

SR. JULIO SIROTA: Muito bom dia a todos que nos acompanham no IX Fórum 14, parte da 10ª Semana de Infraestrutura da Internet no Brasil.

Vamos dar início aqui, à nossa agenda de apresentações para o segundo dia. E, assim, dar um lembrete para vocês, que a gente comentou ontem, que assistindo pelo canal de vídeos do YouTube, vocês vão ter acesso ao chat em que vocês vão poder interagir com a gente, tá?

Então assim, quem entrou para assistir o evento a partir do site do evento, lá no... a partir da página do IX.br, minha dica, assim, geralmente o que eu faço? É abrir uma outra janela, acessa o site do NIC.br e logo... nos primeiros links que você vai ver, vai ser do IX Fórum 14. Aí você clica ali, e ele já te joga no canal de vídeos do NIC.br, e você pode começar a assistir. E na janela do evento você pode estar acompanhando a agenda, tá?

E, na janela de vídeos do YouTube, você pode dar um like na nossa transmissão, que vai ajudar a fazer a divulgação para mais gente da nossa iniciativa.

Então, assim, a primeira apresentação do dia, eu gostaria de convidar o Flávio Correa, da Cisco, que vai estar falando para a gente sobre a tecnologia Wi-Fi 6.0.

SR. FLÁVIO CORREA: Legal. Bom dia, pessoal. Obrigado, Julio. Obrigado pela introdução aí.

Vamos lá, começando aqui mais um dia. Agradecendo já a oportunidade aí, de a gente participar e poder compartilhar um pouquinho de informação aqui, tá?

Bom, então meu nome é Flávio Correa, eu trabalho na Cisco como um arquiteto de soluções. Tenho essa especialização de mobilidade, e estou aqui com vocês para contar um pouquinho hoje como que a gente chegou até aqui, né? Ou seja, o que significa Wi-Fi 6 e, principalmente, quais são as mudanças e benefícios do Wi-Fi 6 versus as tecnologias que antecederam ele, tá?

E aí, no final, também vou fechar um pouquinho com algumas informações de adoção, clientes disponíveis e também a discussão... comentar um pouquinho sobre a discussão de uma alocação de um espectro novo, uma faixa de frequência nova para Wi-Fi, que é o tal do Wi-Fi 6E. Tá bom?

Então vamos lá. Bom, como eu comentava com vocês, a gente está, hoje em dia, falando aqui sobre essa última geração do Wi-Fi, que foi batizada de Wi-Fi 6.

Até esse momento, basicamente o Wi-Fi não tinha um nome comercial bom, né? A gente chamava pelo protocolo mesmo... 802.11

B, G, N, AC. E, finalmente, começou-se agora a usar um nome que as pessoas que não são de tecnologia podem se referir, assim como a gente faz com a tecnologia celular, com as tecnologias celulares.

Então Wi-Fi 6 significa a sexta geração. Eu, enfim, tenho a sorte de ter começado a trabalhar com Wi-Fi em 1999 e acompanhar toda essa evolução.

Nesse momento atual, a gente tem produtos comerciais disponíveis, seja de infraestrutura, sejam *clientes*. Inclusive a gente tem já certificações do Wi-Fi Alliance para esse novo padrão. Tá bom? Então eu diria que é uma tecnologia que está disponível, está padronizada e já está sendo utilizada desde o ano passado, principalmente.

E aí, quais são os benefícios principais? O que o Wi-Fi 6 traz de grandes novidades? Então, como sempre, maior data rate. Então a cada padrão novo de Wi-Fi a gente tem um data rate novo, a gente tem mais velocidade e throughput. E, de verdade, esse não é o essencial.

Mas o próximo item, que é a redução de latência e o fato de a gente ter, com a tecnologia de sexta geração, retornado o Wi-Fi um pouco mais determinístico, e aí eu vou explicar um pouquinho como, para mim, são as características mais importantes, são as mais diferentes. Que não aconteceu nas últimas cinco gerações. A gente vinha usando, basicamente, a mesma forma de modulação e acesso ao meio físico desde a segunda geração, pelo menos.

E aí, tem algumas coisas interessantes também, que abrem novas possibilidades, por exemplo, utilizar Wi-Fi para aplicações e dispositivos chamados IoT, aumento de densidade com a mesma quantidade de espectro de canais disponíveis e também melhoria na eficiência no uso de energia. De novo, para mim, o principal benefício é atrelado ao IoT.

Então, a ideia é detalhar um pouco esses itens agora, nessa primeira parte da apresentação.

Bom, então quando a gente fala de Wi-Fi 6, aquele primeiro item fala de performance, realmente o Wi-Fi 6... o grande ponto do Wi-Fi 6 é a melhoria de eficiência.

E quando a gente fala de eficiência, a gente pode tratar em quatro diferentes aspectos. Um é velocidade mesmo, dado pela modulação, o que a gente está usando para modular o sinal e quantos bits eu consigo transportar por símbolo, nesse caso a gente está falando de OFDM. Então a gente chama de quantos bits por símbolo OFDM eu posso transportar. Tem toda questão do MIMO e número de spatial streams, multiplexação de recursos usando diferentes transmissores e receptores.

Eu posso, simplesmente, aumentar a largura de canal para ter mais velocidade. Mas também eu posso melhorar na parte do overhead do protocolo, ou seja, toda sinalização que acontece, seja na hora de confirmar que um pacote foi enviado, seja a forma como é construído realmente o frame, a gente consegue, com Wi-Fi 6, ter melhorias.

Então a ideia é tocar um pouquinho aqui bem rapidinho nesses quatro pontos.

Então, sob ponto de vista de data rate, até como está nesse slide anterior aqui, a gente, basicamente, estava com Wi-Fi 5 aqui, até 256 QAMs, e a gente adicionou uma nova modulação, 1024 QAMs.

O que significa isso? Significa que, em teoria, essa é uma tabela puramente, diria, teórica e são as velocidades máximas, né? Se eu pegar essa modulação nova, que é o 1024 QAM, e a gente tem os códigos, que são os MCSs, modulation and coding schemes, ela está dentro do 10 e do 11 aqui... Se pegar em um canal tradicional, vamos dizer assim, de 20 megahertz, que é o canal que a gente mais utiliza, largura de canal que a gente mais utiliza, a gente está falando aqui que a gente consegue mandar até 130, 140 megabits por segundo. Mas o padrão permite eu trabalhar com canais mais largos, até 160 megahertz, o que me daria um número de até 1.2 giga.

Bom, isso transmitindo através de um único transmissor, com um único receptor, ou seja, sem usar nada de MIMO, sem usar nenhuma tecnologia de multiplexação. Então, nesse caso, a gente fala que a gente está transmitindo aqui 1.2 giga, com um spatial stream.

E a tecnologia Wi-Fi 6, que a gente vai ver, também, daqui a pouco, ela permite até oito streams desse em paralelo. Que eu tenho access points que podem mandar oito streams, tem oito transmissores, oito receptores, ele pode mandar oito streams de informação paralela.

Então, em teoria, o Wi-Fi 6 me permitiria chegar a mais de 10 gigabits por segundo. Claro que, na prática, a gente não vê isso, por diversos motivos. Um, porque canais de 160 megahertz não são utilizados na prática, a gente não tem espectro suficiente. Então é por isso que eu vou falar do Wi-Fi 6E no final. A gente vai poder começar a pensar nisso com Wi-Fi 6E.

E a gente tem overhead de protocolo. Isso aqui é data rate, vamos dizer assim, é [ininteligível]. Normalmente eficiência do Wi-Fi é de 60%. Então você pegaria 60% desse número.

E, hoje em dia, as redes estão trabalhando mais em 20 ou 40 megahertz ainda. Então, se a gente pegar lá, vamos dizer, 250 megabits por segundo, 60% disso... E aí o número de spatial streams, hoje, também é limitado. Porque a maior parte dos clientes que a gente tem são clientes móveis, como telefone, ou mesmo um laptop, onde

ele não chega, até por estar em padrão anterior, ele não chega a oito spatial streams, a gente usa, talvez, dois, três, no máximo. Legal.

E aí, se a gente for colocar na prática também, vamos dizer: Olha, agora com Wi-Fi 6 eu tenho essa nova modulação, e eu vou poder usar canais mais largos. Também essas modelações mais eficientes, mais complexas e também mais eficientes, elas têm uma cobertura limitada. Então a gente está falando que eu posso colocar isso em operação e talvez eu vou ter um raio de 10 metros, no máximo, entre meu AP, aonde o dispositivo estiver ali embaixo, muito próximo, vai ter essa capacidade.

Bom, então esse é o primeiro ponto, que era o ponto mais de data rate, de novas modulações.

A questão dos spatial streams, eu comentei um pouquinho com vocês já, mas o Wi-Fi 5 tinha até quatro... a possibilidade de ter até quatro spatial streams.

O que isso significa para quem não é muito desse mundo? Imagina que do lado esquerdo aqui, eu tenho o meu access point. E cada quadradinho com esse triângulo aqui, é um transmissor e um receptor, é uma cadeia de TXRX. Então vamos dizer assim, que no Wi-Fi 5 eu tinha os meus produtos de infraestrutura com até quatro rádios transmissores em setores, no Wi-Fi 6 eu passo a ter access points com até oito transmissores e receptores. E elas podem estar mandando individualmente informação para um usuário, cada chain desse mandando informação para um usuário, ou através de combinações.

Mas o importante é o seguinte, eu posso mandar através de cada transmissor e receptor desse no mesmo instante, no mesmo canal, informações diferentes. Então por isso que eu consigo multiplexar e, basicamente, multiplicar, nesse caso por oito, o meu throughput.

Claro, que a gente tem implicações disso, enfim, para eu combinar as melhores condições possíveis de modelação, número de spatial streams, eu tenho que ter uma combinação ideal, seja de nível de sinal, sinal ruído, seja do posicionamento dos APs, eu tenho que ter reflexão para que o MIMO funcione corretamente, enfim, são condições teóricas, mas possíveis que o novo protocolo nos permite.

Sob ponto de vista de largura de canal, a gente basicamente tem a mesma condição. Então eu posso usar canais de 20 megahertz, 40, 80, ou agora posso usar também 160. Isso já veio do Wi-Fi 5 [ininteligível] 2.

Mas, de novo, na prática a gente acaba não usando, por quê? Porque a hora que eu... Essa tabela são as tabelas basicamente de distribuição de espectro no mundo. O Brasil tem uma similaridade maior aqui com espectro alocado pelo o FCC para os Estados Unidos, tem algumas diferenças. Mas a gente está falando para o Brasil em

torno de 21 canais, de 20 megahertz, que são cada um desses polígonos aqui de cima.

A hora que eu combino em 40, eu já, pelo menos, dividi pela metade, então ficam 10 canais, no melhor dos casos. Porque a faixa não é contínua em algumas situações. Se eu colocar 80, em teoria, eu teria, no máximo, 5 canais. E aí eu já começo a ter que reutilizar esses 5 canais com bastante frequência. Então, nem sempre é prático ou é uma... ou traz um benefício a gente usar canais mais largos. Mas é possível. E a gente vai ver que tem hoje um recurso para reuso de canal bem interessante.

Mas o mais importante de tudo é como a gente está... na minha visão, no Wi-Fi 6, é como a gente está, basicamente, hoje, trabalhando na camada física com o que a gente chama de OFDMA. E esse MA do final é de 'acessos múltiplos'. Então, se a gente for comparar com o atual ou com o anterior, que é OFDM, em cada instante de tempo, eu só tinha um dispositivo transmitindo. Então no instante tempo 1, o Flávio está transmitindo, o access point está escutando, e o 2, o 3, o 4, o 5, 6, 7, 8, e assim por diante.

Ou seja, claramente a medida que você vai aumentando o número de usuários, você vai ter um aumento de latência. Você não tem como atender múltiplos usuários em paralelo.

Basicamente, o que o OFDMA está se propondo é mudar isso completamente. E começa desde a forma como ele divide os canais em subportadoras. Então no OFDM teria uma divisão, no OFDMA eu tenho mais subportadoras. E essas subportadoras, basicamente, a gente consegue organizar em recursos chamados resource units, um conjunto de subportadoras. Então como se eu estivesse pegando lá meus 20 megahertz e dividindo em canais ainda mais estreitos, eles são chamados de subportadoras... Desculpa, são chamados de resource units. E aí eu consigo, por exemplo, em um canal de 20 megahertz, eu consigo ter até 9 usuários falando ao mesmo tempo e compartilhando aquele canal. Ou seja, eu deixo de ter a condição de atender um usuário por vez, eu posso ter a condição, em canais de 20 megahertz, de atender até 9. Isso aumenta à medida que eu tenho canais mais largos também.

Então como vocês podem imaginar, isso tem impacto bastante importante, principalmente se a gente considerar que boa parte do tráfego, claro que depende muito do perfil da rede, de tráfego da rede, do uso da rede, mas a gente tem, por exemplo, cada vez mais a infraestrutura Wi-Fi sendo utilizada para todos os tipos de serviços possíveis, incluindo voz.

Então, a hora que você faz lá o [ininteligível], em muitos casos você tem uma quantidade muito grande de pacotes ou de frames, nesse caso, pequenos. Então, o que acontece? Você acaba

subutilizando aqueles canais... aquele momento de transmissão. Você tem lá um canalzão de 20 megahertz, que você poderia alocar muito mais bits e você está alocando só uma parte dele, e está usando só uma parte dele, porque, basicamente, o frame era um frame pequeno.

Então com o OFDMA eu consigo fazer isso de uma forma mais eficiente, no mesmo instante de tempo, atendendo a múltiplos clientes. Então, um pouco do que esse diagrama aqui da direita mostra. E isso muda tudo. Ou seja, se eu consigo atender mais de um cliente ao mesmo tempo, obviamente eu tenho impacto grande em latência, eu tenho impacto grande na densidade, que eu poderia colocar mais clientes com uma densidade mais baixa.

Então, para mim, o grande... a grande mudança é a capacidade de a gente alocar para mais de um usuário que ele se comunique no mesmo instante de tempo.

E aí a gente fez alguns estudos aqui. E esse aqui é um gráfico que mostra um pouco do impacto. Onde a gente tem aqui em verde, o Wi-Fi 6, em azul, o Wi-Fi 5. No primeiro gráfico aqui, em um gráfico que mostra número de usuários e latência.

Então, basicamente o primeiro gráfico mostra que a hora que eu vou aumentando o número de usuários, a latência vai subindo de uma forma bastante significativa, né? Claro, se eu quero fazer voz, eu tenho que manter uma latência baixa, uma latência máxima tal que não tenha impacto na aplicação.

Se eu for para a parte de analisar um pouco mais um tráfego de dados, não necessariamente de voz, que é sensível à latência, mas eu também tenho impacto grande em throughput. Porque a hora que eu começo a colocar muita gente, eu tenho um overhead grande para tratar todos esses usuários, e aí, na verdade, o que acontece, eu tenho uma redução de throughput bastante significativa. No Wi-Fi 6 eu consigo manter isso mais linear, eu diria. Tá bom?

E aí, obviamente, com tudo isso, eu consigo, por exemplo, um dos limitantes, hoje, no design de Wi-Fi, quando eu vou fazer uma rede que precisa atender usuários que vão fazer chamadas de voz, um dos limitantes de densidade justamente são o número de chamadas de voz simultâneas. Então eu acabo tendo que colocar mais access points para receber aquela densidade de atender usuários com chamada de voz. Com o Wi-Fi 6 um dos benefícios imediatos é isso, eu consigo, por exemplo, colocar 70 clientes por AP com uma latência ainda bastante razoável, vamos dizer assim. Tá bom?

Legal. O que mais que a gente tem de interessante para dentro do Wi-Fi 6, né? A gente tem mais três itens aqui... Não sei se o pessoal pode me ajudar aqui. Pessoal da organização. A gente está seguindo o tempo da sessão ou a gente está seguindo o horário mesmo, das 9h30?

Só para me ajudar aqui. Ou seja, eu tenho cinco minutos ou tenho dez minutos?

SR. JULIO SIROTA: Pode considerar os dez.

SR. FLÁVIO CORREA: Tá bom, então. Obrigado.

Então, a gente tem alguns outros recursos interessantes dentro do Wi-Fi 6. Eu vou falar rapidamente desses três aqui: Multi-User MIMO, Target Wake Time e BSS Coloring.

Então, imagina... esquece o que eu falei do OFDMA e pensa só na forma como funcionava o Wi-Fi até hoje, né? Até Wi-Fi 5, eu tinha lá, um instante de tempo eu podia mandar informação para um usuário. Aí, veio que é o que a gente chama de Single-User MIMO, ou seja, eu posso usar meus múltiplos transmissores e receptores, mas a cada momento eu estou mandando essa informação para um usuário. Então eu estou usando os meus múltiplos transmissores e recepção para reforçar sinal ou para mandar múltiplos spatial streams, mas para um único usuário.

Apareceu já no Wi-Fi 5 o tal do Multi-User MIMO. O que é o Multi-User MIMO? Era, no mesmo instante de tempo eu alocava lá o canal de 20 megahertz, para aquele instante de tempo, mas como eu tinha múltiplos transmissores e receptores, com o Multi-User MIMO eu podia mandar, no mesmo instante de tempo, informações diferentes para cada usuário. Ou seja, eu estou usando os múltiplos transmissores para fazer isso.

Então nesse caso aqui, o primeiro terminal está recebendo informação, vamos dizer assim, do transmissor vermelho e do transmissor azul, o segundo terminal do verde e do azul e o outro do amarelo e do azul. Esse era o Multi-User MIMO.

O fato é que Multi-User MIMO no Wi-Fi 5, ele não pegou. Porque ele era opcional e, basicamente, na prática, ele não foi implementado. No Wi-Fi 6 ele volta já mais consolidado à medida que você já tem um mecanismo para que ele funcione bem, que é o tal do mecanismo de sounding ou de feedback que a gente chama. Ele passa a funcionar não só no down link, mas no downlink e no uplink, e ele pode funcionar com mais usuários.

Além disso tudo, lembra que a gente dividiu os 20 megahertz em resource units? Eu posso pegar cada resource units daquele lá, no mínimo do tamanho 106, ou maior, e fazer o Multi-User MIMO dentro dele.

Então assim, é meio *mind blowing*, você fica um pouco confuso com isso na primeira vez que você escuta. Mas é isso, posso multiplexar para vários usuários aquele mesmo canal e eu posso pegar esses pedacinhos e alocar para múltiplos usuários também.

Então, ou seja, a gente está em um momento onde as possibilidades são de novos serviços ou aplicações que a gente pode colocar em cima do Wi-Fi, passa a ser bem interessante.

E isso também tem alguns impactos na hora que a gente falar em novos serviços, porque muitos chamam de serviços IoT, né? A gente colocar, por exemplo, sensores, aonde o grande objetivo é você mandar informação, mas a informação normalmente é pouca informação, em intervalo de tempos espaçados, porque isso também economiza bateria.

Então, o fato de a gente poder usar resource units, vamos dizer, subcanais ou canais mais estreitos, eu consigo economizar bateria, eu consigo, com o mesmo nível de bateria, mandar mais longe, porque é um canal mais estreito, e também eu vou mostrar para vocês que a gente consegue hibernar um client por anos, bem como o Wi-Fi 6 também passa a estar está disponível no 2.4 gigahertz.

Antes, o Wi-Fi 5, nem todo mundo se deu conta, mas ele estava só no 5 gigahertz, o 2.4 parou lá no Wi-Fi 4. Então o Wi-Fi 6 passa a também vir no 2.4.

Então, tudo isso... Aqui o Target Wake Time, que a gente chama de TWT, que é a capacidade de eu colocar um dispositivo para hibernar e ele só voltar a responder alguma coisa depois de semanas, meses ou anos. A gente não tinha essa capacidade, uma vez conectado, o dispositivo tinha que mandar a cada 100 milissegundos, era o padrão, ele tinha que mandar pelo menos um 'A' aqui, dizendo que ele estava ali ainda registrado.

E para fechar, pessoal, essa parte aqui, existe também um novo mecanismo, mecanismo de reuso do espectro, chamado de BSS Coloring, que também promete permitir a gente usar canais mais largos e reutilizar de forma mais eficiente o espectro.

Então imagina que eu tenho dois usuários na mesma célula, a gente chama isso de intrabasic service set, Intra BSS, todos no canal 36, por exemplo, e aí eles têm o mecanismo de quem fala quando, baseado no nível de sinal e baseado no clear channel assessment, que a gente chama. Ou seja, enquanto um está transmitindo, o outro não faz nada, é um por vez, basicamente.

E aí, o que acontece é que quando eu tenho APs no mesmo canal ou até clientes... não necessariamente o AP, mas clients que estão se afastando da célula dele e transmitindo informação, ele está impactando em outras células que estão usando o mesmo canal. Então isso chama de overlapping basic service set. então, hoje, se a Estação A mandar um pacote para o APA, basicamente ela está impactando lá no APB, que está mandando informações para o cliente B. Ou seja,

quando os canais se escutam, mesmo em APs diferentes, eles estão se interferindo.

Então, o que a gente passa a fazer... E a transmissão do Wi-Fi, dependendo da condição e do nível onde acontece o clear channel assessment, que é de menos 82 dBm, as células podem, facilmente, se interferir. Então elas podem estar bem distantes e facilmente se interferir.

Então, basicamente, o que acontece agora, a gente coloca uma variável nova, que é variável cor, vamos dizer assim, onde eu tenho canal 36, e canal 36, mas em cores diferentes. E, com isso, basicamente... Se a célula verde receber um pacote, um frame da célula azul no mesmo canal, basicamente ele ignora e a gente consegue reutilizar bem melhor o espectro.

O meu tempo está terminando aqui. Só fechar com como é que está a situação do Wi-Fi 6.

Então, 2019 eu acho que foi um grande ano para o Wi-Fi 6. A gente teve vários dispositivos sendo lançados e diferentes fabricantes. Então a gente aumentou muito o número de dispositivos Wi-Fi 6 no mercado. A gente tem, por exemplo, uma plaquinha que pode ser usada, pode ser trocada no seu laptop, que é uma interface Wi-Fi 6, que custa US\$ 15. Então a gente tem visto muitos clientes fazendo essa atualização, usando as máquinas existentes.

E 2020, obviamente, era o ano para a gente ter uma expansão muito maior. A gente está vivendo um ano atípico aqui.

E uma coisa muito interessante que aconteceu em 2020, também, é que tanto FCC quanto a Anatel, anunciaram alocação de mais espectro para o Wi-Fi, que é o chamado Wi-Fi 6, 1200 megahertz. Falando linhas gerais, dos 6 gigas a 7 gigas, que poderão ser utilizados para Wi-Fi. Então o espectro que é alocado para uso não licença estrado.

A Anatel já fez análise dela, técnica. A decisão final ainda não foi tomada, de qual a quantidade de espectro. Isso está acontecendo globalmente, essas discussões. E, basicamente, o espectro pode ser alocado completamente, ou seja, os 1200 megahertz, que seriam 59 canais adicionais, ou seja, mais do que o dobro do que a gente tem hoje, ou pode ser alocada parcialmente.

Então, basicamente, tem propostas... tem duas grandes propostas, uma proposta mais do FCC, por exemplo, alinhada com o FCC, que é uma proposta do uso completo do espectro de 1200 megahertz, com algum controle de potência e algumas restrições de uso, só uso indoor, por exemplo. Ou tem uma proposta de uso parcial, que é um pouco mais do que o ETSI está seguindo, para Europa.

O Brasil, a maioria das decisões da Anatel, técnicas, por tudo o que a gente vê ouvindo e discutindo, está mais alinhada com a proposta do FCC, dos 1200 megahertz. Mas a decisão final ainda não foi tomada.

Até deixei um link aqui, de um painel que aconteceu com a Anatel, agora, em novembro, sobre a alocação do espectro de 6 gigahertz para quem quiser saber mais. Tá bom?

Então, fechando aqui, acho que fechando dentro do meu tempo. O Wi-Fi 6 é a nova geração de Wi-Fi, a sexta geração. Ele traz vários benefícios. Mas o mais importante é essa forma mais determinística de atender clientes e conseguir viabilizar que novas aplicações usem o Wi-Fi como tecnologia.

E aí, todo mundo aqui na expectativa da alocação de mais espectros, seja para o uso do tal do Wi-Fi 6E, seja até para o Wi-Fi 7, que também já está em discussão, tá bom?

Então, vida longa para o Wi-Fi. E agradeço aí, a oportunidade de falar um pouquinho sobre o assunto.

Perguntas no chat, alguma coisa, pessoal? Não temos nada por voz, certo?

SRA. ANDREA ERINA KOMO: Obrigada, Flávio. Acredito que as perguntas... A gente tem alguma pergunta para passar agora, Julio?

SR. JULIO SIROTA: Tenho. Que eu não estava conseguindo--

SR. FLÁVIO CORREA: Entrou no mudo de novo agora, Julio.

SRA. ANDREA ERINA KOMO: Julio, seu microfone fechou...

SR. JULIO SIROTA: Está ouvindo agora?

SR. FLÁVIO CORREA: Agora sim.

SR. JULIO SIROTA: Agora tenho que pegar a pergunta aqui. Vamos lá. A gente tem duas perguntas, Flávio. Vamos ver se consegue responder rapidinho aí.

SR. FLÁVIO CORREA: Ótimo.

SR. JULIO SIROTA: Uma do Antonio Carlos Gaspareti, ele pergunta assim: "Aumenta os usuários, diminui o espaço entre as portadoras. Como fica relação sinal/ruído e a largura de banda? E a distância do AP não diminui? Não existe um trade entre velocidade e distância? Para manter a qualidade, eu não tenho que ter mais APs?".

SR. FLÁVIO CORREA: Sim. Uma boa pergunta, um pouco até eu comentei durante a apresentação.

Mas então sim, tem esse trade sempre, né? A hora que transmitir mais rápido, eu preciso de um sinal ruído melhor, então a distância diminui.

A questão de sinal/ruído permanece a mesma, porque as modulações são as mesmas... para as mesmas modulações permanece igual. A gente tem uma modulação nova, 1024 QAM, que exige sinal/ruído maior. Então eu falei que eu mostrei o gráfico que a distância é de cerca de 10 metros de raio para você conseguir aquela velocidade máxima.

Mas o mais interessante, realmente, quando você fala em mais usuários, é você poder colocar mais usuários sem degradação, sem aumentar latência como aumentava antes, no Wi-Fi 5.

SR. JULIO SIROTA: Ok. Outra pergunta, é do Roberval Dantas: "Na prática, em condições normais, quanto de banda se consegue na largura de 20 megahertz?".

SR. FLÁVIO CORREA: Como a gente mostrou lá, na teoria, a gente está falando em 100 megabits por segundo, 120, 130, mas isso é condição máxima para um spatial stream, né?

Então, assim, na prática, a gente continua vendo... Se eu pegar os 100 megabits por segundo e colocar 60% de eficiência, eu teria lá 50, 60 mega, se todo mundo estivesse na melhor modulação, e aí eu posso ter um ou outro usuário fazendo o MIMO, né?

Eu diria que, assim, [ininteligível], um número de... prático, eu não vejo nada além de 60, 70 megabits por segundo, na prática, ou seja, com uma distribuição real de clientes, para um canal de 20 megahertz, nesse momento. Tá?

Então, nesse momento, a gente ainda não tem uma quantidade suficiente de clientes Wi-Fi 6, nos clientes, para ter essa percepção prática e real do impacto, né?

Então eu estou te dando ainda o número que é o número que a gente vê no dia a dia, nos clientes, ainda com mix muito maior de Wi-Fi 5 e pouco ainda Wi-Fi 6.

SRA. ANDREA ERINA KOMO: Obrigada, Flávio. Muito boa essa sua palestra. A gente agora está sabendo bastante sobre o Wi-Fi 6 graças a você.

Bem, para a gente não atrasar muito a nossa agenda, quero seguir para próxima palestra, mas antes eu vou fazer um pedido aqui, é rapidinho. O Júlio falou isso, mas eu vou pedir para vocês darem like no nosso vídeo no YouTube. Isso vai ajudar aí, o vídeo a ser divulgado para mais interessados em rede. Divulguem para os seus colegas também assistirem a *live*. A agenda está disponível no site do evento, para vocês saberem que o vai acontecer no dia de hoje e amanhã.

E, agora, eu queria chamar o gerente Antonio Moreiras, ele vai comentar um pouquinho sobre o mapa de ASs, mapas de sistemas autônomos, né? Então, Moreiras, por favor, a palavra é sua.

SR. ANTONIO MARCOS MOREIRAS: Obrigado, Erina.

Bom dia, gente. Bom, eu vou compartilhar a tela aqui, para mostrar um novo software. Antes de compartilhar, deixa eu começar compartilhando uma apresentação. A apresentação eu acabei de mandar para o pessoal subir no site, então ela talvez não esteja disponível ainda. Aliás, com certeza não está disponível ainda. Mas daqui a pouco estará.

Então deixa eu só mostrar aqui para vocês. Um segundinho. Vamos ver. Apresentação. Compartilhar a tela. Ok. A tela está compartilhada. Imagino que vocês estejam vendo aí.

E a apresentação está seguindo sozinha, sem eu fazer nada. E eu não sei o que eu faço para ela parar aqui. Meu Deus do céu.

Eu estou aqui... 10 a 0 para o Mac aqui, que resolveu tocar minha apresentação sozinho. Ele poderia falar também, daí eu não tinha nem o trabalho, né?

Bom, gente, a gente está lançando um novo mapa de AS, similar àquele mapa de AS que a gente tem no site do IX.br, onde é possível visualizar a localização dos ASs no Brasil.

Então, ele tá nessa URL. Vocês podem acessar essa URL, fazer os testes por si próprios. Já está no ar.

Esse é o principal recado desses dez minutos aqui. Falando só isso, vocês já vão... de resto vocês já vão se virar e entender o site e o software por si mesmos, né?

Agora, é bom enfatizar que é um software beta ainda. Então é um software de teste, frágil, que a gente fez para experimentar alguns conceitos novos, algumas novas ideias, e você vai falar: Mas, Moreiras, não tem nenhum conceito novo nesse site, não. Está igual, ou está um pouquinho mais bonito do que o que está no site do IX.br, mas tem quase a mesma coisa lá.

Bom, não é bem assim. Tem coisas novas sim, eu vou mostrar. E tem coisas novas que não estão liberadas para vocês, mas a gente está preparando, e eu vou mostrar um pouquinho delas aqui.

E um aviso legal aqui, necessário, nenhum estagiário sofreu maus-tratos, nem foi ferido na construção desse software. Isso é bastante importante. A gente faz questão de enfatizar.

Bom, você vai conseguir, no mapa de AS, daqui a pouco eu mostro direto no site, mas você vai conseguir ver a localização dos ASs, a localização aproximada da sede dos Ass. Assim que você clica no mapa, você consegue ver isso daqui, você consegue dar zoom, tirar zoom, você consegue selecionar por estado, e ver só os ASs daquele estado.

Tem também algumas tabelas que mostram, vamos dizer assim, a distribuição dos ASs por região, por estado e por cidade. Na aba 'distribuição' você consegue ver isso daí.

E temos uma novidade... Ah, temos o localizador de AS. Que ainda não é a novidade. Essa função de localizar o AS, ela visa dar uma ideia da quantidade de sistemas autônomos operando em uma determinada região. Então você coloca um CEP, coloca um raio, e ele mostra uma tabelinha com as cidades e com a quantidade de ASs em cada cidade, em cada região. Por exemplo, quando a gente vai estudar um local para criar um PTT novo, é uma funcionalidade que a gente sempre busca, a gente olha os ASs dentro de uma determinada região. Quando a gente vai conversar com o pessoal de um determinado PTT, quando a gente vai, por exemplo, fazer um evento na região, é uma coisa que, geralmente, também, a gente olha e fala: Poxa vida, mas tem um PTT aqui na cidade tal, mas temos só 20 ASs conectados. Se a gente pegar um raio de 80 quilômetros temos 150 ASs conectados, o que está acontecendo? Então vamos tentar descobrir isso daí, né?

E a gente tem uma funcionalidade nova, que já está liberada para vocês, e que eu acho bastante interessante, que é a gente visualizar no mapa os ASs que estão presentes em um determinado PTT. Então isso dá uma ideia da área de abrangência, da abrangência de atuação de um determinado PTT. Então você pode ir lá e, por exemplo, escolher PTT de São Paulo. Aí a gente vai na lista de participantes do PTT de São Paulo, e a gente pilota no mapa ali o lugar onde é a sede do AS, a informação que a gente tem do endereço da sede daquele sistema autônomo. Então dá uma ideia da abrangência.

Mas, o mais legal ainda, que você pode escolher dois PTTs, você pode escolher um segundo PTT. Então, aqui, por exemplo, para tirar esses *screenshot* eu escolhi São Paulo e escolhi Fortaleza. Aí, o que acontece? Os ASs de São Paulo aparecem em azul, os ASs que estão em Fortaleza aparecem em vermelho os pontos. E os ASs que estão nos dois, ao mesmo tempo, aparecem em verde, Então dá para você ter uma ideia, também, da quantidade de ASs que estão, vamos dizer assim, no PTT de uma abrangência mais local e no PTT de uma abrangência mais nacional. No caso eu escolhi dois PTTs enormes para tirar esse *screenshot*, que tem, ambos, abrangência basicamente nacional hoje em dia. Dá para você ver por esse desenho, por exemplo, que tem muitos AS que estão conectados lá em Fortaleza, interligados no PTT de Fortaleza, da região Sudeste, da região Sul. Isso é bastante interessante.

Então, essa funcionalidade aqui já está liberada para vocês. Também tem a visualização por esses marcadores e tem a visualização também por pontinhos vermelhinhos, que eu não tirei *screenshot*, mas vocês podem experimentar com o mapa e vocês vão ver isso daí.

Agora tem algumas funções que estão em desenvolvimento aí. Eu vou dar uma passada rápida, porque eu acho elas bem legais e vocês podem nos dar ideias sobre elas.

Uma função é relacionada a GeoIP. Então, como que eu faço? Eu faço uma busca por um AS. Eu fiz aí para esse *screenshot*, eu busquei o AS 10429. Aí eu identifico todos os blocos IP alocados para esse AS via Rdap ou via Whois, lá no Registro.Br. Separo isso tudo em /24. Pego o primeiro IP desse /24 e faço uma busca de geolocalização naquela base que tem da empresa MaxMind, GeoIP – eu não sei se pronuncia lite ou lite – GeoIp lite, que é uma base gratuita de geolocalização. E daí eu ploto esses pontos no mapa.

Aí, o que você tem? Você tem uma ideia da abrangência daquele AS, de como que aquele AS atua. E você pode plotar também, ao invés de plotar os pontos, eu posso plotar o número de, vamos dizer assim... eu pego o polígono do estado e coloco mais escuro, mais claro, conforme o número de /24. Então dá para ver que esse AS específico, ele tem uma forte atuação no estado do Rio de Janeiro e no estado de São Paulo. Mas ele tem uma atuação quase nacional.

E eu posso fazer isso também com polígono de cidades. Então dá para ver, aí fica mais claro ainda que a atuação é muito, muito forte em São Paulo e na região, vamos dizer assim, sul do Rio de Janeiro.

E é legal. Olha aqui. Eu peguei um outro AS para fazer esse mesmo teste, o AS 28126, e eu consigo... E eu plotei com polígonos de cidades, plotei pela visualização de cidades. Então eu consigo ter uma boa ideia da área de atuação desse AS, por exemplo, que abrange boa parte da região Nordeste do Brasil.

É perfeita a visualização? Não, é a geolocalização aproximada dos IPs dada por essa base de dados aí, que é gratuita. A geolocalização não é perfeita, vai aparecer em uma cidade próxima. Provavelmente a área de atuação desse provedor específico aqui, abrange muito mais municípios do que está plotado aqui no mapa. Mas dá para você ter ideia interessante, uma ideia legal de onde um determinado AS atua e o tamanho daquela... da abrangência da área de atuação dele.

Uma outra funcionalidade que está lá em desenvolvimento é eu fazer uma coisa parecida, mas ao invés de buscar informações de IP na base do Rdap, na base do Whois, agora eu vou olhar para os PTTs, eu vou olhar para o Looking Glass do PTT, lá do Alice. Eu vou olhar o Alice. Que a gente comentou que agora está presente... tem o Looking Glass disponível com API consultável em todos PTTs nossos, menos no de São Paulo ainda, que não está pronto. Mas a gente vai colocar.

Então a gente pega os blocos IP que estão anunciados lá na tabela de rotas do ATM, via Alice, via as APIs do Alice, do Looking

Glass. E a gente separa aqueles blocos IP em /24. E faz a mesma coisa, pego primeiro o IP de cada um desses /24 e procuro a geolocalização na base GeoIp lite da MaxMind. E daí eu ploto no mapa.

Então eu fiz isso daqui para o PTT de Fortaleza. E dá para ter uma ideia de onde vem os IPs... onde estão presentes, vamos dizer assim, os IPs que aparecem na tabela de rotas do ATM do PTT de Fortaleza.

Olha, e é legal. Dá para você ver bem que o PTT de Fortaleza, ele tem uma abrangência não só nacional, mas tem uma abrangência internacional. Tem muitos IPs que estão presentes anunciados na tabela de rotas lá do ATM de Fortaleza que não são IPs de ASs brasileiros, que não estão geolocalizados, vamos dizer assim, no Brasil. Isso é bem interessante.

E nos nossos testes até nos surpreendeu. Porque, aqui, no caso de Fortaleza não surpreende. Porque no caso de Fortaleza é esperado, é um PTT muito grande, que tem uma abrangência muito grande. É sabido isso. Mas às vezes nos surpreende algum PTT que a gente parece que é um pouco menor, tal, e a gente vê que tem IPs, às vezes, do mundo inteiro também, lá presentes na tabela de rotas.

Então é a mesma visão aqui, só que dei um zoom no caso do PTT de Fortaleza, para dar uma olhada com mais detalhes no Brasil, de que regiões que estão os IPs que estão lá.

Pode ter erros aqui, viu? Até porque se essas funcionalidades não estão liberadas é porque...

Já estão me avisando que acabou aqui, mas é o último slide, Erina. Fica tranquila que já está no finalzinho aqui.

Essa funcionalidade não está liberada justamente porque ela não está pronta. Então tem que ter um cuidado até com esses dados que eu coloquei nos slides que vão estar disponíveis para vocês.

E é isso. Já me avisaram que acabou o tempo. Então eu não sei se os moderadores vão abrir, ou não, para perguntas, para dúvidas ou sugestões.

Mas vocês podem olhar depois, com calma, o mapa de AS e vocês podem mandar as suas dúvidas ou mandar as suas sugestões, ideias de outras visualizações: "Poxa, poderia ser legal se tivesse tal coisa, tal coisa. Você fez isso aqui, agora eu tive outra ideia assim, assado" . Manda essas ideias para a gente.

Aí tem meus contatos. Daqui a pouco o pessoal deve subir essa apresentação, vai ficar lá na agenda do evento também. Manda lá um e-mail para mim, entra em contato e dê a sua sugestão, tá bom?

Obrigado. Volto a palavra para os moderadores.

SRA. ANDREA ERINA KOMO: Obrigada, Moreiras. Muito interessante esse sistema aí. Imagino que o pessoal vai usar bastante.

Bem, a gente tem boas perguntas, mas dado o tempo eu escolhi aqui só uma. Peço que você seja breve na resposta. Eu selecionei aqui a pergunta do Rafael Girão(F), ele colocou aqui: "O local do ASN é o endereço de cadastro do ASN? Não é possível um mapa o qual se utilize as informações do Simet para mostrar os ASNs que estão em uma determinada região, por exemplo, um bairro ou um município?".

SR. ANTONIO MARCOS MOREIRAS: Bem interessante. É uma ótima sugestão. E é algo que a gente está pensando sim. Ao invés de pegar essa informação do GeoIP, por exemplo, pegar essa informação da área de atuação do Simet. A gente tem conversado com a equipe do Simet sobre essa possibilidade de buscar esses dados lá.

Eu vou encarar sua pergunta mais como uma sugestão e anotar ela, reforçar. Mas é uma excelente ideia. E é possível que a gente faça isso sim.

SR. JULIO SIROTA: Ok, obrigado, Moreiras.

Vamos dando sequência aqui, a nossa agenda. A gente vai começar... a gente vai ter um painel agora sobre IPv4, né? O título é: 'Existe vida após o esgotamento do IPv4'.

Então eu vou convidar aí, para participar o Antonio Moreiras e o Eduardo Barasal, do NIC.br, que vão ser os dois moderadores. E os nossos participantes aí, que é o Rosauro Baretta, que ele é da EAI e do Comitê Gestor da Internet no Brasil, o Rubens Martins Schner, que é da Brisanet, e Uesley Correa, que é do Brasil Peering Forum. Então que vocês deem vida aí a rede sem IPv4, por favor.

SR. EDUARDO BARASAL MORALES: Muito obrigado, Julio.

Então vamos começar nossa mesa falando aí, então, sobre o fim do IPv4, né? Existe a vida após o esgotamento do IPv4?

E eu gostaria de chamar para começar essa nossa discussão o Rosauro Baretta, que é o conselheiro eleito do CGI.br representando os provedores. Então eu gostaria de uma visão dos provedores, como que eles estão sobrevivendo aí, depois de a gente ter anunciado que não tem mais endereço IPv4 aqui na América Latina.

Então, Rosauro, fique à vontade.

SR. ROSAURO LEANDRO BARETTA: Bom dia, Eduardo. Bom dia a todos, o Moreiras também está junto aqui, enfim, toda equipe do NIC. Também cumprimentar o Uesley e o Rubens, que são dois feras no assunto, que vão estar falando aqui comigo no painel.

Bom, para quem não me conhece, eu sou Rosauro Baretta, fui presidente da Redetelesul, Associação dos Provedores aqui do Paraná,

por quatro anos, e agora estou como conselheiro do CGI na cadeira dos provedores de acesso e de conteúdo. Então eu tenho já uma vivência aí há 28 junto aos provedores de Internet. A gente tem sempre trabalhado muito com relação a isso.

E aí o que a gente tem visto? Como que vai ser a vida dos provedores e do acesso agora que acabou o IPv4?

Então, eu até tenho um levantamento, quero citar dois números só, para ir dando algumas informações. Em julho até a gente fez um outro painel sobre o IPv6 também, e lá em julho eu fiz um levantamento com mais de cem provedores de como estava o uso do IPv6 com eles.

E, na ocasião, nós tínhamos 38% dos provedores ofertando o IPv6 para os clientes. Desculpa. 38% não tinham IPv6, 62% tinham. Ou seja, 38% não estavam colocando IPv6 para os clientes ainda. Só que desses 62% que estão colocando IPv6 para os clientes, nós tínhamos só 14% que tinham mais de 80% dos clientes com o IPv6. Ou seja, a média dos 50%, eles têm uma aplicação pequena, ou média, no máximo, do IPv6.

E por que acontece isso, agora que a gente está nesse momento que a gente tem os ASs, os Autonomous Systems, apenas com IPv6? E aí precisam entrar em técnicas de tradução e tudo mais. E isso eu até vou deixar aí, talvez Uesley e Rubens podem comentar com muito mais propriedade sobre isso.

Só que qual são as dificuldades que a gente tem visto, e os provedores têm encontrado?

Um, ainda os provedores têm tido uma falha, e os sistemas de gerenciamento de provedores, alguns, eles ainda não estão 100% aptos a fazer o gerenciamento, o *accounting* dos IPs e tal. Hoje, com o Marco Civil e tudo mais, os provedores têm uma responsabilidade grande do armazenamento de informações, alguns ainda se sentem um pouco inseguros na oferta de IPv6 devido a esse tema.

Mas eu acho que isso também é uma coisa que pode evoluir mais rápido e tudo mais, até mesmo porque é muito mais seguro e muito mais fácil o provedor fazer o *accounting*, o log de quem tem IPv6, do que ter que fazer IPv4, principalmente quando você não tem IPv4 disponível e tem que usar CGNAT e tudo mais, que é muito mais difícil e muito mais caro de armazenar logs.

Um outro item é o CPEs dos clientes que... Como nós temos quase que um caso único no mundo... O Brasil hoje, de longe, é o país que tem o maior número de operadores, de fornecedores de Internet presencial, e são mais de 20 mil provedores. Isso não se tem replicado em nenhum outro lugar do mundo. Você tem um universo gigante de

equipamentos, de CPEs dos clientes instalados já há alguns anos, e novos que estão sendo instalados.

E esses CPEs, muitas vezes, eles não têm um suporte, de fato, assim, efetivo, que funcione bem com o IPv6. Então, às vezes os provedores encontram alguns problemas, algumas falhas e eles ficam na dúvida o quanto esse CPE, ele, de fato, ele é compatível e funciona bem na pilha dupla com o IPv6.

Até esse é um assunto que talvez depois a gente pode falar mais sobre o tema aí, de talvez um trabalho que vocês, Eduardo, Moreiras já fazem aí no IPv6, há muitos anos. Um trabalho primoroso. Acho que vocês são muito responsáveis já por nós estarmos, nesse momento, com o uso do IPv6, né? Se não tivéssemos esse trabalho do NIC, com certeza estaríamos muito mais atrás.

Mas eu acho que poderia pensar na questão que a gente já falava um tempo atrás, de a gente treinar o pessoal dos provedores a capacitar eles, a eles saberem avaliar bem qual CPE é compatível com o IPv6, não é. Ou seja, ensinar mais pessoas a fazer esses testes e poder, de fato, homologar o CPE de uma forma mais fácil, mais segura do que é compatível com o IPv6 ou não. Porque a gente sabe que muitos CPEs vem lá na caixinha IPv6 ready, mas, na prática, não é tão bem assim, né?

E aí um outro apontamento que vem dos provedores é que às vezes eles encontram algum bug, incompatibilidade, seja em CPE ou seja alguma falha na rede. E aí a gente até... Eu acho que como ainda para muitas pessoas o IPv6 é uma coisa nova, a gente sabe que é protocolo aí já há muitos anos. Mas, às vezes, pode também, ainda faltar um conhecimento técnico ou não, ou, de fato, ter os bugs. Quando eles encontram alguma falha, talvez eles desativam esse serviço, tá? Então, eles desativam o serviço do IPv6 e aí, isso acaba não acontecendo. Um exemplo, até, ontem, eu fui fazer testes de site e tudo mais. E o que eu vi? Nesses sites, por exemplo, sites de grandes portais aqui do Brasil não estão com IPv6 disponível, alguns. Os sites do governo, que eu acho que seria muito importante o governo, já que ele aprovou o marco civil e tudo mais, ele apoiar, né, o uso do IPv6. Se a gente olhar, os sites estão todos com... inacessíveis através do IPv6, não é?

Então, eu acho que o conteúdo também é importante. E talvez até acho que o Rubens ou o Uesley, ou vocês mesmo aí, Eduardo, Moreiras, possam falar até com um pouco mais de propriedade. É uma percepção que às vezes se tem, é quando alguém encontra um problema, talvez agora até esses ataques *hackers*, e tal, eles, às vezes, acabam optando por desativar isso por uma falsa sensação de melhorar a segurança ou uma coisa a menos para tratar, enfim.

Então, eu acho que o conteúdo, ele também é muito importante. Eu acho que aqui no Brasil, pela rápida pesquisa que eu fiz ontem, é um dever de casa muito importante, a gente fazer aqui no Brasil, para que o conteúdo esteja muito mais disponível, né, em IPv6. Até mesmo, por quê?! Os ASNs IPv6 *only*, eles vão ter muito mais problema para fazer essa transição, esse acesso a conteúdos que vão estar só em IPv4, não é? Então, eu acho que é um momento já delicado, que temos que trabalhar com isso para que o conteúdo esteja mais disponível e isso também vai ajudar na adoção da implantação do acesso. Porque se o conteúdo está disponível, é muito mais fácil fornecer o acesso. A gente também pode acabar com essa desculpa que muitas vezes a gente escuta: ah, o provedor de conteúdo não tem acesso, então, não tem por que eu ainda disponibilizar IPv4, ficar colocando uma carga de trabalho a mais para o suporte e tudo mais.

Eu acho também, que esse item é muito importante que todos nós, provedores, a gente procure também fazer um trabalho de educação interna, não é? Porque hoje, a gente sabe que, por exemplo, com esse trabalho que o NIC fez, a gente tem as pessoas do NOC, e tudo mais, elas conhecem o IPv6 e tudo mais. Mas o pessoal do SAC, pessoal do suporte, muitas vezes, eles ainda não conhecem, não é? Então, tem o treinamento do IPv6 lá, on-line e tudo mais, mas eu acho que é importante também, a equipe dos NOCs fazer esse trabalho de educação interna em cada empresa, para que mais pessoas tenham conhecimento do IPv6, não é? Então, eu acho que isso, ainda, a educação também é muito importante, e o conteúdo e o acesso.

Mas acho que já está dando o meu tempo. Então, acho que já agradeço. Inicialmente, seria isso aí, Eduardo, Moreiras.

SR. ANTONIO MARCOS MOREIRAS: A gente é que agradece. E eu gostaria de passar a palavra agora, sem mais delongas, para o Rubens Marins, da Brisagnet. Por favor, Rubens.

SR. RUBENS MARINS SCHNER: Olá, bom dia, pessoal. Obrigado pelo convite, mais uma vez, para a gente poder falar sobre a nossa experiência de IPv6 aqui. Eu só queria comentar antes que, esse AS que o Moreiras falou, 28126, ele me é muito familiar, esse número desse AS, não é? Ele é muito familiar e, sim, a nossa, né, aquela geolocalização ali, não está tão precisa.

Até falando sobre esse negócio, que é na parte do IPv6, eu imagino, realmente, que numa rede como a nossa, ou na maior parte das redes que ele vai usar NAT, no nosso caso, a gente usa o NAT todo concentrado em um ponto, né, quando é o NAT. Então, ele dá uma confusão na cabeça do cara lá. Porque tem algumas pessoas, de uma cidade lá, Fortaleza, chegando lá, daí, de repente, aparece um cara lá de João Pessoa, na mesma rede /24 que está aparecendo para ele lá, não é? Imagino eu que ele está pegando a geolocalização por outros

métodos. Então, eu acho que, realmente, daí, por essa questão NAT, essa geolocalização do IPv4, realmente, ela se torna uma tarefa muito difícil de ficar precisa e ela está variando o tempo todo, não é?

Sobre a nossa questão da migração do IPv6, eu já tive a oportunidade de falar um pouquinho, vou mostrar aqui só um único slide aqui, que eu tenho aqui. Deixa eu voltar aqui para o Zoom. É, pelo jeito eu não vou conseguir mostrar aqui, porque eu não configurarei o Zoom antes para liberar, mas, então, eu vou falar só, do dado. Que a gente está com 94.3% hoje, das nossas cidades, elas estão navegando com *dual stack*, e eu tenho 5,7% das cidades navegando somente IPv4.

Como eu tinha falado na outra oportunidade, o que atrasou a nossa migração de IPv6 foi incompatibilidade com o fabricante, e nesse caso fabricante de *router* e *switch*, né, que não... atrasou muito a nossa migração. E depois, atrasou também para a gente fazer o *terminal deployment*, não é? Mas até o final desse ano, de 2020, a Brisanet vai estar com 100% de IPv6 migrado na rede.

Aquilo que o Rosauro estava comentando antes, do negócio do CPE, realmente, é uma coisa muito interessante. E eu recomendo que você não acredite no que o fabricante lhe conta. Eu recomendaria para todo mundo que você pegue o CPE, coloque em um laboratório, teste isso, teste aquilo, faça um caderno de testes, talvez, de IPv6, o que você quer que funcione. Ah, eu quero que funcione o *prefix delegation*, quero que funcione isso, DNS, etc. e tal. Tem que tudo colocar. Faça de todos esses tipos de testes. Não acredite no que eles falam, porque, virtualmente, todos os fabricantes: ah, eu tive que melhorar uma coisa ou outra aqui. Fabricantes de CPE, certo? Eu tive que testar na bancada, ir, colocar, e vai, e volta, não é? Então, isso é uma coisa muito interessante a se pensar.

E sobre o nosso caso aqui, então, como a nossa rede está quase toda *dual stack*, praticamente, sobre problemas que podem vir IPv6. Que o pessoal, às vezes, comenta: "Ah, se eu tiver IPv6, eu vou ter problema". A gente não tem nenhum problema aqui, que eu lembre, que seja grave, que foi necessário a gente fazer uma coisa ou outra para remediar o problema. Não teve nada que aconteceu, assim, que eu lembre, nenhum evento específico.

E eu concordo também que nesse ponto, assim, a gente, talvez, deveria pressionar mais o governo, ou o próprio governo, que ele quer assim: ah, vamos fazer algumas coisas. Mas os sistemas do governo, nenhum tem IPv6. Secretarias estaduais de Fazenda, que nem aqui, nota fiscal eletrônica, precisa emitir, e nenhum é IPv6. Os bancos, até a última vez que eu chequei, não tinham IPv6 também. E isso é um tráfego que é, apesar de ser pequeno, ele é muito importante, porque você depende do serviço do governo, depende dos serviços do banco,

não é? A nível de volume e de tráfego, o IPv6, ele é bem alto aqui na nossa rede, por causa dos maiores provedores de conteúdo, né, de vídeo e tudo mais, eles já estão tudo com IPv6 habilitado. Então, que é a maior parte do tráfego, isso dizendo o tráfego em bits por segundo, né, que seria Netflix, YouTube e outros, né, está tudo já com IPv6.

Então, basicamente é isso, assim. A Brisanet não tem nenhum problema com IPv6, assim. O problema foi todo antes, de laboratório, e vamos fechar 2020 aí, com 100% IPv6 *dual stack* na rede.

SR. EDUARDO BARASAL MORALES: Bom, muito obrigado, Rubens. Realmente, é muito interessante. E legal saber que vocês já estão prometendo, então, aí, se for um cliente da Brisanet, 2021, não tiver IPv6, liga para o Rubens, não é?

E queria falar também que essa é uma mesa que é quase uma volta no tempo, não é? Por quê? Porque a gente tem dois palestrantes que participaram do Intra Rede. O Moreiras está usando uma camiseta aí, do IPv6 que a gente fez ali para a Campus Party, não sei quantos anos atrás. E agora a gente vai ter o Uesley Correa, usando terno prateado.

SR. ANTONIO MARCOS MOREIRAS: Com muito orgulho aqui, a camiseta, hein?

SR. EDUARDO BARASAL MORALES: É, o orgulho da camiseta. E agora a gente vai ter o Uesley usando o terno prateado dos 10 anos do IPv6. Então, Uesley, fica à vontade.

SR. UESLEY SILVA CORREA: Bom dia a todos. Muito obrigado aí pelo convite de estar participando aqui dessa mesa. Para mim, é um imenso prazer.

Eu trouxe para vocês, além do terno prateado dos 10 anos de IPv6, um slidezinho pequeno, para a gente poder conversar e poder entender um pouco de que existe, realmente, vida após o esgotamento do IPv4. Deixa eu compartilhar minha tela aqui. Ok. Conseguem ver aí a minha apresentação? Ok? Certo? Sim? Me deem um ok aí, por favor. Beleza, beleza.

Então, vamos falar aqui rapidinho sobre se existe, realmente, vida após o IPv4. Essa apresentação vai estar disponível lá para download depois. Aí, tem uma pequena apresentação sobre mim. Depois, se vocês quiserem saber quem sou eu. E eu gosto sempre de usar esse slide aí, quando eu vou falar a respeito da transição entre o IPv4 e o IPv6. Porque desde que a gente começa a estudar, a gente aprende lá na escola, nas primeiras aulas de ciências, o que é uma transição. E aí, a professora de ciências usa o exemplo da transição entre uma lagarta e uma borboleta. E essa transição era o que era proposto entre o IPv4 e o IPv6. Hoje nós podemos dizer que já estamos mais perto da borboleta do que nunca. E para a borboleta, agora, resta

voar. Ela não vai poder ficar o resto da vida dela agarrada ali no casulo. Assim como nós não poderemos e nem deveremos ficar o resto de nossas vidas agarrados no IPv4.

E quando a gente fala um pouquinho sobre transição, sempre vem na nossa cabeça, as técnicas de transição. Os cursos do NIC.br são muito bons, falando sobre isso e sobre a transição entre IPv4 e o IPv6. E eu deixo a pergunta: hoje, essas técnicas são técnicas de transição ou de sobrevivência? Quando essas técnicas de transição foram criadas, aqui eu deixei uma nuvem de técnicas de transição, *4over6*, *464xlat*, *dual stack*, *map-T*, *map-E*, *Teredo SIIT*, etc. Essas técnicas, elas previam uma transição suave e segura entre esses dois protocolos, entre o IPv4 e o IPv6. Hoje em dia, algumas dessas técnicas aliadas a outras, porque as técnicas, novamente, elas eram de transição, e não de sobrevivência. Hoje, essas técnicas, elas estão sendo usadas como sobrevivência. Porque provedores que começam apenas com o IPv6, hoje eles precisam sobreviver em uma internet que ainda tem muito conteúdo em IPv4, como já foi citado pelos colegas anteriormente. E hoje, nós dependemos de algumas delas para sobreviver, principalmente os ASs que estão começando agora.

E aí eu trouxe algumas consultas sobre atualidades, essas consultas desses dados foram extraídas ontem, nós vimos aí que em pouco mais de 10 anos, um pouco mais de dois anos, desculpa, do ponto de vista do Facebook, nós tivemos um aumento de 10% de dispositivos que acessam ao Facebook em IPv6. Então, em um período de pouco mais de dois anos, 10%. É um bom número? É melhor do que nada. Mas significa que estamos caminhando. E isso baseado no tráfego Brasil.

Já do ponto de vista do Google, nós temos aí, uma adoção de 36.38%. Nós, o Brasil, somos o país que mais adotou IPv6 na América do Sul. Baseado na América Latina, nós estamos apenas atrás do México. E então está: México, Brasil, e logo em seguida vem o Equador. Ou seja, são países que estão tendo uma boa adoção de IPv6, 36% é melhor do que nada.

Mas tem um dado que é alarmante. Dos ASs com prefixo IPv6 anunciados, ou delegados para empresas, para provedores brasileiros, apenas 55.5% estão sendo anunciados na DFZ. Ou seja, nem a sua sessão BGP IPv6, o restante desses ASs ainda não fez. Nós não estamos falando de totalidade de operadores, nós estamos falando de totalidade de detentores de prefixos IPv6. Ou seja, apenas 55% têm os seus blocos anunciados por BGP. Ou seja, se ele não tem nem o bloco anunciado por BGP, certeza que ele não tem nenhum cliente rodando com o IPv6 ainda. E isso é alarmante.

Hoje, nós estamos aí terminando 2020, e não podemos mais alegar falta de conhecimento. O que mais temos disponível *à la carte*,

a *self-service*, à disposição de todos é conteúdo. NIC.br tem muito conteúdo, o BPF tem muito conteúdo, o Lacnic tem muito conteúdo, e se você for procurar no YouTube e souber selecionar bem, você também vai encontrar excelentes conteúdos, para que você possa fazer uma implantação do IPv6 na sua rede. Se é que você não quer pagar nenhuma empresa para fazer essa tarefa para você. Então, hoje em dia, já não podemos mais dizer que é falta de conhecimento.

E aí, temos um resumo. E eu vou falar um pouquinho mais sobre algumas outras coisas, no final dessa apresentação. Maior parte do tráfego internet, hoje, já está em IPv6. Vejam que não estou falando que a maior parte dos sites estão em IPv6, mas sim do tráfego. O que representa, hoje, tráfego grosso da internet, o que é? São os grandes geradores de conteúdo, os grandes hospedadores de serviço de internet. Esse tráfego, a maioria dele já está em IPv6.

Temos pouco mais de 50% dos ASNs brasileiros com seus blocos IPv6 anunciados na DFZ, então, temos ainda muito trabalho. Quanto mais IPv6 *only*, menos investimento em CGNAT. E importante, hoje, 2020, dezembro de 2020, praticamente 0% de ataques DDoS são feitos em IPv6. Ou seja, se você tem IPv6 em 100% da sua rede, DNS rodando em IPv6 e tudo mais, você pode se dar ao luxo de, quando estiver sofrendo um ataque DDoS daqueles massivos mesmo, seu serviço de mitigação vai te dar mais problema para resolver do que solução, você pode se dar ao luxo de ir ali, dar uma desligadinha na chave do seu IPv4. A maioria dos seus clientes não vai sentir nada, principalmente, porque os ataques DDoS são em horário de pico, 6 horas, 7h da noite, até as 21h, mais ou menos, que é a hora que o pessoal está em casa assistindo Netflix, vendo seu Facebook, vendo algumas coisas na internet, e esse tráfego está em IPv6. Ou seja, se você der uma desligadinha na chave, uma meia hora, 40 minutos. Daqui a pouco, você dá uma ligadinha na chave de novo para ver o que está acontecendo, se o cara lá parou de te atacar, você vai estar aliviado durante esse momento, tá ok?

E aí, agora, nós vamos falar um pouquinho mais sobre... deixa eu ver se eu ainda tenho tempo. Tenho tempo. E aí, nós vamos falar um pouquinho mais agora... Deixa eu arrastar minha tela do Zoom para o outro monitor, que aí eu fico de frente para vocês, ok? Falar um pouquinho a respeito de alguns temas também, que foram levantados pelos colegas aí, sobre CPEs, sobre sites. Realmente, há uma necessidade que os entes de governo deem uma prioridade maior à implementação de IPv6 nos seus sites, nos seus portais, nas suas plataformas. Porque isso também, obviamente, vai fomentar com que mais pessoas, com que mais ISPs se sintam motivados, ainda que eu não eu concorde com a motivação reversa. Eu não concordo com a justificativa de que "Ah, eu não vou botar IPv6, porque eu não tenho

conteúdo". Não. Nós estamos falando de um protocolo que já tem mais de 20 anos.

Falando sobre as CPEs, uma observação rápida do meu ponto de vista sobre as CPEs. Hoje, eu concordo 100% com o Rubens, façam seus testes na bancada. Só que eu dou uma recomendação, existe uma BCOP sobre CPEs, não vou lembrar agora o número dela, mas ela foi encabeçada e trabalhada, além de outras pessoas, pela Lucimara, do NIC.br. A Lucimara trabalhou muito nessa BCOP, e tem muita coisa de IPv6 ali nessa BCOP. Então, se você quiser escolher um roteador, pega a BCOP, olha o que a BCOP diz ali, e vamos ver o que esse roteador faz. E vamos testar, como disse o Rubens, vamos botar na mesa e vamos testar. Vamos testar. Não, isso não presta. Essa CPE não presta. A próxima, próxima. E aí, a gente chegar em uma definição de qual é a CPE que atende a gente.

E o último ponto, assim, para fechar os meus minutos aqui. Infelizmente, o mercado de equipamentos de soluções de telecomunicação trata a maioria dos seus usuários ou dos seus consumidores, diga-se de passagem, os ISPs, como suas cobaias. Eles enviam os equipamentos com *bug*, com erro, com problema e cabe a nós testarmos o equipamento e descobrir qual o problema, relatar para eles e eles se darem ao trabalho de corrigir o problema. E isso não estou falando de um fabricante, tá? Posso falar que 99,9% dos fabricantes fazem isso, e alguns te amarram em um contrato, para poder te dar a solução do problema que ele mesmo criou. Então, se nós estamos com problema em CPEs hoje, com IPv6, significa que, dado o nosso histórico de *beta testers* de equipamentos de telecomunicações, significa que nós passamos 20 anos sem testar os equipamentos que eles colocaram no mercado. E nós só estamos descobrindo os problemas agora, porque nós só começamos a fazer esses testes agora. E agora que estamos relatando, eles estão se dando ao trabalho de corrigir. Então, quanto mais rápido nós possamos descobrir esses problemas, mais rápido nós vamos ter uma solução também, para esse problema da CPE.

Muito obrigado aí, pelo tempo, pelo NIC.br, pelo IX Fórum, pelo convite. E estou aberto aí à maior discussão da mesa.

SR. ANTONIO MARCOS MOREIRAS: Muito obrigado, Uesley. Eu gostaria de fazer uma pergunta para os três. Eu vou chamando na mesma ordem que vocês fizeram as apresentações iniciais. A gente sabe que o CGNAT é inevitável. Sabe que no NIC.br, de vez em quando, a gente recebe perguntas pelas redes sociais, por e-mail, dos usuários falando: "Poxa, mas o meu provedor está me entregando um IP 'NATeado', tal. Será que ele está de sacanagem comigo, alguma coisa?" Não, está, não é? O CGNAT hoje, praticamente todos os

provedores têm que fazer. Os provedores não têm números IPs suficientes para colocar IPs públicos para todos os usuários.

Então, isso a gente vê como uma necessidade. Agora, tem algum jeito de fazer isso de forma mais correta? Tem um número de usuários, no máximo, pelo qual que você pode compartilhar um IP? Qual que é esse *rate* de compartilhamento ideal? Tem NAT estático, NAT dinâmico. Faz alguma diferença você definir, pré-definir as portas que o usuário vai poder usar? Ou você fazer essa alocação dinâmica de portas? Tem algum jeito de fazer o CGNAT, para que não dê problema nos *games*, para que não dê problema nos aplicativos? Então, Rosauero, por favor, a sua opinião sobre esse assunto.

SR. ROSAUERO LEANDRO BARETTA: Bom, Moreiras, o que a gente tem visto? O CGNAT, né, para a grande maioria dos provedores que não têm IPv4 suficiente, e a grande maioria dos ASNs, ele é uma triste necessidade, não é? Eu acho que aí, infelizmente, muita gente tem que fazer e tudo mais. Eu acho que, principalmente, sobre o item estático, dinâmico, além de alguns detalhes técnicos, eu acho que o que mais pega é como o provedor vai armazenar esses logs, não é? Porque hoje, cada dia que passa, é mais natural o provedor receber um ofício da justiça pedindo quebra de sigilo, rastrear e tal. E a gente tem visto, né, e isso também é outro item para se destacar, né, a polícia, né, eles têm feito um trabalho aí junto com o judiciário, um trabalho muito bom, assim. Eu tenho acompanhado algumas coisas que eles têm feito, eles têm, ou seja, pego muitos criminosos aí, dos crimes digitais, e tal. Então, acho que é um item que a gente tem evoluído bastante. Obviamente, que é um item que tem que andar mais ainda, mas tem sido feito um trabalho muito bom.

Então, acho que o que o provedor tem que definir se é estático ou dinâmico, vai depender, principalmente, de como ele vai fazer essa guarda dos logs. Se ele vai ter uma solução que ele vai pegar um CGNAT pago, não, enfim. Vai usar uma solução mais *open source*. Enfim, acho que é uma decisão muito do momento do que o provedor está fazendo.

Sobre essa questão de número, de quantos usuários você consegue colocar atrás de um IP, e tal, eu penso o seguinte, que esse número seria assim, quanto menos, melhor, não é? Ou seja, esse seria o ideal para poder ofertar uma qualidade melhor. Mas o que eu tenho ouvido dos provedores, do que eles têm feito, principalmente os que têm feito soluções mais *open source*, mais na mão, é aí, alguma coisa de 2 mil portas por usuário e tal. Obviamente, que isso também depende muito da quantidade de IPv4 que ele tem e a quantidade de CGNAT, a proporção que ele tem que fazer. Ou seja, também depende da necessidade que, às vezes, o provedor se vê obrigado a trabalhar, não é? Então, aí, também varia muito dessa necessidade.

Acho que basicamente é isso aí. Acho que talvez sobre essas questões de portas, técnicas, aí, o Rubens e o Uesley também podem comentar com mais propriedade.

SR. ANTONIO MARCOS MOREIRAS: Legal. Obrigado, Rosauero. Rubens, você pode comentar um pouco? Está no mudo, Rubens. Por favor, abre seu microfone.

SR. RUBENS MARINS SCHNER: Ah, desculpa. Então, CGNAT, para nós, sempre foi um problema, porque, devido à escala e o tamanho da Brisanet, né, era sempre problemático fazer NAT, realmente, nessa grande escala, não é? E é um problema para nós, manter isso. Então, com toda a nossa rede praticamente migrada para IPv6, a maior parte do conteúdo em bits, né, tanto já nos grandes provedores, a gente gera 1.2 tera de log de NAT por dia, 1.2 tera de log NAT por dia. Essa é a quantidade que gera.

E não é só o problema de armazenar isso. O problema também, é que, como eles falaram, quando a polícia chega e fala assim: Ó, eu quero saber a identificação de alguém. Você tem que meio que dar um grep em um arquivo de 1.2 tera, e isso é uma coisa que demora dias. Então, na verdade, demora dias para nós podermos processar e responder, porque 1.2 tera, eu comprimo, ele vai para uns 300 giga. Então, eu tenho que descomprimir 300 giga, uma operação que demora quase um dia. Aí, depois, eu tenho achar os IPs lá dentro, uma operação que demora também, muitas horas. Então, CGNAT, realmente, é um problema e uma carga.

Também tem o problema do custo do CGNAT, que é enorme, porque você pode ir fazendo ele em pequena escala, colocando o mais perto possível do cliente, mas aí, você tem que, realmente, ter bastante IP sobrando, rede para isso, não é? A gente resolveu concentrar todo o nosso CGNAT, porque daí você tem uma distribuição melhor dos IPs, não é? Então, você tem uma cidade muito grande, com muitos clientes na mesma caixa com uma cidade muito pequena, senão você é obrigado a fazer uma mágica aí, de balanceamento dos IPs para um lado e para o outro. Então, daí, você otimiza mais.

Então, hoje, a gente está com uma taxa que é variável de 8 a 14 clientes por IP. Por que é variável? Ele é tão dinâmico que, em uma determinada hora, ele faz mais ou menos. Mas esse balanceamento não é preciso, porque em uma caixa, você vai lá e coloca um /22... /22 não, um /21 ou 20, por cada caixa, para ela fazer o NAT de dezenas, centenas e milhares de clientes. Então, dependendo da quantidade de dispositivos conectados e tudo mais, ele tem que fazer mais NATs, certo?

Então, hoje, aqui, a gente está nessa faixa de 12, de 8 a 12 IPs por cliente, não é? E, realmente, é um desafio grande manter o CGNAT mesmo, hoje, no ar. E a gente fica sempre comentando, se nós temos

todo esse trabalho e está tudo com IPv6, imagina os outros? Como eles fazem isso? Olha, eu não entendo, nem quero saber a dor que o cara passa lá, né, sobre isso.

E voltando a essa questão dos logs, não é? A polícia quando quer o dado, às vezes, ele quer na hora, ele não entende, ele não vai... E dependendo, o cara é juiz, o cara manda o negócio: Ó, quero esse dado e quero para amanhã. E você se vire para achar o dado. Eu, realmente, não sei como é que os outros provedores conseguem puxar os dados e entregar em um tempo hábil. Por isso que eu acho que o CGNAT, realmente, é um problema grande, não é?

SR. ANTONIO MARCOS MOREIRAS: Legal. Obrigado, Rubens. Realmente, o CGNAT é um problema, mas é um problema que a gente tem que conviver, não é? E esse tipo de conversa é importante para a gente buscar formas de lidar com esse problema do melhor jeito possível, não é? Fazendo com que ele seja menos um problema.

Eu quero lembrar a todo mundo que está assistindo também, que amanhã, a gente vai voltar nesse tema IPv6. O Eduardo e a Erina vão fazer uma apresentação, onde eles estão fazendo, justamente, um levantamento do que está faltando no Brasil. Então, será que realmente o governo, como muitos painelistas citaram, não está implementando? Bancos, tem algum que já tem? Não tem? Então, tem um levantamento muito interessante que a nossa equipe está fazendo, e que amanhã vai ser apresentado.

Uesley, você pode comentar, por favor, sobre a configuração de CGNAT?

SR. UESLEY SILVA CORREA: Sim, claro. Hoje, nos cenários que eu tenho visto, está girando entre 2 a 4 mil portas por usuário, quando se faz um CGNAT determinístico, não é? Então, os provedores têm escolhido, mais ou menos, essa configuração. Só que ainda, nessa configuração, você fica travado com os *gamers*, que eles usam muito mais portas do que isso, e você precisa ficar abrindo exceções, exceções. E, infelizmente, como o Rubens falou, CGNAT é uma coisa que não escala. Para escalar, você precisa investir muito mais, e você precisa de muito mais dinheiro e você precisa consumir muito mais IPs. No caso de operações grandes, até a operação, talvez, tenha muito IP sobrando, muito IP disponível. Agora, no caso de operações, vamos dizer, até médias, mas que não conseguiram, lá no início, pegar seus blocos /20, /19, e hoje precisam conviver com um ou dois blocos /21 e 22, isso se torna bem mais complicado.

E aí, entram as soluções de *bulk port allocation*, que existem soluções tanto proprietárias quanto *open source*. As soluções proprietárias, infelizmente, você vai estar amarrado em um custo alto. E, como o Rubens falou, é um custo alto, é um custo que você tem que pagar isso, porque, infelizmente, não tem muito para onde correr. E

tem muitos provedores que não têm, não fazem, não se dão conta disso. E alguns, às vezes, semanalmente eu recebo perguntas: como é que eu procuro um log de um CGNAT determinístico que eu fiz aqui? Um CGNAT que eu fiz com netmap? Aí, eu devolvo a pergunta: se você fez o CGNAT e não sabe como consultar um cliente nele, aí fica complicado. Porque muitos fizeram, assim, meio que sem orientação, sem procurar informação, e fizeram da primeira maneira que apareceu na sua frente. E agora eles estão enfrentando o problema de ter que identificar um usuário.

E hoje, temos aí, algumas soluções *open source*, caso do Danos. Inclusive, tem artigos na wiki do BPF falando sobre ele. É um artigo escrito pelo Gondim, muito bem escrito, por sinal. O Gondim está usando lá, é uma solução *open source*, faz BPA. E aí, você tem que gravar em um log externo, em um syslog ou em um graylog, ou alguma outra solução de log externo para você poder ter essa comprovação de quem é o usuário.

Mas, nessa média, está girando, principalmente se você tem um *dual stack*, você pode começar aí, com 2 mil portas, e se você estiver usando um BPA, você pode começar com 256 portas e o BPA vai entregando de 256 blocos de 256 portas, até chegar em um limite de 4 mil portas, ou 5 mil portas, não sei. E nesse limite, você já determina: Olha, esse cliente não compensa estar no CGNAT. Ele usa muita porta. Por mais duro e triste que seja, compensa colocar um IP público para ele, porque ele está onerando demais o nosso CGNAT. E daí, vida que segue.

SR. EDUARDO BARASAL MORALES: Muito obrigado, Uesley. Realmente, tudo que vocês estão falando aí é bem interessante, dos problemas relacionados ao CGNAT.

Bom, queria fazer mais uma pergunta, não é? Olhando os números da Anatel, né, que até o Rosauro comentou, de licenças e dispensa de licenças da SCM, a gente vê que o número de provedores é provavelmente muito maior do que o de Sistemas Autônomos registrados aqui no Brasil, que a gente tem ali perto de 8.557. Provavelmente, metade dos provedores não têm blocos IPs próprios. E hoje, na prática, né, como a gente vê, não tem como mais, receber endereços IPv4 diretamente do registro .br. Tanto que está surgindo, o quê? Sistemas Autônomos IPv6 *only*. E alguns desses Sistemas Autônomos IPv6 *only* já estão até entrando no PTT.

E aí, eu queria saber, na opinião de vocês, como que um provedor consegue sobreviver só com IPv6? Ele usa os IPv4 do trânsito para fazer um CGNAT? Ou isso é insuficiente? E as técnicas de tradução de IPv6 para IPv4? Há alguma outra opção? O que o provedor que está nessa situação deveria fazer? Então, eu gostaria de chamar o Rosauro para comentar primeiro.

SR. ROSAURO LEANDRO BARETTA: Bom, Eduardo, essa é uma boa pergunta e é quase que a pergunta de 1 milhão de dólares aí, de quem está entrando. Porque, o que eu vejo que acontece? A grande maioria, tá? Não todos, mas a grande maioria dos Sistemas Autônomos que estão entrando agora, são de pequenos provedores, são de provedores iniciantes, muitas vezes. E esses provedores iniciantes, tá, não posso afirmar um percentual, mas eu acredito que seja tranquilamente mais de 50%, eles têm algumas deficiências, não é? Que é, talvez, um investimento limitado, também. Então, ele tem que buscar ter o conhecimento. E às vezes, muitas vezes, ele também tem uma certa falta de conhecimento. E eu concordo com o que o Uesley falou antes, que a falta do conhecimento, ela não é uma desculpa, não é? Não pode ser. Como não pode ser uma falta, uma desculpa a pessoa dizer que não conhece as leis que temos no Brasil. Mas, infelizmente, aí você olha um universo tão grande de empresas e pessoas que estão nesse meio, você sempre vai cair em um universo de pessoas que ainda precisam buscar esse conhecimento, e tal, e que talvez precisam se dedicar um pouco mais nisso.

Então, eu acho que esses aspectos, eles impactam nessa implementação, porque hoje não existe como você trabalhar só IPv6 *only*, né, porque você não vai dizer: Olha, eu vou entregar só uma parte do conteúdo, enfim, e tudo mais. Eu concordo também, que a maior parte do conteúdo utilizado, do conteúdo consumido, ele está disponível, mas, que nem foi comentado, em sites, em opções, infelizmente, não tem. Se você precisar usar para, como foi citado, bancos. Eu até fiz uma pesquisa rápida ontem, aí dos seis, sete bancos mais usados, tinha um ou dois só, com suporte de IPv6 na página inicial, não é? Não vou nem falar de outros serviços e tudo mais, tal. E os outros, ninguém tem. E como serviço de nota fiscal, como foi comentado pelo Rubens e tal.

Então, você vai ter que fazer essa questão da tradução, não é? Você vai ter que utilizar. E aí, qual é o caminho para isso? Eu acho que o caminho, primeiro, que o provedor tem que ter, é buscar o conhecimento. Ele aprender para ele poder conhecer e poder optar, né? Porque você vai encontrar soluções pagas, vai encontrar soluções *open source*, e como que você vai definir? Ou você busca o conhecimento, ou você busca quem tem o conhecimento para poder te ajudar a tomar essa decisão, tá? Mas, de fato, é um caminho que é um mal necessário, então, vai ter que ser feito. E, infelizmente, eu acho que a gente ainda vai conviver por muitos e muitos anos com essa questão da transição. Que seria o ideal que não acontecesse, não é? Mas, infelizmente, eu acho que é nessa linha aí.

SR. EDUARDO BARASAL MORALES: Bom, muito obrigado, Rosauro. Vamos chamar agora o Rubens, para comentar sobre o assunto aí, da pergunta de um milhão. Rubens, você está no *mute*.

SR. RUBENS MARINS SCHNER: Olha, eu acho que essa resposta é simples: não tem como você ser um provedor de internet só com IPv6, você não consegue. Não há a menor possibilidade. SmartTV, virtualmente, todas, só funcionam com IPv4. Os videogames, todos só funcionam com IPv4. Eu não sei agora, o Playstation 5, o novo Xbox, mas os outros, se tiver só v6 na rede, ele já diz: ó, não tenho conectividade com a internet. Mesmo que algum jogo implemente. Jogos também, praticamente todos são só Is(F). Então, nisso, você tira uma grande parte do pessoal que não consegue acessar IPv4, somente IPv6, de forma nenhuma.

Eu tinha falado na outra... do Intra Redes, que a gente se esforçou muito por fazer uma coisa, né, somente v6, usar um NAT 64, alguma coisa assim, não teve jeito de, no cliente final, ele ter só IPv6.

Então, eu não acredito ser possível para um provedor de acesso à internet, ter somente IPv6 rodando. Talvez um provedor de conteúdo de alguma forma possa fazer alguma coisa assim, mas eu não consigo imaginar como aquele AS realmente consegue prover serviços para a internet, seja de acesso ou seja de conteúdo, estando em uma coisa somente IPv6.

SR. EDUARDO BARASAL MORALES: Tá certo, Rubens. Agora, Uesley, gostaria de comentar?

SR. UESLEY SILVA CORREA: Sim. Falando aí sobre, até complementando o Rubens, eu já fiz alguns testes de somente IPv6, entre aspas, usando 464XLAT. E te digo que, vamos botar aí em 98% dos casos, ele vai funcionar, porque a CPE do assinante vai entregar IPv4 para aquele dispositivo que não tem suporte a IPv6. E quando chega na CPE, ele encapsula aquilo por IPv6, mas ainda precisa de um IPv4. Porque lá do lado do PLAT, você precisa disso.

O que hoje impossibilita um provedor, uma operação usar o 464XLAT? Soluções, CPEs compatíveis e tudo mais. Eu trabalhei em várias soluções, em várias frentes, fiz vários laboratórios com ISPs pequenos, fiz vários laboratórios internos e, assim, eu não achei uma CPE que funcionasse o 464XLAT bem. Ou seja, eu tive que comprar um roteador que fosse compatível com openWrt, instalar o pacote do CLAT no openWrt, e daí, fazer o laboratório. Só que isso, em uma escala de um laboratório interno para dez CPEs, é fácil. Agora eu quero ver escalar isso. Impossível, isso não escala.

Então, ou a gente consegue um fabricante, como é o caso, por exemplo, da Telecentro, na Argentina. A Telecentro é uma operadora de TV a cabo e de internet, eles conseguiram fechar com um fabricante e desenvolveram, junto com fabricante, o suporte ao 464XLAT nos *cable modems* dele. E aí, esse suporte, essa firma, automaticamente pelo CMTS, foi instalada em todos os *cable modems*, e está todo mundo feliz da vida usando o 464XLAT. Mas nós estamos falando de uma

operação que compra muitas CPEs mensalmente. O fabricante viu negócio nisso.

Então, talvez, pelo lado de uma associação de provedores que vejam que 5, 10, 20, 50 provedores têm interesse nisso, juntar a compra de CPEs desses provedores e ir atrás de um fabricante que se disponha a fazer isso. Mas aí, a gente incorre em outro problema, o casamento com o fabricante da CPE. Porque aí, você vai estar casado com ele e se ele, amanhã ou depois, quebrar, falir, sumir, desaparecer, você vai estar viúvo desse fabricante, com uma solução que você, talvez, não vai dar continuidade. Ainda que o 464XLAT tenha RFC, tenha sido definido, tenha vários *cases* de sucesso. Mais, obviamente, em redes móveis, celulares, mas existem *cases* de sucesso em redes fixas.

Isso, no meu ponto de vista, foi o que o impossibilitou a maior propagação e a maior facilidade do 464XLAT em um ambiente ISP. Mas seria, por isso que eu falei que seria, seria a resposta do milhão, mas não é a resposta do milhão ainda. Então, infelizmente, muitos ainda vão estar reféns do CGNAT. Infelizmente, se tiver só um /29 da operadora ou um /27 da operadora, não vai conseguir escalar, e a gente vai ter que esperar as cenas dos próximos capítulos dessa novela. E eu estou ansioso para fazer parte dessa novela aí, de continuar ajudando os provedores com o que eu puder, com o que a comunidade puder e fazer isso daí acontecer, porque não dá para nadar e morrer na praia.

SR. ANTONIO MARCOS MOREIRAS: Muito obrigado, Uesley. Muito obrigado a vocês três, ao Rosauro, ao Rubens e ao Uesley. A gente sabe que foi um excelente painel. Tenho até certeza que as 307 pessoas que estão assistindo no YouTube agora, vão aproveitar o nosso intervalo para dar aquele like e deixar o vídeo sendo mais divulgado.

Mas o painel deixou, acho que algumas coisas aí, até em aberto, não é? Porque mesmo com essas técnicas de transição que o Uesley citou, ainda precisa de IPv4. Lá por baixo do capô, tem um tipo de NAT sendo feito, mesmo nas técnicas de transição. Então, esses provedores que não têm recursos de IP próprio, eles estão em um mato sem cachorro. Realmente, estão em uma dificuldade enorme. Que vão ter que ser bem criativos para conseguir se virar e conseguir permanecer no mercado, continuar crescendo no mercado. E parece que o caminho, até pelos comentários de vocês todos, o caminho é, realmente, acelerar a implantação do IPv6 e ir buscando a resolução desses problemas todos. O pessoal que não tem, é o governo, os *games*, os equipamentos, etc. e tal. Eu acho que a gente tem que buscar formas de acelerar a implantação do IPv6 e isso acho que vai ser a única solução viável e escalável--

SRA. ANDREA ERINA KOMO: Pessoal, parece que a gente teve algum problema ali na conexão do Moreiras. Mas também gostaria de deixar aqui meu muito obrigada. O painel foi muito rico, acho que esclareceu várias dúvidas do pessoal.

E, então, eu vou dar sequência aqui na nossa agenda. Eu queria propor agora, um intervalo, um breve intervalo, né, para o pessoal pegar aí, um café, esticar um pouquinho as pernas. Então, vamos fazer um intervalo de dez minutinhos, e daqui a dez minutos a gente volta. E durante esse intervalo, a gente vai deixar ali um *timer* rodando no vídeo, junto com alguns vídeos que a gente tem, do projeto Cidadão na rede. Então, para o pessoal que não viu ontem, a apresentação, a gente tem um novo projeto chamado Cidadão na rede, de videozinhos curtos, de 15 segundos. Tentando passar ali, algum ensinamento rápido em relação a redes, internet, boas práticas, não é? Como usar a internet de forma mais segura, e melhor aí. Então, peço para colocarem o videozinho. E vamos iniciar intervalo de dez minutinhos. Obrigada, pessoal.

ORADOR NÃO IDENTIFICADO: Obrigado.

[intervalo]

[exibição de vídeo]

SR. JULIO SIROTA: Bom, pessoal, vamos dar prosseguimento aqui na nossa agenda. A próxima apresentação, a gente vai contar com a participação especialíssima do Alvaro Retana, que é uma pessoa superimportante aí, na comunidade da internet, muito ativo no IETF. Ele vai trazer uma apresentação para a gente, sobre o que tem de novo em protocolos de roteamento.

Como o Alvaro vai estar falando em espanhol, nós vamos ter tradução para o português durante a apresentação dele. E, nesse caso, para quem está nos acompanhando pelo YouTube, a gente vai ter disponível três canais, tá? Esse que quem já estava anteriormente vai ser o canal traduzido em português, a gente vai ter um segundo canal com o som original, ou seja, sem nenhuma tradução, e um terceiro canal traduzido para o espanhol, tá? Então, vamos lá, Alvaro. Pode dar início à sua apresentação.

SR. ALVARO RETANA (por intérprete): Bom dia, Julio. Muito obrigado, em primeiro lugar, pelo convite. É um prazer estar aqui. Aqui onde eu moro faz muito frio. Eu não estou no Brasil, como vocês, onde está mais quente, não é?

Como o Julio falou, eu trabalho no IETF, como diretor da área de *routing*. E hoje vou falar sobre o trabalho que nós realizamos recentemente nessa área. Se alguém tiver alguma pergunta, a

qualquer momento, por favor. Aqui teremos uma visão geral de todo o trabalho da área, que é uma área, um setor bastante grande. Então, eu vou falar em termos mais gerais. A expectativa é que nós possamos discutir diversas coisas sobre o trabalho que estamos fazendo aqui nessa área.

O IETF, como vocês sabem, é a organização que, na verdade, que cria as normas para a Internet. Uma organização aberta, aberta com relação ao fato que essas normas podem ser usadas qualquer pessoa, mas mais importante, qualquer pessoa pode participar dos processos também no IETF, sejam estudantes, engenheiros, operadores, pesquisadores, qualquer pessoa pode participar do processo. É uma organização na qual participamos como pessoa física. Eu trabalho na Futurewei, aqui nos Estados Unidos, mas trabalho no IETF também individualmente, num nível pessoal, como Álvaro. Não tem ninguém no comando. Não tem uma empresa, na verdade, que controle o IETF. Qualquer pessoa pode contribuir. Nós temos que simplesmente escolher uma área que nos interesse, seja IPv6, qualquer área, qualquer processo de interesse. O resultado são as normas, os regulamentos para a Internet que qualquer pessoa poderá usar e todos nós poderemos nos beneficiar dessa colaboração que haverá entre diversos indivíduos que participam do IETF, da IETF, que é a força-tarefa, que tem missão muito simples, muito fácil, e, ao mesmo tempo, difícil, que é fazer com que a Internet funcione melhor. O que nós fazemos sempre é do ponto de vista de engenharia, o que podemos melhorar para ter uma Internet melhor hoje. Muitas das normas, na verdade, são usadas por muitos anos e também demoram para serem criadas e implementadas.

Na última palestra, ouvimos falar de IPv4 e IPv6. Vocês estão acostumados com a evolução da implementação da IPv6. A IETF, na verdade, criou essa norma há mais de 20 anos, e ainda continuamos desenvolvendo a implementação em diversas partes do mundo. Então, na IETF, todos trabalham sobre a camada física e por baixo da aplicação. Muito do que nós fazemos são blocos com os quais podemos construir serviços, aplicações para transporte, para TCP, para todas as normas de e-mail, roteamento, segurança, etc. No momento, há 123 grupos de trabalho diferentes na IETF. Cada grupo, na verdade, focando um tema, um assunto, uma área específica. Esses grupos são formados por participantes individuais, pessoas físicas. Não tem associação. Nós, então, adotamos o processo de consenso e, de forma geral, queremos que existam códigos, implementações. Muito do que fazemos tem a ver com implementações. Consideramos as implementações no momento de criar uma norma. E esse é um dos mantras da IETF, ter códigos, implementações que podem ser implementadas... implementarmos o que nós estamos definindo como

normas, porque já que vai ser usado na Internet, queremos que funcione. E teremos sempre verificar isso.

Grupos de trabalho, no IETF, são divididos por área. Temos sete áreas, como vocês poderão ver na tela. As seis de baixo são áreas técnicas, onde trabalhamos em diferentes temas, segurança, transporte. Em transporte, por exemplo, tem muito TCP, agora também o protocolo [ininteligível], que é novo no IETF, para roteamento, IPv4, IPv6, por exemplo. E a área geral, onde está a área administrativa. Então, é onde são discutidos e definidos assuntos administrativos. Por exemplo, agora que estamos todos trabalhando no mundo remoto, por causa da pandemia, estamos falando sobre como podemos trabalhar melhor, se teremos que cancelar as reuniões físicas no futuro, não só pela pandemia, mas por outras questões que possam acontecer, que... bom, talvez nos levem a cancelar uma reunião, quais serão as melhores ferramentas para reuniões virtuais. São os assuntos que são tratados nessa área geral.

Então, eu vou falar sobre roteamento. E essa área de roteamento é responsável pela operação do sistema de roteamento na Internet. É algo enorme, muito amplo, porque nós queremos ter uma Internet estável, que possa crescer também. Então, temos certas características do protocolo de roteamento que devem ser consideradas para que possa crescer e acompanhar o tamanho da estrutura da Internet. Atualmente, temos 24 grupos na área de roteamento, grupos de trabalho, e três diretores de área. Eu sou um dos diretores de área, da área de roteamento, e é uma área muito grande com relação ao trabalho que nós fazemos. Ainda que muitos dos protocolos já sejam maduros, já existam há muitos anos, onde há implementações que já são usadas há muitos anos na Internet, há muito trabalho. Aqui temos uma comparação entre as diversas áreas, e vocês verão aqui que a área de roteamento, primeira, à esquerda, tem mais que o dobro do trabalho do que a segunda área. Então, medimos isso pelo número de documentos que processamos. E os seis maiores grupos do IETF, bom, todos estão nessa área de roteamento. IDR é o grupo que faz TGP. Todos dependemos disso. Então, realmente, é muito trabalho que é feito aqui nesse grupo do IDR e dos outros cinco que temos aqui hoje.

Então, eu gostaria de falar um pouco para vocês do que nós estamos fazendo. Temos aqui esses 24 grupos em nossa área. E eu tratarei de explicar como nós agrupamos esse grupo, por tipo de trabalho, dependendo do protocolo que estivermos desenvolvendo em cada um. Então, eu vou falar dessa distribuição e falarei também de alguns deles, desses grupos, não todos, senão não acabaríamos. E gostaria também de destacar alguns trabalhos mais recentes que temos nesses grupos, que é interessante também para vocês. Então, vocês poderão ter essas referências aqui, que poderão consultar

depois, no seu tempo livre. Se não houver perguntas até aqui, continuarei, mas fiquem à vontade para fazer perguntas, tá bom? Durante a apresentação.

Nesses 24 grupos de trabalho, estão divididos os protocolos core, importantes, que realmente gerenciam o centro da Internet. São protocolos que fazem roteamento de unicast, IGP, SPF, ISS. Os protocolos fazem multicast. Temos dois grupos de trabalho, PIM e o grupo de trabalho Bier, eu também vou aprofundar um pouco mais em cada um, e o grupo Spring, que desenvolveu, nos últimos anos, tecnologia, uma tecnologia que vem sendo muito usada em diversos protocolos de serviços, e nós incluímos aqui no grupo principal esses protocolos. Por exemplo, o grupo de IDR, grupo da BGB é o maior grupo que temos na IETF, no que diz respeito ao trabalho, e é um dos grupos mais conservadores também. Eu disse antes que é muito importante termos códigos de implementação, e no grupo IDR, nós temos duas implementações, são necessárias antes do documento avançar, para ser RFC. Isso é muito importante porque estamos mudando o BGP. Se houver uma mudança que não funciona ou que vai acabar provocando um defeito ou algo negativo na Internet, nós queremos saber com antecedência, não é? Do documento ser um RFC. Então, requer sempre duas implementações independentes. O IDR antes que os documentos avancem.

E, recentemente, temos feito, por exemplo, ampliamos o tamanho das mensagens BGP. O BGP é usado para transportar um monte de coisas, como vocês sabem. Não só rotas, mas também para transmitir informação de dois documentos, um sobre Flow Specification, que são as regras que posso aplicar na minha rede. Então, para deter um ataque, eu posso me comunicar pelo BGP de um sistema com outro, e enviar as regras, por exemplo, para deter um ataque, impedir um ataque, ou o que chamamos de [ininteligível] também que fala de como transportar informação dentro do BGP, que vai gerar outros protocolos, como SPF ou ISS, e assim poderemos dar informação ao controlador que poderá depois definir como a rede vai se comportar.

E, depois dessa apresentação, haverá uma palestra sobre comunidades, que é algo também importante, que foi definido pelo grupo IDR, large communities, que será um dos assuntos abordados na próxima palestra.

LSR, grupo de link state routing, é um grupo relativamente novo, mas que trabalha com protocolos antigos. E nós fizemos o seguinte. Percebemos que o mesmo trabalho que estávamos fazendo em OSPF estava sendo repetido no ISS. Então, vimos os protocolos e criamos um único grupo de trabalho. Agora, temos sempre uma única discussão e fazemos extensões para os dois protocolos. Então, trabalhamos

sempre juntos, fazemos um trabalho para o ISPF e o trabalho do ISS basicamente ao mesmo tempo. Temos os exemplos que coloquei aqui, o RFC 8919 e o RFC 8920, sobre atributos específicos para os links, para as diferentes aplicações, para poder definir diferentes comportamentos de aplicações dentro de uma rede, tanto para ISS como para OSPF. Os dois, então, andam sempre juntos. Temos outros trabalhos que incluem os dois protocolos ao mesmo tempo. Por exemplo, vocês verão aqui embaixo o trabalho de algoritmos flexíveis. Então, podemos aqui sinalizar que tipos de algoritmo, além do SPF normal, poderíamos usar dentro de um protocolo OSPF ou ISS. Estou ouvindo alguém no fundo. Tem alguém com microfone aberto. É uma pergunta? Mas está muito longe. É uma pergunta? Está muito longe, não dá para ouvir.

O grupo Bier também é um grupo que já existe há quatro, cinco anos. Esse grupo está pensando em novas formas de fazer multicast. Começou como experimento, faziam documentos experimentais. Porque as mudanças que estamos propondo aqui requerem uma mudança de hardware, não apenas de implementações, mas o hardware também, ou seja, os computadores que vão ser... onde a Internet vai ser implementada. Então, vocês podem ver a especificação aqui do Bier.

E temos aqui o RFC 8279, as redes que não são MPLS. Estamos neste momento tratando de temas importantes para todos. Então, como usar Bier em uma rede IPv6. Estamos trabalhando nesse documento que vocês veem aqui, são os requerimentos, os requisitos para ter Bier e esse tipo de multicast que usa um bit field, então uma série de bits para definir onde estão os setores na rede. Isso fazemos em cooperação com os protocolos tradicionais que mantêm o estado dentro da rede. No caso do Bier, não mantemos um estado, mas ele é implementado pelos bits, e assim poderemos ter múltiplos resultados em diferentes lugares.

O Spring é um grupo muito ativo. Tem realmente trabalhado muito ativamente nos últimos anos e trata de uma nova arquitetura, como definir o destino dos pacotes a partir da fonte. Então, a fonte, seja na barreira de domínio, é que define por onde esses pacotes passarão. Então, temos aqui a 8402, que é o número do RFC e já fizeram muita coisa, tanto em... para IPv6. Um documento importante do SRv6 routing(F) que vimos aqui embaixo, Network Programming, temos aqui a informação que pode estar no pacote IPv6, para definir o que vai acontecer com esse pacote. Esse documento está praticamente já concluído. Nos próximos meses deverá ser publicado como RFC já. Esses são os protocolos gerais, portanto, que todos conhecemos, trabalham com IP, e os protocolos que rodam na estrutura da Internet. Temos protocolos que são mais especializados. Nós temos mais desses protocolos que eles são maiores em volume do que os gerais. Eles

usam redes de mesh ou grupo roll(F), que trabalha em roteamento também para Internet das Coisas. Então tem muitas coisas em desenvolvimento aqui. Protocolos específicos, que podem ser, por exemplo, no caso da Internet das Coisas, queremos usar menos energia para manter a tabela de roteamento, é um pouco diferente o que estamos usando, portanto. Temos também algumas implementações muito específicas para diversos cenários.

Esse protocolo Babel, eu gostaria de mencionar, é usado em redes tipo mesh(F), e esse foi um experimento interessante na área de roteamento, porque já trouxemos o protocolo que já existia fora do IETF, especialmente para implementações acadêmicas e de redes comunitárias. E nós padronizamos. Então havia um processo, nós discutimos o protocolo em profundidade, acrescentamos segurança e várias outras coisas que não tinha antes, uma descrição melhor e agora estamos já padronizando, normatizando o primeiro documento. Vemos aí que eu mencionei, RFC 6126bis é o que padroniza esse protocolo Babel, que é muito interessante. Vocês conhecem o protocolo da age RP(F) da Cisco? É muito parecido a esse protocolo.

LSVR é um dos dois grupos de trabalho que criamos há dois, três anos, para desenvolver protocolos especificamente para centro de dados. Então, todos sabemos que podemos usar BGP, SPF, ISS em um centro de dados e há RFCs também que falam especificamente de como usar GP. Temos dois grupos. Esse é o 1. LSVR é dedicado à criação de um protocolo especificamente para centro de dados. Esse protocolo usa uma mistura do transporte BGP, o transporte normal baseado em BGP, com mecanismos ou codificações de BGP [ininteligível] que eu mencionei antes. Então, as codificações usadas para transportar a informação em cima do BGP. Estamos fazendo, portanto, sobre o BGP. Estamos criando um novo protocolo baseado em SPF, similar aos SPF, que usa modificações BGP ou transporte para criar outro protocolo [ininteligível] novo para usar no centro de dados. O grupo de trabalho, recentemente, enviou para publicação o documento já. Vocês podem ler aqui esse primeiro. Para quem estiver familiarizado com o BGP será muito fácil compreender o documento, porque ele usa base e um algoritmo OSPF, que é uma diferença significativa para o leitor.

Outra coisa que está sendo desenvolvida por esse grupo de trabalho é o que nós chamamos de Layer 3 Discovery. É um protocolo novo para descobrir vizinhos de nível 3. Então, principalmente em casos como um centro de dados, onde queremos ser mais dinâmicos, queremos vizinhos mais dinâmicos. O BGP precisa de uma sessão para ter mais informações e assim será mais dinâmico. Esse grupo LSVR está trabalhando nisso, nesse tipo de protocolos.

O grupo Rift, que é outro grupo de trabalho, que também vem desenvolvendo protocolo para centros de dados. E, nesse caso, temos

uma mistura de link-state, tipo SPF, ISS, com distance-vector, que é usado em GLP ou Rift. É uma combinação disso. Basicamente usa link-state, centro de dados, e esse vector para baixo. Envia o default para baixo, para todos saberem por onde sair quando estiverem indo norte, sul, e o grupo de trabalho também considera já este trabalho concluído. Vocês poderão ler o documento. Ele está também acessível aqui.

Temos trabalhado muito também, recentemente, sobre determinística. O DetNet é o grupo que vem trabalhando nisso, para determinar como podemos garantir uma entrega de pacotes na rede. Seja por uma latência, que tem um máximo específico, e que seja confiável. Não pode repetir o fluxo, entre um fluxo e outro, dentro de uma mesma rede. É um trabalho muito parecido e estamos trabalhando em conjunto com triplo A, triplo E, triplo A(F), desculpe, o grupo de TSN também, que eles estão aí, de time sensitive network. É um trabalho importante porque tem triplo A, GTF3, GPP, que vem usando isso já em suas redes. Então temos vários documentos que poderão ler aqui, arquitetura. O trabalho específico de como usar Detnet numa rede [ininteligível] ou IP também. Detnet trabalha com links físicos.

Mas temos outro grupo novo, que existe há menos de um ano, chamado Raw, e tem um objetivo muito parecido ao do Detnet, mas sobre links em âmbitos. Desculpem, sem fio. Sem fio, porque há interferência e outros tipos de ruído. É muito mais difícil garantir a entrega de pacotes. Mas esse grupo Raw vem trabalhando nisso, no wireless, e já está em plena operação. Temos alguns casos de uso aqui embaixo, estão aqui nesse draft. E temos aqui também as tecnologias que [ininteligível] ser usadas, desde, por exemplo, 80215.4 e tecnologias específicas da indústria aeronáutica, chamada LDACS. Também está disponível para leitura, com as especificações e discussões e também o que vem fazendo o grupo Raw.

Outro subgrupo, digamos assim, é área de Sub-IP. Já há muitos anos, há 20 anos, eles têm sua própria área, e temos, acima de tudo aqui esse trabalho sob a camada IP. Estamos falando de MPLS, essa camada 2, tecnologias óticas, [ininteligível] aqui, e esse grupo MPLS, que está sempre muito ocupado. E agora, principalmente, fazendo manutenção, mas com coisas interessantes também, como identificação de fluxo, em uma estrutura MPLS.

O grupo mais ativo é o grupo Teas. E o Teas é encarregado da arquitetura, cuida da arquitetura, sinalização para engenharia de tráfego. Então, trabalha num alto nível na arquitetura. Vai definir, então, a estrutura de tráfego e algumas seções. Então, vemos aqui alguns documentos. Temos aqui o 8283, que fala da arquitetura para usar um controlador central dentro de uma rede. E aqui verão mais embaixo alguns dos documentos. Não só do protocolo PCE, mas

também com Enhanced VPN, que em outros lugares [ininteligível] falam de slicing(F), que é como vou dividir a rede para proporcionar diferentes tipos de tráfego em diferentes partes lógicas da rede.

Também temos aqui, acima de tudo, grupos que dão apoio ao roteamento. Por exemplo, o grupo BFD(F), todos conhecemos o protocolo do BFD, que detecta as falhas mais rapidamente e permite, então, que a operação continue, a manutenção dos links, e eles trabalham muito de perto, sim, com equipes de roteamento. Um grupo que se descarrega de distribuir interface para que entidades externas, controladoras, etc., possam acessar o sistema de roteamento, usando protocolos.

E este é o grupo também muito ativo. PCE, Path Computation Element, que basicamente define um controlador e um protocolo [ininteligível] para poder interagir com os roteadores. Então, temos, por exemplo, aqui, em algumas áreas, temos o mantenedor estado na rede, nessa primeira extensão aqui, 8231, depois extensões para o segment routing, e esse trabalho temos... o spring terá controle usando o protocolo PSP, PCEP para definir e gerenciar computadores. Temos outros também, como mencionei, o Flow Specification, e podemos não apenas receber a mesma informação através de IP, mas também de PCE ao mesmo tempo. Temos, portanto, não apenas o reuso da tecnologia, mas também na área há uma forte colaboração entre os grupos de trabalho. São muitos grupos, tem muito trabalho e existe uma ótima relação entre todos também.

Este grupo de serviços de roteamento também se encarrega, por exemplo, de definir a virtualização, os VPNs nível 2 ou 3, como faz o grupo Bess, por exemplo. E temos outros grupos que já existem há mais tempo, como o Bess, que é o segundo grupo mais ocupado, digamos, do IETF, na área de roteamento, e é quem define serviços, usando BGP. É o controlador. Então, que é mais usado, é o que mais tem trabalho em todo o IETF, e é o grupo que está focado em MVPN, mas os VPNs para multicast também. Vocês podem ver, então, alguns trabalhos aqui, como, por exemplo, como uso e aplicabilidade do MVPN, redes de integração de Routing e Bridging, pontes e roteamento em VPN, por exemplo.

NVO3 é um grupo que está definindo a virtualização. Então, por exemplo, temos, aqui capsulamentos que são normais no centro de dados, Geneve 8926, e agora estão elaborando a norma que vai ser VXLAN-GPE. Espero que saia já no próximo ano essa especificação.

São grupos interessantes porque não trabalham apenas em roteamento, como poderíamos pensar tradicionalmente. Também trabalham em encapsulamento, que é parecido de alguma forma com aquilo que já vem sendo feito no grupo Lisp, que começou como um grupo que inicialmente tentaria fazer com que essas salas crescessem

mais, mas, hoje, tem um número de aplicações que são usadas como overlay, por exemplo. Lisp começou como um grupo experimental e hoje produz... trabalha padrão.

E, como temos tanto trabalho, temos o grupo adicional. E, assim, caso não caiba ou não consigamos fazer os trabalhos nos grupos existentes, podemos recorrer a esse grupo de trabalho em áreas gerais. Então, vem atuar com outros grupos de trabalho. E, claro, tem o trabalho de roteamento em outras áreas. Área de operações é muito importante porque operamos redes e, ao mesmo tempo, geramos implementações novas dentro do GPR.

Então, gostaria de terminar convidando vocês a participarem, porque temos muito trabalho. O IETF sempre poderá contar com a participação de operadores, operadores de qualquer tamanho, grandes, pequenos, tradicionais, não tradicionais, e estão todos convidados a participar. Basta vocês assinarem, se registrarem e submeterem seus comentários, suas ideias. Se tiverem alguma pergunta ou algum comentário, será um prazer conversar com vocês. Ainda temos alguns minutos aqui. Imagino que o Júlio, então, possa coordenar isso.

SR. JULIO SIROTA: Sim, Álvaro. Temos duas perguntas. Eu vou... uma é do Fábio Aquino. Ele pergunta: Então, qualquer pessoa pode colaborar com o IETF? Tipo, escolher um projeto, problema e terá o apoio do IETF e do respectivo grupo para esses estudos?

SR. ÁLVARO RETANA: Sim. A resposta curta é sim. É um pouco mais complexo do que isso. O IETF trabalha com base em consenso. Isso significa que sim, qualquer pessoa pode apresentar uma ideia ao IETF, mas o que nós queremos é que haja interesse de mais pessoas. Então, por exemplo, se for um operador que... se tiver outros operadores com problemas parecidos ou soluções parecidas, nós poderíamos criar uma solução para todos. Então, sim, qualquer pessoa pode, sim, participar, trazer ideias, mas é muito importante encontrar o apoio de outras pessoas para conseguir fazer com que o trabalho avance. Pessoas que talvez leiam o documento, façam comentários e apoiem a ideia. O IETF é uma comunidade. Então, sim, muitas pessoas no Brasil que já participaram e podem ajudar quem tiver interesse a estabelecer relações. Sim, é totalmente aberto.

SR. JULIO SIROTA: Ótimo. A segunda pergunta é do Pedro Henrique Diniz. Ele quer saber como funciona a questão de numeração de RFCs? Cada unidade de milhar está associada a uma área e cada centena a uma subárea ou existe algum tipo de regra ou lógica para essa numeração?

SR. ÁLVARO RETANA: Não, não há um sistema específico. Tem um editor de RFC, um grupo que trabalha e define os números. Alguns números, por exemplo, podem ser solicitados, no caso do BGP, o RFC

4271. Se em algum momento nós revisássemos esse RFC, poderíamos pedir para o editor um número parecido [ininteligível] talvez, e eles vão assim contribuindo consecutivamente. E, além disso, não é só IETF, mas tem outros grupos que produzem RFCs. Não existe nenhum específico, mas vocês podem visitar RFC [ininteligível].org e encontrarão toda informação de como podem fazer isso.

SR. JULIO SIROTA: Ok. Obrigado, Álvaro, pela participação.

SR. ÁLVARO RETANA: Eu que agradeço o convite. Espero que possamos nos ver em pessoa, pessoalmente, em breve.

SRA. ANDREA ERINA KOMO: Participem do IETF e proponham mais RFCs.

Bem, vou seguir aqui na agenda, pessoal. Agora, para o próximo painel, gostaria de convidar aqui o Antonio Galvão de Rezende Filho, o Antonio Marcos Moreiras e o Júlio Sirota, eles vão comentar um pouquinho sobre Blackhole, Large Communities e Novas Communities no IX.br. Então, por favor, a palavra é de vocês.

SR. JULIO SIROTA: Tá ok. Também quem vai participar junto com a gente é o Tiago Felipe Gonçalves, que é o nosso consultor em BGP e routing server. Deixa eu compartilhar aqui a apresentação.

Bom, a ideia dessa apresentação é a gente trazer para vocês algumas atualizações e novidades na área de communities que a gente usa dentro do IX.br, tá? Então, assim, a ideia é meio que iniciar com a comunidade aí uma discussão, uma troca de ideias sobre o que que a gente está implementando. A gente está aberto aí a algumas discussões, a pequenos ajustes que se façam se necessários aí nessa proposta aí que a gente tem. Então, assim, a ideia, hoje, aqui, é fazer uma apresentação rápida, apresentar as informações e a gente poder ter tempo aí para responder algumas perguntas, trocar algumas ideias, tá? A gente vai divulgar esse trabalho através do site do IX, a gente vai colocar o documento em português, em inglês, para que todo mundo esteja ciente aí do que que a gente vai ter, tá?

Então, assim, panorama atual, quer dizer, dos route servers, né? Quer dizer, hoje, a gente tem uma versão em São Paulo que roda multi-BIRD, um suporte a Communities, filtros, validação de origem usando RPKI e os dados do registro BR. E, nas demais localidades, a gente está usando o Bird 1.6, com suporte a communities, com filtro de anúncios inválidos, as coisas normais de validação, mas ainda sem a validação de origem. Tá? Então, um trabalho aí que a gente está desenvolvendo durante esse ano, que é a gente levar essas funcionalidades que a gente tem hoje em São Paulo para todas as localidades, tá?

Então esse é um trabalho que ele está praticamente pronto. A gente estaria iniciando uma implementação em produção, em algumas

localidades agora, já no... a gente queria fazer isso antes do IX fórum, mas, por questão de férias do pessoal e essa época aí meio conturbada aí de Natal e Ano-Novo, a gente preferiu adiar isso para o começo do ano que vem. Mas é um trabalho que ele está muito adiantado, já.

Então, vamos lá. Communities informativas. Ou seja, são communities que a gente insere dentro dos anúncios que saem do routing server com algumas informações.

ORADOR NÃO IDENTIFICADO: Júlio?

SR. JULIO SIROTA: Oi?

ORADOR NÃO IDENTIFICADO: Os slides não estão passando.

SR. JULIO SIROTA: Espera aí. A minha tela não está compartilhada, é isso?

ORADOR NÃO IDENTIFICADO: Está compartilhada, mas a gente está vendo só o primeiro slide, o de título. Agora sim.

SR. JULIO SIROTA: Tá. Agora estão vendo?

ORADOR NÃO IDENTIFICADO: Perfeito.

SR. JULIO SIROTA: Tá ok. Então, vamos lá. As informativas. Ou seja, a gente já informa qual é o ASN de origem que a gente recebeu o anúncio e qual a localidade do PTT que está fazendo esse anúncio. E aí, agora, a gente vai ter umas informações novas. A gente vai estar informando um valor de RTT, uma classe de RTT que a gente percebe entre o routing server e o peer e também uma medida de perda de pacote.

Então, vamos lá. Alguns comentários sobre essa questão de RTT e perda de pacote. O RTT a gente vai estar fazendo alguns testes entre o route server, um dos route server e o peer provavelmente com medida a cada 15 minutos e em janelas, a cada três horas, a gente vai avaliar os 60 melhores resultados que a gente obtiver e vai ter uma medida da latência entre o participante e a infraestrutura de rede do IX, tá? Perda de pacote. A ideia é fazer testes durante horário de pico, entre as 7h e as 11 horas da noite, para a gente verificar se o link do participante tem principalmente algum problema de saturação, tá? A gente quer pegar uma exceção, tá? A gente quer saber se na pior condição existe algum problema, para poder classificar. Ou seja, para quem está fazendo engenharia de tráfego poder tomar alguma decisão durante, por exemplo, os horários de pico. A gente não considera que uma conexão normal, que tenha perda de pacotes, deva continuar em produção, tá? Quer dizer, isso tem que ser aberto um tíquete de suporte, isso tem que ser corrigido. Essa ferramenta aqui não é para resolver esse problema. Tá?

A parte de engenharia de tráfego, já são communities que a gente... algumas a gente já tem, hoje, em uso, que seria anunciar para

um ASN específico ou não anunciar para um ASN, quer dizer, que isso aí substituiu os filtros que a gente tinha. A adição de Prependes sem nenhuma, vamos dizer assim, necessidade extra. Ou seja, a definição de quem está anunciando quer que ponha mais preprendes, e também a gente aceita fazer Graceful Shutdown com o peer.

Agora a gente vai ter algumas possibilidades de fazer engenharia de tráfego em função de que em RIR que o ASN que a gente vai enviar o anúncio pertence. Então, a gente pode escolher não anunciar para um determinado RIR. Ou seja, o ASN que pertence ao Arin, Lacnic, Afrinic, Apnic etc., ou anunciar somente para ASs de um determinado RIR. A gente tem opção também de não anunciar para o BR. Ou seja, ASs brasileiros não recebem esse anúncio ou anunciar somente para ASs brasileiros, tá?

Definição, tá? AS brasileiro, para a gente, é um AS que está listado no arquivo FTP que o registro BR publica diariamente com todos ASs de alocações de blocos IP. A gente não utiliza a base de dados do Lacnic para fazer essa validação, tá? Aí a gente tem uma nova community que foi solicitada pela comunidade, que é não anunciar para uma determinada localidade do IX. Tá? Então, nesse caso, quando esse anúncio chegar naquela localidade, ele não vai ser anunciado, tá? Essa tabela, que hoje a gente usa o DDD das localidades, né? Quer dizer, tanto na... quanto a gente informa qual é a localidade do IX que está fazendo o anúncio quanto essa agora, tá? Então, assim, a gente está discutindo, e provavelmente a gente deve mudar um pouquinho essa tabela, tá? Porque existem algumas situações, tipo no Paraná e acho que lá entre Campina Grande e João Pessoa, em que tem... é o mesmo DDD para mais de uma localidade do IX? Tá? Então, isso aí a gente vai mudar um pouquinho essa tabela, tá?

Quando, dentro dessa lógica, quer dizer, nova, existe uma precedência, tá? Quer dizer, se você vai fazer o anunciar somente, você diz: vou assinar só para um ASN, então isso tem precedência sobre o Brasil ou outro RIR. Se eu falar só vou anunciar para o Brasil e depois fala você fala: não, isso aí tem precedência sobre, por exemplo, alguma coisa em relação ao RIR, que envolveria, por exemplo, o Lacnic. Tá?

Bom, já apresentei para vocês, quer dizer, a informação do RTT e da perda de pacotes, tá? E utilizando esses parâmetros, a classe em que a comunicação entre o peer e o route server estiver, vocês vão poder escolher. Então, ou seja, eu vou querer fazer um anúncio só se tiver com uma latência menor do que um determinado valor. Ou seja, por exemplo, quero anunciar se a latência for maior que milissegundos. Quer dizer, eu tenho outro caminho, outra rota para trabalhar dentro do meu AS, tá? E também você pode inserir de um a três preprendes em função da classe de latência que a gente tem. Então, são essas três.

Algo equivalente sobre... utilizando a perda de pacote. Ou seja, você pode escolher não anunciar se a perda de pacote for maior do que um determinado nível, né? A gente tem dois níveis aí, 2% ou 10%, ou se for desconhecido. Ou seja, a gente não conseguiu fazer o teste de perda de pacotes com o peer. Da mesma maneira equivalente ao RTT, pode inserir de 1 a 3 prepends em função de nível de perda de pacotes que a gente identificou em horário de pico.

Bom, esses outros filtros, agora, a gente entra na parte de validação de origem. Então esses dois conjuntos já são os que estão em uso hoje. Ou seja, a gente marca o resultado da nossa validação em RPKI e em cima da base do registro, lembrando que o mais prioritário é a validação pelo RPKI, e, em seguida, a gente tenta validar com os dados do registro BR.

Agora, a gente também vai poder utilizar dados a partir de AS-SET. Tá? Ou seja, a gente vai consultar os IRRs, ver os AS-SET definidos por cada rede. E se o anúncio tiver contido dentro desse AS-SET, a gente vai progredir, a gente vai marcar o anúncio.

Sobre essa questão do AS-SET. Quer dizer, a gente vai consultar o PeeringDB para pegar essa informação e a gente pode encontrar algumas situações. A gente pode ter o AS-SET sem a informação da origem da onde esse dado foi registrado. Aí, nesse caso, a gente vai consultar todas as bases e vai ter uma informação geral obtida dessa consulta. Ou o que realmente é o preferido, em que a fonte da informação seja definida, tá? Então, o PeeringDB está aceitando dois formatos, que é AS-SET@ o data base, ou o data base dois dois-pontos e o nome do AS-SET. Essa segunda opção é a preferida, é isso que a gente vai, vamos dizer assim, vamos estar trabalhando junto aos nossos participantes, para que façam a... cadastrem a informação com esse formato. Caso tenha múltiplos nomes de AS-SET para definir, podem estar separados por vírgulas. E aí tem uma lista dos sources suportados, que a gente vai estar consultando as bases desses IRRs. Amanhã a gente vai ter apresentação do Jolimar(F) sobre o PeeringDB e provavelmente ele deve colocar mais alguns detalhes em relação a essa informação, tá?

Outro novo teste que a gente vai estar fazendo é validando os anúncios, usando a base de dados dos diversos RIRs. Assim como a gente faz usando a base de dados do registro BR, a gente vai pegar a base dos outros RIRs para fazer validação de origem dos anúncios, tá? Hoje, na situação atual, a gente não está fazendo isso, tá? Então, para ASs que não são brasileiros, a gente marca como unknown, como, ou seja, a gente não conhece a situação da validação de origem, tá? Essas outras marcações, quer dizer, essas communities, elas aparecem em anúncios que vocês podem encontrar na tabela de rotas ou no Looking Glass, mas isso aí é filtrado, ou seja, a gente não exporta para os

participantes. Isso só aparece como uma maneira para informar para quem fez o anúncio de que existe um erro. Então seriam o tamanho de prefixo inválido, prefixos ASN Bogons e anúncios que tenham os ASNs Transit free, tá? Ou seja, isso já são communities. Isso aí já está em produção normalmente. O que a gente vai incluir agora é o nunca pelo route server. Que chama, dentro do PeeringDB, você pode cadastrar o never via route server. É do PeeringDB que a gente vai pegar essa informação para estar fazendo a validação ou não. Então, novamente importante. Quem quiser usar isso, utilizar o PeeringDB. A gente espera que no futuro essa lista aí de Transit free que a gente valida, isso seja substituído pelo never via route server.

E, finalmente, aí a gente vai começar a tratar, a aceitar communities para blackhole. Tá? Então, como que isso vai estar funcionando, tá? Ou seja, a gente vai receber um anúncio do participante que quer solicitar um blackhole para algum endereço IPv4 ou IPv6. Então esses prefixos têm que ser /32 para IPv4 ou /128 para IPv6. Na validação de origem, bom, primeiro, a gente só vai aceitar esses anúncios nesse primeiro momento de ASs brasileiros, tá? Para os ASs estrangeiros ainda a gente não vai estar aceitando. A gente espera fazer isso assim que a gente tiver com essa funcionalidade estável e ok para, vamos dizer assim, para esse mecanismo aí de blackhole esteja ok, a gente vê que não tem nenhum furo, tá?

Com relação à validação para os ASs brasileiros, a gente tem duas opções. A gente ainda está definindo, estamos querendo ouvir aí também a opinião da comunidade. Uma coisa é certa: a gente vai pegar o anúncio e vai validar em cima da base do registro BR. O que ainda a gente tem dúvida é se a gente vai aceitar isso somente se o SN de origem estiver conectado diretamente ao IX.br. Ou seja, for uma conexão [ininteligível]. Isso aí ainda que, vamos dizer assim, a gente está estudando, discutindo. Tudo isso por quê? Por questões de segurança, de confiabilidade do processo, tá?

Então, a gente recebe esse anúncio, valida. Se tiver tudo ok, a gente vai passar a exportar esse anúncio com a marcação de community de blackhole confirmado pelo IX.br, tá? E, nesse anúncio, o next hop vai estar alterado para a gente usar um MAC e um IP específicos, tá? Então, a gente, quando receber pacotes vindos desse MAC, a gente vai estar descartando esses pacotes, tá?

Bom, uma coisa que é superimportante, tá? A efetividade dessa funcionalidade de blackhole, ela é mais eficiente quanto maior for o número de participantes que estiverem aptos a configurar, aceitar os anúncios, tá? Então, para isso, eles vão ter que mudar suas políticas de entrada para aceitar prefixos /32 IPv4 ou /128 IPv6 marcados com a community 26162:666, seja extended ou large, confirmando que é um blackhole válido. Uma coisa que acabei não falando, mas que vocês

puderam ver em todas as communities, é que a gente está definindo e vamos passar a usar as larges communities também. Então essa também é uma outra questão que a gente vai ter que ver se, na prática, existe algum problema técnico ou não em relação às large communities, tá?

Então, era essa a apresentação. Agora a gente queria poder aí estar aberto aí para responder aos questionamentos aí.

SRA. ANDREA ERINA KOMO: Muito obrigada, Júlio. Estou vendo que o pessoal já mandou algumas perguntas no chat. Deixa eu ver aqui. Eu vou começar com a pergunta aqui que o Roberval Dantas enviou, colocou: Essas communities estão disponíveis em todos os IXs?

SR. JULIO SIROTA: Algumas delas sim. Se olharem a documentação que tem no site do IX, que tem um documento lá na área de documentação que descreve as communities que a gente já está usando, tá? Então as que tratam de engenharia de tráfego, elas estão ok, tá? Na parte de filtros, isso está funcionando tá? A parte de validação de origem, validação de anúncios, somente em São Paulo, por enquanto.

SR. ANTONIO MARCOS MOREIRAS: A Erina pediu para eu ajudar aqui na função de ler as perguntas. E, como era de se esperar, tem algumas perguntas e sugestões do Douglas Fisher. Então, o Douglas comentou que, muitas vezes, os ASs, no meio do caminho, filtram algumas communities de engenharia de tráfego que não endereçadas a ele. Ele nem considera isso uma prática muito legal. E ele diz que a vantagem, a grande vantagem das large communities é a possibilidade da gente ter indicado nela o ASN de origem e o ASN de destino. Então, isso facilita os filtros ou pelo menos tira a desculpa, né? Fala assim, o cara fala: "A community, eu tirei ela porque achei que estava endereçada a mim". Não, fica claro na large community que a gente tem origem e destino. E o Douglas notou que a gente não usou essa característica de large community. A gente não colocou, por exemplo, o AS 26162 dentro da large community, e ele coloca isso como uma sugestão. Então não é pergunta, é uma sugestão, mas fica para vocês comentarem um pouquinho, ou para a gente comentar, né?

SR. JULIO SIROTA: Tá. Não, isso aí realmente a gente já discutiu isso, tá? Então, a sugestão é bem-vinda mesmo. A gente já tinha reparado isso e talvez realmente a gente mude, tá? Então, o pessoal analisando aí algumas consequências, na parte prática, como a gente teria, mas provável que a gente mude isso.

Não sei se o Tiago tiver algum comentário a mais aí.

SR. TIAGO FELIPE GONÇALVES: Sim, uma coisa. Essas communities de engenharia de tráfego, a ideia delas, elas seriam mais para um uso local do participante diretamente conectado no IX para

poder fazer a engenharia de tráfego. E não para um ASN que está atrás do participante conectado fazer essa engenharia. Então, pelo menos essa é a ideia. E a gente normalmente limpa large communities em geral que estão marcadas com ASN do NIC para poder ter uma certa segurança e evitar mau uso das marcações feitas pelos route server. Então existe a possibilidade, acho que é interessante a gente discutir isso, só que a gente precisa ver as consequências.

SRA. ANDREA ERINA KOMO: Certo. Obrigada, Tiago. Obrigada, Júlio.

Eu selecionei aqui uma outra pergunta que enviaram no chat do Youtube e eu peguei a pergunta do Lima ou da Lima: Não seria mais seguro ter um route server específico para o blackhole? Então, Galvão, gostaria de comentar sobre, por favor?

SR. ANTONIO GALVÃO DE REZENDE FILHO: Sim. Um dos pontos, depois o Júlio e o Tiago podem complementar, mas nós temos dificuldades com os participantes. Por exemplo, em São Paulo, hoje, já temos quatro route servers. Então ter mais um ou dois para um backup, para não ter somente um, seria uma dificuldade a mais em estabelecimento dessas seções. E só teria efetividade se todo mundo, o maior número participasse. Então, esse é um ponto negativo aí que eu vejo dessa solução.

SR. JULIO SIROTA: Só complementando. A gente sabe que tem outros Internet exchanges que tem route servers específicos para blackhole. E, assim, a gente fica na dúvida se isso é uma situação legada, ou seja, no início, acharam que valia a pena e, agora, talvez tenha uma situação meio dividida, tá?

SR. ANTONIO MARCOS MOREIRAS: Vou fazer uma pergunta aqui que veio do Danton. O Danton, ele pergunta também sobre o blackhole, sobre o 666, se não há perigos de ataque de negação de serviços com uma enxurrada de anúncios nessa community. E eu estou interpretando a pergunta como sendo um ataque de negação de serviços direcionado à estrutura do IX.br. O que a gente pode falar disso?

SR. JULIO SIROTA: Bom, eu não sei, assim, a gente tem que avaliar esse tipo de situação, tá? A gente, durante aí as discussões aí dessa implementação, a gente tentou chegar a criar... a pensar em criar algum tipo de handshake entre o anunciante e route server com algum tipo de senha, validação, para tentar inibir esse tipo de situação, tá? Não sei. Acho que, assim, é uma coisa que a gente tem que continuar trabalhando. Nossa ideia é estar monitorando, né, o uso dessas *communities* de *blackhole*, e se tiver alguma situação indevida aí, talvez a gente tenha alguma ação.

Então, não sei se o Tiago tem alguma consideração sobre essa questão.

SR. TIAGO FELIPE GONÇALVES: E tem um detalhe que, por exemplo, se você está anunciando cem prefixos por X, e você tentar anunciar, sei lá, você tem o limite de cem prefixos e você está anunciando 70. Então, você tem uma margem para anunciar 30 *blackholes*. Se você passar esse limite de prefixo, sua seção vai cair. Então, vai acabar inibindo a possibilidade da pessoa fazer, por exemplo, 4 mil anúncios de *blackhole*.

SRA. ANDREA ERINA KOMO: Obrigada, Tiago. Obrigada, Julio. Chegou aqui uma pergunta do Luiz Gustavo, aí envolvendo um pouquinho do assunto de segurança, não é? "*Como será feita a validação dos anúncios de blackhole com RPKI?*". Então, queria saber se vocês já têm alguma informação em relação a isso, agora que o RPKI começou na nossa região aqui do Brasil.

SR. JULIO SIROTA: Tá. Assim, a ideia é não usar o RPKI para validação de origem de anúncios de *blackhole*, tá? A gente vai usar a base de dados do registro br, tá? Porque, senão, assim, quer dizer, todo mundo, toda ASN, todo AS precisaria gerar um ROA para cada um dos seus endereços IP, não é? Porque teria que ser um /32 ou um /128, tá? Então, no caso específico da validação de origem com a marca do *blackhole*, vai ser feito pela base do registro br.

SR. ANTONIO MARCOS MOREIRAS: Um dos comentários feitos pelo Douglas foi sobre a possibilidade de a gente implementar um ASN *probe*, uma espécie de bot que ficasse checando se os participantes já implementaram ou não a *community* de *blackhole*. Então, a gente podia fazer os anúncios /32 ou /128, IPv6, e, de algum lugar da internet, fazer o teste do ping para o participante específico, para ver se ele aceitou ou não aceitou aquela rota de *blackhole*.

Então, tem uma pergunta implícita aí, se a gente está pensando em fazer isso ou não, em ter algum tipo de *probe* para ver como que vai estar a aceitação da comunidade em relação à implementação dessa política. Porque ela não depende só do IX.br, não é? Como o Julio comentou na apresentação, ela depende dos participantes também aceitarem ou não isso.

SR. JULIO SIROTA: Tá. Bom, não sei. Acho que existe essa possibilidade, não é? Acho que o Galvão pode dar, depois, alguma contribuição aí, assim, em relação a como é difícil a gente monitorar, né, ou mudar as coisas que os participantes já têm em uso, tá? Quer dizer, normalmente, são processos bastante complexos.

Mas, internamente, a gente já chegou, por exemplo, a cogitar, por exemplo, mudar, né, as quarentenas automatizadas, para que elas

verifiquem isso, por exemplo, tá? Então, é uma ideia interna nossa aí que a gente vai ver, mas vamos analisar.

SR. GALVÃO REZENDE: Exato. Nós temos uma dificuldade tremenda com relação a isso. Mas, por outro lado, nós temos outros projetos dentro do NIC, do próprio NIC, que poderia trabalhar em conjunto com a gente nesse sentido. Por exemplo, o Simet, nós temos várias *probes* deles já distribuídas e poderiam ser usadas nesse sentido. Com certeza, é uma boa sugestão.

SR. ANTONIO MARCOS MOREIRAS: Ok. Eu vou continuar aqui nos comentários do Douglas Fischer. Comentários e sugestões aqui, para vocês comentarem também.

Um, voltando na questão das *large communities*, uma sugestão é que a parte das latências sejam... a gente use anotação em microssegundos, no segundo campo das *large communities*, não é? Como se fosse o tamanho da latência em microssegundo, vai dar um tamanho adequado lá, de um número de AS assim, não é?

Não sei se teria alguma vantagem de fazer isso ou não. E eu até vou complementar a dúvida, essas latências, elas não são arbitrárias, correto? Eu não posso colocar lá, 251 milissegundos, ou 23 milissegundos. São aquelas *communities* que já estão pré-determinadas, correto, na implementação. Pedir aí, para o Julio ou para o Tiago comentarem.

SR. TIAGO FELIPE GONÇALVES: Exato, Moreiras. A gente está colocando por grupos, a classificação, porque se a gente... a ideia inicial até era fazer a marcação de RTT e *loss* nas *large communities*, mas o que acontece com isso? Toda atualização do *route server* vai ser um valor diferente, e vai gerar uma quantidade absurda de *updates* para o BGP. Então, essa é a razão que a gente evita. A gente acha interessante porque é uma *community* informativa legal para o participante poder verificar e entender o comportamento, mas a gente tem uma certa cautela pela quantidade de atualizações. Pode ser que, em um futuro próximo, a gente habilite isso, que é bem simples para gente fazer do nosso lado.

SR. JULIO SIROTA: Tá. Uma outra coisa em relação a esses valores de RTT e *loss*, a ideia é que a gente vai ter aí um *script* que vai ficar fazendo essa medição, e a ideia é a gente disponibilizar uma consulta para esses dados, tá? Então, provavelmente no portal ou via alguma API, alguma coisa, a gente vai ter, entendeu? Para que isso possa ser checado, tá?

Assim, a expectativa é que esses valores, eles não mudem com muita frequência, tá? Ou seja, que seja uma coisa relativamente estável, tá?

SR. ANTONIO MARCOS MOREIRAS: Tem uma outra pergunta, que não vou citar o autor, por razões óbvias.

O autor da pergunta notou que o Team Cymru entrou recentemente no ATM do PTT de São Paulo, e ele nos pergunta se está tendo alguma tratativa especial, alguma negociação em relação ao serviço de UTRS. Tem alguma coisa, Julio, Galvão?

SR. JULIO SIROTA: Olha, eu acho que a pessoa mais adequada, que conhece mais ele, o serviço, é vocês, Moreiras. Você pode responder.

SR. ANTONIO MARCOS MOREIRAS: Então, eu responderia de que não. Esse serviço é um serviço bastante interessante, mas nós, do IX, não estamos com nenhuma tratativa, em particular, relacionada a *blackhole*. Mas eu recomendo para o pessoal que está assistindo a live, dar uma pesquisada no Team Cymru e nesse serviço UTRS em particular, porque ele parece bastante interessante.

SRA. ANDREA ERINA KOMO: Bem, pessoal, a gente está com o tempo... está quase acabando. Então, eu queria pedir um último comentário final aí, de cada um dos membros dessa mesa, falando alguma sugestão, alguma dica, algum comentário importante em relação aos assuntos. Então, eu queria pedir primeiro a palavra do Julio, por favor.

SR. JULIO SIROTA: Tá. Bom, assim, a ideia nossa é realmente, assim, é poder interagir com a comunidade, não é? Quer dizer, a gente aceita aí sugestões, a gente tem margem de manobra para estar mudando um pouco a implementação. Quer dizer, a gente está na fase final aí, e ajustes pequenos, isso a gente pode estar fazendo, sem problema, tá?

E assim, eu acho que, assim, existem vários e-mails que o pessoal pode entrar em contato com a gente. E se for o caso, pode abrir um tíquete de suporte dentro do portal do IX.br também, destacando esse tema, aí, que o pessoal vai encaminhar isso para a engenharia, tá?

SRA. ANDREA ERINA KOMO: Obrigada, Julio. Galvão, por favor.

SR. GALVÃO REZENDE: Só queria deixar registrado aqui que esse é um pedido antigo, né, da comunidade, igual o Julio comentou, e, assim, eu estou usando até a camiseta aqui, desde o ano passado, já, para fazer essa parte desse processo. Mas, enfim, acho que agora as sugestões são bem-vindas e acho que agora a gente finalmente vai conseguir implementar a *blackhole*.

SRA. ANDREA ERINA KOMO: Obrigada, Galvão. Tiago, por favor.

SR. TIAGO FELIPE GONÇALVES: Basicamente, eu acho que a participação da comunidade, eu acho que é muito importante nesses processos de mudança para funções, porque vocês têm a melhor visão do que vocês precisam que seja implementado. Então, eu acho que esse é o ponto crucial, e acredito que a gente não vai parar só nisso. A gente tem outras ideias, e, talvez, em um futuro próximo, a gente tenha outra apresentação, com mais outras funções.

SRA. ANDREA ERINA KOMO: Com certeza. Obrigada. Moreiras, suas palavras finais.

SR. ANTONIO MARCOS MOREIRAS: Bom, só chamar a atenção da comunidade técnica para que todos fiquem atentos a essas mudanças, porque algumas delas dependem, inclusive, da colaboração, não é? Como uma das perguntas que foi feita: Ah, como que vocês vão testar se a comunidade técnica está aceitando? Em particular, a *community* de *blackhole*. Se os participantes não fizerem a configuração para aceitar esses anúncios, de nada vai adiantar. Então, é muito importante que a comunidade técnica esteja atenta, que o pessoal aí que é consultor, que está assistindo, acompanhe isso de perto e oriente os seus clientes também. Ajudem a gente a nessa orientação, né, para fazer essa configuração de forma correta e o serviço funcionar bem para todo mundo.

SR. JULIO SIROTA: Então, é isso. Vamos encerrar, então, essa apresentação, painel aí. Eu queria agradecer a participação de todos aí, Tiago, Galvão, Moreiras.

Bom, agora, eu vou, dando continuidade à nossa agenda, eu vou chamar o Milton, tá, que é o diretor do Ceptro, que é a área do NIC que a gente trabalha, que ele vai estar falando sobre o Simet, tá? Que é solução de medição de qualidade, né, de acesso à internet, que o NIC tem. E ele vai estar falando sobre algumas novidades para os Sistemas Autônomos. Então, Milton, por favor.

SR. MILTON KAORU KASHIWAKURA: Bom dia. Eu vou aqui, compartilhar a tela. Então, estão conseguindo ver a tela?

ORADOR NÃO IDENTIFICADO: Sim.

SR. MILTON KAORU KASHIWAKURA: Ok. Então, vamos começar. É, acho que deu algum probleminha aqui, por causa desse compartilhamento de tela. Então... Deixa eu só interromper e começar de novo. Conseguem ver aí? Tudo bem, pessoal? Conseguem ver agora? Tá. Ok.

Então, falando um pouquinho sobre o Simet, não é? O que nós temos trabalhado aí, como novidade. Então... Bem, então, a gente já sabe que o Simet, né, ele faz medições aí de banda, latência, perda de pacote, *jitter* e nós estamos medindo também disponibilidade. E estamos começando aí com a BCP 38, em um outro formato, só para

os participantes do IX.br, que é muito mais fácil de medir se eles estão adotando a BCP 38 ou não.

Colhemos aí, também, né, quer dizer, junto com essas métricas de qualidade, o *timestamp*, métrica de contexto geográfico, não é? Então, pela geolocalização, a gente consegue separar aí por setor, distrito, cidade e estado, não é? E, também, vamos dizer assim, em alguns casos, estamos fazendo algumas medidas aí sobre o caminho para poder se chegar entre um destino até o outro. A novidade é que toda essa estrutura, né, ela está sendo trabalhada para que ele esteja em cima de uma estrutura escalável e também nos padrões do IETF, como o Alvaro Retana acabou explicando para vocês. Então, a gente colocou o Simet em cima de uma plataforma do LMAP, tá?

Então, a gente tem aí a parte do medidor web, não é? Então, é para os browsers de forma geral. Então, o Simet que é disponibilizado na plataforma, no formato da web, ele roda em Chrome, Firefox, Safari. Você pode utilizar também com os navegadores nos mobiles, então, ele funciona muito bem aí. Também na parte de mobile, isso daqui eu vou falar um pouquinho mais depois, sobre a novidade, também a gente tem a versão mobile, a gente tem novidade nessa parte aí.

E também na parte de software e roteador, quer dizer, que a gente também tem algumas novidades aí, né, para que a gente consiga ter mais medições aí, através de softwares, que são disponibilizados, e também através do próprio roteador doméstico que vocês acabam comprando aí nas lojas, desde que suportem o OpenWrt.

Aqui, né, pessoal, a gente consegue ver a quantidade de medições que a gente tem. São mais de 23 milhões de medições, né, únicas. A gente conseguiu aí atingir 5.323 municípios dos cinco mil quinhentos e poucos que a gente tem no Brasil, não é? A quantidade de Sistemas Autônomos que conseguimos detectar está em 7.525, né, dos 8,5 mil que a gente tem. Então, a gente tem uma quantidade de informação bastante interessante aí, no que diz respeito ao Simet.

Na parte de mobile, não é? Isso daqui é novidade aí, pessoal. Vocês podem encontrar aí, na Play Store. Então, eu coloquei o link aí, porque, vamos dizer assim, para achar o Simet Mobile beta, não é? É o que a gente chamou essa versão aqui, ela está na versão beta, não é? Quando vocês testarem, a gente captar as informações, os feedbacks, a gente vai movê-lo para Simet Mobile, tá? Então, aqui, vocês já podem baixar da loja da Google, não é? E vocês podem testar aí, esse novo aplicativo, tá? É um código totalmente reescrito para estar em conformidade com a LMAP, tem novas interfaces e recursos. A novidade é que, em relação a outros medidores aqui, né, para teste de conexão Wi-Fi local, né, porque a gente recebeu muitos feedbacks

de provedores, que gostariam também que se endereçasse o aspecto se tem problema na rede local do usuário ou não.

Então, a gente faz os testes locais para saber como é que está a qualidade local, né, e a gente avisa o usuário do que ele precisa fazer para poder melhorar essa qualidade local aí, não é? Quer dizer, então, ele vai alertar o usuário, caso o problema dele seja local. Quer dizer que não adianta nada você ter um teste contra os nossos servidores que estão no AS14026, que é o AS do Simet, que está presente no IX.br, se o problema, a maior parte do problema é local. Então, todas essas informações sobre latência, perda de pacote e *jitter*, se estiverem na rede local, fica ruim, para você falar que a qualidade de provedor é ruim. Então, primeiro tem que corrigir a parte local para, depois, fazer a medição de forma correta, tá?

Então, todos esses dados, junto com a parte de geolocalização, desde que o usuário permita, né, ela é enriquecida através de um *pipeline*, né, que a gente tem dentro do nosso ambiente, né, para que esses dados possam ser tratados, rá? Então, a gente tem uma estrutura aí, baseada em Kubernetes, isso daí facilita bastante a vida da gente, na parte operacional. Então, é tudo pensado para poder escalar, não é?

E assim, também, assim que eu anunciar a outra parte, né, quer dizer, que hoje, os medidores, né, os servidores de medição só estão presentes nos pontos de troca de tráfego, mas já vou apresentar aí, algumas novidades. Também, a gente alerta o usuário de que, se ele estiver usando a rede móvel, que ele vai gastar franquia, porque ele vai fazer teste de banda. Então, o usuário é alertado. Se ele quiser continuar, ele continua e faz esse teste aí.

Aqui tem a parte do SimetBox, não é? O SimetBox aí, então, ele foi reescrito aí, né, para poder, também, suportar essa estrutura do LMAP, uma estrutura escalável. Então, a gente está chamando dessa reescrita aí, de Simet 2, não é? O Simet 1 é a estrutura monolítica que a gente tinha, e o Simet 2 é essa nova estrutura nesses conceitos mais modernos aí. Então, o que tem de novidade aí, não é? Essa parte de gerência remota e *troubleshoot* remoto, o que vai permitir redução de custo para os provedores que acabarem utilizando o SimetBox. Esse SimetBox está atendendo a exigências do que foi comentado aí, sobre a BCOP que foi discutida dentro do grupo de trabalho do Lacnic. Então, a CPE segura, não é?

Então, a única exceção que a gente tem em relação a tudo isso que lá o pessoal cita, né, é a parte da senha variável para assinante. Quer dizer, isso daqui a gente está trabalhando, a gente vai disponibilizar posteriormente aí, para que cada assinante, quando fizer, vamos dizer assim, a instalação desse SimetBox, quer dizer, desse

software aí, no seu roteador doméstico, né, a gente consiga gravar uma senha variável para que ele possa se cadastrar.

Então, ele também aí, atende a TR-069, telemetria Zabbix, né, com filtro de IP, tá? Melhor visibilidade à rede de acesso com as medições. Então, uma vez que o ISP tem essas medidas que são disponibilizadas para ele, ele vai ter melhor visibilidade de como é que está a qualidade dos seus clientes aí, tá? E o ISP também vai poder fazer a configuração personalizada do firmware. Isso daqui foi uma solicitação feita por vários provedores, para que ele pudesse personalizar o firmware com as configurações desejadas, para ele fazer a distribuição para os seus clientes. Então, isso daqui já está contemplado. E atualização automática do firmware que também ocorre, tá?

Essa daqui é a novidade que eu trago para vocês, porque é o que estamos chamando de Simet-ISP. O que é esse Simet-ISP, pessoal? Muitos provedores pediram para a gente, que pudesse colocar o servidor do Simet dentro das suas redes, tá? Então, a gente pensou: ok, quer dizer, que podemos endereçar isso, não é? E, ao endereçar isso, como que a gente também quer saber como é que está a qualidade da rede desse provedor, em relação às nossas âncoras, aos nossos servidores do Simet, que estão no AS14026. Então, o que a gente pensou? A gente pensou que, quer dizer, os usuários desse provedor vão poder fazer o teste contra o servidor que vai estar dentro da rede desse provedor, mas a gente vai pegar também essa mesma máquina, né, quer dizer, esse daqui é um software para máquinas virtuais, não é? A gente também vai embutir nele, um teste que vai acabar fazendo um teste de qualidade contra os servidores do Simet. Mas não vai fazer teste de vazão, tá, pessoal? Só vai fazer teste do que a gente está chamando de ping, latência e jitter, usando o que a gente chama de TWAMP, tá, que a gente está seguindo o RFC do IETF. Então, a maneira com que a gente está fazendo essas medições é utilizando o TWAMP.

Então, esse Simet-ISP é uma ferramenta voltada e pensada para os provedores de acesso, tá? Vai permitir a visualização também, *peer-to-peer*, não é? Quer dizer que entre os diversos, digamos, provedores que vão ter esse Simet-ISP, tá, ele vai estar fazendo as medidas entre eles, não é? É intuito inicial a gente só disponibilizar esse Simet-ISP, só para os participantes do IX, em uma primeira etapa, tá? Para justamente a gente tentar mapear se, ao traçarmos o caminho entre esses servidores do Simet-ISP, que estão dentro da rede dos provedores, ele está passando pelo IX ou não está passando pelo IX. Isso é uma coisa que a gente vai estar endereçando aí, por isso que os resultados *peer-to-peer* visam conhecer isso e fazer algum alerta para o ISP, dizendo: Olha, você é participante do IX, outro cliente também é participante do IX, mas o caminho adotado entre vocês não está

passando pelo IX. Então, são coisas que vão estar sendo endereçadas aí.

Então, essas medições de qualidades aí, via TWAMP, vai estar endereçando esse aspecto, né, e também a parte de rotas. tá? E isso a gente entende que vai ajudar na parte da operação da rede do ISP, e também endereçar aquilo que os provedores tanto queriam, que o Simet faça as medições contra um servidor que está dentro da rede dele, tá ok? Então, isso vai ser endereçado. Então, todos aqueles softwares que eu falei para vocês, a parte do Simet Web, Simet Mobile, tá, mesmo o SimetBox, todos eles, tendo servidor de medição dentro do AS, ele vai dar preferência para medir contra esse AS. E aí, obviamente, a gente vai ter informação de como está a qualidade desse provedor em relação aos PTTs, via essas medições que a gente tem aí, que vai fazer contra os âncoras que estão hospedado dentro do AS e do Simet.

Aqui, né, é um trabalho feito, né, principalmente utilizando softwares que foram desenvolvidos para o MEC, não é? Usando plataforma Windows, usando plataforma Linux, não é? No qual, os educadores, né, eles podem baixar esse software aí nas máquinas que tem nas escolas e, com isso... baixa o software nessas máquinas, né, seja plataforma Windows ou Linux, e faz, e começa a fazer testes periódicos contra os servidores do Simet, tá? Então, esses testes aí, né, são feitos periodicamente. Hoje já são mais de 40 mil escolas sendo medidas, não é? A gente, em função dessas medições, a gente fez parcerias que eu vou citar no final, tá? Então, é um trabalho bastante interessante aí, porque essas informações estão sendo juntadas com as informações que o MEC tem sobre as escolas, né, que é o número de alunos por escola, entendeu? Quer dizer, que aí, o interessante é que os diretores das escolas, ao acessarem essas informações, estão podendo visualizar que a escola dele está com menor banda do que a outra, está com a latência ruim. Quer dizer que isso está sendo utilizado para poder discutir a parte educacional do país. Então, isso é um trabalho muito legal que está sendo conduzido aí pela equipe e está sendo feita toda uma análise de dados, está produzindo esses mapas aí, para que a gente tenha uma educação de qualidade no nosso país.

Aqui tem, vamos dizer assim, relatórios aí que foram publicados sobre a influência da Covid na qualidade da internet no Brasil, não é? Então, a gente pegou os dados que a gente tinha antes da pandemia, durante o pico da pandemia, que foi em março, e posteriormente, tá? Então, o que a gente observa, né, é que não se resolve o problema de qualidade no nosso país, porque o nosso país, ele tem uma diversidade muito grande de qualidade aí, não é? O que a gente observou é que as regiões que estavam bem antes, elas tiveram um impacto durante as primeiras semanas de isolamento e, depois, com a redução de qualidade do streaming, eles puderam trabalhar nas suas redes e a

qualidade, vamos dizer assim, logo ficou igual ao que estava antes desse pico aí.

Então, vamos dizer assim, resumindo, né, o que a gente enxergou é que as regiões Sul e Sudeste estão com uma internet melhor do que a região Centro-Oeste e Nordeste, que têm, mais ou menos, dados parecidos. E o pior de tudo, obviamente, é a região Norte, tá, pessoal? Então, esse problema de qualidade aí, a gente precisa endereçar, a gente está tentando endereçar, e esses estudos aí que vocês podem ver no nosso site, não é? Então, vocês vão para o site do Ceptro.br e lá vocês vão poder endereçar esses relatórios, e lá baixar, ler e ver aí todos os dados que foram analisados.

Aqui, né, é sobre as parcerias, tá? Então, basicamente, não é, aquele acordo que a gente fez com o MEC, que a gente já tem mais de 40 mil escolas sendo medidas, e esse número está crescendo, tá? Ele foi alvo aí do pessoal da ITU, do pessoal da Unesco, do pessoal da Unicef. Então, isso acabou tendo como referências em vários relatórios aí, né, que foram produzidos pela ITU, pela Unesco, não é? E firmamos acordo, né, com a Unicef, para que essa tecnologia que a gente adota aqui, de medidas on-line nas escolas, né, possam também ser estendidas para outras escolas no mundo inteiro, tá? Então, é bastante interessante, não é, porque o Brasil, segundo a Unicef, é o primeiro país que está fazendo essas medições on-line, tá? Então, a gente consegue ver a qualidade de uma maneira imediata aí, tá?

Então, tudo isso, né, pessoal, foi fruto, também, com a ajuda do Cetic, porque tem bastante relacionamento com esses órgãos aí, e que propiciou esses relacionamentos aí que a gente tem. E também dando subsídios aí, de como que a gente deveria fazer as análises dos dados que a gente tem, coletados. E por isso que, vamos dizer assim, a gente tem bastante interação com o pessoal da área de pesquisa do Cetic, tá ok?

Aí, também, na parte, essa parceria com a RNP, a gente ajudou nessa fase da pandemia, não é? Que houve o endereçamento em relação ao centro de saúde, né, para que os provedores pudessem conectar o centro de saúde, e o Simet entrou como o medidor, para poder validar se a conexão estava no ar ou não. E, com isso, surgiu essa parceria junto com a RNP, para que essa medição de qualidade fosse executada aí, tá? A gente também cita aqui esse programa do Wi-Fi Livre, junto com a Prefeitura de São Paulo, que é bastante interessante, não é, porque, nas praças digitais, onde tem os serviços de acesso gratuito aí, para internet, né, o Simet está sendo utilizado e está fazendo as medições periodicamente. Isso tem mostrado como é que está a qualidade desses acessos aí. E serve também para poder validar se a empresa que está prestando o serviço está com bom serviço ou não, e, com isso, poder cobrar a melhoria de qualidade, tá?

No início da implantação foi bastante interessante porque a gente notou que o usuário só conseguia utilizar tipo 9 horas da manhã, tinha um 'gapzinho' que ele conseguia se conectar, porque os outros horários, estava totalmente saturado. A banda que estava sendo contratada não era atingida. Então, estava um horror esse negócio aí. Então, essas medições aí, propiciaram essa visibilidade e a cobrança da melhoria do serviço. Então, hoje, o Wi-Fi Livre aí tem uma boa qualidade, tá ok?

E aí, na parte do Cieb, a gente tem ajudado a discutir como melhorar a parte do acesso à internet na escola. Estamos discutindo como é que deve ser feito a rede para dentro das escolas. Tem muitas escolas que só usam a internet, só para os seus laboratórios, alguns só para a parte administrativa. Então, temos que estender esse acesso de internet também para os usuários, e isso está sendo discutido junto com a equipe do Cieb, não é?

E aí, né, nesse quadrinho aqui, né, porque é uma tabelinha, né, foi um trabalho que a equipe fez aí. Como é que a gente vai identificar diferentes tipos de serviços que poderiam ser adotado nas escolas? Que bandas mínimas seriam necessárias aí, para que a escola pudesse disponibilizar para seus alunos, para que certos serviços fossem disponibilizados nas escolas, não é? Então, isso daqui foi apresentado, né, está sendo adotado aí para poder ter como referência, não é? E a discussão sobre que banda a escola deva ter está sendo feita em cima de estudos desse tipo aí, com referências bibliográficas que a equipe conseguiu juntar aí. Então, basicamente, né, pessoal, é isso que eu tinha que apresentar. Então, fico à disposição aí para perguntas.

SR. JULIO SIROTA: Obrigado, Milton. Tenho aqui algumas perguntas. Vamos lá. A primeira é do Sergio Eduardo Antonio. É uma sugestão, não é? Se é possível ao NIC realizar um levantamento do custo em reais, né, além do técnico, que seria latência, *jitter* e banda, respectivo à qualidade para cidades não capitais dos estados *versus* a capital.

SR. MILTON KAORU KASHIWAKURA: É. Muito boa a pergunta. De fato, isso daqui, vamos dizer assim, a gente baseou, né, com um primeiro dado que o pessoal dos Estados Unidos tem em relação aos acessos nas escolas deles, não é? Eles mostram exatamente esse aspecto aí do custo, não é? Quer dizer, quanto custa cada escola aí, é a banda que eles têm contratado. Isso daí, vamos dizer assim, está nas pretensões, aí, né, para que essas informações fiquem transparentes, tá? Quer dizer... Mas, assim, a gente está dependendo do MEC, né, porque, vamos dizer assim, como isso daqui é um acordo com o MEC, o MEC tem nos passado várias informações, e eu acredito que uma delas vai ser exatamente essa parte do preço, né, o que cada escola paga para a sua conexão à internet. Porque,

vamos dizer assim, a gente baseou o início do projeto em um projeto americano, lá, que endereça esse aspecto de custo da banda e como é que está isso, tá? Só que a informação deles é simplesmente declarativa, não tem essa medição on-line que a gente realiza.

SR. JULIO SIROTA: Uma outra pergunta do Roberval Dantas, se o servidor do Simet estará disponível para participantes de IX de todas as regiões.

SR. MILTON KAORU KASHIWAKURA: Sim, ela vai estar disponível para os participantes do IX de todas as regiões. Essa é nossa intenção.

Hoje, a gente está em uma fase pré-beta, não é? Que a gente está testando contra 10 ASs aí, para que a gente possa levantar os problemas que possam estar ocorrendo e, para depois dessa fase aí, abrir para um maior número de Sistemas Autônomos, tá, pessoal?

Então, pode entrar em contato com a gente, se tiver interesse, e a gente já coloca o seu AS na fila. Quer dizer, que a gente já tem um documento, que a gente já pode endereçar para vocês, sobre as necessidades do hardware da VM que vocês necessitam disponibilizar para que esses softwares sejam baixados.

SR. JULIO SIROTA: Tá. E tem mais uma pergunta, quem faz é criptografado o nome aqui, eu não consigo saber quem é. Se há alguma expectativa de desenvolver um Simet em CLI para a utilização em scripts?

SR. MILTON KAORU KASHIWAKURA: Bem, a gente não está pensando nisso. Porque a gente, assim, quer endereçar uma quantidade maior de usuários, não é? Eu entendo aí, que você deva estar querendo utilizar em CLI justamente para poder fazer testes pontuais aí, que você queira, talvez para poder fazer a aprovação de links aí, que tenham sido contratados, ou coisa do gênero. É, a gente pode pensar, tá? Endereça o seu desejo, né, como a gente tem, vamos dizer assim, o software aí, digamos, baseado em Linux, talvez isso não seja tão difícil assim de disponibilizar.

SR. JULIO SIROTA: Talvez tivesse pensado em, talvez, alguma ferramenta para automação, não é?

SR. MILTON KAORU KASHIWAKURA: É.

SR. JULIO SIROTA: Então, é isso aí. Muito obrigado, Milton. Queria agradecer também a todos que acompanharam mais um dia do IX Fórum 14. Lembrando aí, para quem não deu, para dar um like aí no nosso streaming.

E lembrando que amanhã a gente vai ter o último dia, tá? E esperamos aí, que todos voltem aqui para compartilhar com a gente, esse evento, tá? Então, obrigado e até amanhã.