MPLS Layer 3 VPN

1st Alberto Filipe
Dept. Ciências de Computadores
FCUP (DCC)
Porto, Portugal
up202400853@edu.fc.up.pt

3rd Maria Fortes
Dept. Ciências de Computadores
FCUP (DCC)
Porto, Portugal
up202400843@edu.fc.up.pt

***Abstract*—MPLS technology is a solution offered by Internet Service Providers (ISPs) to companies with geographically dispersed networks that wish to connect them. The appeal of MPLS lies in its use of labels for packet forwarding, as well as its support for services such as VPN, Traffic Engineering, and Quality of Service (QoS), which increase network efficiency. When applied in conjunction with Layer 3 VPN (L3 VPN), MPLS ensures customer security by creating isolated routes for each client. This report represents the first part of the semester project for the curricular unit Advanced Topics in Networking, which focuses on MPLS L3 VPN. The overall objective of the project is to configure and test an MPLS network, study the exchanged messages, and perform manual and automatic path configuration using Traffic Engineering and/or Layer 3 VPN.**

***Index Terms*—ISP, L3VPN, MPLS.**

I. Introdução

No processo de dimensionamento de uma rede de acesso à Internet, uma empresa ou entidade necessita considerar diversos requisitos fundamentais. Entre os principais estão: a abrangência geográfica, o modelo de tráfego, os requisitos de desempenho, os níveis de segurança exigidos e o custo de implementação. A avaliação desses fatores permite a definição de uma infraestrutura que combina topologias adequadas com tecnologias consolidadas, garantindo desempenho, segurança e viabilidade económica. Em redes *Wide Area Network* (WAN), uma das soluções mais utilizadas é o *Multiprotocol Label Switching* (MPLS), frequentemente combinada com *Virtual Private Networks* (VPNs) de camada 3 (L3 VPN). Esta abordagem possibilita a interligação de redes geograficamente distribuídas, com isolamento lógico de tráfego e suporte a requisitos avançados de desempenho e segurança.

O MPLS é geralmente implementado no núcleo das redes dos *Internet Service Providers* (ISPs), suportando múltiplos protocolos das camadas 2 e 3 do modelo OSI/TCP-IP. Em vez do encaminhamento baseado em endereços IP, o MPLS utiliza rótulos (*labels*), permitindo decisões de encaminhamento mais rápidas e flexíveis. A tecnologia oferece ainda serviços adicionais que justificam a sua adoção, como engenharia de tráfego e suporte a VPNs. Entre esses serviços, destaca-se a L3 VPN, que permite a múltiplos clientes partilhar a mesma infraestrutura, mantendo o isolamento entre redes. Esse isolamento é obtido por instâncias de *Virtual Routing and Forwarding* (VRF), que por sua vez mantêm tabelas de roteamento separadas para cada cliente, simulando redes dedicadas. A combinação de MPLS com L3 VPN permite aos ISPs fornecer uma infraestrutura escalável, segura e eficiente, com menor complexidade de gestão e custos reduzidos, em comparação com a construção de redes físicas dedicadas. A adição de novas VPNs ou alterações em rotas pode ser realizada de forma simplificada, promovendo agilidade na gestão da rede.

Este relatório encontra-se estruturado em cinco secções principais. A Secção I apresenta uma introdução ao MPLS e justifica a utilização de L3 VPN sobre esta tecnologia. A Secção II descreve a arquitetura do MPLS e os seus principais mecanismos. A Secção III foca-se nos conceitos técnicos associados à implementação de MPLS L3 VPN. A Secção IV apresenta o cenário de simulação desenvolvido, incluindo a aplicação prática dos conceitos abordados. Por fim, a Secção V descreve o processo de implementação e os testes realizados em ambiente virtual para o cenário proposto na secção anterior, avaliando o seu funcionamento e validando os requisitos de desempenho e isolamento definidos.

II. MPLS – Multi Protocol Label Switching

O MPLS é um método de encaminhamento de pacotes que toma decisões com base em *labels*, em vez de endereços IP tradicionais. No entanto, o que distingue o MPLS dos demais, encontra-se nos serviços avançados que suporta, como VPNs, engenharia de tráfego (*Traffic Engineering*) e Qualidade de Serviço (*Quality of Service* – QoS).

A. Arquitetura da rede MPLS

O core da rede MPLS é composto por roteadores do tipo *Label Switching Routers* (LSR), que executam funções específicas dependendo da sua posição na topologia.

Estes podem atuar como *Intermediate LSRs* ou *Edge LSRs*. Os roteadores que ligam a rede do cliente à rede MPLS (roteadores CE – Customer Edge) não precisam de suportar MPLS, pois esta é transparente para eles.

Os principais tipos de roteadores numa arquitetura MPLS são:

- **CE (Customer Edge)**: Roteador de borda do cliente que se conecta ao roteador PE do ISP e encaminha tráfego utilizando roteamento IP tradicional.
- **PE (Provider Edge)**: Roteador de borda do ISP que conecta os CEs ao *core* MPLS. Atua como *Ingress PE* ao adicionar um *label* aos pacotes provenientes dos clientes e como *Egress PE* ao remover o *label* e entregar os pacotes ao destino.
- **P (Provider)**: Roteador interno na rede MPLS, que comuta pacotes com *label* entre os PEs. Remove o *label* recebido, aplica o seu próprio e encaminha o pacote conforme a tabela LFIB.

A figura 1 apresenta a topologia básica de uma rede MPLS e os principais elementos envolvidos.

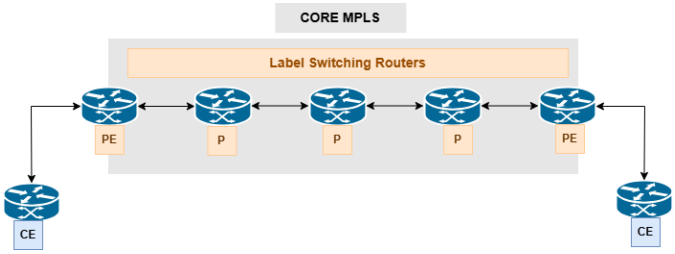

Fig. 1. Topologia da rede MPLS

B. MPLS – Labels

Em MPLS, o *label* é inserido como um *shim header* entre os cabeçalhos das camadas 2 e 3. Por este motivo, o MPLS é frequentemente referido como uma tecnologia de camada 2.5.

O *shim header* contém os seguintes campos:

- **Label (20 bits):** Identificador do fluxo de pacotes;
- **EXP (3 bits):** Campo reservado para QoS;
- **S (1 bit):** Indica se o *label* é o último da pilha;
- **TTL (8 bits):** Tempo de vida do pacote.

A figura 2 mostra o formato do *shim header* MPLS.

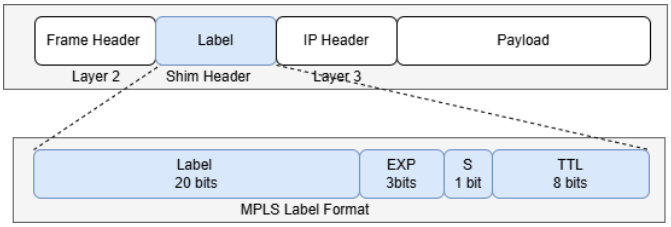

Fig. 2. Formato do Label MPLS

Um roteador com MPLS ativado atribui automaticamente *labels* a todas as redes que conhece. Para isso, além da ativação do MPLS, é necessário configurar um protocolo de roteamento dinâmico (como OSPF) para que os roteadores MPLS aprendam as rotas e preencham as tabelas de *labels*.

Importa destacar que os *labels* têm significado apenas local: cada roteador gera e associa os seus próprios *labels* às redes que conhece. A figura 3 ilustra várias tabelas de *labels* de roteadores MPLS para a rede 10.0.0.0/24.

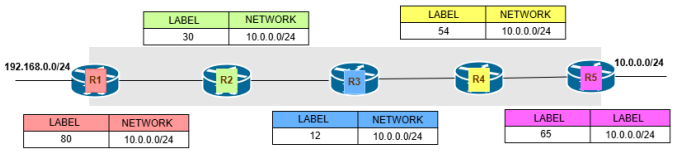

Fig. 3. Tabela de Labels em cada roteador MPLS

C. MPLS- Labels Distribution Protocol

Para construir os *Label Switched Paths* (LSPs), os *labels* precisam ser trocados entre LSRs diretamente conectados. O protocolo mais comum para esta função é o *Label Distribution Protocol* (LDP), utilizado para distribuição de *labels* em prefixos IPv4.

Com MPLS habilitado, as interfaces dos roteadores enviam pacotes LDP HELLO para o endereço multicast 224.0.0.2, através da porta UDP 646. Os vizinhos que também têm MPLS ativo recebem o pacote e estabelecem uma sessão LDP via TCP (porta 646), passando a trocar informações de *labels*.

As tabelas de *labels* (LFIB) são preenchidas com base nessas trocas. A figura 4 apresenta exemplos de tabelas resultantes da troca de *labels* entre os LSRs via LDP.

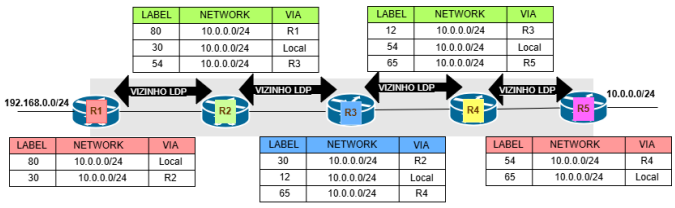

Fig. 4. Tabela de roteamento de Labels nos roteadores MPLS

D. MPLS – Label Switched Path (LSP)

O *Label Switched Path* (LSP) é uma sequência de LSRs pela qual um pacote MPLS deve passar dentro do núcleo da rede. O LSP é unidirecional, ou seja, o caminho de retorno até poderá reutilizar os mesmos LSRs, não sendo obrigatório, mas será sempre estabelecido um novo LSP.

Durante o encaminhamento ao longo de um LSP, os roteadores MPLS consultam apenas a LFIB, não sendo necessário recorrer à tabela de roteamento IP (FIB).

A figura 5 mostra como os *labels* são utilizados para criar e percorrer um LSP.

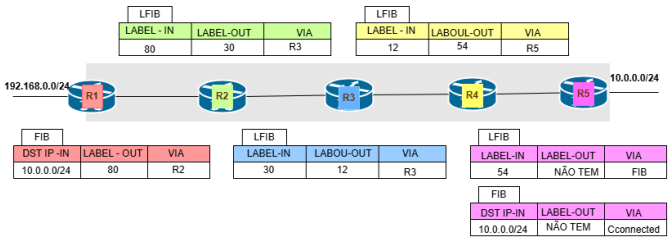

Fig. 5. Label Switched Path entre roteadores MPLS

E. Label Switching e Penultimate Hop Popping (PHP)

O roteador *Ingress Provider Edge* (PE), ao receber tráfego de um CE, consulta a *Forward Information Base* (FIB) para determinar a VRF a que o tráfego pertence, bem como determinar o destino. De seguida, aplica um *label* e encaminha o pacote para o núcleo MPLS. No *core*, os roteadores P utilizam a LFIB para encaminhar o pacote até o *Egress PE*.

Chegando ao último *hop* da rede MPLS, tradicionalmente, o *Egress PE* teria a função de remover o *label* e entregar ao CE o tráfego. Contudo, esse processo adiciona carga de processamento desnecessária ao *Egress PE*. Para otimizar este processo, utiliza-se o *Penultimate Hop Popping* (PHP).

Neste caso, o roteador P que se encontra diretamente conectado ao *Egress PE* fica com a responsabilidade de remover o *label* do pacote antes de o enviar para o *Egress PE*. Essa operação é indicada como *Pop Label* na LFIB. O *Egress PE* então recebe o pacote "limpo" e realiza apenas uma pesquisa na FIB para o encaminhamento final ao CE, reduzindo o processamento.

A figura 6 apresenta este cenário de *Penultimate Hop Popping*, confirmando o comportamento otimizado da comutação de *labels* na rede MPLS.

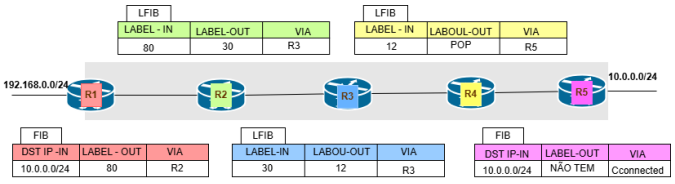

Fig. 6. Roteamento de pacotes na rede MPLS com o PHP habilitado

III. MPLS L3 VPN

O *Layer 3 Virtual Private Network* (L3 VPN) é implementado sobre uma infraestrutura MPLS para interligar redes WAN de diferentes clientes, como por exemplo, clientes que tenham empresas com filiais geograficamente separadas. O serviço é fornecido por um ISP, que conecta as redes do cliente por meio de sua rede MPLS partilhada.

Como múltiplos clientes utilizam a mesma infraestrutura física, é comum diferentes organizações usarem endereços IP privados idênticos. Este *overlap* de endereços, numa situação normal, causaria conflitos de roteamento caso não seja corretamente tratado. A solução para este cenário é a implementação de MPLS L3 VPN, que isola logicamente o tráfego de cada cliente, garantindo privacidade e separação das rotas.

A. MPLS e VRF

Para suportar múltiplos clientes com redes sobrepostas, os roteadores *Provider Edge* (PE) utilizam instâncias de *Virtual Routing and Forwarding* (VRF) para isolar localmente as tabelas de roteamento. Cada VRF atua como um roteador virtual independente, dentro do PE físico, sendo associada a uma interface conectada a um CE específico.

O número de instâncias VRF que pode ser configurado num roteador PE depende do número de interfaces disponíveis para conexão com CEs. As interfaces voltadas para o núcleo da rede MPLS (interligadas aos roteadores P) permanecem na tabela de roteamento global e não participam de VRFs.

Quando o tráfego de um cliente chega à interface MPLS do PE, o pacote recebe duas *labels*:

- A *outer label* (label externa), usada para o encaminhamento dentro da rede MPLS até o roteador *Egress PE*;
- A *inner label* (label interna), que identifica a VRF específica que o *Egress PE* deve utilizar para encaminhar o pacote ao CE de destino.

Essas *labels* são atribuídas com base nas rotas aprendidas pelas VRFs. O PE forma adjacências de roteamento, geralmente OSPF ou BGP, com os CEs e armazena as rotas recebidas numa *Routing Information Base* (RIB) separada por VRF.

B. MP-BGP e Route Distinguishers

Após aprender as rotas dos CEs, o PE precisa propagá-las aos demais roteadores da rede MPLS para garantir a conectividade entre PEs ligados a filiais de um mesmo cliente. Essa propagação é realizada através do *Multiprotocol BGP* (MP-BGP), que tem a capacidade de transportar rotas com prefixos sobrepostos utilizando um identificador adicional chamado *Route Distinguisher* (RD).

O MP-BGP, definido na RFC 4364 *("BGP/MPLS IP Virtual Private Network")*, permite criar um *address family* específico para VPNs sobre MPLS. O RD possui 64 bits e é concatenado ao prefixo IPv4 original, formando o *Network Layer Reachability Information* (NLRI). Isso permite diferenciar rotas idênticas pertencentes a clientes distintos.

As rotas são propagadas entre os PEs via sessões iBGP. Cada PE anuncia suas rotas VRF com o respetivo RD, tornando possível a coexistência de prefixos duplicados. Dessa forma, mesmo que dois clientes tenham o mesmo endereço de rede, o campo NLRI irá distinguir essas redes, para que o roteador *Egress PE* saiba identificar em qual VRF ele deve entregar cada pacote baseado no mesmo. Para que o *Egress PE* saiba qual VRF deve ser usada para encaminhar o pacote, é utilizado um segundo identificador: o *Route Target* (RT).

A figura 7 apresenta um exemplo de configuração de RDs e RTs para múltiplos clientes com redes sobrepostas.

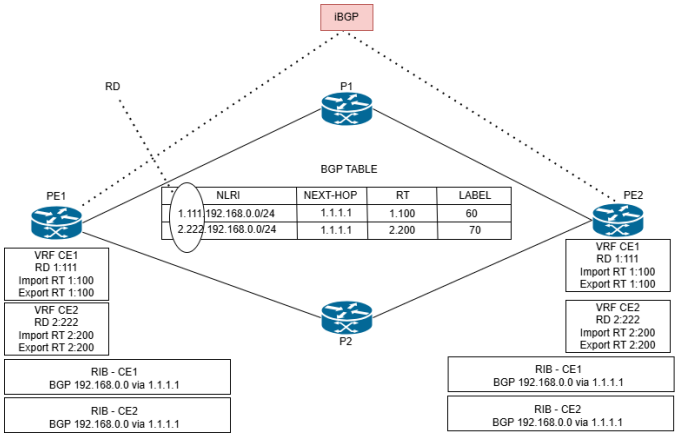

Fig. 7. Exemplo de identificadores NLRI (RD + prefix) e RT

C. MP-BGP e Route Targets

Enquanto o RD serve para diferenciar os prefixos da rede, o *Route Target* (RT) define as políticas de importação e exportação de rotas entre VRFs.

O RT é incluído como atributo BGP nas atualizações de rotas, sendo que no *Ingress PE* é configurado um RT para cada VRF, definindo que rotas devem ser exportadas para os demais PEs. Do lado do *Egress PE*, são definidos *Import RTs* para indicar quais rotas que devem ser importadas para cada VRF local.

Esse mecanismo permite flexibilidade na construção de topologias VPN. As tabelas BGP, portanto, contêm os atributos NLRI, *Next-Hop*, *Label* e RT, permitindo que o roteador *Egress PE* associe corretamente cada rota à VRF correspondente.

IV. ARQUITETURA PROPOSTA

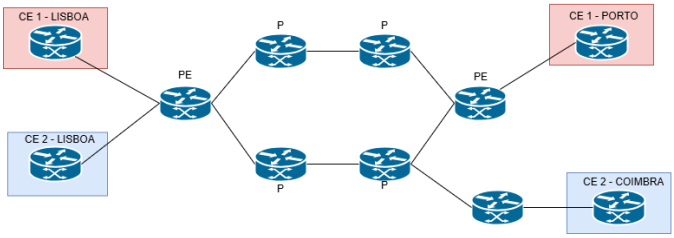

Fig. 8. Cenário proposto para a simulação prática

A figura 8 apresenta o cenário proposto para a simulação da parte prática do projeto.

Neste cenário, dois clientes diferentes encontram-se conectados à infraestrutura de rede MPLS de um ISP. O cliente CE1 possui duas filiais: uma em Lisboa e outra no Porto. Da mesma forma, o cliente CE2 possui redes em Lisboa e Coimbra. Ambas as redes em Lisboa conectam-se ao mesmo roteador *Provider Edge* (PE), sendo, portanto, necessário garantir o isolamento do tráfego entre os dois clientes neste ponto.

Do outro lado da rede MPLS, as redes de CE1 e CE2 estão localizadas em cidades diferentes (Porto e Coimbra, respetivamente) e conectam-se a diferentes PEs. O tráfego ponto a ponto entre os CEs percorre, no mínimo, quatro roteadores da rede MPLS. O cenário apresentado contempla todos os elementos necessários para simular e analisar o funcionamento de uma rede MPLS com suporte a L3 VPNs, incluindo o roteamento de tráfego, a aplicação de isolamento por VRF e o comportamento do protocolo LDP.

Nesta fase, será feita a configuração, teste e análise do tráfego na rede MPLS simulada, onde cada roteador será configurado de acordo com o seu papel na topologia (CE, PE ou P), sendo definidos os protocolos mais adequados para o roteamento e a comutação de *labels*. A análise irá focar sobre como os diferentes roteadores lidam com o tráfego, como são determinadas as rotas e como os diferentes elementos da arquitetura MPLS contribuem para a construção dos *Label Switched Paths* (LSPs). Serão observados os mecanismos de propagação de rotas, o comportamento das tabelas de encaminhamento e a separação lógica entre redes dos diferentes clientes.

A simulação será realizada utilizando o *Graphical Network Simulator-3* (GNS3) para a configuração e teste da topologia, e o *Wireshark* para captura e análise do tráfego de rede, possibilitando a observação do funcionamento do MPLS e das L3 VPNs em ambiente virtual.

V. IMPLEMENTAÇÃO E TESTES

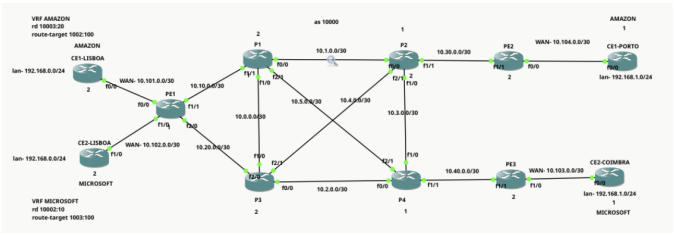

Fig. 9. Cenário Implementado

A figura 9 apresenta a topologia final onde foi implementada a rede MPLS. Após a definição do cenário inicial, mencionado na secção anterior, foram realizadas alterações na estrutura da topologia com o objetivo de otimizar a rede, melhorando a escalabilidade e reforçando a resiliência da mesma.

A principal modificação introduzida diz respeito à reorganização dos roteadores P. Enquanto a topologia proposta anteriormente apresenta um *backbone* linear e simplificado, a versão final implementa uma arquitetura em malha entre os roteadores P (P1, P2, P3 e P4). Essa abordagem permite múltiplos caminhos, oferecendo maior redundância, balanceamento de carga e tolerância a falhas.

As alterações realizadas mantêm os princípios do cenário original: dois clientes distintos (CE1 - AMAZON e CE2 - MICROSOFT), cada um com filiais localizadas em Lisboa, Porto e Coimbra, e com conectividade através da infraestrutura MPLS do ISP. A implementação foi realizada utilizando o simulador GNS3 para configuração dos roteadores e a ferramenta Wireshark para captura e análise do tráfego, como proposto inicialmente. Cada roteador foi configurado de acordo com o seu papel na rede (CE, PE ou P).

A configuração foi realizada em etapas sequenciais, iniciando-se pela conectividade IP entre os roteadores e pelo uso do protocolo OSPF para troca de rotas de forma dinâmica. Em seguida, foi habilitado o suporte ao MPLS nos roteadores do core e nos PEs. Posteriormente, configurou-se o BGP entre os PEs para transporte das rotas VPN e, por fim, foram criadas as instâncias de VRF e estabelecida a L3 VPN, com associação de *route distinguishers* e *route targets* apropriados para o isolamento do tráfego entre os clientes.

Com esta configuração, é possível validar o comportamento da rede MPLS em diferentes cenários de tráfego, incluindo falhas simuladas e recuperação automática de rotas, demonstrando os benefícios da nova topologia em termos de robustez, desempenho e escalabilidade.

A. Preparação do Core MPLS

A primeira etapa da implementação consistiu na preparação dos roteadores do ISP para operar com MPLS. Para tal, o suporte a MPLS foi ativado em todos os roteadores do tipo LSR, incluindo os *Provider Routers* (P) e as interfaces dos *Provider Edge Routers* (PE) conectadas ao core MPLS.

O protocolo de *Label Distribution Protocol* (LDP) foi configurado em todos os roteadores pertencentes à rede MPLS, permitindo a troca dinâmica de *labels* entre os LSRs para o encaminhamento de pacotes através da rede.

Para o roteamento interno no core MPLS, foi utilizado o protocolo *Open Shortest Path First* (OSPF), garantindo a convergência rápida da topologia e a atualização eficiente das tabelas de encaminhamento. Além disso, foi configurado um endereço IP na interface de *loopback* de cada roteador MPLS, utilizado tanto como *router ID* do OSPF, como também LDP *router ID*.

```
router ospf 10
 mpls ldp autoconfig
 router-id 1.1.1.1
 log-adjacency-changes
 network 1.1.1.1 0.0.0.0 area 0
 network 10.0.0.1 0.0.0.0 area 0
 network 10.1.0.2 0.0.0.0 area 0
 network 10.5.0.2 0.0.0.0 area 0
 network 10.10.0.2 0.0.0.0 area 0
P1#sh runn | s ldp
mpls label protocol ldp
mpls ldp router-id Loopback0 force
 mpls ldp autoconfig
```

Fig. 10. Configuração do OSPF, MPLS e LDP no roteador P1

A figura 10 apresenta a configuração dos protocolos OSPF, MPLS e LDP no roteador P1, pertencente ao core MPLS. Configurações equivalentes foram aplicadas aos demais roteadores *Provider* (P), com os respetivos endereços de rede nas interfaces e ajustes na configuração do OSPF.

```
P1#sh ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
10.10.10.10       0   FULL/  -        00:00:33    10.10.0.1       FastEthernet1/1
4.4.4.4           0   FULL/  -        00:00:30    10.5.0.1        FastEthernet2/1
2.2.2.2           0   FULL/  -        00:00:31    10.1.0.1        FastEthernet0/0
3.3.3.3           0   FULL/  -        00:00:32    10.0.0.2        FastEthernet1/0
P1#
```

Fig. 11. Estado das adjacências OSPF do roteador P1

A figura 11 mostra o resultado do comando **show ip ospf neighbor**, que confirma o estabelecimento de adjacências OSPF entre o roteador P1 e os roteadores PE1, P2, P3 e P4.

Todas as adjacências encontram-se no estado FULL, indicando sincronização completa das bases de dados OSPF e troca de rotas bem-sucedida. As interfaces envolvidas são:

- FastEthernet1/1 com o vizinho 10.10.10.10 (PE1);
- FastEthernet2/1 com o vizinho 4.4.4.4 (P4);
- FastEthernet0/0 com o vizinho 2.2.2.2 (P2);
- FastEthernet1/0 com o vizinho 3.3.3.3 (P3).

Estas adjacências são essenciais para a propagação das rotas no domínio OSPF, permitindo ao LDP atribuir *labels* com base na topologia estabelecida.

```
P1#sh mpls ldp discovery
 Local LDP Identifier:
    1.1.1.1:0
    Discovery Sources:
    Interfaces:
        FastEthernet0/0 (ldp): xmit/recv
            LDP Id: 2.2.2.2:0
        FastEthernet1/0 (ldp): xmit/recv
            LDP Id: 3.3.3.3:0
        FastEthernet1/1 (ldp): xmit/recv
            LDP Id: 10.10.10.10:0
        FastEthernet2/1 (ldp): xmit/recv
            LDP Id: 4.4.4.4:0
P1#
```

Fig. 12. Estado do LDP e interfaces MPLS ativas no roteador P1

A figura 12 confirma que o MPLS foi configurado nas interfaces FastEthernet0/0, FastEthernet1/0, FastEthernet1/1 e FastEthernet2/1. O router ID foi manualmente atribuído com o endereço da interface de loopback (1.1.1.1). O comando **show mpls ldp discovery** mostra que P1 estabeleceu adjacências LDP com os seguintes vizinhos:

- P2 (LDP ID: 2.2.2.2:0)
- P3 (LDP ID: 3.3.3.3:0)
- P4 (LDP ID: 4.4.4.4:0)
- PE1 (LDP ID: 10.10.10.10:0)

Estas adjacências validam que o roteador P1 está apto a comutar pacotes MPLS com os seus vizinhos, em conformidade com a topologia da rede.

```
P1#sh mpls forwarding-table
Local  Outgoing    Prefix           Bytes tag  Outgoing    Next Hop
tag    tag or VC   or Tunnel Id     switched   interface
16     Pop tag     2.2.2.2/32       0          Fa0/0       10.1.0.1
17     Pop tag     3.3.3.3/32       54         Fa1/0       10.0.0.2
18     Pop tag     4.4.4.4/32       0          Fa2/1       10.5.0.1
19     Pop tag     10.2.0.0/30      0          Fa2/1       10.5.0.1
       Pop tag     10.2.0.0/30      0          Fa1/0       10.0.0.2
20     Pop tag     10.3.0.0/30      0          Fa2/1       10.5.0.1
       Pop tag     10.3.0.0/30      0          Fa0/0       10.1.0.1
21     Pop tag     10.4.0.0/30      0          Fa0/0       10.1.0.1
       Pop tag     10.4.0.0/30      0          Fa1/0       10.0.0.2
22     Pop tag     10.10.10.10/32   572        Fa1/1       10.10.0.1
23     Pop tag     10.20.0.0/30     0          Fa1/1       10.10.0.1
       Pop tag     10.20.0.0/30     0          Fa1/0       10.0.0.2
24     Pop tag     10.30.0.0/30     0          Fa0/0       10.1.0.1
25     Pop tag     10.40.0.0/30     0          Fa2/1       10.5.0.1
26     26          20.20.20.20/32   0          Fa0/0       10.1.0.1
27     27          30.30.30.30/32   0          Fa2/1       10.5.0.1
P1#
```

Fig. 13. Tabela de encaminhamento MPLS do roteador P1

Na figura 13, o comando **show mpls forwarding-table** revela a *Label Forwarding Information Base* (LFIB) do roteador P1.

A maioria das entradas apresenta a ação *Pop Tag*, o que indica que P1 atua como *penultimate hop*, removendo a label antes de entregar o pacote ao *Egress PE* (função conhecida como *Penultimate Hop Popping – PHP*).

As exceções são os seguintes prefixos:

- 20.20.20.20/32 (label 26)
- 30.30.30.30/32 (label 27)

Nestes casos em particular, a label é mantida pois P1 não é o penúltimo salto para os destinos em PE2 e PE3, respetivamente, como observado na topologia (figura 9).

Este comportamento confirma que o roteador P1 está corretamente configurado como roteador de *backbone* (*P-router*), encarregado da comutação de *labels*, enquanto os roteadores de borda (PE) são responsáveis pela inserção e remoção das *labels* nos limites da rede MPLS.

B. VRF e iBGP nos PEs

No roteador PE1, à semelhança de outros PEs, foram configuradas duas VRFs, uma para cada cliente.

```
PE1#sh run | s vrf
ip vrf AMAZON
 rd 10003:20
 route-target export 10003:100
 route-target import 10003:100
ip vrf MICROSOFT
 rd 10002:10
 route-target export 10002:100
 route-target import 10002:100
 ip vrf forwarding AMAZON
 ip vrf forwarding MICROSOFT
 address-family ipv4 vrf MICROSOFT
 address-family ipv4 vrf AMAZON
PE1#
```

Fig. 14. Configuração VRFs PE1

É possível verificar na figura 14, que a VRF AMAZON está definida com o *route distinguisher* 10003:20 e utiliza o *route-target* 10003:100 para importação e exportação de rotas.

Já a VRF MICROSOFT tem o *route distinguisher* 10002:10 e utiliza o *route-target* 10002:100. Assim sendo, cada cliente mantém uma tabela de roteamento isolada que garante uma separação lógica do tráfego.

Foram também criadas *address-families* do tipo ipv4 para ambas as VRFs, permitindo a troca de rotas IPv4 entre os PEs através de MP-BGP.

```
PE1#sh run | s bgp
router bgp 10000
 no synchronization
 bgp router-id 10.10.10.10
 bgp log-neighbor-changes
 neighbor 20.20.20.20 remote-as 10000
 neighbor 20.20.20.20 update-source Loopback0
 neighbor 30.30.30.30 remote-as 10000
 neighbor 30.30.30.30 update-source Loopback0
 no auto-summary
 !
 address-family vpnv4
 neighbor 20.20.20.20 activate
 neighbor 20.20.20.20 send-community extended
 neighbor 30.30.30.30 activate
 neighbor 30.30.30.30 send-community extended
 exit-address-family
 !
 address-family ipv4 vrf MICROSOFT
 neighbor 10.102.0.2 remote-as 10003
 neighbor 10.102.0.2 activate
 no auto-summary
 no synchronization
 exit-address-family
 !
 address-family ipv4 vrf AMAZON
 neighbor 10.101.0.2 remote-as 10002
 neighbor 10.101.0.2 activate
 no auto-summary
 no synchronization
 exit-address-family
PE1#
```

Fig. 15. Configuração VPNv4 PE1

A figura 15 mostra a configuração feita no roteador PE1 no que concerne o BGP. O *router-id* utilizado é o 10.10.10.10. É possível verificar que foram estabelecidas sessões BGP com dois roteadores PE2 e PE3, com router ID 20.20.20.20 e 30.30.30.30, respetivamente. Todos estes roteadores pertencem ao mesmo ASN 10000.

Estas vizinhanças foram configuradas com a opção **update-source Loopback0**, garantindo estabilidade na comunicação BGP entre os PEs. O **address-family vpnv4** está ativo para ambas as vizinhanças, com a opção **send-community extended**, que permite o transporte de *route-targets*.

Adicionalmente, há sessões BGP configuradas para cada VRF:

- Para a VRF MICROSOFT, a vizinhança é com o IP 10.102.0.2, com ASN 10003.
- Para a VRF AMAZON, a vizinhança é com o IP 10.101.0.2, com ASN 10002.

```
PE1#sh ip vrf
  Name                             Default RD          Interfaces
  AMAZON                           10003:20            Fa0/0
  MICROSOFT                        10002:10            Fa1/0
PE1#
```

Fig. 16. VRF dos clientes associada as interfaces do PE1

A associação das interfaces às respetivas VRFs é apresentada na figura 16. A interface FastEthernet0/0 está atribuída à VRF AMAZON, enquanto a interface FastEthernet1/0 está

atribuída à VRF MICROSOFT. Esta separação física permite a ligação dos CE1 e CE2 respetivamente.

```
PE1#sh ip route vrf AMAZON

Routing Table: AMAZON
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/30 is subnetted, 1 subnets
C       10.101.0.0 is directly connected, FastEthernet0/0
B    192.168.0.0/24 [20/0] via 10.101.0.2, 04:03:59
B    192.168.1.0/24 [200/0] via 20.20.20.20, 04:03:42
```

Fig. 17. Tabela de roteamento VRF AMAZON no PE1

A figura 17 apresenta a tabela de rotas da VRF AMAZON. Nela podemos observar que:

- A sub-rede 10.101.0.0/30 está diretamente conectada à interface Fa0/0.
- A rede 192.168.0.0/24 é alcançável via o endereço 10.101.0.2 (CE1).
- A rede 192.168.1.0/24 é alcançável via o endereço 20.20.20.20 (PE2).

As duas últimas redes, assinaladas com o código “B”, são rotas que foram propagadas através do protocolo BGP com suporte a VPNv4 (MP-BGP). Não é possível visualizar a rede 10.102.0.0/30 pois ela pertence à tabela de rotas da VRF MICROSOFT.

```
PE1#sh bgp vpnv4 unicast all summary
BGP router identifier 10.10.10.10, local AS number 10000
BGP table version is 9, main routing table version 9
4 network entries using 548 bytes of memory
4 path entries using 272 bytes of memory
7/4 BGP path/bestpath attribute entries using 868 bytes of memory
2 BGP AS-PATH entries using 48 bytes of memory
2 BGP extended community entries using 48 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 1784 total bytes of memory
BGP activity 4/0 prefixes, 4/0 paths, scan interval 15 secs

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.101.0.2      4 10002     257     257        9    0    0 04:13:17        1
10.102.0.2      4 10003     257     257        9    0    0 04:13:23        1
20.20.20.20     4 10000     256     257        9    0    0 04:12:52        1
30.30.30.30     4 10000     256     257        9    0    0 04:12:54        1
PE1#
```

Fig. 18. Resumo de todos os vizinhos BGP que trocam rotas VPNv4 com PE1

A figura 18 apresenta um resumo do estado das sessões BGP para o *address-family VPNv4*. Todas as sessões estão ativas e estabelecidas.

- 10.101.0.2 e 10.102.0.2 referem-se às VRFs (AMAZON e MICROSOFT, respetivamente).
- 20.20.20.20 e 30.30.30.30 referem-se aos PEs que trocam rotas VPNv4.

```
PE1#sh bgp vpnv4 unicast all
BGP table version is 9, local router ID is 10.10.10.10
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 10002:10 (default for vrf MICROSOFT)
*> 192.168.0.0      10.102.0.2               0             0 10003 i
*>i192.168.1.0      30.30.30.30              0    100      0 10003 i
Route Distinguisher: 10003:20 (default for vrf AMAZON)
*> 192.168.0.0      10.101.0.2               0             0 10002 i
*>i192.168.1.0      20.20.20.20              0    100      0 10002 i
PE1#
```

Fig. 19. Detalhes de rotas VPNv4 BGP que PE1 conhece

A figura 19 apresenta as rotas VPNv4 aprendidas via MP-BGP. As rotas estão agrupadas pelos seus respetivos *route distinguishers*:

RD 10002:10 (VRF MICROSOFT):

- Rede 192.168.0.0/24 com next-hop 10.102.0.2
- Rede 192.168.1.0/24 com next-hop 30.30.30.30

RD 10003:20 (VRF AMAZON):

- Rede 192.168.0.0/24 com next-hop 10.101.0.2
- Rede 192.168.1.0/24 com next-hop 20.20.20.20

O código ”i” indica que as rotas foram aprendidas internamente via iBGP.

C. BGP CE1

Na figura 20, observa-se que o roteador CE1-LISBOA está configurado com o protocolo BGP, utilizando o *Autonomous System* (AS) 10002 — o mesmo número de AS configurado na VRF AMAZON do roteador PE1. A vizinhança BGP é estabelecida com o endereço IP 10.101.0.1, correspondente à interface FastEthernet0/0 do PE1.

Para permitir a troca de rotas entre roteadores pertencentes ao mesmo *Autonomous System Number* (ASN), foi utilizado o comando **”allowas-in”**. Este comando permite que o CE aceite rotas que contenham o seu próprio ASN no campo AS-Path, o que é necessário em cenários com VRFs replicando o mesmo ASN em múltiplas filiais de um cliente.

A rede 192.168.0.0/24 é anunciada no BGP através do comando **”network 192.168.0.0”**. Essa configuração torna a rede visível na tabela de rotas da VRF AMAZON, permitindo sua propagação pela rede MPLS e a consequente comunicação entre os diferentes sites do cliente.

```
AMAZON-LISBOA#sh run | s bgp
router bgp 10002
 no synchronization
 bgp log-neighbor-changes
 network 192.168.0.0
 neighbor 10.101.0.1 remote-as 10000
 neighbor 10.101.0.1 allowas-in
 no auto-summary
AMAZON-LISBOA#
```

Fig. 20. BGP configurada no CE1 LISBOA - AMAZON

A figura 21 mostra a tabela de rotas atual do CE1-LISBOA. Estão presentes as seguintes entradas:

- A rede 10.101.0.0/30 está diretamente conectada na interface FastEthernet0/0, representando a ligação física com o PE1.
- A rede 192.168.0.0/24 está diretamente conectada à interface de *loopback*, simulando uma sub-rede local do cliente.
- A rede 192.168.1.0/24 é aprendida através de BGP, com *next-hop* 10.101.0.1(PE1).

Esta última entrada confirma que a comunicação entre *sites* do cliente AMAZON (Lisboa e Porto) está operacional: o CE1-LISBOA recebeu via BGP a rota referente à rede remota 192.168.1.0/24, pertencente ao CE1-PORTO.

```
AMAZON-LISBOA#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/30 is subnetted, 1 subnets
C       10.101.0.0 is directly connected, FastEthernet0/0
C    192.168.0.0/24 is directly connected, Loopback0
B    192.168.1.0/24 [20/0] via 10.101.0.1, 04:58:13
AMAZON-LISBOA#
```

Fig. 21. CE1 LISBOA - AMAZON IP ROUTE

VI. TESTES

Para validar o funcionamento da rede de acordo com os conceitos do MPLS L3 VPN, foram realizados testes de conectividade entre os roteadores de filiais dos clientes AMAZON e MICROSOFT. Utilizou-se o comando **traceroute** para verificar o percurso dos pacotes entre os roteadores CE1-LISBOA e CE1-PORTO da AMAZON, e o comando **ping** para testar a comunicação entre CE2-LISBOA e CE2-COIMBRA da MICROSOFT. Este último teste também permitiu capturar e analisar pacotes ICMP e LDP com o *Wireshark*, observando tanto os *labels* MPLS quanto informações relacionadas ao protocolo LDP. No caso da AMAZON, foi utilizado o comando **"traceroute 192.168.1.1 source lo0**" para observar o caminho percorrido até à interface *loopback* do roteador de destino.

A. Teste de conectividade

Com todos os roteadores em funcionamento e a rede operando sem falhas, foi executado um *traceroute* a partir de CE1-LISBOA para CE1-PORTO, utilizando o comando **"traceroute 192.168.1.1 source lo0"**, mencionado anteriormente. O resultado do caminho percorrido pode ser observado na figura 22. O tráfego parte da rede AMAZON-LISBOA e segue um percurso de cinco *hops*, passando pelos seguintes IPs:

- 10.101.0.1 → 10.20.0.2 → 10.4.0.1 → 10.104.0.2 → 10.104.0.1

correspondendo ao trajeto:

- CE1-LISBOA → PE1 → P3 → P2 → PE2 → CE1-PORTO

```
AMAZON-LISBOA#traceroute 192.168.1.1 source lo0

Type escape sequence to abort.
Tracing the route to 192.168.1.1

  1 10.101.0.1 28 msec 20 msec 16 msec
  2 10.20.0.2 92 msec 92 msec 64 msec
  3 10.4.0.1 84 msec 80 msec 84 msec
  4 10.104.0.2 84 msec 64 msec 64 msec
  5 10.104.0.1 84 msec 80 msec 76 msec
AMAZON-LISBOA#
```

Fig. 22. TRACEROUTE CE1 LISBOA → CE1 PORTO

A topologia que utilizamos foi projetada para ter redundância, permitindo que o tráfego encontre rotas alternativas mesmo em caso de falha de ligações. Para validar essa redundância, foi realizado novamente o *traceroute* entre CE1-LISBOA e CE1-PORTO, com as interfaces FastEthernet2/1 e FastEthernet0/0 do roteador P2 desligadas.

A figura 23 apresenta os resultados desse teste. No primeiro cenário, com apenas a interface FastEthernet2/1 de P2 desligada, o tráfego segue um caminho alternativo CE1-LISBOA → PE1 → P1 → P2 → PE2 → CE1-PORTO, em vez do caminho original mostrado na figura 22.

No segundo cenário, com ambas as interfaces FastEthernet2/1 e FastEthernet0/0 de P2 desligadas, o tráfego segue um novo percurso, agora com seis *hops*: CE1-LISBOA → PE1 → P3 → P4 → P2 → PE2 → CE1-PORTO.

Estes testes demonstram claramente a capacidade de resiliência da rede e a existência de caminhos alternativos válidos para entrega de tráfego entre os pontos do cliente.

```
AMAZON-LISBOA#traceroute 192.168.1.1 source lo0

Type escape sequence to abort.
Tracing the route to 192.168.1.1

  1 10.101.0.1 28 msec 40 msec 24 msec
  2 10.10.0.2 84 msec 96 msec 88 msec
  3 10.1.0.1 88 msec 92 msec 100 msec
  4 10.104.0.2 72 msec 60 msec 64 msec
  5 10.104.0.1 84 msec 104 msec 92 msec
AMAZON-LISBOA#traceroute 192.168.1.1 source lo0

Type escape sequence to abort.
Tracing the route to 192.168.1.1

  1 10.101.0.1 32 msec 24 msec 24 msec
  2 10.20.0.2 108 msec 100 msec 108 msec
  3 10.2.0.1 92 msec 72 msec 100 msec
  4 10.3.0.2 108 msec 92 msec 72 msec
  5 10.104.0.2 96 msec 104 msec 92 msec
  6 10.104.0.1 108 msec 112 msec 108 msec
AMAZON-LISBOA#
```

Fig. 23. TRACEROUTE CE1 LISBOA → CE1 PORTO, P2(F2/1,F0/0) DOWN

A figura 24 mostra o resultado do *traceroute* realizado a partir do roteador CE1-PORTO com destino à interface 192.168.0.1 do CE1-LISBOA. Este teste foi efetuado para verificar o caminho inverso do tráfego entre os roteadores do

cliente AMAZON.
Antes da realização deste teste, as interfaces FastEthernet2/1 e FastEthernet0/0 do P2, anteriormente desligadas, foram novamente ativas.
O percurso seguido neste caso também contempla cinco *hops*:

- 10.104.0.2 → 10.30.0.1 → 10.4.0.2 → 10.101.0.1 → 10.101.0.2

O que corresponde ao caminho inverso do teste inicial:

- CE1-PORTO → PE2 → P2 → P3 → PE1 → CE1-LISBOA

Este resultado confirma que, com a rede completamente operacional, o tráfego percorre simetricamente os dois sentidos entre as filiais da AMAZON.

```
AMAZON-PORTO#traceroute 192.168.0.1 source lo0

Type escape sequence to abort.
Tracing the route to 192.168.0.1

  1 10.104.0.2 24 msec 28 msec 20 msec
  2 10.30.0.1 80 msec 72 msec 68 msec
  3 10.4.0.2 104 msec 88 msec 72 msec
  4 10.101.0.1 56 msec 68 msec 60 msec
  5 10.101.0.2 76 msec 80 msec 92 msec
AMAZON-PORTO#
```

Fig. 24. TRACEROUTE CE1 PORTO → CE1 LISBOA

B. Análise no Wireshark: Protocolo ICMP

Para analisar o comportamento dos pacotes desde a origem na rede do cliente, passando pela entrada e saída da rede MPLS, até à chegada ao roteador do mesmo cliente na outra ponta, foi utilizado o *Wireshark*, uma ferramenta que permite capturar informações de pacotes em interfaces de rede, com base nos protocolos ativados em cada interface.

Para estudar os *labels* utilizados entre os *end-points* do cliente CE2, foi executado um *ping* a partir do roteador CE2-LISBOA para o roteador CE2-COIMBRA, utilizando o comando **"ping 192.168.1.1 source lo0"**. Após a execução bem-sucedida do *ping*, procedeu-se à captura e análise dos pacotes ICMP, interface por interface, com base no caminho identificado pelo *traceroute*, que o pacote percorre desde o CE2-LISBOA até ao CE2-COIMBRA.

A figura 25 mostra a captura do pacote ICMP enviado da interface FastEthernet1/0 do CE2-LISBOA para a interface FastEthernet1/0 do PE1. Como a comunicação entre estas interfaces é realizada através de rotas BGP e estas interfaces não pertencem à rede MPLS, não é possível observar informações de *labels* MPLS nos pacotes capturados neste ponto.

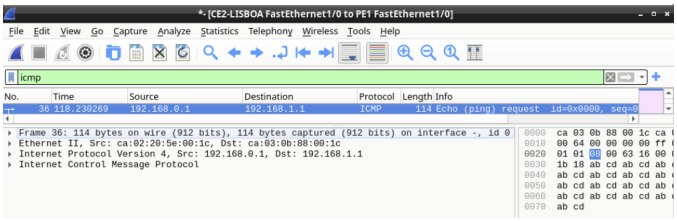

Fig. 25. ICMP CE2-PE1

Quando o pacote entra na interface FastEthernet2/0 do PE1 — já pertencente à rede MPLS — e é encaminhado para a interface FastEthernet2/0 do roteador P3, é possível ver informações do cabeçalho MPLS.

Conforme mostra a figura 26, o roteador PE1 adiciona dois *labels* ao pacote: um identifica o caminho LSP e o outro a VRF (VPN) do cliente. Neste exemplo, o *label* 27 corresponde ao *label* local de encaminhamento atribuído pelo PE1, enquanto o *label* 31 identifica a VPN associada ao cliente CE2.

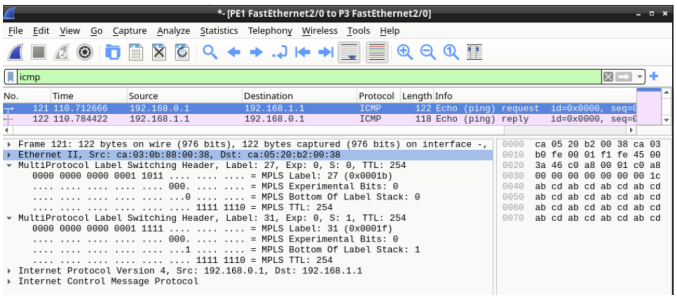

Fig. 26. ICMP PE1-P3

A figura 27 apresenta a captura do mesmo pacote ao transitar da interface FastEthernet0/0 do P3 para a FastEthernet0/0 do P4. Observa-se que os *labels* utilizados pelo P3 são os mesmos aplicados pelo PE1.

A *label* da VPN deve obrigatoriamente permanecer constante durante todo o percurso do pacote entre os pontos do mesmo cliente. Já a *label* de roteamento (*outer label*) pode variar, pois cada roteador MPLS trata os *labels* de forma local. Neste caso, devido à simplicidade do cenário, os *labels* acabaram por se manter iguais.

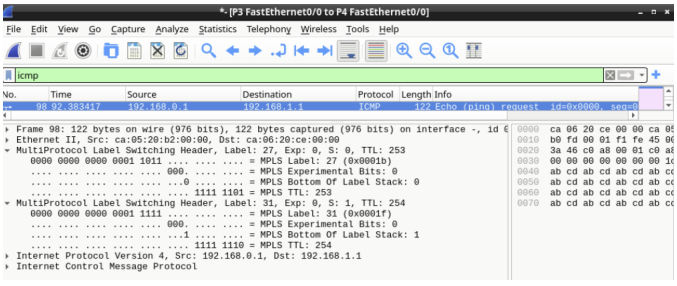

Fig. 27. ICMP P3-P4

Ao receber o pacote, o roteador P4, como ele é o penúltimo salto antes do pacote sair da rede MPLS, executa a operação

Penultimate Hop Popping (PHP), removendo a *outer label* e deixando apenas a *label* da VPN. O pacote é então enviado através da interface FastEthernet1/1 para o roteador PE3, o egress PE, conforme ilustrado na figura 28.

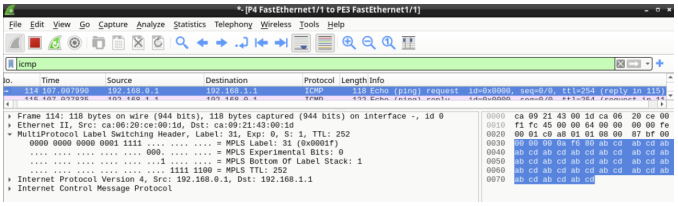

Fig. 28. ICMP P4-PE3

Na figura 29, verifica-se que o pacote enviado da interface FastEthernet1/0 do PE3 para a interface FastEthernet0/0 do CE2-COIMBRA já não contém qualquer informação sobre MPLS. Conforme esperado, estas interfaces não pertencem à rede MPLS, e o roteamento do pacote é efetuado com base na tabela de rotas da VRF, aprendida via BGP.

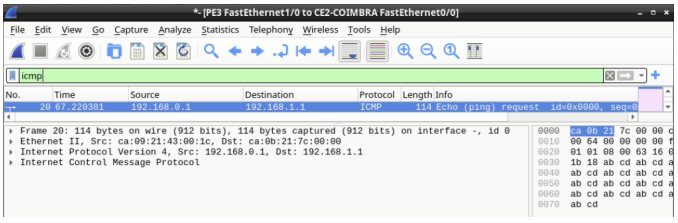

Fig. 29. ICMP P4-PE3

C. Análise no Wireshark: Protocolo LDP

Com o objetivo de verificar o comportamento do protocolo LDP na rede MPLS implementada, capturou-se e analisou-se o tráfego gerado nas várias ligações da topologia, utilizando igualmente o *Wireshark*.

A monitorização incidiu sobre o percurso dos pacotes entre:

- CE2-LISBOA → PE1 → P3 → P4 → PE3 → CE2-COIMBRA

Na ligação entre CE2-LISBOA e PE1, foi aplicado um filtro para visualizar somente pacotes LDP, como apresentado na figura 30.

No entanto, não foi detetado tráfego desse protocolo.

Este comportamento era expectável, uma vez que os roteadores CE não participam no processo de distribuição de *labels*.

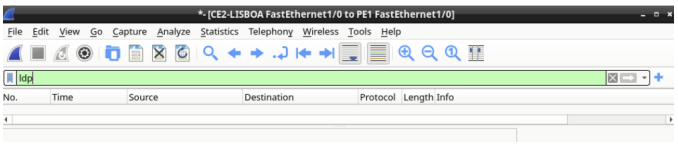

Fig. 30. Tráfego LDP entre CE2-LISBOA e PE1

Na ligação entre PE1 e P3, já dentro do domínio MPLS, foi possível observar a troca de mensagens LDP do tipo "*Hello*" entre os roteadores PE1 e P3, como observado na figura 31.

O tráfego capturado mostra pacotes com origem no IP 10.20.0.1 (PE1) e destino 10.20.0.2 (P3).

A análise detalhada revela o LSR ID do P3 como 3.3.3.3, além de parâmetros como o tempo de manutenção (*hold time*), o endereço de transporte IPv4 e informações da sessão.

Esta troca estabelece a descoberta de vizinhos LDP, sendo essencial para a formação das sessões e subsequente distribuição de etiquetas.

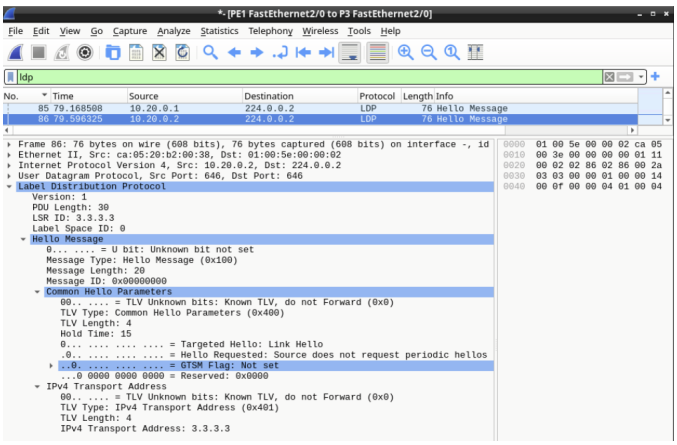

Fig. 31. Tráfego LDP entre PE1 e P3

A comunicação entre os roteadores P3 e P4 segue o mesmo padrão, com o envio de pacotes *LDP Hello* por *multicast* para o endereço 224.0.0.2, utilizado para descoberta de vizinhos (fig. 32).

O LSR ID do P4 foi identificado como 4.4.4.4, confirmando que ambos os roteadores estão devidamente configurados e participam ativamente na distribuição de *labels* no *core* da rede MPLS.

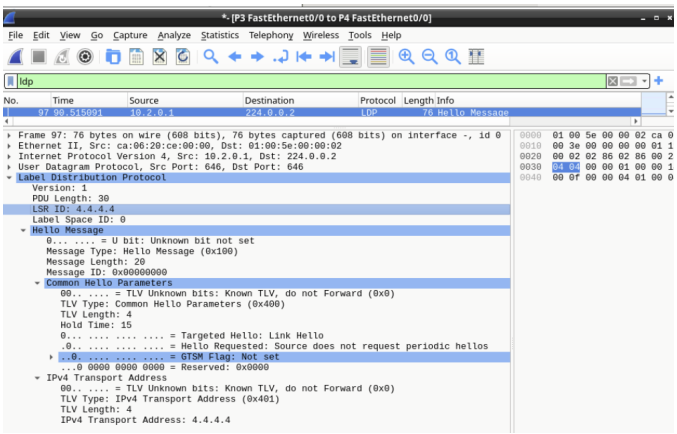

Fig. 32. Tráfego LDP entre P3 e P4

Na comunicação entre P4 e PE3, dentro do domínio MPLS, o tráfego LDP mantém-se ativo, observado pela troca de mensagens, mantendo os mesmos parâmetros verificados anteriormente (fig. 33).

Este comportamento demonstra que o roteador PE3 está corretamente configurado e estabelece sessões LDP com o seu vizinho direto, permitindo a comutação de etiquetas.

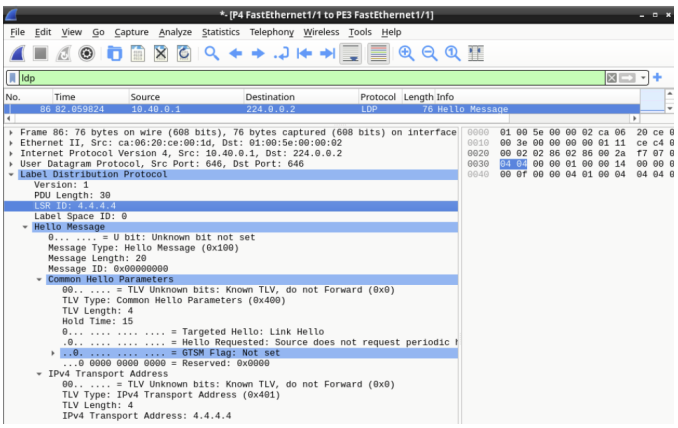

Fig. 33. Tráfego LDP entre P4 e PE3

Por último, tal como na ligação entre CE2-LISBOA e PE1, não foi detetado qualquer tráfego LDP entre PE3 e CE2-COIMBRA. Esta ausência reforça o princípio de que os roteadores CE não participam ao nível do control plane do MPLS, não estabelecendo sessões LDP, uma vez que não necessitam de comutar etiquetas.

Esta análise confirma que o protocolo LDP foi corretamente estabelecido entre todos os roteadores do domínio MPLS (PE e P), permitindo a criação dos *Label Switched Paths* (LSPs).

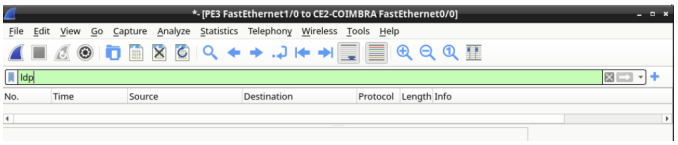

Fig. 34. Tráfego LDP entre PE3 e CE2-COIMBRA

VII. CONCLUSÃO

A tecnologia MPLS, quando combinada com L3 VPN, oferece uma solução escalável e eficiente para o encaminhamento de tráfego ponto a ponto entre diferentes clientes. A simulação de uma rede MPLS com L3 VPN demonstrou a robustez e a eficiência dessa abordagem, mesmo em cenários com múltiplos clientes e sobreposição de endereços IP. O uso de VRFs, MP-BGP e LDP permitiu isolar o tráfego de forma segura e escalável.

Um dos pontos fortes observados no projeto foi o balanceamento de carga no core MPLS, possibilitado pela topologia em malha dos roteadores do backbone e pela utilização do OSPF como protocolo de roteamento interno. Essa arquitetura contribuiu para uma distribuição eficiente do tráfego.

No entanto, apesar de seus benefícios, o MPLS apresenta desafios, como a complexidade de configuração e operação, além de uma certa rigidez diante de ambientes altamente dinâmicos e com rápidas mudanças.

Nesse contexto, tecnologias emergentes como o SD-WAN por exemplo surgem como alternativas mais ágeis, programáveis e orientadas a aplicações, oferecendo maior flexibilidade, redução de custos e facilidade de gerenciamento para redes corporativas distribuídas.

REFERÊNCIAS

[1] U. S. Bashir and E. R. K. Gurm, "Comparative Analysis of MPLS Layer 3 VPN and MPLS Layer 2 VPN," *International Journal of Computer Science Trends and Technology (IJCST)*, vol. 3, pp. 7–13, 2015.

[2] K. Alqamoudi, M. Alqamoudi, M. Ghretli and B. Khamoudi, "Multiprotocol Label Switching Layer 3 VPN Solution for Libyan Oil Company," presented at the *International Conference on Emerging Trends in Computing and Information Sciences*, 2022.

[3] R. Chandra, T. J. Bates, Y. Rekhter and D. Katz, "RFC 4760: Multiprotocol Extensions for BGP-4," Internet Engineering Task Force (IETF), Jan. 2007. [Online]. Available: https://datatracker.ietf.org/doc/html/rfc4760

[4] E. Rosen and Y. Rekhter, "RFC 2547: BGP/MPLS VPNs," Internet Engineering Task Force (IETF), Mar. 1999. [Online]. Available: https://datatracker.ietf.org/doc/html/rfc2547

[5] Y. Rekhter and E. C. Rosen, "RFC 4364: BGP/MPLS IP Virtual Private Networks (VPNs)," Internet Engineering Task Force (IETF), Feb. 2006. [Online]. Available: https://datatracker.ietf.org/doc/rfc4364/

[6] J. Jimenez, "Configure a Basic MPLS VPN Network," Cisco, 10-Dec-2001. [Online]. Available: https://www.cisco.com/c/en/us/support/docs/multiprotocol-label-switching-mpls/mpls/13733-mpls-vpn-basic.html