UNIVERSIDADE DO ESTADO DE SANTA CATARINA – UDESC
CENTRO DE CIÊNCIAS TECNOLÓGICAS – CCT
MESTRADO ACADÊMICO EM COMPUTAÇÃO APLICADA

RODRIGO DE SOUZA FERREIRA

ANÁLISE DE TÉCNICAS DE IP MULTICAST PARA REDES VIRTUAIS PRIVADAS EM INFRAESTRUTURA IP/MPLS BASEADA EM BGP

JOINVILLE
2024

RODRIGO DE SOUZA FERREIRA

ANÁLISE DE TÉCNICAS DE IP MULTICAST PARA REDES VIRTUAIS PRIVADAS EM INFRAESTRUTURA IP/MPLS BASEADA EM BGP

Dissertação apresentada ao Programa de Pós–Graduação em Computação Aplicada do Centro de Ciências Tecnológicas da Universidade do Estado de Santa Catarina, para a obtenção do grau de Mestre em Computação Aplicada.

Orientador: Prof. Dr. Adriano Fiorese

JOINVILLE
2024

Ficha catalográfica elaborada pelo programa de geração automática da

Biblioteca Universitária Udesc,

com os dados fornecidos pelo(a) autor(a)

Souza Ferreira, Rodrigo de
Análise de técnicas de IP multicast para redes virtuais privadas em infraestrutura IP/MPLS baseada em BGP / Rodrigo de Souza Ferreira. -- 2024.
74 p.

Orientador: Adriano Fiorese
Dissertação (mestrado) -- Universidade do Estado de Santa Catarina, Centro de Ciências Tecnológicas, Programa de Pós-Graduação em Computação Aplicada, Joinville, 2024.

1. EVPN. 2. IP/MPLS. 3. BGP. 4. Multicast. 5. MVPN. I. Fiorese, Adriano. II. Universidade do Estado de Santa Catarina, Centro de Ciências Tecnológicas, Programa de Pós-Graduação em Computação Aplicada. III. Título.

RODRIGO DE SOUZA FERREIRA

ANÁLISE DE TÉCNICAS DE IP MULTICAST PARA REDES VIRTUAIS PRIVADAS EM INFRAESTRUTURA IP/MPLS BASEADA EM BGP

Dissertação apresentada ao Programa de Pós–Graduação em Computação Aplicada do Centro de Ciências Tecnológicas da Universidade do Estado de Santa Catarina, para a obtenção do grau de Mestre em Computação Aplicada.

Orientador: Prof. Dr. Adriano Fiorese

BANCA EXAMINADORA:

Dr. Adriano Fiorese
UDESC

Membros:

Dr. Adriano Fiorese
UDESC

Dr. Augusto José Venâncio Neto
UFRN

Dr. Rafael Rodrigues Obelheiro
UDESC

Joinville, 8 de Julho de 2024

Dedico este trabalho à minha família, amigos e professores.

AGRADECIMENTOS

Agradeço a minha esposa Joice pela confiança, parceria e paciência nesses momentos de dedicação. Por sempre estar do meu lado e confiar no meu trabalho. Por estar junto e acompanhar todo esse momento especial, o que tornou essa caminhada possível. Agradeço ao meu filho Ian, que esteve sempre junto e me deu muita motivação. Por compreender e cooperar sempre que precisei me dedicar. Agradeço a Safira e Nalu por ter acompanhado junto essa caminhada.

Agradeço a minha mãe Judite, meu Pai Paulo e meu irmão Ricardo por sempre confiarem e acreditarem das minhas decisões e no meu potencial. Por dar todo o suporte que preciso em todas as etapas da minha vida.

Agradeço ao meu orientador Adriano Fiorese pela oportunidade e por aceitar conduzir o meu trabalho de pesquisa. Por todo o suporte durante esses anos e por todo o conhecimento compartilhado, por sempre acreditar no trabalho e toda sua dedicação foram fundamentais para conclusão deste estudo.

Agradeço ao professor Charles Christian Miers pela oportunidade e aceitação no programa, e por todo o grandioso conhecimento passado na disciplina.

Agradeço ao professor Rafael Rodrigues Obelheiro pelo grande aprendizado na disciplina e por acreditar no trabalho. Agradeço por aceitar compor a banca, pelas revisões e riquíssimas contribuições nesta pesquisa e todo o conhecimento compartilhado.

Agradeço ao professor Augusto José Venâncio Neto que aceitou estar na banca desta pesquisa e por todo o precioso tempo dedicado na revisão da qualificação e nas ricas contribuições.

Agradeço a todo o Departamento de Ciência da Computação, em especial a todos os professores das disciplinas de meu mestrado, da grande oportunidade de aprendizado e pela excelência da qualidade técnica de cada um: Adriano Fiorese, Christian Miers, Rafael Rodrigues Obelheiro, Maurício Aronne Pillon e Marcelo da Silva Hounsell.

Agradeço aos meus amigos e lideres Jucy Silveira, Flavio Azevedo e Luis Guimaraes pelo grande incentivo e acreditar sempre na busca pela evolução. Muito obrigado pela confiança sempre.

Agradeço a todos os meus amigos e colegas que de alguma forma contribuíram durante esse período, em especial ao Alexandre Castro que ajudou muito com as questões técnicas na emulação do laboratório.

Obrigado Deus!

RESUMO

Aplicações que se beneficiam de transmissão de dados do tipo multicast em uma rede IP, tais como aplicações *Over The Top* (OTT) baseadas em vídeo e distribuição de conteúdo, estão em constante desenvolvimento e crescimento. Dessa forma, se tem uma alta demanda por serviços multicast nas redes das provedoras de serviços de telecomunicações. Essas redes, que transportam os serviços de telecomunicações residenciais e corporativos, geralmente são redes de alta disponibilidade e capacidade baseadas na tecnologia IP/MPLS. Nesse contexto, o problema com o qual a rede lida é a capacidade da provedora na distribuição do tráfego multicast, muitas vezes em tempo real, de múltiplos serviços de forma escalável, confiável e em muitos caso com garantias de qualidade de serviço. Este trabalho tem o objetivo de apresentar uma análise das técnicas de transporte de tráfego IP multicast em redes virtuais privadas *Multicast VPN* (MVPN), sobre uma infraestrutura de rede IP/MPLS. O foco do trabalho são técnicas baseadas no protocolo BGP, onde destaca-se um novo método que está sendo padronizado pela *Internet Engineering Task Force* (IETF). Este novo *draft* da IETF é baseado no protocolo BGP EVPN e descreve procedimentos que permitem o roteamento ótimo de tráfego IP multicast entre diferentes LANs de um determinado cliente. Para a execução da análise, foi realizado um experimento em laboratório, visando a comparação entre os dois métodos: um padrão já conhecido e implementado pela indústria (NG-MVPN) e esse novo método que ainda se encontra em *draft*, ou proposta para padronização (EVPN). O ambiente de laboratório é composto de software emulador de rede, roteadores virtualizados da marca Nokia, ferramentas para captura dos dados e análise estatística dos resultados. Para tal análise, foi realizado um estudo que compara o desempenho do protocolo no plano de controle desses dois métodos MVPN em redes IP/MPLS. Os resultados dos experimentos realizados indicam que técnica de MVPN baseado no EVPN apresentou ganhos, em comparação ao NG-MVPN, na comunicação de controle para estabelecimento do serviço MVPN.

Palavras-chave: EVPN. IP/MPLS. Multicast. Redes IP. BGP. MVPN.

ABSTRACT

Applications that benefit from multicast data transmission over an IP network, such as video-based *Over The Top* (OTT) applications and content distribution, are constantly developing and growing. Thus, there is a high demand for multicast services in the telecommunications service provider's network. These networks, which transport residential and corporate telecommunications services, are usually high-availability and high-capacity networks based on IP/MPLS network technology. In this context, the problem that the network deals with is the service provider's ability to distribute multicast traffic, often in real time, from multiple services in a scalable, reliable manner and, in many cases, with quality of service guarantees. This paper aims to present an analysis of IP multicast traffic transport techniques in virtual private networks (MVPN) over an IP/MPLS network infrastructure. The focus of the paper is on techniques based on the BGP protocol, where a new method is being standardized by the IETF. This new IETF draft is based on the BGP EVPN protocol and describes procedures that allow optimal routing of IP multicast traffic between different LANs of a given customer. To perform the analysis, a laboratory experiment was conducted to compare two methods: a standard already known and implemented by the industry (NG-MVPN) and this new method that is still in draft or proposed for standardization, *Optimized Inter-Subnet Multicast* (OISM). The laboratory environment consists of network emulation software, virtualized Nokia routers, tools for data capture and statistical analysis of the results. For this analysis, a study was conducted to compare the protocol performance in the control plane of these two MVPN methods in IP/MPLS networks. The results of the experiments indicate that the MVPN technique based on EVPN presented improvements, compared to NG-MVPN, in control plane communication for establishing the MVPN service.

Keywords: EVPN. IP/MPLS. Multicast. Redes IP. BGP. MVPN.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE CÓDIGOS

LISTA DE ACRÔNIMOS

ADSL	*Asymmetric Digital Subscriber Line*
AS	*Autonomous Systems*
ASM	*Any Source Multicast*
ATM	*Asynchronous Transfer Mode*
BD	*Broadcast Domain*
BGP	*Border Gateway Protocol*
BIER	*Bit Index Explicit Replication*
BUM	*Broadcast, Unicast e Multicast*
CDN	*Content Delivery Network*
CE	*Customer Edge*
CPU	*Central Processing Unit*
DVB	*Digital Video Broadcasting*
eLER	*Egress LER*
EVE-NG	*Emulated Virtual Environment - Next Generation*
EVPN	*Ethernet VPN*
EVPN-VXLAN	*Ethernet Virtual Private Network - Virtual Extensible Local Area Network*
FCS	*Frame Check Sequence*
FEC	*Forwarding Equivalence Class*
FRR	*Fast Reroute*
GRE	*Generic Routing Encapsulation*
HTTP	*Hypertext Transfer Protocol*
IANA	*Internet Assigned Numbers Authority*
IETF	*Internet Engineering Task Force*
IGMP	*Internet Group Management Protocol*
iLER	*Ingress LER*
IP	*Internet Protocol*
IPTV	*Internet Protocol Television*
IPv4	*Internet Protocol version 4*
IPv6	*Internet Protocol version 6*
IRB	*Integrated Routing and Bridging*

IS-IS	*Intermediate System to Intermediate System*
ISP	*Internet Service Provider*
L2VPN	*Layer 2 Virtual Private Networks*
L3VPN	*Layer 3 Virtual Private Networks*
LDP	*Label Distribution Protocol*
LER	*Label Edge Router*
LFA	*Loop-Free Alternates*
LIR	*Local Internet Registries*
LSP	*Label Switched Path*
LSR	*Label Switch Router*
MDT	*Multicast Distribution Tree*
mLDP	*Multipoint LDP*
MP-BGP	*Multiprotocol BGP*
MPLS	*Multiprotocol Label Switching*
MVPN	*Multicast VPN*
NG-MVPN	*Next Generation MVPN*
NLRI	*Network Layer Reachability Information*
OISM	*Optimized Inter-Subnet Multicast*
OSI	*Open System Interconnection*
OSPF	*Open Shortest Path First*
OTT	*Over The Top*
P	*Provider*
P2MP	*Point to Multipoint*
PE	*Provider Edge*
PIM	*Protocol Independent Multicast*
PMSI	*Provider Multicast Service Interface*
QoS	*Quality of Service*
RFC	*Requests For Comments*
RIR	*Regional Internet Registries*
RPF	*Reverse Path Forwarding*
RT	*Route-Target*

RP	*Rendezvous Point*
RR	*Route Reflector*
RSVP-TE	*Resource Reservation Protocol–Traffic Engineering*
SBD	*Supplementary Broadcast Domain*
SMET	*Selective Multicast Ethernet Tag*
SPF	*Shortest Path First*
SSH	*Secure Shell*
SBD	*Supplementary Broadcast Domain*
TCP	*Transmission Control Protocol*
TDM	*Time Division Multiplexing*
TI	*Tecnologia da Informação*
Tree-SID	*Tree Segment Identifier*
TTL	*Time to Live*
VoIP	*Voice over Internet Protocol*
VPLS	*Virtual Private LAN Service*
VPN	*Virtual Private Network*
VPWS	*Virtual Private Wire Service*
VRF	*Virtual Routing and Forwarding*
VXLAN	*Virtual eXtensible Local-Area Network*
WAN	*Wide Area Network*
WWW	*World Wide Web*

SUMÁRIO

1 INTRODUÇÃO

O aumento de aplicações baseadas em vídeo, tais como *streaming* de vídeo, serviço de TV sobre IP *Internet Protocol Television* (IPTV), comunicações corporativas como videoconferência, educação a distância *e-learning* e outras aplicações de distribuição de conteúdo são os principais fatores para alta demanda de tráfego *multicast* nas redes das provedoras de serviços de telecomunicações, ou *Internet Service Provider*s (ISPs), (LI et al., 2021; LI et al., 2023; LAN et al., 2023).

Historicamente, operadoras de telecomunicações possuíam redes separadas para fornecer diferentes tipos de serviço. Por exemplo, a tecnologia *Time Division Multiplexing* (TDM) foi implementada para serviço de voz em tempo real; Frame-Relay e *Asynchronous Transfer Mode* (ATM) para serviços de dados em redes privadas que garantiam uma qualidade de serviço e redes IP para serviços de dados em "melhor esforço"(*Best Effort*), (WARNOCK; SHAHEEN; GHAFARY, 2015). Devido ao alto custo em operar e implementar redes separadas, e ao mesmo tempo atender a alta demanda por novos serviços de telecomunicações, operadoras buscaram implementar uma infraestrutura de rede única. Essa rede única com suporte a todos os tipos de serviço de telecomunicações foi possível através da tecnologia de redes *Internet Protocol* (IP)/*Multiprotocol Label Switching* (MPLS) (NOKIA, 2016).

O MPLS é uma tecnologia de rede que tem como objetivo transportar os pacotes de dados baseado em rótulos, através de caminhos pré-estabelecidos sobre uma rede IP, de uma forma mais eficiente do que uma rede puramente IP. No paradigma de encaminhamento MPLS, uma vez que um pacote é atribuído a um determinado caminho, nenhuma análise de cabeçalho adicional é feita por roteadores intermediários, como uma rede puramente IP. Todo o encaminhamento é conduzido por um valor codificado de comprimento fixo chamado rótulo (VISWANATHAN; ROSEN; CALLON, 2001). Sempre que um pacote entra em uma rede MPLS, ele é rotulado e transportado até seu destino baseado apenas no rótulo ao invés do endereço IP. Isso torna um roteador mais rápido e eficiente em termos de encaminhamento de pacotes (HUNDLEY, 2009). Dessa forma, o protocolo MPLS implementado sobre redes IP (IP/MPLS) foi amplamente adotado pelas operadoras de telecomunicações (LI et al., 2023; SLLAME, 2022). Redes IP/MPLS, além de apresentar melhor desempenho de encaminhamento em comparação com redes puramente IP, possibilitam aplicações de engenharia de tráfego e consolidação de serviços de Internet e de redes virtuais privadas *Virtual Private Network* (VPN) sobre uma única infraestrutura. Ou seja, a operadora fornece uma combinação de serviços de voz, vídeo e dados, para todas as necessidades comerciais, residenciais e da telefonia móvel em uma única rede IP/MPLS (LEYMANN et al., 2014; NOKIA, 2016).

O *Border Gateway Protocol* (BGP) é um protocolo de roteamento IP criado originalmente para troca de rotas IPv4 entre diferentes redes que possuem administrações distintas, ou seja, entre *Autonomous Systems* (AS). Um AS é um domínio de roteamento administrado por apenas uma organização, como por exemplo operadoras de rede de telecomunicações, provedores de

conteúdo e grandes empresas. Uma sessão BGP entre dois roteadores é estabelecida utilizando uma conexão TCP (porta 179), por onde é realizada a troca de rotas IP. Por meio de um processo de avaliação de regras de seleção de rotas recebidas de um vizinho BGP, o roteador aceita uma rota ou não, adicionando-a ou atualizando-a em sua tabela de rotas ou não. O BGP é dito um protocolo de roteamento mais escalável, pois não executa um algoritmo de roteamento sobre uma base de dados como executado em outros protocolos de roteamento. Além disso, o BGP é mais flexível para manipulações de rotas, pela possibilidade de configurações de políticas considerando um grande conjunto de atributos que cada rota BGP possui. Por sua escalabilidade e flexibilidade para manipulações de rotas através de políticas, o BGP se tornou o protocolo responsável pelo roteamento IPv4 e IPv6 de toda Internet. O BGP permitiu também a implementação de extensões habilitando a rede da operadora para criação de diferentes tipos de serviços além da Internet (WARNOCK; SHAHEEN; GHAFARY, 2015; NICHOLES; MUKHERJEE, 2009).

A IETF padronizou o conjunto de protocolos associados à tecnologia MPLS assim como o protocolo BGP e suas extensões que permitem a criação de VPNs e túneis virtuais chamados de *"pseudowires"* que atendem ao mercado corporativo além de serviços residenciais como *Voice over Internet Protocol* (VoIP) e IPTV de uma operadora. O conjunto de protocolos de rede Ethernet/IP/MPLS/BGP, utilizado como infraestrutura neste trabalho, é formado por tecnologias maduras e amplamente utilizadas por operadoras de rede de telecomunicações (HUNDLEY, 2009).

Do ponto de vista dos destinatários do tráfego, existem três tipos de comunicação de dados em redes IP: *Unicast*, *Broadcast* e *Multicast*. *Unicast* é o método de comunicação em que os pacotes enviados por uma origem são destinados para somente um único destino. Nessa comunicação, se mais destinos precisam do mesmo pacote, a origem deve fazer uma cópia para cada destino e encaminhá-los individualmente. *Broadcast* é o método de comunicação em que os pacotes enviados por uma origem são destinados para todos destinos dentro de uma rede. *Multicast* é o método de comunicação em que os pacotes são enviados de uma origem para X destino(s) (TANENBAUM; WETHERALL, 2011).

Particularmente, o tipo de comunicação *multicast* é uma forma eficiente para transmitir dados para vários receptores interessados. Esses receptores precisam demonstrar interesse pelo conteúdo, que é identificado por um endereço IP (inserido no campo de destino) reservado para endereços *multicast* (IANA, 2024). Dessa forma, uma fonte envia um simples pacote que pode ser recebido por vários receptores interessados. Dentro de uma rede *multicast*, os roteadores são responsáveis pela replicação do conteúdo *multicast* para que este chegue para todos os receptores associados a um determinado grupo *multicast*, ou um endereço IP *multicast* (TANENBAUM; WETHERALL, 2011).

Uma VPN, no âmbito da operadora de rede, é um mecanismo que cria uma conexão segura e privada entre diferentes localidades, ou redes geograficamente separadas que necessitam se conectar. Ela permite a comunicação de dados entre filiais de uma empresa, por exemplo. Dessa forma, a operadora de rede de telecomunicações, através de protocolos IP/MPLS/BGP,

pode oferecer o serviço de VPN para empresas conectarem suas filiais como se estivessem em uma mesma localidade (REKHTER; ROSEN, 2006). Por ser uma rede virtual privada, uma VPN não se comunica com outra VPN, ou seja, não há comunicação entre diferentes clientes ou serviços. Assim, cada VPN deve possuir sua instância separada de roteamento com suas próprias políticas. Além de serviços de telecomunicações para empresas, as operadoras também podem ofertar serviços próprios como IPTV e VoIP dentro de VPNs separadas (BAZAMA, 2012).

Dentre os tipos de tráfego que as redes de comunicação devem transportar, o transporte do tráfego IP *multicast* requer configurações e protocolos extras na rede da operadora. Quando a operadora oferece o transporte de tráfego *multicast* (de um cliente ou serviço como IPTV) dentro de uma rede virtual privada, tal serviço é chamado de MVPN. Existem algumas opções de implementação dos serviços MVPN que utilizam diferentes protocolos ou versões, e que será chamado de técnica ou método MVPN neste trabalho (JOSEPH; MULUGU, 2024; WARNOCK; SHAHEEN; GHAFARY, 2015).

Considerando a alta demanda de transmissão de dados de aplicações baseadas em vídeo e consequentemente por serviços *multicast* em VPNs na rede da operadora de telecomunicações, a rede da operadora deve estar em constante modernização para atender todos os serviços de forma escalável. Diante disso, o principal problema encontrado é a capacidade da rede em atender essa crescente demanda de serviços. Essa modernização deve existir tanto na rede física para fornecer principalmente largura de banda suficiente (ARNOULD et al., 2019), quanto na rede lógica através dos protocolos utilizados na rede. Ou seja, os protocolos que atuam no plano de controle dos roteadores de rede consomem recursos computacionais de memória e CPU (MEYER; PATEL, 2006), e são tão importantes quanto o plano de dados dos usuários. Dessa forma, a pesquisa principal sob o qual o trabalho se debruça é encontrar a mais adequada técnica MVPN em termos de desempenho para fornecer serviços *multicast* em VPNs.

Inerente ao tráfego *multicast*, duas questões estão envolvidas. A primeira é como os nós receptores sinalizam o interesse por determinado grupo *multicast*; e a segunda é como encaminhar esses pacotes desde a fonte até os destinos garantindo que o conteúdo seja transmitido apenas uma vez dentro da rede IP. Originalmente, os protocolos *Internet Group Management Protocol* (IGMP) (FENNER, 1997) e *Protocol Independent Multicast* (PIM) (FENNER et al., 2016) lidam com essas questões. Porém, protocolos e extensões adicionais são necessários para garantir o correto funcionamento do serviço MVPN, como o caso das extensões do protocolo BGP (METZ, 2006).

Este trabalho visa realizar um estudo de técnicas MVPN e seu impacto no desempenho do roteador, e consequentemente na rede. A análise se baseia no plano de controle de um roteador, ou seja, no protocolo que faz toda a parte de sinalização para que o serviço MVPN possa funcionar de acordo. O foco do trabalho se concentra em procedimentos definidos em padrões pela IETF descritos em *Requests For Comments* (RFC) e que são implementadas em roteadores comerciais. Dessa forma, este trabalho é direcionado pela seguinte pergunta de pesquisa: Dentre as técnicas de comunicação (MVPN) em redes IP/MPLS encontradas, qual delas apresenta a mais adequada solução para oferecer serviços MVPN em grande escala no *backbone* da operadora,

considerando o seu desempenho? Ou seja, qual das técnicas utiliza a menor quantidade de recursos dos roteadores da rede para oferecer o serviço MVPN?

Dado o desafio que as operadoras enfrentam nas escolhas de seus roteadores e protocolos que compõem o *backbone* da rede para que suporte o crescimento massivo de dados, a principal contribuição deste trabalho é dar fundamentos para as operadoras escolherem qual é a mais adequada técnica MVPN. Esses fundamentos são compostos por uma avaliação teórica do funcionamento e uma experimentação prática em laboratório emulado, considerando as principais tarefas:

- Implantação de uma rede IP/MPLS e duas técnicas MVPN (*Next Generation MVPN* (NG-MVPN) e EVPN OISM) em uma rede virtualizada com roteadores comerciais do fabricante Nokia;
- Comparação de desempenho em roteadores de rede entre as duas alternativas de técnicas MVPN, utilizando ferramentas estatísticas, provendo informações quantitativas e qualitativas sobre qual é a mais adequada técnica sob a condição de rede IP/MPLS de um provedor de serviço.

Dessa forma as duas técnicas MVPN avaliadas foram:

- BGP-EVPN OISM: Ainda um padrão em discussão pela IETF (*draft*), conhecido como draft-ietf-bess-evpn-irb-mcast (LIN et al., 2023);
- NG-MVPN: que está padronizada pelas RFCs 6513 e 6514 (AGGARWAL; ROSEN, 2012; REKHTER et al., 2012).

1.1 OBJETIVOS

Este trabalho tem como objetivo geral realizar uma análise comparativa de desempenho, com foco no plano de controle, das técnicas de implementação *multicast* em redes virtuais privadas MVPN, em uma infraestrutura de rede IP/MPLS.

Os objetivos específicos são:

- Levantamento das técnicas MVPN descritos em RFCs ou *drafts* da IETF;
- Levantamento dos indicadores/métricas para avaliação das técnicas MVPN mencionadas;
- Construção da bancada de teste, em um ambiente de rede emulada;
- Execução de experimento de comparação de desempenho de duas técnicas MVPN em redes IP/MPLS (NG-MVPN e OISM);
- Análise e interpretação dos valores das métricas obtidos com a experimentação;

- Fornecimento do código do experimento;
- Fornecimento de indicadores para a indústria a respeito das técnicas MVPN;

1.2 CARACTERIZAÇÃO DA PESQUISA

Essa seção apresenta a metodologia e a caracterização utilizados para a realização dessa pesquisa.

Conforme (PRODANOV, 2012) o método científico é o conjunto de procedimentos e caminhos para alcançar determinado fim, ou seja a metodologia mostra os caminhos de todo esse processo.

Com relação aos métodos de abordagem, ou métodos gerais, no qual trata-se do raciocínio lógico da investigação, este trabalho se classifica em hipotético-dedutivo. Conforme identificado por (PRODANOV, 2012), o método hipotético-dedutivo inicia-se com um problema ou uma lacuna no conhecimento científico, passando pela formulação de hipóteses e por um processo de inferência dedutiva, o qual testa a predição da ocorrência de fenômenos abrangidos pela referida hipótese, utilizando-se de experimentos.

Quanto à maturidade da pesquisa, (WAZLAWICK, 2009) apresenta uma possível classificação para os tipos de pesquisa realizados em Ciência da Computação e áreas correlatas, considerando o grau de amadurecimento da pesquisa na subárea específica. Essa classificação está dividida em cinco estilos, de 1 a 5, e quanto menor o número, menos maduro. Dessa forma, esta pesquisa se enquadra no estilo 3, chamado de "Apresentação de algo Presumivelmente Melhor". Esse estilo requer que qualquer nova abordagem apresentada seja comparada quantitativamente com outras da literatura, por meio de testes que demonstram que a abordagem em questão é melhor do que outras.

A classificação dessa pesquisa de forma clássica de acordo com (SILVA, 2004), ou seja, quanto à natureza, quanto aos objetivos e quanto aos procedimentos técnicos, se enquadra da seguinte maneira:

- Do ponto de vista de sua natureza, este trabalho pode ser classificado como pesquisa aplicada. De acordo com (PRODANOV, 2012) a pesquisa aplicada visa gerar conhecimentos para a aplicação prática dirigida a solução de problemas específicos. Neste contexto, este trabalho objetiva a formação de conhecimento através de um experimento prático.
- Do ponto de vista dos seus objetivos, este trabalho é classificado como pesquisa explicativa. Através de um experimento prático, visa explicar o porquê do uso de um determinado método (ex: BGP-EVPN) é mais eficiente para o transporte de serviços *Multicast* em uma rede IP/MPLS. De acordo com (PRODANOV, 2012) é a pesquisa que mais aprofunda o conhecimento da realidade, por isso é mais suscetível a erros.

- Do ponto de vista dos procedimentos técnicos, dado a maneira pela qual obtemos os dados necessários para a elaboração da pesquisa, essa pesquisa se caracteriza por pesquisa experimental.

Em uma pesquisa experimental, o pesquisador participa ativamente na condução do experimento, podendo controlar e manipular as variáveis relacionadas ao objeto de estudo. Isso possibilita analisar o impacto dessas interações e testar as hipóteses do pesquisador, para que um novo conhecimento possa ser adquirido ou simplesmente atualizado (SILVA, 2004).

Essa pesquisa conta com um experimento prático em que uma rede IP/MPLS é emulada, para criar um ambiente de teste que represente uma rede real sobre um hardware de baixo custo (laptop). Para tal foi utilizado o *Emulated Virtual Environment - Next Generation* (EVE-NG). O EVE-NG é um emulador de rede que suporta imagens de roteadores comerciais virtualizados (como Nokia, Juniper e Cisco) e roteadores de código aberto. Ele está disponível como uma máquina virtual baseado em Linux e suporta o QEMU-KVM para virtualização de hardware (QEMU, 2024). Nesse experimento o hardware virtualizado é um roteador Nokia (NOKIA, 2023). Os detalhes técnicos utilizado no experimento será abordado no Capítulo 3.

1.3 ESTRUTURA DO TRABALHO

Esse documento está organizado da seguinte forma: o Capitulo 2 apresenta a fundamentação teórica, abrangendo os conceitos utilizados pela pesquisa, além dos trabalhos relacionados. O Capítulo 3 apresenta a experimentação prática, todo o cenário de avaliação das tecnologias, resultados e sua interpretação estatística. O Capitulo 4 apresenta as conclusões sobre os resultados e as considerações finais.

2 FUNDAMENTAÇÃO TEÓRICA

Este capítulo apresenta uma visão geral das principais tecnologias envolvidas nos métodos do serviço MVPN em redes IP/MPLS, especialmente aquelas que são essenciais à realização dos experimentos que serão realizados. A Seção 2.1 revisa os aspectos de redes IP/MPLS mais relevantes para este trabalho. A Seção 2.2 apresenta o protocolo BGP. A Seção 2.3 detalha o que é um serviço VPN de uma operadora e seus modelos de implementação. A Seção 2.4 apresenta as técnicas e protocolos envolvidos dos serviços MVPN existentes. A Seção 2.5 mostra os trabalhos relacionados com essa pesquisa. As tecnologias descritas nesse trabalho são baseados em padrões da IETF descritos em RFCs.

2.1 REDES IP/MPLS

O desenvolvimento do protocolo IP foi formalmente publicado na *Request for Comments for Internet Protocol 791* (RFC791, 1981). A partir disso redes baseadas nos protocolos *Transmission Control Protocol* (TCP)/IP começaram a ganhar espaço. Os fatores contribuintes, inclusão do TCP/IP na distribuição UNIX e a disponibilidade gratuita e fácil compreensão das RFCs, ajudaram na difusão desses protocolos e formaram a base da Internet atual (HUNDLEY, 2009).

Essa natureza experimental da Internet permitiu nos anos 80, do século 20, o desenvolvimento de softwares de roteamento IP, como o *Intermediate System to Intermediate System* (IS-IS) (GREDLER; GORALSKI, 2005), *Open Shortest Path First* (OSPF) (MOY, 1998) e BGP, que eram executados em mini computadores comuns. Nos anos 90 a Internet ganhou o mundo comercial com o avanço de tecnologias como: *Hypertext Transfer Protocol* (HTTP) e *World Wide Web* (WWW), *Asymmetric Digital Subscriber Line* (ADSL) e redes a cabo, desenvolvimento de hardwares específicos para roteamento IP ou roteadores e o avanço do protocolo BGP, (WARNOCK, 2011). A partir disso o crescimento exponencial de aplicações e usuários da rede Internet, transmissão de dados pela rede móvel (ex.: 3G, 4G e 5G) e a massiva distribuição de aplicações de video exigiram e exigem cada vez mais da largura de banda da Internet, chegando às atuais interfaces de 800 Gigabit Ethernet (800GE), capazes de atingir velocidades de transmissão de 800 Gb/s a uma distância de 605 Km (ARNOULD et al., 2019).

A arquitetura de protocolos de rede, que suportam a interconexão de diversos tipos de hardware e sistemas, é dividida em camadas, com o objetivo de simplificar uma tarefa complexa de transmissão da informação, dividindo esse problema em funções mais simples. Dessa forma, cada camada executa uma função específica, contribuindo também para interoperabilidade; ou seja, equipamentos de rede, por exemplo, devem apenas saber do endereço de destino, mas não a aplicação (ex. email, web). Dessa forma, cada camada possui seu endereço de origem e destino. Além disso, tal arranjo adiciona flexibilidade à incorporação de novos protocolos que são introduzidos em uma determinada camada sem alterar as demais (HUNDLEY, 2009). O modelo de camadas TCP/IP, descrito na RFC 1122 - *Requirements for Internet Hosts – Communication*

Layers (BRADEN, 1989), fornece uma padronização no método de comunicação sobre a Internet. Esse modelo foi desenhado para permitir o funcionamento de diferentes dispositivos na rede, sem considerar o fabricante.

O IP é o protocolo da Internet, ou seja, um sistema para se conectar na Internet deve executar o protocolo IP e estar fisicamente conectado à Internet. IP é referido como um protocolo de camada 3 pela semelhança com o modelo de 7 camadas da arquitetura de referência de redes *Open System Interconnection* (OSI). O protocolo IP possui um plano de endereçamento universal e um serviço de entrega de pacotes sem conexão e não confiável.

O plano de endereçamento IP é um processo que garante que cada endereço da Internet seja único, ou seja, fornece um endereço IP exclusivo para cada dispositivo na Internet. Dessa forma os dados enviados por um dispositivo são encaminhados (roteados) para o destino correto. Para que isso funcione, existe uma hierarquia de organizações com o objetivo de controlar o endereçamento de toda Internet. A *Internet Assigned Numbers Authority* (IANA), organização mundial que supervisiona a atribuição global desse endereçamento na Internet, distribui blocos de endereços para os cinco organizações regionais (*Regional Internet Registries* (RIR)) espalhadas pelo mundo. Os RIRs, por sua vez, distribuem esses blocos de endereços para as organizações locais, (*Local Internet Registries* (LIR)), que geralmente são os provedores de serviço, que distribuem endereços para usuários finais da Internet.

O serviço IP é considerado não confiável porque a rede não garante a entrega e não notifica o *host* sobre pacotes perdidos devido a erros ou congestionamento da rede. Não há mecanismo para controle de fluxo no IP, deixando essa responsabilidade para as camadas superiores do modelo TCP/IP. O IP é responsável pelo roteamento de pacotes pela rede. O roteamento é realizado pelos roteadores IP que encaminham pacotes salto a salto.

O *Internet Protocol version 4* (IPv4), principal versão do protocolo IP da Internet, utiliza endereços de 32 bits que são escritos usando uma notação decimal com pontos que divide 32 bits em quatro octetos de 8 bits cada (ex. 192.168.2.100). Cada octeto é escrito como um número decimal com intervalo de 0 a 255. Convertendo cada um dos quatro números decimais, temos, por exemplo, o endereço de 32 bits (ex. 11000000 10101000 00000010 01100100).

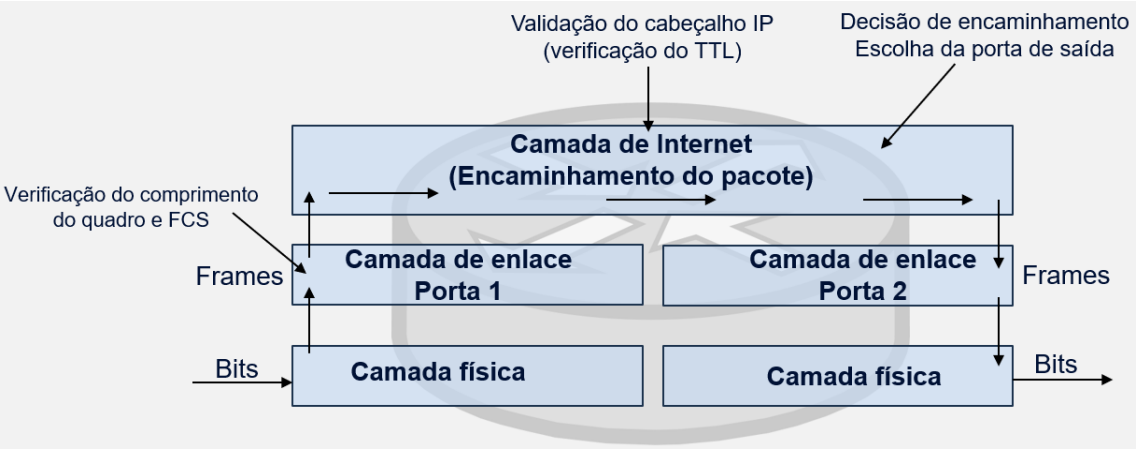
Já o *Internet Protocol version 6* (IPv6) foi projetado para atender às necessidades de crescimento da quantidade de dispositivos conectados à Internet. O IPv6 é composto por 128 bits, o que permite um espaço de endereçamento muito maior em comparação com o IPv4 (32 bits). Isso resulta em um total de 2^{128} endereços possíveis, uma quantidade extremamente grande. A notação de um endereço IPv6 é feita usando oito grupos de quatro dígitos hexadecimais, separados por dois pontos. Um exemplo de endereço IPv6 é: 2001:0db8:85a3:0000:0000:8a2e:0370:7334.

Encaminhamento IP é o processo usado por um roteador IP quando este recebe um pacote IP por uma porta de entrada, inspeciona o campo IP de destino, procura pela rota mais específica em uma tabela de roteamento, determina o próximo salto (roteador ou dispositivo final) e envia esse pacote para a correta porta física de saída. A tabela de roteamento de um roteador possui as redes, ou endereços IP, que um roteador consegue alcançar e para cada rede qual é o próximo

salto, ou seja, pra qual porta o pacote deve ser enviado. A tabela é composta por redes locais, que são as redes diretamente conectadas ao roteador e as redes remotas, que são redes distantes e conectadas a outros roteadores. As redes remotas podem ser aprendidas de duas maneiras pelo roteador: manualmente configurado, o que é chamado de configuração de rotas estáticas, ou dinamicamente aprendida através de um protocolo de roteamento (ex. IS-IS, OSPF e BGP).

A Figura 1 apresenta o encaminhamento de pacote IP por um roteador, em camadas. Na Figura 1, é possível seguir as setas que mostram todo o processo de encaminhamento de um pacote da esquerda pra direita, desde a camada física onde os sinais elétricos são interpretados como bits. Assim, na camada 2 (camada de enlace), os bits são agrupados em uma estrutura de dados chamada quadro L2 (*frame*). A camada 2 verifica o comprimento do quadro e executa uma verificação de erro *Frame Check Sequence* (FCS) sobre os bits do quadro. Na sequência, o conteúdo do quadro é lido e enviado para a camada superior, a camada 3 ou camada IP. Na camada IP, o *Time to Live* (TTL) e outros campos do cabeçalho IP são verificados, a tabela de encaminhamento é consultada e o pacote IP é encaminhado para a interface de saída do roteador apropriada, completando o encaminhamento dos bits do pacote (bits do quadro L2 mais os bits do cabeçalho IP).

Figura 1 – Encaminhamento IP



Fonte: (HUNDLEY, 2009).

O MPLS (VISWANATHAN; ROSEN; CALLON, 2001) é uma tecnologia de rede em que o roteador encaminha os pacotes utilizando rótulos, ou *"labels"*, em vez do endereço IP. Numa rede MPLS, os pacotes de dados dos usuários recebem rótulos assim que eles entram na rede MPLS. Esses rótulos identificam caminhos entre os pontos de origem e destino. Dessa forma o encaminhamento de pacotes é realizado com base no conteúdo do rótulo, sem a necessidade de abrir e examinar o cabeçalho IP do pacote.

No roteamento IP, o roteador determina o próximo salto de um pacote inspecionando o campo endereço de destino do cabeçalho IP e consultando uma tabela de roteamento IP para encontrar o prefixo mais longo que casa com o endereço de destino (*longest prefix matching*). Dependendo do tamanho da tabela de roteamento, esse processo pode consumir muito recurso

do roteador, tornando o processo mais lento do que o encaminhamento por rótulos. Isso pois, o roteador MPLS procura pelo rótulo exato na tabela sem a necessidade de encontrar o prefixo mais específico. Isso torna aplicações em tempo real, como voz e video, mais suscetíveis ao baixo desempenho se comparado ao roteamento realizado por meio do padrão MPLS.

O MPLS não consta na estrutura de 7 camadas do modelo OSI, mas pode ser conhecido como camada 2,5 pelo fato do cabeçalho MPLS ser inserido entre as camadas 2 e 3 do modelo OSI. O MPLS tem a capacidade de encapsular e transportar não somente o protocolo IP, mas também outras tecnologias de rede como ATM, *Frame Relay* e TDM, (EL-AAWAR et al., 2006). Dessa forma o MPLS se torna tecnologia ideal para operadoras provedoras de serviço e empresas.

Além de oferecer vantagens consideráveis como melhora na utilização da rede e redução da latência (no roteamento), as principais características da tecnologia MPLS são:

- Encaminhamento simplificado;
- Engenharia de Tráfego;
- Serviços de Rede (Internet/Voz/Video/VPN L2 e L3);
- Mecanismos de convergência rápida em caso de falha do caminho principal (*Fast Reroute* (FRR));
- Multi-Protocolo: IP, TDM, ATM, Frame Relay;
- Garantia de Qualidade de Serviço, *Quality of Service* (QoS) .

O encaminhamento é simplificado uma vez que é realizado por rótulo em vez do endereço IP de destino. O MPLS suporta engenharia de tráfego, permitindo a configuração de caminhos diferentes do que consta na tabela de rótulos (AWDUCHE et al., 2001). Serviços de rede significa a possibilidade de oferta de diversos tipos de serviços de telecomunicações para clientes residenciais, corporativos ou governamentais. Em redes MPLS é possível oferecer diferentes serviços numa mesma infraestrutura de rede IP/MPLS. Basicamente os tipos de serviços são: acesso à Internet (residencial e corporativo), VoIP/IPTV que são oferecidos dentro de VPNs e serviços de VPN para clientes corporativos e governamentais. A sobreposição dos serviços na mesma infraestrutura é possível, pois não há sobreposição de tabelas de roteamento entre VPNs distintas e com a tabela da Internet. VPNs são redes virtuais em que cada cada uma delas possui suas próprias tabelas, regras e políticas que controlam sua operação. Existem basicamente 3 tipos de VPN: 1) VPNL2 ponto-a-ponto em que 2 *sites* do cliente são conectados como se estivessem diretamente conectados, ou seja, a rede da operadora é transparente ao cliente; 2) VPNL2 multi-ponto em que a VPN opera como um dispositivo de rede *switch* de camada 2 e, portanto, atua como se cada *site* do cliente estivesse ligado numa porta desse *switch*; 3) VPNL3 em que a VPN opera como um roteador IP e, atua como se cada *site* do cliente estivesse ligado em uma porta desse roteador.

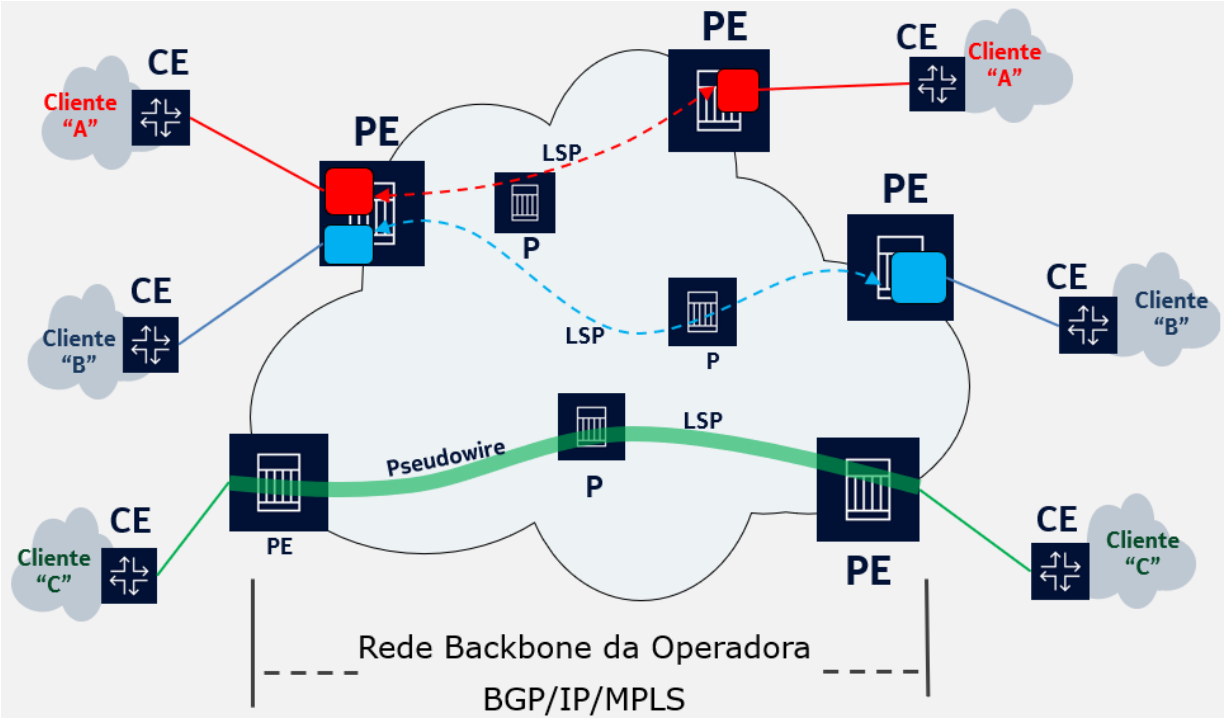
Convergência rápida está relacionada com a alta disponibilidade da rede. Ela significa que na presença de falhas de enlace ou nó de rede, a habilidade da rede em encontrar outro caminho disponível é rápida o suficiente para que não haja interrupção de serviços que executam em tempo real como por exemplo o IPTV. O MPLS oferece mecanismos de roteamento rápido FRR, fornecendo tempos de convergência na casa de milissegundos (< 50 milisegundos) para um grande número de tipos de tráfego. Os caminhos alternativos são pré-computados e já conhecidos pelos roteadores para cada serviço. MPLS é multi-protocolo pelo fato de transportar tecnologias de rede além de IP (ATM, Frame Relay e TDM). Ele também oferece garantia de qualidade de serviço (QoS), pois o cabeçalho MPLS possui 3 bits destinados a identificar e diferenciar tipos de tráfego, significando que o roteador pode dar tratamento diferenciado a cada pacote.

Uma rede MPLS é composta de roteadores que comutam rótulos, chamados de *Label Switch Router*s (LSRs), que possuem a capacidade de rotular pacotes e encaminhá-los com base em seus rótulos, ao longo de um caminho chamado *Label Switched Path* (LSP). Os elementos e a terminologia em uma arquitetura de rede MPLS se dá da seguinte maneira, conforme Figura 2:

- *Customer Edge* (CE) – Roteador pertencente ao cliente, que se conecta a rede da provedora através do PE. Conecta a um ou mais PEs. Não tem conhecimento dos serviços VPN e protocolos que executam na rede da provedora de serviço;
- *Provider Edge* (PE) – Roteador da borda da rede da provedora, onde são conectados os clientes da rede (CE). Roteador responsável por adicionar o rótulo no pacote do cliente que entra na rede MPLS ou remover o rótulo no pacote que sai da rede MPLS no sentido ao cliente. É onde ficam todas as configurações dos serviços do cliente;
- *Provider* (P) – Roteador localizado no coração da rede. Não conecta ao cliente CE; É um roteador de trânsito que apenas encaminha os pacotes baseado em rótulos. Não há configuração de serviços de cliente nesse roteador;
- *Label Edge Router* (LER) – É o PE com referência a sua função, podendo ser *Ingress LER* (iLER)/*Egress LER* (eLER) dependendo do sentido do pacote analisado;
- LSR – é o P com referência a sua função. Conecta o iLER com o eLER para formar o caminho para encaminhamento do tráfico com rótulo, no domínio MPLS.
- LSP – Túnel unidirecional ponto-a-ponto para tráfego *unicast* e ponto-multiponto para tráfego *multicast*.

Na Figura 2, os três serviços VPN são representados pelas linhas pontilhadas e contínua entre os PEs, que passam pela rede *backbone* da operadora. O quadrados nos PEs representam serviços VPN de camada 3 (IP) de cada cliente. Cada cliente tem sua tabela de roteamento dedicada. As linhas pontilhadas representam os caminhos (LSP) tomado por cada serviço. Já a linha contínua, representa uma VPN de camada 2 em que um *site* do cliente é conectado

Figura 2 – Rede IP/MPLS



Fonte: O autor.

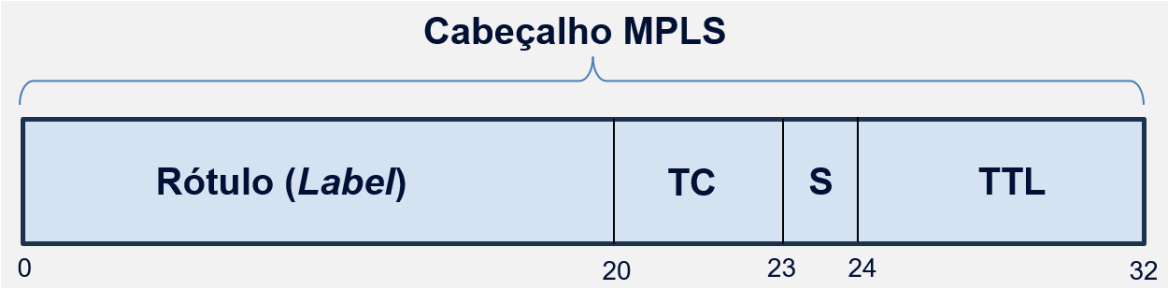
diretamente a outro através de um túnel chamado de *pseudowire*. A nuvem grande que engloba os PEs e Ps representa a rede MPLS da operadora, e as nuvens pequenas junto ao CE representam as redes dos clientes. Os serviços VPN serão melhor definidos na Seção 2.3.

Os LSP são os caminhos pelos quais os dados são encaminhados em uma rede MPLS. Na rede MPLS, um LSP é criado para transportar os dados para uma devida classe, chamados de *Forwarding Equivalence Class* (FEC), ou classe de equivalência de encaminhamento. Uma FEC define um grupo de pacotes para ser encaminhado pelo mesmo caminho LSP com o mesmo tratamento de encaminhamento. Sendo mais objetivo, um FEC corresponde a um destino de rede.

Um rótulo possui 20 bits e é aplicado a cada pacote. O rótulo é um valor arbitrariamente atribuído e tem significado local ao roteador que identifica uma FEC. Assim, o rótulo aplicado a um determinado pacote depende do valor FEC com o qual o pacote foi classificado. O conjunto de pacotes que são tratados da mesma maneira pertencem a um determinado FEC e são encaminhados utilizando o mesmo caminho LSP. Geralmente um pacote é atribuído a um FEC com base em um endereço IP de destino, porém, podem ser levados em consideração outros critérios administrativos. Para implementação de serviços MPLS, como VPNL2, VPNL3 e convergência rápida, um pacote rotulado deve transportar múltiplos rótulos em uma pilha de rótulos, organizados como último a entrar, primeiro a sair. O cabeçalho MPLS tem um tamanho fixo de 32 bits (4 bytes) e é mostrado na Figura 3.

Assim, de acordo com a Figura 3, o cabeçalho MPLS tem os seguintes campos:

Figura 3 – Cabeçalho MPLS



Fonte: (WARNOCK, 2011).

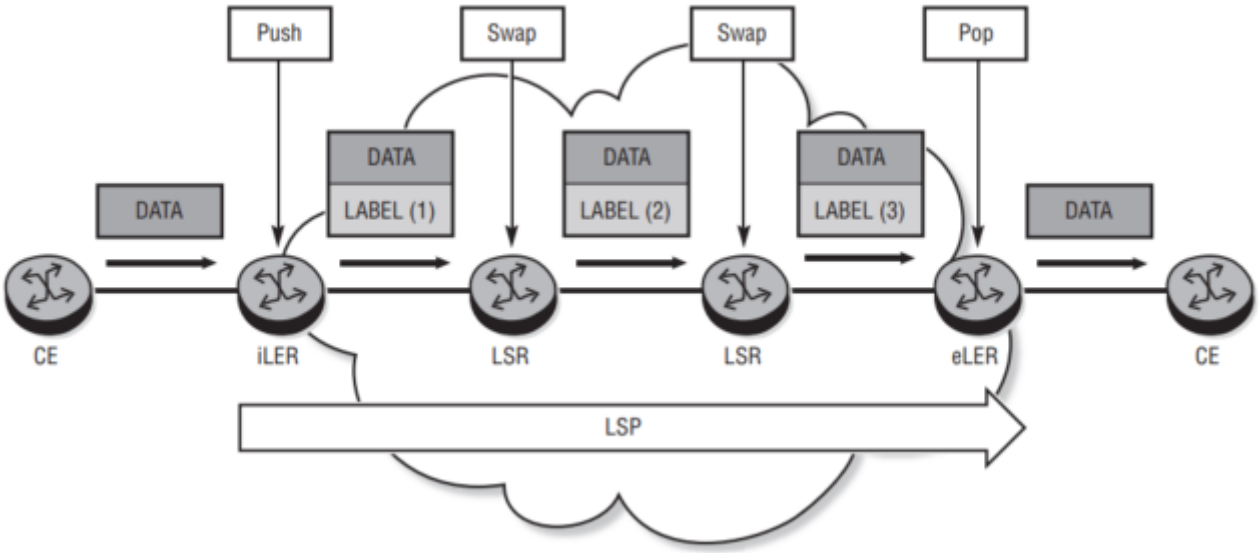
- *Label* (20 bits): Valor do rótulo MPLS;
- *Traffic Class* (3 bits): Classe do tráfego, utilizado para QoS;
- *Bottom of Stack* (1 bit): Valor = 1 significa último rótulo da pilha;
- *Time to Live* (8 bits): Contador de saltos.

Existem três operações que o roteador MPLS executa ao manipular os rótulos: *"PUSH", "SWAP"* e *"POP"*, no sentido de inserir, trocar e retirar. Quando um pacote entra na rede MPLS, ele é classificado em um FEC e vinculado a um LSP. Dessa forma o rótulo correto é adicionado a esse pacote através da operação *"PUSH"* e então é enviado para o próximo salto. Assim que o pacote atravessa a rede MPLS, as decisões de encaminhamento são tomadas consultando o rótulo MPLS e trocando-o por um novo rótulo MPLS antes de enviar ao próximo salto, numa operação de *"SWAP"*. Quando o pacote sai da rede MPLS, todos os rótulos são removidos na operação *"POP"*. A Figura 4 mostra o processo de encaminhamento de tráfego através de uma rede MPLS, onde é executada cada uma das três operações.

Para se ter caminhos de transporte MPLS (LSP) e serviços VPN na rede, é necessário definir os rótulos a serem utilizados pelos LSPs e VPNs. Para rótulos que definem os LSPs, cada roteador é responsável por gerar os rótulos para as FECs, e os rótulos gerados por esse roteador têm significado local. Dessa forma quando o roteador recebe um pacote rotulado, ele sabe a qual FEC pertence. Para rótulos de serviço VPN os roteadores PEs são responsáveis pela geração e sinalização dos rótulos dos serviços VPN. Para a distribuição dos rótulos numa rede MPLS, os principais protocolos são:

- *Label Distribution Protocol* (LDP) - Protocolo de distribuição de rótulos, que funciona em conjunto com o protocolo de roteamento IP, que pode ser IS-IS ou OSPF. Conforme os roteadores aprendem novas redes de destino através do seu protocolo de roteamento, eles usam o LDP para anunciar rótulos dessas novas redes, permitindo assim que seus vizinhos cheguem ao destino com esses rótulos.
- *Resource Reservation Protocol–Traffic Engineering* (RSVP-TE) - Protocolo usado para sinalizar LSPs na rede. RSVP-TE é usado para se realizar engenharia de tráfego, ou seja,

Figura 4 – Emcaminhamento MPLS



Fonte: (WARNOCK, 2011).

um LSP pode ser criado não somente baseado na tabela de roteamento IP, mas também através de configurações adicionais.

- *Targeted LDP* - Extensão do LDP que é usada para troca de rótulos de serviço VPN de camada 2.
- *Multiprotocol BGP* (MP-BGP) - Extensão do BGP para que é usada para troca de rótulos de serviço VPN de camada 3.

Para o experimento executado neste trabalho foram utilizados os protocolos LDP e MP-BGP para distribuição de rótulos de transporte e de serviço VPN, uma vez que o foco deste trabalho é o plano de controle das técnicas MVPN baseada no protocolo MP-BGP. Nesse sentido, outros protocolos como por exemplo, RSVP-TE poderiam ser utilizados, sem afetar resultados; contudo, a análise utilizando BGP torna o uso dos protocolos já mencionados, mais adequada. O *Targeted LDP* não foi utilizado, pois a análise é realizada em serviços VPN de camada 3.

2.2 PROTOCOLO BGP

O protocolo *Border Gateway Protocol* (BGP), é um protocolo de roteamento e foi primeiramente documentado em 1989 na RFC 1105 (LOUGHEED; REKHTER, 1989). Após várias revisões importantes, hoje o BGP está documentado na RFC 4271 (REKHTER; HARES; LI, 2006).

O BGP foi originalmente criado como protocolo de troca de informações de roteamento (ou de rotas IP) entre sistemas autônomos (AS) distintos. Um AS é definido como a rede ou coleção de roteadores sob a mesma administração técnica. Ou seja, podemos dizer que cada

operadora de rede possui seu próprio número AS, que é um número de identificação globalmente exclusivo de 16 ou 32 bits, (REKHTER; HARES; LI, 2006) e (VOHRA; CHEN, 2012). Assim como um IP público, a atribuição desses números AS é controlada pelas RIR.

Cada AS usa um único protocolo de roteamento interno, responsável por encontrar o melhor caminho para cada destino dentro da rede desse AS. Geralmente são utilizados os protocolos de roteamento IP OSPF ou IS-IS, com suas próprias políticas e métricas que determinam como rotear pacotes dentro de um AS. Por outro lado, o BGP é utilizado como protocolo de roteamento externo, entre diferentes ASs que determinam como os pacotes serão roteados entre esses diferentes domínios de rede.

Protocolos de roteamento interno (IS-IS e OSPF) fornecem um roteamento preciso e um tempo de convergência muito rápido. Esses protocolos são classificados como protocolos de estado de enlace (*link-state routing protocols*), ou seja, cada roteador distribui informação da topologia local e armazena informações detalhadas da topologia de toda a rede através da execução de um algoritmo *Shortest Path First* (SPF), também conhecido por "Dijkstra", utilizando-se dessas informações ou base de dados. O SPF calcula caminho mais curto entre um nó e todos os outros nós da rede, e é um exemplo de algoritmo guloso que gera a solução ótima em tempo polinomial e possui uma complexidade $O(M \log M)$, (RUSSELL; COHN, 2012). Dessa forma a sobrecarga de protocolos de roteamento interno aumenta exponencialmente conforme o crescimento da rede, limitando sua escala em nível de toda Internet.

O BGP não utiliza algoritmo de estado de link ou vetor-distância, como nos protocolos de roteamento interno. Em vez disso, ele usa um algoritmo de vetor de distância modificado, conhecido como algoritmo *Path Vector*, ou vetor de caminho. O BGP utiliza informações das rotas juntamente com o caminho para aquele destino, (MEYER; PATEL, 2006). A Internet usa roteamento hierárquico, com BGP para resolver o roteamento entre ASs e OSPF/IS-IS para roteamento dentro de cada AS.

As sessões BGP entre os roteadores são estabelecidas utilizando o TCP como protocolo de transporte, na porta 179. Por ser TCP, é suportada a fragmentação, o reconhecimento e a retransmissão de pacotes de comunicação.

Um roteador BGP envia periodicamente mensagens de manutenção de sessão para manter a conexão. Após o estabelecimento da sessão TCP entre dois roteadores, ocorre a troca de mensagens de atualização com informações de roteamento, ou seja, com as rotas BGP que estão sendo trocadas. Basicamente cada mensagem de atualização é composta de dois tipos de informação: a rota ou o IP e a máscara de rede com o roteador de próximo salto, chamado de *Network Layer Reachability Information* (NLRI); e um conjunto de atributos ou parâmetros que são utilizados para criação de políticas de roteamento. Quando um roteador recebe uma rota (ou rede) de seu vizinho, baseado nas políticas configuradas e atributos que a rota carrega, a rota pode ser aceita ou rejeitada para ser copiada para a tabela de roteamento, ou indicar certas preferências que o roteamento destinado para essa rede deve tomar (NOKIA-UNICAST-GUIDE, 2023).

Por essas características, o BGP é um protocolo muito flexível, permitindo a criação de extensões além do IPv4, como suporte a IPv6 e anúncio de rotas de clientes dentro de VPNs, tanto *unicast* quanto *multicast*. Nesse caso, quando o BGP é utilizado para transportar informações que não são prefixos IPv4, ele é chamado de *Multiprotocol BGP* (MP-BGP) (WARNOCK; SHAHEEN; GHAFARY, 2015).

Neste trabalho, os métodos de *multicast* VPN descritos utilizam o protocolo MP-BGP para anúncio de rotas *multicast* dentro de VPNs.

2.3 SERVIÇOS VPN

O objetivo de um serviço de rede VPN, do ponto de vista do provedor do serviço, é fornecer uma ampla variedade de serviços de telecomunicações de maneira econômica, sob uma infraestrutura de rede única da operadora, de forma individualizada e segura aos seus usuários/clientes. Como já mencionado, uma infraestrutura de redes IP/MPLS/BGP suporta uma série de serviços privados virtuais, *Virtual Private Network* (VPN). VPN é uma rede privada oferecida como serviço aos clientes do provedor de telecomunicação, criada sobre uma rede IP/MPLS, que possibilita a conexão de diferentes pontos de acesso do cliente, como por exemplo a conexão entre matriz e as filiais de uma empresa. A VPN é virtual e privada, pois a mesma infraestrutura IP/MPLS é compartilhada para suportar muitos clientes de serviço VPN, em que cada VPN é totalmente independente e transparente para outros clientes. Dessa forma, cada cliente pode ter suas próprias políticas e endereçamento IP sem conflitos, permitindo à operadora entregar uma rede exclusiva para cada cliente. Assim, basicamente, existem três tipos de serviço VPN (HUNDLEY, 2009):

- *Layer 2 Virtual Private Networks* (L2VPN): Descrito na RFC 4664 (ROSEN; ANDERSSON, 2006). Existem dois tipos diferentes de serviço VPN de camada 2:
  - *Virtual Private Wire Service* (VPWS)
  - *Virtual Private LAN Service* (VPLS)
- *Layer 3 Virtual Private Networks* (L3VPN): Descrito na RFC 4364 (REKHTER; ROSEN, 2006).

L2VPN VPWS é um serviço VPN que fornece um serviço ponto a ponto L2. Nesse caso a operadora de serviço VPN - geralmente a operadora de telecomunicação - fornece um túnel lógico entre dois *sites* do cliente, como se eles estivessem diretamente conectados por um enlace de rede. Esse serviço suporta a conexão de redes Ethernet e clientes que possuem redes legadas como Frame Relay, ATM, ou circuito TDM.

L2VPN VPLS é um serviço L2 multiponto que emula o serviço LAN, que conecta os diversos pontos do cliente. Nesse caso a operadora fornece uma LAN entre os *sites* do cliente, como se eles estivessem conectados a um *switch* de rede.

L3VPN é um serviço L3 multiponto que emula o serviço de roteamento, que conecta os diversos pontos do cliente. Nesse caso, a operadora fornece um **roteador** IP virtual para os *sites* do cliente, como se cada *site* do cliente estivesse conectado em uma interface IP desse roteador, provendo um roteamento entre as diversas redes do cliente. O protocolo BGP (MP-BGP) é usado pela operadora para trocar as rotas de uma determinada VPN entre os roteadores da borda da rede (PE) que fazem interface com os *sites* do cliente. Isso é feito de uma maneira que garante que as rotas de diferentes VPNs permaneçam separadas, mesmo que duas VPNs utilizem o mesmo endereçamento IP. Assim, cada VPN de cliente possui sua própria tabela e políticas de roteamento. Dessa forma, o PE recebe o pacote IP do cliente, examina seu cabeçalho IP e realiza o encaminhamento de acordo com a tabela dessa VPN. Esse tipo de VPN é utilizado para atender clientes que podem ser empresas, ou grupo de empresas, e outras aplicações da operadora como IPTV e VoIP.

A Figura 2 mostra exemplos dos serviços L2 e L3 VPN, sendo L2VPN (VPWS) representado pela linha contínua e L3VPN representado pelos quadrados.

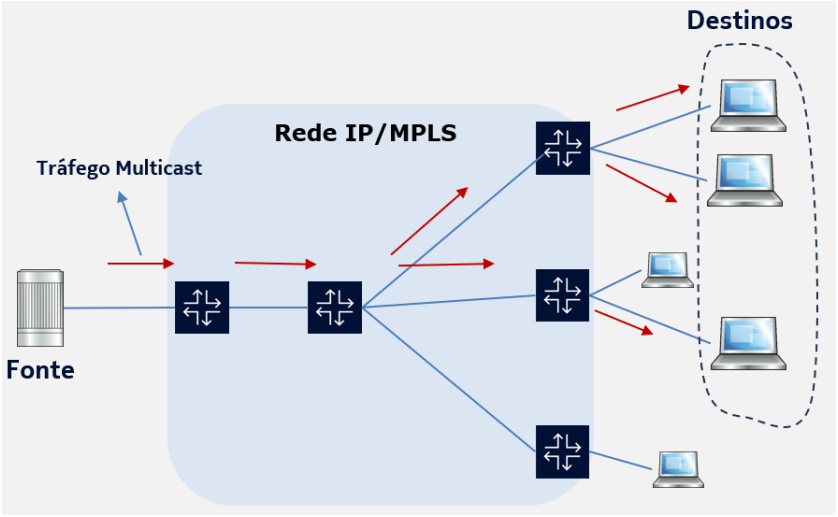
2.4 TÉCNICAS MVPN

Na forma de comunicação *multicast*, uma fonte envia uma única cópia de um pacote que pode ser encaminhado por um roteador *multicast* e entregue para um grupo de receptores interessados. Grupo *multicast* é identificado por um endereço IP do grupo *multicast*. Dessa forma os receptores interessados em um grupo *multicast* devem sinalizar seu interesse para que os roteadores no meio do caminho saibam encaminhá-los de forma correta. No caso, os roteadores devem suportar protocolos de roteamento *multicast* para encaminhar esse tipo de pacote. Dessa forma, com o *multicast* há uma utilização reduzida de recursos e também de largura de banda disponível e consequentemente um aumento da escalabilidade da rede, uma vez que a fonte envia somente um pacote, independente do número de receptores, e os roteadores *multicast* fazem a replicação conforme necessário. A Figura 5 representa a comunicação *multicast*, em que o tréfego *multicast* alcança somente os destinos interessados.

Os principais protocolos utilizados na comunicação *multicast* em redes IP são: *Internet Group Management Protocol* (IGMP) e *Protocol Independent Multicast* (PIM). O IGMP é usado por um *host*, ou receptor, para notificar a rede que deseja receber (ou parar de receber) o tráfego de um determinado endereço de grupo *multicast*. As RFCs 2236 (FENNER, 1997) e 3376 (CAIN et al., 2002) descrevem o IGMPv2 e IGMPv3 respectivamente. O PIM (FENNER et al., 2016) é o protocolo que os roteadores IP utilizam para construir e gerenciar a árvore de entrega *multicast* em toda a rede, a *Multicast Distribution Tree* (MDT). Dessa forma um roteador consegue notificar outro roteador de que ele deseja receber (ou parar de receber) tráfego *multicast* de um determinado grupo.

A RFC 4364 (REKHTER; ROSEN, 2006) (BGP/MPLS IP VPN), que define o serviço L3VPN, aplica-se somente a um tráfego IP unicast, não abrangendo tráfego *multicast* dentro de

Figura 5 – IP-Multicast



Fonte: O autor.

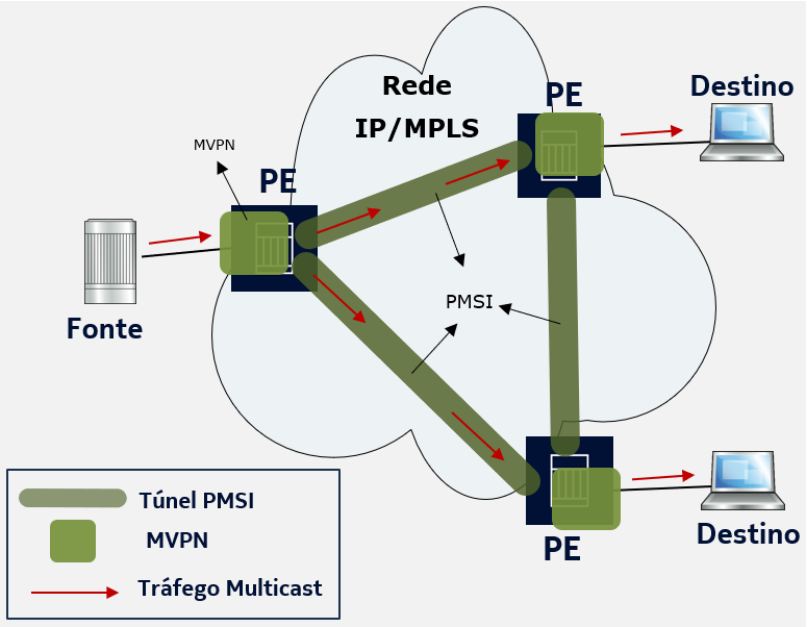
um serviço VPN de camada 3. Dessa forma, são necessários métodos adicionais para transportar o tráfego *multicast* do cliente através da rede IP/MPLS, em um serviço VPN, da operadora. As principais funções que um método MVPN deve implementar são:

- a descoberta dos roteadores PE que participam de um determinado serviço MVPN;
- a criação das árvores de distribuição *multicast* (MDTs) que irão transportar os dados de *multicast* do cliente;
- e a propagação da sinalização PIM do cliente através da rede da provedora.

O *Multicast Distribution Tree* (MDT), ou árvore *multicast* criada na rede IP/MPLS da operadora, é responsável por transportar os dados *multicast* do cliente entre os PEs da rede da operadora. A MDT é composto por interfaces lógicas, ou túneis, formados entre os PEs de um determinado serviço MVPN chamado de *Provider Multicast Service Interface* (PMSI). O túnel PMSI, também conhecido como P-tunnel (*provider tunnel*) é criado utilizando o protocolo PIM ou MPLS *Point to Multipoint* (P2MP). A Figura 6 mostra o túnel PMSI entre os PEs que possuem o serviço MVPN.

Quando o PIM é utilizado para criação do P-tunnel, o tráfego *multicast* do cliente é encapsulado pelo protocolo de tunelamento *Generic Routing Encapsulation* (GRE). O GRE é um padrão de encapsulamento da camada 3 definido na RFC 2784 (LI et al., 2000), usado para encapsular pacotes IP para transmissão (OGUDO, 2019). Quando o MPLS é utilizado para criação do P-tunnel, o tráfego *multicast* do cliente é encapsulado pelo MPLS (através de caminhos LSP P2MP criado entre PEs) e replicado nos roteadores P para alcançar os roteadores PEs. Os dois protocolos MPLS, LDP e RSVP, possuem extensões para criação de túneis MPLS P2MP, e estão definidos nas RFCs 6388 (THOMAS et al., 2011) e 4875 (PAPADIMITRIOU; YASUKAWA; AGGARWAL, 2007), respectivamente.

Figura 6 – PMSI / P-Tunnel



Fonte: O autor.

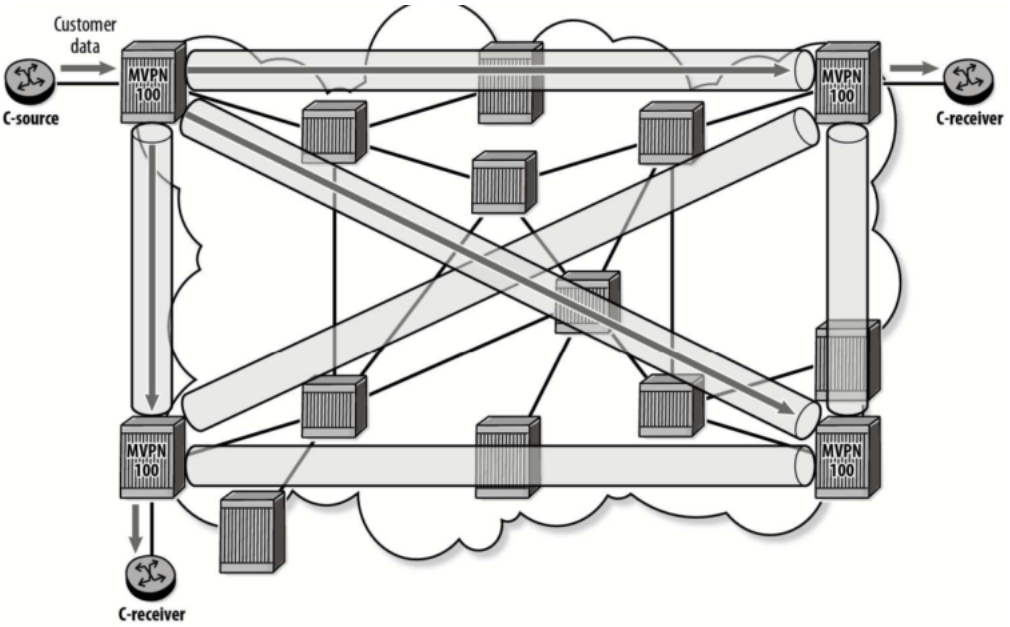
Um LSP ponto multiponto (P2MP) permite que a origem do tráfego *multicast* encaminhe pacotes para um ou mais receptores *multicast* em uma rede sem exigir que um protocolo *multicast*, como o PIM, seja configurado nos roteadores da rede. Uma árvore LSP P2MP é estabelecida no plano de controle cujo caminho consiste em um nó raiz, um ou mais nós intermediários ramificados, e os nós folha. Os pacotes injetados pelo nó raiz são replicados no plano de dados nos nós de ramificação antes de serem entregues aos nós folha. Isso permite que tráfego de clientes com redes IP *multicast* nativo, que executam o protocolo PIM, seja transportado pela rede MPLS (P2MP LSP) da operadora.

Existem dois tipos de túneis PMSI:

- *Inclusive* PMSI (I-PMSI): São túneis criados entre todos os roteadores PEs de um serviço MVPN, no modelo "*full mesh*". Ele emula uma LAN (broadcast) entre todos os PEs membros da MVPN. Utilizado para carregar sinalização do plano de controle e transmitir dados do cliente. Cada serviço MVPN possui seu próprio I-PMSI, sendo um I-PMSI por MVPN. Os dados do cliente enviado por um túnel I-PMSI são distribuídos para todos os PEs (broadcast) desse serviço MVPN, mesmo que não haja receptores interessados, conforme Figura 7.

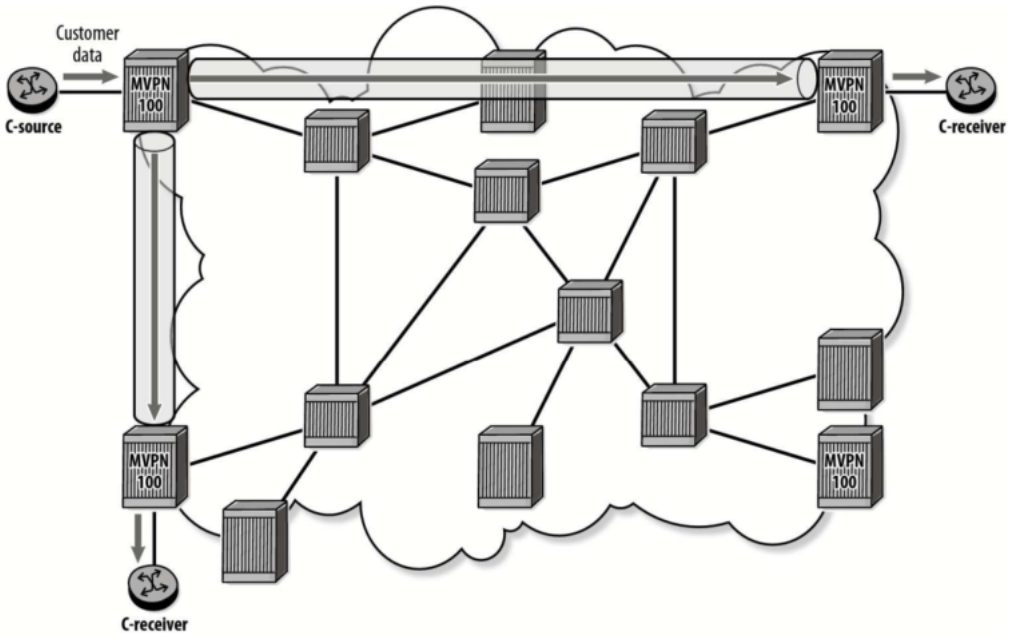
- *Selective* PMSI (S-PMSI): Túneis utilizados para transportar os dados do usuário, de um grupo grupo *multicast* específico, de sua fonte de origem do tráfego *multicast* para apenas os PEs com receptores interessados nesse grupo, e não para todos os PEs como no I-PMSI. Dessa forma podem existir vários S-PMSI por MVPN (um para cada grupo *multicast* ativo) e apenas um I-PMSI por MVPN, conforme Figura 8.

Figura 7 – I-PMSI



Fonte: (WARNOCK; SHAHEEN; GHAFARY, 2015).

Figura 8 – S-PMSI



Fonte: (WARNOCK; SHAHEEN; GHAFARY, 2015).

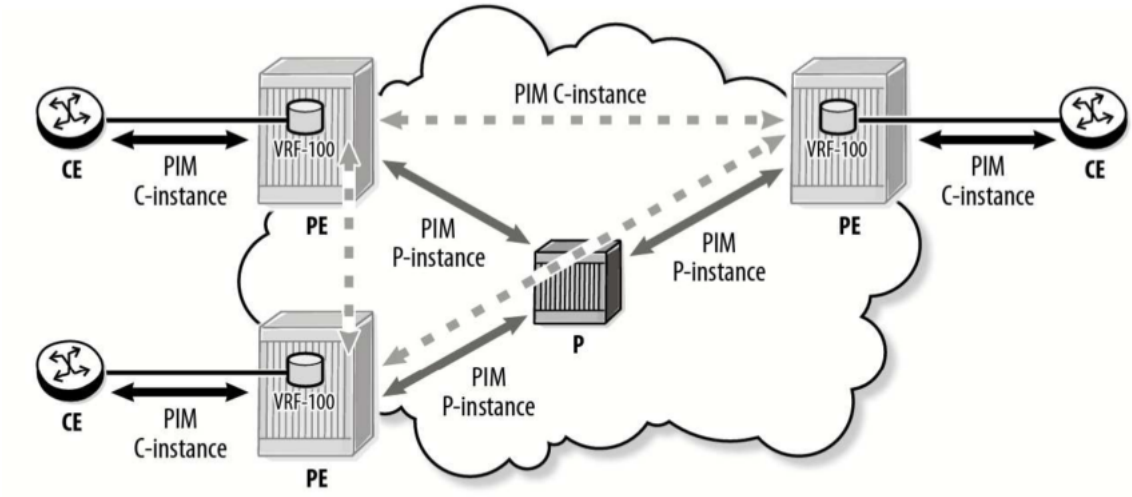
O primeiro passo para a ativação de um serviço MVPN é a criação de um *full-mesh* de túneis entre os PEs membros do serviço MVPN (P-Tunnel) para fornecer o transporte para o I-PMSI. Para a descoberta dos roteadores PEs que participam de um determinado serviço MVPN, e consequentemente a criação do I-PMSI, duas abordagens são utilizadas: utilizando o protocolo PIM *Any Source Multicast* (ASM) ou auto descoberta pelo protocolo BGP, através da mensagem BGP *Auto-Discovery* (chamado de rota BGP A-D).

Nas próximas subseções serão apresentados três esquemas de MVPN para fornecer serviços *multicast* sobre redes MPLS: *Draft-Rosen*, *Next Generation MVPN* (NG-MVPN) e EVPN *Optimized Inter-Subnet Multicast* (OISM). Como esse trabalho se concentra em protocolos e técnicas já padronizadas (ou em padronização) e implementadas, esses esquemas são padrões descritos pela IETF e implementados por fabricantes de roteadores. O *Draft-Rosen* é tido como o primeiro padrão desenvolvido para o MVPN porém é uma técnica já em desuso pois apresenta algumas desvantagens em termo de escala da rede. Apesar de ser considerada uma tecnologia legada, e não incluído nos experimentos desse trabalho, serão descritas suas principais características e suas limitações. As outras duas técnicas são conhecidas como de próxima geração e estão mais alinhadas com a evolução de uma rede da operadora, superando as limitações do Draft-Rosen.

2.4.1 Esquema ROSEN (PIM/GRE MVPN)

O primeiro método de MVPN ficou conhecido como *Draft-Rosen*, desenvolvida pela fabricante Cisco, descrito na RFC 6037 (WIJNANDS; ROSEN; CAI, 2010). Esse método é baseado no protocolo PIM, que deve ser executado em todos os roteadores da rede da operadora, e utiliza o tunelamento GRE para encapsular o tráfego *multicast* do cliente. Dessa forma, são criadas duas instâncias do protocolo PIM: a instância do cliente, pois a rede do cliente é uma rede IP *multicast* (PIM), chamada de *Customer-instance* (C-instance), e a instância PIM da provedora, chamada *Provider-Instance* (P-instance). O C-instance é dado pelas adjacências PIM, endereços de grupo *multicast* e tráfego *multicast* pertencentes à rede do cliente. Por outro lado, o P-instance é dado pelas adjacências PIM, endereços de grupo *multicast* da rede da operadora e o tráfego *multicast* do cliente encapsulado pelo GRE para transporte na rede da operadora. A Figura 9 representa esses conceitos.

Figura 9 – Instâncias PIM

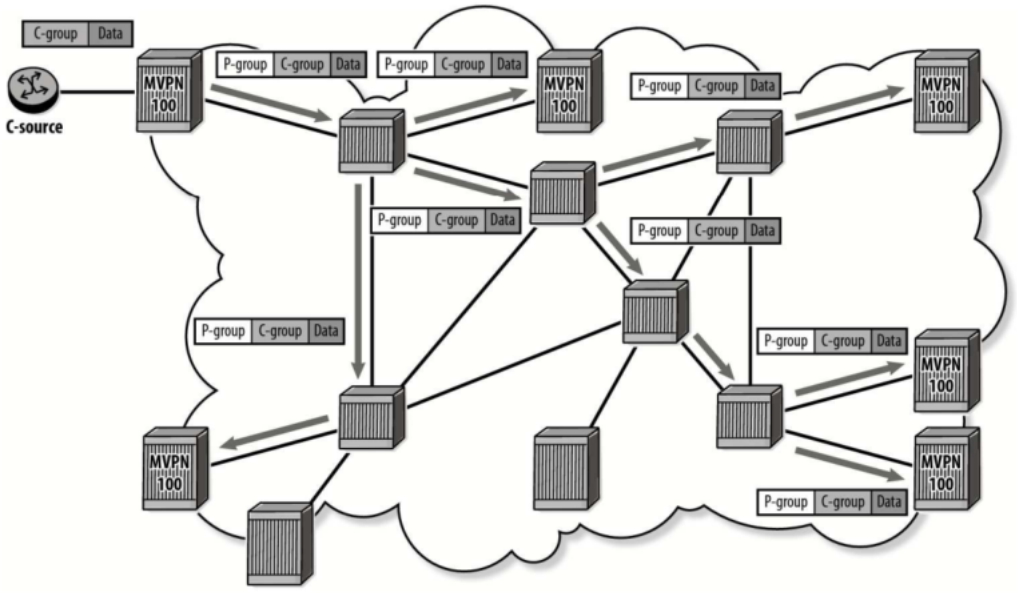


Fonte: (WARNOCK; SHAHEEN; GHAFARY, 2015).

O PIM ASM, utilizado pelo método Rosen, necessita de um roteador na rede da provedora com a função de ponto de encontro entre a fonte do tráfego e os destinos, chamado de *Rendezvous Point* (RP). Cada PE ingressa numa árvore compartilhada (*Shared Tree*) com a raiz sendo do RP. O RP então ingressa numa árvore de origem (*Source Tree*) com raiz sendo cada um dos roteadores PEs de uma MVPN. Dessa forma são formados os tuneis "*full-mesh*"(P-tunnels) para o I-PMSI, e os dados *multicast* podem ser recebidos por quaisquer fontes *multicast*.

Dessa forma, o tráfego *multicast* chegando no PE de origem (fonte) é encapsulado pelo GRE e transmitido aos PEs de destino pelos túneis (P-tunnels) I-PMSI. O tráfego é encapsulado utilizando endereços de grupo *multicast* da provedora (P-group). Como visto na Figura 9, o PE mantém uma adjacência PIM com o CE local e com outros PEs do serviço MVPN. Assim, de um ponto de vista do cliente, a rede da operadora é vista como uma rede IP *multicast* tradicional. A Figura 10 mostra o fluxo *multicast* do cliente (C-group) sendo encapsulado pelo PE da rede com o endereço de grupo *multicast* da operadora (P-group), e entregue para todos os PEs pertencentes ao serviço MVPN.

Figura 10 – Encapsulamento GRE



Fonte: (WARNOCK; SHAHEEN; GHAFARY, 2015).

Porém, o *Draft-Rosen* MVPN é tido como uma técnica antiga que possui algumas desvantagens, principalmente que afetam a escalabilidade da rede:

- O protocolo PIM é requerido por todos os roteadores da rede da operadora. Sessão PIM entre os PEs deve ser mantida para pelo menos um MDT por MVPN;
- Rotas *multicast* do cliente são apenas trocadas entre os PEs utilizando PIM;
- GRE é a única opção para entregar o tráfego *multicast* sobre um serviço MVPN. O método Draft-Rosen MVPN não fornece uma opção de usar protocolos MPLS (RSVP-

TE ou mLDP) para o plano de dados, ou seja, para encapsulamento. Dessa forma o tráfego *multicast* não tira proveito de uma rede MPLS, ao contrário do tráfego unicast.

2.4.2 NG-MVPN (BGP/MPLS MVPN)

Seguindo o método *Rosen*, foi padronizado outro método chamado de NG-MVPN descrito nas RFCs 6513 (AGGARWAL; ROSEN, 2012) e 6514 (REKHTER et al., 2012). O NG-MVPN utiliza o protocolo *Multiprotocol BGP* (MP-BGP) no plano de controle e MPLS (LSP P2MP) para encapsulamento e encaminhamento do tráfego. Assim quando o MPLS é usado para criação dos túneis da provedora (*P-tunnels*), caminhos LSPs P2MP são criados entre os PEs. Da mesma forma, o tráfego *multicast* do cliente é encapsulado com um rótulo MPLS e replicado conforme requerido pelos roteadores do meio da rede.

Para a descoberta dos PEs do serviço MVPN e consequentemente criação dos P-tunnels, o NG-MVPN utiliza a mensagem do protocolo BGP chamada de auto-descoberta (BGP A-D). Essa mensagem é relacionada a uma extensão, ou família, do protocolo BGP, chamada de MCAST-VPN. Dessa forma o protocolo PIM e RP não são requeridos, pois cada PE origina a rota BGP A-D que identifica sua filiação no serviço MVPN. Além disso a rota BGP A-D é utilizada para propagar sinalização PIM da rede do cliente, possibilitando o uso do MPLS na rede da operadora.

Quando o MPLS é usado para criação dos túneis (P-tunnels) I-PMSI, todos os roteadores da operadora (PE e P) devem suportar o MPLS LSPs P2MP, que pode ser o *Multipoint LDP* (mLDP) ou P2MP RSVP-TE. Dessa forma cada PE gera e anuncia um rótulo que identifica o LSP P2MP com raiz em cada um dos outros PEs pertencentes ao serviço MVPN.

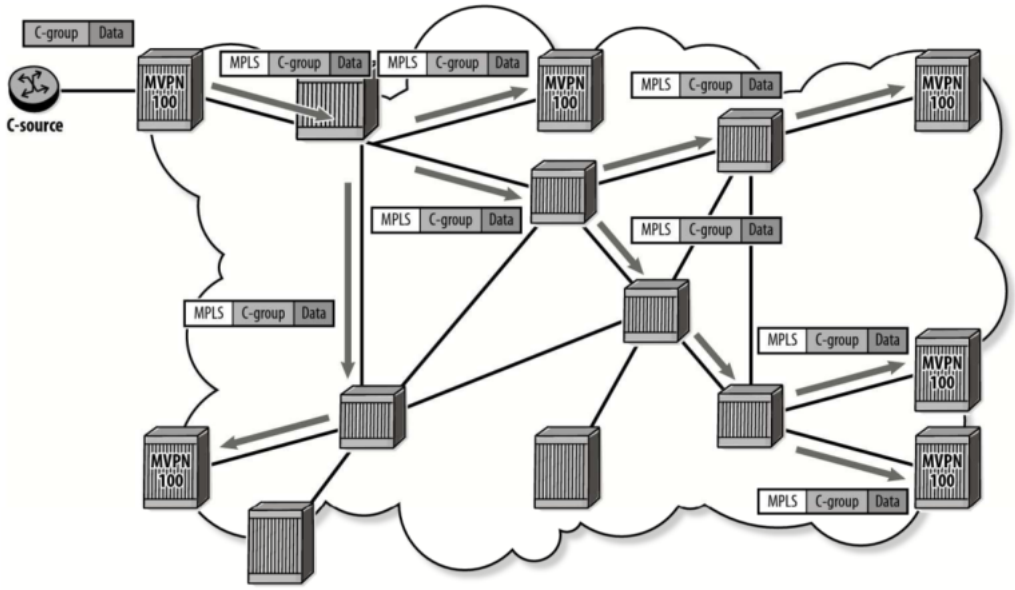
O tráfego *multicast* do cliente transportado por um LSP P2MP é rotulado e encaminhado assim como o tráfego unicast, exceto nos roteadores do meio da rede que tenham recebido mais de um rótulo de saída para aquele LSP P2MP que fará a replicação. A Figura 11 mostra o encapsulamento MPLS do tráfego do cliente, e as devidas replicações no meio da rede.

Pode ser observado que o NG-MVPN fornece um meio mais escalável e confiável de entregar o tráfego *multicast* em VPN, eliminando a necessidade de mensagens periódicas PIM para manter túneis PMSIs. Dessa forma o tráfego *unicast* e *multicast* de um cliente VPNL3 pode compartilhar os mesmos protocolos para ambos plano de controle e plano de dados, ou seja, o BGP e MPLS.

Conforme comentado, o NG-MVPN define uma extensão, que é conhecida como família no protocolo BGP. Essa nova família definida pelas RFCs do método NG-MVPN é a família MCAST-VPN, responsável pela padronização de novas mensagens, ou rotas, chamadas de *Network Layer Reachability Information* (NLRI), e também pelas suas trocas e funções como: descoberta dos PEs envolvidos em uma MVPN, troca da sinalização PIM do cliente e identificação do túnel MPLS a ser utilizado pelo tráfego *multicast*. São definidos sete tipos de NLRI, conforme a Tabela 1.

Às rotas do tipo 1 ao 4, conforme as RFCs, foi introduzido um novo atributo (*PMSI*

Figura 11 – Encapsulamento MPLS



Fonte: (WARNOCK; SHAHEEN; GHAFARY, 2015).

Tabela 1 – Tipos de Rotas NG-MVPN (NLRI)

Tipo	Tipo de Rota	Finalidade
1	Intra-AS I-PMSI A-D	Auto descoberta dos PEs
2	Inter-AS I-PMSI A-D	Auto descoberta dos PEs entre diferentes ASs
3	S-PMSI A-D	Notifica os PEs de um túnel S-PMSI
4	Leaf A-D	Utilizado com tipos 2 e 3 para identificar os nós folhas
5	Source Active A-D	Notifica os PEs de uma fonte C-multicast
6	Shared Tree Join	Sinaliza a entrada em um C-RP (RP do cliente)
7	Souce Tree Join	Sinaliza a entrada em um C-Source (fonte do cliente)

Fonte: Elaborado pelo Autor.

tunnel attribute), que identifica qual túnel, ou qual encapsulamento, utilizar para transportar os dados *multicast* do cliente, ou seja, qual protocolo utilizar no plano de dados. Por exemplo RSVP P2MP, mLDP ou até mesmo o GRE.

2.4.3 EVPN OISM (BGP/MPLS MVPN)

A tecnologia Ethernet VPN (EVPN), descrita na RFC7432 (DRAKE et al., 2015), permite que um provedor de serviço Internet (ISP) forneça serviço VPN de camada 2 (L2VPN) para seus clientes (conhecidos como locatários na RFC7432), utilizando um plano de controle flexível que permite conectividade intra-subrede em redes MPLS. Dessa forma uma única rede local (LAN), ou uma sub-rede, é dividida em vários "segmentos", sendo que cada segmento está localizado em uma localidade (*site*) diferente e os segmentos são interconectados por uma rede IP/MPLS.

A solução EVPN também permite a integração entre serviços VPNL2 e VPNL3 *unicast*, através de funcionalidades, que foram posteriormente padronizadas, como *Integrated Routing*

and Bridging (IRB) e *IP Prefix Advertisement*, que são descritos nas RFCs 9135 (SAJASSI et al., 2021) e 9136 (RABADAN et al., 2021), respectivamente. Essas funcionalidades permitem o tráfego entre domínios de *broadcast* distintos (Inter-subrede), garantindo a correta função de roteamento L3 e processamento IP *unicast* (ex.: decremento TTL). Porém, essas RFCs não definem o encaminhamento *multicast* IP inter-subrede. Assim um padrão está sendo proposto, o *draft* da IETF chamado *draft-ietf-bess-evpn-irb-mcast Optimized Inter-Subnet Multicast* (OISM) (LIN et al., 2023) descreve a funcionalidade de *multicast* IP otimizado dentro de um domínio de um cliente (VPN) que permite o encaminhamento *multicast* IP inter-subrede.

Assim a tecnologia EVPN se torna um modelo unificado para todos os tipos de serviços VPN, com uma única extensão do protocolo BGP (evpn) no plano de controle, podendo fornecer qualquer tipo de serviço VPN (L2VPN, L3VPN e MVPN) para um provedor de serviço que opera uma rede WAN. Além disso o EVPN é tecnologia adequada para redes de provedores de nuvem, pois permite a conectividade, em nível de camada 2 e 3 (L2 e L3 - roteamento e *switch* ou comutação), entre os locatários (*tenants*) de uma empresa, por exemplo um servidor, uma maquina virtual ou uma aplicação. A tecnologia se torna comum em redes *Wide Area Network* (WAN) e Data Centers, permitindo uma integração mais simples.

O EVPN é uma extensão do protocolo BGP, ou MP-BGP quando operado com extensões além do original IPv4. Dessa forma, o EVPN é executado sobre as sessões BGP (TCP) entre os roteadores da borda da rede (PEs), que fornecem o serviço VPN para os clientes. Sobre essa sessão BGP, rotas EVPN (mensagens) são trocadas a fim de realizar todo o controle dos serviços VPN oferecidos. São definidos vários tipos de rotas que são geradas pelos roteadores e utilizadas de acordo com o cenário ou serviço oferecido. A Tabela 2 apresenta as rotas EVPN existentes para serviços L2VPN e L3VPN, em que cada rota tem uma função específica.

A Tabela 2 mostra os tipos de rotas EVPN, a RFC em que está descrito e uma breve descrição de sua utilização. Rotas EVPN tipo 1 e tipo 4 são utilizadas somente quando existe um cenário *multi-homing*, ou seja, o equipamento do cliente (CE) é conectado em dois PEs distintos a fim de prover redundância de conexão ao provedor de serviço. Rotas EVPN tipo 2 são responsáveis pelo anúncio de endereço MAC do cliente conectado a porta do roteador, com opção de incluir o endereço IP. Rotas tipo 3 são utilizadas para descoberta de PEs membros de um determinado serviço VPN, formando a árvore requerida para o tráfego conhecido como *Broadcast, Unicast e Multicast* (BUM). Rotas tipo 5 são utilizadas para anúncio de prefixos IP, utilizado em serviços L3VPN. Rotas tipo 6, 7 e 8 são responsáveis por sinalização do tráfego *multicast*, porém somente para serviços L2VPN, ou sejá, somente dentro de uma mesma LAN.

O documento *Optimized Inter-Subnet Multicast* (OISM) (LIN et al., 2023) especifica novos procedimentos que permitem que o tráfego *multicast* IP seja roteado entre sub-redes (LANs) distintas de um determinado cliente (locatário), ao mesmo tempo em que faz com que o mesmo tráfego *multicast* IP seja comutado (*switch*) dentro de uma mesma LAN (intra-sub-rede) desse cliente. OISM é uma solução baseada em EVPN que permite o encaminhamento de pacotes IP *multicast* em serviços VPN, dentro de uma mesma sub-rede e entre sub-redes diferentes.

Tabela 2 – Tipos de Rotas EVPN

Tipo de Rota EVPN	Utilização	RFC
1 - Ethernet Auto-Discovery	Utilizado em cenários "multi-homing"(Convergencia rápida e "aliasing")	7432
2 - MAC/IP Advertisement	Anuncio de endereços MAC do cliente ou endereços IP	
3 - Inclusive Multicast Ethernet Tag (IMET)	Utilizado para descobrir outros PEs membros de um serviço e criar árvore de "flood"para tráfego tipo BUM	
4 - Ethernet Segment (ES)	Utilizado em cenários "multi-homing"(descoberta de ES e eleição de DF)	
5 - IP-Prefix	Anuncio de endereços IP para conexão inter-subrede, serviços L3VPN	9136
6 - Selective Multicast Ethernet Tag (SMET)	Indica interesse em receber tráfego multicast para (*, G) ou (S,G)	9251
7 - Join	Cenário Multi-homing - Synch o estado de "Join"entre os PEs conectados ao mesmo ES	
8 - IGMP/MLD Leave Synch	Cenário Multi-homing - Synch o estado de "Leave"entre os PEs conectados ao mesmo ES	

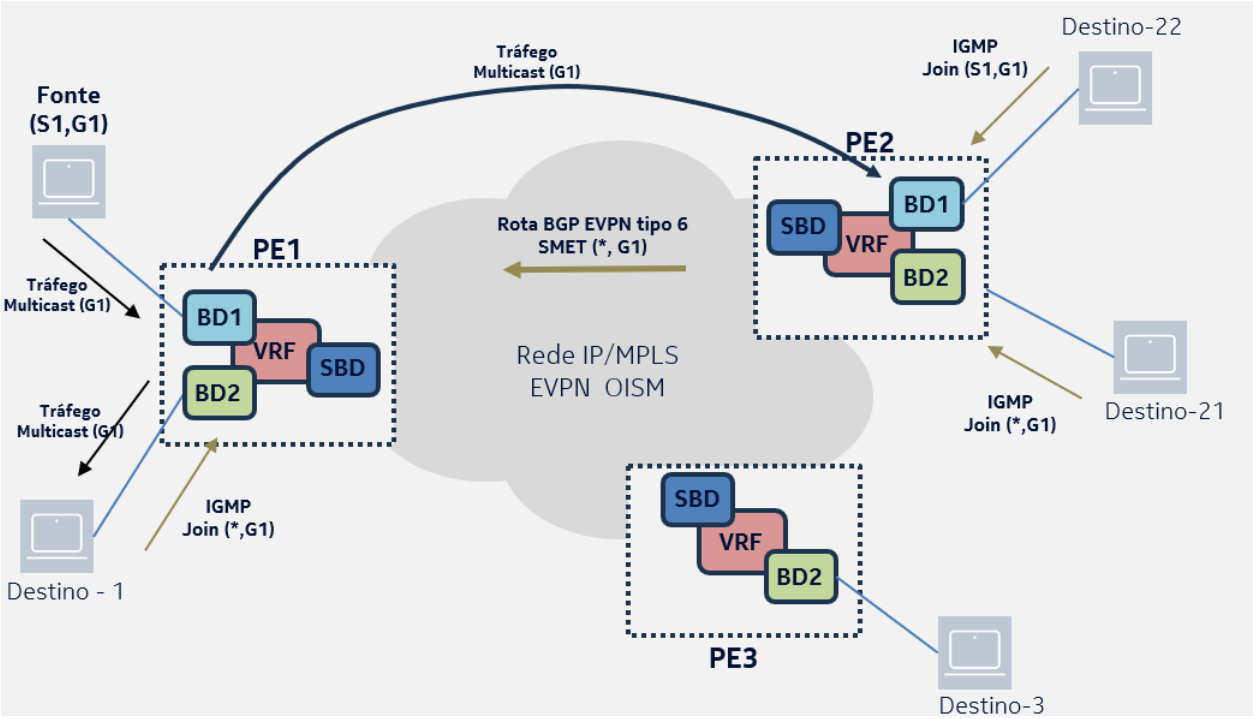
Fonte: O autor.

No plano de controle, o OISM modifica o procedimento das mensagens *multicast* descritas na (SAJASSI et al., 2022). No plano de dados o OISM especifica novos procedimentos para encaminhamento IP entre sub-redes diferentes.

EVPN OISM é compatível com encapsulamento MPLS e também *Virtual eXtensible Local-Area Network* (VXLAN) no plano de dados ou encaminhamento, e suporta grupos *multicast* IPv4 e IPv6. EVPN OISM é semelhante ao NG-MVPN, pois faz roteamento IP *multicast* em VPNs, usa MP-BGP para sinalizar o interesse de um PE em um grupo *multicast* específico e utiliza PMSI entre os PEs para enviar e receber o tráfego IP *multicast*. A Figura 12 mostra uma referência de operação do protocolo EVPN OISM e todos os componentes referentes a esse modelo, conforme a proposta (LIN et al., 2023; NOKIA-EVPN-GUIDE, 2023).

A Figura 12 representa uma rede IP/MPLS com três roteadores de borda de rede (PE1, PE2 e PE3), e o EVPN é o único protocolo *multicast* no plano de controle entre os PEs. Em cada PE são mostrados os componentes do serviço MVPN utilizando EVPN OISM, referente a apenas um cliente. Dessa forma, todas as fontes e destinos conectados pertencem a um mesmo cliente. No PE1 está conectada a fonte do tráfego *multicast* e o destino-1 interessado nesse tráfego. No PE2 estão conectados dois destinos interessados (21 e 22). E no PE3 está conectado o destino-3 mas que não tem interesse no tráfego, e nada sinaliza ao PE3. As setas indicam: o tráfego *multicast* do grupo 1 (G1), a sinalização IGMP dos destinos interessados aos PEs da rede e também a sinalização interna à rede (rota BGP tipo 6) em que o PE2 envia ao receber a sinalização IGMP dos destinos 21 e 22. Abaixo são descritos todos o componentes e funções encontrados na Figura 12:

Figura 12 – Operação EVPN OISM



Fonte: (NOKIA-EVPN-GUIDE, 2023).

- *Broadcast Domain* (BD). Domínio *broadcast* é uma LAN do cliente. O PE1 possui dois BDs, ou duas LANs do cliente. Nesse domínio as fontes e destinos do cliente, ou ambos, são conectados. Como BD1 e BD2 são LANs distintas, para os hosts de cada LAN comunicarem-se é preciso um roteador entre elas, que é a função da *Virtual Routing and Forwarding* (VRF). Veja que cada BD se conecta a VRF, através de uma interface IP.

- *Virtual Routing and Forwarding* (VRF) - É um roteador virtual do cliente. O serviço L3VPN do cliente possui uma tabela de roteamento da rede dedicada a esse cliente. No PE-1, na VRF conectam-se as dois BDs do cliente através de uma interface IP, assim como o *Supplementary Broadcast Domain* (SBD).

- *Supplementary Broadcast Domain* (SBD) - Também se conecta a VRF através de uma interface do tipo *evpn-tunnel*. Esse elemento é obrigatório para uma comunicação *multicast* Inter-subnet. É um domínio de *broadcast* responsável pela comunicação entre as VRFs de todos os PEs.

- Rota tipo 6: *Selective Multicast Ethernet Tag* (SMET) - Rota EVPN que os PEs utilizam para sinalizar o interesse por um grupo específico de *multicast*, pode ser (S, G) ou (*, G). Pode transportar informações para grupos *multicast* IPv4 ou IPv6.

- IGMP Join (S1, G1) ou (*, G1) - Mensagem do protocolo IGMP indicando que o destino tem interesse e deseja ingressar no Grupo-1 de *multicast*. S1 significa o endereço IP da fonte 1, dependendo da versão do protocolo IGMP (v2 ou v3), pode ser especificado na

mensagem IGMP Join (S1) ou não (*). Ao receber a mensagem IGMP Join, o PE gera a rota BGP EVPN SMET tipo 6 e envia aos seus vizinhos BGP.

Dessa forma, a rota EVPN SMET tipo 6 é gerada assim que o PE recebe uma mensagem IGMP *Join* para determinado grupo, com alguns parâmetros como endereço da fonte, endereço do grupo *multicast* de interesse e outros parâmetros referentes ao serviço VPN. Como por exemplo, o parâmetro *Route-Target* (RT), que identifica a qual serviço pertence essa rota SMET e em qual serviço VPN deverá ser importada. No caso da rota EVPN SMET tipo 6, é utilizado o RT do SBD, garantindo que as rotas SMET sejam importadas por todos os PEs do cliente. As rotas SMET também fornecem informação da árvore S-PMSI, garantindo que o PE envie tráfego *multicast* apenas para os PEs que requisitaram esse tráfego. No exemplo da Figura 12, apenas o PE2 requisitou o tráfego *multicast*, então apenas ele receberá.

Ainda na Figura 12, todas as sub-redes do cliente, redes das fontes e destinos, são anunciadas pela rota EVPN tipo 5 (*IP-Prefix*), que são instaladas nas tabelas de roteamento (VRF) dos PEs. Essas rotas também são usadas num mecanismo chamado *Reverse Path Forwarding* (RPF), que faz uma verificação se o pacote *multicast* está vindo pela interface correta, a fim de evitar *looping* na rede.

2.5 TRABALHOS RELACIONADOS

Nesta seção são apresentados trabalhos que lidam com a avaliação de serviços *multicast* em redes MPLS visando elencar as características avaliadas e destacar o diferencial deste trabalho.

Os trabalhos relacionados foram selecionados por apresentarem, principalmente, o tema de *multicast* dentro de VPNs em redes IP/MPLS empregado pela industria de telecomunicações. Ou, seja, tecnologias e protocolos que já possuem um padrão de comunicação estabelecido, e que por consequência já estejam implementados em roteadores comerciais. Nesse sentido foram encontrados apenas cinco trabalhos com essas características, entre 2006 e 2019, em que são apresentados as duas técnicas MVPN já existentes (Rosen e NG-MVPN). Com o intuito de verificar os trabalhos mais recentes no tema, foram selecionados trabalhos que abordavam o *multicast* em redes IP voltado a provedores de serviço, a partir do ano de 2018. Assim foram incluídos mais cinco trabalhos relacionados a tecnologia *Bit Index Explicit Replication* (BIER) e também IPv6. Que juntamente com as novas padronizações do BIER e IPv6 pela IETF, indica uma evolução de redes IP nessa caminho. O BIER trabalha no plano de encaminhamento *multicast*, que ainda assim depende de alguma técnica adicional para estabelecimento de serviços MVPN. Por último, foi selecionado um trabalho de 2024, propondo uma extensão ao protocolo EVPN para se realizar multicast em redes de *data center*. Nos próximos parágrafos serão apresentados cada um dos trabalhos relacionados.

O artigo de (METZ, 2006) examina o serviço *multicast* VPN (MVPN) em redes IP/MPLS, baseado no protocolo IP *multicast* PIM. O objetivo do artigo é apresentar o referencial teórico

envolvido no serviço MVPN existente na época, ou seja, (WIJNANDS; ROSEN; CAI, 2010). Os autores argumentam que a necessidade pelo serviço MVPN é que grandes empresas estão usando cada vez mais aplicações que requerem comunicação IP *multicast*, como distribuição de dados financeiros, e-learning e comunicações corporativas. Os conceitos que envolvem uma comunicação IP *multicast* desde o básico até o serviço MVPN são bem descritos. Porém, apesar de descrever bem a teoria do método MVPN existente na época, não foi realizado nenhum experimento prático ou comparação com algum outro método.

O trabalho de (BAZAMA, 2012) realiza uma investigação e análise de métodos MVPN. Ele realiza também uma implementação e avaliação de escalabilidade e desempenho entre dois métodos de MVPN em redes IP/MPLS: 1) Rosen e 2) NG-MVPN. Como motivador do uso do serviço MVPN (BAZAMA, 2012) inclui a aplicação Internet Protocol Television *Internet Protocol Television* (IPTV), se comparado ao (METZ, 2006), além também de serviços financeiros. Foram executados testes experimentais, ou cenários de avaliação, sendo dois cenários voltados para o método Rosen e três cenários voltados para o método NG-MVPN. A avaliação de escalabilidade se deu medindo dois parâmetros: 1) número de mensagens de controle geradas na rede (*overhead*) e 2) número de sessões/adjacências entre os PEs. No método NG-MVPN o número de mensagens de controle corresponde à variável número de rotas BGP. Por se tratar de escala, não foi medido o número de mensagens que atingem a *Central Processing Unit* (CPU) de fato e também o tempo de CPU tomado. Os dados foram interpretados em cada cenário em separado e mostrados em forma de gráficos, porém nenhuma técnica estatística de comparação foi utilizada.

O trabalho de (LIANG et al., 2014) investiga as seguintes técnicas MVPN existentes: draft-Rosen (que utiliza encapsulamento GRE), RSVP-TE P2MP e *multicast* LDP (mLPD), em um serviço de distribuição de vídeo legado *Digital Video Broadcasting* (DVB). Através de um experimento, em uma rede com roteadores e geradores de tráfego dedicados, avalia o desempenho dessas técnicas. Nesse experimento foi realizado um tipo de teste de convergência, gerando um quantitativo significativo de fontes geradoras de tráfego *multicast* e receptores (20 MVPN, 400 fontes e 400 grupos *multicast* por MVPN e 400 destinos). Como resultado concluiu-se que os três métodos conseguiram uma convergência dentro de 23 segundos. Também foi avaliado um teste de falha em um determinado enlace primário dentro da rede, e verificado o tempo que o tráfego levou para convergir por outro caminho. Foi constatado que o RSVP-TE P2MP apresentou um menor tempo, 14.5 milissegundos. Dessa forma foi concluído que o RSVP-TE P2MP é a técnica preferível para distribuição de vídeo, mas o mLDP também pode ser empregado em outras situações como distribuição de conteúdo (*Content Delivery Network*s (CDNs)) e serviços de videoconferência empresariais. Ao citar as técnicas de MVPN que utilizam o MPLS como plano de dados (encapsulamento MPLS - RSVP P2MP e mLDP), o artigo não deixa claro qual protocolo realiza a sinalização do domínio *multicast* do cliente.

A dissertação de mestrado de (RIAZ, 2015) tem como objetivo investigar e comparar diferentes abordagens de MVPN, que são utilizadas em redes reais de operadoras - Draft-Rosen

e Next Generation MVPN (NG-MVPN). Além de explorar toda a teoria de ambas as técnicas, o relatório traz um capítulo que compara todos os pontos das técnicas MVPN, deixando clara a desvantagem do Draft-Rosen em relação à escala do plano de controle por requerer muitas sessões entre os PEs de uma rede. Ao final é apresentada uma experimentação baseada no esquema Draft-Rosen, porém não faz nenhuma medição e comparação em termos de desempenho ou capacidade dos serviços.

O documento (VENKATESWARAN et al., 2019) defende uma técnica para interoperabilidade entre as técnicas de MVPN: draft-rosen e NG-MVPN. Ou seja, a interoperabilidade entre os novos roteadores que suportam o NG-MVPN, com equipamentos legados que suportam a draft-rosen. A motivação seria a demanda de migração das redes/equipamentos legados para os novos roteadores que suportam o novas tecnologias de MVPN, como o método NG-MVPN. Os novos meios de transporte citados pelo documento, como evolução do encapsulamento legado GRE para o serviço de MVPN, são MPLS, *Bit Index Explicit Replication* (BIER), e *Tree Segment Identifier* (Tree-SID). De fato, um roteador que suporta NG-MVPN provavelmente suporte o legado draft-rosen, porém não é vantajoso consumir recursos de um roteador com protocolos legados que são menos escaláveis. Dessa forma o documento propõe um dispositivo que opere como *gateway* entre as duas redes, realizando uma tradução entre os métodos de MVPN. Para isso esse roteador deve manter um mapeamento de fluxo *multicast* um-para-um para cada serviço MVPN entre os dois mundos. O documento descreve em alto nível os procedimentos utilizados nesse mapeamento numa arquitetura de rede de exemplo, porém não há experimentos envolvidos.

Devido à não adoção pela indústria de um padrão para encapsulamento BIER IPv6, o artigo (LAN et al., 2023) analisa duas tecnologias de encapsulamento multicast: BIERV6 e BIERin6. Com isso, é descrita a arquitetura de rede em alto nivel da operadora China Telecom MCN, considerando o encapsulamento *multicast* BIERV6. A fim de comprovar seu funcionamento, e também a interoperabilidade entre diferentes fabricantes, foi realizado um experimento de laboratório com tráfego IPv4 e IPv6. Esse experimento foi realizado com equipamentos de rede de diferente fabricantes e geradores de tráfego dedicados. Ou seja, o artigo descreve um projeto completo de rede de uma operadora, com testes reais e planejamento para evolução para *multicast* IPv6. Porém, para o plano de controle utiliza o BGP método NG-MVPN para sinalização dos túneis *multicast*.

O artigo (MERLING; STüBER; MENTH, 2023) faz uma análise de um problema da implementação do BIER em grandes redes. Em grandes redes, receptores de um domínio BIER são colocados em subdomínios, e esta condição acarreta duplicação de pacotes pois para cada subdomínio é necessária uma cópia do pacote desde que haja um receptor neste subdomínio. Assim, o artigo propõe e compara algoritmos que lidam com esse problema de subdomínios BIER, pois a correta escolha da arquitetura de subdomínios pode evitar replicações desnecessárias. Porém, o potencial de otimização do tráfego *multicast* utilizando o BIER depende de fatores como topologia e tamanho de rede e número de grupos *multicast*. Mesmo assim, é mostrado que o BIER ainda pode reduzir o tráfego na maioria das topologias de rede.

Devido ao surgimento de novos serviços de vídeo e desenvolvimento de tecnologias 5G e de nuvem, o artigo (LI et al., 2023) faz uma análise de protocolos que atendem essa nova demanda de rede e ao mesmo tempo são compatíveis com IPv6, como BIERv6 e EVPN. Ele apresenta exemplo de uma arquitetura, em alto nível, do serviço de vídeo IPTV utilizando BIERv6 juntamente com BGP NGMPN para MVPN e EVPN para tráfego unicast.

O artigo (DESMOUCEAUX et al., 2018) faz um estudo do uso de BIER para comunicação *multicast*, mostrando que esse mecanismo é eficiente e confiável, em que tráfego redundante é evitado, e que nenhum estado de fluxo é mantido em roteadores intermediários, como em protocolos legados. Tal artigo também faz uma avaliação de desempenho da comunicação *multicast* utilzando o BIER, através de simulações e formulação de um modelo analítico para quantificar esse desempenho.

O artigo (MERLING; LINDNER; MENTH, 2020) faz uma análise de dois mecanismos de encaminhamento do tráfego *multicast* utilizando o BIER em caso de falha de rede, que são: o *Loop-Free Alternates* (LFA) e um mecanismo baseado em túnel. O artigo também mostrou que existem deficiências da abordagem baseada em LFA e propôs extensões para contornar essas deficiências, e deixar ambos os mecanismos com o mesmo tempo de convergência.

A tecnologia de rede *Ethernet Virtual Private Network - Virtual Extensible Local Area Network* (EVPN-VXLAN), que é amplamente utilizada em virtualização de redes em *data centers*, não suporta o serviço *multicast*. Dessa forma, o artigo (WU et al., 2024) propõe uma nova rota, tipo de rota, ou mensagem de roteamento, inserida no protocolo *Ethernet VPN* (EVPN) que permite a troca de informações referente ao serviço *multicast* e seleção de caminho *multicast* para redes de *data centers*.

A Tabela 3 resume os trabalhos relacionados apresentados nesta seção juntamente com o trabalho proposto na última linha. Os trabalhos relacionados estão ordenados pelo ano de publicação. A tabela comparativa contém o título, o autor e as características de cada trabalho, sendo o método MVPN, IP *multicast* que utiliza o BIER e se possui experimento realizado. O principal diferencial de nosso trabalho é a inclusão de um novo método MVPN que está sendo padronizado pelo IETF, baseado no BGP-EVPN. Além disso, incluem-se experimentos que medem parâmetros relacionados ao desempenho do protocolo no roteador, e diferentemente dos outros trabalhos, é o único que inclui, além do número de rotas BGP, o número de mensagens BGP totais que atingem a CPU do roteador. Além disso, este trabalho também apresenta uma análise estatística mais sofisticada na avaliação dos resultados dos experimentos.

Tabela 3 – Trabalhos Relacionados

			Técnica MVPN			**Multicast | EVPN**		**Experimento**
Ano	**Título**	**Autor**	**Rosen MVPN (PIM)**	**NG-MVPN BGP-MVPN**	**MVPN BGP-EVPN**	**IP *multicast* BIER**	**BGP-EVPN**	**Possui experimento**
2006	Multiprotocol label switching and IP. Part 2. *multicast* virtual private networks	C. Metz	x					
2012	Investigation into Layer 3 *multicast* Virtual Private Network Schemes	Muneer Ibrahim Bazama	x	x				x
2014	Evaluation of MVPN Technologies for China's NGB Backbone Networks	Liang et al.	x	x				x
2015	Multicast in MPLS based Networks and VPNs	Hamir Riaz	x	x				x
2018	Reliable *multicast* with B.I.E.R.	DESMOUCEAUX et al.				x		
2019	INTERWORKING BETWEEN LEGACY AND NEXT-GENERATION *multicast* VIRTUAL PRIVATE NETWORK (MVPN) TRANSPORTS	Venkateswaran et al.	x	x				x
2020	Comparison of Fast-Reroute Mechanisms for BIER-Based IP *multicast*	MERLING; LINDNER; MENTH				x		
2023	Efficiency of BIER *multicast* in Large Networks	MERLING; STüBER; MENTH				x		
2023	Research and Verification of New *multicast* BIER IPv6 Technology in IP Network	LAN et al.		x		x		x
2023	"IPv6+" Video Service Solution Based on Metropolitan Area Cloud Network	LI et al.		x		x	x	
2024	A *multicast* Scheduling Method Based on EVPN-VXLAN Extension in Data Center Networks	WU et al.					x	
2024	**Análise de técnicas de IP *multicast* para redes virtuais privadas em infraestrutura IP/MPLS baseado em BGP**	**Este trabalho**	**x**	**x**	**x**	**x**	**x**	**x**

Fonte: O Autor.

2.6 CONSIDERAÇÕES DO CAPÍTULO

Nesse capitulo foi apresentado toda a teria abrangendo as tecnologias mais relevantes para formação dessa pesquisa. O desenvolvimento de redes IP permitiu, e ainda permite, um grande avanço em tecnologias de redes de telecomunicações. A Internet, e toda sua hierarquia, são redes IP. E toda a interconexão das diferentes redes (diferentes *Autonomous Systems* (AS)) que compõe a Internet utiliza o protocolo *Border Gateway Protocol* (BGP). Além disso, o surgimento da arquitetura de redes *Multiprotocol Label Switching* (MPLS) adicionou um ganho extra em redes IP, otimizando o encaminhamento de dados e permitindo novos serviços para as provedoras de rede. Na perspectiva de uma provedora de redes, os serviços *Virtual Private Network* (VPN) que utilizam tecnologias IP/MPLS/BGP, possibilitou a expansão e aumento das redes de telecomunicações e a oferta de novos serviços de redes personalizados.

Foi visto que encaminhamento do tráfego *multicast* possui uma otimização do uso de uma rede IP, evitando duplicação de pacotes sem necessidade. A necessidade do *multicast* se dá quando se precisa distribuir um conteúdo para um grupo de destinos interessados. Esse tipo de encaminhamento *multicast* é muito utilizado por aplicações baseadas em vídeo, por exemplo. Pensando na melhor eficiência de uso da rede, técnicas de MVPN foram sendo padronizadas pela IETF. Uma das principais aplicações que uma provedora de rede pode ofertar juntamento com o serviço de banda larga é o *Internet Protocol Television* (IPTV), além de serviços de VPN corporativos com suporte a tráfego multicast dos clientes.

Técnicas para o estabelecimento de serviços MVPN são necessárias, e envolvem protocolos específicos para este fim. Esse capitulo apresentou as técnicas e protocolos envolvidos em serviços MVPN, padronizados ou que estão em padronização pela IETF. Além disso, a seleção de trabalhos relacionados com esta pesquisa foi discutida.

3 EXPERIMENTAÇÃO

De forma a subsidiar a resposta à pergunta de pesquisa, os dois métodos de serviço MVPN mais recentes, baseados no protocolo BGP (EVPN e NG-MVPN), foram configurados e testados em um ambiente de rede emulado. Trabalhos sobre o método *Draft-Rosen*, como (BAZAMA, 2012; LIANG et al., 2014; RIAZ, 2015), mostraram que a principal desvantagem dessa técnica é a baixa escala de rede. Isso pois o método *Draft-Rosen* utiliza protocolos antigos de *multicast* que consomem muito recurso dos roteadores nós intermediários. Como tais trabalhos já experimentaram essa técnica "legada", este experimento considerou a avaliação dos dois métodos de serviço MVPN baseados no protocolo BGP.

Para que os cenários e parâmetros sejam representativos de cenários reais de rede, esse ambiente é composto por roteadores em rede IP/MPLS, simulando a rede da operadora. Serviços MVPN foram configurados nos roteadores de borda de rede (PEs), simulando os diversos clientes desses serviços MVPN. Experimentos foram realizados para a devida comparação de desempenho dos métodos em relação ao plano de controle, ou seja sinalização necessária para estabelecimento da comunicação multicast. As métricas de comparação utilizadas foram coletadas a partir do protocolo BGP, que foi utilizado para sinalização MVPN por ambos os métodos. A ideia é que cada serviço MVPN, ou seja, cada cliente, gere uma carga no protocolo BGP referente à sinalização de canais multicast, IPv4 e IPv6, e estabelecimento da comunicação. Dessa forma o número de mensagens BGP, memória e CPU analisados nos roteadores mostram o impacto de cada método MVPN na rede.

As métricas coletadas no experimento realizado foram: 1) Quantidade de pacotes BGP direcionadas à CPU do roteador; 2) quantidade de rotas BGP trocadas na rede, 3) memória utilizada pelo processo BGP e 4) utilização da CPU do processo BGP. Essas métricas foram obtidas a partir do sistema operacional do roteador, coletadas através de comandos executados em cada roteador da rede. São todos valores possíveis de serem extraídos do roteador Nokia, (NOKIA-UNICAST-GUIDE, 2023), referente ao protocolo BGP. Além disso, conforme (MEYER; PATEL, 2006), CPU e memória do BGP são indicadores de desempenho e são afetados pelo número de mensagens de atualização e rotas BGP.

Conforme (LILJA, 2000), quaisquer medidas realizadas estão sujeitas a erros de medições (ou ruídos). Portanto, além dos valores das medidas em si, também é necessário determinar se as diferenças de valores encontradas entre os métodos são devido a erros de medição, interpretadas como flutuações randômicas, ou se essas diferenças são estaticamente significativas. Além disso, conforme a análise adotada é possível também mensurar a magnitude dessa diferença, ou qual o tamanho dessa diferença. Nesse sentido, portanto, além da obtenção dos valores da métricas, foram realizadas análises estatísticas para determinar a significância dos resultados. Para essas análises foi utilizado o R Studio, com a linguagem R, ambiente de software livre para computação de estatísticas e realização de gráficos (DALGAARD, 2008), (KABACOFF, 2011).

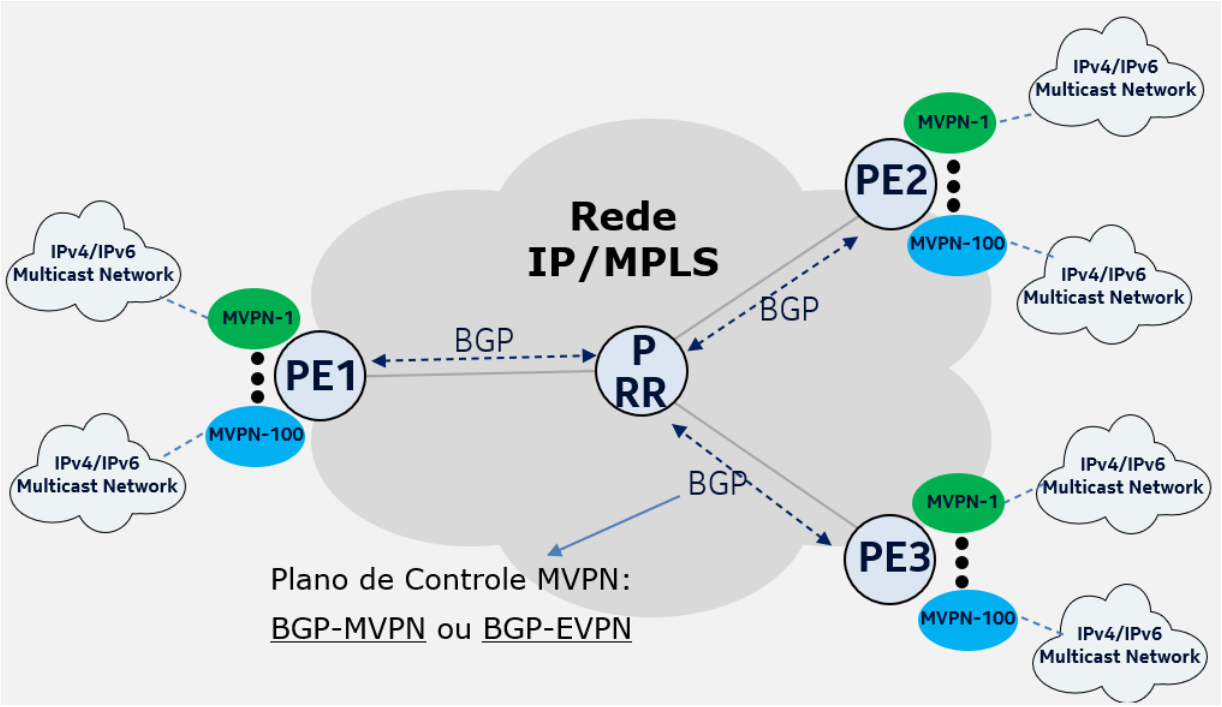
As próximas sessões deste capítulo detalham a topologia de avaliação de desempenho

entre os métodos, a metodologia utilizado para realização do experimento, as tabelas de resultados obtidas para cada condição e as análises estatísticas desses dados. Foi visto que o método MVPN EVPN trouxe ganhos em relação ao NG-MVPN por utilizar menos recurso de plano de controle da rede para executar a mesma funcionalidade.

3.1 CENÁRIO DE AVALIAÇÃO DAS TECNOLOGIAS MVPN

O cenário de avaliação é ilustrado pela Figura 13. A rede IP/MPLS é composta por quatro roteadores, sendo três PEs (PE1, PE2 e PE3) e um P. Todos os três PEs se conectam diretamente com o P, formando a topologia física. Essa topologia deve ser o suficiente para garantir a comunicação entre os roteadores, pois toda a análise é realizada tendo em visto o protocolo BGP.

Figura 13 – Topologia de Avaliação



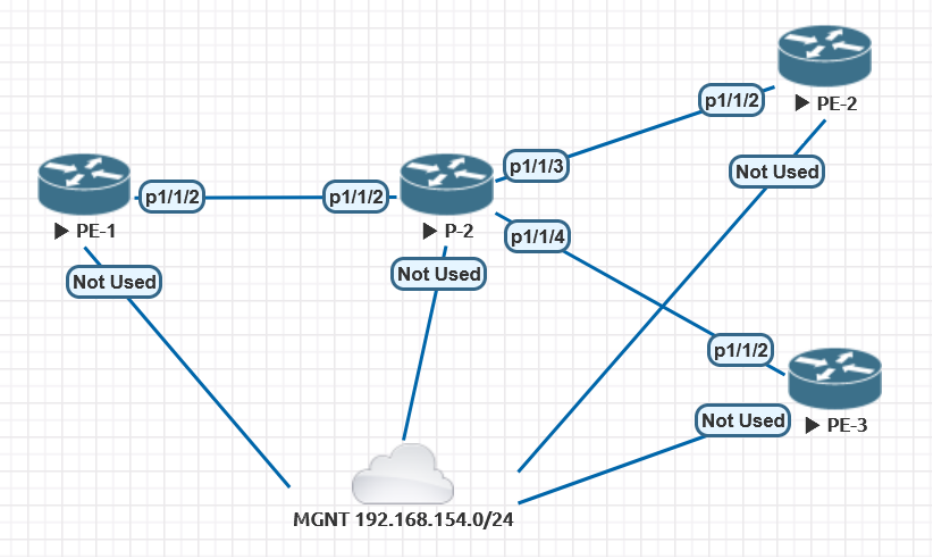
Fonte: O autor.

O cenário de avaliação foi implementado com software de roteadores da marca Nokia modelo 7750SR, versão TiMOS-B-23.7.R1, virtualizados pela seguinte infraestrutura:

- Laptop Lenovo T490 (Intel(R) Core(TM) i5-8365U CPU @ 1.60GHz) com 48GB RAM;
- Sistema Operacional Windows 10;
- Hypervisor VMware® Workstation 15 Player;
- Simulador de rede EVE-NG.

O EVE-NG é um simulador de rede, baseado em Linux, desenvolvido para atender a demanda do mundo de *Tecnologia da Informação* (TI), permitindo que profissionais das áreas de redes, segurança e DevOps criem ambientes virtuais para provas de conceitos, criação de solução ou treinamento. Com ele é possível emular qualquer equipamento de rede, de qualquer fabricante que disponibilize uma imagem de seu equipamento, ou sistema operacional, e conectá-los em rede. A Figura 14 mostra a interface gráfica do EVE com a topologia utilizada. A nuvem chamada de "MGMT 192.168.154.0/24"representa a conexão de acesso aos roteadores, ou seja, por onde é realizado a conexão SSH nos roteadores.

Figura 14 – Topologia EVE



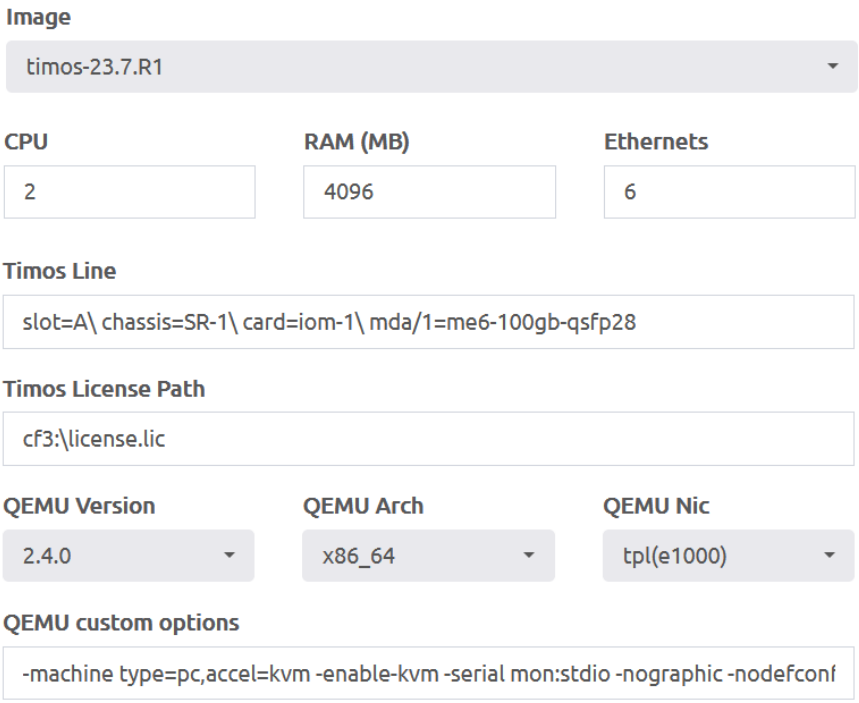
Fonte: O autor.

Cada roteador Nokia é virtualizado utilizando QEMU/KVM (QEMU, 2024), conforme o modelo de implementação (EVE-NG, 2024). A Figura 15 mostra os parâmetros utilizados para a virtualização do sistema operacional do roteador Nokia SROS.

Os roteadores foram configurados para formarem uma rede IP/MPLS entre eles, através dos protocolos de rede IP, IS-IS e LDP. Cada roteador é identificado na rede por um IP interno, chamado de IP de sistema, que é anunciado para cada um dos roteadores vizinhos por um protocolo de roteamento. Neste trabalho foi utilizado o protocolo de roteamento estado de enlace IS-IS. Dessa forma cada roteador consegue alcançar qualquer outro roteador na rede, desde que haja um caminho possível. Isso permite a comunicação de protocolos como LDP e BGP que utilizam o IP de sistema para estabelecimento de sessões. Abaixo o endereçamento IP utilizado na rede:

- Endereço IP de sistema dos roteadores:
  - PE1: 172.16.0.1/32
  - PE2: 172.16.0.2/32

Figura 15 – Parâmetros de Virtualização Nokia SROS



Fonte: O autor.

  - PE3: 172.16.0.3/32
  - P: 172.16.0.5/32

- Endereços de Redes IP dos enlaces entre roteadores:
  - Enlace PE1-P: 10.1.5.0/24
  - Enlace PE2-P: 10.2.5.0/24
  - Enlace PE3-P: 10.3.5.0/24

Este cenário foi escolhido pensando em obter resultados representativos de uma rede real, do ponto de vista do protocolo BGP. Da mesma forma, esse cenário deve ser simples o suficiente para que se pudesse ser implementado em um notebook, utilizando software de roteadores comerciais em ambiente de rede virtualizado. Os quatro trabalhos relacionados que possuem experimentos utilizam cenários de rede com quatro PEs (BAZAMA, 2012; LIANG et al., 2014; RIAZ, 2015; LAN et al., 2023). Neste trabalho o cenário possui três PEs e um P, com a função de refletor de rotas BGP. Os três PEs são suficientes para que seja gerada uma carga considerável na rede (serviços MVPN) e comparação de desempenho do protocolo de controle BGP entre os dois métodos MVPN. Nesse cenário o aumento da carga (pacotes BGP) se dá pelo aumento do número de serviços MVPN nos PEs. Ou seja, o PE apenas gera carga caso ele seja configurado com serviço MVPN. Dessa forma, um pequeno aumento no número de PEs na rede, para realizar esse tipo de análise, não adicionaria novas conclusões. Se pensarmos em uma rede real, seguindo o

padrão IETF *Seamless MPLS Architecture* (LEYMANN et al., 2014), grandes backbones MPLS são divididos em áreas de redes menores (área de acesso - que representam áreas metropolitanas - onde estão localizados os PEs da rede) conectadas a um núcleo de rede central servindo como trânsito dessas áreas menores. Em grandes centros comerciais (ex: São Paulo) podemos assumir que uma determinada área de acesso possui cerca de 30 PEs, em que cada PE possa receber centenas de serviços e clientes, conforme fabricantes de roteadores (NOKIA, 2024), (MX, 2024) e (ASR, 2024). Dessa forma o cenário de experimento desse trabalho conta com três PEs e um P (BGP RR), podendo representar uma rede metropolitana.

Assim, o roteador P assume outra função de rede: a de refletor de rotas BGP, conhecido como *Route Reflector* (RR) da rede. O protocolo BGP necessita que todos os PEs da rede troquem rotas entre si, e para isso é necessário estabelecer uma conexão BGP (TCP) entre todos eles. O modo mais básico para cumprir tal premissa é utilizar um modelo *full-mesh*, em que cada PE estabelece uma sessão BGP com cada outro PE da rede. A presença de um RR na rede significa ganho de escala, em que todos os PEs estabelecem sessão BGP apenas com o RR, e não entre todos eles. Na topologia de rede desse trabalho, por ter poucos PEs (apenas três), isso não representa um problema. Porém, na rede da operadora que possui centenas de PEs, não seria nada escalável se cada PE tivesse que estabelecer conexão com todos as outras centenas de PEs da rede. Além disso para cada novo PE que ingresse na rede, todos os demais PEs precisariam ser configurados. Neste trabalho, o principal motivo de se ter um RR, além de ser um cenário mais próximo possível de uma rede de operadora de telecomunicações, é que é possível mensurar o número total de rotas e pacotes BGP em um único ponto da rede (no P) facilitando assim a coleta das métricas.

Os serviços MVPN foram configurados nos roteadores de borda de rede (PEs), simulando os diversos clientes ou serviços da operadora. A facilidade aqui se dá pela possibilidade de simulação de clientes multicast através de configurações estáticas dentro desses serviços MVPN. Dessa forma, o roteador através do protocolo BGP realiza toda a sinalização e estabelecimento dos caminhos multicast. Para isso são necessárias três coisas:

- Ativação de uma interface física disponível no roteador para o cliente. Para que cada PE suporte 100 clientes ao mesmo tempo, foi utilizada uma única porta física do roteador para todos os clientes, e criadas interfaces virtuais diferenciadas pelas VLANs (VLANs de 1 a 100).

- Ativação de uma interface IP no enlace entre PE e o cliente. As redes IPs (IPv4 e IPv6) utilizados nesses enlaces foram: 192.168.11.0/24 e 2001:cafe::192:168:11:1/64 para PE1, 192.168.12.0/24 e 2002:cafe::192:168:12:1/64 para PE2 e 192.168.13.0/24 e 2003:cafe::192:168:13:1/64 para PE3.

- Configuração estática de canais multicast na MVPN desse cliente.

A fim de gerar certo volume de carga que seja representativo, e considerando centenas

de serviços que uma rede metropolitana possa ter, foram realizados testes com três cargas de serviços MVPN diferentes: 25, 50 e 100 serviços MVPN configurados em cada PE. Cada teste foi realizado utilizando uma determinada carga e método MVPN, representando seis cenários carga/método diferentes (três cargas x dois métodos).

Com relação aos fluxos MVPN, cada serviço MVPN configurado em cada PE simula a solicitação de 10 canais multicast IPv4 e 10 canais multicast IPv6 para outro roteador PE que será sua fonte. Dessa forma, cada PE também é fonte de tráfego multicast. Dessa forma, temos a seguinte configuração: PE1 solicita tráfego ao PE2, PE2 solicita tráfego do PE3, e PE3 solicita tráfego ao PE1. Os canais multicast IPv4/IPv6 utilizados nos testes foram:

- 10 grupos multicast IPv4: 239.90.3.1 - 239.90.3.10
- 10 grupos multicast IPv6: ff3e::0001 - ff3e::000a

Os fluxos MVPN configurados, que representam a carga dos serviços, possuem pares de origem-destino fixos, começam e terminam todos juntos, e são mensurados durante um determinado tempo. O objetivo deste experimento é avaliação de desempenho, com relação a escala ou quantidade de serviços e fluxos MVPN, entre dois métodos. Assim entende-se que realizar variações nesses fluxos levaria aos mesmos resultados. Pois o importante aqui é garantir o mesmo cenário de quantidade de serviços/fluxos, mantendo os mesmos níveis dos parâmetros, para se realizar uma comparação justa entre os dois métodos. Cenários heterogêneos fazem mais sentido em testes de convergência por exemplo, que se mede o tempo de convergência da rede em caso de falhas.

É importante notar que todos os serviços MVPN utilizaram os mesmos IPs de grupo multicast e também os mesmos IPs de interface entre o PE e o cliente. Isso ocorre pois os clientes estão dentro de VPNs separadas. Dessa forma, como as VPNs são independentes e não se comunicam entre si, pode haver sobreposição de IPs entre diferentes VPNs sem haver conflito de endereçamento IP.

Para cada um dos 6 cenários de testes, foram executadas cinco repetições. Assim, foram executados um total de 30 testes. Ou seja, foram executadas três cargas MVPN, isto é, três configurações de serviços MVPN, sendo 25, 50 e 100 serviços MVPN, para cada método (EVPN/NGMVPN) com cinco repetições (3 x 2 x 5 = 30 testes).

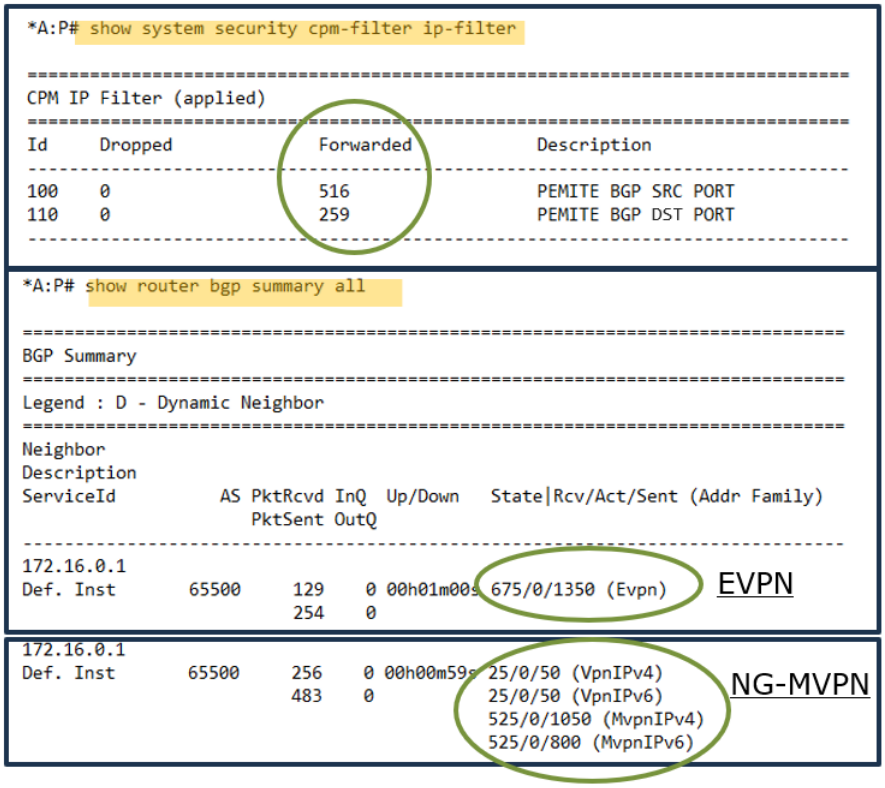
Como já mencionado, as métricas coletadas nos testes foram:

1. Quantidade de pacotes BGP direcionadas à CPU do roteador.
2. Quantidade de rotas BGP trocadas na rede.
3. Memória utilizada pelo processo BGP.
4. Utilização da CPU do processo BGP.

As métricas quantidade de pacotes e rotas BGP foram extraídas do roteador P, pois é o roteador refletor de rotas BGP. Como todos os PEs estabelecem sessão BGP com o P e este recebe todas as rotas dos PEs, o roteador P terá os valores totais de rotas e pacotes BGP utilizados no teste. As métricas memória e CPU do processo BGP foram extraídas de todos os PEs, pois são neles que os serviços MVPN são instanciados, resultando em maior processamento e instalação de rotas na memória do roteador.

A Figura 16 ilustra um exemplo de como as métricas quantidade de pacotes e rotas BGP apresentam-se no console do roteador P, e portanto, de onde foram coletadas. Para quantidade de rotas a Figura 16 mostra também a sessão BGP estabelecida entre dois roteadores, para os dois métodos MVPN (EVPN e NG-MVPN). Para o NG-MVPN é preciso o estabelecimento de quatro famílias BGP para o funcionamento do serviço MVPN: VpnIPv4, MvpnIPv4, VpnIPv6 e MvpnIPv6. Enquanto que para o EVPN é preciso de apenas uma, Evpn. Por outro lado, a Figura 17 ilustra um exemplo das métricas memória e CPU do processo BGP console do roteador PE1. É importante observar, que a amostra de CPU é coletada através de um comando no console do roteador, que especifica o período de amostra (*sample-period*) dado em segundos, que no caso foi de 60 segundos. Na prática, isso significa a média de uso do roteador (sua CPU) nos últimos 60 segundos.

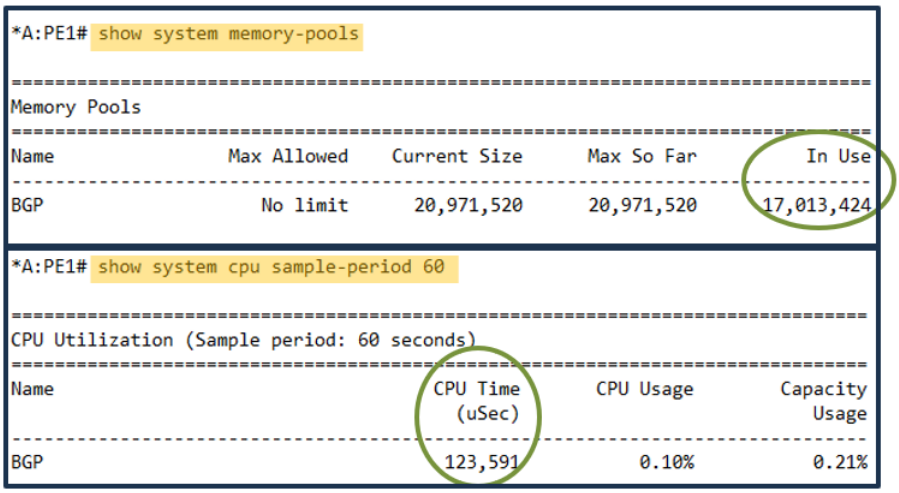
Figura 16 – Exemplo de Métricas do Roteador - Pacotes e Rotas



Fonte: O Autor.

Após realizados os 30 testes, os arquivos textos salvos com os resultados foram formatados em tabelas para sua correta análise estatística, como será visto na próxima sessão.

Figura 17 – Exemplo de Métricas do Roteador - Memória e CPU



Fonte: O Autor.

3.2 EXPERIMENTOS E RESULTADOS

Para realização e padronização dos testes, um processo de coleta dos resultados foi estabelecido. Em cada roteador foi inserido o mesmo **script**, Código 1, de captura de dados, com os comandos do sistema operacional TiMOS da Nokia, para o devido registro dos resultados. Após a inicialização dos roteadores em rede, configurados no seu devido cenário de teste (ex: número de seriços MVPN = 50 / Método = EVPN), é estabelecida uma sessão *Secure Shell* (SSH) da máquina host (a partir do sistema operacional Windows 10, na nuvem MGMT da Figura 14) com cada roteador. Assim que o cenário estiver pronto e a rede estável, o *script* do Código 1 é executado ao mesmo tempo em todos os roteadores. Em cada sessão SSH, todos os comandos inseridos e resultados retornados pelos roteadores são gravados em arquivos texto para armazenamento e posterior processamento dos dados. O *script* leva cerca de 63 segundos para ser executado, que é tempo suficiente para a convergência do protocolo BGP. Basicamente esse *script* desabilita o processo BGP, limpa os contadores das métricas, habilita o BGP novamente, espera 60 segundos e coleta todas as métricas. O *script* executa a sequência ascendente dos comandos, conforme Código 1.

A Tabela 4 apresenta o resultado do número de rotas BGP, por método MVPN e por número de serviços configurados. Esses valores foram coletados do roteador P, pois é nele que todos os PEs fecham a sessão BGP. Dessa forma, o roteador P possui o total de rotas geradas por todos os PEs da rede. Apesar de terem sido executadas 5 amostras de testes para cada método, o número de rotas não varia, sendo sempre o mesmo a cada execução.

Analisando os dados da Tabela 4 em termos da correlação entre o número de serviços e o número de rotas, por meio de análise de correlação, utilizando o ambiente R Studio, nota-se que a mesma é perfeita. Ou seja, o coeficiente de correlação r = 1. Conforme (DALGAARD, 2008) o teste de correlação é usado para avaliar uma associação (dependência) entre duas variáveis,

Código 1 – Script de captura de dados

```
1
2  /configure router bgp shutdown # Desativa o processo BGP
3  /clear cpm-filter ip-filter # Limpa contadores
4  /sleep 3 # Espera 3 segundos
5  /configure router bgp no shutdown # Ativa o processo BGP
6  /sleep 60 # Espera 60 segundos
7  /show system security cpm-filter ip-filter # Coleta Pacotes
8  /show system memory-pools # Coleta Memoria
9  /show router bgp summary all # Coleta Rotas
10 /show system cpu sample-period 60 # Coleta CPU
```

Tabela 4 – Número de Rotas BGP

Número de Serviços MVPN	**Número de Rotas BGP**	
	NG-MVPN	**EVPN**
25	3050	2025
50	6100	4050
100	12200	8100

Fonte: O Autor.

através do coeficiente de correlação. Ele varia de -1 a $+1$, onde os extremos indicam correlação perfeita e 0 significa nenhuma correlação.

Nesse sentido, pode-se observar que ao dividir-se o número de rotas pelo número de serviços para cada linha da tabela, perceber-se-á que o NG-MVPN gera 122 rotas por MVPN, enquanto EVPN gera 81 rotas por MVPN. Essa correlação e razão fixa do número de rotas por MVPN é explicada pelo cenário implementado, em que todas as MVPNs estão configuradas com a mesma carga. De qualquer forma, é inegável que o protocolo EVPN gera 41 rotas, ou 33,61%, a menos que NG-MVPN para executar a mesma função de rede.

Os valores de número de pacotes BGP também foram coletados no roteador P, pelo mesmo motivo do número de rotas. O número de pacotes BGP foi capturado a partir de um filtro aplicado aos pacotes destinados a CPU do roteador P. Nesse filtro, duas entradas foram adicionadas para capturar pacotes TCP com destino ou origem porta 179 (REKHTER; HARES; LI, 2006). O Código 2 apresenta o filtro implementado conforme as instruções de configuração do sistema operacional do roteador.

O resultado do número de pacotes BGP, por método MVPN e por número de serviços configurados, é mostrado na Tabela 5. Esses valores, visualizados em um diagrama de caixa ou *boxplot*, de acordo com a Figura 18, compara a distribuição do número de pacotes BGP entre os métodos MVPN. Para todos os números de serviços MVPN, o método EVPN obteve consideravelmente menos número de pacotes. Em todos casos a mediana do EVPN está distante e fora da caixa do método NG-MVPN, indicando uma diferença significativa.

Realizando análise parecida com a da métrica de quantidade de rotas, a partir das médias

Código 2 – Filtro para captura do número de pacotes BGP, no roteador P

```
1
2       entry 100 create
3           action accept
4           description "PEMITE_BGP_DST_PORT"
5           match protocol tcp
6               dst-port 179 65535
7           exit
8       exit
9       entry 110 create
10          action accept
11          description "PEMITE_BGP_SRC_PORT"
12          match protocol tcp
13              src-port 179 65535
14          exit
15      exit
```

Tabela 5 – Número de Pacotes BGP (TCP 179)

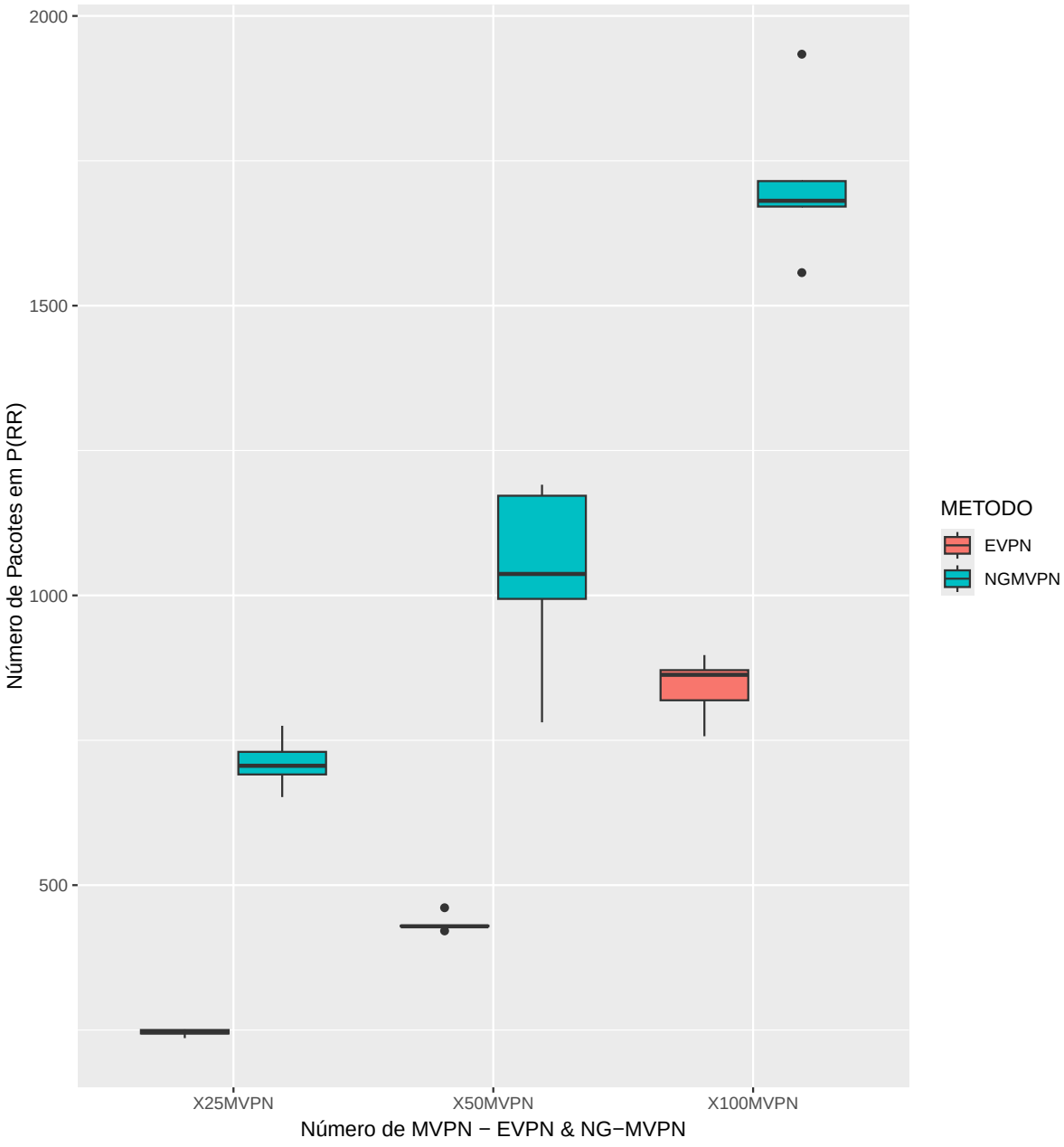
#Serviços MVPN	**Amostras NGMVPN**					
	1	2	3	4	5	**Média**
25	775	691	652	730	706	710,8
50	1172	1191	1037	994	781	1035,0
100	1671	1934	1681	1715	1557	1711,6
#Serviços MVPN	**Amostras EVPN**					
	1	2	3	4	5	**Média**
25	236	244	251	250	246	254,4
50	461	429	421	430	429	434,0
100	871	819	757	897	863	841,4

Fonte: O Autor.

da tabela de número de pacotes BGP (vide Tabela 5), é possível obter a correlação entre o número de pacotes dos métodos e o número de serviços MVPNs. O Código 3 apresenta os comandos para realização e resultados obtidos na análise de correlação, utilizando a linguagem R. Em ambos os métodos a correlação entre o número de pacotes e o número de serviços MVPNs é quase perfeita ($r > 0.999$). Se dividirmos o número de rotas pelo número de serviços para cada linha da tabela, o número de pacotes é diretamente proporcional ao número de MVPNs. Porém quanto mais MVPNs, menor essa razão de pacotes por MVPN. Assim o NG-MVPN requer maior número de pacotes de controle além de atualizações de rotas.

As Tabelas 6, 7 e 8 mostram os resultados dos experimentos de consumo de memória, pelo processo BGP, coletados dos PEs 1, 2 e 3 respectivamente. Foram analisados os dados de memória dos PEs, pois neles é que são instanciados os serviços MVPN, ou seja, tabelas e rotas salvas na memória.

Figura 18 – Boxplot - Número de Pacotes BGP



Fonte: O Autor.

Os valores da tabela são dados em megabytes (MB), e a amplitude do conjunto de todas as amostras é de aproximadamente 16 a 23 MB. A última coluna mostra a média para cada número de serviço MVPN. Para saber se a diferença de consumo de memória entre os métodos é estaticamente significativa, a ferramenta escolhida para tal análise foi o teste de soma de postos de Wilcoxon (Wilcoxon rank sum test) (DALGAARD, 2008).

O Wilcoxon Rank Sum Test é frequentemente descrito como a versão não paramétrica do teste *t* para duas amostras, (FORD, 2017). Isso se justifica pois o teste de Wilcoxon não leva em consideração se a distribuição das amostras é normal. Uma distribuição normal é uma distribuição em que é possível modelar com uma formula matemática, que leva em consideração

Código 3 – Dados e comandos em R para extração da correlação entre número de pacotes de cada método testado

```
1
2  > PACOTES_AVG
3     NSERV NGMVPN  EVPN
4  1     25   710.8 245.4
5  2     50  1035.0 434.0
6  3    100  1711.6 841.4
7  >
8  > (cor.test(formula=~NSERV + NGMVPN, data=PACOTES_AVG))$estimate
9         cor
10 0.9999455
11 > (cor.test(formula=~NSERV + EVPN, data=PACOTES_AVG))$estimate
12        cor
13 0.9998245
14 >
15 > PACOTES_AVG$NGMVPN/PACOTES_AVG$NSERV
16 [1] 28.432 20.700 17.116
17 >
18 > PACOTES_AVG$EVPN/PACOTES_AVG$NSERV
19 [1] 9.816 8.680 8.414
```

parâmetros como média e variância. Wilcoxon, não assume que os dados tenham uma distribuição conhecida, por isso dito como não paramétrico. Segundo (FORD, 2017), para amostras pequenas de distribuição desconhecida, o Wilcoxon Rank Sum é mais adequado. Dessa forma foi realizada a análise dos dados separadamente para quantidade de serviços MVPNs testadas. A hipótese nula do teste de Wilcoxon é a igualdade de medianas das amostras. Portanto, rejeitar a hipótese nula significa que temos evidências de que as medianas das duas amostras diferem.

Tabela 6 – Memória do Processo BGP (PE-1)

PE-1: Alocação de Memória do Processo BGP (MB)						
Núm. Serviços	**NGMVPN**					
Amostras	1	2	3	4	5	Média
25	16,63704	16,64526	16,63696	16,64525	16,63696	16,64029
50	19,0636	19,05341	19,05336	19,04512	19,04515	19,05213
100	22,80443	22,81267	22,81469	22,82285	22,81464	22,81386
Núm. Serviços	**EVPN**					
Amostras	1	2	3	4	5	Média
25	17,01342	17,01341	17,02165	17,01338	17,01339	17,01505
50	18,74382	18,74382	18,74384	18,75206	18,74384	18,74548
100	23,23659	23,23659	23,21747	23,21754	23,21752	23,22514

Fonte: O Autor.

Tabela 7 – Memória do Processo BGP (PE-2)

PE-2: Alocação de Memória do Processo BGP (MB)						
Núm. Serviços	**NGMVPN**					
Amostras	1	2	3	4	5	Média
25	16,64538	16,6371	16,64539	16,6371	16,64541	16,64208
50	19,06358	19,05333	19,0451	19,05334	19,04509	19,05209
100	22,80445	22,8127	22,81275	22,80446	22,81272	22,80942
Núm. Serviços	**EVPN**					
Amostras	1	2	3	4	5	Média
25	17,00387	17,0121	17,0121	17,00387	17,00386	17,00716
50	18,73421	18,74245	18,74243	18,74243	18,73421	18,73915
100	23,23528	23,22704	23,21744	23,21749	23,21754	23,22296

Fonte: O Autor.

Tabela 8 – Memória do Processo BGP (PE-3)

PE-3: Alocação de Memória do Processo BGP (MB)						
Núm. Serviços	**NGMVPN**					
Amostras	1	2	3	4	5	Média
25	16,67816	16,686416	16,678208	16,678176	16,68643	16,681478
50	19,137696	19,127488	19,1192	19,127584	19,11928	19,12625
100	22,944512	22,936288	22,944496	22,936272	22,94446	22,941206
Núm. Serviços	**EVPN**					
Amostras	1	2	3	4	5	Média
25	17,082144	17,082144	17,090368	17,082128	17,082128	17,08378
50	18,81256	18,8208	18,812544	18,8208	18,812544	18,81585
100	23,305344	23,30536	23,21752	23,217632	23,227872	23,25475

Fonte: O Autor.

A Tabela 9 mostra os valores p do teste de Wilcoxon para os dados de consumo de memória do processo BGP nos PEs, para 25, 50 e 100 serviços MVPN. Assumindo o nível de confiança (1-α) de 95% (nível significância α = 0,05) o valor de p < 0,05 em todos os casos. Dessa forma a hipótese nula não é confirmada (para isso p tinha que ser maior que 0,05), e pode-se afirmar que a diferença de consumo de memória entre os dois métodos é estatisticamente significativa, (DALGAARD, 2008; FORD, 2017).

Os gráficos de consumo de memória BGP do PE1, conforme Figura 19, apresentam um comparativo entre os dois métodos para cada número de serviços MVPN. O EVPN é representado pela linha azul e o NG-MVPN pela linha vermelha. Nele, pode-se observar que para 25MVPN e 100MVPN o EVPN aloca em média cerca de 380KB a mais que o NG-MVPN. Porém para 50MVPN, o NG-MVPN é que aloca, em média, cerca de 300KB a mais que o EVPN.

As Tabelas 10, 11 e 12 mostram os resultados de CPU utilizada pelo processo BGP coletados dos PEs 1, 2 e 3, respectivamente. Os dados de CPU também foram analisados nos

Tabela 9 – Valores de p - Teste de Wilcoxon

Resultado do teste Wilcoxon - Memória		
PE	**Número MVPN**	**p-value**
PE1	25MVPN	0,01193
	50MVPN	0,01167
	100MVPN	0,01193
PE2	25MVPN	0,01141
	50MVPN	0,01167
	100MVPN	0,007937
PE3	25MVPN	0,01167
	50MVPN	0,01167
	100MVPN	0,007937

Fonte: O Autor.

PEs, pois neles é que as rotas são processadas. Também foi aplicado o teste de Wilcoxon, separadamente para cada conjunto de serviços MVPN (25, 50 e 100), pelo mesmo motivo da análise do consumo de memória.

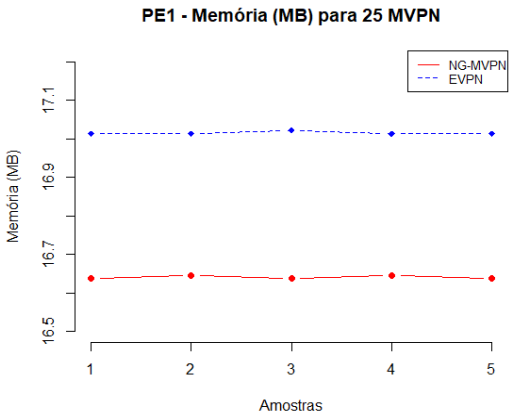
Tabela 10 – CPU do Processo BGP (PE-1)

PE-1: Tempo de uso da CPU do Processo BGP (mSec)						
Núm. Serviços	**NGMVPN**					
Amostras	1	2	3	4	5	Média
25	163,907	151,751	97,84	152,284	178,904	148,9372
50	186,491	156,026	272,345	379,709	168,153	232,5448
100	445,723	685,053	472,858	439,606	511,566	510,9612
Núm. Serviços	**EVPN**					
Amostras	1	2	3	4	5	Média
25	123,591	128,488	118,64	140,294	125,993	127,4012
50	280,06	256,868	273,286	275,774	256,119	268,4214
100	540,457	571,226	439,424	528,302	616,253	539,1324

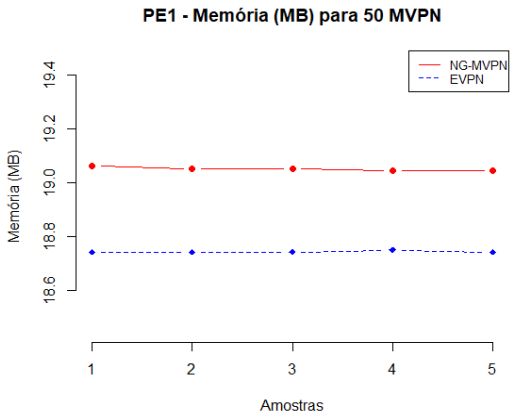
Fonte: O Autor.

A Figura 20 apresenta o gráfico boxplot da variável consumo de CPU do processo BGP do PE1. Para 25MVPN os valores estão mais concentrados entre 100 e 200 ms, com a mediana do EVPN um pouco abaixo de NG-MVPN. Para 50 e 100MVPN, os valores estão um pouco mais dispersos, porém EVPN menos que NG-MVPN. E em ambos os casos a mediana do EVPN se encontra superiaor, entre 60 e 80 ms, do que o NG-MVPN.

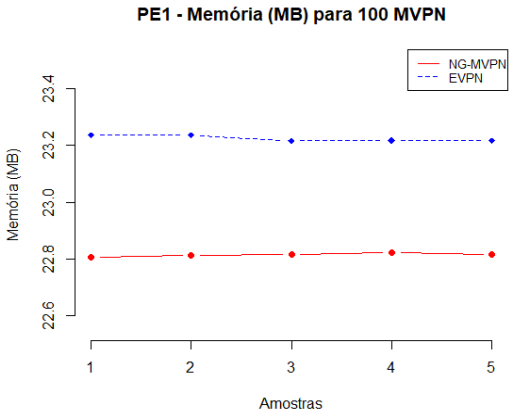
A Tabela 13 mostra os valores p do teste de Wilcoxon para os dados de CPU do processo BGP nos PEs, para 25, 50 e 100 serviços MVPN. Assumindo o nível de confiança (1-α) de 95% (nível significância α = 0,05) o valor de p > 0,05 em todos os casos. Dessa forma a hipótese nula é confirmada, e pode-se afirmar que a diferença de do tempo de uso de CPU entre os dois métodos não é estatisticamente significativa, (DALGAARD, 2008; FORD, 2017).



(a) 25MVPN



(b) 50MVPN



(c) 100MVPN

Figura 19 – Gráfico de linhas - Memória BGP - PE1

Tabela 11 – CPU do Processo BGP (PE-2)

PE-2: Tempo de uso da CPU do Processo BGP (mSec)						
Núm. Serviços	**NGMVPN**					
Amostras	1	2	3	4	5	Média
25	159,291	168,218	130,361	120,401	145,822	144,8186
50	226,679	204,271	264,608	323,537	154,962	234,8114
100	409,831	699,883	501,002	499,813	492,46	520,5978
Núm. Serviços	**EVPN**					
Amostras	1	2	3	4	5	Média
25	151,018	176,437	144,045	120,74	139,963	146,4406
50	363,045	308,262	245,361	205,517	294,688	283,3746
100	870,429	486,589	470,281	612,808	592,529	606,5272

Fonte: O Autor.

Tabela 12 – CPU do Processo BGP (PE-3)

PE-3: Tempo de uso da CPU do Processo BGP (mSec)						
Núm. Serviços	**NGMVPN**					
Amostras	1	2	3	4	5	Média
25	192,698	134,285	132,159	146,651	119,528	145,0642
50	172,247	194,877	302,323	425,13	185,814	256,0782
100	386,873	687,401	415,415	413,613	411,378	462,936
Núm. Serviços	**EVPN**					
Amostras	1	2	3	4	5	Média
25	167,254	169,951	108,12	139,33	169,104	150,7518
50	358,184	216,02	313,602	281,746	241,587	282,2278
100	757,943	631,384	470,373	599,017	4,942	492,7318

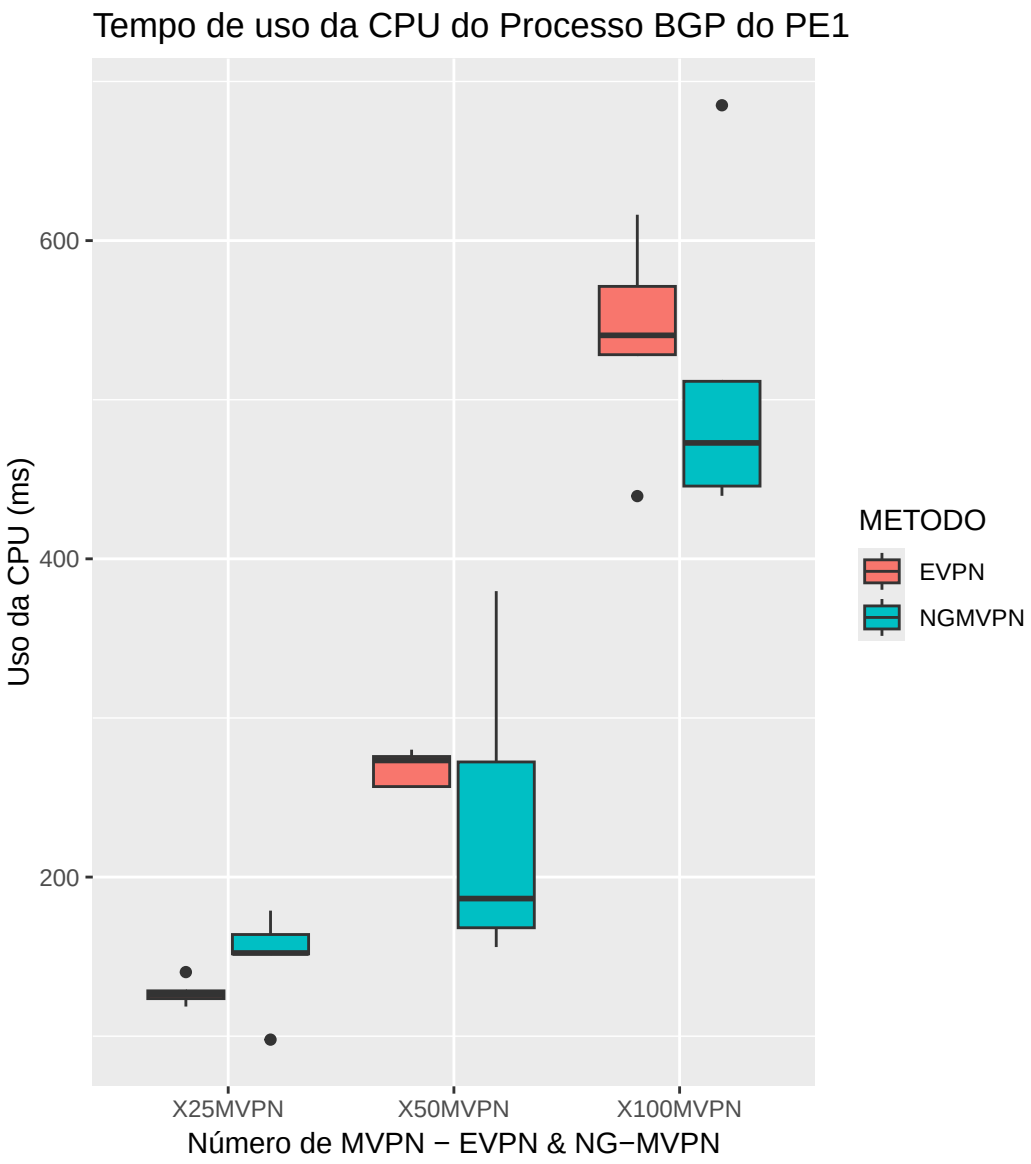
Fonte: O Autor.

Tabela 13 – Valores de p - Teste de Wilcoxon

Resultado do teste Wilcoxon - CPU		
PE	**Número MVPN**	**p-value**
PE1	25MVPN	0,1508
	50MVPN	0,3095
	100MVPN	0,5476
PE2	25MVPN	0,1508
	50MVPN	0,3095
	100MVPN	0,5476
PE3	25MVPN	0,6905
	50MVPN	0,4206
	100MVPN	0,4206

Fonte: O Autor.

Figura 20 – Boxplot - CPU BGP - PE1



Fonte: O Autor.

3.3 CONSIDERAÇÕES DO CAPÍTULO

O Capítulo 3 apresentou toda a metodologia do experimento, que faz uma comparação dos dois métodos de serviço MVPN baseados no protocolo BGP (EVPN e NG-MVPN). O experimento foi realizado em uma rede IP/MPLS emulada pela aplicação *Emulated Virtual Environment - Next Generation* (EVE-NG), que possibilita a virtualização dos roteadores da rede. O roteador utilizado foi o Nokia 7750, que suporta ambas as técnicas MVPN. A topologia de rede IP/MPLS foi formada por quatro roteadores, sendo três PEs (PE1, PE2 e PE3) e um P, que também é refletor de rotas BGP. A carga da rede, ou seja os serviços MVPNs e o fluxos *multicast* IPv4 e IPv6 foram simulados através de configurações nos roteadores.

Neste experimento foi possível monitorar os parâmetros relacionados ao BGP em ambos os métodos MVPN, que impactam diretamente o desempenho do roteador e também da rede. Dessa forma as métricas monitoradas foram: 1) Quantidade de pacotes BGP direcionadas à CPU do roteador; 2) quantidade de rotas BGP trocadas na rede, 3) memória utili-zada pelo processo BGP e 4) utilização da CPU do processo BGP.

Para análise dos dados foi utilizada como ferramenta o R Studio, em que foi possível executar cálculos estatísticos para se obter o máximo de informação dos resultados. Com isso, foi possível verificar que o número de rotas e pacotes BGP foram as métricas que mais apresentaram diferenças entre os dois métodos. O método EVPN troca menos pacotes BGP na rede em comparação com o método NG-MVPN. Em relação a memória e CPU as diferenças foram menores. O método EVPN consome mais memória do roteador para grandes números de serviços MVPN. Enquanto que os resultados de CPU não foram suficientes para apresentarem diferenças significativas, conforme o teste estatístico de Wilcoxon.

Sendo assim, após a experimentação realizada pode-se observar para o resultado de número de rotas BGP entre os métodos, que o protocolo EVPN gerou cerca de 33% menos rotas que o NG-MVN para executar a mesma função de rede. Esse resultado apresentou-se para para qualquer quantidade de serviços MVPN configurado (25, 50 e 100), uma vez que a correlação entre número de serviços e número de rotas é perfeita.

Para o número de pacotes BGP que atingem a CPU do roteador, o resultado da experimentação também aponta que o método EVPN utiliza menos pacotes que o NG-MVPN, confirmado pelo resultado de número de rotas BGP geradas. Nesse caso, o EVPN gerou entre 50% e 65% menos pacotes que o NG-MVPN. Dessa forma, pode-se concluir que o NG-MVPN gera um maior número de mensagens BGP, em relação ao EVPN. Conforme se aumenta o número de serviços MPVN, menor torna-se a diferença entre o número de mensagens geradas pelo método NG-MVPN em relação ao EVPN. Ou seja, o EVPN aumenta o número de mensagens em maior proporção que o NG-MVPN conforme aumenta o número de serviços MVPN.

O resultado da experimentação acerca da memória consumida pelo processo BGP para a configuração dos serviços MVPN mostrou que através do teste estatístico de soma de postos de Wilcoxon, as pequenas diferenças encontradas entre os dois métodos são significativas para

todos os números de serviço MVPN (25, 50 e 100). Contudo, nesse caso, o resultado acerca de qual método consome menos memória depende do número de serviços MVPN testado, uma vez que apenas para 50 MVPNs o EVPN consumiu menos memória que o NG-MVPN (cerca de 310KB). Para 25 e 100 MVPNs o método EVPN consumiu cerca de 380KB a mais que o NG-MVPN.

Em relação ao consumo de CPU, como foi visto que a diferença entre os dois métodos não é estatisticamente significativa, conforme os testes de Wilcoxon, pode-se assumir que para esse cenário de teste, a CPU se apresentou equivalente para os dois métodos. Porém, tanto a metodologia empregada neste experimento, quanto a métrica de CPU, são válidos e podem ser empregados em experimentos futuros com roteadores reais e cargas superiores.

4 CONSIDERAÇÕES FINAIS

O crescimento de tecnologias e aplicações que trafegam dados em redes IP, principalmente das aplicações baseadas em transmissão de vídeo, exigem cada vez mais das redes das provedoras de serviços de telecomunicações. Essa crescente demanda faz com que a rede da provedora necessite sempre de atualizações e alternativas, tanto a nível de hardware quanto software, a fim de aumentar a escalabilidade da rede de forma confiável mantendo a qualidade do serviço para seus clientes.

Neste sentido, este trabalho realizou uma análise de técnicas de transporte do tráfego IP *multicast* dentro de VPNs (MVPN), que são adotadas por redes IP/MPLS de provedoras de serviço de telecomunicações. O foco da análise são técnicas MVPN padronizadas junto ao IETF e implementados por fabricantes de roteadores desse tipo de rede. A mais nova técnica pesquisada e analisada, (LIN et al., 2023), está sendo padronizada dentro do processo da IETF, e ao mesmo tempo já está sendo implementada em roteadores comerciais. Dessa forma, a realização da análise exige a realização de um experimento prático, que nesse caso foi realizado em um ambiente virtualizado utilizando imagens de software de um roteador real (Nokia), a fim de subsidiar a resposta à pergunta de pesquisa.

Assim, essa atividade de análise envolve a aplicação de métodos de análise de desempenho computacional dos protocolos envolvidos no anúncio e troca das rotas para o estabelecimento dos serviços MVPN, entre os dispositivos de roteamento da operadora de telecomunicações. Dessa forma, quanto mais eficiente o protocolo em relação a seu desempenho, maior a escalabilidade da rede. Como nesse trabalho a avaliação se dá sobre o protocolo BGP para serviços MVPN, em termos de escalabilidade, o desempenho está relacionado com o número de serviços MVPN que podem ser ofertados numa rede IP/MPLS pela operadora, sem impacto nos recursos de cada roteador da rede.

Dessa forma foram levantadas três técnicas de MVPN (*Draft-Rosen*, NG-MVPN e EVPN OISM) padronizadas pela IETF e suportadas em roteadores que compõe a rede das provedoras de telecomunicações. Dessas três técnicas, foram experimentadas e comparado o desempenho de duas: NG-MVPN e EVPN OISM, ambas baseadas no protocolo BGP. As métricas de avaliação, dessa forma, são oriundas do protocolo BGP e possíveis de serem extraídas do roteador: rotas BGP, pacotes BGP, memória e CPU do processo BGP. O método *Draft-Rosen* não foi avaliado, pois já existem trabalhos que comprova sua desvantagem em termos de plano de controle da rede. Além disso, esse método não utiliza o protocolo BGP. Por esse motivo que o experimento focou na comparação de desempenho das duas técnicas baseadas no protocolo BGP.

O código fonte do *script* utilizado para obtenção dos resultados, realização da configuração dos serviços MVPN, bem como a configuração da topologia do cenário avaliado, pode ser obtido no endereço web:

<https://drive.google.com/drive/folders/1SWwEvFk4iEsUxrE3uaVk2qi3cCI3KMn6?usp=sharing>

Apesar das pequenas diferenças encontradas em relação ao uso de recursos do roteador (memória e CPU), dependendo da configuração da rede e sua carga, o metódo EVPN pode consumir mais memória que o método NG-MVPN para maiores quantidades de serviços MVPN. Isso pode ser explicado pelo fato da arquitetura do serviço EVPN requerer o provisionamento de domínios de *broadcast* para cada serviço VPN, adicionando tabelas de encaminhamento de camada 2 que são preenchidas por rotas BGP EVPN.

Considerando que, em relação aos valores das métricas avaliadas, quanto menores, melhor, e em função dos resultados apresentados no Capítulo 3, a Tabela 14 mostra que o método EVPN OISM reduziu consideravelmente o número de pacotes BGP pela rede, em comparação ao NG-MVPN, para estabelecimento de serviços MVPN. A redução foi entre 50% e 65% no número de pacotes e 33% na quantidade de rotas a serem processadas pelo roteador. Apesar do método NG-MVPN consumir menos memória do roteador, a redução foi pequena, menor que 2%. Sendo assim, tendo em vista que os valores de CPU não apresentaram diferenças, dentre as técnicas MVPN em redes IP/MPLS, o EVPN OISM apresentou a mais adequada solução para controle de serviços MVPN, melhorando a eficiência no plano de controle da rede.

Tabela 14 – Comparativo EVPN OISM x NG-MVPN

Técnica MVPN	Rotas	Pacotes	Memória	CPU
EVPN OISM	↓ 33%	↓ 50~65%		≈
NG-MVPN			↓ <2%	≈

Fonte: O Autor.

Este trabalho mostrou que a escolha de protocolos de rede pode impactar diretamente o plano de controle e consequentemente na capacidade da rede para oferta de serviços. Dessa forma, protocolos antigos podem ser menos eficientes podendo limitar a escala de uma rede, além de ofertarem menor número de recursos. Por outro lado, a escolha por protocolos mais novos e eficientes pode contribuir na capacidade da rede em atender a grande demanda de novos serviços de telecomunicações. Diante disso, este trabalho conclui que o protocolo EVPN OISM é um grande candidato para evolução na oferta de serviços MVPN em redes IP/MPLS, e se mostrou mais adequado, pois apresentou métricas do plano de controle mais eficientes para entrega do serviço MVPN em IPv4 e IPv6.

Como trabalhos futuros pode-se destacar que novas tecnologias de redes que operam no plano de dados, além da arquitetura MPLS, estão sendo padronizados e já implementadas por provedoras de redes de telecomunicações. Como por exemplo redes baseadas somente em IPv6 (FILSFILS et al., 2021) e novos métodos *multicast* em redes IPv6 (LAN et al., 2023; ZHANG et al., 2024). Dessa forma, cenário equivalentes a esta pesquisa podem ser aplicados considerando essas novas tecnologias de redes.

REFERÊNCIAS

AGGARWAL, Rahul; ROSEN, Eric C. **Multicast in MPLS/BGP IP VPNs**. [S.l.], 2012. (Request for Comments, RFC 6513). Num Pages: 88. Disponível em: <https://datatracker.ietf.org/doc/rfc6513>. Citado 2 vezes nas páginas 18 e 37.

ARNOULD, Aymeric et al. Net 800 GBit/s transmission over 605 km using 99.5 GBaud PDM-64QAM with CMOS digital-to-analog converters. In: . [S.l.: s.n.], 2019. p. 108 (4 pp.)–108 (4 pp.). Citado 2 vezes nas páginas 17 e 21.

ASR, Cisco. **Cisco ASR 9000 Series Aggregation Services Routers**. 2024. Disponível em: <https://www.cisco.com/site/us/en/products/networking/routers/asr-9000-series-aggregation-services-routers/index.html>. Citado na página 52.

AWDUCHE, Daniel O. et al. **RSVP-TE: Extensions to RSVP for LSP Tunnels**. RFC Editor, 2001. RFC 3209. (Request for Comments, 3209). Disponível em: <https://www.rfc-editor.org/info/rfc3209>. Citado na página 24.

BAZAMA, Muneer Ibrahim. **Investigation into Layer 3 Multicast Virtual Private Network Schemes**. Dissertação (Mestrado) — University of Ottawa, Ottawa, Ontario, Canada, 2012. Citado 4 vezes nas páginas 17, 43, 48 e 51.

BRADEN, Robert T. **Requirements for Internet Hosts - Communication Layers**. [S.l.], 1989. (Request for Comments, RFC 1122). Num Pages: 116. Disponível em: <https://datatracker.ietf.org/doc/rfc1122>. Citado na página 22.

CAIN, Bradley et al. **Internet Group Management Protocol, Version 3**. [S.l.], 2002. (Request for Comments, RFC 3376). Num Pages: 53. Disponível em: <https://datatracker.ietf.org/doc/rfc3376>. Citado na página 31.

DALGAARD, Peter. **Introductory Statistics with R**. Second. New York: Springer, 2008. (Statistics and Computing). ISBN 978-0-387-79053-4. Disponível em: <http://dx.doi.org/10.1007/978-0-387-79054-1>. Citado 5 vezes nas páginas 48, 55, 58, 60 e 61.

DESMOUCEAUX, Yoann et al. Reliable multicast with b.i.e.r. **Journal of Communications and Networks**, v. 20, n. 2, p. 182–197, 2018. Citado na página 45.

DRAKE, John et al. **BGP MPLS-Based Ethernet VPN**. [S.l.], 2015. (Request for Comments, RFC 7432). Num Pages: 56. Disponível em: <https://datatracker.ietf.org/doc/rfc7432>. Citado na página 38.

EL-AAWAR, Nasser et al. **Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP)**. RFC Editor, 2006. RFC 4447. (Request for Comments, 4447). Disponível em: <https://www.rfc-editor.org/info/rfc4447>. Citado na página 24.

EVE-NG. **Single Nokia VSR node deployment**. 2024. Disponível em: <https://www.eve-ng.net/index.php/documentation/howtos/nokia-vsr-single-node/>. Citado na página 50.

FENNER, Bill. **Internet Group Management Protocol, Version 2**. [S.l.], 1997. (Request for Comments, RFC 2236). Num Pages: 24. Disponível em: <https://datatracker.ietf.org/doc/rfc2236>. Citado 2 vezes nas páginas 17 e 31.

FENNER, Bill et al. **Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)**. RFC Editor, 2016. RFC 7761. (Request for Comments, 7761). Disponível em: <https://www.rfc-editor.org/info/rfc7761>. Citado 2 vezes nas páginas 17 e 31.

FILSFILS, Clarence et al. **Segment Routing over IPv6 (SRv6) Network Programming**. RFC Editor, 2021. RFC 8986. (Request for Comments, 8986). Disponível em: <https://www.rfc-editor.org/info/rfc8986>. Citado na página 68.

FORD, Clay. web page, **The Wilcoxon Rank Sum Test**. 2017. Disponível em: <https://www.library.virginia.edu/data/articles/the-wilcoxon-rank-sum-test>. Acesso em: 02 jun. 2024. Citado 4 vezes nas páginas 58, 59, 60 e 61.

GREDLER, Hannes; GORALSKI, Walter. **The Complete IS-IS Routing Protocol**. [S.l.]: Springer Publishing Company, Incorporated, 2005. ISBN 1852338229. Citado na página 21.

HUNDLEY, Kent. **Alcatel-Lucent Scalable IP Networks Self-study Guide**. [S.l.]: Wiley, 2009. ISBN 978-1-119-52342-0. Citado 5 vezes nas páginas 15, 16, 21, 23 e 30.

IANA. Request for Comments, **IPv4 Multicast Address Space Registry**. 2024. Disponível em: <https://www.iana.org/assignments/multicast-addresses/multicast-addresses.xhtml>. Acesso em: 02 fev. 2024. Citado na página 16.

JOSEPH, Vinod; MULUGU, Srinivas. **Deploying Next Generation Multicast-enabled Applications**. Morgan Kaufmann, 2024. ISBN 978-0-12-384923-6. Disponível em: <https://doi.org/10.1016/C2010-0-64993-5>. Citado na página 17.

KABACOFF, Robert. **R in Action**. 1st. ed. USA: Manning Publications Co., 2011. ISBN 1935182390. Citado na página 48.

LAN, Shuangfeng et al. Research and verification of new multicast BIER IPv6 technology in IP network. In: **2023 IEEE International Conference on Sensors, Electronics and Computer Engineering (ICSECE)**. [s.n.], 2023. p. 1320–1325. Disponível em: <https://ieeexplore.ieee.org/abstract/document/10263464>. Citado 4 vezes nas páginas 15, 44, 51 e 68.

LEYMANN, Nicolai et al. **Seamless MPLS Architecture**. [S.l.], 2014. Work in Progress. Disponível em: <https://datatracker.ietf.org/doc/draft-ietf-mpls-seamless-mpls/07/>. Citado 2 vezes nas páginas 15 e 52.

LI, Huan et al. "ipv6+" video service solution based on metropolitan area cloud network. In: **2023 International Wireless Communications and Mobile Computing (IWCMC)**. [S.l.: s.n.], 2023. p. 722–727. Citado 2 vezes nas páginas 15 e 45.

LI, Tony et al. **Generic Routing Encapsulation (GRE)**. [S.l.], 2000. (Request for Comments, RFC 2784). Num Pages: 9. Disponível em: <https://datatracker.ietf.org/doc/rfc2784>. Citado na página 32.

LI, Xiangbo et al. Chapter Four - A Survey on Cloud-based Video Streaming Services. In: HURSON, Ali R. (Ed.). **Advances in Computers**. Elsevier, 2021, (Advances in Computers, v. 123). p. 193–244. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0065245821000280>. Citado na página 15.

LIANG, Gong et al. Evaluation of MVPN technologies for China's NGB backbone networks. In: **2014 IEEE International Symposium on Broadband Multimedia Systems and Broadcasting**. [S.l.: s.n.], 2014. p. 1–5. ISSN: 2155-5052. Citado 3 vezes nas páginas 43, 48 e 51.

LILJA, David J. **Measuring Computer Performance: A Practitioner's Guide**. [S.l.]: Cambridge University Press, 2000. Citado na página 48.

LIN, Wen et al. **EVPN Optimized Inter-Subnet Multicast (OISM) Forwarding**. [S.l.], 2023. (Draft, draft-ietf-bess-evpn-irb-mcast-09). Num Pages: 78. Disponível em: <https://datatracker.ietf.org/doc/draft-ietf-bess-evpn-irb-mcast>. Citado 4 vezes nas páginas 18, 39, 40 e 67.

LOUGHEED, Kirk; REKHTER, Jacob. **Border Gateway Protocol (BGP)**. [S.l.], 1989. (Request for Comments, RFC 1105). Num Pages: 17. Disponível em: <https://datatracker.ietf.org/doc/rfc1105>. Citado na página 28.

MERLING, Daniel; LINDNER, Steffen; MENTH, Michael. Comparison of fast-reroute mechanisms for bier-based ip multicast. In: **2020 Seventh International Conference on Software Defined Systems (SDS)**. [S.l.: s.n.], 2020. p. 51–58. Citado na página 45.

MERLING, Daniel; STüBER, Thomas; MENTH, Michael. Efficiency of bier multicast in large networks. **IEEE Transactions on Network and Service Management**, v. 20, n. 4, p. 4013–4027, 2023. Citado na página 44.

METZ, C. Multiprotocol label switching and IP. part 2. multicast virtual private networks. **IEEE Internet Computing**, v. 10, n. 1, p. 76–81, 2006. Citado 3 vezes nas páginas 17, 42 e 43.

MEYER, David; PATEL, Keyur. **BGP-4 Protocol Analysis**. RFC Editor, 2006. RFC 4274. (Request for Comments, 4274). Disponível em: <https://www.rfc-editor.org/info/rfc4274>. Citado 3 vezes nas páginas 17, 29 e 48.

MOY, John. **OSPF Version 2**. [S.l.], 1998. (Request for Comments, RFC 2328). Num Pages: 244. Disponível em: <https://datatracker.ietf.org/doc/rfc2328>. Citado na página 21.

MX, Juniper. **MX Series Universal Routing Platforms**. 2024. Disponível em: <https://www.juniper.net/us/en/products/routers/mx-series.html>. Citado na página 52.

NICHOLES, Martin O.; MUKHERJEE, Biswanath. A survey of security techniques for the border gateway protocol (BGP). **IEEE Communications Surveys & Tutorials**, v. 11, n. 1, p. 52–65, 2009. ISSN 1553-877X. Disponível em: <https://ieeexplore.ieee.org/abstract/document/4796926>. Citado na página 16.

NOKIA. **Evolving to "end-to-end MPLS" architectures Nokia enables seamless, scalable, resilient MPLS networks**. 2016. Disponível em: <https://nokia.sharepoint.com/sites/OneStoreExt/marcoms/OneStoreAssets/Forms/Documents.aspx?id=%2Fsites%2FOneStoreExt%2Fmarcoms%2FOneStoreAssets%2FCID170664%2FNokia%5FEvolving%5FEnd%2Dto%2DEnd%5FMPLS%5FArchitectures%5FWhite%5FPaper%5FEN%2Epdf&parent=%2Fsites%2FOneStoreExt%2Fmarcoms%2FOneStoreAssets%2FCID170664>. Citado na página 15.

NOKIA. **vSIM Installation and Setup Guide**. 2023. Disponível em: <https://documentation.nokia.com/sr/23-3-1/pdf/vSIM_Installation_and_Setup_Guide_23.3.R1.pdf>. Acesso em: 28 jan. 2024. Citado na página 20.

NOKIA. **7750 Service Router**. 2024. Disponível em: <https://www.nokia.com/networks/ip-networks/7750-service-router/>. Citado na página 52.

NOKIA-EVPN-GUIDE. **Layer 2 Services and EVPN Guide**. 2023. Disponível em: <https://documentation.nokia.com/sr/23-3-1/pdf/L2_Services_and_EVPN_Guide_23.3.R1.pdf>. Acesso em: 28 jan. 2024. Citado 2 vezes nas páginas 40 e 41.

NOKIA-UNICAST-GUIDE. **Unicast Routing Protocols Guide**. 2023. Disponível em: <https://documentation.nokia.com/sr/23-3-1/pdf/Unicast_Guide_23.3.R1.pdf>. Acesso em: 28 jan. 2024. Citado 2 vezes nas páginas 29 e 48.

OGUDO, Kingsley A. Analyzing generic routing encapsulation (GRE) and IP security (IPSec) tunneling protocols for secured communication over public networks. In: **2019 International Conference on Advances in Big Data, Computing and Data Communication Systems (icABCD)**. [s.n.], 2019. p. 1–9. Disponível em: <https://ieeexplore.ieee.org/document/8851004>. Citado na página 32.

PAPADIMITRIOU, Dimitri; YASUKAWA, Seisho; AGGARWAL, Rahul. **Extensions to Resource Reservation Protocol - Traffic Engineering (RSVP-TE) for Point-to-Multipoint TE Label Switched Paths (LSPs)**. [S.l.], 2007. (Request for Comments, RFC 4875). Num Pages: 53. Disponível em: <https://datatracker.ietf.org/doc/rfc4875>. Citado na página 32.

PRODANOV, Cleber Cristiano. **Metodologia do trabalho científico: métodos e técnicas da pesquisa e do trabalho acadêmico**. [S.l.]: Universidade Feevale, 2012. ISBN 978-85-7717-158-3. Citado na página 19.

QEMU. **QEMU**. 2024. Disponível em: <https://www.qemu.org/>. Citado 2 vezes nas páginas 20 e 50.

RABADAN, Jorge et al. **IP Prefix Advertisement in Ethernet VPN (EVPN)**. [S.l.], 2021. (Request for Comments, RFC 9136). Num Pages: 31. Citado na página 39.

REKHTER, Yakov et al. **BGP Encodings and Procedures for Multicast in MPLS/BGP IP VPNs**. [S.l.], 2012. (Request for Comments, RFC 6514). Num Pages: 59. Disponível em: <https://datatracker.ietf.org/doc/rfc6514>. Citado 2 vezes nas páginas 18 e 37.

REKHTER, Yakov; HARES, Susan; LI, Tony. **A Border Gateway Protocol 4 (BGP-4)**. [S.l.], 2006. (Request for Comments, RFC 4271). Num Pages: 104. Disponível em: <https://datatracker.ietf.org/doc/rfc4271>. Citado 3 vezes nas páginas 28, 29 e 56.

REKHTER, Yakov; ROSEN, Eric C. **BGP/MPLS IP Virtual Private Networks (VPNs)**. [S.l.], 2006. (Request for Comments, RFC 4364). Num Pages: 47. Disponível em: <https://datatracker.ietf.org/doc/rfc4364>. Citado 3 vezes nas páginas 17, 30 e 31.

RFC791. **Internet Protocol**. [S.l.], 1981. (Request for Comments, RFC 791). Num Pages: 51. Disponível em: <https://datatracker.ietf.org/doc/rfc791>. Citado na página 21.

RIAZ, Hamir. **Multicast in MPLS Based Networks and VPNs**. Dissertação (Master's dissertation) — University of Alberta - CA, 2015. Citado 3 vezes nas páginas 43, 48 e 51.

ROSEN, Eric C.; ANDERSSON, Loa. **Framework for Layer 2 Virtual Private Networks L2VPNs**. [S.l.], 2006. (Request for Comments, RFC 4664). Num Pages: 44. Disponível em: <https://datatracker.ietf.org/doc/rfc4664>. Citado na página 30.

RUSSELL, J.; COHN, R. **Dijkstra's Algorithm**. Book on Demand, 2012. ISBN 9785510951943. Disponível em: <https://books.google.com.br/books?id=LjPtMgEACAAJ>. Citado na página 29.

SAJASSI, Ali et al. **Integrated Routing and Bridging in Ethernet VPN (EVPN)**. [S.l.], 2021. (Request for Comments, RFC 9135). Num Pages: 30. Disponível em: <https://datatracker.ietf.org/doc/rfc9135>. Citado na página 39.

SAJASSI, Ali et al. **Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Proxies for Ethernet VPN (EVPN)**. RFC Editor, 2022. RFC 9251. (Request for Comments, 9251). Disponível em: <https://www.rfc-editor.org/info/rfc9251>. Citado na página 40.

SILVA, C. R. O. **Metodologia do trabalho científico**. Fortaleza: Centro Federal de Educação Tecnológica do Ceará, 2004. Citado 2 vezes nas páginas 19 e 20.

SLLAME, Azeddien M. Performance Evaluation of Multimedia over MPLS VPN and IPSec Networks. In: **2022 IEEE 2nd International Maghreb Meeting of the Conference on Sciences and Techniques of Automatic Control and Computer Engineering (MI-STA)**. [S.l.: s.n.], 2022. p. 32–37. Citado na página 15.

TANENBAUM, Andrew S.; WETHERALL, David. **Computer Networks**. 5. ed. Boston: Prentice Hall, 2011. ISBN 978-0-13-212695-3. Disponível em: <https://www.safaribooksonline.com/library/view/computer-networks-fifth/9780133485936/>. Citado na página 16.

THOMAS, Bob et al. **Label Distribution Protocol Extensions for Point-to-Multipoint and Multipoint-to-Multipoint Label Switched Paths**. [S.l.], 2011. (Request for Comments, RFC 6388). Num Pages: 39. Disponível em: <https://datatracker.ietf.org/doc/rfc6388>. Citado na página 32.

VENKATESWARAN, Arvind et al. INTERWORKING BETWEEN LEGACY AND NEXT-GENERATION MULTICAST VIRTUAL PRIVATE NETWORK (MVPN) TRANSPORTS. **Defensive Publications Series**, 2019. Disponível em: <https://www.tdcommons.org/dpubs_series/2755>. Citado na página 44.

VISWANATHAN, Arun; ROSEN, Eric C.; CALLON, Ross. **Multiprotocol Label Switching Architecture**. RFC Editor, 2001. RFC 3031. (Request for Comments, 3031). Disponível em: <https://www.rfc-editor.org/info/rfc3031>. Citado 2 vezes nas páginas 15 e 23.

VOHRA, Quaizar; CHEN, Enke. **BGP Support for Four-Octet Autonomous System (AS) Number Space**. RFC Editor, 2012. RFC 6793. (Request for Comments, 6793). Disponível em: <https://www.rfc-editor.org/info/rfc6793>. Citado na página 29.

WARNOCK, Glenn. **Alcatel-Lucent Network Routing Specialist II (NRS II) Self-Study Guide: Pre**. [S.l.]: John Wiley & Sons, 2011. Section: 1488 s. ; 24 cm. ISBN 978-0-470-94772-2 0-470-94772-1. Citado 3 vezes nas páginas 21, 27 e 28.

WARNOCK, G.; SHAHEEN, G.; GHAFARY, M. **Alcatel-Lucent Service Routing Architect (SRA) Self-Study Guide: Preparing for the BGP, VPRN and Multicast Exams**. [S.l.]: Wiley, 2015. ISBN 978-1-118-87515-5. Citado 8 vezes nas páginas 15, 16, 17, 30, 34, 35, 36 e 38.

WAZLAWICK, Raul Sidnei. **Metodologia de Pesquisa para Ciência da Computação**. Rio de Janeiro: Elsevier Editora Ltda, 2009. ISBN 978-85-352-3522-7. Citado na página 19.

WIJNANDS, IJsbrand; ROSEN, Eric C.; CAI, Yiqun. **Cisco Systems' Solution for Multicast in BGP/MPLS IP VPNs**. [S.l.], 2010. (Request for Comments, RFC 6037). Num Pages: 25. Disponível em: <https://datatracker.ietf.org/doc/rfc6037>. Citado 2 vezes nas páginas 35 e 43.

WU, Nan et al. A multicast scheduling method based on EVPN-VXLAN extension in data center networks. In: . New York, NY, USA: Association for Computing Machinery, 2024. (CNML '23), p. 332–336. ISBN 9798400716683. Disponível em: <https://doi.org/10.1145/3640912.3640978>. Citado na página 45.

ZHANG, Zheng et al. **Supporting BIER in IPv6 Networks (BIERin6)**. [S.l.], 2024. (Draft, draft-ietf-bier-bierin6-09). Work in Progress. Disponível em: <https://datatracker.ietf.org/doc/draft-ietf-bier-bierin6/09/>. Citado na página 68.