazerem juntos. O Eduardo vai dar explicações aqui, vai dar uma aula, certo? Não tem um laboratório para vocês seguirem juntos. Mas o material, os slides já estão disponíveis lá no site do evento. É só entrar lá, procurar lá a Semana de Capacitação On-line, a agenda, os slides já estão lá disponíveis, tá bom? Então fica, facilita vocês acompanharem. Tem gente que gosta de acompanhar, tem gente que tem duas telas, coloca os slides em uma e o YouTube na outra, então, e vai acompanhando assim.

Eu vou pedir para o Pedro colocar aqui agora um videozinho de 15 segundos, que é o um teaser. É um projeto que a gente está trabalhando ainda, a gente espera conseguir lançar em breve sobre alguns... São alguns vídeos educativos, num formato diferente aí, destinados ao usuário da Internet em geral. [Então, Pedro, você consegue colocar para a gente aí?]

Quinze segundinhos de vídeo, e eu já volto.

[exibição de vídeo]

SR. ANTONIO MARCOS MOREIRAS: Bom, gente, espero que vocês tenham gostado. Depois vocês colocam nos comentários aí no chat. Já tem duas lições para vocês fazerem: colocarem o comentário se estão usando ou não o EVPN, e colocar alguns comentários sobre os videozinhos, se vocês gostaram desse tipo de animação, dessa animação curtinha, enfim. Outra coisa, outra lição de casa para vocês, mas essa é bem facinha, hein? É vocês deixarem aquele joinha para a gente. Quem acompanhou o restante da semana já viu qual foi a qualidade de todas as aulas, de todos os minicursos que a gente trouxe aqui. Hoje não vai ser

diferente. Então deem um voto de confiança para a gente e deixem desde já o seu joinha. Se vocês não gostarem, depois, no final, aí vocês deixam lá o dislike, fazer o quê? Você tem que ser honesto. Mas é importante para a gente que vocês deixem o like para ajudar o YouTube a fazer a distribuição desse conteúdo. Com mais likes, o YouTube faz esse vídeo aparecer para mais gente. Como a gente sabe que o conteúdo é muito legal, que vai ajudar bastante o pessoal dos provedores,a gente quer que esse conteúdo apareça para o maior número de pessoas possíveis, para o pessoal que assina o canal do NICbrVideos no YouTube. Aliás, também é uma ótima ideia para vocês assinarem o canal NICbrVideos no YouTube. E podem já pegar o link do vídeo aí, colar lá no grupo de Whatsapp, liga para aquele colega de trabalho que dormiu até mais tarde hoje, que perdeu a hora, que ainda não entrou aqui na live, fala: "Ô, vai começar agora. O Moreiras está lá enrolando para dar tempo de você entrar, mas o Eduardo da Juniper já vai começar o curso". Manda lá no grupo da família, se tiver alguém técnico lá também, manda no grupo de provedores lá do Face da sua região, certo? Compartilha esse vídeo aí porque é importante. É um assunto bem legal, é um assunto que pode ser muito útil para todo mundo aí dos provedores.

O vídeo, antes que vocês perguntem, sim, vai estar disponível aqui logo depois que a gente terminar a live, o YouTube já deixa ele disponível. O Eduardo vai estar acompanhando o chat aqui na parte que é gravada, na parte de vídeo, ele vai estar interagindo com vocês. Então façam perguntas, coloquem as suas dúvidas, e a gente vai tentar responder. E, no final, o Eduardo vai entrar ao vivo, os Eduardos, o Eduardo Barasal, aqui do NIC.br, e o Eduardo Haro, da Juniper, que vai dar o curso aqui para a gente hoje. Eles vão entrar ao vivo, pegando as perguntas do chat, respondendo as principais. Então vai ter esses dois tipos de interação, esses dois tipos de interação. A interação agora no chat, como está passando um videozinho, o palestrante tem lá toda a liberdade de ir lá e conseguir já responder algumas coisas ao vivo no chat. E vai ter a interação, depois, ao vivo em vídeo ali. Os materiais estão disponíveis. Ah, estão me dando um aviso aqui: links para materiais no site e na descrição do vídeo, certo? Os links para os materiais estão tanto no site quanto na descrição do vídeo. Os óculos aqui é para perto, gente.

A Carina estava segurando aqui um aviso para mim de longe, eu não enxergava nada, só uma folha embaçada. Ela chegou quase aqui, tem isolamento social, não podia chegar muito perto, estava difícil, desculpa aí, certo? Mas os links do material estão lá no site do evento e estão também na descrição do vídeo.

Não se esqueçam de fazer inscrição, quem precisar do certificado. E eu vou passar já a palavra para o Eduardo Haro, da Juniper, para a gente começar a aula de hoje, o curso de hoje. Por favor.

SR. EDUARDO HARO: Olá, pessoal, bom dia. Primeiramente gostaria de agradecer ao pessoal do NIC.br pelo convite para participar da Semana de Capacitação com vocês. Gostaria também de agradecer a participação de vocês aí nesse webinar. Ao final dessa apresentação, a gente vai deixar um tempinho ali dedicado a perguntas e respostas para responder alguma dúvida que vocês possam ter tido aí durante a apresentação.

Meu nome é Eduardo Haro, sou engenheiro de sistemas da Juniper. E nessa seção eu vou falar um pouquinho aqui sobre evolução na tecnologia de transporte de camada 2, de L2VPN e VPLS para o Ethernet, o EVPN. Bom, eu dividi a agenda em alguns itens, a ideia não é entrar num deep diving em EVPN, até porque não sou um expert no assunto, mas a ideia é abordar numa primeira seção, fazer uma introdução sobre os principais motivadores e desafios que o EVPN tenta resolver. Depois, falar um pouquinho sobre os building blocks e arquitetura, ou seja, todos os componentes e elementos que fazem parte do EVPN. Descrever os tipos de serviço, tipos de rota, as operações que são feitas no EVPN.

Descrever o cenário de multi-homing. Abordar um pouquinho o tema de rota tipo 5, para se fazer troca de prefixos IPs utilizando EVPN. Algumas técnicas de otimização de tráfego BUM, Broadcast, Unknown Unicast e Multicast. Algumas delas são nativas, a própria implementação básica de EVPN. Outras delas vieram posteriormente. E finalizar descrevendo um pouquinho de uma arquitetura de um Data Center utilizando EVPN. A apresentação não é focada só em Data Center, a apresentação, ela é focada em EVPN MPLS ou EVPN sobre IP VxLAN. Mas como o ambiente Data Center hoje já tem como protocolo de referência o EVPN, então eu trouxe aqui alguns slides para compartilhar com vocês como ele já está sendo implementado hoje nesses ambientes.

Então, começar pela parte de introdução e motivadores do EVPN. Para falar um pouquinho dos motivadores da criação do EVPN, eu cito aqui a RFC7209, é uma RFC informativa, mas que ela descreve um pouquinho das limitações que nós temos hoje na tecnologia atual, no VPLS, e dos novos requerimentos para o EVPN. Dentre essas limitações e desafios, eu separei aqui alguns, entre eles, o módulo(F) e redundância ativo-ativo, tanto para serviços E-LINE, né? Ponto a ponto, como para serviços E-LAN, multiponto-multiponto. Otimização de tráfego Multicast. Simplificação no provisionamento de novos serviços e novos circuitos. Convergência de rede rápida, independente da quantidade de MAC address e independente do tráfego, se está passando por cima daquela VPN. Redução do domínio de Broadcast do tráfego BUM, o tráfego BUM é o tráfego Broadcast Unknown, Unicast e Multicast. Um controle em cima do MAC address através de políticas, através das políticas iBGP, e até novos serviços como E-TREE.

Na indústria de Data Center, hoje VPN é a tecnologia referência utilizada para implementação de todo novo Data Center, todo novo fabric que as empresas estão utilizando. Principalmente por resolver esses pontos que eu coloco aqui nesse slide. O primeiro deles é interconexão de Data Center. Então [ininteligível] eu comentei no slide anterior a possibilidade de trabalhar com redundância ativo-ativo, um control-plane, um aprendizado de MAC address todo pelo control-plane, funcionalidades interessantes como mobilidade MAC address. Ou seja, se eu tenho uma VM que ela está conectada aqui nesse Data Center número 1, e, por algum motivo, essa VM, ela se movimenta e vai para o Data Center número 2, EVPN possui hoje mecanismos nativos que conseguem identificar essa mudança e redirecionar esse tráfego de forma quase que instantânea.

Interconexão do fabric. Então hoje o que acontece é: muitos fabricantes acabam oferecendo para o mercado soluções de interconexão de fabric de Data Center utilizando protocolos proprietários. Isso acaba fechando a empresa ou a operadora a utilizar aquele determinado fabricante ou, muitas vezes, aquele determinado modelo daquele determinado fabricante. Isso, lógico, além de trazer um lock in para aquele específico modelo e vendor, acaba que não traz toda evolução de rede que você teria se estivesse adotando um protocolo aberto e padronizado.

Além disso, existe a questão da introdução de controladores SDN. Então, no caso, se você tem um fabric totalmente de acordo com o padrão de indústria, de acordo com o padrão de EVPN VxLAN, a adoção de uma controladora SDN para controlar o seu fabric é muito mais simples e efetiva.

O terceiro ponto é justamente se ter uma rede realmente Multi-Tenant. Ou seja, onde eu consiga ter diversas aplicações, inclusive de clientes distintos rodando sobre a mesma rede, sem que uma se fale com a outra. Ou, quando se fala, eu estabeleça alguns parâmetros de como essa comunicação entre Tenants seja feita. Isso sem utilizar, lógico, implementações proprietárias, que acabam sendo complicadas para se operar, e também sem ter um impacto em escalabilidade da solução.

Então o que seria EVPN? EVPN é a tecnologia de VPN camada 2, de próxima geração para serviços que sejam E-LINE, E-LAN e E-TREE. Ou seja, tanto para serviços ponto a ponto quanto também para serviços ponto-multiponto. EVPN é baseado no padrão aberto NRFC e interoperável com outros vendors. EVPN, ele é o control plane que é baseado em BGP, e o data plane, ele pode ser tanto MPLS quanto IP puro. E o principal caso de uso na qual EVPN nasceu foi justamente que eu comentei no slide anterior, que é a interconectividade de Data Centers, tanto para serviços L2 quanto para serviços L3. Porém, cada vez mais ele vem se tornando relevante em outras áreas, tanto outros segmentos quanto outras partes da rede, como a utilização em redes de operadoras em business pass, em roteadores metro ou até arquiteturas como campos em empresas.

Hoje a gente pode dizer que a Juniper é, sem dúvida, um dos líderes nesse segmento. Principalmente pela implementação madura do EVPN, tanto nos roteadores quanto nos Switchs, e também pelas inovações que nós estamos trazendo ao mercado dentro dessa área.

Então, falando um pouquinho sobre as aplicações de EVPN, tanto para operadoras quanto para empresas. Para operadoras, bom, primeiro o serviço de L2, ele pode ser tanto serviço VPLS como H-VPLS, ou LDP PWE, todos eles podem ser substituídos por uma única tecnologia, pelo EVPN. Sendo uma tecnologia que traz mais eficiência do que a tecnologia atual. Pode ser utilizado tanto o data plane MPLS, seja LDP, RSVP, Segment Routing, ou utilizando-se o data plane IP, ou seja, VxLAN ou MPLS sobre o DP. É possível utilização também para serviços de L3VPN, assim como você tem hoje nos serviços de L3VPN tradicionais. E uma outra grande vantagem é a utilização dos serviços multi-homing, ou seja, as operadoras podem substituir implementações proprietárias de multi-homing, como o virtual chassis ou MC-LAG por uma implementação padronizada, utilizando o multi-homing real, ou seja, não limitado a dois PEs, mas utilizando quantos PEs você precisa para aquele seu serviço, e sempre com a possibilidade de trabalhar com as implementações ativo-ativo ou ativo e standby.

Para a parte de Data Center, eu acabei comentando um pouco no slide anterior, mas os principais casos de uso são justamente a utilização de uma rede de serviços Multi-Tenant, L2 ou L3, estendendo-se o serviço entre Data Centers, e também comunicação entre virtual machines do Data Center, seja no próprio Data Center ou entre Data Centers também.

Então o que seria EVPN? EVPN nada mais é que um address family do BGP. É um address family novo padronizado pelo AFI 25 SAFI 70. Ele foi padronizado pelo RFC 7432, que foi a primeira RFC de EVPN, e nessa primeira RFC ela descreve tanto a implementação de EVPN utilizando-se MPLS quanto utilizando-se o data plane IP. E essa primeira RFC, ela descreve as primeiras rotas, ou seja, a rota tipo 1 até a rota tipo 4. São as rotas utilizadas para implementação básica de EVPN. Posteriormente, saíram novos drafts que já estão trabalhando para se tornar RFCs, que seriam as rotas tipo 5, que é uma rota que ela é focada em transportar informações de roteamento, ou seja, prefixos IP. As rotas tipo 6, 7 e 8, que são rotas utilizadas para se fazer otimização de tráfego Multicast, na rede. E nós temos uma última RFC, que anotei aqui no slide, que é o 8365, que ela justamente descreve alguns pequenos ajustes que foram feitos para o cenário de EVPN sobre um transporte IP.

Então, comparando aqui a EVPN com a tecnologia atual de VPLS, essa tabela eu acho bem interessante para conseguir fazer esse resumo. Então nos primeiros pontos que a gente pode citar aqui seriam: aprendizado de MAC address, que no VPLS é utilizando o próprio data plane, modelo tradicional. No EVPN, eu tenho esse aprendizado feito no control-plane, através do próprio BGP, isso traz maior controle, através de políticas BGP e também maior escalabilidade. Mobilidade, então, como eu comentei, o EVPN traz alguns

mecanismos nativos para se tratar mobilidade de hosts L2 e L3. Redundância. Então a gente consegue trabalhar habilitando um balanceamento de carga ativo-ativo ou ativo e standby, e nativamente o EVPN já traz a convergência rápida em caso de falha dos nicks PE CE, ou até de um PE inteiro. Provisionamento mais simplificado, eu consigo ter serviços tanto L2 quanto L3 numa mesma interface. E a possibilidade de trabalhar com diversos data planes, ou seja, no MPLS eu só posso trabalhar com data plane MPLS, já no data plane eu tenho possibilidade de trabalhar com esses dois data planes, tanto MPLS quanto o IP puro.

Então, como eu comentei, o EVPN é uma tecnologia que ele nasceu do Data Center, mas tem se tornado cada vez mais relevante nos outros domínios também. Então nós temos já casos de implementações reais de EVPN em business Edge, equipamentos de metro Ethernet, equipamentos de borda, de Peering, transporte de serviços L2 e L3, e até implementações em redes campos, ou seja, em redes de empresas utilizando a EVPN também. Então agora nesse capítulo eu vou falar um pouquinho para vocês sobre a arquitetura do EVPN, os seus componentes e elementos, e descrever um pouquinho de cada um deles, explicando esses building blocks.

Então, falando um pouquinho para vocês sobre a arquitetura do modelo de EVPN. EVPN, ele é baseado no control-plane BGP. Então todos aqueles controles de políticas que nós temos numa VPN, uma L3VPN, L2VPN tradicional do BGP, como Route Distinguisher, Route Target e todas communities, nós temos também aqui no EVPN. E aqui nessa figura eu coloquei, porque é interessante e eu consigo apontar alguns dos componentes e algumas das siglas que a gente usa, que eu vou usar aqui nessa seção nos próximos slides. Então em cada um dos PEs da minha rede, quando eu habilito o serviço de EVPN, ele é habilitado sempre em uma instância EVPN, que é chamada de EVI. Cada link entre o PE e um CE é um link que é chamado de Ethernet Segment, e para cada link eu tenho um ESI, que é um Ethernet Seguiment Identifier. Quando esse link é um link single homed, como nesse exemplo, eu tenho um host ligado diretamente ao PE, o ESI, ele tem sempre um valor zero. E quando tenho um host que ele é ligado de forma multi-homed, como esse caso aqui, ele está ligado em dois PEs simultaneamente, então o ESI tem que ter um valor diferente de zero, que seja único para toda rede. A comunicação entre PEs, ela é feita utilizando BGP, address family AFI/SAFI 2570, e como data plane eu posso ter tanto MPLS quanto IP.

No caso da implementação de EVPN sobre IP, mais especificamente aqui utilizando VxLAN. Eu cito aqui nesse slide a RFC 8365, que é a RFC onde detalha um pouquinho mais esses pontos. A implementação de EVPN VxLAN, ela tem as mesmas funcionalidades, as mesmas vantagens, os mesmos benefícios que eu tenho na implementação de EVPN MPLS. A única diferença está em algumas operações que nós temos aqui. Então, no caso do EVPN MPLS eu tenho a utilização de labels para identificar os serviços, e já no caso do EVPN sobre VxLAN nós temos utilização de VNIs, que são identificadores, os IDs dos túneis VxLANs. A regra de split-horizon para um PE multi-homing é um pouquinho diferente. Eu vou abordar isso nos próximos slides. E quando uma rota EVPN é anunciada para a rede com VxLAN é sempre enviado em conjunto uma Extended Community, para identificar essa rota dizendo que é uma rota EVPN.

Então, comparando os dois data planes que nós temos num DVPN(F), ambos data planes eu tenho uma camada aqui de transporte, no caso do MPLS é um label de transporte que pode ser um label RSVP, um label LDP, ou um label Segment Routing. No caso da implementação sobre IP, eu tenho aqui um outer header, que é basicamente o meu cabeçalho IP com o cabeçalho DP para eu poder encapsular o VxLAN. Nesse meu campo azul, no meio, é onde eu tenho a identificação do serviço. Então no caso do VPN sobre MPLS eu tenho um label de serviço, que é utilizado aqui para identificar conteúdo desse payload, e no caso do VxLAN tenho aqui justamente o cabeçalho VxLAN contendo o VNI, para identificar de qual Tenant, de qual serviço é esse payload.

Por que o uso de VxLAN para o EVPN sobre IP? Ou seja, onde o VxLAN é mais aplicável? Com o VxLAN você consegue rodar uma conectividade L2 em uma rede flat, um IP fabric flat de um Data Center apenas rodando IGP, pode ser um SPF, pode ser um ISS, pode ser até um BGP, sem a necessidade de eu ter suporte MPLS. Não tenho que me preocupar com loopings L2, com a utilização de spanning tree, e eu consigo utilizar dispositivos mais simples, e, portanto, mais baratos, L2, que suportem apenas uma FIB pequena, só para conseguir ter o endereçamento dos outros Switchs naquele site. Ou seja, com isso eu tenho um interesse grande em VxLAN, tanto para implementação em DataCenters Clouds de operadoras, de empresas, ou até mesmo em empresas que querem utilizar uma conectividade L2 de transporte na sua rede IP.

Então entrando um pouquinho em detalhe o que seria o VxLAN. VxLAN, na verdade, é um túnel que roda em cima do cabeçalho IP e UDP. VxLAN, ele é padronizado nessa RFC, na 7348. Justamente o que ele faz é encapsular esse frame L2 em um cabeçalho VxLAN, onde, dentre esses campos, o mais importante é justamente o VNI. O VNI é o VxLAN Network Identifier, que vai justamente identificar que esse pacote aqui pertence à uma determinada aplicação, a um determinado Tenant, como é o exemplo aqui da figura. Ou seja, tem um Tenant vermelho e um Tenant verde, e eles não se falam, a não ser que eu faça uma configuração liberando a comunicação entre eles.

Esse cabeçalho, VxLAN, ele é encapsulado em um cabeçalho UDP, onde a porta destino é sempre a mesma, é a 4789. A porta origem, ela varia, porque justamente a porta origem, ela é utilizada pelo roteador para identificar aquele fluxo de dados em específico, e assim poder auxiliar no balanceamento de carga dos roteadores subsequentes, né? E logo depois eu tenho um cabeçalho IP e MAC.

Então eu vou falar um pouquinho para vocês agora sobre os tipos de serviço dentro desse framework EVPN. São basicamente três tipos de serviço que a RFC aborda. Eu vou falar sobre cada um deles, as diferenças entre eles e colocar um exemplo de configuração para que fique mais claro como ele é implementado na prática. Bom, começando pelo primeiro tipo de serviço, é o VLAN-based. Nesse tipo de serviço, nós temos... dentro de um único roteador podem ser configuradas várias instâncias EVPN. Tipicamente, cada instância EVPN pode ser dedicada para um Tenant, ou para um cliente, ou para uma aplicação em específico. Cada instância EVPN, ou seja, cada EVI, ela tem um único bridge domain, ou seja, uma única tabela de aprendizado de MAC address e um único domínio de Broadcast, ou seja, um único VLAN dentro daquela EVI. Por conta disso, é permitido fazer tradução de VLANs, ou seja, aqui eu tenho um circuito utilizando VLAN número 1 conectada ao PE1. E no PE2 eu posso ter aqui a VLAN número 11. Nesse tipo de serviço, o VLAN na ID daquele pacote, daquele tráfego, ele pode ser carregado pelo backbone até o outro PE, ou o PE de egress, ele pode retirar esse VLAN ID e mandar o tráfego sem a VLAN até o outro lado. Nesse caso, a Ethernet-tag ID, ele é enviado com valor zero. E eu vou descrever um pouquinho mais à frente o que é o Ethernet-tag ID, mas ele é justamente o valor que identifica o bridge-domain dentro de uma determinada instância EVPN.

Esse tipo de serviço, VLAN-based, ele é descrito na seção 6.1 da RFC original, da 7432, e existem dois cenários onde eles podem ser aplicados. Então é justamente a minha ideia é mostrar todas opções de configuração, como eu faria uma configuração de um serviço do tipo VLAN-based em um equipamento Junos.

Então no primeiro cenário o mesmo VLAN ID, ele é utilizado em todos os PEs, ou seja, é um cenário onde eu não preciso ter tradução de VLAN. Nesse cenário, a seção da RFC, ela não especifica se o VLAN ID deve ser enviado junto com o pacote ou não pelo backbone. Então eu tenho aqui duas opções de configuração,

dependo da utilização do serviço. E, no segundo cenário, onde eu tenho VLANs IDs diferentes nos PEs. Então, consequentemente eu preciso de tradução de VLAN. Nesse ponto, a RFC, ela especifica que o tag de VLAN original deveria ser carregado no backbone de EVPN, e a tradução de VLAN deve ocorrer no PE de egress.

Então no Junos, nos equipamentos da Juniper, nós conseguimos tratar as duas formas, ou seja, eu consigo tratar tanto a opção que está de acordo com a RFC dentro das cláusulas should e must, ou seja, enviando o tag de VLAN original pelo backbone IP, e ele faz a tradução no Egress PI, ou a opção apenas do must, onde eu retiro esse tag de VLAN e faço apenas a tradução do VLAN ID no PE de egress. Isso é muito importante porque implementações de EVPN nós já vimos casos em que outros fabricantes não estavam de acordo com essa cláusula should aqui, ou seja, eles enviavam o tráfego sem o tag de VLAN. Então com isso você não consegue fechar uma comunicação entre os dois PEs. No caso da Juniper, a gente consegue através de uma configuração diferente endereçar cada um desses casos. Em todos esses casos, como comentei no slide anterior, o Ethernet-tag ID da rota, ele é setado em zero.

Então mostrar como isso é feito na prática. Ou seja, na primeira opção onde eu não preciso de tradução de VLAN, e o VLAN ID não é enviado pelo backbone EVPN. Então, nesse caso, eu tenho aqui a configuração de uma interface. Nesse caso o VLAN ID 100 é utilizado em todos os PEs para esse determinado serviço. E eu crio aqui uma Routing instance, e nessa Routing instance eu tenho que configurar, como eu comentei no comecinho da apresentação, os parâmetros de EVPN, Route Distinguisher, Route Target, especificar que é uma instância do tipo EVPN, com protocolo EVPN. E para o serviço VLAN-based eu tenho o comando aqui VLAN ID none, que é justamente onde ele retira o target VLAN ID daquele pacote que veio para o link PE CE. Para a opção número 2, ou seja, a opção onde eu continuo não tendo tradução de VLAN, porém, o tag de VLAN ID é enviado pelo backbone EVPN, eu continuo mantendo aqui a minha configuração do lado da interface, a única diferença é que eu não tenho mais aquele comandinho do VLAN ID none aqui. Eu tenho simplesmente a configuração da minha instância de EVPN, um Route Distinguisher, Route Target. Eu declaro a interface que participa desta EVI e nada mais. Para a terceira opção, onde nesse caso eu preciso ter tradução de VLAN, ou seja, a cada PE CE utiliza uma VLAN diferente, e nesse exemplo aqui 3 o VLAN ID é enviado pelo backbone EVPN. Então aqui eu tenho que configurar. Eu configuro VLAN ID naquela interface específica e eu também utilizo uma configuração aplicando um VLAN map com ação de swap para que a tradução seja feita no sentido de output, ou seja, no egress PE. Dentro da minha instância de VPN eu incluo dois comandinhos para identificar para o Junos que o Ethernet tag ID tem que estar zerado, e aqui o VID, ou seja, o VLAN ID, tem que ser mantido ao enviar o tráfego pelo backbone. Então essa é configuração de VLAN-based utilizando a... estando strict compliance com a RFC. Na quarta opção é onde eu tenho a tradução de VLAN, porém o VLAN ID não é enviado pelo backbone EVPN. Então nesse caso, como eu não tenho VLAN ID enviado pelo backbone EVPN, na configuração da interface eu simplesmente declaro que ela vai ter uma VLAN ID daquele determinado link PE CE, mas eu não preciso ter aquele output VLAN map. Na instância EVPN, eu simplesmente deixo aqui aquela configuração do VLAN ID none, que é justamente para ele retirar o tag de VLAN ID e manter a rota anunciada com Ethernet-tag zero.

Esse é o segundo serviço, tipo de serviço especificado pelo EVPN, que é o VLAN-bundle. A diferença do VLAN-bundle para o VLAN-based é que justamente o VLAN-bundle, dentro de uma determinada EVI, eu continuo tendo um único bridge-domain, ou seja, uma única tabela de MAC address, porém, eu posso ter diversos domínios de Broadcast dentro dessa tabela de MAC address. Nesse cenário específico existem alguns pontos importantes, porque como eu tenho um único bridge-domain ou uma única tabela de MAC address, eu não posso ter MAC address duplicados dentro de uma mesma EVI, então todos MAC address desta EVI tem de ser MAC address únicos. Também não é possível fazer tradução de VLAN. Então dentro

de um único broadcast domain é [ininteligível] aqui uma VLAN, nesse caso VLAN 10, do outro lado, no outro PE eu tenho que manter essa mesma VLAN. E o tag de VLAN ID, ele é enviado pelo backbone de um PE para o outro. Nesse caso, como eu ainda mantenho uma única tabela de MAC address, o Ethernet-tag ID, ele continua sendo zero.

Então, como seria uma configuração dessa? Aqui na minha interface, na interface PE CE, eu tenho duas subinterfaces lógicas, eu tenho uma interface com VLAN ID 100 e uma outra interface com VLAN ID 101. Na minha instância VPN, as configurações tradicionais de EVPN, Route Distinguisher, Route Target, instant type EVPN e eu declaro as duas interfaces que tenho aqui, interface PE CE, dentro da instância EVPN.

Aqui a gente tem um outro exemplo de configuração, que ajuda um pouco a facilitar mais na hora de provisionamento. Ou seja, ao invés de eu criar uma interface lógica para cada interface física, o que eu posso fazer é criar uma única interface lógica e anexar um comandinho aqui, o VLAN ID list, declarando todos os tags de VLANs que estão nessa subinterface e que devem ser transportados para dentro da EVI. Dessa forma, eu tenho uma melhor escalabilidade, porque eu tenho um número menor de subinterfaces, eu tenho uma configuração menor, e se eu tenho uma implementação muito grande, eu vou ter também um commit mais rápido no Junos. Do lado da EVPN, simplesmente declaro essa interface, e todas VLAN IDs já são importadas automaticamente.

Aqui eu tenho o último tipo de serviço, que é o VLAN-Aware Bundle. Nesse tipo de serviço, dentro de uma única instância EVPN, dentro de uma única EVI, eu tenho múltiplos bridge-domains, ou seja, múltiplas tabelas de MAC address. Para cada tabela de MAC address eu tenho um único domínio de Broadcast. Nesse caso é permitido a tradução de VLAN, ou seja, normalização de VLAN. Se eu tenho aqui a VLAN número 1 conectada ao PE1, do outro lado eu posso ter a VLAN número 2, adress número 11 conectado ao PE2, isso não é problema. O tag de VLAN é enviado pelo backbone, do PE1 para o PE2, e uma diferença que para os dois modelos é que Ethernet-tag, ele utiliza justamente o valor da VLAN normalizada, que identifica este bridge-domain específico.

Então, como é a configuração desse tipo de serviço? Do lado do link PE CE ela não muda. Eu tenho aqui as duas subinterfaces, com as duas VLANs, a 100 e a 101. Do lado da minha instância EVPN eu tenho aqui uma modificação no Junos, em que eu declaro que é o tipo de instância é um tipo de instância virtual Switch, sendo que nos outros dois modelos eu tenho um tipo de instância EVPN. Route Distinguisher e VRF-target utilizam mesmo conceito dos outros tipos. Dentro do protocols EVPN, aqui eu já tenho que declarar quais são as VLANs que eu vou estar associando para esta EVI em específico. E aí, dentro dessa minha Route instant, dentro da EVI eu vou configurar meus bridge-domains. Nesse caso eu crio um Bridge domain com o nome BD 100, associando a essa subinterface aqui, e declarando qual é o VLAN ID, que é justamente o VLAN ID normalizado para essa bridge-domain.

Dentro do VLAN-Aware Bundle eu posso ter um cenário onde eu tenho... onde nem todos os bridge-domains pertencentes àquele EVI estão presentes em todos os PEs. Ou seja, em todos os roteadores meus de borda. Nesse caso, existe um espaço aí para otimização, do ponto de vista aqui de control-plane do EVPN. Então o que eu consigo fazer é justamente alocar distintos Route Targets, ou seja, um Route Target que seja específico para cada bridge-domain, e aí, com isso, eu consigo fazer com que essa rota seja importada apenas pelos PEs e EVIs que contenha aquele determinado bridge-domain.

Então, como seria essa configuração? Aqui dentro da minha instância EVPN a configuração é idêntica à do slide anterior que eu mostrei, sendo que aqui o que eu faço é incluir esse comandinho aqui que é o vrf-target auto. Dessa forma as rotas tipo 1, que são as rotas de auto-discovery, que eu vou descrever um

pouco mais à frente, elas utilizam ainda o route target que você configurou manualmente. Porém, as outras rotas, que já são associadas a determinado bridge-domain, como as rotas tipo 2 ou as rotas tipo 5, elas vão ter um Route Target que vai ser gerado automaticamente pelo próprio roteador. Existe também no nosso caso a possibilidade de usar um comandinho aqui que é o domain ID, que é justamente utilizado para quando você precisa utilizar overlapping de VLANs dentro de uma mesma EVI.

Bom, então como funciona o anúncio da rota tipo 2, nesse exemplo aqui, quando eu utilizo o parâmetro domain ID dentro de um determinado bridge-domain. Então, nesse caso a gente pode ver que esse é um output de um Junos, é uma rota tipo 2. A community de Route Target que é enviada é uma community que ela é gerada a partir tanto do valor da VLAN ID do bridge-domain, mas também utilizando o valor do domain ID que você configurou na Route instance, na EVI. A RFC, ela descreve um caso especial do modelo VLAN-Aware Bundle, que é justamente aonde eu tenho uma EVI utilizando o VLAN-Aware Bundle, que tem o Ethernet-tag none zero, porém, utilizando um único bridge-domain dentro daquela instância. Nessa configuração, a diferença que eu tenho para o VLAN-Aware Bundle tradicional é o instance type ao invés de ser um virtual switch, ele é um EVPN, porque eu só tenho um bridge-domain, e eu tenho a configuração desse comando VLAN ID, nesse caso, VLAN ID 200, que seria a VLAN normalizada desta EVI. Então o Ethernet-tag ID vai ser enviado com o valor 200.

[interrupção no áudio]. A questão do MAC address, [interrupção no áudio] nós temos um único bridge-domain, porém, é possível ter mais de um Broadcast domain. E, no caso do VLAN-Aware Bundle é possível ter múltiplos Broadcast domain e múltiplos bridge-domains. A questão do MAC address ser único, ela é exclusiva do modo VLAN-bundle, justamente porque eu tenho um único Bridge-domain, com múltiplos Broadcast domains. Tradução de VLAN é aceitável, nesses dois modelos a ponta, no VLAN-based e no VLAN-Aware Bundle, e o Ethernet-tag ID, que é o que identifica o bridge-domain, ele é zero nos dois primeiros modelos e, no último modelo, no VLAN-Aware Bundle ele identifica o bridge-domain daquele pacote específico.

Vou falar agora sobre os tipos de rota EVPN. Desde rota tipo 1 até a rota tipo 8. É importante a gente conhecer o funcionamento de cada um desses tipos de rota EVPN para a gente entender um pouco do modelo de operação do protocolo e também é importante para a hora de fazer troubleshooting na rede, para entender se alguma coisa está ou não funcionando corretamente.

Esse primeiro slide, ele pode parecer um pouco cheio de informação, mas ele é importante para a gente ter um resumo de todos os oito tipos de rota e suas principais funções. Começando com a implementação mais básica de EVPN, caso eu tenha apenas links PE CE em single-homed. Nesse caso eu vou ter apenas a presença de rotas do tipo 2 e rotas do tipo 3, justamente porque a rota do tipo 3 é uma rota utilizada para estabelecer o caminho do tráfego BUM, do tráfego Broadcast, Unknown-Unicast e Multicast. Ela é uma rota que ela é um single label que ele pode ser por bridge-domain ou por EVI, dependendo do tipo de serviço EVPN que nós temos aqui. E tenho a rota tipo 2, que ela vai justamente anunciar os endereços MAC address e endereços IP, que PE específico aprendeu naquela instância VPN, justamente com o label para promover a conectividade a esse host. Quando eu habilito um link PE CE multi-homed, aí eu tenho a presença também de rotas tipo 1 e tipo 4 na minha implementação de EVPN.

As rotas tipo 1, eu tenho ela em dois escopos diferentes. Uma rota tipo 1, cujo escopo é destinado a todos os PEs que contêm aquele ESI em específico, Ethernet Segment ID, e ela é utilizada para anunciar o label de split-horizon e habilitar convergência rápida na rede. A rota tipo 1 com o escopo EVI ou por bridge-domain, é utilizado para anunciar o label de áreas. E a rota do tipo 4, ela tem o escopo também por ESI, e ela é

utilizada para se fazer a eleição do DF, que eu vou explicar um pouco mais à frente. Essas rotas tipo 4 e tipo 1, elas são utilizadas no cenário de multi-homed. A rota tipo 5 é uma rota utilizada para troca de informações de prefixos IP, muito similar ao que nós temos hoje com a L3VPN. Rotas tipo 6, 7 e 8, elas são rotas focadas na otimização de tráfego Multicast. Cada uma dessas rotas eu vou explicar nessa seção em um slide específico.

Então, como eu comentei anteriormente, dentro do EVPN nós temos um conceito novo, que é o campo Ethernet-tag ID. Esse campo, ele tem 32 bits. Ele é enviado em todas as rotas EVPN, todos os tipos de rota EVPN, e ele pode ter dois valores. No caso da utilização do EVPN-MPLS, ele vai carregar o VLAN ID daquele bridge-domain específico. Então são os 12 bits naquele VLAN ID. E, no caso da utilização do EVPN com VxLAN, ele vai carregar o valor do VNI, ou seja, ele vai carregar o campo de 24 bits do VNI. Para o tipo de serviço VLAN-based ou VLAN-bundle, o Ethernet-tag, ele vai carregar o valor de zero, porque justamente o Ethernet-tag é o identificador do bridge-domain. Nesses dois tipos de serviço tem apenas um bridge-domain por EVI.

Então começando pelas rotas que são específicas por ESI. Então todas as rotas EVPN, ela sempre começa identificando o tipo de rota, nesse caso a rota tipo 1 ou a rota tipo 4, na sequência, tem alguns campos que estão presentes em todos os tipos de rota. Por exemplo, aqui esse primeiro campo é o Route Distinguisher, né? No caso dessas duas rotas, que é a rota tipo 1 por ESI e a rota tipo 4, elas são rotas que elas não são específicas de uma EVI, mas sim elas são rotas que possuem o Route Target, possuem todos os Route Targets das EVIs que estão ataxadas a esse ESI específico. Então nesse caso esse campo aqui que seria o Route Distinguisher é preenchido com router ID do roteador. Na sequência, eu tenho aqui o valor do ESI específico dessa rota, né? E os últimos campos aqui que identificam o Ethernet-tag, no caso da rota tipo 1, por ESI, ele é preenchido com FF, todos os bits em um. A rota tipo 4, da mesma forma que a rota tipo 1, o Route Distinguisher aqui é substituído pelo router ID. Eu tenho a identificação do ESI e, no campo que seria de Ethernet-tag, eu tenho justamente o IP que está originando essa rota tipo ele. Tanto a rota tipo 1 quanto a rota tipo 4, elas são anunciadas, porém, elas são só importadas pelos PEs que têm EVIs com esse determinado SI ataxado.

Agora, indo para as rotas que são específicas por EVI. Aqui eu tenho as rotas nesse slide tipo 1 e tipo 2, ou seja, eu tenho uma rota tipo 1 que anuncia esse ESI específico aqui atrelado a EVI. Então nesse caso eu tenho o Route Distinguisher que identifica aquela EVI, e o Ethernet-tag, ele vai com valor zero. No caso da rota tipo 2, eu tenho duas variações da rota tipo 2, uma variação na qual é anunciado apenas um MAC address do host, que está conectado àquela EVI. E, uma vez que aquele PE descobre o endereço IP daquele host, ele anuncia uma segunda rota tipo 2 com um MAC address e o endereço IP daquele host para toda a rede. Nesse caso aqui nós vemos que esse exemplo é um exemplo que veio de uma EVI configurado com VLAN-Aware Bundle, porque justamente aqui nesse campo de Ethernet-tag nós temos o valor que não é zero. Ou seja, valor 201, que simboliza a VLAN identificadora daquele bridge-domain dentro daquela EVI.

As rotas tipo 3 e tipo 6 também são específicas por EVI, então nesse caso aqui eu tenho a identificação do Route Distinguisher, nelas, eu tenho o Route Target específico daquele EVI, então ela é importada por todos os roteadores que possuem aquela EVI específica, eu tenho o Ethernet-tag. E aqui está a diferença, seria no caso da rota tipo 3, eu tenho o IP que originou a rota. E no caso do IP tipo 6 eu vou explicar à frente, mas ela carrega o Multicast group ID que está sendo anunciado e o endereço IP.

Bom, e as últimas duas rotas que nós temos são as rotas tipo 7 e tipo 8, que são as rotas de Multicast Join Sync e Multicast Leave Sync, que eu coloco aqui. Ela identifica a EVI, ela identifica o ESI específico daquela

operação, e ela identifica aqui também o grupo Multicast e o endereço IP. Esse seria a rota de Join, que é o 7, e a rota tipo 8, ela é similar, possui os mesmos campos, porém, tem a função de fazer Multicast leave.

Uma vez explicada os tipos de rotas, agora eu vou mostrar um pouquinho das operações EVPN, vai facilitar um pouco o entendimento de cada uma dessas rotas.

Então a primeira operação é o estabelecimento do caminho de BUM utilizando o método padrão, que é o Ingress Replication. Nesse caso, quando é configurado uma EVI em determinado PE, esse PE vai anunciar uma rota tipo 3, seja ele por bridge-domain ou por EVI, depende do tipo de serviço. E essa rota tipo 3, ela vai conter todas as informações que eu descrevi na seção anterior, e também um atributo que é o PMSI, o Provider Multicast Service Interface. Esse atributo é um atributo que vai descrever todas as informações para o caminho de tráfego BUM. Então, nesse caso aqui, como a gente pode ver no exemplo, eu tenho esse PE1, é o momento que a gente configurou essa EVI e vai anunciar essa rota tipo 3, dentro do atributo PMSI vai ter a descrição do tipo de LSP utilizado, no caso o Ingress Replication, a gente vai ter ali um label anunciado, nesse exemplo, o label F1, e um Tunnel ID para esse tipo de LSP.

Aqui é um output de uma rota tipo 3 no Junos. Então como ela aparece para você na tela do roteador. Alguns pontos que a gente identifica aqui que são importantes é justamente essa questão do atributo PMSI. Então aqui a gente pode ver que é anunciado um label específico, um Flood label para esse tráfego de Broadcast. Aqui é indicado o tipo de replicação, Ingress Replication. E o Route Target que é anunciado para essa rota em específico é o Route Target do bridge-domain, ou do EVI.

Então, como funciona essa operação? Uma vez que PE1 recebe um tráfego e ele precisa enviar esse tráfego, é um tráfego BUM, precisa enviar tanto para PE1 quanto para PE2, ou seja, todos os PEs que contêm aquela EVI específico. PE1 vai fazer uma cópia de cada um desses pacotes BUM e vai enviar para cada um dos PEs. Então ele vai enviar uma cópia desse tráfego para o PE2, utilizando o label F2, e ele vai enviar uma outra cópia desse tráfego BUM para PE3 utilizando o label F3. F2 e F3 são labels anunciados via rota tipo 3 pelos PE2 e pelo PE3.

Como é que funciona o aprendizado de MAC address? Nos links entre PE e CE o aprendizado de MAC address é feito do modo tradicional pelo data plane. E entre PE PE o aprendizado é feito através do próprio mecanismo do EVPN, através do control-plane, utilizando-se de rotas do tipo 2. Uma vez que o PE1 vai aprender o MAC address de qualquer um dos hosts aqui, ele vai anunciar uma rota tipo 2, que vai conter o MAC address aprendido e um label associado com esse MAC address. Esse label, ele pode ser um label por MAC address, ele pode ser um label por EVI, pode ser um label por bridge-domain, isso depende da implementação daquele fabricante para esse PE em específico.

Então, como funciona o encaminhamento do tráfego conhecido do known unicast. Imaginamos aqui o MAC origem 7, vai enviar um tráfego para o MAC destino 3 que está conectado a PE1, vai bater no PE3, PE3 conhece aquele MAC através da rota tipo 2, e ele entende, ele faz um look up, e ele vai ver que ele precisa enviar esse tráfego utilizando o label A1, foi o label anunciado aqui por PE1. Nesse caso, na nossa implementação, quando a gente utiliza o VLAN-Aware Bundle, o que o PE1 faz é recebendo nesse tráfego como A1, ele vai retirar esse label e vai fazer o segundo look up para determinar o bridge-domain daquele pacote específico. Ele vai determinar isso através do look up na VLAN. Existem algumas implementações, dependendo do fabricante, o PE1, ele pode anunciar labels distintos por bridge-domain, aí fica a cargo do fabricante.

Bom, vamos descrever agora o cenário de multi-homing, como funcionam as operações de multi-homing no EVPN. Um dos elementos-chaves para identificar se o link PE CE, ele é single-homed ou multi-homed é justamente o ESI. O ESI, ele é um campo de dez octetos, sendo que o primeiro octeto identifica o tipo de ESI, e os próximos nove octetos identificam o valor do ESI em si. Se o valor do ESI é zero, isso significa que o link PE CE é um link single-homed. Se o valor do ESI é um valor diferente de zero, significa que aquele link é um link multi-homed. Esse valor tem que ser um valor único para toda a rede. E o ESI, ele pode ser atribuído tanto a nível de interface física, ou seja, compartilhado por múltiplos EVIs. Ou pode ser configurado por interface lógica, ou seja, um ESI sendo único por EVI.

Os tipos de ESI. Coloquei a tabela aqui ao lado, descrevendo os tipos de ESI. São os tipos que constam na RFC. O tipo mais usado é o tipo 0 na qual o próprio operador configura manualmente o valor de cada ESI e faz o controle para que esse valor seja global para a rede. E os outros tipos de ESI produz valores derivados de alguns parâmetros da rede, mais algum denominador para fazer a diferenciação desse valor, como, por exemplo, derivando valor do sistema ID do LSP, derivando o valor do MAC address, de um router ID ou até do Autonomous System.

No cenário de multi-homing, o EVPN possui uma função, que é o Designated Forwarder. Basicamente o Designated Forwarder é responsável por enviar todo o tráfego de BUM para o CE. E os PEs que não são Designated Forwarder, ou seja, que são NDF, eles bloqueiam esse tráfego. Ou seja, no cenário de multi-homing, um CE, ele pode estar conectado com dois, três ou quatro PEs, e dentre esses quatro PEs, um deles é eleito o DF, que é o PE que vai enviar o tráfego BUM para o CE. Nesse exemplo os outros três PEs são NDFs. Todo tráfego que seja BUM não será enviado para o CE.

A eleição do PE, ela é feita a um nível de ESI ou a um nível de SI mais VLAN, depende da configuração. E a eleição é feita utilizando as rotas tipo 4. O método de eleição padrão descrito na RFC original é o service carving, que basicamente utiliza um algoritmo baseado em módulos, onde ele distribui cada combinação de ESI mais VLAN para um PE específico, assim com isso ele consegue fazer um balanceamento de carga a nível de subinterface. Existem outras formas também de se fazer a eleição de DF, desde configurando manualmente na mão, ou até outros métodos que estão saindo através de outras RFCs, mas que não são escopo dessa seção agora.

Então, como é feito a eleição do DF? É através da rota tipo 4. Aqui eu tenho o anúncio de uma rota tipo 4 no Junos. Um ponto interessante é que quando nós verificamos dentro do trabalho de roteamento, nós podemos ver que essa rota tipo 4, ela não pertence a nenhuma tabela, a nenhuma Route instance EVPN específico, ou seja, não pertence a nenhuma EVI específica. Essa rota, ela possui o ESI e, como community, ela possui uma community especial, que é essa ES-Import-Target, é uma Route Target específica, que ela não é associada com nenhuma EVI, mas sim ela é gerada automaticamente a partir do valor de ESI. Dessa forma essa rota tipo 4, ela é importada para trabalhar de roteamento apenas nos roteadores que possuem aquele ESI específico.

Um ponto importante para se notar é que apesar de que o ESI é um campo de dez octetos, apenas os primeiros seis octetos, como é mostrado aqui no slide, são utilizados para se montar o Route Target. Então se eu tenho, como esse exemplo, ESIs na qual eu vario apenas os últimos octetos, todos esses ESIs serão anunciados com o mesmo Route Target. Então todos esses ESIs vão ser importados por todos esses PEs, como nesse exemplo aqui, PE1 até o PE4. Então de forma a ter um controle de rotas mais eficiente é utilizado como melhoras práticas que a variação do ESI esteja entre esses primeiros seis octetos.

Para multi-homing nós temos basicamente hoje três opções de multi-homing. Então eu tenho tanto ativo-ativo, ou all-active, quando quanto opções de single-active, que vou descrever aqui. Opção de all-active, essa primeira aqui da esquerda, eu tenho a atualização de lag com LACP em ambos os lados, ou seja, tanto do CE quanto do PE. Nesse caso eu posso utilizar qualquer tipo de eleição de DF. O tráfego known unicast vai ser balanceado por todos links, e o tráfego de BUM será balanceado dessa forma, ou seja, do link CE/PE, ou seja, o link, tráfego do CE para a rede, para o PE, vai ser balanceado de forma all-active, pelo próprio CE, e o tráfego BUM, que vem da rede para o CE vai ser enviado apenas pelo DF, ou seja, single-active forwarder.

Para o caso dos cenários usando single-active temos duas opções. Então a primeira opção é a opção onde eu tento simular um cenário parecido ao VPLS ativo standby, onde nesse caso não é utilizado o LACP. No caso do PE, eu posso utilizar as interfaces de forma nativa, ou eu posso configurar um lag, mas sem LACP. No caso do CE, eu vou utilizar essas interfaces de forma nativa. O método de eleição de DF não tem impacto aqui, e o tráfego vai seguir essa linha, ou seja, PE/CE continua sendo single-active forwarder, ou seja, todo o tráfego de BUM vai descer apenas pelo DF, e o tráfego de CE/PE vai ser all-active forwarder, ou seja, o próprio CE vai fazer o seu balanceamento de carga e enviar o tráfego para os 4 PEs, o tráfego, tanto de BUM quanto o tráfego de unicast.

No caso do single-active multi-homing por IFD, nós simulamos um comportamento de MC-LAG ativo, standby. Nesse caso LACP é mandatório nos dois lados, justamente porque a diferença aqui é que eu faço uma eleição por DF através da interface física. De forma que o DF vai manter a interface up e os roteadores que são nDF vão colocar as interfaces em down. Dessa forma, tanto o tráfego PE/CE quanto CE/PE vão ser single-active forwarder, ou seja, vão utilizar apenas um dos links, porque os outros links estarão down.

Explicar aqui para vocês [ininteligível] Aliasing, para que ela funciona, qual o intuito dela. Então imaginando aqui um cenário onde eu tenho esse CE, esse MAC número 1, ele está em multi-homing, está conectado a PE1 e PE2. Ambos os PE1 e PE2, uma vez que você tem esse ESI ativo, eles vão anunciar uma rota tipo 1, que é essa rota AD por EVI, com mesmo ESI, anunciando junto um label de Aliasing. Mac 1, ele vai enviar um pacote para a rede, e aqui nesse exemplo ele enviou esse pacote devido ao hash do MAC 1, ele vai enviar esse pacote apenas para PE2. Então apenas PE2 vai anunciar esse MAC número 1 no aprendizado de data plane que ele teve, vai anunciar para a rede usando a rota tipo 2. Quando PE3 for responder aquele tráfego [ininteligível] de um lado para o outro, o PE3, quando for responder, ele vai identificar que aquele MAC address pertence a essa EVI, através da rota tipo 2, porém, ele vai identificar que existe uma rota tipo 1 por EVI, então, com isso, ele faz um balanceamento de carga desse tráfego indo por PE2 e PE1, justamente pela combinação de rotas tipo 2 e a rota tipo 1.

Como é anunciada essa rota tipo 1? Aqui eu tenho um output do Junos mostrando alguns detalhes nessa rota tipo 1. A gente percebe que ela é uma rota tipo 1 por EVI. Um dos pontos aqui é justamente o Ethernet-tag, que na outra rota tipo 1 ele é identificado por FF. Nesse caso, ele tem um número aqui zero. A rota tipo 1, ela já pertence à tabela de roteamento específica da EVI, daquela EVI, e ela é anunciada com um label de roteamento, ou seja, com um label de Aliasing aqui. O Route Target é o Route Target padrão da EVI. Essa é uma rota anunciada para todas as EVIs.

Agora explicar sobre o split-horizon, ou seja, como funciona esse mecanismo dentro do ambiente como multi-homing. O split-horizon, ele funciona aqui pelo seguinte: se eu tenho um host como esse aqui que eu envio um tráfego de BUM, e esse tráfego de BUM, ele chega em um PE, como nesse exemplo aqui, que é um nDF. Nesse caso, o PE, ele vai... esse PE3, ele vai encaminhar o tráfego para todos os outros PEs que

possuem a mesma EVI, então ele vai enviar para PE1, que vai encaminhar para a rede. Ele vai enviar para PE2 [ininteligível] nDF desse ESIB(F), não vai encaminhar para esse CE, mas ele vai encaminhar para outros hosts que ele tem dentro da mesma EVI e vai enviar também para PE4. Porém, como o PE4 é um DF desse mesmo ESI, ele tem que ser avisado que esse pacote em específico, ele não pode voltar para esse ESI. Então o PE3, quando vai enviar o tráfego de BUM para PE4, ele identifica que PE4 possui o mesmo ESI de onde veio esse tráfego, e ele coloca junto o label SH, o label de split-horizon. Com isso, o PE4 vai identificar que esse tráfego, esse pacote específico não deve ser enviado de volta a esse CE, e sim para outros hosts dentro dessa mesma instância.

Então, como é anunciado esse label, esse label é anunciado através da rota tipo 1 por ESI, que a gente já falou ali anteriormente, mas aqui eu tenho um output dessa rota, que a gente pode ver que aqui eu tenho o anúncio do label, do label SH para aquele PE específico. E essa rota, ela possui todos os Route Targets, ou melhor, o Route Target de todas as EVIs que compartilham daquele ESI.

Então a função, resumindo aqui a função da rota tipo 1 por ESI, distribuir o label de SH que é necessário nessa situação de uma situação de multi-homing. E também uma outra função importante é de fazer o mass withdrawal, ou seja, fazer a convergência rápida em caso de falha. Uma vez que o link PE CE falha, aquele PE específico, ele vai remover a rota tipo 1 por ESI da tabela de rotas dele. Com isso, todos os outros PEs da rede, eles vão invalidar todos aqueles MAC address que estão associados àquela ESI específica.

Como é feito o split-horizon no caso de uma rede com EVPN VxLAN? Esse é um dos ajustes que foi necessário ser feito, que é na RFC 8365. No caso do VxLAN, a gente não tem um label SH. Então no caso do VxLAN, como é identificado o split-horizon? Através do IP de origem do cabeçalho de túnel. Ou seja, o PE vai fazer um look up no IP origem e baseado nessa informação ele vai utilizar a funcionalidade de split-horizon para evitar escoar aquele tráfego de BUM de volta para aquele CE que originou o tráfego BUM.

[interrupção no áudio]. Eu coloquei isso na tabela para a gente entender um pouquinho das diferenças e benefícios que o EVPN traz sobre o MC-LAG. Então, o primeiro deles é a questão de você ter um multi-homing com mais de dois PEs, no caso do MC-LAG, eu tenho essa limitação de apenas dois PEs, no EVPN eu consigo ter múltiplos PEs. A questão do suporte ativo standby, ativo-ativo, isso nós temos suporte nos dois lados. A diferença aqui é que EVPN possui... é uma tecnologia padronizada, interoperável entre fabricantes, eu não tenho a necessidade de ter um link inter-chassis. E caso precise ter um gateway L3, esse gateway L3, essa interface L3, ela é nativa no EVPN. Diferente do MC-LAG, que eu preciso ter um VRRP configurado ali entre as duas caixas.

Então, fazendo um resumo dessas informações de data plane, eu coloquei essas duas tabelas que a gente consegue identificar para cada uma das operações quais são os labels ou as informações no caso do VxLAN, informações de VNI. No caso do EVPN-MPLS, eu sempre vou ter um primeiro label que identifica o transporte MPLS, seja ele RSVP, lDP ou até Segment Routing. Para o meu segundo label, ele depende da operação que eu estou utilizando. Então operações Unicast, Unicast single-homed ou single-active, eu vou ter apenas o label anunciado na rota tipo 2, o label do MAC IP para operações Unicast, mas ativo/ativo. Aí eu tenho também utilização do label de Alias(F). Para o tráfego BUM, eu tenho utilização do label Inclusive Multicast, é o label anunciado pela rota tipo 3... e isso para o single-homed. Para o caso onde eu tenho multi-homed, seja ele single-active ou all-active, eu tenho também o anúncio, a utilização aqui do label de Split Horizon. No caso da VPN VxLAN é um pouquinho diferente. Ou seja, eu sempre tenho a utilização do

VNI, que é o identificador do campo, o identificador do VxLAN. E apenas para as operações de BUM multi-home o roteador vai ler o campo de VNI e também o campo de IP origem daquele pacote.

Falar para vocês agora da rota tipo 5, que é justamente a rota utilizada para fazer troca de informações de prefixos IP, entre PS(F). A rota tipo 5, ela foi criada, puxada principalmente pelos casos de uso de Data Center, utilizada para fazer... para estabelecer conectividade inter-subnet e troca de prefixos de IP entre Tenants distintos.

É, os primeiros, os principais casos de uso, então, são estabelecer um roteamento entre distintos Tenants em um mesmo Data Center, quando eu utilizar o tipo de rota 2, tipo 2, eu tenho um roteamento assimétrico, quando eu tenho, utilizar um tipo 5, eu tenho um roteamento simétrico. E também para casos de uso de interconexão de Data Center, onde eu consigo anunciar, por exemplo, todos os prefixos IPs que eu tenho em um determinado Data Center para o outro Data Center, assim, facilitando a comunicação entre ambos.

Então, como seria um roteamento utilizando o VPN, EVPN VxLAN com apenas rotas tipo 2, ou seja, o roteamento assimétrico. Então, aqui eu tenho um exemplo, eu tenho o host nº 1 e o host nº 2. Ambos possuem IPs em subnets distintas e em VLANs e VNIs distintos. O gateway desse host nº 1, ele está configurado aqui no meu Switch Leaf 4, não é? Ou seja, quando ele envia um pacote destinado a outras subnet IP, ele vai bater aqui no gateway do Leaf 4. Esse Leaf 4 vai fazer o roteamento, vai procurar qual que é a rede destino, vai identificar que a rede destino é o VNI 50250, que tem destino aqui, e ele vai mandar esse tráfego direto para esse VNI até o Leaf 6, que vai... quando esse tráfego chegar em Leaf 6, Leaf 6 só vai fazer lookup L2 e encaminhar esse pacote aqui diretamente.

Então, o roteamento é feito uma vez a partir do Leaf de origem. A desvantagem que eu tenho aqui é que se eu tenho uma rede grande, com vários Switches, com vários VNIs e várias VLANs, esse Leaf 4 vai ter que aprender todas as VLANs e ter acesso a todos os VNIs de todos os Switches para poder fazer o roteamento entre Tenants.

Roteamento simétrico, utilizando uma rota tipo 5. Nesse caso, como é feito o roteamento, eu crio a... o gateway, a interface IRB no Junos, aqui no Leaf 4. E eu crio uma outra IRB aqui no Leaf 6. Ou seja, tanto no leaf de origem, quanto no leaf de destino.

Entre esses dois leafs, nós criamos uma VLAN, uma VNI específica, nesse caso aqui a 1100, que é a VNI de roteamento. E a partir da rota tipo 5, os prefixos IP são anunciados de um Switch para outro. Dessa forma, quando o host envia um pacote para Leaf 4, que é o default gateway. Leaf 4 vai consultar a tabela de roteamento, identificar aqui essa rede de host 2, está atrás desse VNI 1100, vai encaminhar o tráfego, o pacote, utilizando essa rede entre Switches.

Quando chegar em Leaf 6, ele vai fazer o roteamento da VLAN 1100 para a VLAN VNI 50240. Dessa forma, as VNIs, ou... e VLANs não precisam ser estendidas de todos os leafs para todos os leafs, apenas tendo uma VNI específica para fazer esse roteamento já é suficiente.

O EVPN já possui alguns mecanismos de otimização de tráfego BUM que são nativos ao protocolo, um deles é o mecanismo para a redução de tráfego ARP, o que eu vou explicar aqui nessa seção.

Quando nós temos uma rede com muitos hosts, é uma rede L2 estendida, com muitos hosts, ela pode ter um impacto negativo na operação, principalmente devido à utilização do ARP para o IPv4 ou o ND para o IPv6. Isso porque, tipicamente, os roteadores, eles vão processar os pacotes ARP através do software. Ou

seja, esse pacote vai subir para a routing engine e, com isso, eu posso causar uma sobrecarga na CPU do roteador, por que ali eu tenho uma limitação maior em termos de recurso. Então, como que o EVPN trata essa questão do ARP?

A forma mais fácil de explicar é usando um exemplo, então eu tenho... esse aqui é um exemplo da funcionalidade de ARP suppression um do EVPN. Eu tenho aqui um host A, ele vai enviar um primeiro pacote de ARP para o host B. Esse pacote vai saído(F) pelo primeiro PE, e esse PE vai fazer o flooding desse pacote para toda a rede, até que esse pacote chegue ao host B. O host B vai receber esse pacote e o PE 1 vai, ao mesmo tempo, apreender essa informação do host A e vai converter isso em uma roda tipo 2. Essa rota tipo 2 vai ser encaminhada para o Router Reflector e vai enviada para todos os PEs da rede, de forma que todos os PEs da rede vão conhecer esse MAC Address e esse IP que gerou esse primeiro ARP.

Quando o host B for responder ao host A, ele não vai encaminhar esse pacote para o primeiro PE que está diretamente conectado, esse PE já conhece o MAC Address A, o IP A, e ele vai encaminhar a resposta de ARP diretamente para o host A. Dessa forma, o primeiro PE, ele vai aprender o MAC B, o IP B, e vai anunciar, da mesma forma, através da rota tipo 2 para a rede, e todos os PEs da rede vão, agora, conhecer tanto o MAC A, quanto o MAC B.

O que acontece quando um terceiro elemento entra na rede? Ou seja, aqui nós temos o host C. O host C, ele vai enviar um ARP request com o target no host B, porém o próprio PE que está diretamente conectado a ele já conhece tanto o MAC quanto o IP daquele host B. Então ele já faz um ARP replying, porque ele tem configurada a função de ARP suppression. Ao mesmo tempo que ele faz esse ARP replying para notificar o host C, ele já anuncia esse MAC Address, ou seja, o MAC Address C e o IP C, para rede, de forma que toda a rede também já vai conhecer o MAC Address C e o IP C.

Quando... imaginemos aqui que o host B, ele vai ter a sua tabela de ARP expirado, então quando ele for fazer novamente um ARP request, esse ARP request vai ser suprimido pelo PE, e o próprio PE vai responder esses ARP requests. Ou seja, os próximos ARP requests e replying, eles não são enviados na rede, porque todos os PEs já conhecem os MAC Addresses e endereço IP de cada um desses hosts na rede.

Eu descrevi aqui nesse exemplo a operação utilizando o ARP, que é para o caso do IPV 4, mas para o caso do IPv6, ou seja, utilizando-se do ND, é exatamente o mesmo processo, a única diferença é o protocolo utilizado.

Vou descrever agora as otimizações que nós temos de tráfego Multicast. Se você lembrar, na sessão anterior, todo o tráfego Multicast estava sendo entregue através do método de Ingress Replication, mas o EVPN traz algumas melhorias, utilizando algumas novas rotas e alguns mecanismos que eu vou descrever aqui.

Então, em uma implementação básica de EVPN, a rota tipo 3, ela anuncia um caminho de BUM utilizando o Ingress Replication. No método de Ingress Replication, o tráfego Multicast ele é entregue a partir do PE de Ingress para todos os PEs de Ingress que participam daquela instância EVPN específica, e cabe ao PE de Ingress entregar ou bloquear aquele tráfego Multicast, baseado em estado de... se ele é um DF ou um NDF, e baseado na informação que ele tem de IGMP, que chegou pela LAN, ou seja, pelo host.

Então, todo o tráfego de Multicast, ele é enviado pela rede, quer seja solicitado pelo receiver ou não. Existem dois aspectos de ineficiência nesta distribuição de tráfego básica do EVPN. Então, o primeiro deles é: se você tem um tráfego Multicast pequeno, esse pode não ser o problema, mas se você tem um tráfego de Multicast um pouco maior, ele pode ser melhor otimizado utilizando algumas técnicas. A primeira delas

é: no EVPN, e no MPLS, ao invés de eu utilizar LSPs ponto a ponto, eu passo a utilizar LSPs ponto multiponto, anunciadas(F) pela rota, pela própria rota tipo 3.

No caso do EVPN VxLAN, nós temos uma funcionalidade chamada Assistant Replication, que eu vou descrever nos próximos slides, onde a replicação de tráfego Multicast pode se dar em um nó centralizado na rede, tipicamente um spine. A outra forma de otimização de tráfego Multicast é que no Ingress Replication, o tráfego Multicast é distribuído para todos os PEs, independente se você tem algum receiver naquele PE ou não. Da mesma forma, existem extensões, que é justamente o que eu vou abordar aqui, as rotas tipo 6, 7 e 8, que podem anunciar se [ininteligível] do PE possui receivers Multicast que estão interessados em um determinado conteúdo, e dessa forma a filtrar o tráfego Multicast a ser enviado.

Então, começando pela utilização do ponto multiponto, então no caso de uma EVPN MPLS, o que pode ser feito é a utilização de um LSP MPLS ponto multiponto na rede. Esse LSP ponto multiponto, ele é anunciado pela mesma rota tipo 3, a diferença é justamente o atributo PMSI, que ao invés de anunciar um LSP de Ingress Replication, ele vai anunciar um LSP com as informações daquele ponto multiponto. Dessa forma, o pacote, quando ele sai do Ingress PE para a rede, ele vai ser enviado apenas uma vez, e a replicação naquele conteúdo, ela é feita mais próximo possível do PL de saída.

A outra forma que nós temos é utilizando o Assistant Replication, como eu comentei nesse caso, é uma funcionalidade mais utilizada no ambiente de EVPN VxLAN. Nesse caso, no ambiente de EVPN VxLAN, tipicamente nós temos uma topologia Clos 3, onde eu tenho dois, três ou quatro spines, e todos os Switches Leafs estão conectados diretamente no spine. Eu configuro o Assistant Replication no spine, então, dessa forma, o meu Switch de leaf, ele vai enviar apenas uma cópia do tráfego Multicast para o spine, e o spine vai ser o responsável por fazer essa replicação de tráfego para os outros leafs. Os spines tipicamente são os Switches que têm mais recursos computacionais, então, você consegue desafogar inclusive os Switches Leafs dessa tarefa de Multicast, caso você tenha uma grande quantidade de tráfego Multicast na sua rede.

Agora sobre as rotas tipo 6, 7, 8. A rota tipo 3, que eu comentei anteriormente, era uma rota onde eu anunciava, por padrão, o Ingress Replication, que ele anuncia uma árvore IMET, que é a Inclusive Multicast Ethernet Tag.

Com a rota tipo 6, eu consigo anunciar um caminho Selective Multicast Ethernet Tag. Como é que funciona isso? O PE ele vai fazer a leitura da informação de IGMP Join, e ele vai converter essa informação de IGMP Join dos hosts em uma rota tipo 6. Então uma vez que ele recebeu esse Join IGMP, ele vai converter isso em uma rota tipo 6 e vai anunciar para a rede, vai anunciar isso para o router reflector, vai redistribuir na rede, de forma que todos os outros PEs vão saber que esse PE, em específico, ele tem receivers Multicast interessados no grupo Multicast A, nesse exemplo aqui.

Então, dessa forma, quando o PE de Ingress for enviar o tráfego Multicast, ele sabe para onde ele tem que enviar. Ou seja, ele tem um source A, ele sabe quem são os receivers daquele conteúdo lá e quando ele receber um conteúdo do source B, ele também conhece quais são os receivers daquele source B.

Existe um outro ponto importante, que é justamente em um cenário de multi-homed, eu posso ter o cenário onde o host vai enviar um IGMP Join em um PE que seja NDF. Nesse caso, pode ocorrer uma falha de sincronismo entre os PEs, porque os estados Multicast não estão sincronizados e isso pode causar problemas.

Nesse caso, foi criado as rotas tipos 7 e tipo 8, que são rotas que são anunciadas aqui entre esses PEs para justamente anunciar o estado IGMP de cada um deles. E como funciona isso, não é? Nesse exemplo aqui, eu tenho um receiver, um Multicast receiver, um host, ele está conectado em dois leafs, esse Leaf 2 é o DF, o Leaf 1 é um NDF. E a origem no conteúdo, o Multicast está conectado em um Leaf 3. Sem a rota tipo 7, quando o receiver, uma vez que ele envia esse pacote Join para um leaf, que é o leaf NDF, ele vai criar o estado IGMP nesse primeiro leaf, no Leaf 1.

O conteúdo Multicast vai chegar até o Leaf 1 e o Leaf 2, porém como esse Leaf 1, ele é um NDF, esse conteúdo Multicast não vai ser encaminhado para o receiver. O Leaf 2, ele é o DF, ele é o Switch que pode encaminhar esse conteúdo Multicast, porém ele não tem o estado IGMP aqui. Então, ele não vai fazer esse encaminhamento de tráfego.

Como a rota tipo 7 resolve isso? Basicamente, o receiver, voltando aqui no exemplo, ele vai enviar o IGMP Join, porém o Leaf 1 vai encaminhar uma rota, vai gerar uma rota tipo 7 para o Leaf 2, de forma que também gere o estado IGMP para o Leaf 2. Dessa forma, quando chegar o tráfego Multicast, o Leaf 2, que é o DF, vai poder encaminhar o conteúdo Multicast para o receiver.

No caso do leaf, do IGMP leaf, é a mesma forma. Ou seja, uma vez que o conteúdo está correndo, pode acontecer de o leaf chegar em... um dos leafs, que eu tenho aqui, ele vai parar o conteúdo, porém o outro leaf, o meu Leaf 1, ele vai continuar enviando o conteúdo Multicast, porque ele ainda tem o estado IGMP.

Então, com a utilização da rota tipo 8, eu consigo fazer esse sincronismo entre os dois leafs, de forma que quando o leaf chega, o IGMP leaf chega no Leaf 2, esse Leaf 2 vai gerar uma rota tipo 8, de forma a apagar o estado de IP de ambos.

Bom, como eu comentei ali no começo do webinar, esse último capítulo eu deixei reservado para falar rapidamente sobre a arquitetura de Data Center utilizando EVPN. A arquitetura do Data Center, ela mudou um pouco com a utilização do EVPN, então, eu queria compartilhar aqui com vocês algumas dessas informações.

Como são feitas as arquiteturas de Data Center, hoje, as mais novas, né, são sempre utilizando um Clos, um IP fabric tipicamente de três estágios. Ou seja, três estágios porque eu tenho os Switches Leafs e eu tenho os Switches Spines. Os meus hosts, ou os meus servidores, os meus serviços tipicamente são conectados aqui nesses leafs. E todo leaf, ele está sempre a três [ininteligível] de um outro leaf. Ou seja, o Leaf 1, por exemplo, para chegar até o Leaf 4, ele vai acessar ou o Spine 1 ou o Spine 2 e vai chegar até o Leaf 4. A questão de uma rede multi-tenant, uma rede onde eu tenha múltiplas subnets por tenant e que eu tenho que prover também trânsito L2 e L3. Todos esses são requerimentos típicos de um Data Center de nova geração.

Então, nesse tipo de arquitetura, quais são as nossas melhores práticas, não é? Nesse caso, a gente usa sempre uma camada de underlay e uma camada de overlay. Qual é a diferença? A camada de underlay a justamente a camada onde... ela prover conectividade entre os hosts, ou seja, entre leafs e spines. Tipicamente a gente utiliza EBGP para isso, para simplificar, até, o designer, mas também pode ser utilizado qualquer protocolo de roteamento, como SPF, ISS ou até mesmo rota estática.

E para a camada de overlay, ou seja, é a camada onde efetivamente roda o EVPN, então, nesse caso, a recomendação é que se use IBGP, utilizando-se dos spines como Router Reflectors para fazer a reflexão das rotas EVPN entre os leafs.

Quande se precisa ter um Clos maior do que o de três estágios, o que nós fazemos é expandir esse fabric para um Clos de cinco estágios. Cinco estágios porque, novamente, o pior caminho entre dois leafs vai ser tendo cinco hops. Ou seja, ele vai partir desses dois hops, mais um super-spine e mais outros dois hops do outro porte. Dessa forma, a gente consegue manter a arquitetura do Data Center o mais simples possível é o mais previsível em termos de latência e throughput.

Quais são as opções que nós temos para conectividade, servidor ou host com os leafs. Então, hoje um Data Center, tipicamente, você poderia utilizar um LAG, um MC-LAG, que é o que se usou aí por muito tempo. Com o advento agora do EVPN, esse host, ele pode continuar tendo o mesmo LAG, porém, aqui, entre os Switches eu não preciso mais rodar MC-LAG. Eu rodo simplesmente EVPN, associando cada uma dessas interfaces, o mesmo ESI, e lançando mão de toda a maquinaria de EVPN que for descrita aqui nesse webinar.

Então como é uma configuração simples dessa, dentro do Switch eu crio uma interface agregada, eu crio um LAG. Para quem conhece um pouco de Junos, então, eu crio uma interface AE0, nesse exemplo, e aí eu vou configurar o ESI. Então, neste exemplo aqui eu tenho um ESI tipo 0, não é? Com todos os outros dígitos em 1, ativo/ativo. Eu configuro um system ID, essas informações, elas têm que ser as mesmas em todos aqueles Switches que são conectados àquele mesmo host, e aí eu coloco, simplesmente eu crio as minhas subinterfaces, nesse caso aqui, a subinterface 200, e associo ela com uma VLAN.

No caso do EVPN VxLAN, essa VLAN dentro do Junos, é o que representa um bridging domain(F), e dentro desse bridging domain(F) eu associo o meu VNI, Nesse caso aqui, um VNI 200, e a associo à interface local. Configuração é bem simples.

Como eu identifico o funcionamento, não é? Uma vez que eu configurei, que eu fiz essa configuração, automaticamente o roteador já vai anunciar as rotas tipo 1, essas são as rotas que eu descrevi no início do webinar, tipo 1 por ESI, a rota tipo 1 por EVI para esse ESI específico, então, tem aqui a identificação desse ESI. E a gente vai ver também as rotas tipo 2, as rotas tipo 2 anunciando o MAC Address daquele host e uma rota tipo 2 anunciando o MAC Address mais o endereço IP daquele host.

A gente pode separar, ou categorizar as arquiteturas de Data Center em basicamente três modelos, ou três tipos, sendo eles o que a gente chama de bridge overlay, centrally-routed bridging ou edge-routed bridging. Quais são as diferenças? Então no bridge overlay, eu não tenho nenhuma configuração de L3 dentro da EVPN aqui. Então todos os meus servidores, eles têm uma conexão em L2 entre eles, ou seja, o fabric é apenas um transporte L2, sendo que os gateways, eles têm que estar em elementos fora do fabric.

No centrally-routed bridging, eu posso configurar o gateway das minhas VLANs nos spines. Então, eu tenho esses gateways centralizados nos spines. A função dos leafs, na verdade, é apenas uma função de L2 gateway, ele apenas encaminha esse tráfego L2 para um spine e esse spine vai fazer toda a função L3. Nesse caso, a conectividade com o mundo exterior, ela é feita aqui no nível de spine.

E eu tenho a outra possibilidade, que é justamente eu trazer os gateways, ou seja, o L3 gateway para os Switches Leafs. Então, nesse caso o host que está conectado, ele vai ter como gateway o próprio leaf, que está aqui distribuído em todos os leafs. Aí o spine, ele tem a função de lean spine. Ou seja, lá ele faz simplesmente a comutação de tráfego VxLAN de um leaf para outro.

Ou seja, como eu comentei, no bridge overlay, se eu tenho aqui uma VLAN azul, ela vai ser... vai ter a comunicação através do próprio leaf. Se eu tenho uma comunicação aqui dessa VLAN verde, ela vai passar pelo fabric e vai sair uma comunicação em L2. Se eu precisar fazer uma comunicação entre Tenants, ou

seja, entre a VLAN azul e a VLAN verde, eu preciso que um roteador externo ao fabric faça essa comunicação para mim.

E no caso das arquiteturas centrally-routed, ou edge-routed, o próprio gateway L3, ele que vai estar no fabric, seja ele no spine ou no leaf. Então aquele mesmo exemplo, quando a VLAN azul, está aqui, precisa se comunicar com a VLAN verde, e esse tráfego vai subir até o spine, onde está o gateway, e vai descer até a VLAN verde.

No caso do edge-routed, quando a VLAN azul precisar se comunicar com a VLAN verde, essa comunicação não precisaria subir até o spine, ela é feita diretamente no próprio leaf.

Bom, esse era o material que eu tinha para apresentar para vocês. Espero que tenha sido claro nas explicações, espero que possa ser bem aproveitado aí por vocês e obrigado. O meu nome e contato estão aqui na tela. E acho que a gente pode ir para as perguntas agora.

SR. EDUARDO BARASAL MORALES: Obrigado, Eduardo. Realmente, foi muito interessante tudo o que você mostrou para a gente. A gente teve um probleminha com a transmissão, eu queria saber se você poderia falar um pouquinho daqueles slides que a gente ficou sem o áudio. O slide, eu acho que era 35. O pessoal ficou aí bem curioso sobre o que você demonstrou. Então, se você puder falar um pouquinho antes de a gente ir para a parte de perguntas, acho que ficaria bom para a gente complementar essa parte.

SR. EDUARDO HARO: Opa. Vocês estão me ouvindo? Ah, agora sim. Desculpa, eu estava no... eu estava rodando aqui o YouTube, em paralelo, não consegui ouvir a tua voz, Eduardo. Deu... Poderia repetir?

SR. EDUARDO BARASAL MORALES: Não, sem problemas. É que eu estava comentando que a gente teve um probleminha na transmissão no slide 35. Você consegue compartilhar aí para a gente, fazer a explicação de novo?

SR. EDUARDO HARO: Deixa eu abrir aqui. Um minutinho. Ver se eu consigo... Deixa eu compartilhar minha tela aqui. Cadê? Share screen. Vocês conseguem ver a minha tela? Beleza. Não sei se eu consigo diminuir isso aqui, bom, deixa eu pôr aqui em uma...

Bom, essa é a tela 35, eu acho que foi nessa tela que parou. Esse slide eu montei aqui pensando em fazer um resumo dos três tipos de serviço que nós temos no EVPN, tá? Ou seja, toda a explicação desse capítulo que eu descrevi os três modelos, não é? E aqui eu coloquei uma tabelinha para poder comparar e ficar mais fácil de a gente entender de uma forma mais resumida a diferença entre os três, não é?

Então, no modelo VLAN Based, no modelo VLAN Bundle e no modelo VLAN Aware Bundle. Esses três modelos, eles utilizam até os... eu estou usando os mesmos nomes da RFC, tá? Então fica bem fácil de você depois abrir lá a RFC 7432 e poder entender e fazer a ligação aqui, não é? Mas de uma forma bem resumida, então, quais seriam as diferenças? Bom, no Junos, a routing instance que eu crio, né, aí já é bem específico do Junos. Para os dois primeiros modelos é do tipo EVPN, aqui no VLAN Aware, eu uso o virtual switch. Deixa eu ver se tem alguma pergunta. Ah, tá.

As principais diferenças aqui estão justamente em como você aloca recursos de tabela de bridging domains(F), tabelas da instância de EVPN, ou seja, a EVI, e o broadcast domain. Então, a tabela de bridging domain(F), que nós temos por EVI, ela, tanto no cenário VLAN Based, quanto no cenário VLAN Bundle, ela é apenas uma única tabela, como a gente vê nas figuras aqui do lado, não é? E o VLAN Aware Bundle é

onde a gente consegue ter dentro de uma única EVI múltiplas tabelas de bridging domain(F). Ou seja, múltiplas tabelas de MAC Address.

A diferença do VLAN Based para o VLAN Bundle está justamente aqui nessas duas linhas, que é a linha do broadcast domain. Ou seja, no VLAN Based eu tenho apenas uma tabela de bridging domain(F) e uma tabela de broadcast domain. Ou seja, um domínio de broadcast domain. No caso do VLAN Bundle eu tenho [interrupção no áudio] uma única tabela de bridging domain(F), mas eu posso dividir ele em vários broadcast domains, ou em várias VLANs, mas a tabela continua sendo a mesma. Por isso a questão do MAC Address único no caso do VLAN Bundle. Ou seja, se você tem duplicação de MAC Address, mesmo que eles estejam em diferentes VLANs, isso pode ser um problema no caso do VLAN Bundle, não é?

A questão de tradução de VLAN é outro ponto também que... determinante aqui. Ou seja, no VLAN Bundle, como... eu não posso, não é permitido tradução de VLAN, justamente porque o target de VLAN é utilizado para poder mapear aquele tráfego dentro de uma determinada, um determinado domínio de broadcast.

E o último ponto interessante aqui é que era justamente o Ethernet Tag, que é o identificador do bridging domain(F), não é? Ou seja, no caso do VLAN Based e do VLAN Bundle ele é zero, porque eu só tenho uma única tabela de bridging domain(F) dentro de uma instância EVPN. E no caso do VLAN Aware Bundle, então aqui eu... é diferente de zero, porque é justamente o identificador daquela minha tabela de bridging domain(F) dentro da EVI, não é? Eu acho que o Eduardo comentou que tinha mais um slide...

SR. EDUARDO BARASAL MORALES: É, tem o slide 62.

SR. EDUARDO HARO: Sessenta e dois, não é?

SR. EDUARDO BARASAL MORALES: Sessenta e dois.

SR. EDUARDO HARO: É esse slide, Edu?

SR. EDUARDO BARASAL MORALES: Sim.

SR. EDUARDO HARO: Tá. Bom, aqui o que eu quis comentar é justamente fazer uma comparação entre o uso do MC-LAG com o EVPN. Eu até comentei no chat, uma das perguntas que eram voltadas aí para EVPN e empresas, não é? Ou empresas... Até tinha um pessoal me perguntando sobre Data Centers, não é? É possível substituir a tecnologia atual de MC-LAG por EVPN. Isso é até um passo evolutivo que a gente tem visto, não é?

E quais seriam as vantagens que nós temos? Você pode... você não precisa ter todo o framework de EVPN funcionando com todas as funcionalidades para substituir MC-LAG. Você pode ter simplesmente dois switches, exatamente como você tem na topologia do MC-LAG, e substituir, e colocar a EVPN apenas nesses dois switches. Você já consegue substituir por completo o MC-LAG.

Quais as vantagens? No caso do MC-LAG você está limitado sempre a dois PEs, apenas, ou seja, dois switches. O EVPN, você não tem essa limitação de apenas dois equipamentos, não é? Você pode utilizar quantos equipamentos você precisar para a sua necessidade de tráfego. Suporte ativo/ativo, ativo/standby.

Um ponto bem importante, a gente não precisa ter o Inter-Chassis Link. Ou seja, no MC-LAG, quem já configurou MC-LAG sabe que você tem que configurar um link entre os dois switches para que seja feito o sincronismo do protocolo, não é? No EVPN, você não precisa ter esse Inter-Chassis Link.

O EVPN é uma solução padronizada, então, ela é interoperável. Então além de trazer, lógico, claro, a questão que você não precisa trabalhar com protocolos proprietários, né, também te traz toda a questão de evolução do EVPN. Ou seja, conforme o mercado for lançando novas funcionalidades de EVPN, isso vem sendo herdado pelo próprio modelo de equipamento que você tem, não é? E a questão de gateways L3, então, dependendo da tua configuração, você não precisa ter um gateway, uma outra configuração de VRP(F), no caso do MC- LAG, para fazer o gateway da sua rede LAN. Isso já é feito inerente no próprio EVPN.

SR. EDUARDO BARASAL MORALES: Muito obrigado aí, Eduardo. Pedimos desculpas aí, pessoal, pela Transmissão que cortou aí esses slides. Mas eu acho que agora, com essa explicação, deu tudo certo.

Bom, antes de ir para a parte de perguntas, eu gostaria de deixar alguns avisos aí para o nosso público. O primeiro deles é relacionado ao formulário de avaliação. Então, a gente tem aí um QR Code que vai colocar na tela. É um formulário para você dizer o que você achou dessa conversa que a gente teve aí com o Eduardo Haro.

Então, o pessoal vai estar postando ali o QR Code. Então, são duas perguntinhas, coisas simples. Uma delas é uma nota de zero até dez, e a outra é: o que a gente pode melhorar? Então a gente levanta estatísticas, a gente estuda os comentários que vocês fazem, tudo isso para a gente poder fazer eventos melhores para vocês. Então, é muito importante que vocês respondam para a gente esse formulário de avaliação. Mas isso daí é um formulário de avaliação, não é relacionado ao certificado. Então são coisas aí independentes.

O pessoal vai colocar agora o link aí no chat que é relacionado ao formulário de inscrição para ganhar o certificado, tá? É um outro link. Que a gente vai fechar ele às 2 horas da tarde. Então, depois que passou as 2 horas, não adianta, a gente não vai fornecer mais nenhum certificado. Então se inscrevam até às 2 horas da tarde para você ganhar aí o certificado de participação nessa live que a gente fez agora.

Então são duas coisas para vocês fazerem, o formulário de avaliação, para dar uma notinha para nós, para a gente, não é? Para a gente saber como é que foi essa live de hoje. E o formulário de inscrição aí para ganhar o certificado, caso alguém queira.

Bom, indo aí para a parte de perguntas, então, eu já queria agradecer, Eduardo, por toda a sua disposição aí no chat, a gente viu que teve bastante interação, o pessoal estava aí bastante curioso sobre essa tecnologia EVPN. E agora a gente vai ler as perguntas que o pessoal postou aí no chat para você.

E já puxando um gancho que você já fez aí na sua explicação final, não é? Teve ali uma pergunta do Gustavo Almeida Villa, que ele falou assim: "Desculpa a pergunta, mas o EVPN é somente para routers e switches da Juniper?". Ele quer saber se é uma coisa proprietária. Você já deu aí até um spoilerzinho, não é? Você até já fez um comentáriozinho, mas é legal você reforçar essa ideia do que é EVPN. Então, fica à vontade.

SR. EDUARDO HARO: Sim, sim. Eu acho que até comentei nessa pergunta, mas EVPN, ela é uma tecnologia que ela está ganhando muita... muita relevância agora, principalmente porque ela não é uma tecnologia proprietária, tá? É uma tecnologia que ela envolve diversos fabricantes e ela é padronizada pelo IETF. Então, você tem uma série de RFCs, eles têm uma primeira RFC, que eu escrevi aqui no webinar, onde foi explicado pelo menos o [ininteligível] básico ali de EVPN, e tem outras RFCs agora que estão sendo colocadas também no mercado, não é?

Então, é uma tecnologia que ela te permite, esse é um dos pontos fortes dela, é interoperável, né, porque ela é entre... Ou seja, qualquer fabricante que suporte, você consegue trabalhar ali com EVPN. E também ela tem garantido o que seria a evolução de rede, não é? Porque se você está preso a uma tecnologia de determinado(F) fabricante, aquele fabricante pode, de uma hora para outra, simplesmente mudar a tecnologia dele, ele aposenta aquele framework que ele está trabalhando, e aí você tem que trocar todos os modelos, você tem que trocar todo o seu modo de operação e, enfim, você fica com todo um equipamento ali parado, não é?

Então, no EVPN, o interessante é que uma vez que a comunidade, ou seja, as empresas operadoras, os fabricantes começam a entrar em acordo sobre o que que faz sentido evoluir o EVPN, isso vai sendo trazido para os equipamentos de uma forma muito mais rápida, né, é só através de evolução de software.

SRA. ANDREA ERINA KOMO: Obrigado, Eduardo. Bom saber. E oi, pessoal. Bom saber, né, que dá para usar em vários dispositivos, tem vários usos. Aí eu escolhi aqui uma pergunta do Renato Rodrigues. "Se tenho uma rede MPLS na WAN e, MAN com serviços de L2VPN, é possível ou indicado eu trocar para EVPN?".

SR. EDUARDO HARO: Sim, sim. EVPN, eu vejo como a evolução natural do que seria o L2VPN e o VPLS, tá?

Lógico que ela ganhou muito mais força nesse primeiro momento em Data Centers, porque é justamente onde, a gente, faltava, ali, uma tecnologia dessa que pudesse ter todas as vantagens do EVPN, mas sem a necessidade de um data plane MPLS, não é? Foi o que eu comentei aqui na apresentação, principalmente olhando no sentido de EVPN com VxLAN. Mas ela tem hoje ganho cada vez mais espaço também nas operadoras e nas empresas, não é? Eu até comentei um caso de uso ali, de alguns clientes de empresas grandes e que estão utilizando os switches com EVPN para ambiente de empresa, não ambiente de operadora mesmo, principalmente para facilitar toda essa questão de gestão do domínio L2.

Nós temos também clientes, operadoras mesmo, que estão utilizando o EVPN MPLS para serviços tradicionais de PL, ou seja, substituindo mesmo L2VPN e VPLS. Então hoje, sim, eu vejo que é uma evolução de rede. Lógico, tudo tem um tempo, não é, para que isso seja feito. Não é de um dia para a noite, não é? Mas eu vejo, sim, como uma evolução. Até porque hoje em dia todos os novos equipamentos já têm suporte, tanto ao antigo quanto ao novo, né, então é só uma questão de você ir migrando isso.

SR. EDUARDO BARASAL MORALES: Muito bom. Bom, tem ali uma outra pergunta, e até que você falou, do PE, né, do William Margel (sic). ?O CE pode ser um switch comum, ou somente o PE rodando EVPN?", somente o PE deve rodar?

SR. EDUARDO HARO: O CE pode ser qualquer equipamento, é só o PE que você precisa que seja, que tenha suporte a EVPN. Para o caso do CE, é totalmente transparente. Então, o CE, ele pode ser um roteador, pode ser um switch, pode ser um servidor, qualquer dispositivo que fale IP. Ele é transparente para o CE.

SRA. ANDREA ERINA KOMO: Deixa eu ver aqui qual a próxima pergunta eu escolho, só um instante. Tem várias. Eu vou pegar essa aqui da Ana Carla. "Como ficariam tecnologias de VPN com o avanço da computação quântica?". Então, o pessoal já está trabalhando nisso, já está pensando nisso? Você tem alguma informação para contar para a gente, Eduardo?

SR. EDUARDO HARO: Eu vi essa pergunta, eu não tenho muita informação, não, sobre esse ponto. Eu até comentei que hoje o EVPN, ele é uma tecnologia de infraestrutura, então, não tem nenhum mecanismo de criptografia nativa no próprio protocolo, não é? Se fosse necessário aí teria que se utilizar outros mecanismos junto, o IPsec, ou um MACsec, ou o que seja, não é? Mas atualmente não.

SR. EDUARDO BARASAL MORALES: Bom, vamos para outra pergunta. Aqui tem a pergunta do William Nascimento. " ?É necessário o uso do Multicast no underlay, mesmo utilizando EVPN?".

SR. EDUARDO HARO: Depende do cenário, não é? Ou seja, se você tem um Multicast rodando com uma aplicação em cima do EVPN, ou seja, dentro da tua EVPN L2, está passando-se um tráfego Multicast, você quer [interrupção no áudio] um tráfego Multicast relevante, existem métodos que você pode utilizar para entregar esse tráfego na tua rede com uma maior eficiência, diferente hoje, mecanismos como o VPLS, não é? Eu até discuti um pouquinho no final ainda apresentação sobre esses mecanismos, né, para a melhoria de eficiência de tráfego Multicast, esse um dos pontos fortes aí do EVPN. Mas depende muito do cenário, não é? Depende muito do cenário que você vai utilizar o Multicast, onde você vai utilizar, de que forma, porque também existem tecnologias como o Multicast EVPN que muitas operadoras têm utilizado aí também. Então depende muito dos requerimentos e de como está esse serviço de Multicast dentro da tua rede.

SR. EDUARDO BARASAL MORALES: Deixa eu ver aqui a próxima, eu peguei a pergunta aqui no Samuel. Ele colocou: "?VPLS utiliza mais recursos de hardware devido ao aprendizado de MAC, no caso de EVPN para no lugar de um VPLS, ela vai utilizar a mesma quantidade de recursos, memória e CPU, que o VPLS?".

SR. EDUARDO HARO: Pensando em quantidade de recursos, é uma pergunta complicada. A quantidade de recursos é um pouco subjetivo. Mas assim, no caso do EVPLS, todo o aprendizado de MAC Address é feito em data plane. Então, os MAC Address todos eles andam por toda a rede e eu não tenho nenhuma... nenhuma técnica para poder diminuir ou reduzir esse meu domínio de broadcast, né, o flooding da minha rede.

Já no EVPN, eu consigo fazer essa redução pelo control plane. Mas no PE, todo o tráfego que vem do acesso, ele é apreendido da forma tradicional, pelo data plane. Então, todos os MAC Address que eu apreendo naquele PE, do lado do acesso, ele é aprendido através do ARP tradicional. E ele é anunciado via IBGP no control plane, não é?

Então, eu acredito que, sim, a gente tem uma diminuição no recurso, na quantidade de recurso utilizado pelo PE, porque justamente todo o tráfego da rede, ele é anunciado através de rotas IBGP e com um controle muito maior. Então sim, existe uma diminuição no recurso, mas quando você olha o lado da rede; quando você olha o lado do acesso, ele utiliza a mesma maquinaria que você tem hoje no VPLS. Ou seja, aprendizado através do data plane.

SR. EDUARDO BARASAL MORALES: Perfeito então, vamos para a próxima pergunta. O Cristian Cardoso? mandou essa pergunta. "No blueprint da Juniper tem uma configuração recomendada, que é utilizar storm control. Se não tem risco de looping, se faz necessário?".

SR. EDUARDO HARO: Não, não. Na verdade, o looping no EVPN é mitigado nativamente pelo protocolo. Então, você não precisa se preocupar em ter mecanismos para bloquear o looping em L2, tá?

O storm control, nos nossos switches Juniper, ele é utilizado justamente para bloquear o tráfego BUM, o tráfego Broadcast, Unknown-Unicast and Multicast, que vem do lado do acesso do equipamento. Então, aquele... você pode ter equipamentos do lado do acesso, ou seja, do teu CE. Você pode ter ali tráfego excessivo de Broadcast, excessivo de Multicast, que você quer confirmar aquilo naquele PE, você quer colocar um limite. Então aí você pode utilizar esses perfis de storm control, mas todo o controle de looping, ele é feito pelo próprio EVPN. Você pode configurar o EVPN sem nenhum storm control na interface, deixar toda a configuração padronizada, ele não vai ter looping na rede.

SRA. ANDREA ERINA KOMO: Agora eu peguei aqui uma pergunta, acho que chegou agora há pouco no chat do YouTube, do Cristian Serra: "?EVPN substitui protocolos de roteamento interno, como OSPF?".

SR. EDUARDO HARO: Não. Na verdade, o EVPN, ele é uma aplicação. EVPN, na verdade, é uma aplicação que roda em cima do BGP. Então... para que o... O EVPN, na verdade, é uma address family do BGP, que ele é utilizado para trocar informações L2. Ou seja, trocar informações de MAC Address, trocar informações de IP entre todos os PEs que fazem parte daquela instância EVPN. Mas por baixo do EVPN, você precisa ter a conectividade entre os PEs, entre os teus elementos de rede. E essa conectividade, ela pode ser feita utilizando desde rotas estáticas mais simples, ou até OSPF, ISS, o que você precisar. Só precisa ter conectividade entre PEs.

Uma vez que você tem conectividade entre PEs e seções BGP estabelecida entre eles, toda maquinaria do EVPN roda por cima disso. Por isso que tem um conceito, eu falei no finalzinho aqui da apresentação de underlay e overlay. Ou seja, o EVPN, ele roda em overlay, mas embaixo dessa camada tem o underlay. O underlay é onde você tem que prover a conectividade entre os PEs. Senão ele não consegue.

SR. EDUARDO BARASAL MORALES: Legal. Tem agora uma pergunta do Christian Cardoso, que veio agora. "Eduardo, essas features estão disponíveis para uso em uma routing-instance? Digo, todas as sinalizações de EVPN e VxLAN?".

SR. EDUARDO HARO: Sim, sim. Justamente a implementação dentro dos produtos Juniper, ela pode variar um pouquinho. Ou seja, por exemplo, no caso de um MX, você pode criar várias routing?instance, cada uma... ou seja, várias instâncias EVPN dentro de uma routing?instance, e criar várias bridge domaings(F), e ter vários Tenants. Nós temos outros produtos, outros switches de menor capacidade, onde você consegue criar apenas uma routing?instance e aí habilitar o EVPN.

Mas sim, temos justamente essa possibilidade de você quebrar em várias routing?instance EVPN, ou utilizar uma única routing?instance EVPN e quebrar em bridgings domaings(F) diferentes, ou broadcast domaings diferente. Aí vai da implementação que eu comentei ali no meio do webinar dos tipos de EVPN que a gente pode trabalhar.

SRA. ANDREA ERINA KOMO: E vejamos, eu peguei aqui agora a pergunta do Edson. ?"Quais imagens Juniper e versões que você aconselha para utilizar com o GNS3, ou EVE-NG, laboratórios virtuais? Funcionará o control plane e o data plane" nessas plataformas aí virtuais? Tem alguma coisa aí para acrescentar sobre isso, por favor?

SR. EDUARDO HARO: Olha, eu não tenho aqui nenhuma dessas duas plataformas, aqui no meu laptop. O que eu consigo recomendar, eu até coloquei ali no chat, o link, a Juniper tem uma iniciativa chamada vLabs, né, virtual labs. Eu até coloquei o link no chat do YouTube, onde você consegue se cadastrar, né, permitir... solicitar o acesso. E ali nós temos várias topologias. É um laboratório que a Juniper tem na qual tem topologia já prontas, utilizando MX, QFX. E tem algumas topologias, inclusive, de EVPN, onde você consegue, com alguns cliques, você solicita, ele vai criar topologia para você, já totalmente virtualizada, não é? Você não precisa se preocupar em baixar a imagem, e tal. E ali é um ambiente fechado, onde você consegue brincar, configurar os equipamentos e poder fazer troubleshooting, e tal. Então, é bem interessante. Eu coloquei um link do vLabs no YouTube. Deve estar no chat aí.

SR. EDUARDO BARASAL MORALES: Ah, perfeito. E depois você passa para a gente, a gente coloca na descrição do vídeo também, e coloca no site o link que você está referenciando, tá bom?

Vamos para a próxima pergunta, do William Nascimento, não é? Ele falou aqui: "As rotas tipo 5 são utilizadas para interconexão com ambiente externo ao DC? Saída para internet por exemplo? É necessário utilizar alguma VRF para isso?". E aí ele complementa: "É necessário um leaf exclusivo para interconexão ao ambiente externo ao Data Center, né, ao DC? Pode ser utilizado algum leaf existente?".

SR. EDUARDO HARO: Sim. A rota tipo 5, ela nasceu muito nesse... para atender primariamente dois casos de uso, não é? Interconexão de Data Center. Porque em uma interconexão de Data Center, você pode ter segregado um Data Center dentro de uma subnet IP, e um outro Data Center dentro de outra subnet IP. Então, você consegue diminuir a comunicação entre o Data Center, se você anunciar o prefixo IP de cada Data Center. Então esse é um dos casos de uso da rota tipo 5.

E o outro eu acabei comentando, mas é o roteamento entre Tenants. Ou seja, em um Data Center, você tem uma rede L2, um Tenant L2, e você precisa que esse Tenant ou essa subnet fale com outra subnet. E a implementação tradicional do EVPN, usando a rota tipo 2, você tem um consumo maior de recursos, porque todos os switches têm que ter conhecimento das rotas tipo 2 e têm que ter VxLANs de um lado para o outro, com todos outros os leafs.

E quando você usa a rota tipo 5, você consegue [interrupção no áudio] camada em roteamento no Data Center. Então, esses foram os dois casos de uso principais aí que a rota tipo 5 foi criada.

Agora, a rota tipo 5, ela também consegue, ela faz um trabalho muito parecido ao que nós temos na L3VPN tradicional, o VRF. Então, você também pode ter serviços L2 quanto L3 rodando dentro da mesma instância de EVPN.

SRA. ANDREA ERINA KOMO: Bacana. Bem, seguindo aqui, eu peguei a pergunta agora da Elaine Cristina. "E o comprometimento do tráfego entre sites na solução EVPN? Podemos ter lentidão?".

SR. EDUARDO HARO: Pode repetir a pergunta, Andrea? O comportamento...

SRA. ANDREA ERINA KOMO: "E o comprometimento do tráfego entre sites na solução EVPN". Então, acho que... usando, né, no caso, aí, a EVPN, vai causar alguma lentidão, aí, durante esse tráfego, entre essa comunicação toda, entre os sites, entre a rede?

SR. EDUARDO HARO: Não, não. Isso... não é o... Isso não é um problema, tá? O que se usava muito antes de você ter EVPN para conexão entre Data Centers, a gente via muitos clientes utilizando o MPLS, utilizando uma VPLS para conexão entre Data Centers. Ou até mesmo fibra escura, não é, fibra apagada, para essa comunicação.

A grande vantagem de você ter o EVPN para essa comunicação entre Data Centers é que você precisa... como ele é independente do data plane, então, você pode utilizar um data plane IP, você não precisa utilizar um data plane MPLS.

Aí, nesse caso, você utiliza o EVPN sobre VxLAN e, entre a tua conexão de Data Centers não precisa ter uma rede MPLS, pode ser uma rede que você... você está aberto a escolher a rede que você precisar. Então, isso te dá maior flexibilidade. O overhead(F) que você tem ali é basicamente o cabeçalho DP e o cabeçalho VxLAN. Então, eles têm que ter uma... em consideração. Mas fora isso, não tem nenhum outro problema de performance.

SR. EDUARDO BARASAL MORALES: Bom, próxima pergunta do Cristian Cardoso. ?"Todas as configurações de spine e leaf de EVPN e VxLAN é possível de se configurar e uma routing-instance em modelos QFX?".

SR. EDUARDO HARO: Sim, sim. A gente suporta hoje, EVPN, dentro do nosso portfólio Juniper, né, a gente suporta EVPN nos equipamentos MX, QFX, e EX, e ACX. Então, hoje, todos eles têm o suporte a EVPN, tá? É só uma questão de release de software e quando você precisa de determinada funcionalidade para fazer esse casamento, não é? Mas hoje todos eles suportam.

SRA. ANDREA ERINA KOMO: Bem, vou fazer aqui a outra pergunta, né, da Elaine. Acho que complementa um pouquinho da pergunta anterior. Aí ela colocou aqui: "Como fica cálculo do gargalo da rede no caso de VPN entre sites que atravessam a Internet?", não é? Ainda relacionado aí, "Pode haver uma lentidão?". Tem alguma coisa a mais que a gente tem que considerar aí no cálculo desse gargalo da rede?

SR. EDUARDO HARO: Não, não. Acho que está... Estaria muito... Acho que está, em linha a o que é a outra pergunta dela, né, de sobre... se haveria degradação de performance. Não teria problema, não. Não vejo nenhum problema, pelo menos.

SR. EDUARDO BARASAL MORALES: Ok. Vamos para a próxima, do Vladimir Borgiani. "?O uso do QFX como extensão satélite do MX altera em algo a configuração e suporte a EVPN?".

SR. EDUARDO HARO: A configuração em satélite é um pouquinho diferente. Porque, na configuração de satélite, o que nós fazemos é: você tem um dispositivo de agregação e você tem um dispositivo satélite na ponta, que... O dispositivo satélite da ponta, basicamente, ele é um... tipicamente, é um outro switch, mas ele é um switch sem tanta inteligência. Então, é um switch que a função dele é mais fazer uma agregação de portas e trazer isso para o elemento agregador, onde a inteligência, realmente, está ali, daquele elemento, não é?

Então, entre o QFX e um satélite, você não tem... ou o MX e um satélite, você não tem o uso ali de EVPN, tá? Você tem, são outros protocolos que rodam ali. E a inteligência está dentro do site de agregação, né, o dispositivo de agregação. Tanto que, quando você tem um ambiente em satélite, você só configura o teu equipamento agregador. Você não precisa entrar e configurar os equipamentos de satélites, não é? Então, acaba sendo coisas separadas, não é?

SRA. ANDREA ERINA KOMO: Certo. Seguindo aqui, a próxima. O Lucas Rosa colocou, não é? "Nesse caso do EVPN, não necessariamente precisamos de MPLS? Apenas conexões BGP entre os devices?".

SR. EDUARDO HARO: Sim, existem dois. EVPN, ele é um control plane, ele é uma aplicação. E ela pode... ela é independente do data plane. Então, por isso que eu comentei, existem duas grandes frentes aí, que é o EVPN MPLS e o EVPN VxLAN, ou EVPN sobre IP. Você não precisa ter MPLS fim a fim, mas, se você tiver, o EVPN ele pode utilizar o data plane MPLS que você já tem.

Então, alguns exemplos que eu coloquei, eu tinha ali utilização de EVPN MPLS, onde toda a sinalização de labels de serviço para determinados tipos de rota é feito utilizando o label MPLS, em si, não é? E, para os casos onde eu tenho EVPN rodando em cima de um data plane IP, eu mostrei exemplos onde a identificação do serviço se dá pelo VNI, que é o VxLAN na ID. Existem outras formas de se rodar EVPN sobre IP, como por exemplo o GRE. Mas isso acabou... acabei não abordando aqui.

E o que a gente mais vê na indústria hoje é justamente o EVPN sobre MPLS ou EVPN sobre IP usando o VxLAN. O que você precisa do lado do data plane é basicamente de um protocolo que possa fazer o tunelamento daquele tráfego, ou seja, a separação do tráfego de overlay com underlay, e gerar algum tipo de ID, de identificação, para aquele determinado tipo de tráfego, para que o controle do EVPN possa entender o que está chegando.

SR. EDUARDO BARASAL MORALES: Ah, bem interessante. Bom, tem uma pergunta que chegou agora do Wanderson Thallys. "Fazendo referência a ganho de desempenho e confiabilidade, qual seria o ponto fundamental em substituir minhas VPNs VPLS por EVPN?".

SR. EDUARDO HARO: Eu acho que o maior ganho que você tem no VPLS, é que no caso do VPLS, todo o tráfego... Você está... No VPLS, você estabelece a tua instância VPLS na tua rede e você configura todos os PEs, mas você não sabe, você não tem muito controle do tráfego que está em cima do VPLS. Ou seja, os MAC Addresses, eles entram, você tem um domínio de broadcast, que ele é estendido por toda a sua rede. É como se você um grande switching(F) que se estendeu por uma rede WAN, uma rede que pode estar distribuída por diversos estados ou até a nível nacional, não é?

Tanto que existem hoje técnicas no VPLS, que é justamente, por exemplo, o H-VPLS, o VPLS Hierar(F), que é uma forma de você conseguir dar uma maior escalabilidade ao VPLS, porque ele tem problema de escalabilidade.

No EVPN, você não tem problema de escalabilidade. Você não precisa lançar mão de VPLSs hierárquicos quando vai começando a crescendo muito o teu domínio VPLS, porque o próprio EVPN já faz gestão, essa redução do domínio de broadcast para você nativamente.

Outro ponto que a gente consegue apontar aqui de melhorias é: no EVPN, você consegue tratar o tráfego dentro da tua aplicação de EVPN. Então, um exemplo é o próprio tráfego Multicast. Se eu tenho um tráfego Multicast rodando ali naquela aplicação, eu consigo... e tenho eu tenho um tráfego que está crescendo, um tráfego Multicast crescendo, eu consigo estabelecer mecanismos para uma entrega mais eficiente de tráfego Multicast na rede. Por exemplo, lançando mão de LSPs e MPLS ponto multiponto. Ou eu consigo utilizar aquela outra técnica de assistant replication. Enfim, você tem algumas técnicas para poder trabalhar isso também, não é? Outros pontos, bom, a questão de ativo/ativo. Enfim, aí eu acho que até montei uma tabelinha, em um dos slides aqui, que tinha uma comparação boa sobre isso, mas os pontos que me lembro aqui, principais, seriam esses.

SRA. ANDREA ERINA KOMO: Bacana. Então, seguindo aqui, né, próxima pergunta, eu peguei a do Cristian Cardoso. "Eu não poderia sinalizar o cluster-ID dentro do overlay, ?e assim, ter menos um BGP group?". Então, um pouquinho mais específica aí essa pergunta.

SR. EDUARDO HARO: Ah, eu lembro dessa pergunta. Na verdade, ele referenciou um blueprint que, na documentação da Juniper, eles têm... a gente tem um blueprint publicado para se você quiser montar um fabric EVPN. E aí tem a configuração de cada um dos grupos BGP ali.

É que esse é o grupo BGP específico que ele citou era um grupo que se utilizava aí para fazer a comunicação BGP entre router reflectors. Então, era um ponto bem específico. Aí acabei detalhando um pouco mais aí nas perguntas do chat do YouTube. Acho que ficou mais fácil.

SR. EDUARDO BARASAL MORALES: Ah, sem problemas. Se está escrito lá, o pessoal já viu e já ficou satisfeito. Teve uma ali, uma pergunta também do Douglas Fisher, relacionado ali aos MAC Addresses, não é? Como você estava apresentando sobre isso. Ele estava apresentando "Se os MAC Addresses únicos, mas separados por VLAN? Ou um MAC Address pode existir em múltiplas VLANs?". E se o "provisionamento disso é suportado por NetConf?".

SR. EDUARDO HARO: Sim, NetConfit é suportado, a gente já... NetConf é uma forma de provisionamento. Ela meio que independe do EVPN. No Junos, nós já temos suporte a NetConf por muito tempo. Então, sim,

é possível. Muitos clientes fazem isso, até por questão de automação de processos, não é? E qual era o outro ponto mesmo? Era... eram duas perguntas.

SR. EDUARDO BARASAL MORALES: Era relacionado sobre os MAC Addresses únicos.

SR. EDUARDO HARO: Ah, os MAC Addresses, não serem iguais. Justamente o... depende do tipo de serviço EVPN que você está trabalhando, não é? Que foi aquele último slide que acabei repetindo ali.

Então, a necessidade de você ter o mesmo MAC Address, ela vem muito em linha da quantidade de tabelas de bridging domaing(F) que você tem naquela instância EVPN. Porque, se você tem uma única tabela de bridging domaing(F), naquela tabela, ela é indexada pelo MAC Address.

Então, no caso de você utilizar um tipo de serviço que você tem uma única tabela de bridging domaing(F), mesmo que você tenha múltiplos domínios de broadcast, muitas VLANs. Como a indexação é feita pelo MAC Address, você não pode ter MAC Addresses iguais ali. Você não pode ter... Você tem que sempre ter MAC Addresses únicos.

Esse é o caso... não é o caso, por exemplo, do VLAN Aware Bundle. Então no tipo de EVPN VLAn Aware Bundle, eu tenho múltiplas tabelas de MAC Address. Ou seja, múltiplos bridging domaing(F), associados a cada broadcast domain. Então, ali fica mais fácil, porque cada VLAN tem a sua própria tabela de MAC Address. Então, você pode repetir os MAC Addresses, porque eles são separados, né, você não tem esse conflito na tabela de MAC.

SRA. ANDREA ERINA KOMO: Então, seguindo aqui, a próxima pergunta, chegou acho que agora há pouco também, do Renato Rodrigues. ?"No caso de não usar VxLAN e sim Geneve, é possível implemetar EVPN?".

SR. EDUARDO HARO: É, eu acho que eu citei, em um dos slides desse webinar tem uma referência a uma RFC, que ela saiu posterior à RFC original do EVPN, eu acho que a 8365, se não me engano, que ela descreve um pouco dos detalhes e nuanças de você trabalhar com EVPN em cima do... do data plane IP. E até comentado alguma coisa sobre isso, mas eu não entrei no ponto aqui, não. O que a gente vê mais é sobre VxLAN mesmo, hoje, que é o que é mais implementado aí pelos clientes emais empurrado pelo mercado.

SR. EDUARDO BARASAL MORALES: Tudo bem. Tem também uma pergunta aqui do Welisson Tome. "Não sei se teve algum comentário sobre isso, mas poderia falar sobre o uso do EVPN em substituição do MPLS para redes de operadoras?".

SR. EDUARDO HARO: Eu acho que a gente acabou comentando aqui em algumas perguntas anteriores, mas, sim. Você tem algumas vantagens, você tem grandes vantagens em cima disso.

Eu acabei... a apresentação foi muito focada em cima disso, né, ou seja, quais as vantagens... Tem até slide, acho que eu coloquei, sobre vantagens de EVPN, sobre... VPLS sobre L2 circuit. Ou seja, o EVPN, ele traz vantagens se tem tanto tráfego multiponto/multiponto, tanto tráfego ponto a ponto. Ele te traz vantagens.

Então, a meu ver, é uma evolução natural que a gente vai estar tendo. É importante a gente estar por dentro, porque, hoje em dia, já é uma tecnologia que já está implementada aí há alguns anos, em alguns clientes. Então, ela vai sendo implementada cada vez mais gradativa, não é? Não é do dia para a noite isso, mas eu vejo, sim, como a evolução natural aí. Muitas grandes operadoras já estão adotando aí EVPN, mas de uma forma um pouco mais massivo até.

SRA. ANDREA ERINA KOMO: Bem, a próxima pergunta aqui que eu peguei talvez você já tenha comentado um pouquinho sobre, onde eu me lembro, mas para reforçar. O Cristian Cardoso tinha colocado aqui: "É possível efetuar o underlay via OSPF, e o overlay via BGP?".

SR. EDUARDO HARO: Sim, sim. O underlay é qualquer método de conectividade que você tenha, que você use para que um PE consiga se conectar com o outro. Você pode utilizar OSPF, você pode utilizar ISS, você pode utilizar inclusive rota estática, se você quiser, com tanto que os PEs consigam se falar, tenham conectividade direta.

Já o overlay, ele sempre é BGP, porque, justamente, é onde roda o EVPN. Então, o EVPN, ele é um address family do BGP. Então, no overlay, eu sempre tenho o BGP. Normalmente é um IBGP, para facilitar a implementação. Algumas vezes a gente também usa, como eu comentei no finalzinho, ali, no cenário de Data Center, a gente também usa para o underlay BGP novamente.

Então, a gente tem cenários de que no underlay, a gente usa BGP, normalmente... um EBGP, né, o BGP externo; e no overlay, a gente usa um IBGP. Ou seja, a gente usa duas vezes o BGP, tanto para underlay quanto para overlay. É até uma boa prática que a gente para Data Center. Mas, no underlay, é qualquer tecnologia e, no overlay, aí tem que ser o BGP.

SR. EDUARDO BARASAL MORALES: Ah, legal. Tem aí uma pergunta simples agora do Milton Oliveira Vieira. "A partir de qual versão do Junos tem suporte a EVPN?".

SR. EDUARDO HARO: Aí vai depender do que nós temos, de qual linha de produtos, não é, que você está falando. Mas nós já temos aí a EVPN já faz algum tempo, implementado. E eu, particularmente, eu me lembro que eu testei EVPN já nas releases de 2018. Mas eu acho que nós temos suporte a antes. Ou seja, a releases antes das 18.X. Eu acho que a gente já deve ter até antes. Teria que buscar ali, os releases novos. Mas já tem algum tempo.

Hoje, dentro da Juniper, todos as releases do software da Juniper, o primeiro dígito significa o ano, ponto, e aí, o próximo dígito identifica, ali, basicamente, o... dentro do ano, qual a release que foi lançada. Então, a release atual é a release 20 ponto alguma coisa. Então, se você buscar já há algum tempo, aí, já desde releases 18, até anteriores, 17, eu acho que a gente já tenha suporte, já, a EVPN.

SRA. ANDREA ERINA KOMO: Essa pergunta, agora, que eu selecionei, chegou agora há pouco também. Então, do Wanderson. Para criar uma instância EVPN no BGP foi inserido uma nova família referente aos protocolos de rede?

SR. EDUARDO HARO: Para criar uma instância... Pode repetir a pergunta, Andrea?

SRA. ANDREA ERINA KOMO: Claro. Para criar uma instância EVPN no BGP foi inserido uma nova família referente aos protocolos de rede? Então, se foi criada aí uma nova família para isso, né, no EVPN.

SR. EDUARDO HARO: Sim, sim. A gente tem uma... é uma nova address Family, que foi criada... é uma nova NLRI, não é?

Eu estava buscando aqui... não sei se eu tinha até um slide aqui. É a nova address family 2570. AFI 25, SAFI 70. É nova address family. Então, quando você tem o... quando você configura a EVPN na sua rede, você tem que justamente colocar lá o address family e você tem que colocar o address family de EVPN para ele poder divulgar e trocar... NLRIs, que são EVPN.

SR. EDUARDO BARASAL MORALES: Bom, Eduardo, já quero fazer os agradecimentos, tá? A gente, agora, já liquidou todas as perguntas. Muito obrigado aí pela sua participação. Realmente foi muito importante, aí, para o nosso público ouvir todas essas respostas e tudo o que você apresentou durante esse tutorial. Então, eu já faço aí o agradecimento do NIC.br a você, tá, por ter aceitado o nosso convite. Quer dar umas últimas palavrinhas aí para o público?

SR. EDUARDO HARO: Queria agradecer a vocês pela participação, agradecer ao pessoal. Espero... É um tema... Eu acabei fazendo um tema muito teórico, tinha um termo(F) meio... foi até um pouco extenso. Mas, bom, espero que vocês tenham aprendido pelo menos alguma coisa. Pelo menos uma ideia do que... como funciona o protocolo por cima.

A ideia era mais trocar um pouco ideia sobre tecnologia, sobre o que está acontecendo, não é? E, bom, espero ter ajudado alguma coisa. O material ficou disponível aí para vocês. É bom, é um material bom até para ser usado como consulta, para referência, não é? E, bom, obrigado para todo mundo aí.

SR. EDUARDO BARASAL MORALES: Ah, a gente que agradece. Realmente ajudou bastante, e esclareceu bastante dúvida aí do pessoal. Assim, foi excelente, muito obrigado, viu?

Bom, agora, eu queria, de novo, dar o aviso do formulário de avaliação, pessoal. Então, a gente vai colocar o QR Code aí na tela. Deixe aí o seu recado para a gente saber o que você achou desse tutorial. Se quiser mandar uma mensagem aí também para o Eduardo Haro, fica à vontade, tá? A gente passa para ele depois a avaliação. Então, são duas perguntinhas. Uma é uma nota de zero a dez, só para a gente saber o que você achou, e outra é um comentário do que a gente pode melhorar em outras edições. Então, coisa rápida.

Depois disso, a gente vai colar o link no chat do YouTube do formulário de inscrição para ganhar o certificado. Então, novamente, vai até as 2 horas da tarde. Se você quiser ganhar o certificado de participação dessa live, se inscreva no nosso link de inscrição, que foi colocado no chat do YouTube.

Por fim, vou querer dar aí alguns últimos avisos, tá, para o pessoal que está acompanhando a gente. A gente está com o curso BCOP EAD com inscrições abertas, tá? Então, ela vai até dia 6/9, as inscrições. Então, se quiser participar do nosso curso aí de Boas Práticas Operacionais para Sistemas Autônomos, curso gratuito, se inscreve lá no site do cursos e eventos, onde que você também já fez a inscrição aí para ganhar o certificado dessa live. Então, é no mesmo site lá, você pode entrar na parte do curso BCOP EAD e se inscrever.

Outro aviso que eu também gostaria de dar é relacionado ao nosso podcast, o Camada 8, que também a gente traz sempre aí informações sobre redes, tá, informações aí atualizadas das coisas que estão acontecendo no momento e ensinamentos técnicos, também, sobre tecnologia e como vocês podem trabalhar. Temos episódios de IPv6, temos episódios aí do IX.br. Temos episódios de PGP, como que faz criptografia, tá? Então, coisas aí bem interessantes. E a gente deve lançar todo mês um episódio novo para vocês aí sobre redes.

Depois disso temos também o Intra Rede no dia 30 de setembro. É a nossa próxima edição de Intra Rede. Então, vai ser sobre segurança, focado ali nos principais ataques que estão acontecendo no mundo de provedores. A gente vai montar mesa recheada de especialistas. Então, não perca aí. Anota na agenda, no dia 30 de setembro, a gente vai estar de volta no canal do YouTube, conversando no nosso programa do Intra Rede, tá?

Então, é um programa aí que a gente traz gente de fora para fazer uma discussão, assim, uma discussão até que genérica com vários especialistas da área. Diferente do que a gente teve nessa semana de capacitação, que foi ali temas bem específicos. A gente deu uma aprofundada nos assuntos, deu ali tutoriais de três horas. E eu gostaria de agradecer todos, a vocês que participaram, né, durante essa semana de capacitação. Realmente foi uma coisa nova para a gente. A gente gostou muito.

A gente não esperava tanto público, tá? Porque eram temas muito específicos, temas técnicos. Três horas é maçante, e foi durante uma semana inteira. Mas a gente viu que foi um sucesso o evento, né, e que vocês gostaram bastante. E quem sabe a gente não consiga replicar esse evento. Então, deixa ali o comentário para a gente, no formulário de avaliação, se você quer saber mais sobre isso, mais sobre esses assuntos, quer mais tutoriais técnicos. Porque às vezes a gente faz eventos mais tangenciando no superficial, as discussões, e agora a gente está se aprofundando em temas técnicos e está tendo um respaldo muito bom. Realmente é uma coisa muito gratificante ter feito essa semana de capacitação com tantos especialistas aí na área, não é?

Teve dia de RPKI, teve o dia de segurança básica com a Cisco. Teve aí com... Ah, o pessoal da ICANN, a questão ali de DNS, né, como DNS recursivo, hyperlocal, não é? Como configurar isso no unbound. Teve o dia do Lacier, junto com o Luiz Puppin, também falando aí de communities, no BGP, que foi uma coisa aí extremamente interessante, de fazer automatização do seu BGP. E hoje a gente teve aí o Eduardo Haro, da Juniper, explicando para a gente sobre EVPNs.

Então, foi uma semana aí cheia de conteúdo. Foi muito interessante. Se você perdeu alguma dessas lives. Está tudo no nosso canal, basta ir aí, e assistir. Não esqueçam de deixar o like. Já deixa o like também nos outros vídeos, aí, para a gente conseguir ter aí uma disseminação desse conhecimento ampla no nosso canal, tá?

Lembrando também que os links para os materiais estão no site e também na descrição do vídeo. Então, aí... os slides da live de hoje, e das outras lives estão tudo lá no site. Então, quer ver de novo? Assistir todos os episódios? Quer seguir os materiais? Entra lá no site da Semana de Capacitação, ou dá uma olhadinha aí nos links que estão na descrição.

Principalmente, né, porque alguns tinham laboratório ao vivo. Então, se você precisa baixar a máquina, quer fazer o passo a passo, quer digitar comando por comando, ver qual que é o resultado, ver como está na tela, então... você consegue acompanhar com os materiais que a gente utilizou. E utilizar eles também, como o Eduardo falou, como referência. Então, se você quiser até lecionar, depois, com esse conteúdo, não é? São materiais, aí, bem-feitos.

Então, novamente, eu queria agradecer, tá, ao nosso palestrante de hoje, o Eduardo. Queria agradecer também toda a equipe do NIC.br, teve a equipe de cursos, que trabalhou aí pegando as perguntas. A Mariana, a Fernanda, a Tuane(F), a Erina, o Tiago(F), todo mundo ali ajudando na equipe. Teve também o pessoal da equipe de comunicação. Teve a Adriana, teve a Carina, teve a Soraia(F). Teve um monte de gente aqui trabalhando para tudo dar certo nessa semana e, inclusive o Pedro, aí, que também faz a nossa parte aí técnica da transmissão.

Então, tem muita gente para agradecer. E... eu já deixo aqui o meu muito obrigado porque, realmente, a semana foi um sucesso, tá? Muito obrigado a todos. E até mais.