SR. ANTÔNIO MARCOS MOREIRAS: Para todo mundo. E vamos começar aqui mais um dia na semana de capacitação online do NIC.br

Hoje nós temos o Prof. Lacier e o Prof. Luiz Puppin, da VLSM, que vão falar para a gente sobre automatização de anúncios no BGP, usando communities, usando BRF para Huawei e para Mikrotik. Um assunto muito interessante, complementa tudo o que a gente já vem tratando na semana, cada dia um assunto diferente, sempre assuntos relevantes para você aí, implantar no seu provedor, para você conseguir melhorar sua rede.

Bom, então lembrando como nos demais dias, a gente vai oferecer um certificado de participação hoje, que é para quem está aqui acompanhando a gente online, ao vivo.

Para ter certificado vocês vão ter que se inscrever no link que o pessoal da equipe está colando no chat do Youtube. "Moreiras eu estou acessando do celular, não consigo acessar o chat agora. Eu estou vendo no Facebook, estou vendo pela página do evento, não está aparecendo chat aqui".

Bom, você tem a oportunidade de fazer essa inscrição até às 14h, depois a gente fecha. Então tenta, de agora até às 14h, vai nesse videozinho no Youtube, vai ficar lá disponível depois de a gente terminar live, pega o link que vai estar lá no chat. O chat, o histórico do chat também fica lá disponível, se inscreve. Se você não se inscrever até às 14h, a gente não tem como fornecer esse certificado para você de outra forma. Para a gente, é a forma que a gente usa para ver que você realmente estava aqui online acompanhando a gente ao vivo.

Bom, o que mais? O curso de hoje, o minicurso de hoje, ele tem, como o de ontem, uma parte prática que você pode acompanhar aí, junto com os instrutores. Então o material dessa parte prática já está disponível no site do evento, já está disponível já algum tempinho lá, alguns dias. Então tem lá as máquinas virtuais para você baixar, têm lá as instruções, e tem um guia de comando, comando a comando que o pessoal vai digitar aqui para facilitar.

Você sabe, às vezes, na hora quando a gente compartilha a tela, às vezes não fica tão visível no vídeo e no Youtube, principalmente se você estiver assistindo no celular em uma telinha pequena, fica um pouco complicado de acompanhar. Então tem lá um guia comanda a comando, você pode baixar aquilo, você pode ir visualizando em separado, pode ajudar.

Então convido... Mesmo quem não quiser acompanha ao vivo agora, quem não tiver baixado as máquinas virtuais, não quiser baixar, não quiser fazer a parte prática junto com o Puppin, junto com o Lacier, baixa lá o material e acompanha usando o material também, porque vai facilitar, vai ficar mais claro, mas fácil de acompanhar a parte prática. Vai ter uma parte teórica também.

Como nos outros dias, a gente pediu, por favor, para o Lacier e para o Luiz Puppin, de pré-gravar um videozinho para essa live para a parte inicial, para parte de explicação.

Então, quando eu parar de falar aqui, acabar a introdução, passar a palavra para o Lacier e para o Luiz, na verdade, vai entrar um vídeo que já está gravado.

Só que o Lacier e o Luiz estão aqui com a gente, estão aqui na transmissão, e eles estão acompanhando ao vivo o chat do Youtube, então eles já estão vendo as perguntas de vocês, eles já vão interagir com vocês, acho que já devem estar interagindo no chat do Youtube, eles vão já responder as questões. Mas, no

finalzinho, eles entram ao vivo, para conversar com vocês, batem um papo, responder tudo o que ficou de dúvida. Então, do mesmo jeito que funcionou nos primeiros dias da semana.

Amanhã vai ter o último dia da semana, a gente vai ter um pessoal da Juniper falando da evolução da internet, de VPN. Também já deixem marcado aí, já vão lá no Youtube, habilita a notificação do vídeo para vocês não esquecerem, não perderem.

E como sempre, vocês aí, muitos de vocês que estão acompanhando hoje, já acompanharam os outros dias da semana, os primeiros três dias, vocês já puderam ver a qualidade do pessoal que a gente trouxe, a qualidade do material que a gente preparou para vocês durante essa semana. Então deem um voto de confiança aí para a gente, e deixa aí o joinha no vídeo. Por quê? Porque o Youtube, na distribuição orgânica, na distribuição dos vídeos, mesmo para as pessoas que estão lá assinando o canal, ele não faz isso para todo mundo, ele tem um algoritmo dele, e a gente não paga para fazer a distribuição para os vídeos aparecerem. O like de vocês ajuda o Youtube, incentiva o Youtube a fazer esse vídeo aparecer para mais gente. E é um conteúdo de qualidade que a gente faça muita questão de que apareça para mais gente, que apareça para o maior número de pessoas possível.

Então, deem seu like aí, porque isso ajuda a gente para caramba. Depois, no final se vocês não gostarem, vocês tiram lá o like, dá o 'deslike'. Entendeu? Mas dá o voto de confiança para a gente e põe o like já dei desde o início.

Compartilhe o vídeo aí, no grupo de Whatsapp, não precisa compartilhar no grupo da família, mas pega lá no grupo dos provedores, no grupo de trabalho, tal. Se tiver o pessoal da família que também é de tecnologia, que também é de provedor, pode pôr lá no grupo da família também, que não tem problema. Certo?

Eu vou pedir agora para o Pedro colocar o videozinho do nosso novo projeto. Não vou falar mais sobre eles para vocês. A gente está apresentando esses vizinhos aí como como um teasing de um projeto novo que a gente está trabalhando, com vídeos educativos para a comunidade de usuários de internet. Então um videozinho de 15 segundos, o Pedro vai colocar e eu já volto.

[exibição de vídeo]

SR. ANTÔNIO MARCOS MOREIRAS: Bom, gente, depois vocês coloquem seus comentários aí no chat do Youtube sobre o que vocês acharam desce videozinho educativo de 15 segundos.

Bom, eu acho que eu já falei tudo que eu tinha que falar, reforçando só as inscrições, para quem precisa do certificado, ficam abertas até as 14h. Não se não se esqueçam, porque a gente não tem outra forma de saber que vocês estavam aqui nos acompanhando, e emitir o certificado se vocês não fizerem essa inscrição dentro do horário.

E eu passo, agora, a palavra para o Lacier e para o Luiz Puppin. Bom curso para todos.

SR. LACIER DA COSTA DIAS JUNIOR: E aí, meus queridos? Prof. Lacier começando aí, a gravar para a semana de capacitação, junto com o meu querido Prof. Puppin.

SR. LUIZ COSME PUPPIN MAGALHÃES: Fala, galera, tudo bem?

SR. LACIER DA COSTA DIAS JUNIOR: Vamos estar abordando a matemática de automação de anúncios de trânsito BGP, com community e VRF, usando os dois brinquedos mais famosos dos provedores aí, Huawei e Mikrotik.

O pessoal, às vezes, brinca que eu e Puppin deve ter algum tipo de rixa. E aqui vocês vão ver que os nossos corações estão unidos aí, para... com foco em resolver sempre os problemas dos provedores e sempre levar a melhor solução para cada tamanho de provedor.

Prof. Lacier, depois aí vocês leiam com calma nosso histórico, LinkedIn e afins. Nosso querido Prof. Puppin também. Depois vocês podem ler com calma nosso pequeno histórico. Estamos com fios brancos, né, Puppin?

SR. LUIZ COSME PUPPIN MAGALHÃES: Pouquinhos. Aqui, ó.

SR. LACIER DA COSTA DIAS JUNIOR: A ementa. Então, assim, a gente vai passar pela plataforma, porque o alcance do treinamento pode permear por alunos que não conhecem o EVE. A gente vai também disponibilizar um manual junto com a ferramenta, manualzinho simples, um PDF, como é que você instala ele e já põe para funcionar.

Então, conceitos básicos de como é que você tira o equipamento da caixa, como é que o roteamento funciona, características e facilidades principais de cada um dos equipamentos. Comandos mais utilizados, para o pessoal não ficar perdido, quem for o primeiro contato. Conceitos básicos de MPLS, iBGP, MP-BGP, Community. Porque usar a VRF, conceitos básicos de VRF. E aí a gente vai partir para laboratório, hands on, mão na massa.

Então a gente vai entrar com o cenário já da rede funcionando. A parte de IP, endereçamento vocês vão poder baixar depois, um scriptzinho já colar no roteador para não ter perda de tempo e ficar configurando IP no laboratório. E depois a gente vai mostrar toda a parte de automação, tanto como ela é feita no Huawei quanto como ela e fita no Mikrotik. E mostrar essa compatibilidade entre os dois mundos, porque a gente vê bastante transição, pessoal que começou com Mikrotik, hoje já está usando o Huawei, mas parte da rede já tem [ininteligível], como é que isso funciona, como é que essa mágica acontece. Né, Puppin?

SR. LUIZ COSME PUPPIN MAGALHÃES: Isso mesmo. A ideia é juntar os dois no treinamento e mostrar que é possível que uma rede Huawei e Mikrotik funcione, e também não só mostrar isso, mostrar que redes de múltiplos vendedores, múltiplos vendors, Huawei, Mikrotik, Juniper, Cisco, não importa, isso é padrão. Você seguindo o padrão, todo mundo vai conseguir fazer e vai funcionar tranquilamente.

SR. LACIER DA COSTA DIAS JUNIOR: Esse é o principal foco, não é mostrar o Mikrotik e o Huawei. Que a gente tem muita habilidade com esses dois produtos, e a gente escolheu eles por conta disso. Mas mostrar para vocês que a gente segue a [ininteligível], e que o universo é um universo de compatibilidade, e um universo de [ininteligível] é um universo muito próximo da gente, então, por isso a escolha desses dois vendors aí, para a gente poder começar o treinamento.

Então, vocês vão receber o manual do EVE. EVE é uma plataforma gratuita que a gente utiliza para dar aula. A gente disponibilizou o link, um AVA(F) que ele já vem tratado, então ele já vai ter aí, a imagem do Huawei, a imagem do Mikrotik dentro dele. Porque se você baixar ele do site do próprio EVE, ele vai vir vazio, você vai ter que caçar essas imagens na Internet. A gente já mandou as imagens prontas.

Existe esse movimento de integração de copiar esse arquivo e colocar lá na pastinha, porque o Huawei a gente utiliza o VNC para acessar a caixa. O Mikrotik também requer uma integraçãozinha, porque a gente usa Winbox para acessar caixa. Então, para ficar mais fácil a gente resolveu fazer um manual à parte. Que senão a gente ia ficar aqui 20 minutos explicando o manual, você pode ler, a gente faz isso em todas as aulas. Então o manual é bem tranquilo, já passou na mão de um monte de aluno, então é um manual bem 'fácinho' de você conseguir seguir.

No final, você vai ter uma particularidade do EVE, que é ele gerar esse endereço IP aqui, que é um endereço IP que ele gera para cada máquina, cada computador gera um IP diferente. Esse é o IP que gerou para o meu computador, essa imagem é do meu computador. Para o Puppin a imagem é a mesma, mas o IP é outro. Porque ele faz um cálculo a partir do [ininteligível], uma coisa dessa natureza. Vai gerar um 'ipzinho' para você, você joga o IP no navegador e vai funcionar via browser. Caso não apareça o IP para você ali, o login e senha é Root EVE, perdão, aí está UML, porque essa foto é pouco antiga. Depois eu vou pedir para trocar a foto. Root EVE, não tinha nem reparado que estava UML.

E você dá o comando IP add show pnet0 e ele vai te mostrar qual foi o IP que sua interface pegou, porque tem um DHCP nela. Enfim, é bem 'fácinho' de fazer funcionar. Essa é a tela que você vai ver. Então, admin EVE, a senha de tudo é EVE. Dentro dos roteadores a gente, depois, durante a aula, eu ficar(F) explicando o Mikrotik, eu vou falar [ininteligível] sobre o Mikrotik [ininteligível], no Huawei para vocês terem anotado aí.

Beleza. Passada essa parte aí do EVE, que vocês vão receber junto com o link para download o arquivo em PDF, e o emuladorzinho para vocês poderem acessar, vamos entender como é que funciona cada caixa, cada sistema tem uma maneira de lidar, tem uma maneira de usar. Então a gente vai permear por esse caminhar dentro das caixas de forma inicial, começando pelo nosso querido brinquedo da Huawei. Puppinzinho, passei a bola.

SR. LUIZ COSME PUPPIN MAGALHÃES: Bom, galera, a ideia, como o Lacier falou, alguns que estão assistindo o treinamento não têm muita prática com os equipamentos, ou pode ser o primeiro contato que tem com o equipamento, então a ideia é mostrar algumas coisas básicas que você precisa saber para mexer no equipamento Huawei.

E o principal de tudo: Tirei o cara da caixa, como é que eu acesso? Diferente do Mikrotik, que você tem o Winbox lá, conectou, acessou pelo Winbox, pelo Mac, tal, no Huawei, no Cisco, no Juniper, no Datacom, nos outros fabricantes você tem que ter um primeiro acesso via console.

E, nesse caso aqui, eu estou usando o PuTTY, mas tem gente que usa o Tera Term e outras ferramentas para acessar console, você tem que ter aquele cabo de console, o cabo que converte o conector UTP ou conector serial, alguns equipamentos ainda usam o conector DB9, para USB para conectar no computador. E você configura lá em qual com que o seu computador configurou, seu Windows apareceu lá. E o famoso 96008N1, que é 9600 de velocidade, 8 de bit de dados e stop bit 1, para que você consiga acessar via console.

Acessamos a console lá. Abrimos a telinha preta, CLI, primeira coisa que a gente precisa fazer em qualquer um dos fabricantes, o mais recomendado para qualquer um dos fabricantes, tirei da caixa, vejo qual é a versão do sistema operacional, entro no site do fabricante e verifico qual é a versão recomendada. Por quê? Cara, se a versão que está no equipamento não é a que consta como recomendada no portal, você

pode sofrer bugs que já são conhecidos, já foram resolvidos, já foram solucionados, e você vai ficar apanhando com o equipamento por besteira.

Então, no Huawei, para verificar o sistema operacional, eu dou um display version, e eu vejo a versão do sistema operacional. Nesse caso aqui era um NE40, e ele está na via 800R11C10SPC100, que, por um acaso, do NE40M2KB é a versão recomendada, é a versão que você deve usar em produção. Caso essa versão não esteja... Você entrou lá no portal, no caso da Huawei aparece um simbolozinho de joinha, um likezinho do lado da versão do portal, se não for a versão recomendada, você faz a atualização. Sendo essa versão, você pode deixar.

Não menos importante eu tenho o patch. No caso da Huawei, além da versão eu tenho que verificar o patch. O patch é onde eu corrijo bugs, corrijo problemas que são conhecidos nessa versão, que já foram encontrados e já foram solucionados por essa versão.

Então, no caso eu dou o display patch e eu vejo qual é a versão do patch que está rodando no momento no equipamento. O patch é recomendo que esteja sempre no último disponível lá no portal, porque ele soluciona os problemas conhecidos.

Outra coisa que é uma das principais que a gente precisa fazer no equipamento: Ajusta o horário. Pior coisa que tem, quando eu tenho um problema sério no meu ambiente, um problema que eu tenha que correlacionar onde que aconteceu esse problema, pior coisa que tem é: Cada equipamento da minha rede tem um horário diferente. "Ah, poxa, mas eu tenho NTP". Sim, depois você vai acabar configurando o NTP. Aqui eu estou tirando equipamento da caixa para colocar em produção. O NTP normalmente a galera configura depois que você já está lá, você já vai passar por uma fase de configurar monitoramento, tudo isso, o pessoal configura o NTP.

Mas se eu fizer essa atividadezinha básica na hora que eu estou tirando da caixa o equipamento, eu já consigo fazer com que, pelo menos, o relógio próximo do sincronizado eu já vou ter no equipamento. E é muito simples, não é nenhum absurdo fazer essa configuração. Aqui eu peço desculpas, porque está invertido. Primeiro eu tenho que colocar o timezone e depois colocar horário. Se eu fizer dessa forma que está aqui na tela, eu coloquei 23h aqui. Na hora que eu boto o timezone, ele vai cair para 20 horas. Então vai estar com três horas de diferença do horário que você colocou.

O correto aqui é: primeiro coloca o timezone e depois a gente vai e coloca o clock date time e ajusta o relógio, tá bom?

E a estrutura do sistema operacional da Huawei é muito similar a grande parte dos fabricantes que a gente vê aí, no nosso dia a dia. Quando eu entro no equipamento Huawei, eu entro em modo leitura. O que me indica que eu estou em modo leitura? É esse sinal de maior e menor. Na verdade menor e maior, quando o nome do equipamento está entre os sinais de menor e maior, quer dizer que eu estou em modo leitura. Eu estou no user view, no caso da Huawei. O user view, ele só me permite visualizar algumas configurações e alguns status do equipamento. Na Huawei o user view vem dessa forma, em outros fabricantes vem de outra.

Quando eu quero sair do user view e entrar no modo de escrita, no modo de configuração, eu, na Huawei eu digito system view. Na Cisco eu boto enable, na Juniper eu boto o edit. Todos eles têm alguma forma de pular do modo de leitura para o modo de escrita. Tá bom?

Quando eu vejo entre colchetes quer dizer que eu estou em modo de escrita no meu equipamento. A partir de agora eu consigo configurar alguma coisa.

Outras views que eu tenho, como eu falei, o equipamento, a estrutura do sistema operacional, como está escrito aqui, ela é hierárquica. Se eu quero configurar uma interface, eu entre no interface view. Eu digito lá: Interface gigabit 0000, a hora que eu der enter aparece o nome do equipamento, o tracinho, em qual interface eu estou para fazer a configuração. Ah, eu quero entrar na configuração do MPLS. Eu digito lá MPLS e dou enter, ele vai aparecer Huawei-MPLS. Quer dizer que eu estou dentro da configuração do MPLS. Beleza?

E aqui a função mais importante de qualquer fabricante. Essa você nunca pode esquecer: O interrogação salva vida. Principalmente para quem trabalha com múltiplos fabricantes e tem que decorar comandos de todos eles, o interrogação é o que salva a gente. Não preciso saber exatamente o comando, como é que escreve, qual é a sequência de informação que o comando apresenta. Se eu souber o interrogação, ele vai socorrer a gente ali. Se eu sei, por exemplo, o comando e esqueci um parâmetro dele, comando espaço e interrogação, ele mostra a lista de parâmetros e com um descritivozinho básico de cada parâmetro. Isso aqui pode socorrer a gente no momento em que esquecemos o comando, não lembramos exatamente qual é a sintaxe do comando.

A identificação do equipamento. Todo equipamento vem com Huawei como nome. Para entrar em produção, o ideal é que tenha uma identificação. A pior coisa que tem, além do problema do horário, e eu já peguei muita rede e assim, o cara não muda Sysname do equipamento. E quando você tem um momento de crise, você está com três, quatro telas, e você nunca sabe qual é o equipamento que você está mexendo. Então, eu sempre recomendo que a gente utilize esse nome aqui para que facilite a nossa operação no dia a dia.

Proteger a console, aquela console, que é o primeiro acesso que a gente faz, alguns equipamentos, na hora que você faz o primeiro acesso, ele pede para você criar uma senha. Outros equipamentos, ele não pede para criar essa senha, ele já acessa diretamente. Então, na Huawei, caso você esteja usando um equipamento, uma versão de equipamento que não pede para criar a senha no primeiro acesso, não custa nada você colocar lá user interface, console zero e setar uma senha. Ah, coloquei o equipamento num pop distante, um pop com pouca segurança. É sempre bom que você tenha uma senha, por mais básica que seja, para dificultar a vida do cara que vai acessar aquele site lá, e se ele quiser fazer alguma besteira na tua rede, ele vai ter uma dificuldade um pouco maior.

Eu digo que por mais bobo que isso seja, se a gente fosse pensar que toda medida de segurança era boba, a gente nunca colocaria chave na porta da nossa casa, fechadura na porta da nossa casa. Porque você chama o chaveiro e o cara, em alguns segundos, ele consegue abrir qualquer fechadura. Então isso aí é como se fosse uma fechadura. É básico, bobo, mas vai atrapalhar a vida de quem quiser entrar no teu apartamento.

A interface de gerência IP nos switches você tem a interface METH001, nos roteadores é a GIGA000. Mas a grande maioria dos equipamentos de rede da Huawei, elas possuem uma interface de gerência que é out of band. Então é uma interface de gerência que eu consigo fazer o acesso a ela, mesmo que o equipamento esteja inoperante. O sistema operacional está rodando, essa interface tá no ar.

Ah, tipo um looping de spanning tree e a CPU do equipamento está extremamente elevada. Por essa interface, ela é separada do processamento da caixa, você consegue acessar e fazer alguma coisa. Eu já vi

provedor, por exemplo, que todos os equipamentos da rede dele colocou IP 10.0.0.1. Por quê? Deu um problema na rede e o técnico da rua está com notebook, mas, putz, a maioria não tem um cabo de console junto com ele. Ele chega no pop, um cabo UTP ele tem em todo lugar. Ele pluga e acessa pelo IP 10.0.0.1, ele sabe que todo equipamento da rede está com IP 10.0.0.1, e ele faz a manutenção mesmo sem ter o cabo de console. Ou então eu já vi provedor também que ele colocou um switch, um switch básico no pop, ligou as interfaces de gerência todas nesse switch, cada equipamento com seu IP, colocou um roteadorzinho com modem 3G que fecha a VPN para rede de gerência dele. Então, quando ele tinha algum problema no rádio, o pop saiu do ar, ele, via 4G, via VPN, ele conseguia acessar as interfaces de gerência de todos elementos e fazer essa manutenção sem dor de cabeça nenhuma, por fora da rede, sem que a rede estivesse no ar.

Usuário de acesso, para configurar um usuário e acessar o equipamento, na Huawei eu tenho o triple A, o authentication authorization e accounting. Eu entro lá no AAA e crio um local user, nesse caso eu estou criando o local user chamado oper e botando a senha criptografada Teste123. Por que eu boto cipher? Porque na hora que eu der enter essa senha não vai ser gravada como Teste123, vai aparecer na configuração como uma chave criptografada, um hash dessa senha.

Se eu tiver que compartilhar esse arquivo com alguém, ninguém vai saber que a minha senha é Teste123, não vai ter como descobrir isso.

Claro, esse hash existem alguns aplicativozinhos que aparecem aí na Internet, que você consegue voltar atrás. Mas, mais uma coisa baseada naquilo que eu falei: Toda política de segurança, por mais boba que pareça ser, ela é alguma forma de atrapalhar a vida de quem está querendo fazer o ataque.

E eu boto lá nesse usuário oper o tipo de acesso que ele vai ter. No caso desse usuário eu estou dando FTP, SSH http. Mas posso criar usuário só com acesso ao SSH, e aqui no service-type eu digo que só o SSH. Se eu colocar FTP, eu tenho que dizer qual é o diretório que ele vai abrir, isso aí é padrão do protocolo FTP, não é uma característica Huawei. Quando eu crio um usuário de FTP, eu tenho que dizer qual é o diretório. Nesse caso ele vai abrir a flash, a raiz da flash.

Eu digo qual vai ser a chave de acesso. Se for um switch, para que ele seja admin eu boto nível 15, e, se for um roteador, para que ele seja admin eu boto nível 3. E eu posso diminuir esse nível para tirar alguns acessos do cara, tirar alguns privilégios que ele vai ter. Depois que eu criei o usuário na caixa, para ativar o SSH, uma coisa que a Huawei ajuda bastante na nossa vida, é que em alguns momentos ela chama o SSH de stelnet, em outros momentos ela chama de SSH. Então, por exemplo, eu estou dentro do equipamento, quero fazer um SSH para um outro equipamento da minha rede ,eu não digito SSH e o IP. Eu digito stelnet e o IP. Ah, mas agora quero criar um usuário de SSH, é stelnet user? Não, é SSH user.

Então, para facilitar a nossa vida, acho que não foi o mesmo chinês que desenvolveu todos os modos, um chamava de stelnet, o outro de SSH, isso aí a gente tem que ter um pouco de atenção na hora de fazer a configuração. Depois você vai acabar acostumando em que momento ele chama de stelnet, em que momento de SSH, mas é a mesma coisa.

Habilitei o servidor de SSH, vem desabilitado por padrão, eu habilito o servidor de SSH, crio aquele usuário oper, que a gente criou lá no triple A, eu venho aqui e crio o SSH user oper. Eu digo que o tipo de autenticação que ele vai ter vai ser por senha. Quando eu falo isso, ele vai lá dentro do triple A perguntar qual é a senha que esse usuário vai usar. Então, quando eu digo que authentication-type é password, eu

digo que vai ser local, e aí vai pegar a senha que eu criei localmente. Se eu digo Radius, quer dizer que ele vai no servidor Radius perguntar se a senha do usuário oper está certa ou está errada.

E assim como e botei service-type SSH lá em cima. No SSH user eu tenho que colocar service-type stelnet. E aqui não chama de SSH, ele chama de stelnet.

Vamos dizer que eu quero autorizar que esse usuário faça cópia por SCP. Aí eu venho aqui , service-type stelnet e SFTP, e ele vai permitir que as cópias de arquivo desse usuário possam ser feitas por SCP.

E eu venho lá no user interface, VTY 0 a 14. O que é isso? São os terminais virtuais, são os acessos remotos. Aqui eu estou configurando 15 usuários remotos. Ou seja, eu posso ter 15 usuários de administração simultâneos nesses equipamentos. E eu digo que os VTY de 0 até 14 vão utilizar o tipo de autenticação do triple A, ou seja, ele vai pedir usuário e senha para acessar o equipamento.

Quando eu vou atualizar o sistema operacional de um equipamento Huawei, no manual aparecem diversas formas de atualização. Eu posso acessar via http e copiar o arquivo. Eu posso subir no servidor FTP no equipamento e fazer um FTP para ele. Mas a forma mais correta, ou, melhor dizendo, a forma que menos dor de cabeça te dá é você, de dentro do equipamento, abrir uma sessão com o servidor de FTP. Ou seja, aqui fora do system view, ou seja, lá no user view eu digito FTP e o IP do servidor e ele vai me pedir usuário e senha do servidor.

A partir desse momento, eu estou dentro de um prompt de FTP, e os comandos, a partir daqui, são de FTP normal. Eu entro em modo binário. Sempre que eu quiser transferir um arquivo eu tenho que entrar em modo binário para que esse arquivo não seja corrompido. Isso é um padrão do FTP, não é nada característico Huawei. E eu faço um get do arquivo. Faço get do arquivo patch e faço get do arquivo .cc, que é arquivo da imagem do sistema operacional. Copiei esses arquivos, saio do FTP, dou o quit para sair do FTP e faço startup system software, o nome do arquivo .cc. Vou pedir para que no próximo boot ele atualize para esse que colocamos. E startup patch o arquivo .patch, o novo arquivo .patch. Ou seja, no próximo boot, vocês podem olhar aqui, no próximo boot ele vai subir um novo arquivo de CC e o novo arquivo de patch. Ele vai fazer atualização do sistema operacional e do patch. Tá bom?

Para ativar o SNMP nenhum mistério. Única dica é que o SNMP da Huawei vem habilitado o v3 somente. Então eu preciso colocar esse comando para ativar o v2c. O v2c é o que a galera usa por padrão. Então um ponto de atenção, depois de configurar a community eu sempre preciso colocar para ativar o v2c. Se eu não fizer isso, e você usa somente o v2c, você não vai conseguir acessar o SNMP desse equipamento.

E o mais importante, principalmente para galera que está acostumado com o Juniper e com o Mikrotik, se você não salvar, no próximo boot você perde tudo o que você fez. Isso aí é uma característica Cisco, uma característica que a Huawei também herdou, se você não salvar a configuração, você perde depois do boot.

Existe uma forma de automatizar isso, que é o set save-configuration interval 30; 30 é o mínimo que o roteador trabalha. O que ele vai fazer? A cada 30 minutos ele vai verificar se tem alteração na configuração. Se houver uma alteração que não foi salva, ele vai salvar essa configuração para você automaticamente. Ou seja, alterei uma configuração, não rebootei o equipamento dentro de 30 minutos, ele vai salvar a configuração para que você não perca no próximo boot.

E, se você fizer esse comando aqui de cima, além de salvar a configuração localmente, se houver uma alteração, ele vai pegar essa configuração que foi salva e vai fazer um backup para um servidor de FTP,

TFTP ou SCP. Aí você escolhe o transport-type que você quer para que faça o backup dessa config para você. Tranquilo?

Bom, isso era o básico que eu tinha para mostrar para vocês de Huawei. Acho que vai ajudar a galera que nunca viu a um Huawei, a pelo menos ter o primeiro contato. E vamos passar para o básico de Mikrotik, para quem nunca teve contato com Mikrotik, algumas coisas que ele vai passar, o Lacier vai passar aí para vocês de básico da operação de Mikrotik.

É contigo, Lacier.

SR. LACIER DA COSTA DIAS JUNIOR: Vamos lá.

Então galera aí que tiver alguma dúvida com o nosso querido RouterOS, vamos desmitificar ele aqui. Só clicar para passar o slide.

Então, o que ele tem aí? Uma ferramenta de CLI, mas que praticamente ninguém usa. A maioria esmagadora usa uma ferramenta auxiliar chamada Winbox, ela tem para Mac, tem para Windows. E esse Winbox é como se fosse uma espécie de interface gráfica do Mikrotik. Por trás ele está dando os comandinhos, mas pela frente é clica, clica, clica. Ele se comunica pela porta 8291, é gratuito. Ele tem um security mode, caso você queira operar com criptografia, e você baixa ele gratuitamente no site da própria Mikrotik, nesse link para download que está aí na tela de vocês.

O RouterOS, via de regra, ele vem com uma série de recursos, contudo a gente elenca alguns recursos que a gente entende como mais funcionais. Então o roteador dedicado, ele sim, faz controle de banda, ele tem algumas instruções de falha, que a gente chama de access list, porque firewall teria que ter um conceito um pouco maior do que as regras que ele faz.

Gerenciamento de usuário. Então você pode ter seu RouterOS para BGP? Pode, pode ter para OSPE, pode para PF, PLS. Pode. Pode ter [ininteligível] para PPPoE? Pode. Então também vai ter a gerência de usuário, vai interagir com servidor de Radius.

A gente tem modelos que tem parte de Wi-Fi. Em ambiente de escala a gente não utiliza, porque as caixas maiores não têm Wi-Fi. Mas existem versões para doméstico. Então tranquilamente você consegue usar ele para fazer a parte de Wi-Fi. E tem alguns modelos, inclusive, para produção de ambiente de backbone. Fazer lá longa distância e tal. Entre outras opções que o Mikrotik traz consigo dentro do sistema operacional.

Além disso, além desses roteadores, essas boards que já vem montadas, você também tem a possibilidade de baixar uma imagem e instalar no X86, Inclusive a nossa imagem [ininteligível] não é uma imagem de X86. "Lacier, o que ela muda da caixa real para o X86?". Absolutamente nada em termos de funcionalidade. Você vai ter talvez uma caixa com hardware a mais, com Wi-Fi, por exemplo e outra não. Em termos de funcionalidade, tanto no X86, quanto em uma placa propagada para isso em uma Routerboard eles vão funcionar exatamente da mesma forma.

Pacotes relevantes. No Mikrotik você tem essa possibilidade de você remover pacotes de dentro do sistema operacional, do RouterOS. Então, por exemplo, ele vem lá com o pacote de controle do Wi-Fi. E a sua RB, o seu roteador não tem Wi-Fi. Então você não tem porquê ter aquele pacote Wi-Fi, pacote wireless dentro do seu equipamento, até porque se tiver vulnerabilidade que explore esse pacote, se você não tem

o pacote, ok, você não precisa se preocupar com ela. Você tem pacote vagando no seu equipamento, buscando um hardware que nunca vai chegar, isso é um problema.

Então a recomendação é: Prepara os equipamentos que você vai usar como roteador, dentro da sua estrutura, você tem pacote System, tem PPP, DHCP, PPP e DHCP deixa lá, porque são pacotes passivos. Então a gente pode vir a utilizar. Caso você queira remover, pode também. Advanced-tools, NTP, porque ninguém merece ficar vendo hora de 1970, principalmente na hora de ler um log é de suma importância. Pacote IPv6, MPLS, os próprios drives da Routerboard, o pacote routing e security multicast.

Então os pacotes não utilizados ficam consumindo processamento desnecessário e pode ser um risco para sua segurança. A gente sempre recomenda que você não os tenha.

Existe a questão do modo seguro, que você pode usar ela através do comando Ctrl+X. O que esse modo seguro te traz de bacana? Você está fazendo uma intervenção remota, eu uso muito isso, vou fazer uma intervenção remota e posso fazer alguma movimentação caixa que a caixa vai me desconectar. O que ele vai fazer? Se a caixa me desconectar, ele apaga as configurações que eu fiz e volta para configuração de quando eu tinha condição de login. Então isso é uma coisa que ajuda muito. No dia a dia eu percebo que o pessoal não usa bastante. Mas quando o pessoal está mexendo em alguma coisa que está muito longe, não tem uma pessoa fisicamente lá, costuma-se ter esse cuidado de usar esse recurso de logar em modo seguro.

Então você também tem aí, para quem for logar em dupla na caixa, fica esse flag R para saber o que está sendo feito, que não está efetivamente aplicado na caixa. Caso a pessoa não dê o Ctrl+B para salvar, ela vai perder aquela configuração e o que já está realmente dentro da caixa. Uma outra coisa bacana é que você tem o system history print, que é você ver o histórico, quando aquele seu técnico gente boa que fala: "Não, eu não fiz nada na caixa". Você tem condições de ver o histórico do que foi feito na caixa, os 100 últimos comandos que foram dados na caixa, e verificar, aferir ali o que pode ter acontecido que levou aquele comportamento que você não queria ou comportamento que não está adequado. Então são procedimentos aí, que a gente tem um cotidiano usual para eles.

A parte de manutenção dos equipamentos, ela é bastante facilitada. Então a atualização, ela é tão facilitada que ela chega a ser nociva para o próprio equipamento. Tem que ter um cuidado especial com essa questão da atualização, por quê? Porque o Mikrotik é um fabricante que solta muita atualização. E nem sempre essas atualizações ficam 100% funcionais, e aí você só vai descobrir isso em produção. Então o que a gente normalmente recomenda? Que você atualize para uma versão chamada long term, que é a versão que está quase com a mão no fogo por ela, uma versão que consegue ter aí 99% de certeza que você não vai ter uma instabilidade no seu equipamento. Pessoal às vezes fica em uma agonia, coraçãozinho ali fica palpitando forte, querendo colocar a última versão, mas eu não recomendo que você coloque a última versão. E quiçá uma versão escrita palavra 'teste' nela. A não ser que você seja cobaia, a não ser que você seja um aluno, ou até um próprio dono de provedor, [ininteligível] um Mikrotik na sua casa. Aí, lá na sua casa, você colocou essa versão porque você quer fazer um teste, o wi-fi fica na sua mesa de trabalho, no seu escritório, na sua casa, e aí você é bacana, você quer fazer um teste ali, tudo bem. Acho justo, acho válido, eu, inclusive, faço isso, não é? Tem uns equipamentos pequenininhos. Eu até tenho um aqui do lado, só um minutinho.

Vantagem de estar no escritório é essa, tá vendo? Então, olha, eu tenho esse brinquedinho aqui, que toda vez que eu quero fazer um teste, eu jogo a configuração aqui dentro. Inclusive esse aqui está com a versão 7, a versão unicórnio, tão famosa, tão falada, a versão beta. Então está aqui dentro por quê? Porque é um

'Wi-Fizinho' que fica na minha mesa, só eu que conecto nele. Ele tem portinha Ethernet, quando eu quero fazer alguma conexão via cabo. Então ele facilita minha vida para quando eu quero testar ou homologar alguma coisa. Você vai colocar em produção? Nunca na vida. Esse aqui é um equipamento que ele cabe na palma da mão, é de teste, não é equipamento para entrar em produção de nada. Meu Wi-Fi de produção não é esse equipamento aqui, esse é meu Wi-Fi de teste.

Então, você quer fazer uma atualização, você quer validar, testar, ou você usa o emulador EVE, que vai te dar aí 99.9% dos recursos de um hardware, caso você não tenha um hardware aí fácil como eu tenho aqui, para você fazer seus testes, aí você pode sim, atualizar na última versão, a versão mais top, e moer o equipamento para fazer sua validação.

No mundo real a gente tem cliente em cima do equipamento. O equipamento está em produção, é crítico. O momento atual deixou a Internet cada vez mais crítica, mais sensível, então não dá para fazer teste em produção. Recomendo aí que você tenha equipamento ou use um emulador para fazer isso.

Essas são as licenças, caso você tenha alguma necessidade de operar o X86, por quê? Porque as licenças físicas, elas basicamente todas vem na licença nº 6. São poucos equipamentos que vem com licença menor que a licença 6, hoje praticamente tudo é limitado. Então caso você precise de uma licença, essas são aí as limitações de cada uma dessas licenças que o fabricante tem, e seus respectivos preços.

Beleza. Backup. Backup é um negócio que eu não considero importante, eu considero vital. Porque se o seu backup der problema, você vai ter problema. E o Mikrotik também facilita sua vida com o backup. Embora eu considere que esse botão backup aqui, ele não é seu amigo. Esse botão backup, ele existe para te atrapalhar. Por quê? Poxa, o fabricante criou um botão backup para me atrapalhar? Olha, já falei isso para o fabricante em um evento. Porque, assim, ele não é um backup, ele é uma foto do equipamento. Em versões mais antigas ele ainda vinha com [ininteligível], trazia um monte de lixo, quando você colocava ele em outro equipamento, ele virava uma bagunça.

Porém, o fabricante também tem uma maneira de você tirar esse backup, que é maravilhosamente perfeita, impecável. Inclusive a gente fez um scriptzinho para poder facilitar sua vida. O comando em questão que efetivamente faz o backup é esse aqui, export file. Esse aqui é o comandinho que faz igual, e aí você bota o nominho do equipamento.

O que é esse script aqui que o professor vai deixar para vocês? Esse script é um facilitador. Por quê? Porque tu não vai entrar todo dia lá, meu queridão, e ficar colocando para rodar o backup, você quer automatizar isso de alguma forma. Então existem dezenas maneiras de automatizar. Essa aqui é apenas uma sugestão que a gente sabe que funciona e que vai te dar uma tranquilidade, depois você pode ir melhorando ela, que é: Ele manda isso para uma conta de e-mail. Então, todo dia, no horário que você colocar o agendamento, ele vai mandar um backup para uma conta de e-mail. Obviamente eu peço para os alunos não mandarem para essa conta router@vlsm, essa conta está no meu cliente de e-mail, e toda vez que eu dou aula, os alunos ficam mandando e-mail, e eu respondo: Olha, recebi o seu backup, muito obrigado. Mas eu não vou conseguir guardar ele para você. O aluno: "Poxa, professor, foi mal, esqueci de trocar". Então manda parta uma conta sua.

E uma coisa principal também, que tem aqui nesse arquivo, que é o nome da caixa. Em todas RBs, como o Puppin muito bem colocou, elas vem escrito o nome do fabricante, ou vem escrito admin, vem o nome padrão. Então não manda o backup com o nome padrão, porque você vai ter 30 backups com o nome

igual. E aí isso vai ser um problema na hora que está com a faca no pescoço tentando achar o backup para recuperar.

Então dicas para usar esse script, acerta nome da caixa, bonitinho, coloca o IP aqui também, que esse IP não é o IP correto. Coloca a conta que vai enviar, tudo certinho, aqui a gente faz elegantemente uma correção de ANTP para hora poder ficar certinha. E manda o e-mail, funciona lindamente. Então, assim, essa aqui é uma sugestão para você poder mandar o seu backup por e-mail.

Beleza? Então a gente fica por aqui com essa introdução aí do RouterOS. E vamos, agora, partir para parte do MPLS com o nosso querido Prof. Puppin.

SR. LUIZ COSME PUPPIN MAGALHÃES: Bom, Lacier, obrigado. Vamos continuar, então, com a nossa ementa.

Seguindo lá aquele planejamento que a gente fez, falar um pouco do básico dos equipamentos e tal. E não tem como a gente trabalhar com VRF sem ter o MPLS. Sei que MPLS não é um protocolo que todo mundo que está assistindo conhece plenamente. Não é o objetivo desse treinamento explicar como configura passo a passo o MPLS em si. O nosso objetivo final é mostrar a VRF, que é um serviço que roda em cima do MPLS. Mas, para contextualizar um pouquinho, a gente vai passar um pouco da teoria do que é o protocolo.

E a gente já começa pela sigla. O que quer dizer MPLS? Esse protocolo que todo mundo fala o tempo todo. A gente escuta falar o todo momento, Um protocolo relativamente antigo, foi criado no final dos anos 90, 97, 98 mais ou menos, e muito utilizado no início dos anos 2000 pela... desde o início dos anos 2000 pelos grandes operadores, e a gente vem escutando no mercado de provedores tem quatro anos, mais ou menos, que ele começou a se popularizar no mercado de provedores, porque começaram a surgir opções de menor custo no mercado, e com confiabilidade para implementar a MPLS. Que é um protocolo muito útil para o provedor. Eu digo que, inclusive, que ele é essencial, principalmente para o provedor que trabalha com trânsito ou com transporte. Não só aquele provedor que trabalha vendendo varejo, assinante final, mas principalmente os provedores de atacado, eu acho essencial a implantação do MPLS.

E a sigla nada mais é do que o Multi Protocol Label Switching. Ou seja, ele é um protocolo de encaminhamento de pacotes através de label, através de etiquetas, e multiprotocol, ou seja, qualquer coisa que você quiser transportar, ele consegue transportar por dentro dele. Porque ele tem a capacidade de esconder o conteúdo do pacote dentro de uma etiqueta.

Ele bota uma etiqueta na frente e, mesmo que o meio do caminho não saiba interpretar o que tem dentro do pacote, ele vai passar, vai encaminhar normalmente só lendo aquela etiqueta. Ele substitui a decisão de roteamento IP que originalmente é feita por pacote, e ele acaba realizando a comutação dos pacotes por fluxo, por circuitos. Então como a gente sempre diz: No mundo da telecom nada se cria, tudo se transforma. E o MPLS não foi um protocolo inventado do zero. A Cisco que desenvolveu originalmente o MPLS, e ele não foi inventado da cabeça de um desenvolvedor do nada, sem nada para se basear. Ele é baseado e é muito similar ao frame relay. Ele foi um protocolo que usou muito do que de bom tinha no frame relay, e ele veio para resolver os problemas que o frame relay trazia. Por isso que ele tem uma característica tão próxima do frame relay, que era estabelecimento de circuitos e circuitos individuais para que os clientes pudessem fazer a comutação dos pacotes dele sem necessitar de roteamento.

Eu substituo a decisão do cabeçalho IP por uma etiqueta. Então, no lugar de cada pacote ter que ser processado individualmente e a cada salto, cada pacote ter que ser tomada uma decisão de roteamento,

quando o pacote entra em uma rede MPLS o caminho já está pré-estabelecido. Então o meio do caminho não tem que ficar processando a cada pacote. Eu crio um circuito e todos os pacotes vão seguir esse mesmo circuito enquanto não haja nenhuma modificação, nenhuma convergência nessa rede.

Aqui tem uma observação, uma das vantagens do MPLS é a maior eficiência no encaminhamento de pacotes. E classicamente se diz que essa é a maior vantagem que o MPLS tem. Eu gosto de acrescentar aqui uma informação: A maior vantagem que o MPLS tem, que é a maior eficiência no encaminhamento de pacotes, só é perceptível quando eu tenho múltiplos saltos no meio do caminho. Um provedor de pequeno, médio porte que implementa MPLS, normalmente ele tem dois, três saltos no máximo, de distância entre o cliente e a borda dele.

E numa rede desse tipo, ele normalmente não percebe essa grande vantagem que o MPLS traz, que é a maior eficiência no encaminhamento. Ele mal vai perceber isso. Por quê? O processamento que você economiza no meio do caminho se torna quase nulo pelo que acrescenta no processamento da entrada do pacote.

Eu digo que para o provedor de pequeno e médio porte, a maior vantagem que o MPLS traz é, por exemplo, a possibilidade de você ter múltiplos caminhos na sua rede sem a preocupação de que o spinning tree feche um loop nessa rede. Ou eu não quero usar spanning tree numa rede de provedor, em uma rede metro, e tenho que usar protocolos de proteção de anel, ERPS, EAPS, só que eu fico limitado a um anel. Dois caminhos: Um caminho parado e um caminho passando tráfego. Então, se eu quero ampliar a minha redundância nessa rede eu não consigo. Já com o MPLS essa é uma das vantagens, essa é uma das características que são úteis do MPLS para um provedor que vai trabalhar com esse tipo de serviço.

E cada rótulo indica um índice para uma rota na tabela de roteamento do próximo roteador. Eu gosto de dizer que uma rede MPLS ideal é aquela que na tabela de roteamento que gera label você só tem as rotas das loopbacks dos roteadores.

A rede MPLS, ela é feita para ser uma rede de transporte. Ou seja, os pacotes dos clientes não passam por dentro da rede MPLS, os pacotes dos clientes são encapsulados em um serviço que utiliza a rede MPLS para trafegar. Só que se você olhar a tabela de roteamento do MPLS, não tem rota de cliente nenhuma. Você não tem nenhuma rota diferente das rotas de loopback e, no máximo, as rotas dos ponto a ponto que você usa entre os equipamentos.

Como diz essa terceira característica aí, o objetivo do regime MPLS não é o de conectar diretamente os sistemas finais. Ao invés disso ela é uma rede de trânsito.

Então, para fazer trânsito eu tenho uma VPN do ponto de origem, da loopback do ponto de origem com a loopback do ponto de destino. E o pacote do cliente vai passar dentro dessa VPN.

Agora, não confundam VPN com criptografia. Muita gente fala assim: "Ah, se é uma VPN, então, ela é segura?". Não. Ela é uma VPN que ela isola o tráfego de um cliente para o outro. Ou seja, um cliente não consegue enxergar o tráfego do outro. Agora, se você capturar um pacote no meio dessa rede, o tráfego do cliente, se o próprio cliente não criptografou, o tráfego do cliente vai estar aberto, em texto plano, normalmente. Porque eu não criptografo. VPN, o próprio nome é Virtual Private Network, não diz em momento nenhum criptografia. Existem protocolos de VPN que criptografam e protocolos que não criptografam. Beleza?

Como eu falei lá no início, ele é chamado multiprotocol, multiprotocolo, porque eu consigo passar qualquer protocolo por cima dele. E aí a gente tem uma VPN que é bem característica para isso, que é APWE3, VPWS, no Cisco o X-Connect, na Juniper o L2 Circuit, não importa qual o nome que cada fabricante usa, todas elas estão baseadas na mesma RFC, que é a RFC do PWE3, que é a RFC que especifica o ponto a ponto, a VPN do tipo ponto a ponto.

Então, se eu tenho de um lado um equipamento que sabe falar um protocolo que ninguém mais sabe falar, e ele se conecta em uma rede IP normal, falando protocolo MPLS, e na outra ponta dessa rede eu tenho outro equipamento que escute MPLS e transforme de volta nesse protocolo desconhecido, no meio do caminho eu posso ter qualquer fabricante que fale MPLS, que esse protocolo vai ser passado pelo meio do caminho. Porque ele fica oculto para o meio do caminho, o meio do caminho não enxerga o conteúdo desse pacote que está sendo passado.

Antes do MPLS a gente tinha uma característica, lá no final dos anos 90, a gente tinha uma característica em que eu tinha redes separadas, redes segregadas, com cabos separados, com equipamentos separados, backbones diferentes. Eu tinha uma rede inteira de telefonia móvel segregada da rede de telefonia fixa, segregada dos dados que rodavam em ATM, frame Relay, segregado de Internet em si, segregado da TV à cabo. Eu tinha um emaranhado de tecnologias diferentes para falar protocolos diferentes. E as operadoras tinham que lidar com essa infinidade de redes e serviços. Cada serviço tinha sua própria rede, e isso fazia com que houvesse muito desperdício de recursos. Muitos equipamentos que ficavam lá, às vezes ociosos, tendo equipamento, por exemplo, equipamento de telefonia fixa que ficava ocioso, e tinha equipamento da rede de telefonia móvel sobrecarregado, e você não podia utilizar os recursos excedentes de um para o outro.

E lá o final dos anos 90, início dos anos 2000, buscava-se muito a tão falada next generation network, as redes de nova geração. O que era isso? Qualquer tipo de acesso, independente do meu tipo de acesso, eu tinha um único backbone IP, com alta disponibilidade e performance, e, ligado a esse backbone, um conjunto único de aplicações e conteúdos. Então não importava se o cliente estava no móvel, estava no DSL, estava discado ou no ISDN, não importava. O conteúdo e aplicações estavam todas sendo compartilhadas por qualquer tipo de acesso.

Por exemplo, a TV à cabo, eu tinha o serviço de TV à cabo que podia ser entregue para diversos tipos de acesso, independente de necessitar de um backbone independente para passar esse serviço. Tá? Foi o MPLS que conseguiu ajudar a trazer. Não digo que foi o único, mas ele foi um dos grandes elementos que fizeram com que a gente alcançasse a tão buscada rede de nova geração.

E o que é o MPLS em si? O MPLS, na verdade, ele pega o pacote normal, que eu tenho o cabeçalho de L2, o cabeçalho de L3 e o payload do pacote, e ele chega entre cabeçalho de L2 e o cabeçalho de L3 e coloca uma etiqueta, que é MPLS label. Ele pode botar uma, duas, três, quatro, várias etiquetas, cada etiqueta com a sua função. Por isso que quando a gente fala que sobe o MPLS no backbone, o backbone, por padrão, pacote máximo que ele passa é 1500. Se eu subo o MPLS nesse backbone, eu preciso aumentar a MTU padrão desse backbone. Por quê? Se eu tenho pacote de 1500 e coloco uma label, ele já vai para 1504. Se o meu backbone está restrito a 1500, ele vai começar a fragmentar. Se eu rodo... se eu tenho a label de transporte e eu tenho uma label de serviço, já são duas, vai para 1508. Se eu tenho um fast rerout, eu já vou para três labels, pelo menos, já vai para 1512. Então eu preciso aumentar o MTU do backbone para garantir que os pacotes com etiquetas não sejam fragmentados só porque ultrapassaram o limite de 1500, caso eu precise passar um pacote de 1500 de tamanho por ela.

Esses 32 bits, ou seja, 4 bytes, que eu tenho que inserir na etiqueta, nada mais são do que os primeiros 20 bits, são a label, são a etiqueta, um número que identifica aquele índice da tabela de roteamento. O campo exp, que é o campo de classificação de serviço. Ou seja, eu posso criar QoS para protocolos que não suportam o QoS. Eu crio um QoS para uma VPN, para que ela, caso haja algum tipo de enfileiramento no meio do caminho ela possa passar à frente de outro pacote no buffer do roteador.

Eu tenho o campo S, o campo de Stack. No próximo slide eu mostro o que seria o Stack. Que mostra para quem está processando esse pacote que eu tenho a label principal e uma label reserva, uma label secundária depois. Se ele estiver marcado com bit 1 quer dizer que eu tenho uma label depois, que é a label de backup, label de redundância.

E eu tenho o campo TTL, em que eu posso copiar o TTL original para, ele decrementa nos saltos que ele der na rede, e, depois, no final, eu copio o resultado e sobrescrevo o TTL original do pacote.

Aí falando um pouco do label stack, eu falei que eu tenho uma label de transporte, só que pensa, se eu tenho a comutação por circuito do MPLS, vamos dizer que esse circuito tem oito saltos, e no sexto salto tem um rompimento de fibra. Todos os pacotes que já estão na rede, que já estão trafegando por esse circuito, se eu não tivesse uma redundância, o circuito alternativo, todos os pacotes teriam que ser descartados e o protocolo de controle, protocolo de L4, os protocolos que controlam a transmissão, teriam que retransmitir esses pacotes, seriam perdidos esses pacotes. Eu posso ter, dentro do próprio pacote, uma label secundária que vai estipular um caminho alternativo. Se houver um rompimento no meio, eu tenho uma label secundária para que esse pacote não tenha que ser jogado fora e esperar retransmissão. Então os pacotes que já entraram na rede, eles já vêm com o caminho alternativo marcado como segunda label, como stack da primeira label, tá?

E crio esse caminho, eu estou falando o tempo todo que o MPLS, ele tem um caminho pré-estabelecido. Existem três formas de criar um caminho MPLS, que é a LSP, Label-Switched Path. A forma mais básica, mais simples é o Label Distribution Protocol, o LDP. Foi um protocolo desenvolvido lá nos primórdios do MPLS, que ele usa a inteligência do OSPF para fazer a criação das labels para o MPLS funcionar.

Só lembrando, o MPLS não é um protocolo de roteamento. O MPLS é um protocolo de encaminhamento de pacotes, ele é um protocolo de camada 2. Então ele é escravo de um protocolo de roteamento. Qual é o protocolo de roteamento que o MPLS obedece? Ou o OSPF ou o ISIS. São os dois protocolos de roteamento em que o MPLS pode se basear. E o LDP, ele vai se basear em um dos dois protocolos para escolher o caminho e criar a label.

E as labels são sempre criadas do destino do pacote nesse sentido, destino para origem. Na hora que eu ligo esse roteador na minha rede, ele avisa para o vizinho o seguinte: "Olha, vizinho, eu sou dono dessa rede. Eu sei chegar nessa rede 128.89. E, se você quiser me mandar por MPLS um pacote, me mande para essa rede, me mande com etiqueta 9 na frente". O cara do meio do caminho grava na tabela dele, e ele recebe desse outro vizinho: "Se for para 171.69, mande com etiqueta 7". Ele também grava na tabela dele. E ele escolhe duas labels e avisa para o vizinho diretamente conectado a ele: "Vizinho, se você for mandar para 128.89, me mande com etiqueta 4, e se for mandar para 171.69 me mande com a etiqueta 5". E, depois que toda rede convergir, eu terei em todo o mundo uma tabela de roteamento com esses índices de label criados nessa tabela.

Depois que esses índices estão criados, eu posso fazer o encaminhamento. E como é que funcionaria o encaminhamento? Chegou um pacote com destino à uma rede conhecida, esse pacote vai receber a

etiqueta referente àquela rota na tabela. Vai colar a etiqueta lá naquele campo de label do MPLS entre a camada 2 e a camada 3, e mandar pela interface indicada para o vizinho. O vizinho olha: "Opa, eu recebi pela interface que está conectada a esse meu vizinho, um pacote com etiqueta 4. Eu tenho que mandar esse mesmo pacote pela interface 0 com a etiqueta 9". Então ele tira essa etiqueta 4 e coloca a etiqueta 9, e manda pela interface 0, que é o que está mostrando na tabela dele.

Observe aqui que ele não olhou o destino do pacote, ele olhou a etiqueta. E a etiqueta já mostrou para onde ele tem que mandar. Chegou aqui nesse roteador, ele falou: "Opa, eu recebi do meu vizinho por essa interface com etiqueta 9, eu tenho que mandar pela interface 0, sem etiqueta, porque aí já não é mais MPLS". Ou seja, somente esse núcleo aqui tá trabalhando com o MPLS, e a gente trabalha com etiqueta. Esse cara no meio do caminho é conhecido como P da rede. Ele escuta a MPLS e fala MPLS. Esses caras aqui da borda são conhecidos como PE. Eles escutam IP, nesse caso, mas poderia ser qualquer protocolo, e falam MPLS para o meio do caminho.

Para facilitar, vamos fazer uma analogia com o sistema do Correio. Vamos fingir que o sistema de correio funciona com MPLS. Como é uma analogia, vai ser aproximada. Eu estou aqui no Brasil InterPart, que é o prédio do NIC.br. E aqui em Londrina eu tenho a Torre Pietra, que é aonde fica a VLSM e o shopping Aurora, que é o prédio do lado da VLSM. Do lado do prédio da VLSM. E tenho aqui agência de Correio de Londrina, que seria um PE da rede; o centro de distribuição de Curitiba, um P; O centro de distribuição de São Paulo, que é outro P; e a agência do Morumbi, que seria o outro PE na outra ponta.

Na hora que eu ligo o sistema de correio, eu ligo agência Londrina, ela avisa para o centro de distribuição de Curitiba o seguinte: "Curitiba, se chegar qualquer coisa aí com destino a alguém que esteja no Shopping Aurora, coloque a etiqueta 12. Agora, se chegar alguma coisa aí em Curitiba com destino a qualquer empresa que esteja no Torre Pietra, mande com etiqueta 3". Curitiba: "Ah, beleza, Londrina. Obrigado".

Avisa para São Paulo: "São Paulo, se mandarem alguma coisa para o Shopping Aurora, mande com etiqueta 7. Mas se qualquer coisa que chegar aí o destino for a Torre Pietra, mande com etiqueta 9". O centro de São Paulo aprende isso e ensina para todas as agências ligadas a ele, inclusive a agência de Morumbi: "Agência Morumbi, se mandarem alguma coisa para o Shopping Aurora, mande com etiqueta 5 para mim, que eu sei fazer. Agora, se mandarem alguma coisa para a Torre Pietra, me mande com etiqueta 2".

Liguei a minha rede. Minha rede já está com as labels criadas lá, ou seja, o meu label switch PF já está pronto, já está preparado esperando o primeiro pacote chegar. Aí o pessoal do NIC chega lá na agência Morumbi com uma carta escrito: "VLSM, Torre Pietra, aos cuidados do Luiz Puppin". Aí o que agência Morumbi vai fazer? Vai pegar essa carta, vai colocar uma etiqueta em cima do endereço de destino, ou seja, ninguém mais vai ver o endereço de destino, vai pegar uma etiqueta vermelha bem grande e colar em cima do endereço.

Ninguém sabe mais para onde essa carta vai. Única coisa que existe nessa carta é um número 2 colado, e ela manda para o centro de distribuição de São Paulo. O centro de São Paulo vai olhar e falar assim: "Opa, eu recebi uma carta vindo do Morumbi, e ela está com etiqueta 2. Eu não sei para quem é. Mas eu sei que se vier do Morumbi com etiqueta 2, eu tenho que tirar a etiqueta 2 e botar etiqueta 9. E mandar para Curitiba". Aí chegou em Curitiba, Curitiba: "Opa, veio de São Paulo com etiqueta 9. Eu não sei mais para quem é. Não preciso saber para quem é. Eu sei que se vier com etiqueta 9 de São Paulo eu tenho que mandar para Londrina, com etiqueta 3". E cheguei em Londrina. Cheguei em Londrina, Londrina sabe que ele tem que tirar a etiqueta 3, olhar quem é o destinatário, que é VLSM e mandar... Minto. Ele não olha

que é a VLSM. Ele tira etiqueta 3 e manda para a Torre Pietra. Na hora que a Torre Pietra recebe a carta, ela olha: "Ah, é para o escritório da VLSM, aos cuidados do Luiz Puppin, entrega no escritório da VLSM".

Assim funciona uma rede MPLS. Eu faço o transporte do pacote, o meio do caminho não sabe quem é a origem e quem é o destino. O meio do caminho só sabe quem é o vizinho que vai receber e qual a label que o vizinho espera. E, na hora que o cara recebe, ele sabe para qual label ele tem que transformar, ou ele sabe se ele tem que tirar a label e encaminhar para algum cliente, algum CE específico dele.

Ah, e como eu falei, existem três formas de criação desse caminho, dessa LSP. Uma das formas a gente já viu como funciona, que é o LDP, Label Distribution Protocol. E existem outras duas formas. A segunda forma que a gente vê aí na tela é o RSVP-TE. Ele é feito para túneis TE. O túnel TE, ele é um aditivo do MPLS, ele é um serviço do MPLS que, como eu falei, o MPLS, ele é escravo do protocolo de roteamento. O MPLS TE, ele faz com que você tenha outras opções antes de perguntar ao protocolo de roteamento, se houver algum empate de rota. Então eu consigo designar túneis por dentro dessa rede que desobedecem o protocolo de roteamento da minha rede.

Então eu consigo, por exemplo, se eu tenho dois caminhos, um caminho com o que o SPF diz que é preferencial e um que o SPF diz que é mais longo, com o RSVP-TE eu consigo fazer com que o MPLS obedeça a esse caminho mais longo e desobedeça o SPF.

Nas labels de transporte eu posso substituir o LDP pelo RSVP-TE. E nas L2 VPN eu preciso do LDP ou do MP-BGP, que é terceira forma de geração. Como o próprio nome já diz, ele é baseado no BGP, e ele é um multiprotocol BGP. Ele é uma extensão do BGP que gera label. Ele é utilizado para VRF. Esse é o protocolo que a gente vai utilizar para VRF. E ele faz a distribuição das labels da VRF, para que a gente consiga fazer o roteamento das L3VPNs aí por dentro dessa rede. Tá bom?

De MPLS, basicamente isso que a gente precisava dar um overview para vocês.

Agora eu passo aí para o Lacier para falar um pouquinho de BGP. Que vai ser necessário para a gente entender de VRF, e entender dessa automatização, dessa automação que a gente vai fazer aí, no laboratório. Vai lá, Lacier, é contigo agora.

SR. LACIER DA COSTA DIAS JUNIOR: Obrigado, Puppin.

Cara, eu vou te falar que eu amo sua explicação de MPLS, principalmente a parte do Correio.

SR. LUIZ COSME PUPPIN MAGALHÃES: Aprendi com você, só mudei algumas coisinhas.

SR. LACIER DA COSTA DIAS JUNIOR: Até porque eu estou com um ódio nesse momento do correio. Mas vamos nós aqui. Gente--

SR. LUIZ COSME PUPPIN MAGALHÃES: Quem sabe um dia eles usam o MPLS e passam a funcionar melhor, né?

SR. LACIER DA COSTA DIAS JUNIOR: Exatamente. Vai que essa sua aula vaza para alguém da engenharia dos Correios, se Deus quiser.

Então assim, não tem condição de a gente operar sem protocolos empilhados hoje em dia. Então a gente brinca que o SPF, ele é o chão, aí vem o MPLS, a gente tem o nosso querido BGP aí, para poder fazer isso, mas é o nosso querido iBGP. A gente vai falar de iBGP.

Então, o que é o BGP? O BGP é apoiado aí em uma modalidade numérica chamada ASN, são os Autonomous System. Obrigatoriamente o provedor de Internet aí bem organizado, ele tem que ter o AS dele. Então obrigatoriamente um provedor bem organizado tem que ter o AS dele. E o AS dele vai fazer com que ele tenha esse número dessa licença, vamos chamar assim, para ele poder operar.

"Pô, Lacier, eu não tenho, por N motivos, mas eu já quero montar isso, eu quero montar um laboratório, meu NPE para poder entender. Que número que eu uso?". Você pode usar essa faixa de 64.512 até 65.535, que é uma faixa privada dos AS, seria equivalente a IP 968, o IP F180, são IPs internos aí. Os números efetivos são liberados aí pelo Lacnic na nossa região através do NIC.br, que faz esse trabalho de controlar e fazer essas entregas.

Beleza. Então o protocolo de distance vector, recordando o nosso querido e antológico RIP. Então o BGP também opera como vetor de distância. A versão do versão BGP é 4, nasceu na RFC 1771, os prefixos da rede são anunciados ali e encaminhados entre essas sessões do BGP. Isso é BGP clássico.

Então a topologia interna, graças a Deus, ela não é informada, então vamos pensando aí [ininteligível] em BGP, você não sabe como que é a rede do vizinho. Você sabe como que é a sua rede. E o pacote passa pela rede do vizinho e vai embora sozinho. E lá dentro da rede do vizinho, problema dele, fazer esse pacote transitar.

Ele troca aí, as informações que a gente chama carinhosamente na tradução de encontrabilidade, através das mensagens de LNRI. E o BGP opera na porta 179. Recomendo que a gente não mexa nessa porta, inclusive.

Mensagens do BGP. Então, para que a coisa funcione, os dois BGPs precisam se comunicar e precisam lá estabelecer entre eles algumas regras. Essas regras permeiam por essas mensagens que uma caixa fica mandando para outra, que a gente chama de BGP speaker, que é o responsável pelas informações, enviar informação de um vizinho para o outro.

Então durante o intercâmbio o BGP pode cair, ter rompimento de fio. enfim, falha no iBGP. E devido a isso ele tem um processo de sinalização open, update, keepalive ou notification e uma quinta, que é o route-refresh, que depende se a caixa está com esse recurso ativado ou não, para você poder forçar a leitura do iBGP.

Itens que não podem faltar? Route ID. Imprescindível, ele identifica o remetente. Se você não escrever nada, vai ser o maior IP de interface, ou o IP de loopback, a gente sempre recomenda que use o IP de loopback para poder fazer isso, igual a gente faz na configuração do OSPF. O número do próprio AS, número do AS do remetente, o BGP identify, que nem o Router ID a gente também usa a loopback e autenticação. Para iBGP a gente não usa muito, mas o recurso existe. Para eBGP é recomendadíssimo que se utilize essa chave de autenticação.

E agora a gente vai passar ali pelos estados do vizinho, porque a gente vê muito aluno falando: "Ah, professor, a minha sessão está conectada e não funciona". De fato, conectada ela não funciona, o BGP tem um nome específico que é o estabelecido para dizer que a sessão está ok, e que o BGP vai começar a funcionar. Então ele começa no idle, connect, active, opensent, que que é o estado que começa a esperar resposta. Até então só checagem de TCP. Open confirm, a conexão se estabeleceu e ele começa a trocar as mensagens de keepalive, notificações e a tabela de rota efetivamente começa a popular.

E quando é que o roteador sabe que é eBGP ou iBGP? O roteador sabe pelo número do AS. Então, se os números de AS são iguais é I; se os números de AS são diferentes, é eBGP.

Por que essa informação é importante? Porque o iBGP, por padrão, não são em todos os fabricantes, mas, por padrão, ele tem um peso diferente na rota quando é I e quando é E. Quando é E o padrão é 20, quando é I o padrão é 200. Então isso é bastante importante, porque muitas vezes você pode receber determinado bloco em uma caixa, e quando você fizer transferência para outra por iBGP, esse valor muda e você pode ter um erro de cálculo ali, e você não perceber, que é porque o peso da rota mudou, uma vez que você transitou de um E para o iBGP.

Então, assim, é tranquilo a gente não aprofunda no iBGP, por quê? Porque ele só vai servir como mecanismo de transporte para VRF, para uma necessidade que a VRF tem de fazer esse intercâmbio aí, usando o protocolo BGP. Puppin?

SR. LUIZ COSME PUPPIN MAGALHÃES: Voltei. Me enrolei com o mute, como sempre.

SR. LACIER DA COSTA DIAS JUNIOR: Faz parte.

SR. LUIZ COSME PUPPIN MAGALHÃES: Estamos aprendendo a fazer aulas online, quem sabe um dia a gente aprende.

Sim, exatamente isso, a ideia do BGP não é aprofundar muito, até porque teoricamente quem vai aproveitar bastante esse treinamento já trabalha um pouco com o BGP, porque a gente vai falar de algo avançado, normalmente para provedores de trânsito que vão utilizar essa ferramenta que a gente vai ensinar, que é automatização dos anúncios através de community.

E outra coisa básica que a gente precisa saber, além de noçãozinha básica do BGP é a VRF, que é a L3VPN. Um dos tipos de VPN que o MPLS usa, um dos tipos de serviço que o MPLS usa. E nada mais é do que eu vou fazer com que a minha rede MPLS, toda a minha rede MPLS finja ser um único roteador, em que cada PE da minha rede funcione como se fosse um slot de roteador modular único. É como se eu pegasse um roteador gigante no meio da minha rede, e cada slot fosse um dos meus PEs, e ele colocaria os clientes conectados em cada slot desse aí, com uma controladora única. A VRF finge ser isso, e ela usa o MP-BGP, o iBGP com o MP-BGP, para que as várias VRFs se sincronizem e virem uma única tabela de roteamento.

Se vocês lerem o slide, se vocês observarem, a gente não está lendo o slide, o slide é mais uma base para vocês lerem depois. Vocês vão receber isso aí para vocês. A VRF, ela é uma tabela isolada no roteador aonde ela é criada.

Eu, nos meus treinamentos, eu gosto de dizer que a VRF... a gente finge que VRF é um corpo. E o MP-BGP são as pernas, depois eu entro no BGP e pego as pernas, que são o MP-BGP e grudo nesse Frankenstein, nesse corpo, que é a VRF, e faço com que ela ande pela rede. Andando pela rede ela vai encontrar semelhantes a ela em outros roteadores, ou irmãs clones dela em outros roteadores, e se juntam para formar um único roteador virtual na minha rede inteira.

Simplesmente é essa a sensação que o meu cliente tem. Meu cliente, não importa... Vamos dizer que eu sou um provedor que atendo várias cidades ou vários estados, não importa em qual estado que os meus dois clientes estejam, se os dois estiverem conectados na mesma VRF, a sensação que eles vão ter é que eles estão conectados no mesmo roteador. E é isso que a gente precisa. É isso que facilita a vida do

provedor que vende transporte. Essa noção de roteador único, de tabela única de roteamento no seu backbone inteiro.

Só que, ao mesmo tempo, sem misturar com a sua tabela de roteamento do MP LMPLS, sem misturar com a tabela de roteamento de outros clientes ou outros serviços. Eu posso usar, por exemplo, a VRF de voz e uma VRF de IP, de dados. E aí toda a minha rede de voz vai ficar totalmente segregada da minha tabela de roteamento de dados. Ou seja, alguém via Internet nunca vai conseguir atacar a minha rede de voz. Por quê? Todos os meus clientes de voz estarão em uma VRF isolada, em uma tabela de roteamento isolada, que chegarão em um ponto único, que é a minha central de comutação lá, que é o meu CIP(F) server, o que quer que seja, da minha estrutura de voz, e esse cara está protegido da internet, só tem as conexões que tiver que ter para tráfego de voz. E acabou, o mundo é externo, não sabe da existência dessa rede, ela é isolada. Eu não tenho como pular de uma rede para outra, sem que eu faça uma configuração prévia, que diga que vá ser feita feito esse tipo de ação... vai ser tomada esse tipo de ação.

Como aqui está até em vermelho no slide anterior, a VRF não é uma aplicação para grande porte, porque ela não é escalável. Por que ela não é escalável? Ela é existente apenas naquele roteador em que ela foi configurada.

Ou seja, o que faz com que ela seja escalável, o que faz com que eu tire as limitações de escala que a VRF tem são as implementações de MPLS ou SPF, e do MPBGP em cima do MPLS. Como eu falei, o MPBGP é que faz com que a VRF saia daquele mundinho isolado dela e descubra que, no roteador vizinho, ou no roteador da outra cidade, ou do outro país, existe uma VRF clone dela. E aí elas vão se juntar e sincronizar as tabelas de rota, fingindo ser uma única tabela de rota, tá? Esse é o principal objetivo.

Em uma implementação típica o tratamento das rotas é feito direto no CE. Com a VRF, o tratamento das rotas é divulgado para os PEs, ou seja, se eu não tenho uma VRF, o CE do cliente trata as rotas, e aí eu tenho uma L2VPN até o CE do outro lado. Vamos dizer, eu vendo trânsito para outro provedor e uso a L2VPN. Eu tenho dois provedores aqui em Londrina, que são clientes da minha rede, só que o meu roteador de iBGP fica em São Paulo, e eu vendo trânsito para esses dois provedores, através de L2VPN. Ou seja, os dois provedores de Londrina, se o Lacier tiver em um provedor e eu tiver em outro, nós quisermos fazer uma ligação de Whatsapp de um para o outro, como são dois provedores, mesmo que conectado no mesmo provedor de TIER2, os dois vão lá em São Paulo para descobrir que estão a poucas ruas de distância um do outro. Se o provedor que vende transporte, que vende trânsito, não fizer por L2VPN, fizer por VRF, esses dois clientes, esses dois clientes de provedores diferentes conseguem utilizar a vantagem de que os dois provedores deles estão conectados em um provedor de trânsito com o VRF.

Então, eu saio da minha casa... O pacote sai da minha casa, chega no provedor de trânsito aqui em Londrina, e o roteador dele, em Londrina, sabe que o Lacier está no provedor que também é cliente aqui em Londrina. E a gente faz a comutação aqui, sem preciso ir até São Paulo e voltar.

Você imagina um provedor de porte nacional, um provedor de trânsito, de porte nacional, que tem centralizados os seus BGPs e os provedores clientes têm que ficar saindo da capital onde ele está até uma outra região do país e voltar. E a gente sabe que existem provedores de trânsito no Brasil que fazem isso no Brasil. E a VRF traz uma vantagem absurda no ponto a ponto entre os clientes.

SR. LACIER DA COSTA DIAS JUNIOR: Puppin, e usando a VRF na própria rede do cliente, sem ser transporte, cria o mesmo efeito.

SR. LUIZ COSME PUPPIN MAGALHÃES: Sim, sim, o mesmo efeito, o mesmo efeito. Eu consigo fazer com que o roteamento fique sempre local, eu não preciso ir para o ponto central para descobrir que o cara está do meu lado. Eu tenho uma economia de banda e uma... É o que a gente sempre diz no nosso treinamento, no primeiro dia do nosso treinamento: O cliente compra banda, mas, na verdade, o que ele quer é velocidade.

O cliente compra da gente 100 mega, 200 megabit por segundo, mas, na verdade, o que ele quer é velocidade. Se eu vendo 100 megabit por segundo e eu tenho que fazer com que o cliente rode minha rede inteira, para descobrir que o destino dele está do lado, eu não estou vendendo velocidade, eu estou vendendo banda. Quando eu boto inteligência nessa rede, por exemplo, a VRF é uma inteligência que vai ajudar nesse caso, aí, sim, eu estou vendendo velocidade, porque eu não desperdiço esse tempo de propagação. Por melhor que seja minha rede, eu tenho tempo de propagação. Eu tenho atraso gerado por vários elementos no meio do caminho, que eu posso simplesmente eliminar usando a VRF para otimizar o meu processo de roteamento, dentro da minha rede.

SR. LACIER DA COSTA DIAS JUNIOR: Fora o desperdício computacional, né?

SR. LUIZ COSME PUPPIN MAGALHÃES: Sim.

SR. LACIER DA COSTA DIAS JUNIOR: [ininteligível] infraestrutura, enfileirando pacotes que não precisavam estar passando por ali.

SR. LUIZ COSME PUPPIN MAGALHÃES: Sim, realmente. Outra característica clara é que a rede de backbone pode ser completamente transparente. Aí eu coloco um 'pode ser', porque existe uma configuração que você faz em que a sua rede de backbone pode aparecer para o seu cliente final.

Mas o legal de uma VRF é você não configurar dessa forma. Então, o cliente vai ter a sensação de que ele entrou no roteador, no PE da tua rede e saiu do outro lado, independente de quantos saltos ele deu no meio. Isso é muito interessante que aconteça.

E as rotas de toda a rede serão mantidas através do iBGP. Você vai aprender, via eBGP, as rotas, e vai divulgar por dentro do seu backbone, sincronizar toda sua tabela por iBGP e passar por outro lado essas rotas, fazer os anúncios que forem necessários. Beleza?

Agora, passo aí de novo para o Lacier, para mais um detalhezinho do BGP, que nesse caso a gente vai usar bastante durante o laboratório. Então, é legal que a gente fale também, né, Lacier?

SR. LACIER DA COSTA DIAS JUNIOR: É, nesse laboratório, a gente usa muito, e eu costumo brincar que community é o nível máster do BGP. A galera brinca com os filtros, tal, mas filtro propriamente dito a gente não precisa aprender tantos assim para pilotar um BGP.

SR. LUIZ COSME PUPPIN MAGALHÃES: A inteligência está na community, né?

SR. LACIER DA COSTA DIAS JUNIOR: A inteligência está na community, exatamente. Vamos lá.

A community é um dos atributos que o BGP é capaz aí de caminhar. É um atributo opcional e intransitivo, que são mecanismos de rótulos com objetivo de assegurar a consistência e a política de seleção de rotas. Eu costumo dizer na aula que a community ela é uma espécie de botão, que ele pode ser para a sua equipe, ele pode ser para o cliente utilizar, para o cliente AS, não o cliente doméstico, um cliente AS utilizar. Por quê? Porque eu posso fazer no meu roteador um determinado filtro, e colocar que a ação

desse filtro acontece quando a rota chega com uma community. Por isso que eu brinco que ele é um botão. Por exemplo: Ah, eu tenho PTT São Paulo e o Puppin compra comigo link IPI PTT São Paulo. Só que agora o Puppin se conectou no PTT/SP, ele não precisa mais eu faça o anúncio no PTT São Paulo, mas como ele comprou transporte, ele sabe que minha fila está direta no PTT, ele não quer ficar sem esse recurso. Então, o que que eu posso fazer pra facilitar a minha vida e a do Puppin? Eu crio uma community e digo para ele: Puppin, você me manda seu anúncio de BGP com essa community, porque essa community eu tenho um filtro que diz: Olha, tudo que vier com essa community, não anuncia no PTT. E aí você vai para o link IP tranquilamente. E se um belo dia seu transporte cair, você tiver alguma necessidade de usar o meu PTT, não tem problema. Só você remover essa community que eu já vou automaticamente voltar a te anunciar para o PTT.

Por que isso é bacana? Primeiro porque não precisa ligar 3h da manhã, porque a gente sabe que só acontece coisa maluca nesse horário. Isso não acontece às 10h30 da manhã, com todo mundo no escritório feliz e contente. Isso acontece 3h da manhã com a galera dormindo, suporte dormindo, e frio ainda para completar, e todo mundo enroscadinho na cama, e o cara te liga para resolver uma bucha, e a internet é 24 por 7, você tem que resolver. Então a community é uma maneira de começar a automatizar a tomada de decisão de filtros, isso quando a gente está falando de cliente.

Internamente, você também pode criar várias automações, que é o que a gente vai fazer aqui, para facilitar a sua vida, para você configurar os filtros uma vez e, na ponta, quando você for entrar com o cliente AS novo, você ter menos trabalho para isso se permear pela sua rede, para você saber por onde que ele vai sair, para você não ter que ficar toda hora mexendo em roteadores de missão crítica no seu ambiente, ter uma mão de obra que tem essa capacidade de mexer em roteador de missão crítica o tempo todo.

Entoa, isso basicamente acontece nos roteadores de iBGP, que podem rotular os updates de rota, que entram ou saem, fazendo uma redistribuição. Qualquer roteador iBGP pode filtrar as rotas que entram e que saem, e selecionar as rotas baseadas nessas community. E por padrão, as community são retiradas dos updates de BGP que saem do roteador. Então, na hora que sua rota transita de um [ininteligível] para outro, ele remove essa community, até porque vai que, por um azar do universo, o outro operador pensou no mesmo ID de community para ele. E aí vai ter um big problema de a função do cara lá, ela acontecer porque a community dele deu match com a sua community.

SR. LUIZ COSME PUPPIN MAGALHÃES: E acredite. Eu já fiquei louco com cliente por causa disso. Por acaso a community dele era a mesma do cliente dele. Então, o cliente marcava e deixava passar para ele e fazia as ações que ele não queria que fizesse. Até descobrir foi fácil, né?

SR. LACIER DA COSTA DIAS JUNIOR: E é incrível, porque, assim, existe um padrão, não é? É o número do AS do camarada, dois pontos, o ID que você entende que é o ID relevante para aquela community. Existem IDs clássico como o 666, que é community, que a gente usa como lixo ou black hole. E ela tem uma padronização das communities, você pode seguir ou criar suas próprias, livre. Mas a gente sempre pede que se comece, pelo menos, com o número do seu AS.

E aí uma pergunta que sempre surge: "Poxa, professor, mas tem AS de quatro dígitos, AS de cinco dígitos, AS de seis dígitos". Sim, todos eles suportam o community. O de seis dígitos tem uma particularidade, que a gente chama de extender community, que é uma community que tem um bit a mais, ela tem um dígito a mais, e aí ela não fica junto com as outras communities. Mas todas funcionam perfeitamente bem e de forma muito similar. Só a de seis dígitos que tem um tratamentozinho um pouco diferenciado.

E mostrei a community no-export, que você tem que informar que não é para propagar para outros vizinhos externos aquilo que você está contando naquele BGP. No-peer, não é para propagar no-peer bilateral. Porém, cada operadora tem a sua lista de community, você tem que conversar com o seu operador para ele poder te passar isso.

A gente vai trazer aqui alguns exemplos clássicos de listas de community bem antigas que funcionam até hoje, e a cabeça de lista delas é a Embratel. Eu tive a oportunidade de trabalhar na Embratel. Então é a mesma community até hoje. E é uma lista que eu acho bastante interessante para a gente entender qual é a lógica efetivamente.

Então, por exemplo, se você é cliente Embratel, você faz anúncio na Embratel, e você coloca lá no anúncio community 4230:4, 4230 é AS da Embratel, agora Claro, ele só anuncia aquele... ela só considera aquela rota para dentro da tabela de roteamento da própria Embratel. Então, ela não passa isso para frente.

Se você coloca o 33, 4230:33, ela faz esse efeito aí, e ela manda esse anúncio para quem é cliente Embratel. Então, fica basicamente na rede da Embratel e para os caras que compram o link da Embratel. Se você manda o 32, ela já abre mais, ela manda para os trânsitos nacionais, manda para a rede RNP. Então, por exemplo, você é cliente Embratel tomando um ataque, que a maior parte de ataque vem de um volume de tráfego internacional, se você anunciar para a Embratel para a community 4230:32, esse ataque tende a cessar, porque vai [ininteligível] o trânsito internacional dela. Ela só vai [ininteligível] você para o trânsito nacional dela. Você não vai precisar ligar para ninguém para fazer isso. A community já está lá, é uma community pré-existente. É um botão que você pode apertar sozinho. A 31, ela já aponta você para todo backbone internacional e a 30 conta você para todas conexões que a Embratel tem, que seria o equivalente a você mandar sem community nenhuma.

Então, assim, é bem bacana porque, se você olhar, são várias maneiras de você reagir com seu próprio bloco. A antiga GVT, hoje Vivo, também tem algo bem parecido, só que é o número do seu AS. Então, Ah, eu quero bloquear um anuncio internacional, número do seu AS :1. Eu quero bloquear um anúncio nacional, eu quero bloquear meu anúncio para cliente GVT, eu quero bloquear para [ininteligível] GVT. Eu não quero que a GVT me anuncie em PPP nenhum. Aí é o número do seu AS :6. Aí embaixo está até uma das maneiras de se fazer esse filtro aí.

A gente vai ver obviamente isso na aula prática daqui a pouco. Então, assim, é muito bacana o uso de communities. É muito inteligente, assim, muito gostoso de fazer o mapa de community, como a gente chama, porque isso facilita muito o processo para todos os operadores. A gente deixa assim, a rede muito mais fácil de você fazer.

Então, você pode prever todo tipo de filtro, alimentar o seu roteador com todo tipo de filtro, e colocar 'communityzinha' referente a cada um daqueles filtros, e aí você cria o que a gente chama carinhosamente de operador de community. O cara não é operador de BGP real, ele é operador de community. Ele é um cara que conhece o mapa community, ele sabe que filtro que ele faz para marcar aquela community ali, e pronto, dali para frente, a rede reage sozinha. É um nível de inteligência altíssimo que a gente tem no que tange aí, aos filtros de BGP. Tá?

Então, eu acredito que a parte teórica, o arcabouço aí, teórico, o piso para a gente começar a prática seria esse, né, Puppin?

SR. LUIZ COSME PUPPIN MAGALHÃES: Isso aí. Eu acho que, é claro, nós não falamos aí, tudo que você precisa, você vai precisar ter o SPF rodando, vai precisar ter o MPLS rodando. A gente só falou o que é o protocolo, mas não ensinou como configurar, porque aí são vários fabricantes, diversas formas de fazer.

SR. LACIER DA COSTA DIAS JUNIOR: Muitas horas.

SR. LUIZ COSME PUPPIN MAGALHÃES: Muitas horas. O meu treinamento são três dias para deixar essa rede aí, funcionando, e explicando passo a passo, item a item, com certeza. A nossa intenção era contextualizar um pouco dos protocolos que nós estamos usando.

Basicamente nosso laboratório será esse aí. Nós vamos usar, como tínhamos mencionado, Mikrotik e Huawei simultaneamente. Infelizmente, no EVE e NG, nós teremos que usar o USG 6000, que é firewall da Huawei. Então, as pequenas diferenças que nós observamos no uso do USG 6000, no manualzinho a gente vai mandar para vocês executarem, para que ele fique mais parecido com os roteadores e os switches da CISCO.

SR. LACIER DA COSTA DIAS JUNIOR: O especialista é você, mas, de coração...

SR. LUIZ COSME PUPPIN MAGALHÃES: Não, então, a diferença básica é aquilo que a gente vai ensinar. É liberar a regra de firewall, porque ele é um firewall, então é fazer a liberação da regra de firewall para que as interfaces possam se comunicar. Como ele é um firewall... Igual um Router. Ou seja, nós vamos ensinar--

SR. LACIER DA COSTA DIAS JUNIOR: Cinquenta e sete e qualquer coisa.

SR. LUIZ COSME PUPPIN MAGALHÃES: Isso. A única diferença que vocês vão observar é essa: Nós temos que transformá-lo de firewall em roteador de novo. Ele deixar de funcionar como firewall e passar a funcionar como roteador. A partir do momento que vocês executarem o procedimento que a gente vai mandar, ele vai se comportar como um roteador ou como um switch 6730 que você usaria normalmente. Certo?

SR. LACIER DA COSTA DIAS JUNIOR: Perfeito. Então vamos ao laboratório.

SR. LUIZ COSME PUPPIN MAGALHÃES: Vamos lá. Fala, pessoal! Voltamos agora, já passamos por toda a teoria com vocês, espero que tenham conseguido entender o que a gente estava tentando mostrar para vocês. E vamos para a parte prática, a parte mais interessante do treinamento.

Vamos começar aqui na prática com vocês mostrando o básico de configuração de cada um dos equipamentos. Vocês receberam aí o material, mas, para ficar mais fácil a visualização aqui, nós estamos usando o PE01 e o PE04 como equipamentos Huawei de núcleo, e o BGP02, também com equipamento Huawei. E todos os demais equipamentos são Mikrotik, para mostrar para vocês que essa integração é possível, e que o que nós estamos tentando mostrar para vocês é tão padrão que a gente consegue formar uma rede multi vendor aí sem dor de cabeça nenhuma. Da mesma forma que a gente fez Huawei e Mikrotik, vocês vão conseguir fazer Huawei com qualquer outro fabricante sem dor de cabeça nenhuma, ou Mikrotik com qualquer outro fabricante.

Bom, vou arrastar a tela aqui do PE01. E a intenção é mostrar para vocês a configuração básica desse equipamento.

Display current. Podem ver que eu configurei o MPLS, ativei o protocolo MPLS, disse quem é o identificador. Normalmente a gente coloca loopback. Ativei o protocolo LDP.

Quando nós chegamos lá nas interfaces de backbone, vocês veem que a gente configurou o ponto a ponto, algumas otimizações. O SPF network type peer-to-peer, o SPF LDP Sync, são configurações para que ele faça convergência mais rápido em caso de falha. E ativei o MPLS, e o MPLS e o LDP nas interfaces de backbone.

Podem observar também aqui que o MTU está em 1600. Sempre que você sobe uma rede MPLS, o núcleo dessa rede tem que estar com MTU maior do que 1500. Nesse caso aqui, usamos 1600, porque é o máximo que essa imagem de simulação consegue utilizar, mas a gente sempre recomenda que coloque um valor aí maior, caso você vá passar o L2VPN que precisa de mais espaço de MTU você não tenha dor de cabeça nesse núcleo de rede. Tá bom?

Configuramos aqui as interfaces. Subimos o OSPF e pronto. Se você for olhar, display MPLS, MPLS P(F), ele já está com loopbacks, com as labels criadas para os loopbacks de todos os equipamentos da rede. Beleza? Esse é o básico do MPLS que a gente precisa.

Vou passar agora para o Lacier mostrar para vocês a mesma configuração no Mikrotik, para que o básico do MPLS funcione, e depois, a gente volta para começar a falar sobre a VRF.

Vai lá, Lacier, é contigo.

SR. LACIER DA COSTA DIAS JUNIOR: Valeu, Puppin. E aí, meus queridos? Voltando aqui. Vamos ver como é que a gente consegue interoperar a RouterOS com outras caixas.

Entoa a gente vai acessar aqui o PE3. Então a configuração do MPLS... O laboratório já vai levar para vocês o SPF montado. A configuração do MPLS segue o mesmo rito.

Então a gente tem que ativar o serviço MPLS, a gente sempre usa o identificador LCE(F), o IP da loopback, porque ele é único, e o transporte [ininteligível], a gente usa ele global, aqui em DP settings, que é o IP da lookback. Então a gente não pode confundir que o ID, embora pareça, não é, ele é um identificador. E o transporte [ininteligível] sim, ele é um IP. A gente usa igual por uma formalidade para ficar mais fácil de identificação.

Beleza. Ativamos o serviço, colocamos aqui as interfaces que vão participar do MPLS seguindo aqui as saídas no meu equipamento, Ether 4 e Ether 2, e a própria interface loopback. Ela já informa em LDP [ininteligível] que fechou a vizinhança, com quem que fechou a vizinhança, qual é a identificação de quem fechou a vizinhança conosco. Uma dica fundamental nesse cenário do MPLS é você alterar MTU para evitar a fragmentação. Então, o Mikrotik já vem com 1508, mas o ideal é que você coloque o máximo que a porta suporta, sem causar o efeito que a gente chama de cone. Então você tem um lado do equipamento que suporta 1600, como é o caso da imagem do Huawei que a gente está usando, do outro lado, você também vai ter que pôr 1600, mesmo que outro lado suporte 9000, a gente não recomenda que você crie esse efeito de cone, um lado maior do que o outro, em condição nenhuma.

Então, o menor MTU é o que vai prevalecer. E aí você precisa analisar o equipamento par que está fazendo aquela conexão, porque você pode ter aqui Ether 2G 101 fechado em um valor de MTU, e você pode ter Ether 4 e Ether 2 aqui fechado em outro valor de MTU, não tem problema. O que você não pode é Ether 2 estar em um valor, e a G101 estar em um valor diferente.

Beleza. Configurada a MPLS, a gente agora vai partir para a configuração da nossa querida VRF. A VRF no Mikrotik, ele está dividida em duas partes. Então você tem IP Route, uma aba chamada VRF, aonde você tem a sua instância da VRF criada.

Uma dica importante é o que o nome da VRF [ininteligível] ele é case sensitive. O que eu quero dizer com isso? Esse teste maiúsculo aqui é importante que você sempre detecte que ele é maiúsculo. Em todos os lugares ele vai estar como maiúsculo. Caso você coloque ele como minúsculo em algum lugar, você pode perder... Pode não, você vai perder a sua conexão com a VRF, porque ele vai entender que o T minúsculo é diferente do T maiúsculo.

Uma outra dica também importante é que a gente aqui está usando a interface Ether 3, porque a gente está no laboratório, e a gente tem uma fartura infinita de interface. Mas, no mundo real, normalmente a gente usa VLAN. Por quê? Porque você pode ter uma porta aí de 40 gigas, de 100 gigas... Outros fabricantes, a Mikrotik não tem portas desse tamanho, a maior porta é de 25. Mas você pode ter uma porta de 10 gigas e você estar ligado nessa porta no switch, e você não está passando os 10 gigas para um único cliente. Então você vai usar uma VLAN para fracionar essa porta. Se você colocar essa porta dentro da VRF, ela vai assumir a porta inteira.

Então, a gente dá essa dica da VLAN caso precise fracionar a porta. Caso aquela porta esteja dedicada ao cliente, como a gente fez aqui, não tem problema. Aí você pode, sim, usar a interface física como um todo.

Caso aqui, na frente do nosso PE3, tivesse um switch, tivesse quatro, cinco clientes aqui embaixo, cada um comprando 1 giga, 2 giga, outro 5 giga, se estivesse chegando tudo em uma única porta de dez, você teria que fazer aqui o uso de VLAN, uma vez que você não ia conseguir colocar três clientes em uma porta física porque a VRF travaria isso.

Beleza. Identificação da VRF e a habilidade de importar e exportar a tabela com a mesma identificação, pegando a VRF. Feito isso, você cria uma VRF que a gente chama de VRF light. Ela está estanque, ela só existe dentro desse roteador. Essa VRF, ela não tem pernas, e a gente precisa dar pernas à VRF para que ela possa se deslocar entre os roteadores da rede que possuem a mesma VRF.

E aí vem a outra metade da configuração, Routing BGP, VRF, e aqui é aonde está a instância da VRF... E uma dica importante aqui é: Escolha o nome da VRF, não digita o nome. Porque, se eu digitar teste minúsculo aqui e der um [ininteligível], ele vai aceitar. E isso vai causar um erro na VRF. Então, a gente sempre faz essa observação para você escolher o nome.

E a gente vai redistribuir [ininteligível] distribuir outros BGPs, a gente já vai explicar porque essas opções aqui estão marcadas nesse cenário.

E a última dica é que em peer, você precisa configurar a seção BGP e informar essa seção BGP que ela vai ter a capacidade de transportar a VRF. Como a seção é iBGP, é uma seção mais soft, uma configuração mais tranquila. Então, você tem, por hábito a gente coloca o nome do vizinho, com quem a gente está fechando a seção, o remote ID dele... o remote [ininteligível], perdão, [ininteligível] sempre a loopback dele, porque é a interface que não cai. Então, eu consigo analisar pela tabela do SPF qual é a melhor maneira de chegar a esse remote [ininteligível] para fechar minha seção BGP, e caso meu segundo caminho caia, eu tenho uma segunda opção de caminho, como é o caso do nosso desenho que está em anel, eu vou pelo outro caminho e estabeleço a seção.

O remote AS dele, como é iBGP, os números dos ASs são iguais, o nosso modelo aqui é o 65000, e todo restante da configuração você pode deixar padrão, não vai ter problema.

O único detalhe que você não pode esquecer de forma, maneira ou circunstância é de habilitar o VPN4, que é o mesmo objetivo do que o Puppin colocou lá para a gente, que é a VPN instance. Então, esse VPN4 aqui, se você não marcar ele, você não vai dar condição dessa seção BGP divulgar a VRF. E o update source também a gente sempre recomenda que você use a loopback para fechar a instância, porque caso você use uma interface, ou não informe nada, ele vai escolher à revelia, ele pode escolher uma interface, e essa interface [ininteligível] seção BGP vai ficar prejudicada.

Então essas são as dicas de configuração para a gente começar a estabelecer a seção e criar as pernas ali da VRF, para a gente poder analisar como vai se comportar esse cenário com os clientes entrando agora, começando pelo Huawei, com o Puppin. Vai lá, Puppinzinho.

SR. LUIZ COSME PUPPIN MAGALHÃES: Bom, já que ele mostrou a parte da VRF em Mikrotik, vamos mostrar agora a mesma configuração em Huawei, como que eu faço essa configuração. E vamos alfinetar um pouquinho o Lacier. Vocês vão ver que é mais fácil do que no Mikrotik. Então vamos lá.

Display current. Lembra que eu tenho que criar a VRF aqui, VPN instance, teste. Aquele nome maiúsculo, minúsculos da VPN, ela tem relevância local. Então, eu tenho que sempre observar se eu criei a VPN com teste minúsculo, toda vez que quiser fazer referência a ela no meu roteador, eu tenho que fazer referência com teste minúsculo. Se eu criei com teste, o T inicial maiúsculo, toda vez tem que falar... fazer a referência com o T maiúsculo dessa VRF, mas ela tem relevância local. O que identifica a VPN instance na rede, como um todo, é o identificador que é Route target, o VPN target nesse caso aqui, que é 100:100. Vocês viram que lá no Mikrotik está 100:100 e no Huawei também. E isso é que vai fazer com que o Huawei e o Mikrotik falem um para o outro que estão com a mesma VRF. Tá? O Route distinguish, que é community de RD, que ele vai marcar na rota também. Normalmente eu coloco a loopback : e o ID da VRF, e isso é que vai fazer com que quando a rota chega no roteador, eu consiga identificar quem foi que injetou essa rota na tabela.

Criada a VPN instance, como o Lacier mesmo falou, essa VPN, ela fica presa no roteador, ela não sai daqui. O que eu preciso fazer agora? Eu preciso criar as pernas dessa VPN. Eu preciso que ela ande pela rede e ela descubra que, em outros equipamentos, ela tem uma parceira, uma VPN igual, para sincronizar a tabela.

Então, eu tenho que subir o BGP. Naquele caso o Lacier mostrou para vocês o PE03, que é um PE normal da rede, e eu estou no PE01 que é PE que a gente elegeu como route reflector. Se vocês observaram lá no PE03, ele tem seção com o 1 e com o 2 apenas, no caso do PE01, como é route reflector, ele tem seção com todos os demais, e aqui o conecte interface, mostrando para vocês que eu tem que marcar qual é a interface de conexão do BGP, que é loopback. Outro detalhe, como ele é o route reflector, cada cliente de reflexão, eu tenho que marcar o comando reflect client. Ou seja, estou autorizando esse roteador de BGP refletir as rotas para os demais. Toda rota que ele aprende do PE03, ele reflete para o 2 e para o 4, e assim por diante.

Uma outra coisa, nós vamos trabalhar com community. E como o Lacier, quando explicou para vocês community, lá na teoria, ele disse que é um parâmetro, é um atributo que não é enviado por padrão, no anúncio BGP. Na Huawei, eu preciso colocar o comando autorizando ele a encaminhar essa community para frente, que é esse comandado advertise community.

Outra coisa que eu preciso fazer: fechei a seção de BGP, eu ativo as pernas da VRF. Ou seja, eu faço com que o meu BGP fale a extensão MPBGP, que é o VPNV4. Essa extensão é que vai fazer com que a VRF de um roteador encontre a VRF do outro e faça com que a sua rede inteira se comporte como se fosse um grande roteador virtual único.

Criei as pernas, o que que eu preciso fazer? Pegar a minha VRF e espetar as pernas na minha VRF. Montei o Frankenstein. Aqui são as pernas da VRF e aqui é o corpo da VRF. Espetei o corpo nas pernas, ela vai sair andando. Isso tudo dentro da BGP. Se vocês olharem, eu estou dentro do BGP aqui. Coloquei a VPN dentro dele, mandei importar as rotas diretas e a rotas estáticas. Esses peers aqui daqui a pouquinho a gente vai mostrar para vocês.

Então, só revisando, nesse processo todo aqui, a gente criou a VPN, subindo aqui, nós criamos a VPN instance. Nós criamos as pernas para VPN instance e nós colocamos as pernas para que ela ande pela rede e sincronize com as vizinhas.

Então, beleza, minha rede MPLS está pronta, meu provedor com VRF está pronto, o serviço está no ar, mas, por enquanto, não tem ninguém dentro desse serviço.

Vamos colocar o primeiro cliente dentro desse serviço. Vamos aprovisionar o primeiro cliente. Como é que eu faço aprovisionamento de um cliente em VRF? Vamos lá olhar. No nosso diagrama eu tenho o cliente 1 conectado ao PE4. Certo? Vamos abrir aqui o PE4 e mostrar para vocês, display current configuration BGP. Mostrando para vocês que a VPNV4 já está aqui, as pernas já estão aqui, a VPN instance já está aqui. E o que eu preciso para provisionar um cliente? Primeira coisa que a gente faz é colocar o IP que a gente deu para o cara, para o ponto a ponto dele, na nossa interface. Aqui está o primeiro passo, display current interface. Eu dei para o nosso cliente a interface giga 102, como vocês podem olhar no nosso diagrama, a giga 102.

Qual é a diferença que eu tenho nessa giga 102, além de simplesmente colocar o IP que eu dei para o ponto a ponto? Eu tenho que colocar o IP binding VPN instance teste. O que seria isso? Eu estou plugando o cabo da interface giga através de um cabo virtual, nesse roteador virtual. Eu estou fazendo com que essa interface deixe de pertencer ao roteador principal e passe a pertencer à VPN instance.

Até aí tudo bem. Fechei. Vamos fechar a seção de BGP com o nosso cliente. Qual o IP que o nosso cliente vai usar para fechar o BGP com a gente? 192021. Tá? Que é o IP do meu lado da interface. Vamos olhar o nosso BGP, display current confirme BGP. Dentro da IPV4 family VPN instance teste eu fecho o peer com o meu cliente.

Ou seja, não fecho no meu BGP principal. Eu fecho no meu BGP da VPN instance essa seção. O que vai acontecer? Deixa eu abrir aqui esse Mikrotik, que é o cliente 01, para mostrar para vocês. Vem aqui em routing BGP, você vê que ele fechou a seção com o meu AS? 6500, o meu AS, e, em networks, ele fez o anúncio das rotas dele, beleza?

Como ele fez o anúncio das rotas dele, eu posso, no meu PE, vou criar uma route policy. Display current conf route policy. O que estou configurando nessa route policy aqui? Eu estou falando que, se eu der match no prefixo dele, eu vou aplicar as communities 65000100, 65000200, 65000300. Essas são as communities do nosso plano de community que a gente vai mostrar para vocês funcionando, daqui a pouquinho. Mas a intenção aqui é mostrar que o cliente não precisa marcar nada, só precisa nos anunciar. E, no PE, eu faço a route policy, dizendo o que eu quero marcar de community para ele.

Agora o Lacier vem aqui mostrar pra vocês o aprovisionamento do cliente no Mikrotik, e vai mostrar para vocês um pouco do funcionamento dessas communities, depois eu mostro no Huawei também o resultado para vocês.

SR. LACIER DA COSTA DIAS JUNIOR: Vamos lá, meus queridos.

Essa interoperabilidade dos fabricantes é uma coisa que me deixa muito feliz.

Então, vamos acessar o nosso PE3. Novamente. Cliente 2 está conectado lá na Ether 3 do PE3, como a gente tem aqui no nosso diagrama.

Então, para estabelecer um cliente BGP, route BGP, e aí eu tenho uma seção BGP com meu cliente 65200. A consideração dessa seção BGP é que eu preciso de uma outra instância, que eu batizei ela como VRF. Por que eu preciso dessa outra instância? Porque essa outra instância de BGP, ela vai escrever na minha tabela routing table teste. Que é a tabela da minha VRF, que você poderia ter colocado Internet, poderia colocar o nome que você achar mais pertinente.

Beleza. Feito isso, eu tenho um peer no qual a instância é a minha instância que eu batizei como VRF. Por quê? Porque eu quero que essa seção BGP escreva o que o cliente me contar, dentro da seção.

E o procedimento normal é em routing filter. Faço o filtro [ininteligível] tradicional, que é o bloco que o Registro.br deu para o cliente, de 21 a 24, que é o maior bloco que ele pode me mandar é o /21 e o menor é o/24. Action accept. A gente marca as communities que a gente acha pertinente de saída. Então a gente marcou 100, 200 e 300, que é nossa BGP 1, nossa BGP 2, nossas CDNs. Eu poderia, dentro das communities, ter ali a 301, 302, 303. Vamos supor que eu tivesse Google, Netflix e Facebook, e o cliente quisesse só o Facebook como CDN. Então, eu não usaria 300, eu usaria, por exemplo, a 301, e a 300 ficaria caso ele quisesse usar as três CDNs. Então eu posso montar um mapa de community de acordo com a minha necessidade. Eu podia ter no meu BGP 2, duas operadoras, eu fazer 201, 202, se mandasse 200, sairia pelas duas operadoras que estão no meu BGP 2; se eu mandasse 201, sairia pela operadora que está no meu BGP 2 e eu considero ela como operadora 1, ou 202, que eu sairia pela minha segunda operadora do meu BGP 2.

Então, esse mapa de community é que é o pulo do gato. Por quê? Porque você tem uma figura cara dentro do provedor, que é o operador de BGP. Só que você pode ter uma figura um pouco mais barata, que é um operador de community. O cara que não mexe nas suas caixas de cima, é o cara que só mexe no seu PE, ele mexe onde está entrando o cliente. E o Mikrotik tem uma particularidade que você tem que fazer [ininteligível] freio. Então, eu tenho mesma regra, com o mesmo nomezinho, AS-6502020-in, e eu tenho um descarte. Por quê? Porque o padrão do Mikrotik é accept, o padrão do Huawei e outros fabricantes é drop, então eu tenho que fazer uma regra de freio.

E aqui eu fiz regrinha de out(F), dizendo que vou contar a minha tabelinha para ele, uma regra de accept, só para ficar preenchido o campo lá como o exemplo do mundo real.

Beleza. Feito isso, a minha seção vai estabelecer, porque o cliente, creio em Deus, que ele já fez a metade dele, e eu vou receber aqui a tabela desse cliente.

Então eu recebi essa tabela aqui do meu cliente. Posso dar um detail na frente do [ininteligível]. E ele vai e mostrar que recebi e eu já estou marcando aqui as communities de entrada, para que isso se popularize dentro da minha estrutura.

E eu vou passar para nosso querido Puppin, para ele também mostrar para vocês como que essa mágica acontece [ininteligível]. Vai lá, Puppin.

SR. LUIZ COSME PUPPIN MAGALHÃES: Deixa eu arrastar de volta a tela aqui. Essa dinâmica de compartilhar computador com o Lacier nem sempre é nosso dia a dia, né?

Então vamos lá. Display [ininteligível] a tabela da minha VRF. Agora que eu já estou... Eu estou no PE4, o PE4 está conectado ao cliente 1, mas eu disse que a VRF, ela é sincronizada entre todos os PEs. Então o cliente 1 está injetando na VRF a tabela dele, e eu estou marcando as communities como eu mostrei. O cliente 2, que está conectado lá no Mikrotik, no PE3, ele também está injetando as rotas dele.

Então, no Huawei, como é que eu vejo essa tabela de rota? Eu vou colocar o display IP routing-table VPN instance teste. Aqui eu vejo somente a tabela de roteamento de teste da VRF teste.

Vocês podem olhar que o cliente 1 e o cliente 2 estão aparecendo. Se você observar, o IP de next holp das rotas que o cliente 1 está anunciando é o IP dele, e na minha tabela aparecem as rotas do cliente 2 apontando para um loopback do roteador PE3. Por quê? A VRF é uma VPN de camada 3. Então, eu tenho um túnel do meu PE2... do meu PE4 com o meu PE3, para que os pacotes encaminhados diretamente para esse cliente não precisem ficar rodando pela minha rede.

E como que eu vejo a community? Olhar o detalhe da rota, display BGP VPNV4, VPN instance, teste, routing-table. Vê toda tabela de rota do meu roteador, da tabela, da VRF teste, e eu quero ver especificamente uma rota para olhar os detalhes dessa rota, para ver o que que está sendo anunciado. Coloco lá o IP e a máscara, eu vejo aqui que eu recebi do meu PE4... do meu PE3 o anúncio que o cliente mandou, e o PE3 marcou essas communities.

O que é isso vai fazer para a gente? O que é isso vai ser útil para a gente? A gente vai chegar lá no BGP 2, ou seja, o BGP 2, que é um cliente da minha rede MPLS... Aqui uma observação interessante, os meus roteadores de BGP de borda, meu roteador de CDN, ele é tão cliente da minha VRF quanto os meus clientes propriamente ditos.

O meu BGP, ele não participa da minha rede MPLS. Minha rede MPLS é o núcleo de transporte da minha rede. A minha rede MPLS, ela transporta os pacotes e transporta os serviços. Os meus serviços têm os equipamentos que os fornecem, que são conectados como clientes desse serviço de transporte.

Então, eu chego lá no meu BGP2, vou mostrá-lo aqui para vocês. Quando eu dou o display IP routing-table nele, ele está recebendo todas as rotas da minha VRF.

Pode olhar que, no display IP routing-table dele não tem aquele 1099991 que é loopback do meu MPLS. Não tem nada referente ao meu MPLS. Só tem referente à minha VRF.

Se você der um display current, no meu BGP, pode olhar tranquilamente, não existe nenhuma configuração de VRF, não existe nenhuma configuração de MPLS, não existe nada. Ele tem um BGP fechado com a minha VRF, da mesma forma que eu teria se eu fosse um cliente de outro AS. Tá bom? Ah, eu tenho aquele meu roteador de PPPoE. Ele é cliente da minha VRF. Ele pode nem fechar BGP com a minha VRF, mas ele vai ser um cliente da minha VRF e vai receber as rotas e anunciar as rotas dele.

Aqui, para exemplificar para vocês melhor, a gente fez uma route-policy, e eu fiz um community filter. Esse aqui é o BGP02. Eu fiz o community filter dizendo que ele só irá receber as rotas que forem marcadas com a community 65000:200, e fiz a route policy dizendo para aceitar se der match na community. Correto?

No Huawei, se eu dou um node 10 de permit e não tenho nada depois, o que não der match nesse permit vai ser negado, ele tem um deny implícito, como o Lacier falou. Na Mikrotik o permit é implícito, você tem que criar uma regra de bloqueio no final, para ele parar. No Huawei o deny é implícito. Então você não precisa criar nada além do permit que você quer.

Então se eu olhar aqui, eu estou aceitando as rotas que estão com essa community 65200 marcada. Vamos mostrar um pouco da automação. Vou mostrar para vocês novamente o display IP routing. Eu recebi as rotas do cliente 2 e as rotas do cliente 1.

Vamos mostrar como que vai funcionar aquele operador de community que o Lacier chamou, o operador de BGP que não precisa saber quase nada de BGP, basta que ele saiba ativar ou desativar community. Está vendo que aqui no PE04, display current conf route policy, eu marquei todas essas communities no recebimento do meu cliente, eu entro aqui, vamos dizer, agora eu sou operador de community. O cliente ligou para mim e falou assim: "Olha, eu não quero mais sair pela operadora 02 sua, ela está me dando problema, eu quero que você me coloque para sair só pela operadora 01". Se você não tivesse isso aqui, essas communities marcadas, o teu operador de BGP teria que entrar no seu roteador de borda e alterar a apólice desse cliente lá no teu roteador de borda. Quanto mais se mexe no equipamento, mais é possível gerar problema nesse equipamento.

Então, dessa forma aqui, eu vou lá no PE mais perto do cliente, ou seja, se eu fizer qualquer besteira nesse roteador, eu vou afetar somente os clientes daquele PE, eu já não afeto 100% da minha rede. E chego na route-policy dele e coloco a apply community 100, tiro o 200 e deixo o 300. Se você olhar display list(F), ele está com 100 e o 300. Se nós formos agora no BGP02, ele tem que esperar um pouquinho. Vamos olhar como que está a rota. Display BGP routing-table. A rota que a gente anunciou. Está sem a community. Então vamos ver por que não funcionou. Display current conf route-policy também. Estou permitindo, se der o match no community filter.

Está no sentido errado. Eu tenho que vir aqui. Está configurado no peer errado, no sentido errado. Então, a gente vem aqui, coloca no peer da VRF a route-policy no sentido import. Vamos ver agora se ele sumiu. Ele desapareceu. Então, treinamento às vezes a gente comete erro no sentido da policy, mas está aí. Consegui mostrar para vocês que se eu tiver sem a community marcada, com a policy correta, aqui eu só tenho os anúncios de quem está com a community 652:200, 65000:200 marcado aqui. O Lacier vai mostrar agora como que seria essa automação lá no Mikrotik, como é que esse operador de community conseguiria fazer isso no Mikrotik, e mostrar também que, instantaneamente, ele desaparece essa rota lá da tabela.

Vai lá, Lacier, é contigo.

SR. LACIER DA COSTA DIAS JUNIOR: Vamos lá, meus queridos. Eu gosto assim, chute real time.

SR. LUIZ COSME PUPPIN MAGALHÃES: Se desse tudo certo.

SR. LACIER DA COSTA DIAS JUNIOR: Não teria emoção. Não teria emoção.

SR. LUIZ COSME PUPPIN MAGALHÃES: Não teria.

SR. LACIER DA COSTA DIAS JUNIOR: Então vamos pular aqui para o meu PE2. beleza.

Então, aqui, como eu mostrei para vocês, a gente já vai ter o filtro, que eu recebo e marco as communities, e em route eu já tenho aqui os IPS que eu recebi na minha seção que meu cliente me mandou. Nessa faixa prevista aqui 19819, já recebi aqui os IP, e já coloquei as communities.

Tenho aqui a minha seção BGP com a minha operadora. Mesmo cenário. Eu tenho que ter duas seções. Uma dentro da instância teste, para que eu possa pegar o que eu aprendi dentro da tabela e contar. Por quê? Porque a tabela está perdida por dentro da VRF, e eu vou pegar aqui, redistribuir outros BGPs. Uma vez que aqui em IP route eu recebo já com a tag teste que é a tag da minha VRF.

Então, eu tenho que ter esse cuidado de abrir, vamos dizer assim, a VRF para que eu possa pegar esses IPs e fazer um anúncio para minha caixa de BGP.

Lá na minha caixa de BGP, uma vez feito esses anúncios, meu peer fechado, meu peer fechado com outras caixas, minha loopback, minha VPN 4, tudo certinho, como a gente mostrou no outro módulo de configuração, a gente vai ter que Route BGP a nossa seção com o AS nosso, fechando a seção, e in route filter, eu vou ter meu filtro de in, informando que eu recebo nessa caixa a community 6500100.

Então, não adianta eu achar que eu vou receber o meu cliente 19819, aqui, se eu não vier aqui no PE3 e, na hora que eu receber, eu não marcar a community 100.

Vou colocar aqui os dois na tela. Esse mouse gamer do Puppin, de 600 botões, tem que ser um polvo para usar.

Então, olha. Tirei a community 100 do meu anúncio. Na hora, o meu BGP para de receber esse anúncio. Então, se o cliente, como o Puppin bem colocou, se o seu operador de community não quiser que o BGP 1 receba esse anúncio, é só ele suprimir a community 65000:100. Caso ele queira, é só ele colocar aqui automaticamente a caixa BGP1 recebe o anúncio e propaga esse anúncio para frente.

Então, você tem aí essa condição de fazer esse tipo de cenário operar com qualquer montagem que você precise. Por exemplo, eu tenho aqui a CDN. Na caixa da CDN, nós criamos um exemplo, como se a gente tivesse FNA, GGC e OCA, e nos filtros, mesma coisa. Então aqui eu tenho a community 65300, IP Route. Minha tabela. Bem bonitinha. Com a community 65300. Recebendo o meu bloco.

E aí, novamente, eu consigo vir no meu PE03, e, facilmente, excluir esse - vamos aumentar um pouquinho aqui o zoom, para a galera que usa óculos, que nem a minha pessoa e o Puppin, enxergar bem - eu consigo novamente vir aqui em filter e dizer: Olha, não, esse cara não tem mais CDN. E, automaticamente... Gosto assim. 65300...

E se você fizer o filtro e não aplicar o filtro, acontece isso, né, meu querido? Não é só fazer o filtro. Você precisa aplicar o filtro.

Então, olha, subiu a seção. O que não vem com a community 300 marcada, não vai entrar na tabela.

Quando você marca a community 300, ela volta para a tabela. Por quê? Porque a community 300 veio habilitada.

Então, é esse tipo de automação, esse facilitador, que a gente gostaria de mostrar pra vocês. Porque você consegue, não só baratear o custo operacional da rede, mas você também consegue blindar a sua rede, porque a VRF traz essa camada de blindagem para o seu ambiente. Traz essa automação, e traz uma lista enorme de benefícios para que você tenha uma capacidade de gestão mais simples do seu provedor.

Uma vez que montado esse mapa de community associado às VRFs, você vai ter uma oportunidade, vamos dizer assim, de ter um operador mais barato, uma vez que, como o Puppin colocou maravilhosamente

bem, ele só vai mexer no seu PE. E uma vez que só mexe no seu PE, ele só tem a chance de derrubar aquele PE, caso ele venha a errar alguma instrução. Beleza, Puppin?

SR. LUIZ COSME PUPPIN MAGALHÃES: Acho que a gente conseguiu mostrar qual era o nosso objetivo, mostrar para vocês que é possível, primeiro, que é possível operar uma rede com VRF, com multi vendor, sem a necessidade de ficar todo mundo preso no fabricante. E outro objetivo era mostrar que a automação desses anúncios é possível, a facilidade e a simplicidade no aprovisionamento de um novo cliente é possível quando a gente usa community com VRF.

SR. LACIER DA COSTA DIAS JUNIOR: Eu ouso dizer que é estado da arte aí, porque a gente mostrou VRF com automação de BGP. Você pode colocar o PPPoE por dentro da VRF, você pode usar outros recursos dentro da VRF, [ininteligível] separando a camada de gestão da rede, da camada de serviço.

Então, é esse material aí, com muito carinho, que a gente queria dividir com vocês. Agradecer o pessoal do NIC pelo convite, pela oportunidade de a gente estar dividindo esse conhecimento com vocês. Espero que vocês gostem. E, ao final dessa gravação, a gente vai estar disponível para perguntas, dúvidas, anseios e angústias que possam vir a surgir. Muito obrigado a todos aí.

SR. LUIZ COSME PUPPIN MAGALHÃES: Estamos aí online, agora, a partir de agora, para tirar dúvidas de vocês, esperando que vocês tenham conseguido aproveitar bastante esse conteúdo. Muito obrigado.

SR. LACIER DA COSTA DIAS JUNIOR: Obrigado, pessoal, um abraço.

SR. LUIZ COSME PUPPIN MAGALHÃES: Um abraço.

SR. EDUARDO BARASAL MORALES: Não, excelente isso. Muito obrigado Lacier. Muito obrigado, Puppin. Gostei muito do que vocês apresentaram para os nossos alunos.

Só não sei se ficou muito boa essa máscara do lado negro da força, falando de Mikrotik e Huawei, mas vocês que escolheram. Fiquem à vontade.

Bom, antes da gente ir para a parte de perguntas, pessoal, eu gostaria de pedir um favor para vocês preencherem o formulário de avaliação. A gente vai colocar agora na tela um QR Code, e um link aí no chat, relacionado ao formulário de avaliação. Não é o formulário do certificado. É um formulário para você dizer se você gostou da live, o que a gente pode melhorar. Então, preencha. São duas perguntinhas, coisas simples. Vamos colocar aí o QR Code, é só dizer ali uma nota de zero a dez do que você gostou da live e o que a gente pode melhorar.

Então, por favor, aí, preencham esse formulário, é muito importante para a gente saber se a gente precisa melhorar alguma coisa para as próximas edições.

E também vou pedir aí para o pessoal do NIC.br que está no chat, colar também o link do certificado. Lembrando que até 2h da tarde vai estar ali possível fazer o certificado, vai poder conseguir o certificado. Basta se inscrever até as 2h e aí você vai ter o certificado dessa live.

Bom, sem mais demoras até porque a gente não tem muito tempo, esse vídeo foi pouquinho grandinho, mas a gente vai tentar atender o público que mandou as dúvidas no chat. Se bem, pelo que eu acompanhei, o Lacier e o Luiz escreveram um monte ali no chat. Já responderam um monte de coisa aí, que vocês mandaram, então foi excelente.

Mas vamos lá. Pegando ali pergunta do Amir Alves de Paiva: "Lacier Dias, uma pergunta para iBGP, como boas práticas eu poderia estar usando uma loopback para garantir esse roteamento, caso tenha mais de um caminho?". Então, Lacier, fica à vontade?

SR. LACIER DA COSTA DIAS JUNIOR: E aí, meus queridos? Pessoal, sendo bem direto aí na resposta, deixar os agradecimentos para depois, essa questão do uso da loopback, ela é de extrema importância não só para o BGP, mas para o SPF, para todo o cenário da estrutura, para você não atrelar a interface física ao protocolo.

Porque aí você tem desconexão dessa interface, rompimento de fibra, ou a desconexão mecânica, alguém vai lá e tira o cabo, o protocolo vai ter que recalcular, traçar toda uma estratégia na sua estrutura, vai ter que recalcular [ininteligível] SPF, BRBDR, se for BGP, vai ter que restabelecer a seção. E quando você está preso a uma loopback, essa interface só vai cair se você der o comando, se o roteador sair da tomada. E aí essa será a sua menor preocupação, se ele sair da tomada. Então sempre atrele os protocolos à uma loopback, para você não ter problemas.

SRA. ANDREA ERINA KOMO: Oi, pessoal, tudo bem? Obrigada, Lacier.

Como o Eduardo falou, o tempo está curto. Passar já para próxima pergunta, que eu peguei uma pergunta aqui do Fernando. Colocou: "Hoje eu trabalho com BGP direto e nos concentradores. Ou seja, os concentradores não falam direto somente através do BGP. Se eu ativar o MPLS eu ganho alguma performance na rede?". Puppin gostaria de falar, por favor, alguma coisa?

SR. LUIZ COSME PUPPIN MAGALHÃES: Bom, eu gosto de, no início do meu treinamento de MPLS, falar que o MPLS não serve para todo mundo, e alguns dos alunos terminam o meu treinamento, terceiro dia do meu treinamento com a certeza absoluta de que ele passou três dias aprendendo MPLS e que não vai usar o MPLS na rede dele.

Então, a resposta para essa pergunta, a gente até colocou no chat, na hora que ele fez essa pergunta. Eu preciso conhecer o ambiente dele. Nem todo mundo tem benefício com MPLS. Algumas pessoas podem ter alguma complexidade a mais na rede desnecessária, porque tudo depende do tamanho da rede dele, do tipo de serviço que ele vai trabalhar.

Então, a gente precisa conhecer o cenário, olhar o desenho dele, conhecer o que que ele vende, porque eu já tive cliente com 35 mil assinantes, que a rede dele era desenhada de uma forma que o MPLS só vai trazer complexidade, não vai trazer benefícios para você. Então, depende muito. A gente precisa conhecer o cenário.

SR. EDUARDO BARASAL MORALES: Muito bom falar isso, porque realmente cada cenário exige uma coisa diferente, e precisa se ter um estudo, não basta, assim, querer uma fórmula mágica para todos os casos. Não dá!

Bom, seguindo as perguntas, vem uma do Edson, da Cefet do Paraná: "Os palestrantes poderiam comentar as vantagens, serviços para [ininteligível] implementar em MPLS VPN oportunidades de vender novos serviços na sua rede? Obviamente a viabilidade depende de SP para SP". Então queria que o Lacier comentasse pouquinho sobre isso.

SR. LACIER DA COSTA DIAS JUNIOR: Então, pessoal, essa questão de serviço sobre MPLS, ela é de suma importância. Por quê? A gente falou aí de VPN L3, mas existe também em cima do MPLS o PWE3, que seria o L2 connect ou o L2 VPN. Precisamos aí transportar fio a fio de forma transparente o tráfego.

Então, quando você coloca o MPLS, você não traz(F) só uma camada de serviço, você traz(F) uma camada de segurança na rede, que você consegue separar serviço de gerência.

Eu acho que esse é um dos pontos que eu vejo como mais importante, mesmo para o pequeno provedor. Mesmo o cara falando: Não, sou só, que eu chamo carinhosamente de picotador de link. Eu pego o link por ataco, picoto e entrego ele para os meus assinantes. Não faço mais absolutamente nada. Mal atendo empresa, quando atendo empresa, atendo igualzinho usuário doméstico. Quanto mais seu provedor Top de linha, com equipamento de primeira linha, e com OMUs, e rede ótica, etc., etc., você tem um nono serviço.

Pô, Lacier, mesmo assim eu preciso da VRF? Precisa, porque ela vai te trazer uma camada de segurança que nenhuma outra situação vai te colocar de forma tão confortável, e é separar os seus serviços, ou seu único serviço, da camada de gerência na rede.

Então, você vai ter, além disso, a oportunidade de novos negócios: Ah, preciso ligar os semáforos. Uma VRF para os semáforos. Ah, eu preciso entregar... preciso [ininteligível] uma empresa de câmera. Então, todos esses serviços você pode separar cada um [ininteligível] VRF. E dependendo da natureza do serviço, você vai usar um L2 connect, que também é um serviço solto na rede MPLS.

Então eu recomendo extremamente que você use e abuse dos recursos do MPLS, até porque na maioria dos roteadores a licença já está lá, já está paga. Você só não usa se você não quiser.

SRA. ANDREA ERINA KOMO: Obrigado, Lacier. Então, vejamos aqui a próxima pergunta. Tem aqui uma pergunta do Silvio Rezende: "MPLS VMAN são parecidos?". Puppin, gostaria de comentar sobre? Por favor.

SR. LUIZ COSME PUPPIN MAGALHÃES: Bom, a VMAN é o antecessor do MPLS em si. A VMAN, era como os provedores de rendimento utilizavam e prestavam os serviços de links. O MPLS, ele veio para melhorar isso. E quando eu uso o VMAN, eu tenho que utilizar protocolos de proteção de anel. E como o nome já diz, proteção de anel, eu [Ininteligível] anel sendo utilizado, o outro ficava ocioso, ou eu tinha que ficar criando balanceamento, dois anéis, um em cima do outro. E o MPLS, ele veio para que eu pudesse ter múltiplos caminhos, utilizando a inteligência do roteamento da camada três para proteção desses loops.

Então eu entendo que a VMAN, ela é um legado, que o MPLS veio para substituir, e assim como a gente já tem visto várias perguntas aí sobre VXLAN, segment routing. O segment routing, a VXLAN e o EVPN está vindo para substituir o MPLS. O MPLS é protocolo de 97, com certeza tem suas deficiências, e a evolução dele são os novos protocolos que estão surgindo, que o pessoal já está fazendo laboratório, alguns já estão utilizando, que são EVPN, VXLAN e o segment routing.

SR. EDUARDO BARASAL MORALES: Muito bom, Puppin. Até porque você já faz o gancho com a nossa apresentação amanhã, que é sobre EVPN.

Então quem quiser saber um pouquinho mais sobre o que o Puppin falou, amanhã a gente vai ter uma outra live. O último dia da semana de capacitação, e é sobre esse assunto de EVPN.

Mas isso é pra amanhã. Vamos voltar aqui para as perguntas, que tem muita gente querendo tirar dúvida. Então, Lacier, o Luciano 3 aqui: "Nas brincadeiras aqui, com MPLS e VRF, tudo lindo. Porém, fiquei na

dúvida com IPV6. Pelo fato de não ter VRF, está correto usar VPLS e um OSPF nessas pontas para trocar em roteamento IPV6?".

SR. LACIER DA COSTA DIAS JUNIOR: Então, existe a VRF sim, para IPV6. A Mikrotik, infelizmente, ainda não terminou a implementação desse recurso. E aí, como uma alternativa, até porque você não precisa, necessariamente, algumas topologias, ter o IPV6 dentro do backbone, a gente usa uma técnica de transporte chamada PWE3. Então você vai ter o BGP com IPV6, você vai ter o backbone todo transparente, sendo transportado [ininteligível]. E lá no PPPoE você vai ter o IPV6 de novo. Então você tem uma conexão entre o BGP e o PPPoE direta, só tem IPV6 nesses dois equipamentos, e na CPE dos clientes, sendo entregue já na residência do assinante.

E aí o seu backbone todo, no meio do caminho, fica transparente para o IPV6, você não enxerga esse caminho, porque ele está passando dentro desse túnel, PWE3. Então um recurso, uma maneira de projetar a rede que a gente utiliza, principalmente no começo da implantação do IPV6, quando o operador ainda não está com toda a equipe treinada, ou a equipe toda ainda está com um pouco de medo de IPV6, onde ele pode ter algumas dúvidas, a gente usa essa técnica para implantar o IPV6 no mínimo de equipamento possível, para poder chegar o IPV6 no assinante. Então, fica o BGP transportado via PWE3, PPPoE, CPE do cliente.

Assim você consegue subir o seu V6 sem necessariamente precisar de VPN L3V6 no primeiro momento. Obviamente, se você já tem uma caixa que suporta isso, recomendadíssimo que você já suba IPV6 no backbone todo, e já descubra o maravilhoso mundo do IPV6.

SRA. ANDREA ERINA KOMO: Obrigada, Lacier. Então, como ele reforçou, pessoal, vamos trabalhar com IPV6, a gente reforça isso bastante com os nossos cursos aqui do NIC.

Mas seguindo para a próxima pergunta aqui. Tem pergunta do Evandro Nascimento: "Quais seriam as principais vulnerabilidades atuais do protocolo MPLS? E qual o impacto nas redes das operadoras?".

Aí eu aproveito também, já o gancho aqui com a pergunta do Lucas de Souza: "Sou uma rede educacional e não tenho um provedor. Existe alguma vantagem colocar MPLS na minha rede?". Então, aí, o fato da rede da operadora e uma rede, aí, no caso de uma instituição de ensino. Puppin, gostaria de comentar sobre, por favor?

SR. EDUARDO BARASAL MORALES: Puppin, a gente não tá conseguindo te ouvir.

SR. LUIZ COSME PUPPIN MAGALHÃES: Está ouvindo agora?

SR. EDUARDO BARASAL MORALES: Agora sim.

SR. LUIZ COSME PUPPIN MAGALHÃES: O mute sempre me pegando, como sempre.

Vamos lá. O que a gente mais bate, não necessariamente nas vulnerabilidades do protocolo MPLS, e sim, na característica dele, que você acaba tendo um empilhamento muito grande de protocolos para conseguir prover os serviços.

Se você for observar, só [ininteligível] colocou aí, eu tenho o SPF como protocolo de roteamento, eu tenho por cima o LDP fazendo a distribuição das labels, em cima do LDP eu tenho iBGP para poder ativar MPBGP, para gerar as labels da VRF. Então eu tenho plano de controle extremamente sobrecarregado quando eu uso o MPLS. Relembrando aqui, é um protocolo de 97. Então a gente tem todo esse processo, todo esse

legado para carregar. Exatamente por isso que amanhã vocês vão ver os novos protocolos que estão substituindo.

Então, o impacto nas operadoras é realmente esse. O MPLS, ele traz uma sobrecarga no plano de controle dos equipamentos, e buscando uma solução para essa sobrecarga, que estão vindo dos protocolos [ininteligível] além de outras vantagens que eles vão trazer.

E no caso da rede educacional, mesma coisa, a gente precisa conhecer a estrutura dessa rede e entender que serviços que ela precisa. Ah, eu preciso só interconexão entre os prédios. Não entendo que o MPLS possa trazer uma grande vantagem. Ah, não, eu tenho uma rede full match, todos os prédios superconectados um com o outro, e eu tenho um tráfego absurdo entre eles, então eu preciso que sempre use o melhor caminho e não fiquem caminhos ociosos. Aí o MPLS pode vir a ser bastante interessante.

Por isso que até naquela primeira pergunta eu falei: Depende muito da arquitetura da sua rede. Depende muito da característica. Então, não necessariamente preciso ser ISP para usar os benefícios do MPLS. Beleza?

SR. EDUARDO BARASAL MORALES: Perfeito, Luiz.

Vamos chegando aí ao final da nossa live. Eu queria deixar um espaço para vocês fazerem uns últimos comentários, até porque veio tanta pergunta, e a gente já não consegue mais selecionar aqui.

Então, Lacier, manda seus últimos comentários. Quer deixar aí um contato para o pessoal. E já faço o convite para fazer outra live para responder todo esse monte de perguntas que veio. Então, Lacier, manda bala.

SR. LACIER DA COSTA DIAS JUNIOR: Meus queridos, muito obrigado. Queria agradecer aí a oportunidade que o NIC nos deu, de estar compartilhando com vocês esse conhecimento. É sempre um prazer. Professor não vive sem aluno. O oxigênio do professor são os alunos. Então, eu tenho essa oportunidade de estar com vocês, para mim, enquanto professor, já há mais de 15 anos dando aula, é uma oportunidade maravilhosa.

E convidar vocês a continuar acompanhando o NIC nos próximos treinamentos, fazer o treinamento de IPV6. Porque agora que esgotou o V4 não tem para onde correr. Tem que botar o V6 para funcionar.

E dizer que a VLSM continua com seus trabalhos, a pleno vapor, todo mundo remoto, mas trabalhando com 100% da carga. Então, muito obrigado. Passo a palavra para o Puppin. Antônio e Eduardo, muito obrigado pelo convite.

SR. LUIZ COSME PUPPIN MAGALHÃES: Bom, agradeço ao NIC pela oportunidade. Principalmente pela oportunidade de dar uma aula junto com o Lacier, que a gente trabalha junto, mas nunca conseguiu dar uma aula em conjunto.

Foi uma oportunidade bem interessante. Apesar de que a gente teve que perder alguns quilinhos para caber na mesma câmera, os dois eram gordinhos. Então a gente se preparou alguns meses para isso.

A gente fica muito satisfeito com o retorno que ela teve, com as perguntas. É muito bom para nós, que somos professores, conseguir levar conhecimento para tanta gente, e ver que o pessoal se interessou bastante no conteúdo.

O recado é esse aí. Estamos a todo vapor. Quem precisar, pode procurar a gente. E a disposição é exatamente essa: levar conteúdo, levar informação, buscando sempre o melhor para o mercado.

SR. LACIER DA COSTA DIAS JUNIOR: Puppin, eu queria te agradecer, meu querido, porque realmente a gente nunca deu aula junto. Tem esse detalhe. Então o NIC conseguiu proporcionar que a gente coubesse na mesma tela.

E fico à disposição do NIC, tanto eu quanto o Puppin, todos os professores da VLSM, para responder todas as perguntas e novas lives. Se quiserem convidar a gente, é sempre um imenso prazer estar aqui com vocês. E responder perguntas, para a gente, é maravilhoso, porque a gente vê o nível de interação do pessoal. Então, fico aqui à disposição de vocês, sempre. Muito obrigado.

SR. ANTÔNIO MARCOS MOREIRAS: Muito legal, Lacier. Muito legal, Puppin. A gente agradece muito a participação de vocês. A gente agradece muito a presença de vocês. O que o Lacier perdeu de peso, ele ganhou em barba.

O que o Puppin perdeu em peso, ele ganhou em capacidade didática. O Lacier também. Estou brincando. A aula foi excelente. Muita gente gostou. Temos muitos likes no vídeo. Podíamos ter um pouquinho mais de likes, tem mais gente acompanhando do que likes. Tem o deslike. Quem não gostar também pode dar o deslike. Sejamos justos. Mas é importante também, para a gente, a gente pede esses likes e deslike para o Youtube poder distribuir o vídeo para mais gente. Essa interação de vocês, tanto no chat quanto nos comentários, quanto dando os likes, ajudam o Youtube a fazer o conteúdo chegar para mais assinantes do canal, para mais pessoas, e a gente sambe que é um conteúdo de qualidade, e a gente quer fazer o conteúdo chegar para o maior número de pessoas possível.

Estou vendo também no chat, tem pessoal desesperado. Não consegui fazer. Não consegui baixar. Não consegui fazer funcionar. Olha, gente, o material não vai sair do site do curso. O vídeo vai estar disponível aqui no Youtube, gravado. Então, dá para vocês assistirem depois, com calma, dando pausa, olhando o material. Colocando... Até colocando as dúvidas no comentário do vídeo, na medida do possível, às vezes a gente não vai estar ao vivo, respondendo na hora, mas, às vezes, passando algumas horas, passando um dia, passando dois dias, a gente vai tentar responder ali o que vocês colocaram. E por que não, podemos pensar, sim, em outras lives, até em outros horários. Às vezes o pessoal dá sugestão aí.

Até queria ouvir de vocês, aí, antes de encerrar, do pessoal que tá ainda interagindo aí no chat. Às vezes a gente escuta algumas sugestões de fazer essas lives em horários alternativos, como fazer mais no final da tarde. Vocês acham que isso atenderia mais... mais pessoas do que nesse horário? Porque a gente está vendo também que a participação nesse horário tá muito boa. Se vocês quiserem colocar alguns comentários em relação a isso no chat. Seria legal para a gente ter uma ideia, assim, do que que vocês pensam e de a gente poder se programar. Porque, enfim, fica aí.

Bom, lembrando, amanhã continuamos com o evento. Amanhã temos o pessoal da Juniper falando de EVPN, falando da evolução do Ethernet. Então um tema também muito importante. O vídeo já está criado no canal do Youtube. Então, vocês podem já acessar o link do vídeo, já pode compartilhar ele nas listas de WhatsApp, nos grupos do Facebook, já podem clicar lá na notificação para ser avisado na hora que a live for para o ar, para não ter o perigo de amanhã de manhã dormir até mais tarde e esquecer de entrar na live. Enfim...

Meu like é pelos deslikes, o Almir está falando. Não entendi. Você está falando like... Você gostou do deslike? Então tá bom. Eu vou pedir deslike sempre, para ganhar like então. O Eduardo fez cara de que eu

estava falando coisa errada. Não devia pedir deslike. Ganhamos um like explícito, Eduardo, porque eu falei para o pessoal dar deslike se não gostou. Mas é justo. Se não gostaram, dão deslike.

O Almir está perguntando se o evento atendeu a expectativa do NIC como dos participantes? Sim o evento está atendendo nossas expectativas. E a nossa expectativa é levar o conteúdo para o maior número de participantes possível, para atingir a comunidade técnica da forma mais ampla possível. E a gente está vendo que isso tá acontecendo com esses eventos A gente tem muito feedback positivo da comunidade. Enfim...

Não esqueçam de preencher a avaliação online. O pessoal da equipe está me dando o recado. Eu não entendi se o QR Code já apareceu, se não apareceu. Se o QR Code não apareceu, vai aparecer daqui a pouquinho. Está aparecendo aí agora. Certo? Então... Mas tem o link também. O pessoal está colando o link no chat, e... bit.ly/semanacap4. Facinho, facinho.

Então não esqueçam, por favor, de preencher a avaliação. São só duas questões, cara. Você tem que dar uma nota lá, de zero a dez para o evento, para a gente calcular, comparar, ver se a aceitação foi boa, se vocês gostaram, se vocês realmente não gostaram. A gente acompanha, a gente cria uma métrica e a gente acompanha. E daí tem um espaço para você dizer no que que a gente pode melhorar. Pensa na pior coisa do evento. Se você gostou muito, gostou muito mesmo, pensa na que foi menos boa, certo, e põe lá para a gente, porque a gente vai tabular aquilo, a gente vai ver o ponto principal, o ponto que foi mais falado, e a gente vai tentar melhorar nas próximas lives.

E não se esqueçam, quem precisa de certificado, quem quer um certificado de participação, tem que fazer a inscrição até as 14h, no nosso site. O link também vai ser colado aí no chat do Youtube. Ah, Moreiras, mas estou aqui no celular e não consigo ver o chat agora. Ok, corre agora, na hora do almoço, acessa um computador, olha esse vídeo. Vai estar lá no histórico do chat, vai ter o link da inscrição. Faz a sua inscrição até às 14h, senão você não vai ter o certificado. Não adianta procurar a gente depois, contar uma história A gente não consegue, gente, atender as exceções. É muito difícil de operacionalizar isso. Vai estar aberta a inscrição até às 14h. Tá bom?

Agradeço muito, muito a participação de todos. Agradeço ao pessoal da minha equipe, que organizou o evento. O Eduardo, a Erina, a Tuane, o Tiago, todo mundo que participou da organização. Agradeço muito o pessoal que fez essa parceria com a gente para trazer o conteúdo, no caso de hoje, a VLSM com o Lacier, com o Luiz Puppin.

Agradeço muito a participação de vocês todos da audiência, vocês foram fantásticos, interagiram muito, fizeram muitas perguntas inteligentes, relevantes. E isso ajuda, ajuda aos professores, ajuda a gente fazer os comentários. É muito legal quando a gente tem uma participação assim.

Agradeço ao Pedro, do suporte técnico aqui do NIC, que cuidou de toda transmissão, colocou os vídeos, fez os cortes, fez toda parte técnica. Agradeço todo o pessoal da equipe de comunicação, a Carol Davo, a Karina, e um monte de mais gente que ajudou no contato com o pessoal que nos trouxe o conteúdo, que ajudou na divulgação, que ajudou produzindo site. O pessoal do Flávio [ininteligível] que produziu o site. Muita gente no NIC.br trabalhou para que essa semana de capacitação online acontecesse. Muita gente fora do NIC.br, como a VLSM e os outros parceiros de conteúdo também colaboraram para que isso acontecesse. E isso também não aconteceria se a gente não tivesse essa audiência de vocês, esse público maravilhoso, participante.

O Almir está perguntando se isso vai estar disponibilizado via podcast? Não. Esse evento, essa semana, não, não vai estar disponibilizado via podcast porque tem muita coisa gráfica, tem muito comando, tem muita coisa, não tem como a gente colocar isso sobre podcast.

Mas já que você lembrou, Almir, eu vou lembrar a todo mundo que a gente tem um podcast, que é o Camada 8, e a gente já tem vários episódios lá disponíveis. Procura na sua plataforma preferida de podcast. Tem o PTT, tem IPV6, tem sobre Coronavírus, tem sobre criptografia, tem vários episódios do podcast já disponibilizados muito legais, com Eduardo, com a Erina, com o Tiago, E, logo, logo, a gente vai ter mais episódios e mais novidades. Por enquanto, é um episódio por mês, aí, sempre na segunda semana do mês. Já tem vários lá para vocês verem. Quem não conhece, vale a pena. Procura Camada 8, podcast, na sua plataforma de podcast preferida que vale a pena ouvir. Eu gosto. Já ouvi várias vezes aqui, hein?

Ajudei a fazer, mas eu gosto de ouvir o pessoal falando, que o pessoal escreveu, assim, fez roteiros incríveis para o podcast, está muito legal e muito divertido até.

Bom, muito obrigado, gente, pela participação. Agradeço novamente, a todos, e a gente encerra por hoje. Conto com a presença de todo mundo amanhã, às 9h da manhã, para o último dia dessa fantástica semana de capacitação on-line do NIC.br. Obrigado.