INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO AMAPÁ
Campus Macapá

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO AMAPÁ
CAMPUS MACAPÁ

CURSO SUPERIOR DE TECNOLOGIA EM REDES DE COMPUTADORES

RAILSON ROCHA DA SILVA

IMPLEMENTAÇÃO DE SOLUÇÃO DE TRANSPORTE L2 UTILIZANDO MPLS NA REDE DE UM PROVEDOR DE SERVIÇOS DE INTERNET (ISP)

MACAPÁ - AP
2023

RAILSON ROCHA DA SILVA

IMPLEMENTAÇÃO DE SOLUÇÃO DE TRANSPORTE L2 UTILIZANDO MPLS NA REDE DE UM PROVEDOR DE SERVIÇOS DE INTERNET (ISP)

Trabalho de conclusão de curso apresentado ao curso Superior de Tecnologia em Redes de Computadores do Instituto Federal de Educação, Ciência e Tecnologia do Amapá - IFAP, como requisito avaliativo para obtenção de título de Tecnólogo em Redes de Computadores.

Orientador: Prof. Dr. Klenilmar Lopes Dias

MACAPÁ - AP
2023

Biblioteca Institucional - IFAP
Dados Internacionais de Catalogação na Publicação (CIP)

S672i Silva, Railson Rocha da
Implementação de solução de transporte L2 utilizando MPLS na rede de um Provedor de Serviços de Internet (ISP) / Railson Rocha da Silva - Macapá, 2023.
45 f.

Trabalho de Conclusão de Curso (Graduação) -- Instituto Federal de Educação, Ciência e Tecnologia do Amapá, Campus Macapá, Curso de Tecnologia em Redes de Computadores, 2023.

Orientador: Klenilmar Lopes Dias.

1. MPLS. 2. Transporte L2. 3. Provedor de Serviços de Internet. I. Dias, Klenilmar Lopes, orient. II. Título.

Elaborada pelo Sistema de Geração Automática de Ficha Catalográfica do IFAP
com os dados fornecidos pelo(a) autor(a).

RAILSON ROCHA DA SILVA

IMPLEMENTAÇÃO DE SOLUÇÃO DE TRANSPORTE L2 UTILIZANDO MPLS NA REDE DE UM PROVEDOR DE SERVIÇOS DE INTERNET (ISP)

Trabalho de conclusão de curso apresentado ao curso Superior de Tecnologia em Redes de Computadores do Instituto Federal de Educação, Ciência e Tecnologia do Amapá - IFAP, como requisito avaliativo para obtenção de título de Tecnólogo em Redes de Computadores.

Orientador: Prof. Dr. Klenilmar Lopes Dias

BANCA EXAMINADORA

Prof. Dr. Klenilmar Lopes Dias

Instituto Federal de Educação, Ciência e Tecnologia do Amapá

Prof. Me. Célio do Nascimento Rodrigues

Instituto Federal de Educação, Ciência e Tecnologia do Amapá

Prof. Esp. Eonay Barbosa Gurjão

Instituto Federal de Educação, Ciência e Tecnologia do Amapá

Apresentado em: 30/06/2023

Conceito/Nota: 10

A minha mãe, que sempre se dedicou para garantir uma edução de qualidade para mim. E ao meu orientador Prof. Klenilmar, que me apoiou em cada etapa desse trabalho.

AGRADECIMENTOS

Ao eterno e bom Deus pela oportunidade de ter chegado até aqui, por cada noite de sono mal dormida, por cada espera na parada de ônibus, e pelas forças nos dias em que o tempo foi divido entre trabalho e faculdade.

Aos meus professores que contribuíram significativamente com minha formação, ao meu orientador que me deu total apoio nessa jornada.

A minha família, minha base sólida.

RESUMO

Com a Internet desempenhando um papel primordial em diversos serviços atualmente, a infraestrutura responsável por fornecer conectividade aos usuários finais se tornou tão crítica quanto a estrutura de uma fornecedora de energia elétrica. Esse fato faz com que os Provedores de Serviços de Internet (ISPs) busquem constantemente tornar suas infraestruturas físicas e lógicas o mais disponíveis, escaláveis e resilientes possível, visando garantir a melhor experiência aos usuários. Nesse contexto, a implementação do *Multiprotocol Label Switching* (MPLS) no provedor se tornou uma proposta relevante, pois visa contribuir principalmente para a resiliência e escalabilidade da rede, com impacto direto na qualidade dos serviços de Internet oferecidos. Ao executar a proposta de implementação do MPLS, foram identificados pontos positivos em que essa tecnologia se mostrou eficaz ao assegurar a qualidade dos serviços e a convergência de tráfego, principalmente nos casos em que as rotas principais apresentaram falhas. O MPLS, por meio da criação de caminhos alternativos e da utilização de rótulos para encaminhamento de pacotes, proporciona uma maior flexibilidade e capacidade de roteamento, resultando em maior resiliência e eficiência na entrega dos serviços de Internet. A resiliência da rede é aprimorada pelo MPLS, pois, em situações de falhas em rotas principais, ele permite o redirecionamento do tráfego através de rotas alternativas, evitando interrupções significativas no acesso à Internet. Além disso, sua escalabilidade possibilita o gerenciamento eficiente do crescimento da demanda por conectividade, acompanhando o aumento do número de usuários e do tráfego de dados. Com a adoção do MPLS, os ISPs podem oferecer uma conectividade mais confiável e estável, com menor impacto nas interrupções do serviço. Dessa forma, os provedores podem atender às expectativas dos usuários, garantindo uma experiência de Internet mais satisfatória e sem interrupções indesejadas.

Palavras-chave: MPLS; Provedores de serviços de Internet; convergência.

ABSTRACT

With the Internet playing a fundamental role in various services today, the infrastructure responsible for providing connectivity to end users has become as critical as the structure of an electricity provider. This fact leads Internet Service Providers (ISPs) to constantly strive to make their physical and logical infrastructures as available, scalable, and resilient as possible, aiming to ensure the best user experience. In this context, the implementation of Multiprotocol Label Switching (MPLS) in the provider has become a relevant proposal as it primarily aims to contribute to network resilience and scalability, with a direct impact on the quality of Internet services offered. By executing the MPLS implementation proposal, positive aspects were identified where this technology proved effective in ensuring service quality and traffic convergence, particularly in cases where primary routes failed. MPLS, through the creation of alternate paths and the use of labels for packet forwarding, provides greater flexibility and routing capacity, resulting in enhanced resilience and efficiency in delivering Internet services. Network resilience is enhanced by MPLS as it allows traffic redirection through alternative routes in situations where primary routes fail, avoiding significant interruptions in Internet access. Additionally, its scalability enables efficient management of the growing demand for connectivity, accommodating the increasing number of users and data traffic. Through the adoption of MPLS, ISPs can offer more reliable and stable connectivity with minimal service interruptions. This way, providers can meet user expectations, ensuring a more satisfying Internet experience without unwanted disruptions.

Keywords: MPLS; Internet service Providers; convergence.

LISTA DE FIGURAS

LISTA DE SIGLAS

AAA	Authenticantion Autorization Accounting
AC	Access Circuit
AToM	Any Transport over MPLS
BGP	Border Gateway Protocol
BNG	Broadband Network Gateway
CE	Customer Edge
CGNAT	Carrier Grade NAT
DNS	Domain Name Service
DoD	Downstream on Demand
DSCP	DiffServ Code Point
DU	Downstream Unsolicited
EVE-NG	Emulated Virtual Environment Nex Generation
FEC	Forwarding Equivalence Class
GPON	Gigabit Passive Optical Network
ICMP	Internet Control Message Protocol
IETF	Internet Engineering Task Force
IGP	Interior Gateway Protocol
IP	Internet Protocol
IPoE	Internet Protocol over Ethernet
ISP	Internet Service Provider
L2VPN	Layer 2 Virtual Private Network
LACP	Link Aggregation Control Protocol
LDP	Label Distribution Protocol
LIB	Label Information Base
LSP	Label Switched Path
LSR	Label Switch Router
MPLS	Multiprotocol Label Switching
MTU	Maximum Transmit Unit
OLT	Optical Line Terminal
OSPF	Open Shortest Path First
P	Provider
PE	Provider Edge

PHP	Penultimate Hop Popping
PPP	Point to Point Protocol
PPPoE	Point to Point Protocol over Ethernet
QoS	Quality of Service
RSVP	Resource Reservation Protocol
STP	Spanning Tree Protocol
TE	Traffic Engineering
TLDP	Targeted Label Distribution Protocol
TTL	Time To Live
VC	Virtual Circuit
VLAN	Virtual Local Area Network
VLL	Virtual Leased Line
VPLS	Virtual Private LAN Service
VPN	Virtual Private Network
VPWS	Virtual Private Wire Service
WAN	Wide Area Network

SUMÁRIO

1 INTRODUÇÃO

A Internet e as Tecnologias Digitais têm desempenhado um papel crucial na consolidação de um novo paradigma social, conforme descrito por diversos autores, como a sociedade em rede (CASTELLS, 2003) e a sociedade da aprendizagem (POZO, 2004). Com o intuito de atender a essa demanda, têm sido desenvolvidas diversas tecnologias para garantir e suportar tais serviços. Desde o momento em que o protocolo *Internet Protocol* (IP) (RFC 791, 1981) emergiu como o protocolo dominante na Internet, tem havido uma série de evoluções contínuas, visando satisfazer as exigências das aplicações utilizadas pelos usuários (GHEIN, 2007).

No contexto dessas evoluções, destaca-se a criação do *Multiprotocol Label Switching* (MPLS) (RFC 3031, 2001), uma tecnologia projetada para interconectar redes IP (KUROSE e ROSS, 2014). O MPLS foi introduzido em 1996 pela Ipsilon Networks, uma empresa de tecnologia de rede que foi adquirida pela Nokia em 1997, e foi posteriormente padronizado pelo *Internet Engineering Task Force* (IETF) em 2001, na RFC 3031. O MPLS surgiu como uma solução para simplificar o encaminhamento de pacotes, baseando-se não no cabeçalho do pacote (especificamente no campo endereço IP de destino), mas também no conceito de rótulos (labels) para realizar o encaminhamento (RFC 3032, 2001).

É importante ressaltar que o MPLS desempenhou um papel fundamental no aumento do desempenho dos backbones das grandes operadoras em períodos anteriores. Isso se deve ao fato de que o cabeçalho MPLS, conhecido como *Shim Header*, exige menos processamento por parte dos roteadores. Em comparação com o roteamento IP tradicional, observa-se que o roteador precisa realizar menos operações para atingir o mesmo objetivo de encaminhar pacotes em trânsito ao utilizar o MPLS. Assim, o MPLS é considerado mais eficiente nesse aspecto (FURTADO, 2020).

Atualmente, com o advento de arquiteturas de roteadores mais modernas, que possuem áreas dedicadas em hardware para o processamento de pacotes, a diferença entre a utilização do roteamento IP tradicional e do MPLS não é tão significativa. No entanto, isso não diminui a atratividade do MPLS. Pelo contrário, ao longo dos anos, o MPLS tem ganhado destaque no contexto das redes, especialmente em ambientes de provedores de serviços de Internet ou *Internet Service Provider* (ISP), devido à sua capacidade de oferecer uma variedade de serviços (FURTADO, 2020).

Um dos serviços amplamente utilizados do MPLS em ambientes de ISPs são as *Virtual Private Networks* (VPNs) de camada 2, no qual se destaca o serviço de *Layer 2 Virtual Private Network* (L2VPN). Essas VPNs são frequentemente empregadas para o transporte de tráfego de camada 2 dos assinantes até o *Broadband Network Gateway* (BNG) (FURTADO, 2020).

O BNG é um elemento essencial na infraestrutura de rede de um provedor de serviços de Internet. Ele desempenha um papel central no roteamento e gerenciamento dos assinantes. O BNG é responsável por receber o tráfego proveniente dos assinantes e encaminhá-lo para o destino apropriado. Além do roteamento dos pacotes dos assinantes, o BNG também oferece outros serviços típicos de um provedor, como *Authentication*, *Autorization* e *Accounting* (AAA), gerenciamento de políticas de serviço e *Quality of Service* (QoS). Esses recursos permitem que o provedor forneça diferentes níveis de serviço aos assinantes, priorizando o tráfego e garantindo uma experiência de rede adequada para cada tipo de serviço. Daí se dá a necessidade de levar o tráfego dos assinantes para o devido tratamento no BNG.

No contexto das VPNs de camada 2 baseadas em MPLS, o tráfego de camada 2 dos assinantes é encapsulado em *labels*, e então é transportado através da rede MPLS do provedor até o BNG. Lá, o BNG identifica o destino correto do tráfego e encaminha os pacotes para os próximos passos da comunicação, como o roteamento para a Internet ou outros serviços dentro da rede do provedor.

A tecnologia de camada 2 Ethernet (IEEE 802.3, 1983) é amplamente utilizada como a tecnologia de acesso para os assinantes de Internet banda larga. Portanto, esse é o protocolo frequentemente transportado pela L2VPN, permitindo uma integração eficiente dos serviços oferecidos pelo provedor com a infraestrutura de rede existente.

Em resumo, o BNG desempenha um papel fundamental na recepção, roteamento e gerenciamento do tráfego dos assinantes em um provedor de serviços de Internet. O uso das VPNs de camada 2 baseadas em MPLS permite o transporte eficiente do tráfego de camada 2 até o BNG, garantindo o fornecimento adequado dos serviços aos assinantes e a integração com a infraestrutura de rede do provedor.

A utilização do MPLS em conjunto com o IP expande as possibilidades de transporte de dados. Por meio do uso de *labels*, é possível transportar diversos protocolos sobre uma infraestrutura MPLS de Camada 3, tais como IPv4, IPv6, *Point-to-Point Protocol* (PPP), Ethernet e outras tecnologias de Camada 2. Esse recurso, pelo qual qualquer frame de

Camada 2 pode ser transportado por uma rede MPLS, é conhecido como *Any Transport over* MPLS (AToM). O AToM permite encapsular e transportar frames de Camada 2, como frames Ethernet, através de uma rede MPLS. Essa capacidade é extremamente útil em cenários em que é necessário transportar tráfego de Camada 2 sobre uma rede baseada em MPLS, permitindo a interconexão eficiente de diferentes tipos de tecnologias e protocolos. O AToM permite uma integração eficiente e flexível, facilitando a comunicação e o transporte de dados entre diferentes redes de Camada 2 em uma infraestrutura MPLS de Camada 3.

O MPLS oferece diversas vantagens significativas, como escalabilidade e flexibilidade, priorização de tráfego para uma transmissão de dados mais eficiente, garantia de níveis de serviço, utilização de QoS e engenharia de tráfego (OLIVEIRA et al., 2012). Essas características contribuem para a otimização do desempenho da rede e aprimoram a experiência do usuário ao garantir a entrega de serviços de forma adequada e com qualidade. Através do MPLS, é possível estabelecer políticas de priorização de tráfego, permitindo que os pacotes sejam encaminhados de acordo com suas necessidades e requisitos específicos. Isso resulta em uma melhor utilização dos recursos de rede disponíveis e na melhoria da eficiência geral do sistema. A utilização do MPLS em conjunto com mecanismos como o QoS e a engenharia de tráfego proporciona maior controle e gerenciamento dos fluxos de dados, permitindo uma alocação inteligente dos recursos de rede e uma adaptação dinâmica às demandas em constante mudança. Essas vantagens tornam o MPLS uma tecnologia amplamente adotada em ambientes de provedores de serviços de Internet e redes corporativas, onde a eficiência, a confiabilidade e a garantia de desempenho são essenciais.

Diante das vantagens e dos serviços oferecidos, busca-se a implementação do MPLS na rede do provedor, visando migrar a rede L2 "pura" para uma rede escalável e flexível com MPLS. Essa migração para uma rede MPLS oferece benefícios significativos, como melhor escalabilidade, flexibilidade e capacidade de priorização de tráfego, resultando em uma experiência aprimorada para os usuários e um ambiente de rede mais eficiente para o provedor.

Este trabalho propõe analisar e avaliar a implementação do MPLS em uma rede de provedor de serviços de Internet, com o objetivo de investigar sua capacidade de garantir a escalabilidade, eficiência de encaminhamento e suportar múltiplos serviços, como roteamento unicast, roteamento multicast, VPNs, Engenharia de Tráfego e QoS.

O mesmo está organizado em cinco capítulos. No primeiro capítulo, são abordados o tema, a justificativa, e os objetivos. No segundo capítulo são apresentados temas relevantes para o desenvolvimento do trabalho, fazendo referência toda parte conceitual que envolve o

MPLS, além de uma explanação básica sobre o funcionamento do serviço L2VPN. No terceiro capítulo, são descritos os aspectos da rede do provedor antes da implementação do MPLS, bem como a proposta de implementação, sendo usado um emulador para simular a implementação. Em seguinda é apresentado a execução da proposta. Por fim, o quinto capítulo consiste nas considerações finais, seguidas das referências bibliográficas.

1.1 Justificativa

Em uma arquitetura típica de provedores de acesso, o transporte do tráfego dos clientes até o equipamento de autenticação e concentração de sessão, conhecido como BNG, é um desafio. Geralmente, o BNG está localizado distante do cliente, exigindo o transporte do tráfego L2 Ethernet dos clientes que vem da *Optical Network Unit* (ONU) e chegam até a *Optical Line Terminal* (OLT), que são componentes típicos da rede *Gigabit Passive Optical Network* (GPON), passando por vários equipamentos do provedor, como roteadores e switches, até chegar ao BNG.

No contexto em que a tecnologia Ethernet (IEEE 802.3, 1983) é predominante para fornecer acesso aos clientes, a solução comumente adotada é o uso de *Virtual Local Area Networks* (VLAN). Porém, é importante observar os fundamentos de L2, que estabelecem que cada VLAN não deve ter mais de dois caminhos para o mesmo destino para evitar loops de camada 2.

Nesse cenário, os protocolos da família *Spanning Tree Protocol* (STP) são comumente utilizados para permitir caminhos redundantes sem gerar loops. No entanto, esses protocolos apresentam desafios significativos em termos de escalabilidade quando aplicados em ambientes de provedores de serviços de Internet. Como mencionado anteriormente, o protocolo STP não escala adequadamente e não foi projetado para operar em ambientes de rede *Wide Area Network* (WAN) (IEEE 802.1D, 2009).

Ao analisar o ambiente do provedor que utiliza a tecnologia de VLANs nativamente para o transporte dos clientes até o BNG, identificou-se a necessidade de configurar cada equipamento no caminho com a VLAN correspondente. Além disso, foi identificada uma má configuração do protocolo STP, representando um risco constante de loop, mesmo que não houvesse caminhos redundantes dentro da rede do provedor até então. Essa configuração limita a escalabilidade e inviabiliza a implementação de redundância na rede do provedor.

Diante desse contexto, a implementação do MPLS na rede do provedor, especialmente o serviço de L2VPN usando AToM, torna-se essencial. Estudos como Furtado (2020) e Lacoste e Edgeworth (2020) destacam o MPLS como uma solução altamente eficiente e flexível, desempenhando um papel crucial no atendimento à crescente demanda por serviços de aplicativos e usuários no ambiente dos ISPs.

1.2 Objetivos

1.2.1 Objetivo Geral

Fazer a simulação da implementação do MPLS em ambiente virtualizado e controlado, utilizando o software *Emulated Virtual Environment – Next Generation* (EVE-NG) , para identificar as consequências das configurações e dessa forma evitar paralizações no ambiente do provedor que fujam do controle.

Após os resultados do ambiente simulado, será possível implementar o MPLS na rede do provedor em produção, para realizar o transporte dos clientes até o BNG, utilizando o serviço de L2VPN (AToM) transportando o protocolo *Ethernet*.

1.2.2 Objetivos Específicos

- Realizar simulações em laboratório para validar a implementação do serviço de MPLS, tendo como base a topologia atual da rede do provedor.
- Configurar o protocolo de roteamento *Open Shortest Path First* (OSPF) e o MPLS no ambiente de produção do provedor, garantindo a correta comunicação entre os equipamentos.
- Configurar e implementar o serviço de L2VPN no ambiente de produção do provedor, estabelecendo a conectividade eficiente entre os clientes e o BNG.
- Validar o serviço de L2VPN, realizando testes de conectividade e avaliando seu desempenho.

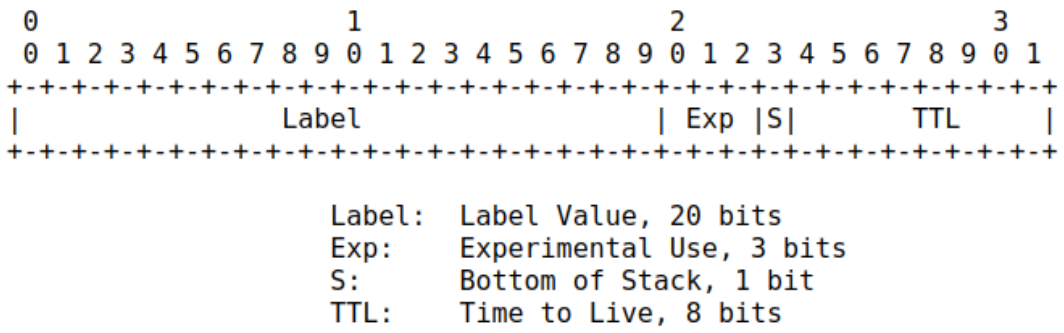
2 BACKGROUND CONCEITUAL

Neste capítulo, serão feitas apresentações de trabalhos que abordam conceitos mais aprofundados sobre o MPLS, bem como o transporte da tecnologia Ethernet pelo serviço de L2VPN, além de cenários de configuração explorados por outros estudos, incluindo a simulação em ambientes virtualizados.

2.1 Conceitos Clássicos

Assim como qualquer outro protocolo, o MPLS possui seu próprio cabeçalho com campos específicos. A figura abaixo ilustra os campos que compõem o cabeçalho MPLS, conhecido como *shim header*:

Figura 1 - *Shim Header* MPLS.



Fonte: RFC 3032 (2001).

O campo "*label*" possui 20 bits e desempenha um papel essencial na identificação da etiqueta atribuída ao pacote. É importante destacar que os valores utilizáveis começam a partir do valor 16, enquanto os valores anteriores são reservados para outros fins, porém isso pode variar de fabricante para fabricante. Por exemplo, a label com o valor 3 é denominada "*Implicit Null*" e é atribuída pelo *egress Label Switching Router* (LSR), que seria o equipamento de saída da rede MPLS. Essa label indica que o penúltimo salto do *Label Switched Path* (LSP) deve remover a label e encaminhar o pacote. Esse processo específico é conhecido como "*Penultimate Hop Popping*" (PHP) (RFC 3032, 2001). Através do PHP, o *egress* LSR é responsável por eliminar a *label* e direcionar o pacote adequadamente.

O campo “*Exp*” é utilizado para fornecer QoS. Já o campo "S" indica se o *label* em análise pelo LSR é o último, uma vez que os pacotes frequentemente possuem vários labels. Se o valor do campo "S" for igual a "0", significa que o label não é o último do pacote. Caso seja igual a "1", indica que o label é o último do pacote. Além disso, o campo *Time to Live* (TTL) desempenha uma função semelhante àquela presente nos pacotes IP, sendo utilizado para controlar loops (RFC 3032, 2001).

A label, que é o campo mais significativo no *shim header*, possui um tamanho variável e é utilizada para identificar uma *Forward Equivalence Class* (FEC). Uma FEC representa um grupo ou fluxo de pacotes que são encaminhados pelo mesmo caminho e tratados da mesma forma. Todos os pacotes pertencentes à mesma FEC possuem a mesma label.

No entanto, é importante destacar que nem todos os pacotes com a mesma label pertencem necessariamente à mesma FEC. Isso ocorre porque seus valores no campo “*Exp*” podem ser diferentes, o que implica em tratamentos de encaminhamento distintos. Portanto, o valor do campo “*Exp*” tem influência no encaminhamento dos pacotes, mesmo que compartilhem a mesma label. O roteador responsável por decidir quais pacotes pertencem a cada FEC é o ingress LSR. Alguns exemplos de FEC são:

- Pacotes com o endereço IP de destino correspondendo a um determinado prefixo.
- Pacotes multicast pertencentes a um certo grupo.
- Pacotes com o mesmo tratamento de encaminhamento, baseado na precedência ou no *DiffServ Code Point* (DSCP).
- Frames de camada 2 transportados através da rede MPLS sendo recebidos em um *Virtual Circuit* (VC) ou (sub)interface no *ingress* LSR e transmitidos para um VC ou (sub)interface no egress LSR (GHEIN, 2007).

Esses exemplos ilustram diferentes critérios pelos quais os pacotes podem ser agrupados em FECs, permitindo um tratamento específico de encaminhamento com base em suas características e requisitos de rede.

De forma resumida, o processo de alocação e distribuição de *labels* no MPLS é realizado pelos LSRs em uma rede. Cada LSR aloca *labels* com base nos prefixos do *Interior Gateway Protocol* (IGP) de sua tabela de roteamento. Esses prefixos podem ser gerados ou recebidos por protocolos como OSPF, rotas estáticas ou diretamente conectadas, e a cada um é atribuída uma *label* específica.

Após esse procedimento, cada LSR distribui suas *labels* alocadas locamente para seus vizinhos. Isso pode ser feito de duas maneiras: no modo *Downstream Unsolicited* (DU) o LSR distribui as labels sem a necessidade de recebimento de uma mensagem de solicitação de

labels do vizinho. No modo *Downstream on Demand* (DoD), o LSR só irá distribuir as *labels* após o recebimento de uma mensagem requisitando as *lebels* (HUAWEI, 2023).

Cada roteador recebe as *labels* e as armazena em uma tabela específica, como a *Label Information Base* (LIB) em roteadores Cisco (CISCO, 2021). Em seguida, cada roteador verifica em sua tabela de roteamento a melhor rota para cada destino mencionado em uma label recebida. Se houver várias labels recebidas de diferentes vizinhos, o MPLS no roteador escolhe o label anunciado por um vizinho que seja, na tabela de roteamento, o próximo salto (next hop) para o encaminhamento do tráfego para aquele destino/rota específica.

Para realizar a distribuição de labels, é utilizado um protocolo específico, sendo o *Label Distribution Protocol* (LDP) o mais comum. Outra opção é o *Resource Reservation Protocol* (RSVP), que é frequentemente utilizado em conjunto com o *Traffic Engineering* (TE).

Ao implementar o MPLS em uma rede de provedores, existem termos específicos para designar a função de cada equipamento que executa o protocolo. Em geral, o equipamento que roda o MPLS é chamado de LSR. Existem três tipos de LSRs em uma rede MPLS:

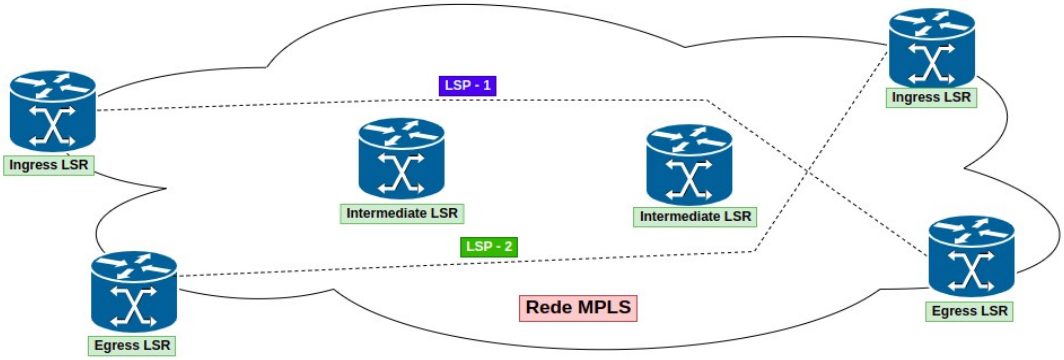
- *Ingress* LSRs: Esses equipamentos recebem pacotes sem labels, inserem uma label na frente dos pacotes, e os encaminham pelo link de dados.
- *Egress* LSRs: Esses equipamentos recebem pacotes com labels, removem as labels e encaminham os pacotes pelo link de dados. Os ingress e egress LSRs são LSRs de borda.
- *Intermediate* LSRs: Esses equipamentos recebem pacotes com labels, realizam operações sobre eles e encaminham os pacotes para o link correto

Há também o conceito de LSP, que consiste em uma sequência de LSRs que encaminham pacotes com labels através da rede MPLS. O primeiro LSR do LSP é o ingress LSR, responsável por receber o pacote sem label e atribuir a primeira label. O último LSR do LSP é o egress LSR, que remove a última label e encaminha o pacote para seu destino final. Todos os demais LSRs entre o ingress e o egress são intermediate LSRs (GHEIN, 2007).

É importante ressaltar que um LSP é unidirecional, o que significa que o tráfego entre o ingress e o egress pode seguir caminhos diferentes dentro da rede MPLS. Isso ocorre devido à natureza da comutação de labels, que permite que diferentes pacotes compartilhem o mesma LSP, mas sejam roteados de forma independente. Portanto, um LSP é uma rota predefinida e estabelecida na rede MPLS, composta por uma sequência de LSRs que trabalham em conjunto para encaminhar pacotes com labels ao longo do caminho determinado.

A figura abaixo exemplifica os conceitos citados anteriormente:

Figura 2 - Arquitetura MPLS típica.



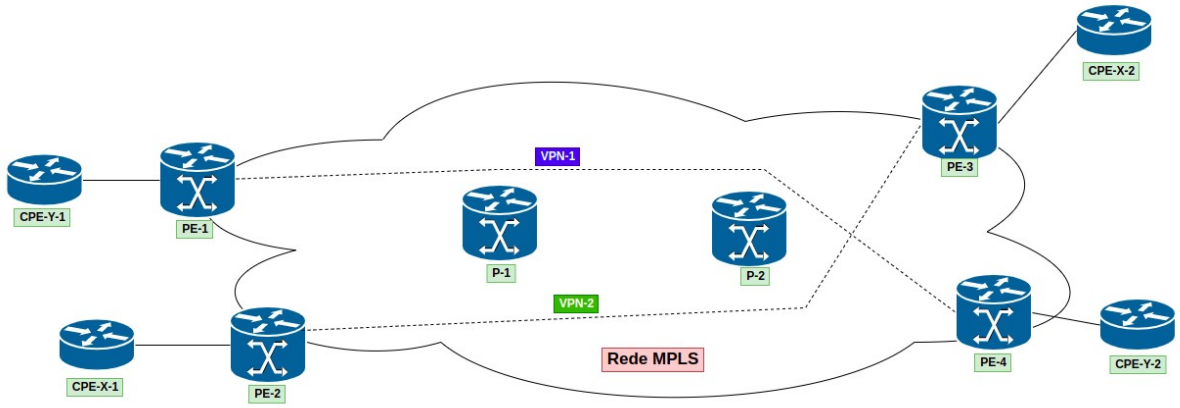
Fonte: Elaborado pelo autor (2023).

Já quando o MPLS é abordado no contexto de VPNs, como é o caso do serviço L2VPN, as nomenclaturas dos equipamentos são diferentes. Nesses casos, temos:

- *Costumer Edge* (CE) ou *Costumer Provider Edge* (CPE): É o equipamento do cliente que faz conexão com o equipamento do provedor.
- *Provider Edge* (PE): É o equipamento do provedor que faz conexão com o equipamento do cliente. Ele atua como a interface entre a rede do provedor e a rede do cliente.
- *Provider* (P): É o equipamento do provedor que possui conexões apenas com outros equipamentos dentro da infraestrutura do provedor. Ele não possui conexões diretas com os clientes e é responsável pelo tráfego de encaminhamento entre os PEs (OLIVEIRA *et al*, 2012).

A figura abaixo exemplifica os conceitos mencionados anteriormente:

Figura 3 - Arquitetura MPLS VPN.



Fonte: Elaborado pelo autor (2023).

Nessa topologia, o CPE representa o equipamento do cliente, o PE é o equipamento do provedor que se conecta ao CE e o P é o equipamento do provedor que faz o trânsito do tráfego entre os PEs. Essa arquitetura é comumente utilizada em VPNs baseadas em MPLS para fornecer serviços L2VPN, além de outros serviços também.

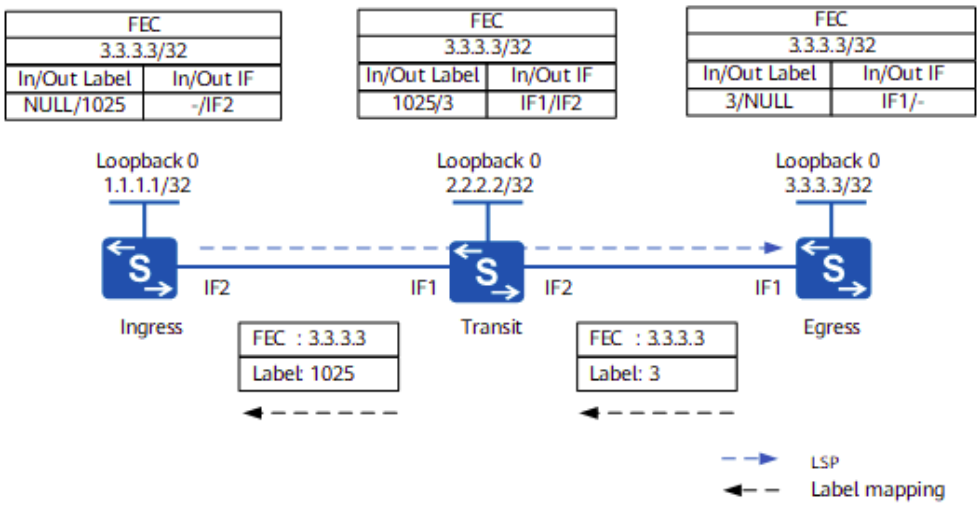
Outra abordagem importante é compreender as operações executadas pelos LSRs no nível de *Data Plane* (Plano de Dados) dos equipamentos quando um determinado pacote chega. As operações realizadas pelos LSRs variam de acordo com sua função, seja como ingress LSR, intermediate LSR ou egress LSR. Existem três operações principais executadas pelos roteadores MPLS:

1. Operação de PUSH: Essa operação é realizada por um ingress LSR, ou seja, quando um pacote chega sem label, o ingress LSR adiciona uma ou mais labels ao pacote, realizando o PUSH das labels.
2. Operação de SWAP: Essa operação é frequentemente executada por um intermediate LSR. Quando um pacote chega com labels, o intermediate LSR realiza a troca da label de topo (a primeira label no caso de um stack de labels) por outra label, substituindo-a. Essa operação é conhecida como SWAP.
3. Operação de POP: Essa operação é geralmente realizada por um egress LSR. Quando um pacote chega com labels, o egress LSR remove a label. Em alguns casos, um intermediate LSR também pode executar a operação de POP na label de topo, conhecida como PHP (GHEIN, 2007).

Essas operações são essenciais para o encaminhamento de pacotes no MPLS, permitindo que os LSRs adicionem, troquem ou removam as labels de acordo com as necessidades da rede e os requisitos de roteamento.

Nesse trabalho, o LDP será o protocolo utilizado para a distribuição de labels, tanto nas referências técnicas quanto nas práticas. O processo de execução do LDP começa com o mapeamento das labels para as FECs, o qual é realizado localmente. Em seguida, essas labels são distribuídas para os vizinhos LDP. Abaixo está uma figura que ilustra o processo:

Figura 4 - Execução do LDP.



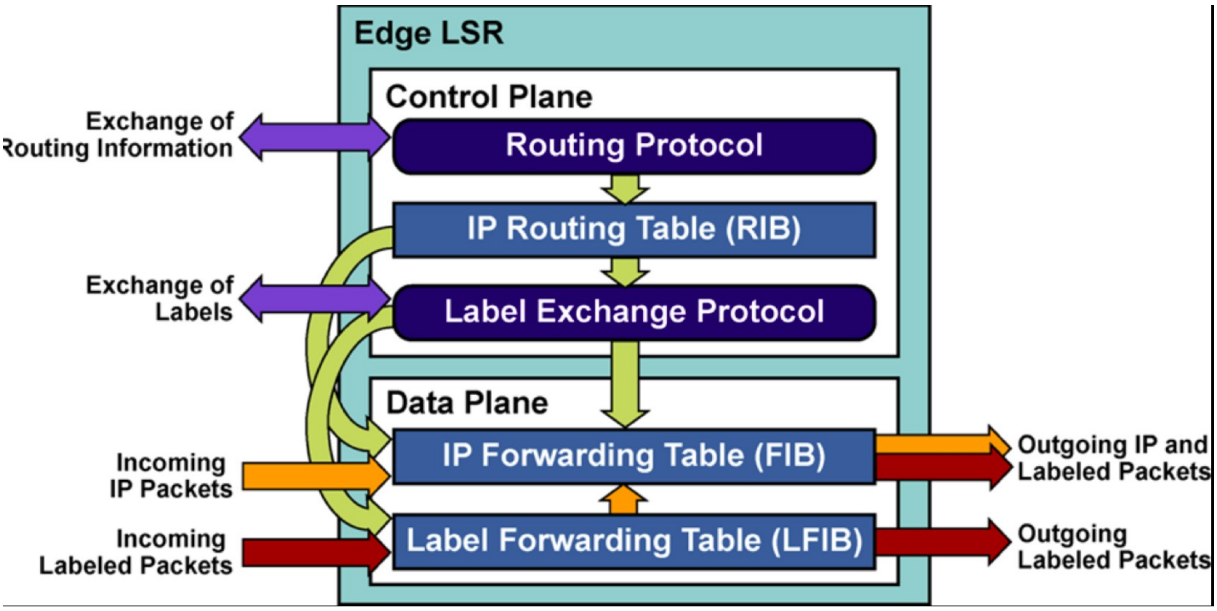
Fonte: Huawei (2023).

No caso da figura acima, é feita a distribuição da label correspondente à FEC 3.3.3.3/32, que representa o endereço IP de loopback (interface lógica) do LSR e*gress*. O *egress* gera a label 3 para essa FEC, onde o valor 3 significa *Implicit Null*, relacionado ao processo de PHP. O LSR *transit* recebe a label, a armazena em sua LIB e aloca uma nova label local, nesse caso, a 1025, e a envia para o LSR Ingress. O LSR Ingress, por sua vez, armazena a label em sua LIB, associando-a à FEC 3.3.3.3. Assim, quando um pacote chega ao LSR Ingress com destino a 3.3.3.3, ele realiza o PUSH da label 1025 no pacote e o encaminha para o LSR Transit. No LSR *transit*, ocorre o SWAP da label 1025 para a label 3 e, em seguida, o pacote é encaminhado para o LSR e*gress*.

É importante ressaltar o comportamento do MPLS e do LDP nas arquiteturas de roteadores atuais, levando em consideração os conceitos de *Control Plane* (Plano de Controle) e Plano de Dados. O LDP, nesse caso, está inserido no plano de controle, pois é o protocolo responsável por associar os prefixos IGP (FEC) às labels correspondentes, realizar a

distribuição das labels e estabelecer estados de vizinhança com os vizinhos LDP. Além disso, ao receber labels dos vizinhos, o LSR as armazena em sua LIB. Por outro lado, no plano de dados, temos a Label Forwarding Information Base, que é uma representação simplificada da LIB, contendo as labels e as ações correspondentes, como PUSH, SWAP ou POP.

Figura 5: Visão das estruturas do MPLS dentro do roteador.



Fonte: Brasil Peering Forum (2020).

2.2 Solução de Transporte do Ethernet

A solução AToM para o transporte do Ethernet sobre o MPLS é estritamente ponto-a-ponto, também conhecida popularmente como *Virtual Private Wired Service* (VPWS) sendo considerado um serviço do tipo L2VPN. Isso significa que todos os frames Ethernet são transportados de um ingress PE para um egress PE, não permitindo conexões multiponto. Para o transporte Ethernet multiponto, existe outra solução chamada *Virtual Private LAN Service* (VPLS), no entanto, ela está fora do escopo deste trabalho.

No caso de um *Access Circuit* (AC) ou Circuito de Acesso em uma VPWS, ele pode ser uma porta Ethernet ou uma VLAN. Quando o AC é uma VLAN, o PE verifica o ID da VLAN nos frames recebidos e, caso corresponda à configuração, o frame é transportado pela VPWS. No caso de um AC com porta Ethernet, o PE transporta os frames de forma transparente, sem realizar qualquer inspeção de VLAN (GHEIN, 2007).

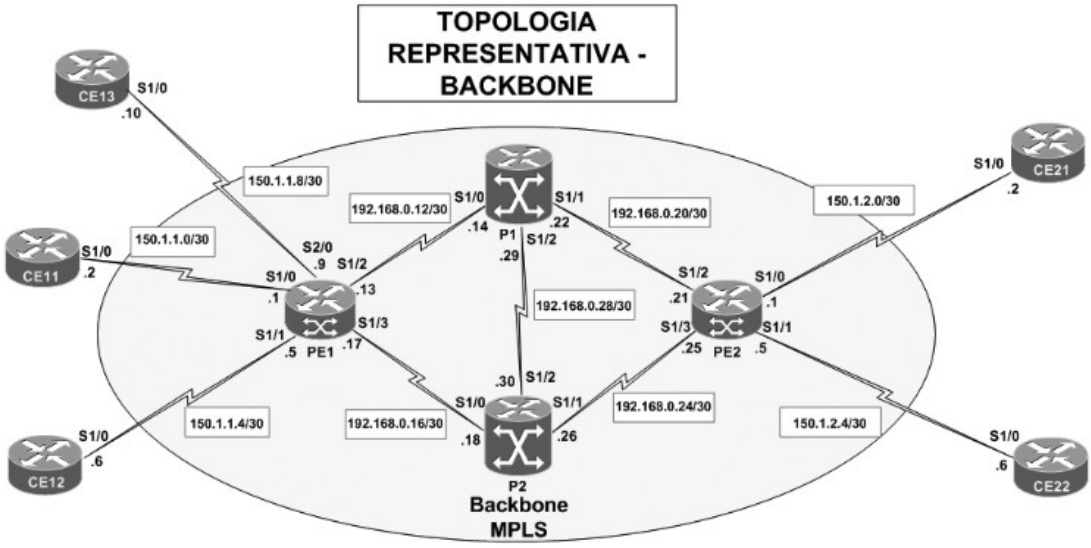
2.3 Emuladores de Redes

Emuladores de rede são amplamente utilizados para testar e simular cenários de rede em ambientes virtualizados, evitando a necessidade de realizar esses testes diretamente no ambiente de produção. Esses cenários podem envolver migrações ou mudanças na infraestrutura de rede em produção, permitindo que os administradores de rede avaliem o impacto das alterações sem afetar o funcionamento real da rede.

Ao contrário dos simuladores, que geralmente reproduzem apenas algumas características dos dispositivos de rede reais, os emuladores são softwares desenvolvidos para traduzir instruções de um processador específico para o processador em que estão sendo executados. Eles são capazes de emular funções de circuitos integrados e arquiteturas de hardware de sistemas reais. Esses softwares têm a capacidade de transformar um computador comum em um dispositivo de rede virtual, replicando virtualmente todas as funcionalidades dos dispositivos reais, como roteadores, switches e firewalls (FILIPPETTI, 2008).

No trabalho de (OLIVEIRA, 2012), é descrita a configuração de uma solução MPLS L2VPN VPWS utilizando o emulador GNS3. O GNS3 é uma plataforma de emulação de rede amplamente utilizada que permite criar ambientes de laboratório virtuais. Ele utiliza imagens de equipamentos de rede Cisco para emular o comportamento desses dispositivos. Essa abordagem permite que os pesquisadores e profissionais de redes realizem testes e experimentos em um ambiente controlado, replicando de forma precisa as configurações e comportamentos esperados na rede real. Isso é especialmente útil para estudar, aprender e validar configurações de rede complexas sem impactar o ambiente de produção.

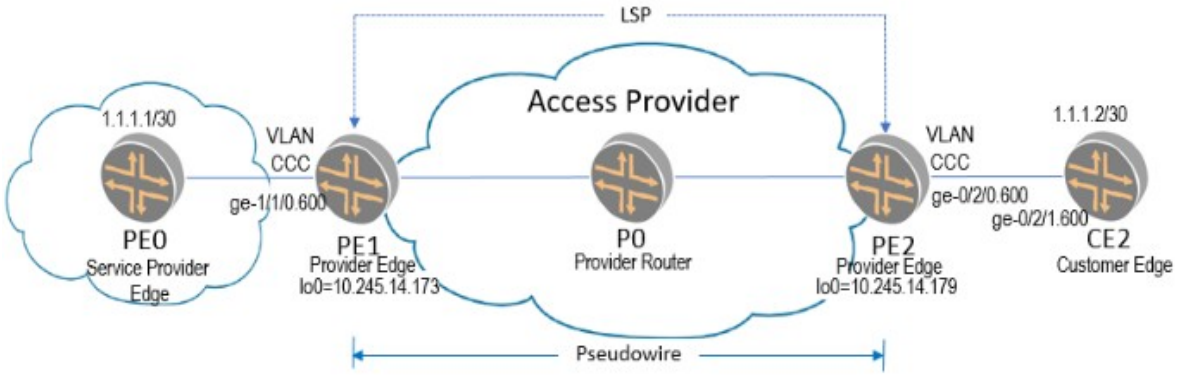
Figura 6: Topologia laboratório VPWS com Cisco usando GNS3.



Fonte: Oliveria *et al (*2012).

Já no trabalho de (JäRVI , 2020), é apresentada a configuração da tecnologia VPWS utilizando equipamentos da Juniper. No entanto, o autor não fornece informações detalhadas sobre a plataforma de emulação ou se utilizou equipamentos físicos para realizar o laboratório.

Figura 7: Topologia laboratório VPWS com Junniper.



Fonte: Järvi (2020).

Neste trabalho, será utilizado o emulador EVE-NG (EVE-NG, 2023), uma poderosa plataforma de emulação de redes que oferece suporte para emular equipamentos de diversos fabricantes. O EVE-NG é amplamente utilizado para criar ambientes de laboratório virtualizados, permitindo aos pesquisadores e profissionais de redes testar configurações e cenários sem a necessidade de usar equipamentos físicos reais.

Com o EVE-NG, é possível emular uma ampla variedade de equipamentos de rede, incluindo roteadores, switches e firewalls, de diferentes fabricantes. No contexto específico deste trabalho, a topologia do provedor será emulada com equipamentos da Huawei e Mikrotik. Essa abordagem permite simular e testar a configuração e o funcionamento de redes usando os equipamentos específicos utilizados no provedor em questão.

A utilização do emulador EVE-NG oferece diversas vantagens, como a flexibilidade de criar e modificar topologias de rede de forma rápida e fácil, a possibilidade de executar múltiplas instâncias dos equipamentos emulados simultaneamente e a capacidade de realizar experimentos e testes sem impactar a rede de produção. Além disso, esse emulador fornece recursos avançados de monitoramento e análise, permitindo uma avaliação abrangente do desempenho e comportamento da rede emulada.

Dessa forma, o uso do emulador EVE-NG neste trabalho oferece uma solução eficiente e escalável para a criação do ambiente de laboratório. Isso proporcionará a oportunidade de realizar experimentos e testes com base nesses equipamentos, contribuindo para a compreensão e análise da tecnologia MPLS em um contexto mais próximo do ambiente real.

3 METODOLOGIA

Com base nos objetivos da pesquisa, será adotada a metodologia de pesquisa exploratória. Conforme descrito por Gil (2008), essa abordagem tem como finalidade proporcionar uma maior familiaridade com o problema investigado. Dessa forma, serão realizadas sondagens em diversas fontes, como livros físicos e digitais, bem como consultas em sites especializados. O objetivo é compreender quais são os principais entraves relacionados aos serviços oferecidos para assinantes de provedores de serviços de Internet sem a utilização da tecnologia MPLS, como também toda a parte conceitual envolvendo o protocolo.

Em relação aos métodos, será adotada a pesquisa-ação com a finalidade de implementar a tecnologia MPLS na rede do provedor de serviço de Internet. Como procedimentos iniciais, serão realizadas o diagrama da rede do provedor, evidenciando as principais interconexões entre os equipamentos de *backbone*, além disso será feito o mapeamento lógico, para compreender os fluxos de tráfego atuais.

Após a compreensão de como a rede do ISP está atualmente, será possível simular a implementação do MPLS em um ambiente virtualizado, utilizando o software EVE-NG. Essa ferramenta é utilizada para emular equipamentos de diversos fabricantes, inclusive Huawei, que é o fabricante principal que o provedor utiliza. Após a simulação em ambiente virtualizado, será realizada a implementação do MPLS na rede do provedor.

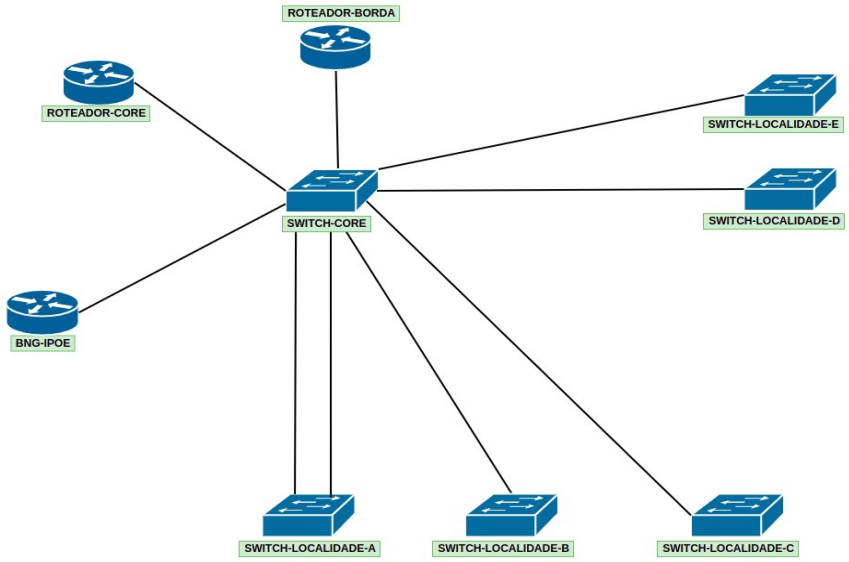
Como última tarefa da pesquisa-ação será feito um monitoramento dos primeiros clientes que forem migrados para o MPLS, para validação completa do serviço.

4 IMPLEMENTAÇÃO

4.1 Aspectos Lógicos da Rede do Provedor

Nesta parte do trabalho, será descrito como a rede do provedor está atualmente, no que diz respeito à parte lógica. A figura representada abaixo ajudará a compreender a descrição lógica que será feita, destacando apenas a parte da rede necessária para a compreensão deste trabalho:

Figura 8: Topologia da rede do provedor.



Fonte: Elaborado pelo autor (2023).

Temos o "ROTEADOR-BORDA", responsável por receber os links das operadoras e encaminhar o tráfego do provedor para a Internet. Além disso, temos o "BNG-IPOE", que é encarregado de autenticar os usuários. O *Internet Protocol over Ethernet* (IPoE) é uma das formas de autenticação utilizadas para usuários de banda larga, sendo outra opção o *Point-to-Point over Ethernet* (PPPoE). Neste provedor em particular, o IPoE é utilizado para essa finalidade.

Com relação aos switches, temos o "SWITCH-CORE" responsável pela interconexão com todos os equipamentos, enquanto os outros switches marcados como "SWITCH-LOCALIDADE-X" são responsáveis por receber o tráfego das OLTs em cada localidade e

encaminhá-lo para o BNG. Nesse caso, eles atuam apenas como "L2 puro", ou seja, encaminham o tráfego baseado apenas no ID das VLANs.

Um fluxo básico de um cliente proveniente de uma OLT, por exemplo, seria o seguinte: o tráfego chega de uma OLT que está conectada ao "SWITCH-LOCALIDADE-C", e a VLAN que transporta o tráfego dos clientes é a VLAN 100. O switch recebe os *frames* e os aceita, pois a VLAN 100 está configurada na porta que se conecta à OLT. Em seguida, encaminha esses *frames* para as demais portas que também estão configuradas para a VLAN 100. Nesse caso, a porta de *uplink* se conecta ao "SWITCH-CORE", uma vez que é esse switch que se conecta ao BNG. Chegando no "SWITCH-CORE", ele aceita os *frames* e os encaminha para as demais portas configuradas para aquela VLAN, incluindo aquela que se conecta ao BNG. Assim, o tráfego L2 do cliente chega ao seu concentrador. A partir do BNG, é realizado o roteamento do cliente e, em seguida, é encaminhado para o "ROTEADOR-BORDA", passando novamente pelo "SWITCH-CORE". No entanto, o switch apenas analisa campos do cabeçalho da camada 2, já que não atua como roteador. Chegando no "ROTEADOR-BORDA", o cliente é roteado para a Internet. Neste exemplo, a figura do *Carrier Grade* NAT (CGNAT) será dispensada.

Falando sobre a parte L3 da rede, temos o "ROTEADOR-CORE" responsável pelo roteamento central da rede, principalmente no que diz respeito a parte de gerência e serviços internos do provedor, como *Domain Name Service* (DNS). O roteamento de/para a Internet está sob responsabilidade do "ROTEADOR-BORDA". Por exemplo, para fins de gerenciamento do "SWITCH-LOCALIDADE-A", uma VLAN era criada nesse switch e também no "SWITCH-CORE", sendo configurada nas respectivas portas e encaminhada para o "ROTEADOR-CORE". Outro exemplo é um servidor de DNS, onde a VLAN era criada no "ROTEADOR-CORE" e estendida até a máquina que hospeda o serviço de DNS. Resumidamente, a inteligência da rede está concentrada no "ROTEADOR-CORE", "BNG-IPOE" e "ROTEADOR-BORDA".

É importante observar a conexão entre o "SWITCH-CORE" e o "SWITCH-LOCALIDADE-A", onde existem duas rotas entre eles para garantir o tráfego dos switches no caso de falha de uma rota. Conforme mencionado anteriormente, não é possível encaminhar uma determinada VLAN por dois caminhos que se conectem ao mesmo dispositivo remoto, pois isso causaria um *loop* de camada 2 e derrubaria a rede. Para assegurar a disponibilidade da rota no ambiente onde não tem MPLS, se utilizou a tecnologia de agregação de links, conhecida popularmente como *Link Aggregation Control Protocol* (LACP), para garantir a redundância da rota e evitar problemas de *loop*.

Com o LACP, o switch passa a reconhecer os dois links como um único link, e isso é perceptível durante a configuração. Portanto, a VLAN não será mais configurada individualmente nas duas portas, mas sim em uma interface lógica que é criada na configuração. Vejamos abaixo como seria essa configuração em switches Huawei (HUAWEI, 2023):

```
interface Eth-Trunk0
 port link-type trunk
 port trunk allow-pass vlan 10

interface XGigabitEthernet0/0/1
 eth-trunk 0

interface XGigabitEthernet0/0/2
 eth-trunk 0
```

Podemos notar que a porta *XgigabitEthernet0/0/1* e *XgigabitEthernet0/0/2* fazem parte da interface *Eth-Trunk0*, loga a VLAN 10 passa nessa porta e não nas portas físicas. Logo, se a rota que sai pela porta *XgigabitEthernet0/0/1* ficar *down* o tráfego ainda continuará saindo pela porta *XgigabitEthernet0/0/2* e assim os clientes ainda conseguirão chegar ao “BNG-IPOE”.

Não abordaremos neste trabalho as vantagens do uso do LACP na rede do provedor, mas é importante ressaltar que o LACP é um protocolo que permite a agregação de links, desde que esses links estejam entre os mesmos equipamentos. Em outras palavras, se houver dois links entre o equipamento A e B, é possível realizar a agregação utilizando o LACP. No entanto, se esses links passarem por algum outro dispositivo de rede que faça o tratamento de informações ao nível da camada 2, a agregação não será possível.

Isso significa que, se houver a necessidade de estabelecer uma rota de backup do "SWITCH-LOCALIDADE-B" para o "BNG-IPOE" passando pelo "SWITCH-LOCALIDADE-A", não será possível utilizar o LACP. Nesse caso, se a rota principal entre o "SWITCH-LOCALIDADE-B" e o "SWITCH-CORE" falhar, será necessário redirecionar manualmente o tráfego dos clientes.

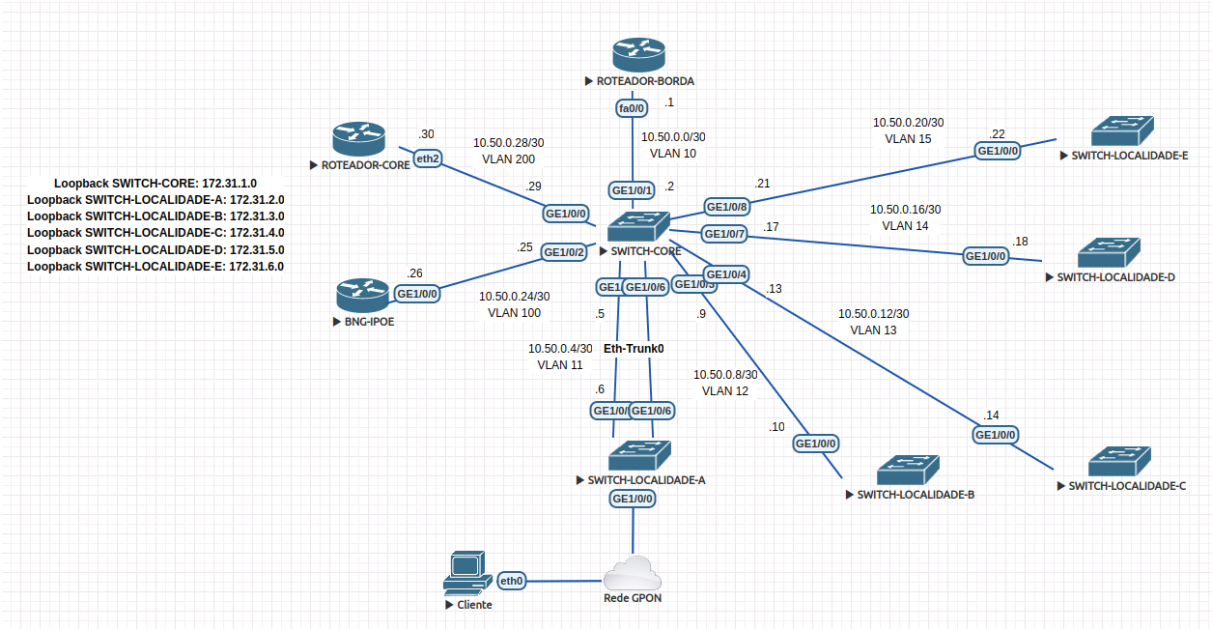
Ao analisar o cenário atual do provedor, foi identificada a problemática mencionada anteriormente, em que havia a necessidade de ativar uma rota de backup para um switch em uma determinada localidade. No entanto, com a rede operando em modo "L2 puro", seria necessário acionar manualmente a rota de backup. É importante mencionar que a

possibilidade de utilizar protocolos da família STP foi descartada, uma vez que o provedor não os utiliza em sua rede. Portanto, como solução mais avançada, já foi desenvolvido um projeto baseado em MPLS, tanto para resolver essa problemática quanto para outras situações.

4.2 Implementação no Ambiente Virtualizado

A seguir, será apresentada a topologia que será utilizada no EVE-NG para simular a implementação do MPLS L2VPN:

Figura 9: Diagrama do ambiente para simulação no EVE-NG.



Fonte: Elaborado pelo autor (2023).

Na figura apresentada, temos os ativos de rede mencionados anteriormente, e foi adicionado o "PC Cliente" que faz parte da rede GPON, com o objetivo de realizar testes com o VPWS.

Na topologia, foram incluídas as primeiras informações importantes para a simulação da implementação, como os endereços das interfaces loopback de cada ativo, o endereçamento IPv4 dos links ponto a ponto e o ID de VLAN usado para cada rede /30 entre os ativos. Essas informações são essenciais para possibilitar a comunicação principal entre os equipamentos. Vale ressaltar a importância de definir o *Maximum Transmission Unit* (MTU) com o maior valor possível nas interfaces de backbone. Isso se deve ao fato de que essas interfaces irão transmitir pacotes com vários cabeçalhos de protocolos, incluindo o próprio

MPLS. A título de exemplo, a seguir temos a configuração da rede entre o "SWITCH-CORE" e "SWITCH-LOCALIDADE-A", em que a VLAN 11 foi utilizada, conforme mostrado no diagrama:

Bloco de configuração 1

[SWITCH-CORE] *vlan 11*
[SWITCH-CORE-vlan11] *description P2P-SWITCH-LOCALIDADE-A*
[SWITCH-CORE-vlan11] *interface Eth-Trunk0*
[SWITCH-CORE-Eth-Trunk0] *port trunk allow-pass vlan 11*
[SWITCH-CORE-Eth-Trunk0] *interface Vlanif11*
[SWITCH-CORE-Vlanif11] *description P2P-SWITCH-LOCALIDADE-A*
[SWITCH-CORE-Vlanif11] *mtu 9000*
[SWITCH-CORE-Vlanif11] *ip address 10.50.0.5 255.255.255.252*

[SWITCH-LOCALIDADE-A] *vlan 11*
[SWITCH-LOCALIDADE-A-vlan11] *description P2P-SWITCH-LOCALIDADE-A*
[SWITCH-LOCALIDADE-A-vlan11] *interface Eth-Trunk0*
[SWITCH-LOCALIDADE-A-Eth-Trunk0] *port trunk allow-pass vlan 11*
[SWITCH-LOCALIDADE-A-Eth-Trunk0] *interface Vlanif11*
[SWITCH-LOCALIDADE-A-Vlanif11] *description P2P-SWITCH-CORE*
[SWITCH-LOCALIDADE-A-Vlanif11] *mtu 9000*
[SWITCH-LOCALIDADE-A-Vlanif11] *ip address 10.50.0.6 255.255.255.252*

Após a configuração das VLANs e dos endereços IP, procedeu-se à validação da comunicação entre os dispositivos que estabelecem as conexões ponto a ponto. Para isso, utilizou-se o teste básico com a ferramenta de ping, a qual utiliza o protocolo *Internet Control Message Protocol* (ICMP). Após confirmar a comunicação, realizou-se a configuração completa do protocolo de roteamento dinâmico OSPF, anunciando as redes /30 dos enlaces ponto a ponto e os IPs das interfaces loopback de cada dispositivo. A seguir, apresentamos um exemplo dessa configuração realizada no "SWITCH-CORE", no qual o router-id do OSPF foi definido como o IP de loopback do switch.

Bloco de configuração 2

[SWITCH-CORE] *ospf 1 router-id 172.31.1.0*

[SWITCH-CORE-ospf-1] *area 0.0.0.0*
[SWITCH-CORE-ospf-1-area-0.0.0.0] *description AREA BACKBONE*
[SWITCH-CORE-ospf-1-area-0.0.0.0] *network 172.31.1.0 0.0.0.0 description INTERFACE-LOOPBACK*
[SWITCH-CORE-ospf-1-area-0.0.0.0] *network 10.0.50.5 0.0.0.0 description P2P-SWITCH-LOCALIDADE-A*
[SWITCH-CORE-ospf-1-area-0.0.0.0] *network 10.0.50.9 0.0.0.0 description P2P-SWITCH-LOCALIDADE-B*
[SWITCH-CORE-ospf-1-area-0.0.0.0] *network 10.0.50.13 0.0.0.0 description P2P-SWITCH-LOCALIDADE-C*
[SWITCH-CORE-ospf-1-area-0.0.0.0] *network 10.0.50.17 0.0.0.0 description P2P-SWITCH-LOCALIDADE-D*
[SWITCH-CORE-ospf-1-area-0.0.0.0] *network 10.0.50.21 0.0.0.0 description P2P-SWITCH-LOCALIDADE-E*
[SWITCH-CORE-ospf-1-area-0.0.0.0] *network 10.0.50.29 0.0.0.0 description P2P-ROTEADOR-CORE*

Vale ressaltar a importância da ativação do OSPF no enlace entre o "SWITCH-CORE" e o "ROTEADOR-CORE". Essa ativação é necessária, uma vez que, como mencionado anteriormente, o "ROTEADOR-CORE" desempenha um papel central no encaminhamento interno do provedor, abrangendo redes de gerenciamento e serviços, como DNS e monitoramento. Portanto, o "SWITCH-CORE" precisa receber as rotas para essas redes desde o início, garantindo a entrega adequada de pacotes com destino a esses prefixos.

Após a configuração do OSPF, prosseguiu-se com a configuração básica do MPLS e LDP. Realizou-se a ativação global do protocolo nos switches e ativou-se também nas interfaces de backbone. Nesse processo, optou-se por utilizar o IP de loopback como identificador (ID) para cada LSR. A seguir, apresentamos um exemplo da configuração realizada no "SWITCH-CORE", considerando a interface de backbone responsável pela comunicação com o "SWITCH-LOCALIDADE-A":

Bloco de configuração 3
[SWITCH-CORE] *mpls lsr-id 172.31.1.0*
[SWITCH-CORE] *mpls*
[SWITCH-CORE] *mpls ldp*

[SWITCH-CORE] *interface Vlanif11*
[SWITCH-CORE-Vlanif11] *mpls*
[SWITCH-CORE-Vlanif11] *mpls ldp*

Após a conclusão dessa configuração, foi possível estabelecer o serviço de L2VPN utilizando o VPWS. Na primeira simulação, uma VLAN de comunicação (VLAN 400) foi transportada entre o "PC Cliente" e o "BNG-IPOE". O "SWITCH-LOCALIDADE-A" e o "SWITCH-CORE" desempenharam o papel de LSR PE como parte do VPWS, pois o túnel MPLS foi estabelecido entre eles.

A configuração do serviço L2VPN é realizada nos switches PE "SWITCH-CORE" e "SWITCH-LOCALIDADE-A". Primeiramente, é feita a sinalização do peer, ou seja, o PE remoto com o qual deseja-se estabelecer o túnel. Em seguida, ocorre a ativação do serviço L2VPN. No "SWITCH-CORE", a porta *GigabitEthernet1/0/2* é utilizada, a qual está conectada ao "BNG-IPOE". Já no "SWITCH-LOCALIDADE-A", a porta GigabitEthernet1/0/0 é utilizada, sendo a porta que se conecta à OLT, onde a rede GPON tem início. A seguir, apresentamos a configuração dos dois PEs:

Bloco de configuração 4
[SWITCH-CORE] *mpls l2vpn*
[SWITCH-CORE] *mpls ldp remote-peer switch-localidade-A*
[SWITCH-CORE-*mpls-ldp-remote-switch-localidade-A*] *remote-ip 172.31.2.0*
[SWITCH-CORE-*mpls-ldp-remote-switch-localidade-A*] quit
[SWITCH-CORE] *interface GigabitEthernet1/0/2.400*
[SWITCH-CORE-GigabitEthernet1/0/2.400] *description VPWS-VLAN-400*
[SWITCH-CORE-GigabitEthernet1/0/2.400] *mtu 9000*
[SWITCH-CORE-GigabitEthernet1/0/2.400] *dot1q termination vid 400*
[SWITCH-CORE-GigabitEthernet1/0/2.400] *mpls l2vc 172.31.2.0 400*

[SWITCH-LOCALIDADE-A] *mpls l2vpn*
[SWITCH-LOCALIDADE-A] *mpls ldp remote-peer switch-core*
[SWITCH-LOCALIDADE-A-*mpls-ldp-remote-switch-core*] *remote-ip 172.31.2.0*
[SWITCH-LOCALIDADE-A-*mpls-ldp-remote-switch-core*] quit
[SWITCH-LOCALIDADE-A] *interface GigabitEthernet1/0/0.400*
[SWITCH-LOCALIDADE-A-GigabitEthernet1/0/0.400] *description VPWS-VLAN-400*

[SWITCH-LOCALIDADE-A-GigabitEthernet1/0/0.400] *mtu 9000*
[SWITCH-LOCALIDADE-A-GigabitEthernet1/0/0.400] *dot1q termination vid 400*
[SWITCH-LOCALIDADE-A-GigabitEthernet1/0/0.400] *mpls l2vc 172.31.1.0 400*

Como o ambiente do provedor é composto por switches do fabricante Huawei (Huawei, 2023), nos guias de configuração fornecidos pelo fabricante é apresentada a sintaxe utilizando o comando "l2vc". Esse comando é utilizado para criar uma L2VPN VPWS do tipo *Martini*, também conhecido como *Virtual Leased Line* (VLL), de acordo com a documentação do fabricante.

Martini é um dos modelos de implementação do VPWS, sendo o outro modelo chamado Kompella. Conforme mencionado por (Furtado, 2020), na implementação Martini, o protocolo LDP é utilizado para sinalizar a label da L2VPN entre os PEs, sendo utilizado o conceito de *Targeted Label Distribution Protocol* (T-LDP). Nesse modelo, o peer da L2VPN deve ser explicitamente configurado na sinalização. Já na implementação Kompella, o protocolo *Border Gateway Protocol* (BGP) é utilizado tanto para a descoberta do peer quanto para a atribuição da label da L2VPN.

Após a realização da configuração, foi verificado que o cliente foi autenticado no BNG e conseguiu navegar com sucesso.

[~BNG-IPOE]display access-user domain TESTE

UserID Username Interface IP address MAC
Vlan IPv6 address Access type

8321 c83a3500dea3@TESTE GigabitEthernet1/0/0.400 100.76.11.218 c83a-3500-dea3
400/- - IPOE

Pode-se observar que o usuário com identificador "c83a3500dea3" do domínio "TESTE" chegou através da porta "*GigabitEthernet*0/1/0.400" e da VLAN 400, e foi atribuído o endereço IP 100.76.11.218.

Para uma compreensão mais simplificada das configurações mencionadas anteriormente neste capítulo, apresentamos um fluxograma a seguir:

Bloco de configuração 1

1 - Cria a vlan 11
2 - Coloca uma descrição para esse vlan
3 - Entra na interface física que conecta com o switch remoto
4 - Permite a vlan 11 de trafegar nessa interface
5 - Cria a interface lógica (l3) da vlan 11
6 - Ajusta o MTU da interface para 9000
7 - Coloca o endereço IP na interface lógica da vlan 11

Bloco de configuração 2

1 - Ativa o processo OSPF com *process* ID 1 e router-id 172.31.1.0
2 - Entra na configuração da area 0 do OSPF (area backbone)
3 - Coloca uma description na seção de configuração da area
4 - Habilita o OSPF na interface loopback e consequentemente divulga o IP dessa interface na rede
5 - As demais linhas de comando habilitam o OSPF na interface que estiver com o IP especificado e divulga a rede dessa interface

Bloco de configuração 3

1 – Define o router ID do MPLS que irá identificar um LSR na rede
2 – Ativa o MPLS globalmente
3 – Ativa o MPL LDPglobalmente
4 – Entra na interface lógica
5 – Ativa o MPLS na interface
6 – Ativa o LDP na interface

Bloco de configuração 4

1 – Ativa a funcionalidade de L2VPN do MPLS
2 – Fecha uma sessão LDP remota
3 – Define o IP do LSR remoto
4 – Cria a subinterface de acesso da VPWS
5 – Coloca uma descrição para identificar aquele *tunnel*
6 – Define o MTU da interface, que consequentemente será o MTU do *tunnel*
7 – Define qual VLAN será transportada
8 – A configuração do *tunnel* em si, onde é apontado o *peer* remoto e o ID do *tunnel*

Por fim, é importante destacar que a implementação no ambiente virtualizado foi bem-sucedida, permitindo validar a entrega do serviço ao cliente. Além disso, não foi abordada a solução do STP para a topologia do provedor, uma vez que o MPLS já é uma solução mais avançada e escalável (FURTADO, 2020). O MPLS é capaz de resolver a questão de enlaces redundantes e também oferecer suporte a serviços futuros de forma mais eficiente.

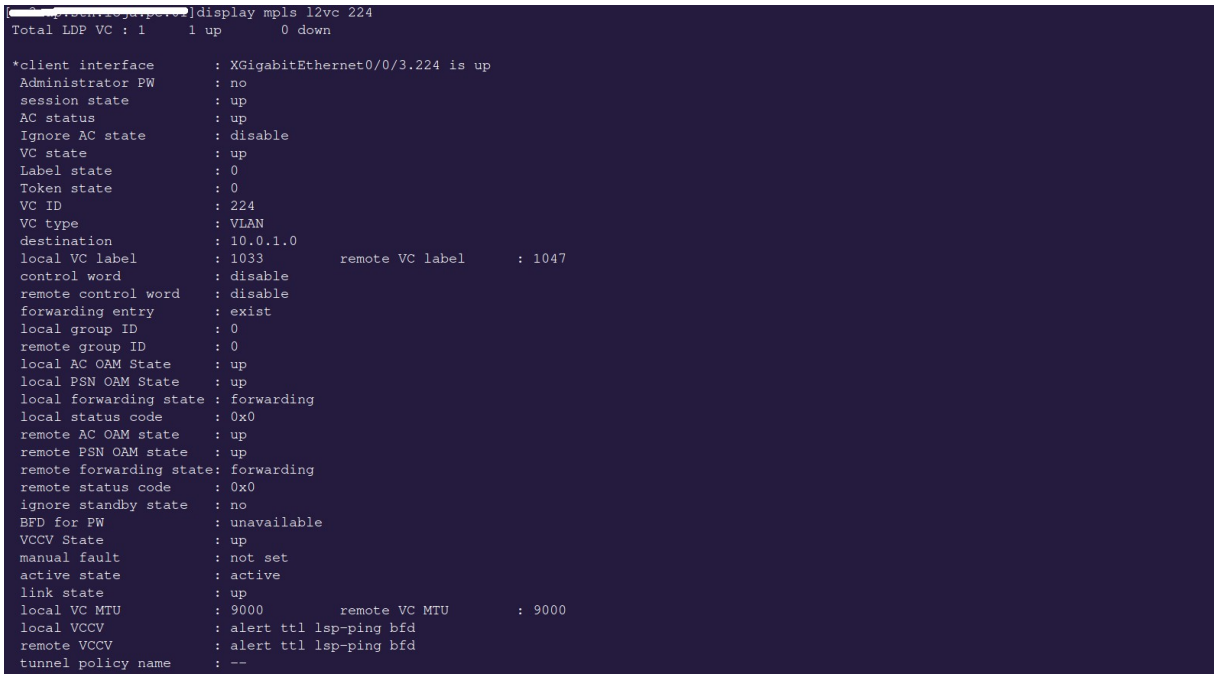
4.3 Implementação no Ambiente em Produção

Após obtermos resultados positivos no ambiente virtualizado, foi possível realizar a implementação no ambiente de produção do provedor. Seguimos a mesma sequência de tarefas apresentada no capítulo anterior, adaptando as variáveis, como as portas de entrega.

Realizamos um teste inicial com um número reduzido de clientes, visando validar as configurações e, caso ocorresse alguma falha, minimizar o impacto para apenas um pequeno

grupo de usuários. Após a configuração foi executado o seguinte comando para visualizar informações do *tunnel*:

Figura 10: Comando para diagnóstico da L2VPN no LSR lado OLT.



```
[~HUAWEI]display mpls l2vc 224
Total LDP VC : 1     1 up       0 down

*client interface       : XGigabitEthernet0/0/3.224 is up
 Administrator PW       : no
 session state          : up
 AC status              : up
 Ignore AC state        : disable
 VC state               : up
 Label state            : 0
 Token state            : 0
 VC ID                  : 224
 VC type                : VLAN
 destination            : 10.0.1.0
 local VC label         : 1033         remote VC label      : 1047
 control word           : disable
 remote control word    : disable
 forwarding entry       : exist
 local group ID         : 0
 remote group ID        : 0
 local AC OAM State     : up
 local PSN OAM State    : up
 local forwarding state : forwarding
 local status code      : 0x0
 remote AC OAM state    : up
 remote PSN OAM state   : up
 remote forwarding state: forwarding
 remote status code     : 0x0
 ignore standby state   : no
 BFD for PW             : unavailable
 VCCV State             : up
 manual fault           : not set
 active state           : active
 link state             : up
 local VC MTU           : 9000         remote VC MTU        : 9000
 local VCCV             : alert ttl lsp-ping bfd
 remote VCCV            : alert ttl lsp-ping bfd
 tunnel policy name     : --
```

Fonte: Elaborado pelo autor (2023).

Neste caso específico, foi realizado o transporte da VLAN 224 do LSR conectado à OLT. O tráfego é recebido através da porta *XgigabitEthernet*0/0/3 e, quando marcado com a VLAN 224, é encaminhado para o LSR conectado ao BNG.

O comando "display mpls l2vc 224" permite verificar informações específicas sobre o L2VC (VPWS). Neste caso, o L2VC com identificador (ID) 224 é exibido. É importante observar algumas informações relevantes na linha "client interface", onde é mostrada a interface de acesso do túnel.

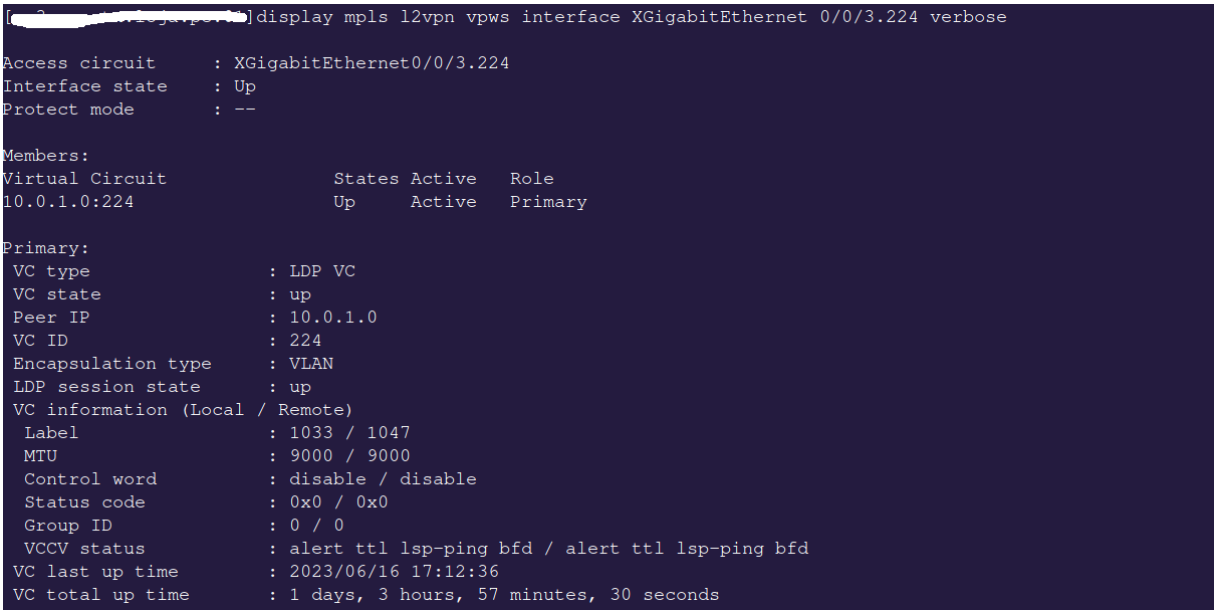
O campo "session state" indica o estado da sessão com o peer remoto. Já o campo "AC status" refere-se ao Access Circuit do L2VC, que, neste caso, seria a porta *XgigabitEthernet*0/0/3.224, e indica que a porta está UP (ativo). O "VC state" exibe o estado do Virtual Circuit, que se refere ao próprio túnel em si. Essas informações fornecem uma visão geral do estado e funcionamento do L2VC (HUAWEI, 2023).

Outros detalhes importantes a serem observados incluem o campo "destination", que representa o IP do LSR PE remoto. Vale ressaltar que existem parâmetros que devem ser idênticos em ambos os lados do L2VC, como o VC ID, o VC type e o MTU. Além disso, se o

"control word" estiver habilitado em um lado, também deve ser habilitado no outro lado. Por padrão, essa opção está desabilitada.

Outro comando útil para diagnóstico do L2VC é o "display mpls l2vpn vpws interface *XGigabitEthernet*0/0/3.224 verbose", que exibe tanto as variáveis locais como aquelas recebidas do LSR remoto no momento em que as mensagens são trocadas para fechar o túnel. Esse comando fornece informações mais detalhadas sobre o estado do túnel (HUAWEI, 2023).

Figura 11: Segundo comando para diagnóstico da L2VPN no LSR lado OLT.



Fonte: Elaborado pelo autor (2023).

Existem informações sobre a label local e remota, bem como o MTU local e remoto, entre outras variáveis. No caso específico mencionado, a label 1036 será utilizada por esse LSR para encaminhar o tráfego para essa L2VPN específica, cujo destino é o LSR com o IP 10.0.1.0, conforme indicado no campo "Peer IP".

Abaixo está o mesmo comando anterior sendo executado no LSR 10.0.1.0, que está conectado ao BNG:

Figura 12: Comando para diagnóstico da L2VPN no LSR lado BNG.

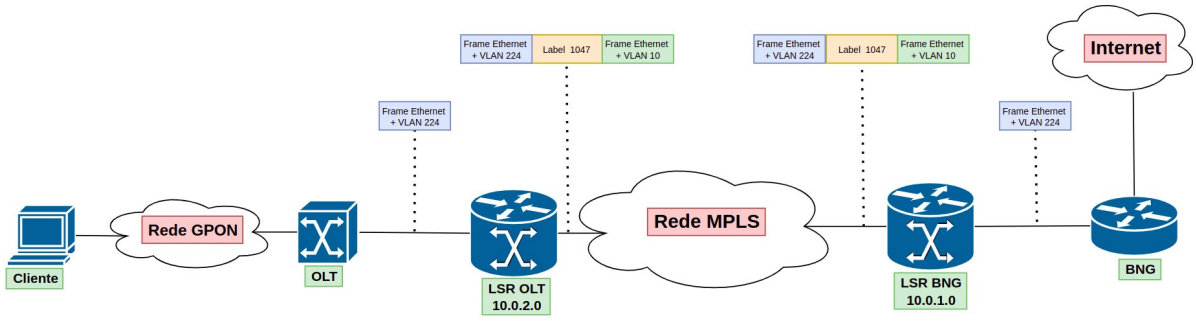
```
[~au2-[redacted]]display mpls l2vpn vpws interface XGigabitEthernet 0/0/4.224 verbose

Access circuit     : XGigabitEthernet0/0/4.224
Interface state    : Up
Protect mode       : --

Members:
Virtual Circuit              States Active   Role
10.0.2.0:224                 Up     Active   Primary

Primary:
 VC type               : LDP VC
 VC state              : up
 Peer IP               : 10.0.2.0
 VC ID                 : 224
 Encapsulation type    : VLAN
 LDP session state     : up
 VC information (Local / Remote)
  Label                : 1047 / 1033
  MTU                  : 9000 / 9000
  Control word         : disable / disable
  Status code          : 0x0 / 0x0
  Group ID             : 0 / 0
  VCCV status          : alert ttl lsp-ping bfd / alert ttl lsp-ping bfd
 VC last up time       : 2023/06/16 17:12:24
 VC total up time      : 5 days, 9 hours, 25 minutes, 9 seconds
```

Fonte: Elaborado pelo autor (2023).

Neste caso, a porta de acesso é a interface *XGigabitEthernet*0/0/4.224, que está conectada ao BNG. Podemos observar que a label local utilizada é a 1047, a qual o LSR conectado à OLT recebe. Isso é evidenciado pelo campo "Peer IP" sendo 10.0.2.0, exatamente o IP do LSR conectado à OLT. Dessa forma, foi possível realizar o mapeamento da L2VPN com identificador 224, a qual transporta a VLAN 224 dos assinantes para ser processada no BNG.

Abaixo está um diagrama que ilustra o processamento do tráfego na rede MPLS, com origem no cliente:

Figura 13: Diagrama para representação do tráfego.



Fonte: Elaborado pelo autor (2023).

Analisando a trajetória do frame Ethernet desde a chegada ao LSR vindo da OLT, podemos observar que o frame já possui a marcação de VLAN, especificamente a VLAN 224. Ao chegar ao LSR, a VLAN é analisada e identifica-se a existência de uma L2VPN associada

a essa VLAN. Nesse momento, o LSR realiza o encapsulamento desse frame no *shim header* do MPLS, atribuindo a ele a label 1047, como mencionado anteriormente. Além disso, é adicionado a VLAN 10 com o frame Ethernet, que representa a VLAN de backbone entre os dois LSRs.Ao chegar ao LSR do lado BNG, a label é analisada e o LSR identifica o serviço L2VPN com o identificador 224. Em seguida, o *shim header* é removido e o frame Ethernet com a VLAN 224 é entregue ao BNG.

No entanto, neste cenário, há uma diferença em relação ao uso frequente de duas labels pelo LSR (HUAWEI, 2023). Normalmente, o LSR adiciona tanto a label da L2VPN quanto a label do LSP para o endereço IP de loopback do LSR com o qual o túnel é estabelecido. No entanto, no caso mencionado, o LSR do lado OLT adiciona apenas uma label, uma vez que a conexão entre esses dois LSRs é direta, sem a presença de outro LSR intermediário. Assim, a label distribuída pelo LSR do lado BNG para o LSR do lado OLT, referente à FEC 10.0.1.0 (endereço IP de loopback do LSR do lado BNG), possui um valor de 3. Conforme mencionado em capítulos anteriores, essa label indica que o LSR que recebeu a distribuição deve encaminhar o pacote sem a utilização de labels. O LSR do lado OLT recebe essa informação e, portanto, envia o pacote apenas com a label da L2VPN.

Dessa forma, após a configuração da L2VPN do tipo VPWS, foi verificado que os clientes da VLAN 224 conseguiram navegar normalmente, mesmo após um período de 24 horas em que foram mantidos em monitoramento. Após essa validação inicial, foi possível migrar os demais clientes para a L2VPN, sendo necessário configurar uma L2VPN específica para cada VLAN.

5 CONCLUSÃO

A implementação do MPLS na rede em produção do provedor alcançou resultados altamente positivos, alinhados com os objetivos estabelecidos no início deste trabalho. Além disso, foram destacadas as vantagens da adoção do protocolo MPLS como uma solução avançada para o transporte dos clientes até o BNG, proporcionando escalabilidade e resiliência através da tecnologia L2VPN VPWS. Essa abordagem permitiu superar as limitações do tradicional L2 "puro", que é inflexível e restritivo.

A possibilidade de realizar a implementação em um ambiente virtualizado, utilizando o EVE para simular a conectividade e antecipar eventuais problemas que poderiam surgir na rede em produção, foi fundamental. Isso permitiu mapear as características necessárias para cada configuração, desde a definição do MTU adequado até as VLANs que seriam transportadas. Porém em alguns momentos foi necessário reiniciar o ambiente para algumas configurações surtirem efeito, em outros até mesmo reiniciar a máquina virtual em que estava hospedado o EVE.

Em determinado momento onde foi necessário trabalhar o MPLS entre fabricantes diferentes, no caso do provedor sendo Huawei e Datacom, houve a necessidade de consultar guias de interoperabilidade. Foram feitas pesquisas, e no site de documentação da Huawei não foi identificado nenhum guia, possívelmente pelo fato da fabricante Datacom ser brasileira. Porém nos guias da fabricante Datacom foi possível encontrar um guia de configuração no qual cita as integrações com diversos fabricantes, entre eles com Huawei. Foi utilizado um guia que proporcionou uma correta configuração e validação do serviço de L2VPN VPWS entre Huawei e Datacom (DATACOM, 2022).

Com todas as configurações mapeadas, foi possível aplicar cada etapa de forma cuidadosa, evitando paralisações indesejadas na rede. A fim de validar a migração da primeira VLAN, os clientes foram monitorados por 24 horas para garantir a eficiência dos serviços durante o processo. Essa migração foi realizada em um horário de baixo uso da rede pelos usuários, minimizando assim qualquer interrupção nos serviços para os usuários da VLAN 224.

Após a conclusão da implementação do MPLS na rede, foi identificado o uso positivo dessa tecnologia. Em uma situação específica, uma rota secundária foi ativada para uma localidade, e no momento em que a rota principal ficou inoperante, a convergência automática do tráfego dos clientes ocorreu sem qualquer necessidade de intervenção manual,

demonstrando plenamente a eficácia do serviço. Esse resultado validou completamente o MPLS como solução para a rede do provedor.

Dessa forma, a implementação do MPLS na rede do provedor trouxe resultados extremamente satisfatórios, alinhados com os objetivos estabelecidos inicialmente. As vantagens do MPLS em termos de escalabilidade e resiliência foram evidenciadas, especialmente ao utilizar a tecnologia L2VPN VPWS, superando as limitações do L2 convencional. A abordagem de implementação cuidadosa, com monitoramento e validação contínua, demonstrou a eficácia do MPLS em garantir um transporte eficiente e confiável para os clientes.

REFERÊNCIAS

CASTELLS, Manuel. **A Galáxia Internet**: reflexões sobre a Internet, negócios e a sociedade. Rio de Janeiro: Zahar, 2003.

CISCO. **Multiprotocol Label Switching MPLS on Cisco Routers**. Disponível em: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mp_basic/configuration/xe-16/mp-basic-xe-16-book/multiprotocol-label-switching-mpls-on-cisco-routers.html. Acesso em: 20 de abr. 2023.

DATACOM. **DmOS Interoperabilidade com outros Vendors**: Guia de Configuração para Interoperabilidade. Rio Grande do Sul: Datacom, 2022.

EVE. **The Emulated Virtual Environment for Network, Security and DevOps Professionals**. Disponível em: https://www.eve-ng.net/. Acesso em: 25 de mar. 2023.

FILIPPETTI, Marco Aurélio. **Uma arquitetura para a construção de laboratórios híbridos de redes de computadores remotamente acessíveis**. Instituto de Pesquisas Tecnológicas do Estado de São Paulo, 2008.

FURTADO, L. **Redes MPLS para Provedores**. Disponível em: https://wiki.brasilpeeringforum.org/w/Redes_MPLS_para_Provedores. Acesso em: 03 de dez. 2022.

FURTADO, L. **Transição de Soluções L2VPN MPLS tradicionais para o EVPN**. Disponível em: https://wiki.brasilpeeringforum.org/w/Transicao_de_Solucoes_L2VPN_MPLS_Tradicionalis_para_o_EVPN. Acesso em: 07 de mai. 2023.

GIL, Antonio Carlos. **Como Elaborar Projetos de Pesquisa**. 4. ed. São Paulo: Atlas, 2008.

GHEIN, Luc De. **MPLS Fundamentals**: A Comprehensive Introduction to MPLS. Indianopolis, USA: Cisco Press, 2007.

HUAWEI. **LDP Working Mechanism**. Disponível em: https://support.huawei.com/enterprise/en/doc/EDOC1000178173/22b0901d/ldp-working-mechanism. Acesso em: 22 de abr. 2023.

HUAWEI. **Link Aggregation Configuration**. Disponível em: https://support.huawei.com/enterprise/en/doc/EDOC1100197892/7abaffd5. Acesso em: Acesso em: 25 de abr. 2023.

HUAWEI. **Configuring a Martini VLL**. Disponível em: https://support.huawei.com/enterprise/en/doc/EDOC1100277013/8d2e85c6/configuring-a-martini-vll. Acesso em: 25 de abr. 2023.

HUAWEI. **VLL PWE3 Configuration Commands**. Disponível em: https://support.huawei.com/enterprise/en/doc/EDOC1100075369/9885cdf/vll-pwe3-configuration-commands. Acesso em: 28 de abr. 2023.

HUAWEI. **VLL Fundamentals**. Disponível em: https://support.huawei.com/enterprise/en/doc/EDOC1100277013/d7e90b00/vll-fundamentals. Acesso em: 02 de mai. 2023.

HUAWEI. **VLL Modes**. Disponível em: https://support.huawei.com/enterprise/en/doc/EDOC1100277013/a0ee3b96/vll-modes. Acesso em: 04 de mai. 2023.

IEEE 802.3. **IEEE Standard for Ethernet**. Disponível em: https://standards.ieee.org/ieee/802.3/7071/. Acesso em: 12 de fev. 2023.

IEEE 802.1D. **Spanning Tree Protocols**. Disponível em: https://www.ieee802.org/1/files/public/docs2009/aq-seaman-merged-spanning-tree-protocols-0509.pdf. Acesso em: 12 de fev. 2023.

JäRVI, Tuukka. **Layer 2 Solutions in Access Provider Networks**. Finland: Helsinki Metropolia University of Applied Sciences, 2020.

KUROSE, J. e ROSS K. **Redes de computadores e a internet**: Uma abordagem top down 6ª ed. São Paulo: Pearson eduaction do Brasil, 2013.

LACOSTE, Raymond. Edgeworth, Brad. **CCNP Enterprise Advanced Routing**. Hoboken, USA: Cisco Press, 2020.

OLIVEIRA, José Mário. Lins, Rafael Dueire. Mendonça, Roberto. **Redes MPLS**: Fundamentos e Aplicações. Rio de Janeiro: Brasport Livros e Multimídia, 2012.

POZO, Juan Ignacio. **A sociedade da aprendizagem e o desafio de converter informação em conhecimento**. Disponível em: http://www.udemo.org.br/A%20sociedade.Pdf. Acesso em: 08 de fev. 2023.

RFC 3031. **Multiprotocol Label Switching Architecture**. Dispoível em: https://www.rfc-editor.org/rfc/rfc3031#page-3. Acesso em: 01 de dez. 2022.

RFC 3032. **MPLS Label Stack Encoding**. Disponível em: https://www.rfc-editor.org/rfc/rfc3032. Acesso em: 01 de dez. 2022.

RFC 791. **Internet Protocol**. Disponível em: https://www.rfc-editor.org/rfc/rfc791. Acesso em: 10 de fev. 2023.

RFC 2516. **A Method for Transmitting PPP Over Ethernet (PPPoE)**. Disponível em: https://www.rfc-editor.org/rfc/rfc2516. Acesso em: 26 de abr. 2023.

RFC 2131. **Dynamic Host Configuration Protocol**. Disponível em: https://www.rfc-editor.org/rfc/rfc2131. Acesso em: 26 de abr. 2023.

APÊNDICE A – TERMO DE AUTORIZAÇÃO DE PESQUISA

Gnex Telecom
Termo de Autorização para divulgação de informações de empresa privada

Razão social: Gnex Telecom
CPNJ: 09.011.207/0001-36
Endereço Completo: Avenida Santana, 2952, Paraiso, Santana - AP, 68925-076, Brasil
Nome do responsável: Cristian Socorro da Silva Guerreiro **Função:** CEO
Telefone: 0800 280 0325 **E-mail:** cristian@gnex.com.br
Tipo de produção intelectual: ( ) Monografia; (X) TCC; ( ) Relatório de estágio; ( ) Dissertação; ( )Tese; ( ) Outro:

Título/Subtítulo: Implementação de Solução de Transporte L2 utilizando MPLS na rede de um Provedor de serviços de Internet (ISP)
Autor: Railson Rocha da Silva **Código da matrícula:** 2019110110010
Orientador: Klenilmar Lopes Dias
Nome do Curso: Curso Superior de Tecnologia em Redes de Computadores
Instituição de ensino: Instituto Federal de Educação, Ciência e Tecnologia do Amapá – Campus Macapá.

Como representante da empresa acima nominada, declaro que as informações e/ou documentos disponibilizados pela empresa para o trabalho citado:
(X) Podem ser publicados sem restrição
( ) Possuem restrição parcial por um período de _____ anos, não podendo ser publicadas as seguintes informações e/ou documentos:
_____
_____
( ) Possuem restrição total para publicação por um período de _____ anos, pelos seguintes motivos:
_____
_____

Representante

Santana, AP - 31/01/2023
Local e Data