XXI Escola Regional de Redes de Computadores (ERRC). doi: 10.5753/errc.2024.4645

Artigo Curto/Short Paper

VPN de camada 2 de baixo custo para unidades remotas

Low-cost Layer 2 VPN for remote sites

Leonardo Bitzki • bitzki@cpd.ufrgs.br
Universidade Federal do Rio Grande do Sul (UFRGS)
Caciano Machado • caciano@cpd.ufrgs.br
Universidade Federal do Rio Grande do Sul (UFRGS)

Resumo. Este artigo explora o desafio enfrentado por muitas instituições de ensino e pesquisa na extensão de serviços de rede para campi geograficamente isolados. Ele relata a estratégia adotada pela UFRGS de estender redes através de túneis para sites remotos usando o protocolo EoIP do Mikrotik. A solução implementada se destaca pelo menor custo em comparação com as opções tradicionais, ao mesmo tempo em que fornece uma qualidade de serviço semelhante.

Abstract. This paper explores the challenge faced by many universities and research centers in extending network services to geographically isolated campuses. It reports on the strategy adopted by UFRGS to extend through tunnels to remote sites using Mikrotik EoIP protocol. The implemented solution stands out for its lower cost compared to traditional options, while provides a similar quality of service.

Palavras-chave: Layer 2 VPN • EoIP • Tunnelling • Pseudowire
Keywords: VPN de camada 2 • EoIP • Tunelamento • Pseudowire

1 Introdução

A UFRGS possui a maior parte de suas dependências em Porto Alegre. A interligação física dos Campi na cidade se dá através de fibras escuras dedicadas disponíveis para UFRGS através do consórcio METROPOA [1], um projeto da REDECOMEP [2] para a região metropolitana de Porto Alegre. Entretanto, a UFRGS possui diversas unidades acadêmicas e administrativas geograficamente distantes, fora da área de alcance do METROPOA, sem conectividade própria da UFRGS para o backbone da rede. Via de regra, a conectividade dessas unidades remotas se dá através de provedores de Internet locais e sempre representaram um desafio de integração com os serviços do domínio administrativo da UFRGS.

Para que alguns serviços pudessem ser oferecidos nessas unidades, havia a necessidade de replicação de instâncias de serviços em ambiente local, como controladores de domínio, sistemas de telefonia, serviços de autenticação para redes sem fio, entre outros. Isto aumentava significativamente o número de equipamentos a serem administrados, muitas vezes operando em ambientes não ideais para funcionamento, além da falta pessoal local habilitado para gerenciá-los. Ao longo do tempo diversas abordagens foram implementadas, com diversas especificidades, tecnologias e dificuldades, convergindo atualmente para uma solução de VPN de camada 2 [3] unificada para extensão de redes do núcleo até as unidades remotas, utilizando equipamentos Mikrotik de baixo custo. Esse artigo apresenta um panorama da solução com túneis EoIP e os desafios atuais que impedem sua continuidade para o cenário da UFRGS, além de indicar uma possível alternativa substituta, utilizando VXLAN em switches Huawei.

Leonardo Bitzki e Caciano Machado são Analistas de Tecnologia da Informação da Divisão de Engenharia de Redes do Departamento de Infraestrutura de TI do Centro de Processamento de Dados da Universidade Federal do Rio Grande do Sul.

2 Cenários e suas necessidades

Com as fibras óticas do METROPOA à disposição em Porto Alegre, a UFRGS pode conectar os equipamentos do backbone diretamente a 40 Gbps, com total gerência e autonomia e sem restrições de conectividade para extensão das VLANs (Virtual Local Area Network) dos diversos serviços (WiFi, telefonia, videomonitoramento, etc). Dessa forma, a experiência dos usuários com os serviços fornecidos pelo Centro de Processamento de Dados (CPD) é a mesma em qualquer unidade acadêmica conectada através da rede METROPOA.

Entretanto, a UFRGS possui diversas unidades que não estão sediadas em Porto Alegre (Figura 1), como o Campus Litoral Norte (CLN) e o Centro de Inovação da Pró-Reitoria de Inovação e Relações Institucionais (PROIR), localizados em diferentes regiões da cidade de Tramandaí, o Centro de Estudos Costeiros, Limnológicos e Marinhos (CECLIMAR) na cidade de Imbé, a Estação Experimental Agronômica (EEA) na cidade

de Eldorado do Sul e a Unidade Barro Vermelho do Laboratório de Metalurgia Física (LAMEF), na cidade de Gravataí, além de outras sete unidades do projeto TelessaúdeRS [4], espalhados pelo interior gaúcho. Em geral o objetivo é estender as VLANs de serviços do núcleo da rede para as unidades remotas para centralização destes serviços no CPD por questões de otimização de recursos de infraestrutura e pessoal.

2.1 Análise inicial

Tendo em vista que o principal objetivo é fazer com que os equipamentos de distribuição da unidade remota estejam logicamente no mesmo domínio de broadcast de serviços originários no datacenter, o ponto de partida foi o estudo de quais tecnologias poderiam suportar esta necessidade técnica. Ficou em evidência que o protocolo Ethernet Over IP (EoIP), uma implementação proprietária do fabricante Mikrotik do protocolo Generic Routing Encapsulation (GRE) para VPN de camada 2, seria o principal candidato, devido a sua simplicidade de implantação e ao baixo custo dos equipamentos. A solução com túneis EoIP é utilizada pela UFRGS desde 2016.

Avaliou-se como melhor opção a utilização de um equipamento de maior capacidade instalado no datacenter do CPD para o papel de concentrador de túneis das unidades remotas da UFRGS, um equipamento de capacidade intermediária para atuar como concentrador dos túneis dos pontos do projeto TelessaúdeRS, e na padronização de equipamentos mais simples para todos os locais remotos.

Equipamentos de fabricantes mais tradicionais, como Cisco, Huawei, Juniper entre outros, poderiam alcançar o mesmo objetivo, mas certamente a um custo muito mais elevado. A adoção de equipamentos Mikrotik (Routerboard) é uma tendência bastante evidente, segundo os números de penetração do fabricante dentro de cenários como pequenos provedores [5] e até mesmo nos IXP (Internet Exchange Points) [6], muito em decorrência da simplicidade das soluções oferecidas e da disparidade dos preços dos equipamentos.

2.2 Equipamentos utilizados

Foram adquiridos: um Mikrotik RB4011iGS para a concentração dos túneis de unidades acadêmicas e administrativas, um Mikrotik RB3011UiAS para a concentração dos túneis do TelessaúdeRS e várias unidades do modelo RB750Gr3 para as unidades remotas. Cada concentrador é capaz de atender até 10 pontos remotos na topologia adotada, o que atende a todas as demandas de conexão que a Universidade possui, sendo atualmente 5 túneis de unidades acadêmicas e administrativas e 7 túneis do Projeto TelessaúdeRS.

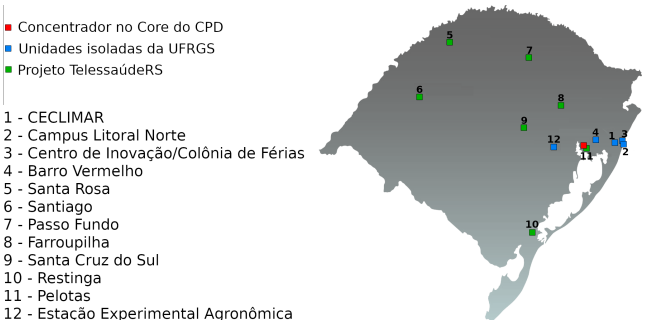

Figura 1. Unidades e pontos *remotos* conectados no modelo.

3 Modelos de conexão

Parte dos links de Internet das unidades remotas da UFRGS é contratada por intermédio da RNP [7] que nos entrega IPs fixos e públicos. No entanto, em algumas unidades, o fornecimento de Internet se dá através de contratação direta de operadoras locais, muitas vezes com NAT/CGNAT, o que num primeiro momento inviabiliza a implementação direta do EoIP, tendo em vista que o EoIP é um protocolo ponto-a-ponto.

3.1 EoIP direto

Nas unidades com links contratados pela RNP, tunelamento EoIP é feito de uma interface do equipamento de núcleo da rede para uma interface do RB750Gr3 no local remoto, de foram que as VLANs configuradas na interface do concentrador são estendidas através da Internet para a interface Ethernet da outra ponta. Do ponto de vista prático, é como se ambas interfaces estivessem com uma bridge. Para este modelo, o link de Internet remoto precisa ter IP fixo.

3.2 EoIP sobre WireGuard

O WireGuard [8] um é protocolo de tunelamento cujo objetivo é substituir soluções como IPSec (IP Security Protocol) e OpenVPN para a maioria dos casos. Esse protocolo apresenta desempenho até 30% superior ao do IPSEC quando utilizado com hardware de propósito geral [9], mas 15% menor se comparado com versões do IPSEC com aceleração AES[10]. O Wireguard é amplamente utilizado em sistemas de VPN e possui implementação nativa do RouterOS (sistema operacional do Mikrotik). Utilizando uma combinação de tunelamento de camada 2 com EoIP e tunelamento L3 com WireGuard, é possível obter o mesmo resultado final, de extensão Ethernet através da Internet, mesmo que o link não possua IP fixo, cenário bastante comum

quando se trata da contratação de operadoras locais. Apesar do Wireguard implicar em um sobrecusto maior de processamento em relação ao EoIP, ainda atinge uma qualidade de serviço bastante satisfatória.

4 Resultados e discussão

As soluções de tunelamento de camada 2 empregadas até então nas localidades remotas foram eficazes para a integração desses locais aos serviços do datacenter da UFRGS. Os túneis com EoIP alcançam banda de 180 Mbps, e os com Wireguard + EoIP chegam a 160 Mbps. Recentemente, alguns requisitos surgiram trazendo a necessidade de reformulação do modelo em operação.

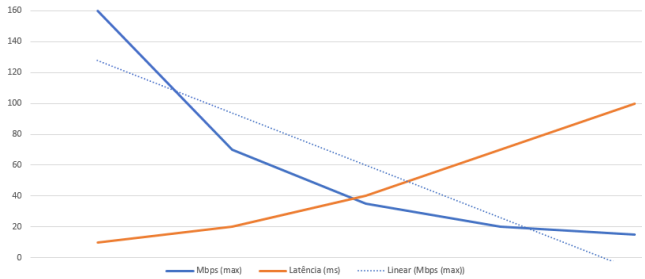

Figura 2. Velocidade do EoIP x Latência do link.

Como regra geral, contratamos links com endereçamento IP público e fixo, que permitam o tunelamento limpo, sem sobrecusto na rede e no processamento dos equipamentos. No entanto, em algumas situações que não foi possível contratar essa modalidade de serviço, nos deparamos com ambientes com NAT e CGNAT, que exigem soluções que atravessem o mapeamento de portas. Aplicamos temporariamente soluções de tunelamento com PPTP e L2TP em ambientes com NAT, até a contratação de links com IP fixo. Avançamos para uma solução com Wireguard, um protocolo mais seguro e com menor sobrecusto de rede e processamento.

Recentemente, a solução com WireGuard foi empregada em um ambiente com link via satélite da Starlink. Nesse caso, nos deparamos com dois desafios que estão em análise. Primeiro, esse é um dos poucos links cuja operadora não está presente no IX/RS da UFRGS, gerando uma latência muito elevada, na ordem dos 150 a 200 ms. Segundo, o contrato desse link prevê conformação de tráfego automático, a critério da operadora, supostamente para evitar congestionamentos na sua infraestrutura. Percebemos que o tráfego máximo com o tunelamento Wireguard + EoIP é cerca de 5 vezes menor que o tráfego normal. Isso nos leva a crer que a operadora aplica ativamente alguma política que prejudica o tráfego cifrado dos túneis Wireguard.

Também observamos em experimentos algumas limitações no protocolo EoIP, como a considerável queda de desempenho na medida que a latência aumenta entre os peers do túnel (Figura 2), conforme relatado também por Aung e Thein [3]. Considerando que os links contratados para as unidades remotas apresentam latências maiores, a depender do provedor, essa característica do protocolo EoIP prejudica a capacidade do link. Finalmente, os links contratados até o ano passado eram de até 200 Mbps, pouco acima do limite da capacidade dos modelos de Mikrotik que adotamos. No entanto, este ano estamos acionando links com 1 Gbps, muito além da capacidade estimada desses equipamentos, sobretudo nos túneis com Wireguard, o que demanda uma reformulação do serviço.

Uma alternativa a essa limitação dos Mikrotiks de baixo custo é a utilização de túneis VXLAN nas unidades remotas que recentemente adquiriram switches Huawei na suas entradas de rede. Em testes preliminares, verificamos que, não haveria limitação de banda nos links de 1Gbps, como acontece com os Mikrotiks. Além disso, essa alternativa eliminaria o Mikrotik como ponto de falha. Ainda resta efetivar ajustes no MTU do link dos provedores [11] para comportar os cabeçalhos VXLAN apropriadamente.

5 Conclusão

Desde 2016, a solução com túneis EoIP Mikrotik, atende satisfatoriamente as demandas de conectividade das unidades remotas da UFRGS, se consolidando no modelo de conexão apresentado nesse artigo. No entanto, nossa expectativa é que a ampliação e diversificação da demanda de serviços nas unidades remotas da UFRGS (sistemas acadêmicos, ferramentas de aprendizado, telefonia, acesso à Internet em geral, etc) torne obsoleta essa infraestrutura, seja por defasagem da capacidade de vazão, seja pela necessidade de interconexão de pontos além da capacidade dos concentradores. Além disso, existem desafios em relação a provedores de serviço com latências elevadas, como os links de satélite Starlink, e requisitos de qualidade de serviço como os do TelessaúdeRS. Estamos avaliando as melhores soluções que permitam utilizar os novos links contratados de 1Gbps na sua integralidade e que possam ser replicadas nas unidades remotas com o menor custo financeiro. Atualmente, a solução com VXLAN parece ser a mais promissora.

Declarações complementares

Disponibilidade de dados e materiais adicionais

Os dados e/ou materiais adicionais poderão ser disponibilizados mediante solicitação.

Referências

1 METROPOA. *Rede Comunitária de Educação e Pesquisa da RegiãoMetropolitana de Porto Alegre*. 2024. Disponível em: https://metropoa.tche.br/. Acesso em: 1 out. 2024.

2 REDECOMEP. *Redes Comunitárias de Educação e Pesquisa*. 2024. Disponível em: https://www.rnp.br/sistema-rnp/redecomep. Acesso em: 10 out. 2024.

3 Aung, S. T.; Thein, T. Comparative analysis of site-to-site layer 2 virtual private networks. *In*: Yangon, Myanmar. 2020 IEEE Conference on Computer Applications (ICCA). 2020. DOI: 10.1109/ICCA49400.2020.9022848.

4 TelessaúdeRS. *Projeto TelessaúdeRS (2024). Missão e História do Núcleo de Pesquisa do Programa de Pós-Graduação em Epidemiologia da Faculdade de Medicina da Universidade Federal do Rio Grande do Sul (UFRGS)*. 2024. Disponível em: https://www.ufrgs.br/telessauders/. Acesso em: 2 out. 2024.

5 Prescott, R. *Associação Brasileira de Internet: Provedores de menor porte adotam roteadores de baixo custo baseados em software aberto*. 2014. Disponível em: https://www.abranet.org.br/Noticias/Provedores-de-menor-porte-adotam-roteadores-de-baixo-custo-baseados-em-software-aberto-113.html. Acesso em: 2 out. 2024.

6 Ceron, J. M. *Mapping Concentrations of Device Vendors in IXPs*. 2020. Disponível em: https://labs.ripe.net/author/joao_m_ceron/mapping-concentrations-of-device-vendors-in-ixps/. Acesso em: 3 out. 2024.

7 POP-RS. *Ponto de Presença da RNP no Rio Grande do Sul*. 2024. Disponível em: https://www.pop-rs.rnp.br/. Acesso em: 2 out. 2024.

8 Donenfeld, J. A. *The WireGuard Project*. 2015. Disponível em: https://www.wireguard.com/. Acesso em: 3 out. 2024.

9 Abdulazeez, A. M. *et al.* Comparison of VPN Protocols at Network Layer Focusing on Wire Guard Protocol. *International Journal of Interactive Mobile Technologies (iJIM)*, v. 14, n. 18, pp. 157–177, nov. 2020. DOI: 10.3991/ijim.v14i18.16507.

10 Osswald, L.; Haeberle, M.; Menth, M. Performance comparison of VPN solutions. Universität Tübingen, 2020. DOI: 10.15496/publikation-41810.

11 Elmadani, M.; Sati, S. O. MTU Analyzing for Data Centers Interconnected Using VxLAN. *In*: 2024 ASU International Conference in Emerging Technologies for Sustainability and Intelligent Systems (ICETSIS). 2024. p. 1825–1829. DOI: 10.1109/ICETSIS61505.2024.10459403.