**SR. EDUARDO BARASAL MORALES:** Bom dia, pessoal. Sejam todos bem-vindos aí a mais uma live Intra Rede. Uma live que a gente tenta trazer aí as discussões do dia a dia aí dos sistemas autônomos, daqueles operadores de redes. E hoje a gente vai falar sobre Aprimore a Eficiência do seu Provedor Por Meio das Melhores Práticas Operacionais. Então, nós convidamos aí especialistas de diversos roteadores, como Cisco, Juniper, Mikrotik, Huawei, para falar com vocês aí o que precisa ser feito nessas máquinas para a gente ter ali maior eficiência delas e conseguir o melhor proveito na hora de colocar essas máquinas na nossa rede. E vamos ter também o lançamento de uma ferramenta nova da equipe do Simet. Mas eu não vou falar muito dela, não, que eu quero deixar aí, depois, o Paulo apresentar para vocês. Tem novidades aí para quem é provedor de Internet.

Mas, antes da gente montar a nossa Mesa, eu gostaria de agradecer aos nossos patrocinadores. A gente tem a Juni Link IP & Cloud Netword by Giovaneli Consultoria; Wztech Networks; Icann; Netfindersbrasil; Novatec Editora; Eletronet; GlobeNet Telecom; Mundivox; 4Linux, Solintel; Cisco e Logicalis; 4Bios IT Academy; Globo; Netflix; FiberX e Huawei; e o apoio de mídia da Revista RTI e Infra News Telecom. Lembrando a todos que a gente o certificado de participação dessa live. Então, o pessoal está colocando o link no chat do YouTube, no chat do LinkedIn e no chat aí do Facebook, para que você possa se inscrever e ganhar o certificado dessa live. Lembrando que esse link vai funcionar até às 2 horas da tarde, e você vai receber um e-mail e precisa confirmar no link que é enviado por e-mail. Então, são duas etapas. Se inscreve no link que está sendo colocado no chat e, depois, olha a sua caixa de e-mail para confirmar que você está assistindo, até às 2 horas. Gostaria também de falar que a gente vai ter seis sorteios aí ao longo dessa live. Então, o pessoal vai colocar agora o link de cada um dos sorteios. O primeiro é o do NIC.br, junto com alguns patrocinadores da live, que é um grande kit. Então, a gente vai ter uma caneca da Icann, um kit de acessórios para vinho, um kit Moleskine e caneta da Logicalis, um voucher de acesso grátis por dois meses da Globoplay, um livro Vida de Programador - Volume 0, da Novatec Editora, um livro Vida de Programador - Volume 1, da Novatec Editora, uma garrafinha de alumínio e uma caneta personalizada da Juni Link IP & Cloud Network da Giovaneli Consultoria, uma camisa polo da Semana de Capacitação, uma lapiseira da Semana de Capacitação e kit de adesivos de IPv6 e RPKI do próprio NIC.br. Então, o pessoal vai estar colocando o link para vocês se inscreverem. É o mesmo link do certificado, porque esse daí é um sorteio nosso junto com alguns dos patrocinadores. Basta você se inscrever. Temos agora dos patrocinadores, tá? Então temos aí o sorteio do Netfindersbrasil, que é uma vaga no curso BGP e MPLS avançado em Huawei no modo gravado. Então é um novo link para se você inscrever. Temos aí o sorteio da Eletronet, que é um voucher da Americanas.com, no valor

de R$ 200,00. Então é um outro link para se você se inscrever. Esse é o sorteio da Eletronet. Também temos o sorteio da GlobeNet Telecom, que é uma caixa de som acústica bluetooth. Então, mais um link para você se inscrever. Vão aí se inscrevendo em todos os links, que aí aumenta a chance de você ganhar alguns dos brindes. Temos também o sorteio da Globo, que é um voucher da Globoplay com acesso grátis por dois meses. E o sorteio da FiberX e o Huawei, que é um kit de roteador match 5800. Então, é importante se inscrever. Dá uma lida em cada um dos formulários. Tem às vezes alguma regrinha extra que você precisa fazer, tá? Então presta atenção, porque é assim que você vai conseguir participar de cada um dos sorteios.

Bom, como já é de praxe e todo mundo já sabe, a gente vai começar agora passar o videozinho do Cidadão na Rede. Lembrando que esse é um projeto que a gente quer transmitir conhecimento de cidadania digital, ou seja, como ser um bom cidadão na Internet. E é um videozinho que tenta trazer ali um conhecimento para um usuário comum. Então, é interessante que vocês peguem esses videozinhos, façam download lá no site e divulguem aí para grupo de família, grupo de colegas de trabalho, grupo de escola, de faculdade. Para o quê? Para a gente melhorar a Internet para todos. Se todo mundo aí saber usar a Internet da melhor forma, vai melhorar a Internet para todos. Então, pode tocar o videozinho.

[exibição de vídeo]

**SR. ANTONIO MARCOS MOREIRAS:** Bom dia, gente. Bom dia a todos e a todas que estão aí nos acompanhando. Vocês acompanharam o vídeo do Cidadão na Rede. E o Cidadão na Rede chegou agora a um marco que nos orgulha bastante, nós chegamos ao 50º vídeo, vídeo de número 50. O que é muito legal para a gente, né? A gente tem mais ou menos um ano desse projeto, e eu estou aqui tentando enfatizar ele para vocês. Muitos dos vídeos, a gente fez com base em sugestão do pessoal dos provedores, do pessoal que trabalha com redes. Não são vídeos para vocês que trabalham com redes, não são vídeos para vocês que são técnicos dos provedores. São vídeos para os usuários de vocês, para os clientes de vocês. São vídeos para quem é leigo em tecnologia. São vídeos que sempre dão alguma dica útil sobre como a Internet funciona, como a gente pode usar a Internet de forma mais segura. Como a gente pode conhecer os nossos direitos, os nossos deveres na Internet, usar a Internet de uma forma mais plena, de uma forma melhor. E é um projeto em que a gente conta com o apoio de vocês. Vocês podem fazer downloads desses vídeos e publicar nas mídias sociais de vocês. Não precisa colocar o link da nossa página do YouTube, o link do vídeo do nosso site, sobe o vídeo no site de vocês, no site do provedor. Vê que vídeos que são úteis, que vídeos que falam de assuntos que interessam para os usuários, para os clientes de vocês, e subam esses vídeos no site, nas mídias sociais

de vocês. A gente conta muito com essa colaboração de vocês aqui, que estão nos acompanhando, acompanhando o nosso trabalho. E se vocês quiserem, vocês ainda podem apoiar formalmente, preenchendo lá um formulário de apoio, e ter um vídeo gerado com o seu logotipo como apoiador, um vídeo customizado, e esse vídeo customizado você pode também subir no seu site, na sua mídia social. Então, a gente conta muito com o apoio de vocês.

Bom, gente, estamos aqui começando mais uma live Intra Rede, e eu queria saber de onde são vocês. Coloquem aí no chat, quem está acompanhando. Já digam aí, antes da gente passar a palavra para os painelistas, para os palestrantes, como que está a transmissão, se a qualidade do vídeo, se a qualidade do áudio, está tudo bem, como que está, de onde vocês são. Está na hora também, vocês podem fazer aquele aviso naquele grupo de WhatsApp, naquele grupo de Telegram, no grupo do Facebook, para os colegas da área, de que a live está começando. Temos aqui hoje gente muito experiente, muito tarimbada aqui no assunto. Vários consultores, cada um especialista em um tipo de tecnologia, um tipo de vendor. Então, temos Mikrotik, Cisco, Huawei, Juniper. Acho que só, né? Não sei se... E tem o Paulo, com o lançamento do novo site aí que usa a tecnologia do Simet. Vamos ver aqui o pessoal no chat aqui, o que estão falando. Estância, Sergipe, Campinas, São Paulo, o Forte de Fortaleza, Ceará. O Jair está dizendo que a transmissão está muito boa. O Joester, Brasil Tecpar de Santa Maria, do Rio Grande do Sul. Muito bom, gente. Tem gente aí do Brasil inteiro. Eu sempre também costumo enfatizar a importância de vocês deixarem o like no vídeo, já desde agora do começo, porque é importante para o YouTube distribuir, para o YouTube avisar para todo mundo que esse vídeo está rolando, está acontecendo. Quanto mais likes, mais o conteúdo é divulgado, e quem nos acompanha aqui já sabe que o conteúdo é um conteúdo de qualidade. A gente toma bastante cuidado. Claro, não é só graças a gente, graças aos nossos convidados, que geralmente são fantásticos. E a gente agradece muito, agradeço já muito de antemão a eles pela presença. Olha aqui. Tem um enxurrada agora de gente falando no chat. Itabira, Minas Gerais. Tocantins, Rio de Janeiro, Caucaia, o Renan. Juazeiro do Norte, o Carlos Barreto. Muito bom. Legal.

Então, sem mais delongas, vamos começar com o assunto do vídeo. Antes, antes, só mais uma coisa. Eu preciso explicar como que é a dinâmica da live, hoje, para quem está aqui pela primeira vez. Talvez tenha gente que não tenha... Alguém está aqui pela primeira vez? Coloca aí no chat. Diz aí para a gente: "Primeira live de vocês que estou acompanhando". A gente sempre tem um público aqui bastante cativo, mas eu gostaria de saber se tem alguém pela primeira vez. Se tiver, seja muito bem-vindo e seja muito bem-vinda, né? Mas como que funciona? A gente vai chamar agora os painelistas para uma

rodada inicial. Cada uma vai ter aí dez, 15 minutinhos, e vai fazer uma apresentação sobre o assunto da live, que são as boas práticas, e cada um vai falar um pouco mais da tecnologia específica, dos equipamentos específicos com que ele trabalha, com que o painelista é especializado. Por exemplo, o Giovaneli, que vai começar, imagino que vai falar um pouquinho mais do Juniper. O Leonardo vai falar um pouco mais do Cisco. O Luiz vai falar um pouco mais do Huawei. E o Wadner Maia vai falar dos Mikrotiks. Vão falar das boas práticas nos provedores. Cada um vai ter esse tempo. Nesse tempo, vocês podem interagir com a gente no chat do YouTube. Nossa equipe aqui do NIC.br vai estar anotando as perguntas, para a gente, depois, ter uma rodada de debate com os painelistas todos. E vocês podem também interagir durante essa rodada de debate. Mas podem já ir fazendo as perguntas, colocando as perguntas, durante essas apresentações iniciais. Se algum painelista quiser ficar lá prestando atenção e falar alguma coisa, ele pode fazer isso. Claro, à vontade. Mas às vezes, na hora que ele está ali fazendo a apresentação, é difícil ficar prestando atenção ao mesmo tempo no chat do YouTube. Por isso que a nossa equipe está anotando tudo, e a gente vai ter depois a rodada com as perguntas e respostas, aí um debate. Se um painelista também quiser perguntar ou complementar alguma coisa, fazer comentários em relação à apresentação do outro, também pode. Então, temos essa segunda parte do evento, que é essa rodada de perguntas, resposta e debate. E assim que vai funcionar.

Então, eu vou agora... Não vou apresentar cada um no sentido de falar, colocar o currículo, tal. Os currículos dos painelistas, dos nossos palestrantes estão no site intrarede.nic.br, vocês podem estrar lá. Tem um minicurrículo de cada um. As apresentações também vão ser colocadas lá, em breve. Já tem algumas que eu acho que já estão por lá, mas, se não estão, durante ainda aqui a live, a gente vai fazer o esforço de subir todas lá para o site para vocês poderem acompanhar. Algumas a gente já recebeu, outras os painelistas ainda estão passando para a gente. E é isso. Eu vou chamar agora para começar o Alexandre Giovaneli, da Giovaneli Consultoria. Então, Giovaneli, o palco é seu. Fique à vontade.

**SR. ALEXANDRE GIOVANELI:** Bom dia, pessoal. Tudo bem? Sejam bem-vindos. Obrigado novamente ao NIC.br pelo convite, né? E vamos começar, tá? Vou compartilhar minha tela aqui. Só um minutinho, por favor. Ok. Todos estão vendo? Como que está aí? Já chegou? Beleza. Vamos em frente. Então, pessoal, falando um pouquinho... A gente vai falar um pouquinho mais de Juniper, dos problemas e dos erros mais comuns e como ajustar isso de uma forma bem breve, por conta do tempo. Então, primeiro, a gente vai começar a falar dos erros mais comuns que acontecem, tá, pessoal? Então, antes mesmo do equipamento entrar em produção, já começa a ter

alguns problemas aí ali, se você não seguir à risca. Então a gente está tratando principalmente da linha Juniper. Qual é o primeiro erro mais comum? Primeira coisa, configurar equipamento em bancada, com a temperatura não recomendada pelo fabricante. Por exemplo, você, no seu ambiente lá de configuração, coloca o equipamento lá em bancada, e a temperatura está lá 45, 50 graus, de repente, ali do equipamento. O que vai acontecer? Já ali, você já começa a danificar o equipamento, ou seja, você já ligou ali em um ambiente que não é recomendável pelo próprio fabricante. A temperatura exigida para operar esse equipamento. Então, você acaba danificando o equipamento. O segundo erro mais comum que acontece, pessoal, principalmente em equipamentos Juniper, é misturar fonte AC e DC no mesmo equipamento, tá, pessoal? Isso é proibido. Não pode ser feito, tá? Isso daí é um erro bem comum. Normalmente, qualquer equipamento, ou você trabalha ele totalmente AC, ou trabalha ele totalmente de DC. Não existe essa mistura no equipamento. E os erros mais básicos de operação. Não configurar o NTP, tipo, você vai debugar log e não consegue saber que hora que aconteceu o problema. Não configurar os thresholds de ARP principalmente para o IX.br, o IX de São Paulo, então você tem lá uma solicitação de ARP muito grande. E o roteador, por padrão de fábrica, ele vem com limite de processamento de ARP. Então, você precisa definir qual é o limite exigido para ele fazer esse processamento de ARP nesse equipamento. Isso vale para a maioria dos equipamentos. Não é só para Juniper, tá? Isso é bem geral. Outra coisa também é subir um equipamento sem atualizar, ou seja, você pega o equipamento, simplesmente configura e coloca em produção. Isso daí é um erro também muito... que acontece muito. É um erro grave, inclusive. Você precisa atualizar o equipamento antes de colocar ele em produção. Você atualiza, beleza, ok, coloca a versão recomendada do fabricante e coloca em produção. Outra coisa que acontece muito em equipamentos Juniper, não ajustar os valores de anti-DDoS para o ambiente, ou seja, cada ambiente tem a sua configuração padrão para DHCP, para ARP, para Pppoe, para o BGP, para os protocolos ali, para os pacotes que a caixa vai processar. Para ele não entender que às vezes vier uma requisição muito grande de pacotes, ele não entender que é ataque DDoS no equipamento. Então precisa ser ajustado isso de ambiente para ambiente. Não existe uma receita padrão. Então o ambiente X, vai ser um valor, ambiente Y, outro valor. Outra coisa também é o fato de ajuste de filtros de BGP, de EGP e IGP geralmente, é um erro muito comum. O cara só configura o SPF e não configura os filtros corretamente, ou BGP, e assim por diante. Não segue as boas práticas. Outra coisa também que acontece, que é muito comum. Às vezes, você tem um problema com o equipamento e não aciona o fabricante. É importante, quando você tiver qualquer tipo de problema, o primeiro passo é você acionar o fabricante e avisar ele daquele problema. Que às vezes pode ser um

bug no equipamento, um bug na versão, ou às vezes pode ser um defeito de hardware. Então, o fabricante consegue ali rapidamente identificar o porquê que aquele equipamento parou. "Ah, parou, não fiz nada". Não. Você tem que chamar o fabricante para tomar uma ação. Nem que só for para ver o que aconteceu. Não é nada, é relacionado a um BGP, alguma coisa. Então, você precisa, após um problema, ou defeito no equipamento, você acionar o fabricante, para que ele tome aquela ação o mais rápido possível, para que aquilo não ocorra novamente. Às vezes, por um erro de configuração, ou por um defeito de hardware, ou bug, seja lá qual for. Outra coisa que é importante que a gente recomenda, vamos dizer assim, 70%, 80% dos provedores pequenos não fazem isso, que é manter o suporte e garantia do equipamento ativo com o fabricante. Isso é essencial. Não é porque venceu a garantia, você, beleza: "Ah, o equipamento não vai dar mais pau". Mas pode ser que surja um bug, alguma vulnerabilidade, e você precisa atualizar esse equipamento e você não tem essa atualização, simplesmente porque você não renovou a sua garantia ao suporte. Então, você precisa, como boa prática, como boa prática de gestão de TI, você ter uma garantia e o suporte desse equipamento antigo. Isso é básico, tá, pessoal? Não tem como fugir, entendeu? Você precisa ter para você garantir a disponibilidade do seu provedor. Aí, de repente, depois de um ano, não renova e tal, aí você começa sofrer com problemas de bug ou problemas de vulnerabilidade que surgiu. Então você não está coberto por isso. Isso é extremamente importante, pessoal. Outra coisa que o pessoal tem muito costume é pegar o equipamento, depois que venceu a garantia, não consegue mais atualizar o firmware. Vai lá no site duvidoso, no 4shared da vida, no repositório não oficial, e baixa essa firma e atualiza o equipamento. E aí, automaticamente, atualizar o equipamento com certeza vai ter um backdoor específico, deixando seu roteador livre aí para os hackers atacarem seu equipamento e usar até mesmo ataques DDoS. Isso é básico, baixar firmware só de fontes oficiais do fabricante. O fabricante tem seus canais, seja via tíquete, seja via portal de acesso mesmo do fabricante oficial, para você baixar essas firmwares. E outra coisa também que acontece muito é deixar o equipamento com acesso root ativo, então você deixa o seu login de root ativo para acesso remoto. Isso não pode, pessoal. Então, aqui a gente está dizendo principalmente os erros mais comuns em provedor que jamais devem ser cometidos. Então, com isso, você já sabe mais ou menos qual decisão tomar.

Então, os pontos iniciais que a gente precisa tratar em um equipamento, principalmente Juniper, são coisas básicas. Configurar credenciais de acesso independentes para cada usuário, ou autenticação via redes ou via tacacs, proteções de firewall. Não importa o equipamento, não importa se é Mikrotik, se é Huawei, se é Cisco, se é Juniper, não importa. Você precisa proteger o equipamento com

regras de firewall eficientes, você precisa proteger o seu equipamento de ameaças externas. Se você subir simplesmente, você pega o seu equipamento e configura o BGP, o Pppoe ou seja lá qualquer protocolo e não protege seu equipamento, com certeza, ele pode ser derrubado por hackers ou por ataques DDoS. Isso é básico. Você precisa fazer isso, tá? Outras coisas também, você precisa ajustar os valores de proteção de anti-DDoS nativos do equipamento. Então, nativamente, ele vem com proteções de anti-DDoS, então o que você precisa proteger? A parte de ARP, parte de Pppoe, caso necessário, a parte de DHCP v4 e v6. Esses são os quatro mais importantes que a gente costuma configurar. É claro que cada consultor vai fazer ajuste fino em cada protocolo, mas basicamente é isso que você precisa ajustar no seu roteador Juniper. E outras variáveis para, na verdade, de proteção... de otimização de tráfego. Quando você tiver uma convergência de rota ali, uma convergência de peering, por exemplo, a gente ativa, geralmente, o BFD para ter uma convergência rápida no equipamento e também o Gracefull Restart, para fazer uma troca graciosa de rotas. Ele vai fazer uma troca bem suave, não vai dar aquele impacto de tirar todas as rotas, parar tudo e volta. O Gracefull Restart, ele entra com a rota nova e vai apagando a rota antiga, faz de uma forma suave, vamos dizer assim, ou graciosa, que é o nome correto. Gracefull de graciosa. Outra coisa, sempre manter equipamentos atualizados com a última versão de Junos SR, que é a service release. Nós, particularmente, recomendamos sempre a Junos SR, que a gente tem uma assertividade melhor de estabilidade das novas features, por exemplo. Isso tem que manter sempre atualizado da última versão. Importante: sempre verificar temperatura da FPC e da Routing Engine. Para quem não sabe o que é cada coisa, a Routing Engine é o processador que controla o equipamento, e a FPC é o processador que vai encaminhar os pacotes. Então, você precisa definir que esses chips fiquem na temperatura correta e também o fluxo de ar. Se o ar entra de frente para trás ou de trás para frente. Então, isso é importantíssimo você verificar o fluxo de ar do equipamento, tá? Porque às vezes o equipamento, ele ventila... ele puxa o ar pela frente e solta por trás, e você está injetando o ar atrás, ou seja, esse ar não está circulando dentro do equipamento, esse ar mais frio, por exemplo. Então você acaba danificando o equipamento aí de bobeira por uma configuração do ar-condicionado do seu ambiente. Então, isso é importante você verificar. Só uma aguinha, por favor. A gente fala muito aqui, o tempo é curto. Então, isso são os pontos iniciais que a gente precisa definir no equipamento, tá, pessoal? Então, desde a parte física e também da parte lógica, de configuração.

Então, a gente só vai dar um exemplo aqui só, rápido. Acho que estou dentro do meu tempo ainda. Então, a parte do usuário. Então, cada usuário... caso você não possua autenticação, você cria um usuário para cada operador com as permissões corretas, tá? Então,

para um usuário de nível 1, você não vai dar uma permissão all, por exemplo, permissão de leitura escrita. Isso é importante definir. Aí só um minutinho, por favor. Outra coisa também, pessoal, importantíssimo, configurar NTP server. Então, aqui, um exemplo básico da gente configurar os NTP server, apontando para os NTP preferencialmente da NIC.br, é o que a gente gosta e confia [ininteligível] NTPs da NIC.br e também o timezone. Isso você precisa por uma questão de gestão de logs, gestão de informação. Você precisa saber tudo o que aconteceu no milissegundo possível para fazer um troubleshoot do equipamento. Então isso é básico. Outra coisa também, quando a gente ativa SSH, a gente bloqueia o login de root, tá, pessoal? Então a gente vai permitir que acesse [ininteligível] dentro da rede, mas eu vou bloquear os logins de root, então você acessa só com logins criados para cada usuário. Outro detalhe também é configurar host-name do equipamento. É básico. Você precisa definir o nome do equipamento, colocar o modo que ele vai operar. Geralmente na linha MX, a gente como coloca como errância de IP, ou seja, ele vai otimizar o chip 7, vai trabalhar com buffer maior, vai otimizar o buffer do equipamento para trabalhar com roteamento IP EGP para Internet. Então você tem IP [ininteligível], você tem vários tipos de otimização de tráfego. Então, aqui, você otimiza para IP Internet. E também, pessoal, a parte de log. Você precisa configurar os logs do equipamento. Não existe... você não consegue fazer gestão de equipamento sem log. Isso é básico. Então, a gente configura os logs de emergência, os logs de notícia do equipamento, tudo que está informando ali de BGP caiu, BGP subiu, porta ficou down, porta ficou up, os logs de atualização, quem logou no equipamento. E o interessante é o Interactive Commands. O que significa isso? Tudo que o operador digitar na linha de comando, ele vai ser gravado para uma possível auditoria depois. Então você consegue saber e também mensurar o que cada operador está fazendo dentro desse equipamento. Então você consegue saber: ele está cometendo muito erro, digitando isso. Então, você consegue otimizar aquela operação daquele usuário. E também a gente cria o log de firewall, para saber tudo o que está batendo no equipamento. Tentativa de acesso, tentativa de abertura de porta, porta scan. E assim por diante, tá, pessoal? Estou dentro do meu tempo ainda, né?

E outra coisa também importante, pessoal. E isso é boa prática da NIC.br. Nos cursos é sempre falado. Quando a gente configura o SNMP, a gente define quais clientes irão acessar. Então, eu tenho aqui os clientes que irão acessar esse equipamento, se os clientes são os setores de monitoramento, e também as communities e os clientes que vão acessar. Mas um detalhe importante, pessoal, mesmo você setando os clientes aqui, isso é um detalhe, a porta SNMP vai continuar aberta, tá, pessoal? Então, você precisa ter mecanismos de segurança, que é via firewall, bloqueando essa porta SNMP para a Internet. Se

você fizer essa configuração e não configurar as regras de firewall, aí você vai ativar o PPT lá de São Paulo, o NIC.br vai falar lá, o Antônio Moreiras ou o Eduardo vai falar: "Pode não. Sua porta SNMP está aberta, então não vou ativar seu PPT". Então você precisa criar mecanismos de firewall para poder proteger esse equipamento. Como a gente faz isso, tá? E algumas configurações também padrões, "no multicast echo", "no redirect" de SNMP, "no ping record route". Algumas configurações ali padrões ali para a gente deixar no equipamento por boa prática. Não vou abordar cada uma, porque senão o tempo meu estoura, tá?

Outra coisa. Depois de configurado no básico... Deixa eu ver aqui. Só um minutinho, por favor. Ah, ótimo, tenho mais cinco minutos. Depois da gente configurar isso, a gente vai monitorar o que está entrando no equipamento para depois definir as regras de firewall, tá? Você não aplica umas regras de firewall sem saber o que entra dentro do equipamento. Então, o que eu faço? Eu pego uma interface aqui, dou esse comando: run monitor traffic interface, coloco a interface e analiso o que está entrando dentro do equipamento. Com base nisso, o que eu vou fazer, então? Fazer a proteção do equipamento. Então, basicamente, isso é meio que padrão para todos os fabricantes, não importa se é Cisco, Juniper ou Huawei. O que a gente vai proteger? ICMP fragmentado de entrar dentro do equipamento da Internet, SNMP, a gente vai bloquear todos os pacotes, leitura de SNMP vindo de qualquer ambiente, exceto da minha rede, BGP, só vou aceitar pacote de peering pré-configurados. Aceito pacotes de OSPF, MPLS, LDP, NTP eu aceito e ARP, faço as configurações de ARP e TCPs não estabelecidas também. Então, é assim aí geralmente o pessoal pergunta: "Alguns protocolos precisam liberar, precisam deixar a porta aberta, por exemplo, como SNMP ou NTP. O que eu faço, então?". Eu libero, porém, libero com limite de velocidade, tá, pessoal? Então seria isso. Então, cada protocolo que eu liberar aqui, deixa eu voltar aqui. Vamos. Um desses protocolos, geralmente, eu preciso liberar pelo menos ICPM normal, um ping para a Internet. Eu preciso liberar. Eu libero, só que aplico uma policy de velocidade. Assim, se vier uma exceção de SNMP muito alto no equipamento, vou estar protegendo ele. Então, eu consigo tratar isso de forma mais delicada, tá, pessoal?

Bom, por enquanto, o que eu tinha para falar era isso. Alguma dúvida, pessoal? Ou dúvidas.

**SR. EDUARDO BARASAL MORALES:** Ô, Giovaneli, vamos deixar isso daí para a parte final.

**SR. ALEXANDRE GIOVANELI:** Ótimo.

**SR. EDUARDO BARASAL MORALES:** O pessoal está postando dúvidas, tem bastante coisa já colocando lá no chat. Pessoal, se vocês ficarem aí com alguma dúvida, fique à vontade, pode postar no chat.

A gente está selecionando essas perguntas e, no final ali, que a gente vai fazer uma rodada de perguntas, a gente vai chamar o Giovaneli de novo para comentar. Então, Giovaneli, obrigado aí pela sua apresentação. Se quiser, pode parar o compartilhamento, tudo. E vou seguir aí as apresentações iniciais chamando o nosso próximo palestrante, que vai ser o Leonardo Furtado. Leonardo Furtado, você que é um grande especialista de Cisco, fique à vontade aí para falar um pouquinho sobre como aprimorar a eficiência de um provedor com os equipamentos da Cisco. Então, o palco é seu.

**SR. LEONARDO FURTADO:** Olá. Muito bom dia. São 10 horas e 34 minutos, aqui no horário do Rio de Janeiro. Meu nome é Leonardo Furtado. Será um prazer poder contribuir para a comunidade novamente, por intermédio desse convite aí do NIC.br. Meus cumprimentos aos Moreiras e Morales, dupla aí. Pelo convite muito bacana. Eu acompanhei... Todos os palestrantes aqui presentes são colegas de profissão. A gente se encontra nos eventos, nos conhecemos, trocamos figurinhas e atuamos de forma cooperativa. Concordo muito com o discurso do meu amigo Giovaneli, muito conhecedor do equipamento que ele estava falando a respeito. No meu lado aqui, eu procurei fazer uma coisa mais holística, ou seja, até mesmo porque na wiki do Brasil Peering Forum, no BPF, nós temos muito material falando de boas práticas, o que deve fazer, mínimo disso, mínimo daquilo. Eu convido que acessem a wiki do Brasil Peering Forum, a URL está citada no material que estou compartilhando aqui nessa live, né? E eu optei por fazer uma coisa mais holística. Eu vou compartilhar aqui minha tela para mostrar minha linha de raciocínio, como eu entendo que determinados projetos de infraestrutura devam ser executados. Determinados não, todos, para falar a verdade. Estou compartilhando aqui a minha tela no momento.

Eu organizei o meu discurso e a minha linha de raciocínio com base nesse painel, que é um diagrama de interações aqui, que eu chamo de um ciclo de vida para adoção e investimentos tecnológicos [interrupção no áudio]. Então a primeira coisa que eu sempre recomendo. Como é uma coisa bem holística aqui, tá bom? Vou explicar por que exatamente isso. Primeira coisa que a gente nota no pequeno operador de telecomunicações e até mesmo em outros mercados verticais: investimentos realizados com ênfase muito forte no equipamento, ou seja, não há uma compreensão muito clara dos próprios requisitos de negócio que devem ser saneados por intermédio das tecnologias que estão embarcadas nesses equipamentos. Então, em outras palavras, o indivíduo, ele tem muita pressa em adquirir o equipamento. Muitas vezes, ele faz isso de forma incorreta. Ele não escolhe o produto que é designado ou especializado para aquela missão, na parte da infraestrutura. Então, tudo começa, no primeiro momento, de acordo com as minhas visões aqui, você compreendendo

o teu... Botar aqui um... Os teus requisitos de negócio. Começa entendendo qual problema você tem que resolver, porque as tecnologias, elas foram criadas para idealmente servirem de encontro ou irem de encontro a essas necessidades do negócio. Aí aqui você vai começar, então, no dois aqui, a entender ou compreender o ciclo de vida desse projeto que você vai associar o teu negócio. Pode ser um projeto novo na área de expansão da tua empresa ou na área de concessão, ou até mesmo um projeto para revisitar as tuas práticas operacionais, que eu entendo ser o foco desse evento aqui. Vamos fazer com que na nossa rede, os nossos equipamentos, em primeiro momento, sejam modificados, para que eles performem na sua magnitude, na sua excelência em termos dos KPIs, que vou falar aqui daqui a pouquinho. Uma vez que você entende os requisitos de negócio, e, aqui, na verdade, eu deveria ter trocado, seriam requisitos técnicos. Aqui que você vai usando o teu conhecimento e, principalmente, aqui usando o ecossistema de parceiros do teu fabricante ou dos fabricantes que você está considerando, é que você vai compreender. Para eu cumprir com essas tantas necessidades, tem as partes interessadas no negócio, que são as áreas internas e externas que vão consumir ou se beneficiar dos serviços de infraestrutura que você vai entregar, você vai escolher as tecnologias. Aí quais são... eu tenho... porque para determinar... olha que interessante. O conceito de inovação. Muitas das necessidades que você possui no seu ambiente. Vamos falar de [ininteligível] aqui, então, elas são imutáveis, por exemplo, transportar serviços de [ininteligível] 2 ou serviço de [ininteligível] 3, é uma coisa que a gente faz desde 1900 e bolinha, lá atrás. Mas até os dias de hoje temos as mesmas necessidades. O que vem evoluindo de lá para cá? Qual a ferramenta que usamos para fazer isso. Você vai começar o quê? Identificar quais tecnologias, funcionalidades, recursos e tudo mais você precisa considerar para melhor atender aquele teu projeto, porque cada opção de cenário tem um pró e um contra. Esse aqui é melhor que esse aqui, por essas razões. Então, você começa a comparar, de forma qualitativa, como uma tecnologia difere da outra, para aquela demanda específica, dentre tantas demandas que você vai ter, obviamente, elencadas no teu círculo aí de requisitos técnicos, para você falar: "Isso aqui é mais interessante do que isso aqui". Até mesmo para você identificar, por exemplo, tecnologias primárias e secundárias. Então isso aqui é um requisito indispensável. Sem isso aqui, eu não tenho como entregar o meu serviço. Já esse aqui, ele melhora ou aprimora alguma experiência de alguma coisa, de alguma característica do meu projeto, mas ele é tido como uma característica secundária. Você vai elencar a primária, secundária, primária, secundária, para quê? Na verdade, depois que você identifica essas funcionalidades, protocolos, serviços, recursos, você vai, então, planejar aí a capacidade, que é onde eu vejo muitas pessoas falhando. O cara compra um

equipamento, bota para rodar, e como eu tenho a missão LAN, ele coloca no peering de acesso de uma rede meta Internet e depois ele fala: "Ah, não faz label". Lê o data X: suporta NPNS, exemplo, aí ele precisa fazer load-sharing no backbone por camada 2, aí ele descobre que o cara não faz um FAT, o Flow-Aware Transport, ou não faz um [ininteligível]. E agora, vou fazer o quê? Enfim, o cara vai descobrindo com o andar da carruagem que "aí, eu preciso fazer uma engenharia de tráfego de um L2 VPN no meu TE". Ó, o cara faz TE, faz L2 VPN, mas não permite você associar um túnel de tráfico para uma L2 VPN específica. Ele não tem essa... não vai suportar. Aí você, depois, que gastou não sei quantos mil reais, às vezes, dezenas de milhares de reais, inclusive, você fica: "E agora?". Aí tu vai botar a culpa no fabricante. Na verdade, tem várias pessoas são culpadas disso aí, mas uma delas é você mesmo, com todo respeito. Então, até mesmo, às vezes, você compra um equipamento que ele não escala para a quantidade de sessões que você precisa, ou que ele não escala para largura de banda de comutação que você precisa, ou que ele não escala para quantidade de filler Qos por porta, entendeu? Porque você não compreendeu aquela capacidade daquele recurso que você teve que embarcar no projeto. Então, começa por aqui.

A última coisa que você vai fazer, são dois passos aqui, que estão até meio [ininteligível], renomeio e mando de novo para o NIC.br, que é a identificação do equipamento. Aqui que você vai escolher o equipamento. Depois que tu compreender os requisitos do negócio, conhecer os requisitos técnicos, identificar quais tecnologias melhor atendem a proposta de fornecimento, acho que vai... O Morales, eu vi aqui, está em tela cheia para mim, está em tela cheia para mim. Pelo menos no meu... se não estiver em tela cheia, me fala. Posso dar um zoom. Vou dar um zoom daqui a pouquinho também, que acho que ajuda um pouco mais. Acho que fica mais... Então, voltando aqui, a última coisa que você vai querer fazer de fato é escolher o equipamento. Nessa hora que te remete aqui o seguinte: nós temos uma coisa muito interessante, a gente tem um termo chamado KPI, indicadores chaves de performance, que são vários. Aqui tem uma lista bem resumida. E você tem vai ter uma coisa que é parecida, mas, na verdade, é diferente, que são os fatores críticos de sucesso, que são os CFS, Critical Sucess Factors. Aí você tem, por exemplo, depois que você compreende teu projeto, seja para aquele perímetro ou para aquela solução específica, ou na rede como um todo, que você vai estudar coisas como, por exemplo, qual deverá ser a escalabilidade da minha solução? A escalabilidade, ela é uma coisa até um pouco ampla, porque ela transcende em outras áreas. Por exemplo, a escalabilidade do equipamento em relação à quantidade de instruções que ele consegue acomodar ou operações que ele pode executar mas também a capacidade da tua rede de crescer sem que haja mudanças significativas no projeto original. Então isso tem muito a ver com o tipo

de equipamento que vai acabar escolhendo. Só que você não pode errar nessa conta, mas se você fez esse trabalho prévio que eu comentei, você não teria dificuldade em fazer isso aqui. Então, a parte de escala, a parte de performance, ou seja, as matrizes de tráfego, os fluxos de tráfego, as taxas de pacotes por segundo. Quantas sessões de um determinado serviço você vai ter por segundo, máximas concorrentes, novas conexões por segundo etc.. Essa parte de escala de... Idem para segurança. Essa solução, quais são os meus indicadores chave de performance, meus fatores críticos de sucesso para área de segurança aqui, e idem com gerência, facilidade de gerenciamento. Aqui é um tema extremamente grande. Tem um artigo muito interessante, não é porque eu escrevi, não, é porque ele está bom mesmo, na wiki do Brasil Peering Forum que lida com fundamentos de FCAPS, falhas, configuração, auditoria, performance e segurança, e ele entra na área do eaton BPF, que não tem nada a ver com Brasil Peering Forum, que é o Business Process Framework. Dá uma olhada lá, porque aqui você tem gerência de falha, de configurações, de performance, de segurança e outras tantas áreas e disciplinas de gerenciamento. E aí você vai entender sua parte quantitativa de usabilidade, de disponibilidade, que tem a ver com redundância, SLA. Aqui que você vai decidir também o equipamento. Esses três caras são coisas diferentes, mas se interconectam. Resiliência, confiabilidade, disponibilidade, são coisas que se interrelacionam. A resiliência tem a ver como a rede reage a eventos de falha. Disponibilidade, o que posso fazer para que ela fique mais tempo possível disponível. Confiabilidade são as características dos componentes que você embarca. E o Giovaneli citou um caso, no material dele, BFD. Mas boto aqui, FRR, Fast Reroute [ininteligível]; TLFA; IPFRR; ou ASPF [ininteligível], BGP PIC. E tantas outras ferramentas que você tem que você... a parte de redundância de módulos de supervisão e controle. Fontes de alimentação elétrica redundante, módulo de ventilação redundante. Aqui que você escolhe: o perfil do meu equipamento, ele é de chassi fixo, configuração fixa, ou, então, não, ele precisa ser um equipamento de característica modularizada, por causa do meu diagrama... Aqui que você vai fazer esses três caras que chamo de diagrama de bloco de confiabilidade, isso que vai fazer você ficar satisfeito com a escolha que você fez: "Eu acertei no meu processo. Ele não foi chutado. Ele nasceu direitinho. Ele teve todo o namoro inicial". E você terminou o projeto com excelência. Enfim, isso tudo quando você compreende que esse bloco aqui da direita, que estou passando aqui agora, aqui, tudo isso aqui, na verdade, você vai fazer o quê? Você vai conseguir encaminhar para o princípio de projeto executivo. Cara, não façam investimento sem projeto. Nem que seja um projeto simplista, no ponto de vista de conteúdo, ou de tamanho, ou de abrangência, ou de complexidade, vai ter que ter um projeto. Tem que saber apontar qual ponto liga qual

ponto na tua decisão. E você tem que convencer pessoas aqui. Convencer teu gestor financeiro, o teu diretor técnico e outras... O que chamamos de SMEs, inclusive, SMEs, muitos estão na sua organização, mas por que você não se consulta com quem é referência naquele tipo de solução? Vou falar de Cisco aqui. Daqui você talvez tenha que produzir um projeto técnico detalhado. Aqui que você vai detalhar de fato como a tua arquitetura deve funcionar, o que vai acontecer mediante determinados eventos e coisas nesse nível aqui, tá? Então, a parte de compreensão de ciclo de vida é o que vai fazer diferença. Por exemplo, a Cisco é uma empresa que tem um excelente serviço de suporte, o TAC da Cisco, ela tem um gigantesco sistema de canal integrador, então você tem os integradores, os parceiros certificados autorizados Cisco, que passam por processos bem extensos de cumprimento das suas especializações. Consulta o teu integrador. Permita com que teu integrador conheça tuas demandas com propriedade. Deixa o integrador participar dessa compreensão para que ele consiga te indicar, porque muitas vezes você também não tem conhecimento daquilo que você precisa ter para resolver o teu problema. Nessa hora que o integrador, que, inclusive, está muito colado no fabricante, ele consegue te ajudar, te assessorar. A ideia é o quê? Posicionar uma solução que ela consiga... A segurança da informação aqui, nesse caso, ela tem que estar embarcada desde o início do projeto, obviamente. Aí o teu plano diretor de investimentos, como que vai ser feita a tua adoção tecnológica. O ciclo de vida do projeto permite a Cisco e o seu canal integrador, seus parceiros, poderem te ajudar nesse processo. Aí você vai ter uma solução que escala, que performa, que é muito segura, que é muito disponível, que é muito resiliente e ela entrega exatamente aquilo que você está precisando. É a cultura, na verdade. Embora isso aqui seja uma coisa da minha cabeça, mas que são anos, anos e anos atuando pela Cisco, ajudando os parceiros, ajudando os clientes, e tem essa filosofia na casa de conseguirmos entregar projetos excelentes, quando são observadas estas diretivas. Onde dá errado, obviamente, quando o cara compra um equipamento que ele não é nem sequer da categoria ou da classe de solução que ele precisa para suportar aquela realidade tecnológica, enfim.

Aí que entra a parte onde o NIC.br, os grandes NOGs também mundo afora. De certa forma, também o pedacinho aqui, BPF, o Brasil Peering Forum. Cara, tem muita BCOP. Você vai economizar anos de dor de cabeça e de estudos, cara, participando dos eventos do NIC, acessando os materiais que outros eventos de outros NOGs ali, o próprio BPF, enfim. Mas o NIC.br, na condição do que eles fazem, cara, tem sido excelente. Você está aqui agora participando está desse evento, você já está contribuindo para entender, por exemplo, as minhas dicas, as dicas de Giovaneli, dos outros colegas, o Puppin que vai falar daqui a pouco, que é colega meu também da área, enfim. Foca

aqui, irmão, foca aqui. Porque, na hora que você concluir o seu projeto técnico, ou estiver em vias de conclusão da filosofia da tua adoção tecnológica, é que você vai diluir aquilo quanto às BCPs, quanto às BCOPs. Como você deve fazer para manter teu sistema autônomo, para manter a Internet segura, proteger teu current client de cliente, para tu proteger teu sistema de peering, teu serviço de trânsito. Enfim, você começa a fazer a tua parte, e a soma de vários esforços é que promovem o bem comum.

Para finalizar aqui, falando de Cisco, você tem duas arquiteturas. Não vou demorar muito aqui, não. Deixa eu até ver quanto tempo eu tenho sobrando. Beleza, dá certinho. Temos arquiteturas centralizadas, de comutação centralizada, por exemplo os ASR 1000, a família ASR 1000, uma taxa de multisserviços espetacular. E tem os roteadores, por exemplo, ASR 9000, que é uma outra classe de produto. Eles até compartilham, tem uma área de interseção. Tem projetos que pode ser um, pode ser outro. Aí você tem que entender toda a parte restante aqui que eu falei, para você: "Vou escolher esse cara. Não vou escolher esse cara". Mas ambos atendem para uma diversidade de missões. Beleza. Aí você tem três tipos de tráfego em uma rede. Você tem o tráfego de trânsito, que passa pela caixa, você tem o tráfego de gerenciamento e dos protocolos de roteamento, dos protocolos de resiliência, que são direcionados ao módulo de supervisão e controle do equipamento. Mas, por exemplo, em uma ASR 9000 você também tem o tráfego local, do line card, ou seja, porque o processamento é distribuído. Alguns protocolos de plano de controle residem no line card e não no módulo de supervisão e controle. Enfim, então você tem cada uma dessas áreas, que são áreas sistêmicas de arquiteturas, planos de controle, onde residem os protocolos, as estruturas de dados, tabela de roteamento, LSDB, tabela BGP, Lock RIB, BDJ RIB in, LJ RIB out e aquela coisa toda. Planos de controle. Protocolos. Plano de dados são suas estruturas de comutação em hardware, especializado, uma FIB, por exemplo. [ininteligível]. Plano de serviços, você tem coisas, por exemplo, como, PPPOE, Ipoe e por que não CGNAT, [ininteligível] parte de gerência. Cada uma das áreas tem componentes vulneráveis. O protocolo é vulnerável, então, mas a Cisco tem na sua linha de produtos diversas facilidades que você vai... na verdade, tudo que está mostrado aqui embaixo você pode encontrar em BCOP. Vou desenhar aqui. Isso aqui está citado nas BCOPs. Por exemplo, no plano de controle, você vai autenticar teus protocolos de roteamento. Você vai policiar, que é o que... o recurso similar que o Giovaneli do firewall feature, você vai ter RPTS, o ASR 9000, o control plane policy no ASR 1000, para você proteger a tua CPU contra ataques lançados contra seu protocolo. Você vai proteger teus protocolos de acordo com as características de cada um, limitar a quantidade de prefixos, enfim, coisas do gênero. E muito importante é a parte política de roteamento, que faz filtros, não aceita bogons, não fazer Route link, não fazer

sequestro de prefixo. Você tem que ter um cuidado aqui bastante severo nas tuas políticas de roteamento. E você pode obviamente estender isso para todo o resto. Plano de dados, anti-spoofing, Manrs fala disso aqui, anti-spoofing de pacote, ACLs, Qos para você filtrar classes proibidas de entrar na conclusive e proteger tuas estruturas de dados de acordo com cada característica.

E para finalizar aqui, cara, o mesmo com área de serviços e gerenciamento. Então, não vai usar Telnet para gerenciar tua rede. Botar um SSH. Você não vai usar o SNMP versão 2, V2C, para fazer uma community de [ininteligível] na tua rede. Pela amor de Deus, você não vai configurar por SNMP, pô... ou bota SNMP versão 3 ou já migra logo para modelos Netconf/yang. Você talvez queira fazer um controle de admissão de... Talvez não, você vai querer fazer controles de admissão chamada, por exemplo, PPPOE e, cara, cada equipamento tem lá suas características e as recomendações do fabricante. Então, para finalizar aqui: hardware installation guide, software configuration guide e Cisco validate design. São três coisas ali que vocês vão considerar no projeto e isso que vai te dar uma coisa executada de acordo com as melhores práticas, seguindo aqui minhas sugestões. Desculpa a leve ultrapassagem aí, tá, pessoal? Morales, mil perdões. Prometo um chope na próxima semana da Infra para vocês ali. Na verdade, eu vou pegar o chope de vocês, na caneca de vocês, e devolvo para vocês. Obrigado, gente, não tenho mais nada para compartilhar, mas vou ali conectado aqui para poder responder as dúvidas de vocês, caso vocês tenham interesse ali. Espero ter sido útil acima de tudo.

**SR. ANTONIO MARCOS MOREIRAS:** Muito legal, Leonardo. Eu, o Eduardo e outras 377 pessoas que estão acompanhando ao vivo agora pelo YouTube vão esperar esse chope na próxima semana de Infra, certo? Agora já não sei se vai ter chope gratuito lá na semana de Infra, porque você já prometeu mesmo o seu. Então, estamos contando com o seu, agora.

**SR. LEONARDO FURTADO:** Tá bom, obrigado.

**SR. ANTONIO MARCOS MOREIRAS:** Brincadeiras à parte, foi excelente a apresentação. Que diagrama, hein, cara? Você vai vender esse diagrama a preço de ouro ou ele vai estar disponível aqui para o pessoal?

**SR. LEONARDO FURTADO:** Tá, olha, só. Eu sei que eu passei material para o Eduardo Morales, ele tem esse material lá com ele, mas tudo meu é muito dinâmico, né? Já tenho ideias de melhorar isso aí. Eu vou... se você concordar, o NIC.br concordar e você comunicar isso para o seu público, prometo, até o final do dia, dar uma pincelada nesse negócio, fazer uma versão 2.0, que ela vai ser muito diferente da primeira. Vou dar um fermento, esteroides e anabolizantes. Passo para o Morales novamente, ele publica lá na página, e vocês

comunicam aí para seu público. Você que está acompanhando agora, você vai ter a versão 2.0 disso aí. Eu prometo, ou mudo de nome. Não, não quero mudar de nome, não.

**SR. ANTONIO MARCOS MOREIRAS:** Não? Já está comunicado e aceito. O Eduardo não sei se já teve oportunidade de subir lá no site, mas se não subiu, daqui a pouquinho vai estar lá essa versão no site para quem quiser dar uma olhada. E mais tarde vamos ter a versão revisada e aprimorada desse único slide com múltiplos conteúdos. O Eduardo já subiu, já está lá no chat. Então, quem quiser fazer um download dessa figura que o Leonardo usou, já está lá. E depois, à tarde, voltem no site do Intra Rede, porque vai ter uma versão aprimorada ou melhorada. Ou amanhã, se quiserem, para terem mais certeza, dar tempo de subir, tudo certinho.

Bom, gente, vocês estão gostando da live? Estou vendo que tem bastante gente fazendo pergunta, interagindo. Alguém comentou aí que eu falei que a live não era para técnicos, e a live estava bastante complicada. Eu estava falando do vídeo do Cidadão na Rede, aquele vídeo de 15 segundinhos que a gente exibiu, sempre para fazer propaganda do Cidadão na Rede. A gente exibe normalmente um vídeo no começo da live, no final da live. Mas obviamente essa live é para técnicos. Essa live só tem assunto técnico, assunto técnico de alta qualidade aqui, discussões técnicas de alta qualidade, com esses nossos convidados. Então, estamos falando aqui de assuntos técnicos sim. Se vocês estão gostando da live, não esqueçam de deixar os likes, né? Temos aqui 379 pessoas acompanhando no YouTube, só 190 likes até agora. Estou um pouquinho triste com isso. Mas estou esperando aqui. Quem sabe vocês topam aí deixar alguns likes a mais. Eu quero lembrar também até na esteira aí da gente ter tido problema com a grande plataforma, alguns dias atrás, de uma indisponibilidade, que a gente não transmite ao vivo só via YouTube. A gente tem transmissão ao vivo também no Facebook e no LinkedIn. Então, a gente normalmente concentra mais, fica batendo papo mais aqui, porque o chat é pouquinho mais dinâmico, mas quem quiser acompanhar pelo LinkedIn, quem quiser acompanhar pelo Facebook, dar uma olhada na qualidade das transmissões por lá, também fica à vontade. Se alguma hora a gente tiver por acaso uma indisponibilidade aqui do YouTube ou qualquer outras plataformas, as outras continuam transmitindo, continua a transmissão. Então, eu estou comentando aqui para que todos vocês saibam disso, para que a gente não coloque aqui todos os ovos em uma mesma cesta. Ou você mesmo... às vezes tem um problema na plataforma ou às vezes tem um problema na nossa conectividade com uma determinada plataforma. Então, se algum momento vocês sentirem alguma dificuldade de conectividade com o YouTube, vai para o LinkedIn, ou está com dificuldade de conectividade no LinkedIn, vai para o Facebook, ou vice-versa, né? Fiquem à vontade

para nos acompanhar em qualquer uma das três plataformas aqui em que a gente transmite ao vivo, e os vídeos também ficam lá disponíveis, depois, nas outras plataformas.

Eu gostaria de chamar agora o Luiz Cosme Puppin Magalhães, da FiberX, para continuar aqui a nossa live, para assumir o palco e fazer a apresentação. Por favor, Puppin.

**SR. LUIZ COSME PUPPIN MAGALHÃES:** Bom dia, pessoal. Obrigado de novo aí ao NIC pelo convite. Mais um evento aí apoiando o NIC, apoiando essa iniciativa de transferência de conhecimento, que é sempre muito importante para o nosso mercado. Deixa eu compartilhar minha tela aqui. É sempre bem difícil falar depois do Giovaneli e do Furtado, porque é uma pena meu nome começar com L, e o deles ficar na frente, porque eles já falam quase tudo, e a gente acaba ficando repetitivo. Mas é interessante que vocês podem observar que não importa qual é o fabricante, as recomendações são basicamente as mesmas. Vocês vão ver que as recomendações do Giovaneli, de atualização, de segurança, as recomendações do Furtado, de projeto, principalmente, são basicamente as mesmas recomendações que a gente tem no fabricante, na Huawei, tá?

Eu separei aqui um pouquinho, coloquei quatro itens principais aí para a gente discutir. Desativar serviços desnecessários. Eu vou falar um pouquinho sobre isso. Quais são os principais serviços que a gente precisa desativar. Ativar policies de controle de acesso básico que a gente precisa para os equipamentos. E o Giovaneli bateu bastante em Juniper, o que precisa, e eu vou mostrar um pouco... A Huawei é um pouquinho diferente, mas a ideia principal é a mesma, de trazer segurança para o seu equipamento. Manter as atualizações indicadas pelo fabricante e manter o contrato e suporte ativo. E manter as configurações otimizadas para melhor desempenho. Quanto às atualizações, eu coloquei aqui como você consegue acesso à atualização. O site da Huawei. Muita gente procura www. huawei.com. Mas a Huawei, ela trabalha com divisões, e o site principal dela, o www, ele mistura todas as divisões, que ali no www, você encontra a área de clientes finais, de residenciais, consumer, que aí é relógio, celular, e tudo mais. E acaba ficando misturado com o enterprise, que é o que a gente usa, que são produtos de telecom, que são os produtos que a gente usa no nosso dia a dia. Então, quando você entra no e.huawei.com, você está entrando especificamente no site onde você vai conseguir as informações da linha de produto que a gente trabalha. E buscando lá no e.huawei, na área de suporte técnico, eu consigo acesso direto a download de software, documentação, base de conhecimento, comunicados: "Ah, saiu um alerta de segurança, alguma coisa". Cursos on-line. Tudo, tudo, tudo que a Huawei puder disponibilizar de suporte, nesse site, na área de suporte técnico, você clica aqui e você escolhe qual é a linha de produtos. A linha de produtos

que a Huawei oferece vai desde ODN, desde a fibra lá na rua, lá no poste que você vai colocar, até o data center modulado, data center pré-fabricado. Então, toda linha de produtos que você consegue comprar da Huawei hoje, você consegue ter acesso a toda documentação, base de conhecimento, por esse link aqui, tá? Claro, a documentação, os manuais, a maioria deles são públicos. Você não precisa ter contrato firmado com a Huawei para ter acesso. Mas o download de software você precisa ter um usuário registrado e, nesse usuário, um contrato de suporte vinculado para você fazer o download do software. Assim como funciona em qualquer outro fabricante, acabou o período de garantia, você perde as atualizações de software, tá?

Eu gosto de falar para os clientes que o contrato de garantia, ele é um seguro. Quando você compra um carro, você paga um seguro para se você tiver uma emergência ou você vai ser socorrido, lá vai ter o reboque para te socorrer. Se você bater com o carro, você vai ter algum tipo de assistência. Se o carro for roubado, você tem algum tipo de assistência. Nos equipamentos, o contrato que você assina com o fabricante, que você renova a cada ano, ele vai servir para quando você tiver uma dúvida, quando você tiver alguma questão, algum problema no equipamento, ele vai ter um TAC lá para te atender. E aí esse equipamento teve uma falha de hardware, alguma coisa assim, você tem o direito de substituição desse hardware. Se não foi alguma coisa que você provocou. Ah, você enfiou uma chave de fenda e queimou o equipamento, não vai ter esse tipo de atendimento. Mas queimou uma fonte, uma interface parou de funcionar, uma placa parou de funcionar, se você tem o contrato e o suporte ativo, dependendo do contrato que você assinou, junto com o fabricante, no próximo dia útil, você está com a peça lá para fazer a substituição. Então, você investe centenas de milhares, ou dezenas de milhares de reais em um equipamento, e, depois de um ano, você joga fora toda a garantia que você tem, todo o suporte que você teria, porque você não vai renovar por alguns mil reais aquele tipo de atendimento, aquele tipo de garantia que você tem. Então é muito importante manter isso atualizado.

Quando você clica lá naquela parte do suporte, ele abre essa telinha. Eu dei um print na tela. Por exemplo, eu escolhi aqui os switches da linha 6700. E eu escolhi a versão de software. Você vê que ele tem várias versões de software aqui. Uma delas está com esse likezinho, com o dedinho aqui, indicando em douradinho. O que ele está indicando? Que essa é a versão recomendada pelo fabricante. Não adianta: "Ah, saiu, se você..." Aqui é só um print. Mas se você entrar no site, você vai ver que já tem a versão 22 disponível. Só que a versão 22 ainda está em desenvolvimento, a versão 22 ainda não foi plenamente testada no mercado. Ela está lá disponível para fazer

download, somente para algumas empresas que, por acaso, precisam de alguma funcionalidade que vai ser inserida na versão 22. E se você clicar e, por alguma casualidade, você conseguir fazer o download, se você instalar, a primeira coisa que vai acontecer, se você abrir um chamado, vai ser te perguntarem quem autorizou você a instalar essa versão. Porque ela não está... não é uma versão testada, aprovada e utilizada em larga escala. Para quem é cliente FiberX, quem é cliente aqui da FiberX, a gente tem o portal, que é o SAC, que é o nosso portal de atendimento, e a gente usa a mesma política de marcar a versão recomendada. Enquanto você tiver contrato de suporte do teu equipamento com a gente, você tem o direito de fazer o download, cria um servidor de FTP temporário, já faz o download direto para o equipamento. Não precisa nem subir em um outro servidor de FTP. Aqui você faz download de licença, abre RNA, abre chamado, interage com a nossa equipe. Quando você tem o nosso suporte ativo aqui com a FiberX.

Passando um pouquinho ali para as políticas de controle, para as policies de controle, a Huawei, ela tem uma ideia um pouquinho diferente... O Giovaneli pode concordar comigo. A Juniper, ela... O equipamento vem aberto, e você faz as políticas de fechamento do equipamento para o seu ambiente. Então, você tem que analisar o teu ambiente e fechar, como o próprio Giovaneli falou, você captura o pacote, entende o que está entrando e aí você fecha de acordo com o seu ambiente. Isso é muito útil para você granularizar política de segurança. A Huawei, ela trabalha com uma política um pouquinho diferente, que o equipamento, ele já vem quase todo fechado. Ele tem uma política, esse CPU defend bem agressiva, e só os serviços... se você subir os serviços sem nenhuma ACL, ele está totalmente aberto. E se eu quiser controlar o serviço, eu vou lá e coloco uma ACL no serviço. Por exemplo, uma ACL nos SSH, coloco uma ACL no SNMP, e aí a ACL do SNMP, ele só vai abrir aquele serviço, só vai responder aquele serviço SNMP para aqueles IPS que estão autorizados. Nos SSH, a mesma coisa. E claro, estou cansado de ver equipamento que o pessoal não coloca o mínimo da segurança, que é uma senhazinha da console, porque ele acha assim: ”Ah, lá no meu data center, só minha equipe entra”. Só que ele esquece, por exemplo, que ele coloca Switch no alto de um morro, em uma torre de transmissão que ele tem lá, e ele fica pensando que: “Ah, não, a única forma de derrubarem meu provedor é cortar a fibra”. E se o atacante for um pouquinho mais inteligente e você não toma esse tipo de cuidado, o cara invade lá, bota um cabo na console, injeta uma rota default, ele faz qualquer tipo de configuração que eu te garanto que vai provocar uma dor de cabeça muito maior na tua rede do que ele simplesmente cortar a fibra. E o pessoal não toma esse mínimo cuidado, que é colocar aí uma senhazinha pelo menos na console do equipamento. Outra medida aí que a gente recomenda bastante é desativar serviços desnecessários

ou inseguros. Por exemplo, o HTTP, nos roteadores não, mas nos switches, ele vem ativado por padrão, porque a ideia dos switches é eles terem uma interface simples de gerenciamento e o HTTP, bem ou mal, interface gráfica bem mais simples para o cliente leigo. Então, só que o HTTP, por natureza, é um protocolo inseguro. E se você olhar a quantidade de vulnerabilidades encontradas nos equipamentos Huawei, Cisco, que têm HTTP ou qualquer fabricante que tenha interface HTTP, o volume de vulnerabilidade em cima da HTTP é infinitamente superior a qualquer outro protocolo que o equipamento possa vir a ter. Então, o que é recomendado: esquece interface gráfica, dá um "no HTTP server" lá, desativa o HTTP, e diminui aí um grande foco de problema que você possa vir a ter. A gerência por Telnet normalmente já vem desabilitado, mas eu já vi em inúmeros equipamentos aí que o pessoal habilita porque é: "Ah, é mais fácil que o SSH". Só que tudo que é fácil normalmente não é seguro. A segurança normalmente é avessa à facilidade. Então, confere se ninguém ativou o Telnet por padrão, colocou lá no scriptzinho ativando o Telnet. O Netconf, você não usa o Netconf por padrão, na hora que eu subo a configuração de SSH na Huawei, o Netconf, ele sobe automaticamente. Então, se você não usa, eu subo SSH, vou lá e desativo o Netconf. O Netconf é uma forma de configuração, é um protocolo que você usa para configurar o equipamento, mas se você deixar ele aberto sem uso, sem proteção nenhuma, ele vai virar uma fonte de vulnerabilidade para você. E nos equipamentos Huawei, você tem um protocolo chamado DCN, nos roteadores da Huawei, tem um protocolo chamado DCN que ele vem ativado por padrão. Ele funciona como ZTP, o Zero Touch Provisioning. É um equipamento que ele fica escutando. É um equipamento não... É um protocolo que ele fica escutando. Enquanto ele está ativo, ele escuta, esperando que um sistema de gerência injete configuração para ele, ou seja, ele é um facilitador. Mais uma vez, tudo que facilita tua vida, nem sempre é seguro. Ele é um facilitador para... Eu pego o equipamento, mando um técnico que não entende muito, não precisa entender muito, ele só precisa parafusar no rack e plugar o cabo. Ele plugou o cabo, e se eu tenho o sistema de gerência da Huawei, aquele equipamento vai procurar o sistema de gerência e já baixar a pré-configuração. E uma das primeiras coisas que você faz quando baixa a pré-configuração é desativar de novo esse protocolo. Então, como o sistema de gerência da Huawei, normalmente, não é adquirido pelos provedores de serviços, esse protocolo aqui, ele só serve para ficar aberto e criando aí uma possível porta de entrada, se um atacante descobrir uma vulnerabilidade dele. Então, simples. Vou lá e boto 1 do DCN. Digo que: Sim, quero desativar, e ele vai desativar. Isso em bancada. Na hora que eu ligo o equipamento, já posso fazer isso aqui.

Ativar configurações recomendadas. Eu não vou bater muito nisso aqui, porque o Giovaneli já falou bastante lá com o Juniper. Mas

o NTP, é óbvio, a pior coisa que tem é quando te chamam para resolver problema na rede e cada equipamento está com uma hora diferente. E você tem que ficar com calculadora fazendo conta para descobrir que log bateu com que log e dependendo você nunca vai identificar de onde o problema surgiu. Então o NTP é fundamental. Eu até digo que antes de fazer o NTP, antes de configurar a primeira coisa no equipamento, nem que seja manual, pega o horário do seu relógio, coloca lá no clock do equipamento, aí você começa a configurar, depois você vai, pega, bota o NTP para ele sincronizar automaticamente. O SSH, sempre substituir o Telnet por SSH. Como o próprio Furtado falou, sempre que possível, principalmente se for escrever por SNMP a versão 3, aí uma característica, a Huawei, ela só vem com versão 3 ativada por padrão. Então, se o cara subiu a versão 1, ele subiu uma vulnerabilidade na caixa porque ele quis, porque a versão 1 não vem ativada, e a versão 2, V2C não vem ativada nos equipamentos da Huawei. E aí é bem clássico isso aqui. Se você ativar, você está assumindo o risco de ativar um protocolo que tem as vulnerabilidades.

E uma coisa que, sempre que possível, a autenticação por Radius e Tacacs, por quê? Demitiu um funcionário, eu tenho que trocar todas as senhas de acesso aos equipamentos? Quando eu tenho Radius e Tacacs, eu demiti um funcionário, eu deleto a conta de acesso dele e pronto. Ele não vai ter mais acesso a nenhum dos equipamentos. Então isso aqui facilita muito para a gente, no dia a dia.

Ajustes principalmente para o ISP. Como eu falei, a Huawei, ela já tem uma CPU defend muito agressiva. E aí como o próprio Giovaneli falou, na Juniper também precisa, na Cisco precisa você melhorar ou aumentar o threshold para que ele não ache que o PTT está atacando ele. Principalmente o PTT de São Paulo ou o do Rio está começando a fazer com que caixas Huawei achem que estão sendo atacadas. Então você ajustar alguns parametrozinhos aqui para que a caixa não fique achando que está sendo atacada, quando, na verdade, no PTT, é normal que o volume de broadcast ARP, o volume de network solicitation do IPv6 seja maior do que a caixa acha conveniente.

E um último lembrete aqui. Eu coloquei essas duas caixas, que são as caixas de borda, são as caixas multisserviço mais vendidas pela Huawei e que os provedores mais enxergam aí, que é o M8 e o F1A. Agora, o F1A também. Sempre respeitar os limites de funcionamento dos equipamentos. Por quê? A caixa é multisserviços, sim. Então eu posso subir BGP, PPPOE, MPLS na caixa? Posso. Devo subir em uma caixa de [ininteligível] MPLS? Aí a gente vai começar a discutir a arquitetura e a Live teria que ser muito maior. Mas ela vai fazer. Se você fizer arquitetura errada, ela vai aceitar, porque o protocolo vai funcionar, ela é uma caixa multisserviço. Agora, se o fabricante diz que essa caixa aqui faz 32 mil PPPOE e 4 milhões de rotas BGP, não queira fazer os 32 mil PPPOE e os 4 milhões de rotas simultaneamente na

caixa, e achar que ela vai responder com a velocidade que ela responderia você respeitando os limites. Trinta e dois mil é o máximo que a caixa suporta, 4 milhões é o máximo que a caixa suporta. Se eu misturar os serviços, é claro que esse máximo diminui um pouco, porque eu estou compartilhando funções da caixa com outros protocolos. No F1A, a gente sobe um pouquinho, são os mesmos 4 milhões de rotas na FIB, mas aí eu subo para 64 mil PPPOE, mas o lembrete também é o mesmo. Eu divido os recursos da caixa. Não é recomendado que eu use o volume total que ela diz que suporta. Tá?

Bom, acho que eu fiquei dentro do tempo. Um lembrete aí que eu vi, na apresentação, e eu reforço isso com o Huawei também, o que o Furtado falou. A Huawei, ela tem toda uma estrutura de empresas que ela cobra certificação, ela obriga que essas empresas tenham profissionais certificados, para dar um suporte de qualidade para o cliente final. Então, a gente vê muito que o equipamento... Como o Giovaneli falou, o pessoal procura aí no mercado cinza os equipamentos, procura no mercado paralelo comprar o equipamento. "Ah, porque é mais barato". Só que, na hora que ele precisa de um suporte, as empresas que são indicadas, as empresas que são parceiras da Huawei, elas têm a equipe técnica para te dar esse suporte, e se você procurar no mercado cinza, você vai ter que procurar o seu suporte também no mercado cinza. E aí o barato pode sair caro, e a sua operação pode ficar parada por algum tempo, sem necessidade. Às vezes só porque você economizou 5, 10% na compra do equipamento. Você ter uma operação parada pode ser muito mais caro. Tá bom? Obrigado. E eu fico aí para responder as perguntas mais tarde.

**SR. EDUARDO BARASAL MORALES:** Obrigado, Puppin. Realmente foi muito interessante. Vocês estão vendo aí, a gente acabou passando por vários roteadores e ainda falta falar do Mikrotik. Então, a gente já vai chamar uma pessoa para ser o especialista do Mikrotik e comentar um pouquinho aí do que vocês devem fazer nessa caixa para melhorar a eficiência.

Mas antes de eu chamar a próxima pessoa, eu gostaria de reforçar o aviso dos sorteios, porque algumas pessoas estão pedindo aí no chat. Então, lembrando, a gente vai ter o sorteio do NIC.br, junto com alguns patrocinadores. Então é um kit completo. O pessoal vai colocar o link aí no chat. Que é uma caneca da Icann, kit de acessórios de vinho da Cisco, um kit Moleskine, caneta da Logicalis, um voucher da Globoplay. Um livro Vida de Programador - Volume 0 e Volume 1. Temos a garrafinha de alumínio, uma caneta personalizada da Juni Link IP & Cloud Network da Giovaneli Consultoria. Tem a camisa polo da Semana de Capacitação. A lapiseira da Semana de Capacitação e um kit adesivos. Temos também o sorteio da Netfindersbrasil, que é uma vaga no curso do BGP, MPLS avançado em Huawei. Então, quem

quiser... Modo gravado. Um outro link para você se inscrever. Temos também o sorteio da Eletronet, que é voucher da Americanas no valor de 200 reais. Também é um outro link para você se inscrever, sorteio da Eletronet. Sorteio da GlobeNet Telecom, que é uma caixa de som acústica bluetooth. Então quem quiser, também pode se inscrever no sorteio de GlobeNet. Temos da Globo, que é voucher de acesso grátis também ali à Globoplay. Ao sorteio direto da Globo. E da FiberX e Huawei, que é um kit roteador match 5800. Tá, então. Esses são os sorteios que a gente tem. São seis sorteios. Por favor, quem quiser, se inscreva para participar, porque logo a gente já vai fechar e, depois, no final da live, vamos falar quem são os ganhadores.

Bom, continuando aí as apresentações, eu vou chamar nosso especialista em Mikrotik, que é o Wardner Maia. Maia, fique à vontade para você falar como aprimorar uma rede com esse dispositivo. Tá, então, o palco é seu.

**SR. WARDNER MAIA:** Olá, pessoal. Bom dia a todos. Em primeiro lugar, agradecendo aí ao convite do pessoal do NIC. É um desafio bem grande aí falar depois de todas essas feras aí, não só de conhecimento técnico e tal, e falando de equipamentos bastante poderosos. E vamos falar um pouco do Mikrotik que, na verdade, ele é um dos grandes responsáveis até, acredito eu, pela evolução do mercado de ISPs no Brasil. Nós começamos aí há muito tempo atrás um movimento de, digamos assim, libertação das grandes teles, e o Brasil é um mercado de ISPs que se difere praticamente do mundo todo, pela quantidade de pequenos ISPs que ele tem. E o Mikrotik, ele representa, tem representado durante esse tempo uma espécie de porta de entrada. Hoje, o mercado de ISPs está passando por um momento de bastante transformação, com a incorporação de grandes provedores, grupos se tornando maiores, e a gente vê com bastante satisfação que muitos daqueles que estão até comprando outros provedores, há bem pouco tempo atrás, tinham como solução quase única o Mikrotik.

Bem, os colegas que me precederam aí já disseram várias práticas que eu não vou... vou procurar não repetir e vou procurar focar naquilo que o Mikrotik se diferencia, as particularidades específicas do Mikrotik. Vou compartilhar minha tela aqui. Tá ok aí, pessoal? Bem, como roteiro aqui, a gente vai fazer uma pequena introdução, falar das boas práticas, vamos dizer, na largada, quando a gente começa aí, instala o Mikrotik. A questão de administração de usuário, senha. A própria segurança física. Algumas facilidades que o Mikrotik oferece e que podem, de certa forma, causar alguns problemas, algumas dificuldades. Vou falar um pouco de segurança de serviços e algumas boas práticas operacionais. Bem, como eu disse anteriormente, o Mikrotik, o RouterOS, ele é a porta de entrada para a grande maioria dos ISPs devido ao seu custo-benefício, devido à sua

interface amigável. Essa interface amigável, ela também é muito interessante que ela facilita muito o aprendizado daquele pequeno empreendedor que, às vezes, era dono lá de uma lan house, de alguma coisa e viu no mercado de provimento de acesso uma oportunidade de empreender e, então, começou com Mikrotik. E essa interface amigável, ela permite que a gente aborde conceitos complexos, como BGP, MPLS, protocolos complexos e de uma forma simples. E o Mikrotik é um verdadeiro canivete suíço, a gente... Porque ele tem praticamente tudo que a gente imaginar que a gente vai fazer em uma rede, desde a parte de wireless, a parte de BGP, a parte de MPLS, ele tem lá no sistema operacional. E as caixas, como... pela política da Mikrotik, toda caixa, independente da capacidade do hardware, ela vai com isso aí tudo. Então, eu consigo ter um hardware de baixo custo até para treinar a BGP, para ver como que funciona o BGP ou outros protocolos aí em um baixo custo. Como ponto negativo, eu citaria a escalabilidade. Os hardwares da Mikrotik, eles não têm, de certa forma, acompanhado as necessidades de banda, necessidades de volume de pacote que o mercado necessita. O próprio foco global, a Mikrotik é uma empresa que a gente pode dizer ainda, uma empresa pequena, um player pequeno, e bastante sintonizado com o mercado do Leste Europeu, que hoje tem um foco até maior ainda na parte de rádio e nem tanto de fibra.

Bem, mas falando em boas práticas na largada. A primeira coisa: escolher a versão correta do sistema operacional. As versões se dividem em long term, stable e beta. Embora o nome stable sugira que ela é mais estável, na verdade, a mais estável que a gente aconselha que seja escolhida é a long term, porque ela é versão que vai sofrer poucas alterações e não vai sofrer nenhum tipo de serviço novo. A stable já passa a ter serviços novos. A beta de forma alguma deve ser utilizada em produção. Então, primeira coisa, escolher sempre a versão long term. Um detalhezinho que muitas vezes passa desapercebido, quando eu instalo um Mikrotik novo, quando eu instalo o RouterOS ou quando eu faço um upgrade, é que existe o Boot Loader. O Boot Loader é programinha que roda antes e que carrega a versão do RouterOS para caixa. Esse upgrade, ele não é feito automaticamente. Quando eu faço upgrade de uma versão, o Boot Loader não é atualizado automaticamente, e isso tem que ser feito de forma manual, né? Eu... se eu digitar lá na linha de comando: system routerboard print, e eu encontrar ali o current firmware e o current firmware em versões diferentes, que pode ser também um downgrade. Se fiz downgrade na caixa, vou ter que fazer downgrade no Boot Loader e aí eu tenho que digitar: system routerboard para fazer isso. E exige um novo boot a cada atualização.

Pacotes. O Mikrotik, ele é... como eu disse, ele tem várias coisas, várias... serve para várias funções e, dependendo da finalidade da

minha caixa, eu vou instalar os pacotes necessários. Então, por exemplo, se ele vai ser um concentrador PPPOE, eu vou colocar lá o pacote PPP e mais alguns, como o NTP, que foi várias vezes citado aqui, que é importante que ele esteja ativo, a parte de segurança etc. Mas, de fato, é que, quando eu faço pelo pacote da Mikrotik, que é o pacote que já vem todos os pacotes combinados, quando a gente coloca, faz a instalação, normalmente, existem muitos pacotes desnecessários. Um pacote desnecessário, ele pode ser um problema. Ele pode ser um problema, tanto de segurança como de performance, porque é um pacote que está ali ativo. Então, o importante quando você tem um roteador é eliminar esses pacotes que você vai... se você digitar lá: system package remove, e o número do pacote você vai agendar para desinstalar esse pacote. Para desinstalar definitivamente vai ser necessário um boot na caixa. Então, o ideal: quando for instalar, se possível, já instale só com os pacotes separados, porque a Mikrotik oferece, lá no site dela, o pacote combinado, mas ela também oferece a possibilidade de você baixar eles em separado e subir somente aqueles que vão ser necessários. Lembrando que a qualquer momento você pode adicionar um pacote, quando, eventualmente, você esqueceu, no momento da instalação, é possível fazer isso sem necessariamente ter uma nova instalação.

Questão de usuários e senhas. Como a Mikrotik tem uma interface bem fácil ali de criar os usuários e senhas, a gente tem uma facilidade de criar ali, com acesso full ou com acesso só de leitura e tal, muitas vezes, a gente nota em muitos provedores, o pessoal cadastrar todos os funcionários lá que têm acesso nos Mikrotiks, cadastrar nessa base de dados. Isso é bastante ruim. Foi citado aqui, por exemplo, que, sei lá, você tem um funcionário que se desliga da empresa, você tem que entrar em todas as caixas e fazer... eliminar isso aí, né? Então, usar preferencialmente a autenticação via Radius, que é permitido pelo Mikrotik. Um momentinho só aqui. Estão pedindo para tirar a janelinha do Zoom aqui. Bem, então, evitar deixar usuários locais nos roteadores. Se for necessário mesmo cadastrar um usuário local, e principalmente quando a gente tem locais em que a gente não tem acesso físico, ou de difícil acesso físico, muitas vezes locais compartilhados com outros ISPs e tal, é importante a gente criar uma chave para uso do Mikrotik e garantir que só os notebooks que tenham aquela chave instalada possam fazer esse acesso. Nos slides aí está o passo a passo para você criar, fazer e criar esse usuário com acesso restrito. Se eu tenho isso aí, eu tenho uma garantia que ninguém vai acessar de forma local, possuindo um usuário obviamente, mas sem ter a chave.

Sobre segurança física. Houve uma época que os provedores, em grande parte, eram puramente rádio, e isso... existia uma grande parte dos equipamentos que ficam lá nas torres, que ficam nos topos de

prédio etc.. Muitas vezes o equipamento está na própria dependência do cliente, né? Importante desabilitar interfaces não utilizadas porque, como foi dito aqui, muitas vezes você tem o teu data center protegido, mas não tem parte da sua rede protegida, e uma interface habilitada pode significar uma porta de entrada para se fazer coisas que podem derrubar o seu provedor, como já foi citado aqui. Então, às vezes, ataques de camada 2 podem ser feitos. O Mikrotik, ele tem dois arquivos que eu vou citar aqui, que é o backup e o suppout. O backup, ele, muitas vezes, ele é gerado até automaticamente quando existe algum problema. Digamos assim, um upgrade, quando é feito o upgrade, quando é feito... quando cai a energia, por exemplo, quando existe um problema, é gerado esse suppout rif, que esses suppout rif é um arquivo que você pode gerar ele manualmente e mandar lá para o suporte da Mikrotik, caso você tenha algum problema. Esses dois arquivos, eles trazem informações importantes do hardware. Muitas vezes, eles trazem até os usuários e senhas. O backup, por exemplo, ele traz usuário de senha de acesso ao Mikrotik. Importante não ter esses arquivos. E como muitas vezes eles são criados até automaticamente, é importante que, na instalação, e aí é uma tela que feita por net install, você defina um script que verifique nos arquivos se eventualmente em todo boot... se existir um arquivo desse tipo que ele seja simplesmente eliminado. Até o LCD, o nosso LCD que alguns equipamentos da Mikrotik tem, ele pode ser um problema de segurança. Quando eu tenho ali um PIN que ele é por default 1, 2, 3, 4 e você tendo acesso, você pode adicionar o IP, você pode rebotar aquela máquina e você pode até resetar o roteador. Então isso... normalmente ele vem por padrão em brigde on, importante assegurar que ele esteja em bridge on. Mikrotik também tem facilidades que acabam podendo representar dificuldades. MAC-Server, por exemplo, o MNDP que é o equivalente ao CDP da Cisco, que são facilidades de gerência de rede, que acessa via máquina etc., que, dependendo do ambiente, dependendo onde você está, pode ser explorado para vários ataques aí de camada 2. A ideia é desabilitar esses serviços, desabilitar esses serviços sempre que possível. E existem também alguns serviços que, por padrão, estão desabilitados que a gente tem que, de vez em quando, dar checada lá se ninguém foi lá. Essa grande facilidade de gerenciar o Mikrotik, muitas vezes, ela representa aí um perigo. Muitas vezes pessoas sem muito conhecimento podem ter acesso e habilitar esses serviços. Esses serviços devem a todo custo serem mantidos desabilitados.

Sobre segurança dos serviços. Nós temos... se a gente pegar um Mikrotik 0 quilômetro, recém-instalado e rodar um NMAP nele, a gente vai encontrar aí as portas abertas, os serviços 21, 22, 80, 2000 e 8291. São os serviços que estão disponíveis no Mikrotik. Importante: desabilitá-los e mudar as portas default e restringir também o acesso a determinados endereços IP. O teste de banda, que é a porta 2000,

também ele vem por padrão habilitado. Nunca entendi direito porque isso, mas a gente deve sempre deixá-lo desabilitado. Aliás, até uma forma de você escanear... Encontrou a porta 2000 aberta, provavelmente é um Mikrotik que está ali naquele endereço IP. Rodando aí o OpenVAS para descobrir vulnerabilidade, ele descobre somente uma vulnerabilidade de severidade média, que é a criptografia. A criptografia forte, ela é desabilitada por padrão, e é isso que o OpenVAS mostra. Então, sempre que essa aplicação da caixa justificar, por exemplo, é um concentrador de VPN, uma aplicação mais crítica, a gente deve habilitar. Isso só se faz pela linha de comando, a criptografia forte. Bem, como eu falei, Mikrotik é um canivete suíço que serve para várias coisas. Mas um canivete suíço, geralmente, a gente não usa todas as ferramentas ao mesmo tempo. E um dos grandes erros que a gente nota, que já foi citado aqui também, que é você achar que aquele equipamento, porque ele tem a capacidade de ser um roteador de borda, mas, ao mesmo tempo, ele pode ser um processador PPPOE, por exemplo, ele pode fazer as duas coisas ao mesmo tempo. Poder ele pode, mas certamente não é uma prática recomendada. Roteador de bordo, é recomendado que seja só roteador de bordo, concentrador só concentrador. Firewall, apenas usar o firewall para a proteção da caixa em si, nas devidas caixas. Mas, se você tem firewall da entrada da rede total, é bom que ele seja também um equipamento em separado, e não vamos culpar os nossos Mikrotiks por decisões equivocadas.

Bom, pessoal, então era isso aí. Para não... Já até estourei um pouquinho o tempo aí. Me desculpa por isso. Sobre segurança em si, como é um assunto bastante extenso, então procurei resumir os pontos principais que, de certa forma, diferem dos outros equipamentos. Mas, nessas apresentações aí existe uma abordagem... nesses três links existe uma abordagem maior sobre segurança, englobando outras partes de segurança de roteamento, segurança de camada 2, MPLS etc.. Ok? Bom, pessoal, agradeço aí mais uma vez pela oportunidade, pelo convite. E estamos à disposição aí para eventuais perguntas.

**SR. ANTONIO MARCOS MOREIRAS:** Nós é que agradecemos, Maia. Excelente. Tem bastante perguntas, viu? Bastante perguntas o pessoal fez no chat, muitas sobre a versão 7 do Mikrotik. Vamos ver aí o que vai dar tempo da gente fazer. Eu vou chamar daqui a pouquinho o Paulo. O pessoal ficou falando aí. Da última vez que eu falei aqui, eu falei que tinha 300 pessoas assistindo, tinha quase 500 pessoas. Meu browser estava aqui estava precisando de um reload e na hora que dei, tudo funcionou. Apareceram os likes, apareceram as pessoas. Então eu fiquei mais feliz aí agora. Mas se quiserem dar mais likes, podem, não tem problema.

Antes de chamar o Paulo, eu quero só dar um aviso. Não quero deixar todos os avisos para o final. Eu gostaria de falar para vocês

sobre o curso BCOP, até porque tem a ver com o assunto da live. Apesar de que o assunto da live são boas práticas relacionadas aos equipamentos específicos, e a gente convidou especialistas nos equipamentos específicos para falar disso. E que é algo que a gente não aborda no curso BCOP, que também é um curso de boas práticas, mas são boas práticas mais gerais, relacionadas a como operar o BGP na Internet, como operar o BGP dentro de um PTT, no IX.br. E outras também relacionadas à segurança dos equipamentos, a hardware de equipamentos, RPKI, ao uso de IPv6. Então, a gente... há muito tempo a gente dá esse curso BCOP, a gente oferece esse curso BCOP e é um curso oferecido com os recursos do registro de domínios Ponto BR. Então é um curso oferecido hoje gratuitamente. E a gente começou já, vamos dizer assim, com uma semente desse curso quando a gente começou oferecer os cursos de IPv6, lá em 2008, porque dentro do curso de IPv6 tinha uma série de questões de boas práticas embutidas. E daí quando a gente transformou, depois, o curso IPv6 em um curso a distância, a gente acabou criando um curso só relacionado a boas práticas. Inclusive, trazendo algumas boas práticas de IPv6 para dentro desse curso também. E é um curso que não está estático. A gente tem ele há muitos anos, e ele vai sendo renovado. Então, há pouco tempo, por exemplo, a gente colocou o RPKI. Toda a questão de RPKI, laboratórios de RPKI. Os laboratórios vão sendo sempre renovados. Hoje, a gente usa o EVE-NG, a gente usa laboratórios baseados em Mikrotik mas também outras versões do curso tiveram laboratórios baseados em outras tecnologias. Isso pode ir mudando ao longo do tempo. De qualquer jeito, o que é importante no curso não é um roteador X ou um roteador Y, mas são as diferentes práticas que a gente aborda. Mas por que eu estou enfatizando isso? Porque quem fez o curso também há três anos atrás, há cinco anos atrás, há oito anos atrás (sic), pode valer a pena fazer de novo, porque a gente tem assuntos novos. Conforme outros assuntos vão ficando relevantes, por exemplo, o RPKI, o RPKI não era relevante para a gente há três anos atrás, há cinco anos atrás (sic), a gente não tinha suporte RPKI aqui no Brasil, na América Latina. Então, não dava para fazer. Hoje é super-relevante. Então, é um assunto super-relevante no nosso curso também, para colocar um exemplo de N exemplos diferentes que a gente poderia dar. Então, olha, gente, a gente tem as duas últimas turmas do ano abertas agora. Uma vai ser de 8 a 12 de novembro. E o último dia para fazer a inscrição nessa turma é hoje. Certo? E a gente tem uma outra turma de 22 a 26 de novembro. E as inscrições vão até dia 10 de novembro. Então, quero enfatizar isso. São 80 vagas em cada turma. Aproveitem o curso. Façam as inscrições. Alguém aqui que está no chat, que está acompanhando aí, está acompanhando pelo YouTube já fez esse curso BCOP? Diz aí para gente o que achou, se achou bom, se achou ruim, se foi interessante, não foi interessante, se recomenda ou não recomenda para os colegas que estão assistindo

aqui. Espero que vocês recomendem mas também se acharem que não, também podem ser sinceros e colocar aí no chat. A gente também ouve aí críticas construtivas. Que legal. Muita gente já fez e está recomendando.

Bom, gente, já perdi tempo aqui demais. O Paulo está esperando para falar. O Paulo, considero aqui que é da nossa equipe, do Ceptro, da equipe de medições, responsável pelo Simet, por outros projetos relacionados à medição de qualidade da Internet. E ele tem um recado para dar aqui, que é o lançamento de uma nova ferramenta, nessa linha de medições. Então, Paulo, por favor, o palco é seu. Fique à vontade aí.

**SR. PAULO KUESTER:** Bom, bom dia a todos. Em primeiro lugar, gostaria de agradecer ao Moreiras, ao Barasal, por esse espaço aqui para a gente estar falando um pouco sobre as iniciativas que também são do Ceptro e do próprio NIC, né? E acho importante destacar isso. Aos meus colegas painelistas, pelo excelente debate técnico de boas práticas ligadas às vendas de rede, e a você que está nos assistindo em casa. Então eu acho que é importante estar se alimentando de novos materiais, como o Moreiras comentou. A gente está sempre divulgando os nossos trabalhos, as nossas iniciativas e as iniciativas do NIC voltadas à sociedade. Vou compartilhar a minha tela.

Bom, vou começar a minha apresentação. Então, o intuito, o objetivo dessa apresentação, é falar um pouco dessa nova plataforma que o NIC está divulgando, que está lançando, de... como um apoio, no fundo, para identificar e mensurar uma Internet significativa. Eu vou comentar sobre a plataforma ao longo da apresentação. Mas aí ele se soma a outras iniciativas do NIC, no apoio, na melhoria, nas ações propositivas do ecossistema de Internet brasileira. Iniciativas essas como já foi comentado pelo Moreiras, nesses cursos de capacitação técnico-científicos, voltado ao pessoal de provimento de acesso, iniciativas como a que o Barasal já comentou, do Cidadão na Rede, que é importantíssimo, do ponto de vista de conscientização dos usuários, e as iniciativas, lógico, que se somam a outras, dentro do NIC. Então, eu convido vocês também que já conhecem ou não conhecem ainda o NIC, a visitar o site do NIC, a se alimentar desses materiais, e são muitas ações, todas elas voltadas à sociedade de maneira gratuita.

Começando aqui a minha apresentação, eu tenho 15 minutos, de 15 a 20 minutos. Vou estruturar em alguns tópicos. Em primeiro lugar, eu vou comentar um pouco sobre a área de medições, a importância de medir, como medir. Depois, vou comentar um pouco sobre o portal de medições, que foi lançado em junho deste ano, e de como ele concentra as iniciativas de área de medições. O terceiro, o lançamento da plataforma a Internet que preciso, que é o foco e objetivo maior dessa apresentação. E comentar um pouco sobre outros projetos,

dentro da área de medições, do Simet AS e o Simet ISP. No final, vou resumir tudo isso, trazendo alguns destaques e mensagens para vocês levarem para casa. E é isso, os tópicos dessa apresentação serão esses.

Bom, vou começar a apresentação falando dos usos de tecnologia. Acho que a tecnologia vem mudando bastante, ao longo dos anos. A gente se alimentava dela de uma maneira mais simples. No passado, basicamente, navegando na Internet. Mas isso vem mudando, tanto do ponto de vista pessoal, você utilizando na sua residência, na sua casa, quanto do ponto de vista profissional e da educação, né? E acho que é importante destacar que a tecnologia, ela permeia todos os aspectos da nossa vida, hoje. Então, assistimos aulas on-line, usamos smartphones com os mais diversos aplicativos, para os fins mais diversos possíveis. Nos alimentamos de vídeos de streaming, para entretenimento ou não, para outras ações, jogamos on-line, antes os jogos eram off-line, mas, hoje em dia, há opção de você, há um bom tempo, conseguir jogar on-line, isso demanda uma qualidade de serviço, participamos de reuniões, lives etc., como essas que estamos aqui hoje, além de compartilharmos ou conversarmos com as pessoas por meio de redes sociais. Então, para que a gente consiga dar conta dessa miríade de usos de tecnologia, a área de medições já vem há mais de dez anos se debruçando para poder entender um pouco sobre a qualidade de banda larga fixa e móvel, por meio do que vocês já conhecem mais, que são os medidores da família Simet. Comentando um pouco das iniciativas e comentando sobre o recente portal que foi lançado, o portal de medições aqui do NIC.br. Então, ele é um portal que foi lançado em junho desse ano, visando justamente concentrar as diversas iniciativas, os medidores, as aplicações, o trabalho que a gente vem realizando ao longo desses anos. Ele é um portal pensado para três públicos distintos. É o público consumidor final, onde ele pode avaliar a qualidade da sua própria banda larga, e acompanhar isso e visando ali entender um pouco os usos que ele tem. Os provedores, acho que muitos de vocês que estão participando aqui fazem também uso das nossas aplicações, dos nossos medidores. E aplicações voltadas ao provedor, para que ele possa entender a qualidade, como que está a qualidade da dentro da sua própria rede, e atuar de maneira preventiva, às vezes. Não esperando que o usuário entre em contato ou, enfim, você tenha algo mais reativo. E a gente vem desenvolvendo essas ações com diversas aplicações também voltadas para o provedor. E, por fim, o setor público. A gente cresceu bastante, principalmente nessa época de pandemia, em ações voltadas para a área de educação, onde a gente já acompanha a banda larga em 47 mil escolas públicas pelo país. Os dados são públicos, eles são alimentados... alimentam o portal, que depois a sociedade se alimenta deles, o MEC, gestores estaduais, municipais, sociedade, jornalistas etc. Então são ações voltadas ao

setor público e começamos um projeto recente com as unidades básicas de saúde também. Onde, de novo, os medidores gratuitos, ofertados à sociedade, podem avaliar condição de banda larga nessas instituições públicas.

Bom, esse é o Portal de Medições. Eu convido vocês depois a anotar URL, visitá-lo. E lá temos as nossas ações. Eu não vou ter tempo de comentar sobre todas. Os agentes de medição. Os agentes da família Simet que vocês já conhecem. Então, são agentes desenvolvidos gratuitamente, de novo, para a sociedade, para os dispositivos móveis, por exemplo. O medidor para android, recentemente lançado, onde permite que você avalie instantaneamente. Quando eu digo instantâneo, é porque o usuário clica, ele não é uma periódica, que existem em outros tipos de medidores, e ele faz a avaliação da banda larga fixa e móvel, além de testes da rede Wi-Fi local. Ele está disponível na loja do Google para vocês baixarem. Medidores voltados para o desktop, notebook, roteador. Roteador, o Simet Box, acho que é conhecido de boa parte de vocês. Temos tentado angariar novas parcerias, novos fabricantes para poder expandir aí o leque de sistemas suportados, baseado em OpenWrt. O site do GitHub está aqui disponível para que vocês consigam não só verificar o código mas também participar desse projeto, então, contribuir com ele. Então, você não precisa ser só um espectador. Eles são medidores de medição periódica e, como disse, tanto o Simet Box para o roteador quanto o Simet MA para Linux, você consegue fazer essa avaliação da banda larga fixa. E o código é aberto, como eu comentei. E, por último, o medidor web. O Simet Lite. Ele permite fazer a avaliação instantânea. O usuário vai lá e clica. E aí você consegue avaliar as duas famílias de IP, IPv4 e IPv6, sem necessidade de qualquer instalação. Então basta você apontar o site e fazer essa avaliação da qualidade da sua banda larga. Então esses são os nossos instrumento de coleta. Mas eles são importantíssimos, fundamentais, mas eles alimentam todo um ecossistema de tratamento de dados e depois de publicar os dados no portal, nas aplicações. Então a gente conta com o apoio de vocês para incentivar, engajar o uso. De novo, são ações voltadas para vocês e para a sociedade, de maneira gratuita.

Aqui é um pouco sobre a cobertura hoje do Simet, dos medidores. Então, a gente, já no ano de 2020, aqui o recorte, são 27 milhões de medições únicas. E estou falando de medições, não de métricas. Se falasse de métricas, isso explodiria para mais de uma centena de milhões. E a cobertura municipal, já estamos presentes hoje em 5.455 municípios, com pelo menos uma medição. Então, daí o mapa aqui do lado já dá a ideia da nossa representatividade geográfica, são pouquíssimos locais onde hoje o Simet não está presente. Mas queremos crescer ainda mais, na representatividade, em níveis geográficos menores, como o setor censitário, por exemplo, que

é uma subdivisão do distrito. Então, aí eu conto com vocês de novo para poder incentivar e esses dados, de novo, estão a favor da sociedade. E os sistemas autônomos. Então, já temos, hoje, pelo menos uma medição, 7.525 sistemas autônomos brasileiros. Acho que é um pouco do cenário do que temos hoje. De novo, recorte só de 2020.

E aí eu vou falar um pouco da plataforma. Acho que o objetivo maior aqui, hoje, é lançar essa plataforma, essa aplicação, conhecida agora como internetquepreciso.nic.br, que você pode acessar, e vou comentar de como ela está estruturada, de como ela foi concebida, planejada, pensada, para você que está na sua residência mas também para o provedor. E aí a gente estruturou essa plataforma em três diferentes áreas. A primeira, acho que a mais simples de eu explicar, é como medir e avaliar sua conexão. Aí você pode clicar em medir e, por meio do Simet Lite, que está embarcado na própria plataforma, você faz uma avaliação da sua conexão, e, embaixo, tem um quadro com usos, para que você consiga contrastar: "Qual é o uso que eu tenho com aquilo que eu estou recebendo de provimento". Bom, enfim, de conectividade. A segunda caixa, que está listado aqui no meio, é: "Descubra o quanto de Internet você precisa". Então, uma revisão bibliográfica extensa que fizemos, uma metodologia bem pensada e planejada, ele visa, baseado em alguns critérios que vou comentar depois, gerar uma calculadora que diz, baseado em tudo aquilo que você preencheu no formulário, o quanto ele estima de banda que você precisaria, um limite mínimo. Então, essa é a segunda caixa. E a terceira é: "Veja os provedores da minha área". Então, clicando ali, vai tentar te geolocalizar. A aplicação pede que você compartilhe a geolocalização, mas respeitamos a privacidade, só para avaliações estatísticas, então fiquem tranquilos. Respeitamos a LGPD por princípio. Então clicando lá, você vai verificar a sua localidade, os provedores que atendem aquela região e a qualidade de Internet naquela região. Então, eu vou explicar um pouco disso depois, mas vocês já têm o site. Tem um QR Code aqui, para que vocês consigam, depois, participar desse projeto, porque, além de listar os provedores, queremos divulgar também o canal de contato. Então, para vocês, pequenos e médios provedores, imagino que isso seja importantíssimo, que a ação vai ficar pública, os consumidores vão utilizar, então eles vão ter acesso a quais provedores estão atendendo aquela região. Imagino que esse ecossistema se retroalimente. Então, por favor, nos ajude a divulgar e participem dessa iniciativa.

De maneira muito breve, como comentei há pouco, na área do "Medir sua Internet", existe o medidor de Simet Lite, embaixo um quadro com os usos e as métricas, listando um pouco quais são os limites. Essa não é a métrica só sugerida, é uma métrica limite, na verdade, uma avaliação média para que você consiga entender qual é

a demanda de um serviço de áudio, do uso geral de Internet, de um download, de um jogo on-line e de serviços de vídeo. Então, é basicamente o que temos aqui.

Vou passar para a próxima. A Internet que preciso. Então, a calculadora de banda, ela é baseada em alguns conceitos. Então, "o número de usuários na sua residência", "qual é o número de usuários de uso intensivo", ou heavy users. Então, você preenche isso como um primeiro critério para a fórmula. Depois, "qual é o número de dispositivo e qual o tipo deles". Então, a gente tipificou os dispositivos e, depois, deixou que você liste a quantidade deles, para poder calcular também isso de forma adequada. E, por último, "qual uso eu faço da Internet". Lembrando, eu faço uso geral? Eu faço uso de streaming, de jogos? Eu faço múltiplos usos? Então a calculadora também, por meio de um processo de somatória, ele tenta dar conta de tudo isso. Então essa é a segunda caixa, a segunda área dentro da aplicação Internet que Preciso. Por último, a área dos provedores. Então, lembrando, ele tenta geolocalizar... bom, tenta te geolocalizar, à medida que você acessa a plataforma. Ele pergunta se a localização está correta. Se não estiver, ele tenta te dar a opção de digitar o CEP e aí ele lista os provedores na sua região. A partir disso, ele verifica quais são as atividades possíveis de desenvolver com a qualidade para aquela região. E a região, estou falando de setor censitário, que é a menor unidade administrativa reconhecida pelo IBGE. Depois disso, na última coluna, ele permite você destrinchar as métricas de qualidade. A gente discretizou as variáveis quantitativas aí com faixa de velocidade, no caso da métrica de download mas também temos métrica de latência e perda de pacotes, isso tudo baseado em frame internacional da OCDE.

Por último, vou comentar de maneira mais breve agora porque eu acho que já estou um pouco estourado no tempo. Mas temos duas iniciativas importantíssimas para você, provedor, que é o Simet ISP, que é a possibilidade de realizar essas medições dentro da rede do provedor e no IX.br. Então, ele é composto de dois componentes, são máquinas virtuais. O Simet-MP, o peer de medição, onde ele é responsável pelos testes de qualidade, e o cliente terá opção de medir também contra a rede do provedor mais no IX.br como já realizamos. E o Simet AS responsável pelos testes de interconexão nos ASs. Então, se você tem um Simet AS e o outro também tem, participante, você consegue realizar os testes de RTT, enfim, de [ininteligível], de latência e de perda de pacotes entre esses participantes, dentro do IX. As premissas para o projeto: ter um ASN, estar conectado direto ou indiretamente em qualquer localidade do IX, ter um hypervisor, os mais conhecidos de mercado estão aqui listados aqui, e para cada virtual machine que... para cada máquina virtual ter pelo menos um IPv4 e IPv6 com conectividade com AS do NIC, 22548, e os clientes, e

por fim, recursos físicos de CPU, RAM e rede que são escritos no manual que a gente, de novo, compartilha com vocês, quando vocês se cadastrarem na iniciativa. Deixo aqui também o QR Code listado.

Para terminar, estou finalizando minha apresentação, vou deixar algumas mensagens. A importância dos medidores da família Simet para o mapeamento de indicadores de banda larga no país. São medidores importantes para você, consumidor, para você, provedor, para você, setor público, mas ele alimenta todo um ecossistema de dados, tanto dentro do NIC quanto para fora dele, para poder investigar, analisar, correlacionar essas investigações da tecnologia da informação e comunicação, com diversos aspectos da sociedade. E ressalto aqui a importância das pesquisas TIC do Cetic. Segunda iniciativa... São iniciativas importantíssimas para apoiar a comunidade, e aí apoiar com os medidores, com as aplicações, como eu comentei, isso tudo de forma gratuita. É um trabalho imenso realizado aqui dentro do NIC, mas voltado para vocês. Terceiro, acho que temos desenvolvido essas soluções com três públicos distintos: consumidor, provedores e setor público, e contamos com o apoio de vocês para divulgar as nossas ações e as nossas iniciativas. E aí termino a minha fala. Gostaria de receber o feedback de vocês e agradeço.

**SR. EDUARDO BARASAL MORALES:** Obrigado, Paulo. Realmente muito interessante tudo o que você falou. Já veio algumas perguntas direcionadas aí para você, perguntando sobre o Simet. Mas vamos fazer agora a nossa rodada de perguntas para todos os painelistas. Então, pessoal, podem escrever no chat, a gente está lendo as perguntas e está selecionando elas para fazer para os nossos painelistas.

Eu vou começar com uma outra pergunta. Não vou começar com a pergunta do Paulo, porque ele foi o último a apresentar. Vou começar com uma outra pergunta, até relacionado ao que o Moreiras estava comentando sobre o curso BCOP. O Elvis Candido perguntou: "O curso é gratuito?". Sim, o curso BCOP é gratuito. Pode se inscrever, não tem nenhum custo. O que gente espera, pessoal, é que vocês não faltem, uma vez que a gente chama vocês para participar do curso, lembra, tem uma seleção. A gente chama ali 80 alunos, mas se inscrevem 300, 400, 500 pessoas. Então, aqueles 80 que foram selecionados participem do curso. Por quê? Porque senão você está roubando a vaga de outra pessoa que gostaria de participar do curso. Então, o curso é gratuito. Teve também uma pergunta aí do David Assis Monteiro: "Por falar em LGPD, o NIC vai ter cursos voltados nessa área?". Uma coisa que posso te dizer é que a gente teve uma Intra Rede voltada à essa questão de LGPD e outras mais jurídicas. Então entra lá no canal do NIC.br, vê a live do Intra Rede sobre esse assunto, pode também olhar no próprio site do Intra Rede tem essa informação. Então, a gente trouxe especialista para falar de LGPD ali nas redes. O que o provedor

precisa fazer, o administrador de redes precisa fazer. Assiste lá que ficou bem interessante.

Pergunta agora, né? Veio uma pergunta do Solistik, para o Leonardo Furtado, que vou acabar estendendo para todos os painelistas, porque é pergunta muito interessante. Ele perguntou sobre a virtualização dos serviços na mesma caixa. Então queria pensar ali em todos os roteadores e todos os especialistas. Como que vocês enxergam isso, de muitos serviços na mesma caixa, virtualizando, rodando containers? Ou separar os serviços em caixas diferentes é melhor? Do que depende essa decisão, quando chega na mão do administrador de redes? Se o fabricante influencia nisso. Vou chamar na ordem e gostaria de ouvir a opinião do Giovaneli, o Alexandre Giovaneli falando aí de Juniper nesse quesito. Então, fica à vontade.

**SR. ALEXANDRE GIOVANELI:** Bom, sim e não. Não, porque, assim, a gente, primeiro, analisa a topologia de rede. Se você tem dois equipamentos iguais, idênticos, sim, você pode rodar tudo em um único equipamento. Se esse equipamento falhar, o outro roda todo... e roda todo o serviço em outro equipamento. Os dois podem ser idênticos, sem problema nenhum. Desde que respeite os limites do equipamento. Tem equipamentos que suporta que rode todos os serviços e tem equipamentos que não. Vai depender do modelo, do tipo de controlador ou do equipamento, se é redundante ou não, se o próprio equipamento é redundante ou não. Então, assim, modelos, supondo que você tenha dois MX 204 em sua rede, você pode fazer isso. Suponhamos que você tenha um único MX 960 com componentes redundantes, sim, você poderia fazer. Nesse cenário, sim. Entendeu? Então seria, de uma forma extremamente superficial, da minha parte.

**SR. EDUARDO BARASAL MORALES:** Tá certo. Muito obrigado. Vou passar agora, então, para o Leonardo Furtado. Até a pergunta foi direta para ele. Leonardo, fica à vontade.

**SR. LEONARDO FURTADO:** Estou muito à vontade. A pergunta do Solistik, eu acho que sei quem seja Solistik. Mas vamos lá, vamos dar uma moral aqui. Na linha do que o Giovaneli comentou, procede. Você tem família de produtos que foram projetadas para missão multisserviço. Vamos dar exemplo de Cisco, famílias SR 1000. Se você adquirir um produto desse, fazer um projeto com SR 1000 obviamente, você, ali dentro, de acordo com as especificações de capacidades, chamamos de figuras de escalabilidade, quantas sessões simultâneas de PPPOE, quantas traduções máximas de CGNAT concorrente, a taxa de novas sessões por segundo e a largura de banda por comutação, quantidade de [ininteligível], quantidade de peers, BGPI, etc. O [ininteligível], ele foi projetado para uma missão de serviços. Então você pode colocar aquele camarada, modelo 1001 X, 1001 HX, 1002 HX, 1006 e por aí vai, você tem os diversos modelos dessa família que

por perfil do provedor regional brasileiro são excelentes. Há cases, cases, cases dessa solução rodando com múltiplos serviços. Agora, o que você deve fazer? Certifique-se de projetar ou de selecionar o modelo, ou equipamento, ou arquitetura que vá de encontro com suas figuras de escalabilidade. Então, voltando ao tema da minha apresentação. Você tem que compreender exatamente o que você está comprando. Agora, o ar é importante. Você não vai centralizar toda tua empresa em um único equipamento. Pelo amor de Deus, não faça isso. Para isso que nós chamamos de diagrama de bloco de confiabilidade. Então, você tem que compreender. Talvez você queira ter uma arquitetura centralizada muito redundante, e você tem protocolos, por exemplo, para [ininteligível] que foi falado no minicurso do PPPOE aqui no NIC.br, ou BNG Geo Redundancy e outros procedimentos para você maximizar a disponibilidade do ambiente. Você não vai querer centralizar todo teu negócio em uma única caixa. Ninguém é doido. Enfim, dá para fazer. E por mais, também, vários equipamentos são... já suportam containerização, ou seja, você hospedar múltiplas aplicações, inclusive, que não têm nada a ver com roteamento, em cima da mesma caixa. Tudo depende se o equipamento suporta essa arquitetura, ele foi projetado para essa missão multisserviços e respeitando teu projeto técnico, em particular, aqui a área de disponibilidade e a confiabilidade do ambiente. Então essa é a minha contribuição aqui, tá, Morales? Espero ter atendido aí as expectativas. Caso não, pode refazer a pergunta ou evoluir pouquinho mais ela. Espero ter ajudado.

**SR. EDUARDO BARASAL MORALES:** Então tá certo. Ajudou bastante. Bom, seguindo aí, vamos chamar agora o Luiz Magalhães, também conhecido como Puppin. Puppin, fica à vontade. Como você enxerga essa questão de virtualização, de todas as coisas estarem dentro de uma caixa só. Ou você deve repartir em várias caixas? Fique à vontade.

**SR. LUIZ COMES PUPPIN MAGALHÃES:** Bom, eu cheguei, na minha apresentação, eu cheguei a comentar sobre isso. Eu acho que existem caixas multisserviços, como o Furtado falou. Na Cisco existem as caixas multisserviços, na Huawei também, o NE800M8 e F1A, eles são caixas multisserviço. Só que aí eu preciso sempre ter em mente a minha arquitetura. Não é porque a caixa é multisserviço que vou colocar o PPPOE e o BGP dentro da caixa, deixar aquela caixa na borda e vou fazer [ininteligível] como PE de MPLS, como eu já vi muita gente fazendo. A caixa vai funcionar, dependendo de quanto de carga você consumir, ela vai funcionar perfeitamente. Agora, arquitetura, falando da arquitetura, é correto o meu BGP de bordo, ele ficar... ele funcionar com o PE da minha rede? Falando em MPLS, dentro da minha rede. Aí a gente já entra em um desenho de arquitetura, que aí o Furtado falou muito bem na apresentação dele sobre você planejar a sua rede antes

de implementar. Eu concordo plenamente que os provedores pequenos e médios, que não tenham o volume de assinantes absurdamente alto, você comprar uma caixa para cada coisa acaba onerando demais. Então, eles acabam utilizando dessas facilidades do multisserviço, sim. Não vou dizer que não vai funcionar, mas os cuidados com o desenho da arquitetura a gente precisa. E, principalmente, os cuidados que a gente tem que ter de segurança nessa minha rede e a segurança nessas caixas, que vão fazer mais de uma funcionalidade. Segurança também quer dizer redundância. Mais uma vez, eu não posso colocar tudo... colocar BGP, PPPOE e botar uma caixa só para fazer isso. Se eu colocar com redundância e aceitando os limites de funcionalidades, eu não vejo problema nenhum.

**SR. EDUARDO BARASAL MORALES:** Tá certo, Puppin. Muito obrigado. Agora vou chamar o Maia para complementar esse assunto. Maia, qual é a sua visão?

**SR. WARDNER MAIA:** Bem, como eu disse, o Mikrotik, por padrão, ele roda tudo o que você pensar de uma rede, mas, de forma alguma, a gente aconselha que isso seja feito, né? A não ser em um ambiente muito pequeno. Então, eu... tem muito pouco tráfego, muito poucos usuários. Eventualmente eu posso, por uma questão de economia, sei lá. Ou dá um PPPOE e um BGP na mesma caixa. Mas é extremamente desaconselhável que isso seja feito. Se você recordarem, inclusive, o meu primeiro ou segundo slide, eu falo de uma certa limitação de hardware que a Mikrotik tem, que não acompanha as necessidades de provedores médios, aí. De... né? Então, de forma alguma, a gente aconselha essa... rodar serviços diferentes na mesma caixa. Com relação à virtualização especificamente, a versão 7 do Mikrotik, que ainda é experimental, não deve ser usado em produção, ela suporta Docker, que é uma novidade aí, que pode ter alguma solução criativa. Você rodar isso dentro do próprio Mikrotik. Mas apenas para comentar, uma vez que, como eu disse, a V7 ainda é experimental e não deve ser usada em produção.

**SR. ANTONIO MARCOS MOREIRAS:** Muito obrigado. Muito obrigado, Maia. O Alexandre Carvalho comentando no chat lá: "Evento de alto nível, muita informação relevante". E eu também concordo com isso. Muito legal. O Paulo está pedindo aqui que quer fazer um comentário. Não, não, é depois. Eu que estou viajando na maionese. Eu estou olhando aqui o nosso chat interno, estou me perdendo. Desculpem aí. Bom, eu estava dizendo aí do comentário do chat que o evento está sendo relevante. O evento está sendo muito bom. Também estou achando. Também aprendi muita coisa aqui com o pessoal. E eu quero já convidar vocês para colocar na agenda a data do próximo evento. O próximo Intra Rede vai ser no dia 15 de dezembro. Vamos falar sobre padrões, sobre novas tecnologias, mas, antes desse próximo Intra Rede, no dia 15 de dezembro, a gente tem também a

Semana de Infraestrutura, que esse ano ainda vai ser on-line. Esperamos que o ano que vem a gente retome os eventos presenciais, mas esse ano a Semana de Infraestrutura ainda vai ser on-line. Temos o GTR, o GTS e o IX Fórum. Isso vai ser dia 29... desde 29 de novembro até 3 de dezembro. O IX Fórum vai ser dia 1, 2 e 3 de dezembro. Então estamos preparando um evento bem legal. Tivemos chamada de trabalho, tem bastante propostas interessantes, estamos preparando a agenda. Logo, logo, talvez a semana que vem aí a gente tenha uma primeira versão da agenda publicada. Mas coloquem aí já no calendário de vocês, na agenda de vocês, reservem as manhãs, pelo menos, de 29 de novembro a 3 de dezembro, para acompanhar a Semana de Infraestrutura.

E vamos voltando aqui para as perguntas. Temos uma pergunta, que foi feita pelo Leonardo Mesquita, no chat. E ele perguntava da certificação de entrada para Huawei. Mas eu quero generalizar essa pergunta. Eu queria que os nossos painelistas respondessem, falassem sobre certificações em geral. Então, por equipamento no qual você é representante, caro painelista, existe uma certificação disponível? Tem uma certificação para Huawei, para Cisco, para Juniper, para Mikrotik? Como funciona essa certificação? Como que alguém, um profissional pode estudar para essa certificação? Qual é a melhor maneira? Essa certificação é uma certificação que dá realmente condições para o cara trabalhar no mercado? Se o cara tiver certificação, eu tenho certeza que o cara vai conseguir lidar com aquele equipamento e fazer configurações e trabalhar no mercado? O mercado valoriza essa certificação? O que vocês conseguem falar para a gente das certificações específicas aí dos equipamentos com que vocês trabalham, vocês são especialistas? Giovaneli, você consegue comentar isso para gente?

**SR. ALEXANDRE GIOVANELI:** Bora agora. Vamos lá. A certificação inicial da Juniper a gente considera o JNCIA-JUNOS, só que depende muito da trilha que você vai seguir dentro do fabricante. Eu tenho trilha de automação, de cloud, data center, de desenho de redes, de enterprise, de wireless, de segurança e também de service provider. Tratando do track específico, que é a trilha de conhecimento que a gente fala de treinamento, a gente tem a de service provider routing e switching, que é mais usado pelos provedores. Então começa com o diretório JNCIA-JUNOS. Então, eu tenho o todo conteúdo na Internet para poder treinar, para poder fazer o treinamento dessa prova, e, inclusive, boa parte desse conteúdo, vamos dizer, de 60 a 70% do conteúdo dessa prova, ele é ensinado já nos cursos de BCOP e nos cursos da própria NIC.br, conceito de IPv6, IPv4 que é a prova inicial. E você tem as certificações mais avançadas, especialista, profissional e expert. Então, inicialmente, é o JNCIA-JUNOS. Fazendo o curso da NIC.br, você já tem uma baita de uma base de conhecimento para

poder estar realizando essa prova. E a prova, você pode marcar pelo portal da própria Juniper. Juniper Learning portal. Você pode digitar no Google e é feito pela Pearson, é a empresa que faz essa certificação aí do pessoal. O próprio Portal da Juniper, Juniper Educação, você digitar no Google, já vai ter todos os passos lá.

**SR. ANTONIO MARCOS MOREIRAS:** Obrigado, Giovaneli. Leonardo, você pode comentar?

**SR. LEONARDO FURTADO:** Claro, posso comentar. Assim, é muito... novamente aqui ao vivo... o programa de certificações da Cisco acho que dispensa apresentações. É o mais consagrado, mais abrangente programa de educação na área de tecnologia de redes do mundo, não desmerecendo, não desrespeitando os programas de certificação dos demais colegas, dos fabricantes, mas a verdade é que a Cisco, ela foi um divisor de águas nisso aí. Tem uma certificação de entrada que é o CCP, que é [ininteligível], o certificado Cisco, que ali para o cara que está muito... ele é muito cru em fundamentos de rede, não conhece como as redes funcionam. Mas o que entendo ser a certificação porta de entrada é a certificação CCNA da Cisco. Eu recomendo demais. O profissional que está começando, isso falo por experiência própria. Muitos profissionais que hoje lidam, inclusive, com sistemas autônomos, em ambientes aí com interação frequente com pessoal do NIC, tal, o cara não tem a menor ideia do que ele está fazendo. Ele reproduz uma configuração, ele reproduz uma [ininteligível], mas ele não compreende o básico, como é que funciona uma comunicação L2, um roteamento, tal. Nessa seara, CCNA é espetacular. Então a minha recomendação, você pode procurar no site da Cisco. Pode procurar no Google: Cisco Training & Certifications. Bota lá. Vai cair na página. Tem um PDF lindo que vai descrever todas as verticais de certificação. A exemplo do que Giovaneli falou, tem o enterprise, service provider, segurança, a parte de cyber ops, data center e, agora, DevNet. Então a porta de entrada é o CCNA, recomendo demais. Inclusive, vou até fazer um convite aqui para aproveitar o espaço do NIC.br. Nesse exato momento, estou conduzindo gratuitamente uma formação CCNA que começou com 879 alunos pelo programa Cisco Network Academy, pela MC Academy do meu colega Marcelo [ininteligível]. Você pode me caçar lá no YouTube, Leonardo Furtado, Cisco, por exemplo, você vai encontrar meu canal e lá tem uma playlist bastidores da formação e você pode se inteirar do que é o projeto. Ele é muito ousado e vai abrir uma nova turma agora, no segundo curso, já em... na segunda, terceira semana de novembro. Pode... você pode solicitar pleitear a participação, gratuita, obviamente. E, cara, isso que eu tinha que falar.

Faz isso, por favor. Pode, pode, pode. Faz isso, por favor. E, cara, recomendo. Certificações de entrada. Domínios, fundamentos, saiba como as redes funcionam nos seus aspectos mais básicos, que é o

ICMP, o que é TPC, o que é UDP, o que é Ethernet, enfim. Isso o CCNA da Cisco, ele é extremamente funcional e permite com que você consiga lidar com as soluções da Cisco, enfim, VLAN, fazer um roteamento. Isso você vai conseguir usar na prática. Agora, depende muito do teu cargo que você ocupa na companhia. Tu é um júnior, tu é um NOC, tu é um engenheiro, tu é um pleno, tu é sênior n1, n2, n3. Aí, por exemplo, você vai para posição n3 e você não manja de redes, esse CCNA, ele será insuficiente, óbvio. Então, para isso que você vai evoluir na pirâmide de certificação da Cisco, por exemplo, CCMP. E dá para... Alguma pergunta que eu vi aqui. Dá para ir direto também. Você não precisa mais fazer CCNA para ir para o CCNP. Pode tentar o CCNP direto. Espero, novamente, Moreiras, e Morales, a dupla MM aí, ter ajudado vocês aí. Permita-me saber, por favor. E desculpa aí pela demora, mas é o meu padrão de discurso é esse aí. Valeu.

**SR. ANTONIO MARCOS MOREIRAS:** Eu não posso reclamar de comentários longos. Eu não tenho moral para reclamar disso, né? Então, vamos chamar agora o Puppin. Puppin, você pode comentar?

**SR. LUIZ COMES PUPPIN MAGALHÃES:** Bom, eu acho que posso comentar. Eu sou gerente de training center. Então, acho que eu preciso responder isso aí. Bom, a Huawei, ela tem todo um ecossistema de certificação. A Cisco e a Juniper possuem as certificações baseadas em data centers, service provider. A Huawei segue o mesmo caminho, que, no caso da Huawei, seria o HCIA Datacom, HCIP Datacom, HCIE Datacom, que seria o antigo routing switching. O routing switching vai deixar de sair agora até o final de ano. Ele está sendo substituído pela linha de certificação de Datacom. Mas, como eu mostrei lá também na minha apresentação, a Huawei tem uma gama de soluções diferenciadas. Então, eu tenho HCIA de cloud services, eu tenho HCIA de 5G, HCIA de LTE. Eu tenho em cada área, DWDM, tenho HCIA, HCIP e vai vir o HCIE de DWDM, eu tenho HCIA, HCIP e também virá o HCIE de Gepon, de FTT. Então, a Huawei tem todo um ecossistema que engloba as certificações no mesmo padrão que todos os fabricantes. A para o nível de entrada, P para o profissional e E para o expert, que aí você vai crescendo na pirâmide de certificações. Cada nível de certificação para um nível de conhecimento, dentro da empresa. Tá bom? Para o service provider, as certificações de Datacom são as mais indicadas, e aí talvez de security, que fala de firewall ou de WLAN, que vai falar de Wi-Fi, poderiam ser interessantes também, tá?

**SR. ANTONIO MARCOS MOREIRAS:** Legal, muito bom. Tem gente comentando no chat, lá, que vai fazer agora a CCIE direto, CCNP direto, depois dos comentários do Leonardo. O pessoal está animado. Mas é isso mesmo, tem que buscar certificações, buscar conhecimento. Maia, você pode comentar em relação à Mikrotik, como que é isso?

**SR. WARDNER MAIA:** É, a linha de certificação da Mikrotik, ela cresceu bastante nos últimos tempos. Houve bastante investimento, e hoje tem várias linhas. Se não me engano, se não me falha a memória, 14 diferentes certificações em diferentes áreas. Normalmente, o ISP, ele tem a entrada, que é o MTCNA, seria o equivalente ao CCNA da Cisco, mas voltado mais ao Mikrotik, e as certificações mais ligadas a roteamento, que é o MTCINE, MTCRE, em que se vê coisas mais ligadas aos provedores. Diferentemente de outros fabricantes, a Mikrotik, ela tem uma política que é necessário fazer o treinamento presencial e o exame para certificação, ele é feito... embora seja remoto, seja via web, mas é feito presencialmente. E nós temos, no Brasil, vários trainings centers homologados aí que podem fazer. Então, se a gente entrar lá no site da mikrotik.com/training, tem todas as informações aí de como podem ser obtidas essas certificações.

**SR. EDUARDO BARASAL MORALES:** Bom, muito obrigado, Maia. Tem uma pergunta aqui para o Paulo. Pergunta do Henry Alves Godói e da Letícia Pereira: "O Simet teria como obter dados estatísticos se o usuário final está usando Internet através de algum tipo de NAT ou usando IP público global? Teria como ter esses dados?". Então, Paulo, fique à vontade.

**SR. PAULO KUESTER:** Bom, eu vou, antes de responder à pergunta, vou fazer comentário: se livra do NAT. Assim, não sou um fã particular fã de NAT e tampouco são meus colegas aqui. Então se eu te dou um conselho, se livra disso. Vai para o IPv6, conhece o site do NIC que incentiva engajamento nessas ações. Respondendo a sua pergunta sobre estatísticas em relação ao NAT, a gente usa geolocalização por outras maneiras. Então eu não uso IP geolocation, por exemplo, para fazer uma avaliação da geografia, de modo que não limitaria nesse sentido, estatisticamente, porém, tecnicamente, vejo que você está limitado de outras maneiras. Enfim, não NAT.

**SR. EDUARDO BARASAL MORALES:** Tá certo. Muito obrigado, Paulo. Pessoal, a gente está chegando no final da nossa live. Eu vou só pedir agora uma contribuição de vocês. Vou pedir para o pessoal colocar o QR Code aí na tela porque agora eu queria que vocês nos dissessem o quê? Uma nota para essa live. Fizesse um comentário do que vocês estão achando da live até agora. Até para a gente saber o que a gente deve melhorar para a última live e para o ano que vem. Então, esse comentário é muito importante para a gente. Então, o pessoal está colocando agora o QR Code na tela, está colocando aí no chat um link, para vocês nos darem ali uma avaliação de como que vocês estão achando dessa live até agora. Bom, enquanto vocês estão preenchendo aí, eu queria dizer já os ganhadores da nossa Live. Então, teve aí do kit do NIC.br, o ganhador é o Carlos Adean de Souza. Do kit ali da Netfindersbrasil, o ganhador é o Vicente Brito, que ganhou o curso BGP MPLS avançado em Huawei. E o ganhador da Eletronet, que

é o voucher da Americanas no valor de 200 reais, o ganhador é o Jonathan dos Santos Aprígio. Da GlobeNet, que é um caixa de som acústica bluetooth, é o Willeson de Souza. E da Globo, voucher da Globoplay, de dois meses, é o Renan Mota Medeiros. E, por último, o sorteio da FiberX, da Huawei, que é o kit, o roteador match 5800, que é o Ezio Segger. Esses aí são os ganhadores. O pessoal está colocando aí para vocês aí a informação.

Bom, gostaria de dar alguns últimos avisos, lembrando: todo mês tem episódio do Camada8. Quem puder acompanhar, seguir a gente aí no podcast, é um jeito de aprender mais, é um conteúdo extra ao que a gente já faz aqui nas lives, ao que a gente já faz nos cursos, tá? Então é um jeito de você aprender um pouquinho mais sobre redes e tecnologia. Então, o podcast Camada8, episódios mensais. Tem aí o curso IPv6 EAD para aqueles que querem fazer. Como o Paulo estava comentando, que a gente é bem fã de IPv6 aqui. Então a gente tem o curso de IPv6 EAD, é gratuito, pode se inscrever. Tem o curso BCOP, como o Moreiras comentou, EAD, tem duas turmas em aberto. Uma termina hoje as inscrições, que é a turma 17. E tem a turma 18 que as inscrições vão até dia 10 de novembro. Vocês podem se inscrever. São as nossas últimas turmas do ano, do curso BCOP. Fica aí uma oportunidade para vocês. Fiquem atentos lá no site de cursos e eventos, porque toda vez que a gente tem curso, a gente publica lá. Teremos também o Intra Rede, no dia 15 de dezembro sobre novos padrões tecnológicos [interrupção no áudio], o que vem acontecendo no IETF e fóruns técnicos internacionais. Tem também a Semana de Infra, como o Moreiras já comentou. São aí os nossos últimos eventos do ano. Então fica muito interessante vocês participarem e contribuírem nas discussões, por quê? Porque vai ter chat, os painelistas vão estar lendo e vão estar interagindo com vocês. Lembrando, certificado, as inscrições vão até as 14 horas e precisa clicar no link enviado pelo e-mail. Gostaria aí de agradecer os nossos patrocinadores, deixa eu pegar aqui, que é a Juni Link IP & Cloud Network para a Giovaneli Consultoria; Icann; Wztech Networks; Netfindersbrasil; Novatec Editora; Eletronet; GlobeNet Telecom; Mundivox; 4Linux, Solintel; Cisco e Logicalis; 4Bios IT Academy; Globo; Netflix; FiberX e Huawei; e o apoio de mídia da: Revista RTI e Infra News Telecom. Agora, vou pedir para passar o videozinho do Cidadão na Rede, o videozinho novo para vocês verem aí um pouquinho sobre aí como ser um bom cidadão na Internet. Então, pode tocar.

[exibição de vídeo]

**SR. ANTONIO MARCOS MOREIRAS:** Esse vídeo do Cidadão na Rede foi sobre a ferramenta que o Paulo apresentou para a gente, que, afinal de contas, é uma ferramenta que pode ser bastante útil para o usuário leigo, no sentido dele calcular o tamanho adequado do plano

de Internet, da velocidade a ser contratada de Internet ali de um determinado provedor, e, inclusive, de saber quais provedores atuam na área em que ele está. O vídeo trata disso.

Eu quero agradecer a todos que estão aqui, quero agradecer de novo aos painelistas todos, ao Alexandre, ao Maia, ao Paulo, ao Luiz Puppin, ao Leonardo. Foi excelente a participação de vocês. Essas lives só acontecem por conta da colaboração do pessoal que topa vir aqui e fazer esses painéis com a gente. E tem sido muito legal. Eu quero agradecer também a colaboração do público todo. Vou fazer um comentário sobre o Camada8, que o Eduardo já falou do Camada8. Teve uma pergunta aí no chat que alguém falou: "Será que essa indisponibilidade que aconteceu com o YouTube foi um sequestro de prefixos, alguma coisa assim?". Olha, pelo que se publicou de informações, pelo que se viu na tabela de BGP, eu já vou adiantar que não, mas a gente gravou esses dias um episódio do Camada8, que ainda não foi lançado, ainda está em processo de edição, ainda vai demorar uns dias para sair. Não sei se vai ser o próximo ou se ainda vai mais. Mas a gente gravou um episódio sobre isso, sobre BGP, e a gente comentou algumas coisas desse incidente, que teve, sim, a ver com o BGP, mas, aparentemente, não, não foi um sequestro de prefixo. Fiquem atentos ao Camada8. É bem interessante. Tem nas principais plataformas de podcast. Tem no site do NIC.br também, para quem não está acostumado a ouvir podcast. Pode ir lá ouvir direto no site web do NIC.br.

Então, de novo, agradeço a todos. Muito obrigado pela presença. Muito obrigado pelos likes, muito obrigado pelos comentários no chat do público. Muito obrigado a toda equipe interna aqui que também colaborou, o pessoal da comunicação, o pessoal do técnico, o Pedro, tal, que colaborou para gente conseguir também fazer essa live. Muito obrigado aos patrocinadores. E até a próxima, gente. Até mais, tchau, tchau.