Bruna Rafaela
Ramos Pires

Estudo de Tecnologias para Redes de Datacenter

Study of Technologies for Datacenter Networks

Universidade de Aveiro
2023

Bruna Rafaela Ramos Pires

Estudo de Tecnologias para Redes de Datacenter

Study of Technologies for Datacenter Networks

Dissertação apresentada à Universidade de Aveiro para cumprimento dos requisitos necessários à obtenção do grau de Mestre em Engenharia Eletrónica e Telecomunicações, realizada sob a orientação científica do Doutor António Manuel Duarte Nogueira, Professor auxiliar do Departamento de Eletrónica, Telecomunicações e Informática da Universidade de Aveiro.

Aos meus pais, que sempre me deram tudo, e não permitiram que desistir fosse uma opção.

o júri / the jury

presidente / president

Prof. Doutor José Manuel Matos Moreira
professor auxiliar da Universidade de Aveiro

vogais / examiners committee

Prof. Doutor Leonel Filipe Simões Santos
professor coordenador no Instituto Politécnico de Leiria - Escola Superior de Tecnologia e Gestão, no Departamento de Engenharia Informática

Prof. Doutor António Manuel Duarte Nogueira
professor auxiliar da Universidade de Aveiro

agradecimentos / acknowledgements

Gostaria de expressar profundos agradecimentos a todos que contribuíram para o meu percurso académico e, em especial:

Aos meus pais, neste momento de celebração e conquista, é com uma gratidão imensurável que dedico uma parte significativa deste agradecimento a vocês, os pilares inabaláveis que sustentaram cada passo do meu percurso académico. Reconheço que este sucesso é, em grande parte, resultado do vosso amor, orientação e valores incutidos em mim ao longo dos anos. Cada sacrifício feito em prol da minha educação não foi em vão, e hoje celebro não apenas a minha realização, mas também a dedicação exemplar dos meus pais. Vocês são a base sólida sobre a qual construí o meu percurso académico, e a vossa influência transcende o contexto educativo, moldando a pessoa que me tornei. Este marco não é apenas meu, mas também de vocês, que partilharam esta etapa comigo.

Agradeço também à minha avó Irene, que sempre me questionava ansiosamente sobre a "minha neta Engenheira" — hoje, avó, estou a um passo de concretizar esse sonho.

À minha família como um todo, pela presença constante e encorajamento.

À Patrícia, quero agradecer pelo apoio inestimável, pela generosa ajuda, por sempre confiar em mim, pela presença constante em todos os momentos, pela incrível pessoa que é e por ter contribuído para o meu crescimento pessoal.

À Inês, agradeço pelos valiosos conselhos, pelas sessões de estudo e pelo apoio constante que tornaram estes anos de curso mais leves.

Ao Willy, que dedicou horas a explicar-me eletrónica.

Ao Gui, pela partilha de conhecimento.

Ao João Francisco, pela presença nos momentos cruciais.

Ao professor António Nogueira, é com profunda gratidão que me dirijo a si neste momento especial da conclusão da minha dissertação. Gostaria de expressar o meu sincero apreço pelo seu apoio incansável e pela compreensão valiosa que me proporcionou ao longo desta etapa desafiadora. Desde o início, a sua orientação foi fundamental para o sucesso desta dissertação. A sua disponibilidade para esclarecer dúvidas, a paciência demonstrada face aos desafios e a dedicação incansável foram verdadeiramente inspiradoras.

Ao meu avô, que sempre se interessava pelo meu percurso académico. Embora não estejas presente para testemunhar este momento, espero que estejas orgulhoso.

Ao Duarte, pelos dois anos de alegria constante e por ensinar-me a encarar a vida com um sorriso, mesmo nas adversidades. Infelizmente, não estás cá para presenciar este dia importante, mas espero que estejas igualmente orgulhoso.

Cada uma destas pessoas, mencionadas de forma especial, partilhou algo em comum: inspiraram-me a ser uma pessoa melhor, uma profissional mais dedicada e a perseguir os meus objetivos com determinação.

Obrigada a todos!

Palavras Chave

Datacenter, Virtualização, Rede Local Extensível Virtual, Rede *Ethernet* Privada Virtual, Rede Definida por *Software*.

Resumo

A presente dissertação tem como objetivo estudar tecnologias relevantes para redes de *datacenter*. Inicia com uma introdução que destaca a motivação, objetivos e estrutura do documento. Em seguida, o enquadramento teórico explora a evolução das redes de computadores, abrangendo conceitos desde os primórdios da conectividade até aos desafios de escalabilidade e eficiência. O enfoque é nas redes locais, com especial atenção na necessidade de segmentação. Seguidamente, são analisadas as redes locais virtuais, o isolamento lógico e a sua aplicação em *datacenters*. Para além disso, são abordadas as *overlay networks*, realçando a flexibilidade e escalabilidade que oferecem. O documento aborda a integração com tecnologias emergentes, as tendências em redes definidas por *software*, a eficiência energética, a sustentabilidade, a segurança em redes de *datacenter*, bem como a influência que a inteligência artificial poderá ter no desempenho destas infraestruturas. Em termos de implementação prática, a dissertação concentra-se na construção de redes utilizando as tecnologias *Virtual eXtensible Local Area Network* (VXLAN) e *Layer 2 Virtual Private Network*/*Ethernet Virtual Private Network* (L2VPN/EVPN) com transporte VXLAN. A integração do protocolo EVPN-VXLAN numa infraestrutura empresarial é detalhada, juntamente com a recolha de informações sobre o desempenho destas redes. Os resultados do estudo serão apresentados nos capítulos finais, incluindo uma análise das simulações realizadas e conclusões relevantes. O trabalho conclui com uma reflexão sobre as limitações do estudo e perspetivas de trabalho futuro. Esta dissertação pretende proporcionar uma visão abrangente das tecnologias essenciais para as atuais redes de *datacenter*, abordando tanto os aspetos teóricos quanto práticos, com foco na eficiência, escalabilidade e segurança das redes de *datacenter* num ambiente de constante evolução.

Keywords

Datacenter, Virtualisation, Virtual eXtensible Local Area Network, Ethernet Virtual Private Network, Software-Defined Networking.

Abstract

This dissertation is focused on studying relevant technologies for datacenter networks. It starts with an introduction that highlights the motivation, objectives, and document structure. Subsequently, the theoretical framework explores the evolution of computer networks, encompassing concepts from the early days of connectivity to the challenges of scalability and efficiency. The emphasis is put on Local Networks (LANs), with a special focus on the need for segmentation. The concepts of Virtual Local Networks (VLANs) and logical isolation are explored, together with their application in datacenter scenarios. Furthermore, the work addresses overlay networks, emphasizing the flexibility and scalability they provide. Then, the document explores the integration with emerging technologies, trends in Software-Defined Networking (SDN), energy efficiency, sustainability, security, and the influence of Artificial Intelligence (AI) in datacenter networks. The practical part of the dissertation work is centered on building networks using Virtual eXtensible Local Area Network (VXLAN) and Layer 2 Virtual Private Network/Ethernet Virtual Private Network (L2VPN/EVPN) technologies with VXLAN transport. The integration of the EVPN-VXLAN protocol into a corporate infrastructure is detailed, along with the collection of information on network performance. The study results are presented in the last chapters, including an analysis of the conducted simulations and conclusions based on the obtained results. The work concludes with a reflection on the study's limitations and prospects for future work. This dissertation provides a comprehensive view of essential technologies for datacenter networks, addressing both theoretical and practical aspects, with a focus on efficiency, scalability, and security in the ever-evolving datacenter environment.

Conteúdo

Lista de Figuras

Siglas

4G Fourth Generation. 7

5G Fifth Generation. 4, 7

ANACOM Autoridade Nacional de Comunicações. 5

ARPA Advanced Research Projects Agency. 4

AS Autonomous System. 47–49

AWS Amazon Web Services. 22

BGP Border Gateway Protocol. 3, 47–49, 51–53, 57, 58

CE Customer Edge. 52

COTS Commercial-Off-The-Shelf. 30

CPU Central Processing Unit. 7

DCGW Datacenter Gateway. 20

DE-CIX Deutscher Commercial Internet Exchange. 5

EH-WSN Energy-Harvesting Wireless Sensor Network. 31

EVPN Ethernet Virtual Private Network. 2, 3, 25, 26, 44, 47–53, 55, 56, 60, 61

GB Gigabyte. 5

GDPR Regulamento Geral sobre a Proteção de Dados. 33

GEE Gases com Efeito de Estufa. 31, 32

GNS3 Graphical Network Simulator-3. 2

GPU Graphics Processing Unit. 7

HCI Hyper Converged Infrastructure. iii, 20, 21

HIPAA Lei de Portabilidade e Responsabilidade do Seguro de Saúde. 33

HPC High-performance computing. 14

I/O Input/Output. 21

IA Inteligência Artificial. 7, 14, 30, 34, 35, 61

IaaS Infrastructure as a service. 14

IAM Identity and Access Management. 33

IBM Internacional Business Machines Corporation. 1, 22

IDS Intrusion Detection System. 32

IEEE Institute of Electrical and Electronics Engineers. 8

IoT Internet of Things. 5, 7

IP Internet Protocol. 33

IPS Intrusion Protection System. 33

IPv4 Internet Protocol version 4. 45

L2VPN Layer 2 Virtual Private Network. 2, 3, 44, 48, 50–52, 55, 56

LAN Local Area Network. 8, 9, 11, 25, 26, 60

MAC Media Access Control. 36

ML Machine Learning. 7, 14, 30, 31, 34

Net Network. 4

NFV Virtualização de Funções de Rede. 30

NIDS Network-based Intrusion Detection System. 32

Ofcom Office of Communications. 6

OSI Open System Interconnection. 8

OSPF Open Shortest Path First. iii, 25, 37, 38, 43, 45–47

PDOs Pulsing Denial of Service. 34

PE Provider Edge. iii, 37, 38, 40, 43, 44, 46–49, 52, 53

QoE Quality of Experience. 31

QoS Quality of Service. 10, 31

RF Radiofrequência. 6

SAN Storage Area Network. 21

SDN Software Defined Network. i, 26–28, 31, 60, 61

SPB Shortest Path Bridging. 19

STP Spanning Tree Protocol. 18, 19, 36

TCP Transmission Control Protocol. 34

TI Tecnologia da Informação. 1, 5, 13

TIC Tecnologias de Informação e Comunicação. 31

ToR Top-of-Rack. 15

Trill Transparent Interconnection of Lots of Links. 19

UDP User Datagram Protocol. 57

VIF Virtual Interface. 43

VLAN Virtual Local Area Network. 11, 12, 25, 36, 37, 60

VM Virtual Machine. 16, 19, 25, 29, 30, 34, 36, 54

VNI Virtual Network Identifier. 25, 29, 43, 51

VPLS Virtual Private LAN Services. 51, 52

VPN Virtual Private Network. 24, 25, 33, 44, 47, 48, 50

VTEP VxLAN Tunnel End Point. 28, 29

VXLAN Virtual eXtensible Local Area Network. iii, 2, 3, 20, 24, 25, 28, 29, 36, 37, 44, 47, 49–51, 54–56, 60, 61

WAN Wide-Area Network. 9, 24

Capítulo 1

Introdução

O aparecimento dos *datacenters* remonta à década de 1960, quando a empresa *Internacional Business Machines Corporation* (IBM) lançou o primeiro *mainframe* da Série *System/360*. Este acontecimento é considerado um marco fundamental na evolução da computação empresarial.

A Série *System/360* não introduziu apenas uma nova geração de *mainframes*, "o compartimento que aloca o processador central e a memória principal" [1], mas também sinalizou uma transição significativa na forma como as organizações abordavam a gestão e o processamento de dados em larga escala. Estes *mainframes* eram projetados para responder à crescente procura de capacidade de processamento, escalabilidade e flexibilidade, representando um avanço significativo na infraestrutura de Tecnologia da Informação (TI) da época. À medida que os sistemas computacionais se tornaram mais poderosos e as necessidades de processamento de dados intensivos cresceram, surgiu a necessidade de criar ambientes centralizados e dedicados para albergar esses sistemas.

Ao longo das décadas seguintes, houve uma grande evolução no número e complexidade dos serviços de comunicação, com o consequente aumento exponencial da quantidade de dados que se tornou necessário manipular e guardar. Atualmente, à medida que a computação se tem deslocado progressivamente para a nuvem, os *datacenters* têm desempenhado um papel cada vez mais importante no suporte às redes empresariais e aos serviços de computação em nuvem, tais como cálculos em larga escala, pesquisa *web*, jogos *online*, redes sociais, entre outros. Estes serviços são tipicamente fornecidos por *datacenters* partilhados, uma vez que a manutenção dos seus equipamentos físicos (servidores, dispositivos de rede, sistemas de arrefecimento, sistemas de iluminação, etc) é muito dispendiosa. As redes de *datacenter* que interligam os servidores são fundamentais para fornecer serviços de elevado desempenho e fiabilidade: de facto, todos os recursos do *datacenter* devem trabalhar de forma orquestrada, o que só pode ser atingido através de uma aproximação holística ao projeto e implementação da infraestrutura.

1.1 Motivação

Numa era fortemente marcada pela revolução digital, os *datacenters* destacam-se como a base que suporta a infraestrutura tecnológica atual, impulsionando e dando margem para constantes inovações, para além de possuírem a capacidade de sustentar o crescente e infindável fluxo de dados.

O projeto de *datacenters* tem recebido cada vez mais interesse por parte da academia e da indústria devido à sua crescente importância no suporte e sustentabilidade de uma vasta gama de aplicações, incluindo motores de busca (como o *Google* e o *Bing*), plataformas de distribuição de vídeo (*YouTube*, *Netflix*, entre outras), redes sociais (*Facebook*, *Twitter*, etc), e computação em larga escala (*data mining*, bio-informática, indexação).

Esta dissertação visa estudar o complexo ecossistema das tecnologias para redes de *datacenter*, procurando compreender os mecanismos que garantem a sua eficiência, escalabilidade e segurança. Começando por uma resenha histórica dos primórdios da conectividade e terminando nas tendências mais avançadas, este trabalho pretende analisar, recorrendo a cenários realistas, as tecnologias e os protocolos mais recentes que têm vindo a permitir a constante evolução destas infraestruturas.

1.2 Objetivos e metodologia

Este estudo tem como objetivo principal analisar e compreender as diferentes tecnologias que têm vindo a ser utilizadas no contexto das redes de *datacenter*, procurando dessa forma identificar todas as funcionalidades e capacidades que é possível obter neste tipo de infraestruturas de comunicação.

Nesse sentido, o trabalho começará por fazer um levantamento detalhado dos diferentes tipos de redes de *datacenter* e das tecnologias mais utilizadas, passando depois a explorar as vantagens da utilização dessas tecnologias através da implementação de cenários práticos realistas que permitam demonstrar a eficiência das soluções adotadas.

De uma forma sucinta, os principais objetivos da presente dissertação de mestrado podem ser enumerados da seguinte forma:

- Recolher informação pertinente sobre todos os conceitos que se mostrem relevantes para o estudo, tais como: tipologias de rede, redes virtuais, segurança nas redes virtuais, entre outros;
- Criar três cenários práticos, com recurso ao emulador *Graphical Network Simulator-3* (GNS3), que permitam integrar as tecnologias de *datacenter* mais utilizadas nas modernas implementações: a tecnologia *Virtual eXtensible Local Area Network* (VXLAN), a tecnologia *Layer 2 Virtual Private Network* (L2VPN)/*Ethernet Virtual Private Network* (EVPN)

e um cenário final que permitirá estudar as vantagens de integrar estas duas tecnologias com o protocolo *Border Gateway Protocol* (BGP).

- Realizar testes e recolher os dados necessários para comprovar as vantagens e eventuais desvantagens dos cenários estudados;
- Proceder à análise dos dados recolhidos, tendo em conta toda a fundamentação teórica;
- Concluir o estudo através da elaboração de um cenário final de integração das três tecnologias de *datacenter* estudadas ao longo desta dissertação: VXLAN, L2VPN/EVPN e BGP.

1.3 Estrutura do documento

O documento encontra-se dividido em quatro capítulos: Introdução, Enquadramento teórico, Implementação prática e Conclusão.

O primeiro capítulo pretende contextualizar o tema e identificar o principal propósito deste estudo.

Segue-se o Enquadramento teórico, que concentra toda a fundamentação teórica que serviu de base para o desenvolvimento desta dissertação. Nesse sentido, foi elaborada uma revisão bibliográfica dos conceitos mais relevantes no âmbito do trabalho que se pretende realizar.

No capítulo seguinte, a Implementação prática, são incluídos os três cenários experimentais desenvolvidos para desta dissertação: uma rede baseada na tecnologia VXLAN, uma segunda rede baseada na tecnologia L2VPN/ EVPN com transporte por VXLAN e, por último, um cenário com a integração destas diferentes tecnologias. Será ainda feita a recolha e verificação de dados relativos ao desempenho dos diferentes cenários bem como a comparação dos dados recolhidos e elaboração das conclusões relevantes.

O último capítulo, agrega algumas considerações finais, quais as limitações encontradas no estudo realizado, o que se pode considerar como contribuição deste trabalho e quais as perspetivas de trabalho futuro no âmbito deste tema.

Capítulo 2

Enquadramento teórico

O segundo capítulo desta dissertação tem como finalidade sistematizar um conjunto de conceitos e a informação recolhida sobre a temática que constitui o objeto de estudo, as redes de *datacenter*.

2.1 Introdução

A necessidade de superar os obstáculos que lhe são impostos *à priori* e o desejo permanente de comunicação são características intrínsecas do ser humano. A invenção do telégrafo, em 1857, revolucionou a forma de comunicar a grandes distâncias, uma vez que possibilitou a troca de informação entre continentes de um modo muito mais célere. No entanto, foi a invenção do telefone, em 1876, que despoletou a verdadeira evolução na era das Telecomunicações, já que tornou viável a transmissão de voz em tempo real, ligando pessoas como nunca antes havia sido feito.

Ao longo do século XX, a evolução nas tecnologias de comunicação foi bastante rápida. Foram introduzidos sistemas de transmissão de rádio e televisão, sistemas de comutação automatizada, para além do aparecimento da Internet. A *Advanced Research Projects Agency* (ARPA) *Network* (Net), conjeturada para interligar os diferentes pólos do Departamento da Defesa dos Estados Unidos da América, na década de 1960, constituiu a primeira rede de computadores baseada na comutação de pacotes e pode ser considerada como o protótipo da Internet. Seguiu-se o desafio de alargar o acesso a cidadãos individuais, que culminou em grandes avanços no que respeita à escalabilidade e eficiência da rede [2].

Recentemente, a sociedade tem-se tornado gradualmente mais digital, sustentada numa ampla gama de serviços, cada vez mais exigentes. Tecnologias como o *Fifth Generation* (5G), a fibra ótica, a massificação dos dispositivos móveis e o aparecimento de sensores e múltiplos dispositivos inteligentes interligados podem ser considerados como a base para novos patamares de conectividade.

2.2 Desafios de escala e eficiência

Com o crescente aumento do número de dispositivos e utilizadores ligados, tornou-se imperativo dimensionar as redes por forma a garantir as condições de escalabilidade e eficiência necessárias para um padrão adequado de qualidade.

Atualmente, o aumento no número de dispositivos é fruto de uma mudança de paradigma na área da TI, denominada *Internet of Things* (IoT), que se pode definir como: "*Uma rede aberta e extensa de objetos inteligentes com a capacidade de se auto-organizarem, partilharem informações, dados e recursos, reagindo e agindo perante situações e alterações no ambiente*" [3].

As redes devem, assim, ser projetadas para crescer de uma forma eficiente e sustentada, sem nunca comprometer o seu desempenho.

Devido ao aumento da complexidade dos sistemas e à expansão da computação, surgiram desafios bastante significativos no que respeita à escala e eficiência das redes, tais como:

- **Aumento do volume de dados:** A exposição global à pandemia COVID-19 veio evidenciar, de uma forma mais vincada, o aumento do tráfego de dados em contexto digital. Depois de anunciada a segunda vaga da pandemia, um novo recorde foi alcançado no nó de interligação *Deutscher Commercial Internet Exchange* (DE-CIX) em Frankfurt, onde a 3 de novembro (de 2020) houve um pico de 10 Terabits por segundo [4]. Os valores referidos representam um aumento homólogo de 40%, e ilustram a magnitude do crescimento da geração de dados e do consumo na Europa. Considerando uma escala global, em 2020, bilhões de dispositivos IoT geraram 507,5 zettabytes de dados [5].

  Esta variação no tráfego de dados ainda se faz sentir atualmente, mais especificamente no panorama português, uma vez que, segundo a Autoridade Nacional de Comunicações (ANACOM), no primeiro semestre do presente ano, verificou-se um aumento (em relação ao período homólogo) de vários indicadores no que respeita a serviços móveis, tais como:

  - + 1,8% de telemóveis, o que totaliza 12,8 milhões de telemóveis;
  - + 6,5% de telemóveis com acesso à Internet, o que representa 9,4 milhões de telemóveis com acesso à Internet
  - + 2,6% de serviço telefónico móvel, o que significa que, por cada 100 habitantes, existem 130 serviços telefónicos móveis;
  - + 37,9% em tráfego médio mensal com recurso a banda larga móvel, rondando os 10 *Gigabyte* (GB) por mês [6].

- **Latência e tempo real:** A transmissão de quantidades tão grandes de informação, resultantes do aumento do volume de dados, vai proporcionar cenários mais propensos à existência de erros, além de aumentar o período de latência e a probabilidade de perda de pacotes. Um grande período de latência vai originar problemas ao nível da sincronização entre os pedidos efetuados pelo cliente e a resposta dada pelo servidor, sendo esta a maior causa de atraso nos serviços em tempo real [5].

- **Diversidade de dispositivos:** A enorme variedade de dispositivos e das suas características/funcionalidades, vai resultar em diferentes graus de qualidade de sinal num local específico, mesmo que estes sejam servidos pela mesma torre, da mesma operadora de rede móvel. Podem ser apontados diversos motivos para esta variação na qualidade do sinal, incluindo, mas não se limitando a:

  - **design da antena:** a utilização de uma antena interna ou externa, bem como as dimensões da mesma, podem afetar o ganho da antena do dispositivo;
  - **design do dispositivo:** materiais de dispositivos distintos podem apresentar diferentes índices de absorção de sinais de rádio;
  - **design do recetor de Radiofrequência (RF):** ruído e não linearidade no circuito do recetor do dispositivo podem afetar o desempenho;
  - **número de bandas de frequência suportadas:** à medida que são adicionadas mais bandas de frequência à antena do dispositivo, a complexidade do design do recetor aumenta, o que torna mais difícil alcançar uma boa qualidade de sinal. Além do referido, fatores como a mobilidade do utilizador, a orientação do dispositivo, a humidade e a temperatura podem ter impacto na variação do sinal, porém são condições transversais a todos os dispositivos.

  Esta informação é suportada por um estudo efetuado pela *Office of Communications* (Ofcom), entidade reguladora do Reino Unido, que testou a sensibilidade de vários dispositivos diferentes a sinais de rádio e bandas de frequência distintas, em espaço livre, observando variações dos valores de força do sinal recebido [7].

- **Virtualização e *cloud computing*:** a virtualização refere-se ao processo de abstração relativamente aos recursos físicos e procura mascarar a complexidade do *design* do *hardware* subjacente. Também dissocia o forte vínculo que liga as redes às suas aplicações, aquando da sua utilização. Desta forma, a técnica referida fornece um mecanismo

de isolamento entre os recursos físicos e as aplicações que correm nas camadas superiores, pelo que o *hardware* em questão não sabe qual a aplicação que está a servir, e esta é executada independentemente da infraestrutura física [8].

No que respeita ao *cloud computing*, este termo refere-se a um modelo de serviços que permite que servidores, *Central Processing Unit* (CPU)/*Graphics Processing Unit* (GPU), armazenamento, redes, entre outros, sejam disponibilizados como recurso (e não como produto) aos utilizadores. Este modelo de serviços facilita o desenvolvimento de aplicações inovadores que impliquem transmissão de informação em tempo real, de uma forma mais eficiente e rápida. Outro ponto a evidenciar caracteriza-se pelo assegurar do processo de autenticação do utilizador, além de garantir a segurança e integridade de informação num ambiente partilhado [8].

- **Redes 5G:** a quinta geração de tecnologias móveis veio proporcionar velocidades de transmissão de dados maiores que as redes *Fourth Generation* (4G) permitiam, atingindo os *gigabits* por segundo, uma menor latência, maior capacidade para alocar dispositivos ligados e suporte para IoT. O objetivo das redes 5G passa por assegurar serviços de comunicação fiáveis, com taxas de transmissão bastante altas, baixa latência e ubiquidade. Esta tipologia de redes tem capacidade para suportar uma vasta gama de serviços de comunicação, suportar diferentes fluxos de tráfego e servir vários utilizadores [9]. As redes 5G podem ser definidas como "*um ecossistema end-to-end que viabiliza uma sociedade totalmente móvel e conectada. Potencia a criação de valor para clientes e parceiros, através de casos de utilização existentes e emergentes, com uma experiência consistente e com modelos de negócio sustentáveis*" [10].

- **Gestão do tráfego:** Com o crescente número de dispositivos interligados e com o consequente aumento da quantidade de dados gerada, toda a gestão e processamento manual de um volume tão grande de informação, por parte dos administradores de rede, não se torna viável, uma vez que não vai garantir tempos de resposta dentro de intervalos razoáveis. Este contexto requer uma gestão dos recursos autónoma, eficiente e rápida. A Inteligência Artificial (IA), na forma de *Machine Learning* (ML), é apontada como uma possível solução para este problema, uma vez que permite encontrar um padrão útil a partir de dados, num período de tempo razoável, para além de permitir que o operador de rede analise o tráfego e obtenha conhecimento a partir dele [11].

- **Compatibilidade e padronização:** Ao tentar interligar vários sistemas, o desafio passa por garantir a comunicação entre as diferentes

tecnologias e dispositivos que coexistem, ou seja, assegurar a interoperabilidade.

Não menos importante, a padronização permite uma produção em massa de dispositivos e componentes, o que representa uma redução de custos. Além disso, facilita a manutenção e o suporte a longo prazo, tornando os sistemas de telecomunicações ainda mais acessíveis. Para além disso, a padronização viabiliza a comunicação global, aspeto essencial nas comunicações internacionais, comércio global e cooperação à escala global.

De forma a uniformizar a forma como os dispositivos e equipamentos de diferentes tecnologias comunicam entre si, foram criados padrões de referência, como é exemplo o *Open System Interconnection (OSI)* [12].

2.3 Redes locais

Uma *Local Area Network* (LAN) consiste na interligação de vários computadores numa mesma área geográfica relativamente pequena, possibilitando que diversos utilizadores consigam trocar ficheiros e/ou mensagens e aceder a recursos partilhados como, por exemplo, impressoras ou servidores [12].

De acordo com o *Institute of Electrical and Electronics Engineers* (IEEE), *uma LAN distingue-se de outras tipologias de rede de transmissão de dados pelo facto da comunicação estar limitada a um determinado espaço geográfico, não muito vasto, como um prédio, um armazém ou um campus, e depende de um canal de comunicação físico com taxas de transmissão relativamente rápidas e com baixo índice de erros.*

As Figuras 2.1 e 2.2 ilustram a representação física e lógica de uma LAN, respetivamente.

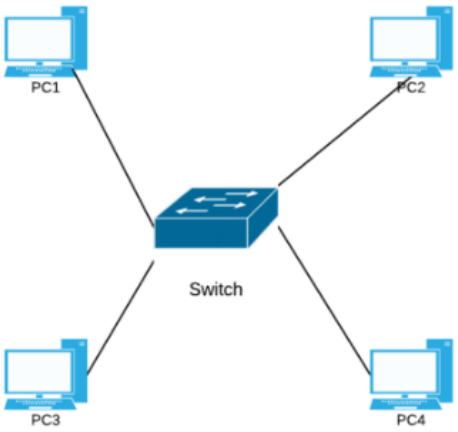

Figura 2.1: Representação física de uma LAN
[13]

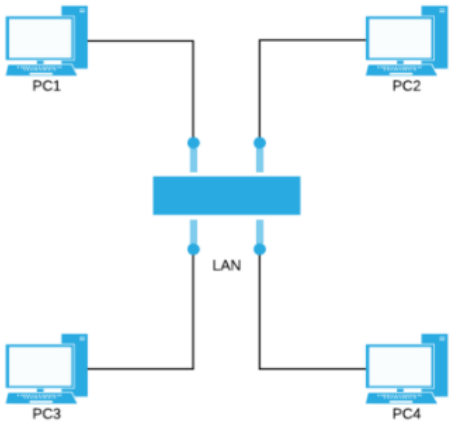

Figura 2.2: Representação lógica de uma LAN
[13]

Uma LAN é composta por três elementos base de *hardware*: um meio de transmissão (por exemplo, um cabo coaxial ou fibra ótica), um mecanismo para controlar a transmissão através do meio e, por último, interfaces de rede. Para além destes três componentes físicos, há um quarto elemento de grande relevância: um conjunto de protocolos de *software*, implementados nos computadores ou outros dispositivos ligados à rede, que controlam a forma como a informação é transmitida entre estes recorrendo aos elementos de *hardware* da rede [14].

As LANs evoluíram para redes abrangendo distâncias cada vez maiores, denominadas *Wide-Area Networks* (WANs), tornando possível ligar utilizadores dispersos geograficamente. Os três fatores principais que contribuíram para essa evolução foram o facto de LANs isoladas tornarem a comunicação entre departamentos impossível, o facto de a duplicação de recursos resultante do mesmo *hardware* e *software* ser fornecido a cada departamento implicar um aumento de custos e, por último, a ausência de uma gestão integrada da rede [12].

2.4 Necessidade de segmentação

Parte da eficiência, segurança e organização de uma rede deve-se à forma como esta se encontra segmentada. Este conceito pode definir-se como a divisão da rede em secções ou segmentos, permitindo controlar as comunicações entre secções e entre secções e a Internet [15].

Podemos assim entender a segmentação de uma rede como o controlo dos fluxos de tráfego entre as várias secções, o que se pode traduzir em impedir

o tráfego entre dois segmentos, limitar o fluxo tendo em conta a origem, destino ou outras condicionantes.

A CISCO aponta quatro benefícios para a segmentação [16]:

- **Melhor desempenho operacional:** torna-se possível isolar o tráfego em diferentes partes da rede, o que permite, num contexto corporativo, por exemplo, separar os vários departamentos e evitar que dados sensíveis se misturem. Além disso, desta forma garante-se uma redução no congestionamento da rede, uma vez que o tráfego é direcionado apenas para as secções da rede onde é necessário, evitando sobrecarregar segmentos específicos. Por outro lado, torna-se mais fácil implementar qualidade de serviço (*Quality of Service* (QoS)), garantindo que certos tipos de tráfego têm prioridade sobre outros na alocação da largura de banda;

- **Limitar os danos de ciberataques:** ao isolar as secções da rede, aumenta-se a segurança, uma vez que se limita o alcance de um possível ataque;

- **Proteger dispositivos vulneráveis:** é através da segmentação que se torna exequível a proteção de dispositivos que não foram concebidos de forma a conseguirem defender-se de possíveis ataques, como são exemplo equipamentos hospitalares cruciais para a sobrevivência dos pacientes;

- **Reduzir o âmbito de aplicação da conformidade:** a segmentação permite uma redução de custos associados à conformidade regulamentar, já que limita o número de sistemas abrangidos.

Além destas, podem se identificadas outras mais-valias da segmentação de rede:

- **Melhor gestão e organização:** em contextos onde as redes sejam de grandes dimensões, a sua gestão e organização podem ser difíceis. Através da segmentação torna-se possível conseguir uma visão mais clara de como os dispositivos estão interligados, o que facilita toda a organização e gestão da rede;

- **Redução de riscos:** ao isolar partes de uma rede, é possível reduzir os riscos associados a problemas técnicos, tais como falhas de *hardware* ou *software*. Desta forma, um problema numa determinada secção da rede não tem de afetar necessariamente os restantes segmentos;

- **Facilitar a escalabilidade:** por intermédio do processo de segmentação de uma rede, verifica-se uma maior facilidade no que respeita à escalabilidade, já que novos segmentos podem ser adicionados sem

afetar necessariamente o desempenho ou a segurança dos segmentos existentes.

Neste sentido, surgiram estratégias específicas para fomentar a segmentação das redes, como são exemplo as *Virtual Local Area Networks* (VLANs) e o isolamento lógico.

2.5 VLANs e isolamento lógico

Uma VLAN pode definir-se como uma rede comutada que está logicamente segmentada numa base organizacional, por funções, equipas de projeto ou aplicações, e não numa base física ou geográfica [17]. Desta forma, a reconfiguração de uma rede no sentido de suportar VLANs pode ser feita com recurso a *software*, sem haver a necessidade de remover dispositivos, ter de alterar o seu posicionamento ou alterar as ligações.

Na referência [18], a VLAN é designada *como um grupo de dispositivos numa ou mais LANs que estão configurados para se ligarem como se estivessem ligados através do mesmo cabo. As VLAN são baseadas em ligações lógicas e não em ligações físicas, tornando-se bastante flexíveis.*

As Figuras 2.3 e 2.4 ilustram a representação física e lógica de uma VLAN, respetivamente.

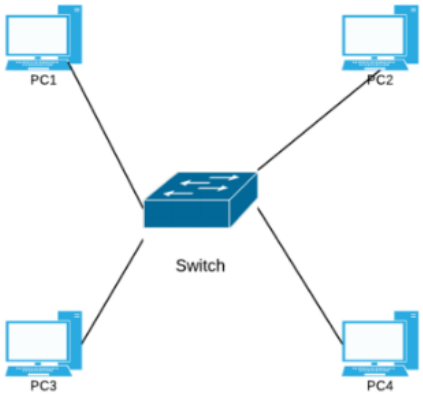

Figura 2.3: Representação física de uma VLAN
[13]

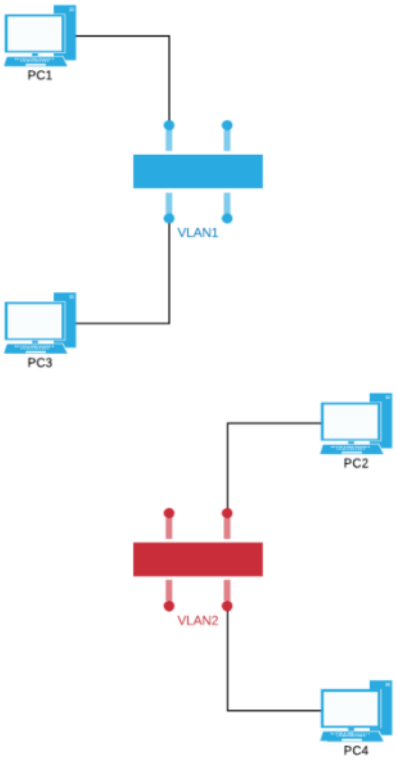

Figura 2.4: Representação lógica de uma VLAN
[13]

Uma VLAN é constituída por um certo número de dispositivos, quer sejam terminais ou equipamentos de rede (como *routers*), ligados num único domínio de *broadcast*. Esse domínio de *broadcast* pode ser suportado por vários *switches* interligados através de portas interswitch [17].

O isolamento lógico caracteriza-se por ser uma estratégia fundamental para garantir a segurança e a eficiência das comunicações. Este princípio envolve a separação de diferentes fluxos de tráfego na rede, impedindo que informações sensíveis ou tráfego crítico se misturem com outros dados. Uma das abordagens para alcançar o isolamento lógico passa pelo uso de políticas de controlo de acesso, que restringem quais os dispositivos ou utilizadores que têm permissão para aceder a determinadas partes da rede. Esta questão mostra-se particularmente importante em ambientes corporativos, onde a segregação de dados confidenciais é vital para a proteção contra ameaças cibernéticas.

Para implementar o isolamento lógico, as redes de comunicação podem aplicar técnicas de segmentação de tráfego e encaminhamento inteligente, o que permite que diferentes segmentos de rede operem independentemente,

garantindo que falhas ou ataques numa parte específica da rede não afetem as outras áreas. Além disso, a criptografia de dados desempenha um papel essencial no isolamento lógico, garantindo a proteção das informações durante a transmissão e o armazenamento. Ao manter os diferentes fluxos de dados devidamente isolados e protegidos, as redes de telecomunicações são capazes de responder aos requisitos de segurança e eficiência de comunicação em diversos ambientes.

2.6 *Datacenters*

Os *datacenters* têm-se tornado um elemento imprescindível no nosso quotidiano. De facto, uma grande parte dos serviços a que recorremos diariamente são suportados por *datacenters*, como por exemplo, motores de busca, redes sociais, telecomunicações, serviços de *streaming* e muitas outras aplicações pessoais e de negócios. Os *datacenters* constituem também bases estruturais e operacionais das plataformas de *cloud computing* [19].

Um *datacenter* pode ser definido como uma instalação física onde estão localizados e são geridos servidores, dispositivos de armazenamento, equipamentos de rede e outros componentes de *hardware* necessários para manter sistemas de TI. Podem variar em tamanho, desde pequenas instalações locais até grandes complexos globais, e são projetados para garantir a disponibilidade, viabilidade e segurança dos dados e serviços.

Na sua versão mais tradicional, o *hardware* é dedicado maioritariamente a tarefas específicas e não é partilhado de forma dinâmica entre diferentes aplicações ou clientes.

De acordo com a CISCO, um *datacenter* é uma *"instalação física que as organizações utilizam para alocar as suas aplicações e dados críticos. A conceção de um datacenter baseia-se numa rede de recursos de computação e armazenamento que permite a entrega de aplicações e dados partilhados. Os principais componentes da ligação de um datacenter incluem routers, switches, firewalls, sistemas de armazenamento, servidores e controladores de entrega de aplicações"* [20].

Na composição dos *datacenters* é possível encontrar conjuntos de computadores interligados, denominados *clusters*, cujo objetivo é executar as tarefas como se constituíssem uma única unidade. Para o autor da referência [21], este conceito pode ser definido como um grupo de servidores, e de outros recursos, que atuam como um único sistema e permitem uma elevada disponibilidade, equilíbrio de carga e processamento paralelo. Estes sistemas podem variar desde um sistema mais simples, como dois computadores pessoais, até um supercomputador com uma arquitetura de *cluster*. Os clusters são implementados com o intuito de salvaguardar o bom funcionamento dos *datacenters*, procurando assegurar a sua eficiência, desempenho e disponibilidade.

As principais mais valias que os *clusters* conferem são:

- **Alta disponibilidade:** a conceção dos *clusters* é elaborada de forma a lidar com eventuais falhas, quer de *hardware*, quer de *software*, procurando garantir um serviço sem interrupções.
- **Apoio à virtualização:** é possível identificar modelos de serviço em *cloud* que utilizam *clusters* na sua implementação. As Infrastructure as a service (IaaS) recorrem a estes de forma a criar *pools* de recursos (armazenamento, processamento e rede). Além do referido, os *clusters* de *cloud* são projetados de forma a serem altamente disponíveis e tolerantes a anomalias, redirecionando aplicações e serviços para outros nós disponíveis, em caso de falha. Podem-se apontar ainda outras mais valias, tais como a capacidade de identificar quais os recursos consumidos e cobrar aos utilizadores apenas a utilização efetiva desses recursos. De referir, também, a possibilidade de utilizar ferramentas de gestão simplificada, tornando todo este contexto mais eficiente.
- **Suporte para as arquiteturas modernas:** algumas das arquiteturas modernas envolvem a configuração de *clusters* para otimizar a comunicação e a eficiência dos recursos, como é exemplo a arquitetura *spine-leaf*.
- ***Bid Data* e a necessidade de segmentação:** com a crescente responsabilidade dos *datacenters* no processamento de grandes quantidades de dados, a organização em *clusters* vem permitir a implementação de *frameworks* que viabilizem a divisão de tarefas em *clusters* distribuídos.
- **Apoio às tecnologias emergentes:** os *clusters* têm evoluído de forma a dar suporte de diversas formas a tecnologias como IA e ML. A High-performance computing (HPC) é um desses contextos, onde se observa uma maior capacidade dos *clusters*, através da incorporação de GPUs e TPUs especializados para acelerar operações matemáticas e algoritmos de IA e ML. Também o facto de ser possível coexistirem vários *clusters* paralelos, permite um processamento em simultâneo de dados e, por isso, respostas mais rápidas.

A Figura 2.5 clarifica a distribuição dos espaços pelos diferentes componentes físicos que constituem um *datacenter* tipo.

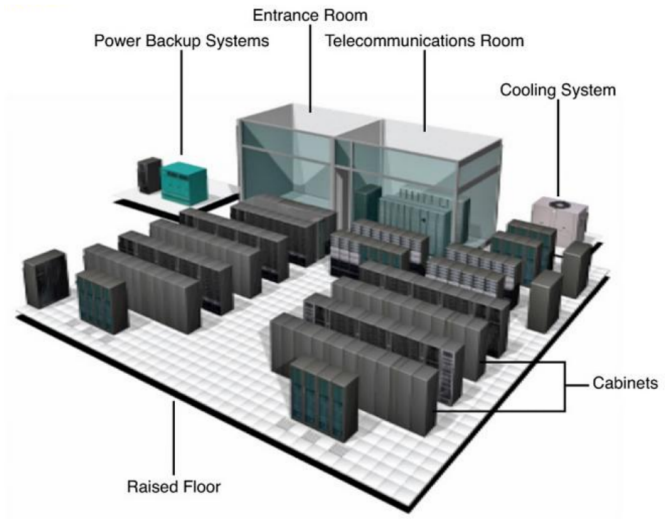

Figura 2.5: *Layout* físico de um *datacenter* [22]

No momento de planear e construir um *datacenter*, a definição da arquitetura é muito importante uma vez que define a forma como os dados circulam tanto no interior como para fora do *datacenter*, bem como a alocação dos recursos (servidores, redes de armazenamento, *racks* e outros recursos essenciais) e de que forma estes se encontram interligados, procurando assegurar o melhor funcionamento possível.

Na referência [23], a topologia da arquitetura de uma rede *datacenter* refere-se à disposição estrutural e à organização dos componentes da rede, com o principal objetivo de permitir uma troca de dados rápida, fiável e segura entre servidores, dispositivos de armazenamento e redes externas. São identificados sete elementos fundamentais para a estrutura de um *datacenter*:

- ***Racks* e Armários:** estruturas que otimizam o espaço e permitem um ambiente organizado para alocar os componentes.
- ***Switches* e *routers*:** elementos responsáveis por encaminhar o tráfego, com os *switches* a interligar dispositivos dentro do *datacenter* e os *routers* a permitirem a comunicação com redes externas.
- **Cablagem:** estrutura física que interliga servidores, *switches* e *routers*. Consoante a distância e a velocidade necessárias, podem ser cabos Ethernet, fibra ótica ou cabos de cobre.
- ***Top-of-Rack (ToR) switches*:** estes *switches* encontram-se no topo dos *racks* e interligam os servidores que se encontrem nesse *rack*, minimizando a cablagem necessária e facilitando a manutenção de rede.

- ***Load Balancers*:** elementos responsáveis pela distribuição uniforme do tráfego de rede pelos diferentes servidores, de forma a evitar sobrecargas e garantir o melhor desempenho possível.
- **Firewalls:** responsáveis pela proteção contra ameaças e acessos não autorizados.
- **Virtualização:** permitem a criação de redes virtuais, servidores e recursos de armazenamento, que se mostram essenciais para possibilitar a otimização e flexibilidade dos recursos.

O conceito de *datacenter* virtualizado caracteriza-se por ser uma extensão da versão física, mas com a condicionante de agrupar e dividir os recursos de *hardware* em máquinas virtuais (*Virtual Machine* (VM)) ou ambientes virtuais, recorrendo a *software* específico.

A virtualização possibilita a partilha dos recursos de *hardware* de forma mais flexível, criando VMs que podem executar diferentes sistemas operativos e aplicações de forma independente, o que se traduz em níveis mais altos de eficiência dos recursos, simplifica a escalabilidade e agiliza o processo de criar, migrar e gerir VMs.

Na Figura 2.6, está representada a virtualização de um *datacenter*.

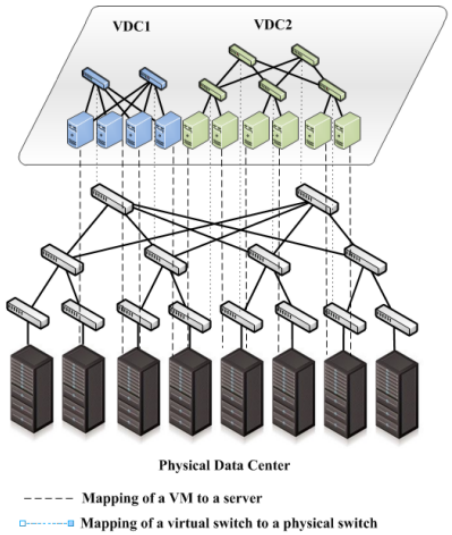

Figura 2.6: Virtualização de um *datacenter*
[24]

De uma forma geral, as arquiteturas de *datacenters* podem ser divididas em dois grupos principais: tradicionais e modernas. A Figura 2.7 descreve de uma forma mais detalhada duas arquiteturas tradicionais e três modernas.

Figura 2.7: Arquiteturas de redes de *datacenter*

Existe uma vasta gama de modelos a seguir, no momento de idealizar a arquitetura de um *datacenter*. A escolha depende das especificidades de cada organização, tais como orçamento, escalabilidade, segurança e requisitos de desempenho. Muitas empresas utilizam uma combinação de várias arquiteturas para encontrar uma resposta capaz para as suas necessidades.

Durante vários anos, as redes de *datacenters* foram construídas seguindo uma arquitetura organizada em camadas, de acordo com uma estrutura hierárquica. Porém, este tipo de arquitetura apresenta algumas limitações.

Nos *datacenters* com estrutura hierárquica, tal como representado na Figura 2.8, a parte inferior da árvore é a camada de acesso (*access layer*), na qual os *hosts* se ligam à rede. A camada intermédia é a camada de agregação (*aggregation layer*), à qual a camada de acesso se liga de forma redundante. A camada de agregação fornece conetividade aos *switches* adjacentes da camada de acesso e às linhas do *datacenter* e, por sua vez, ao topo da árvore, conhecido como núcleo (*core*). A camada de núcleo fornece serviços de encaminhamento para outras partes do *datacenter* e para o exterior do mesmo, seja para a Internet, seja para *datacenters* geograficamente separados.

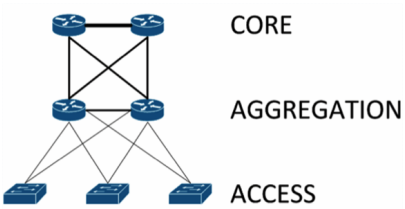

Figura 2.8: Arquitetura hierárquica para redes de *datacenter* [25]

Esse modelo tem uma escala relativamente grande, mas está sujeito a obstáculos se as ligações de *uplink* entre as camadas forem sobrecarregadas. Essa situação pode ocorrer devido à latência gerada pelo fluxo de tráfego através de cada camada e ao bloqueio de *links* redundantes (pressupondo o uso do *Spanning Tree Protocol (STP)*) [25].

O modelo ***Three-Tier*** também se caracteriza por uma divisão em três níveis, como é apresentado na Figura 2.9: *Core*, *Aggregation* e *Edge*. No entanto, esta arquitetura resultou de uma evolução do modelo apresentado acima.

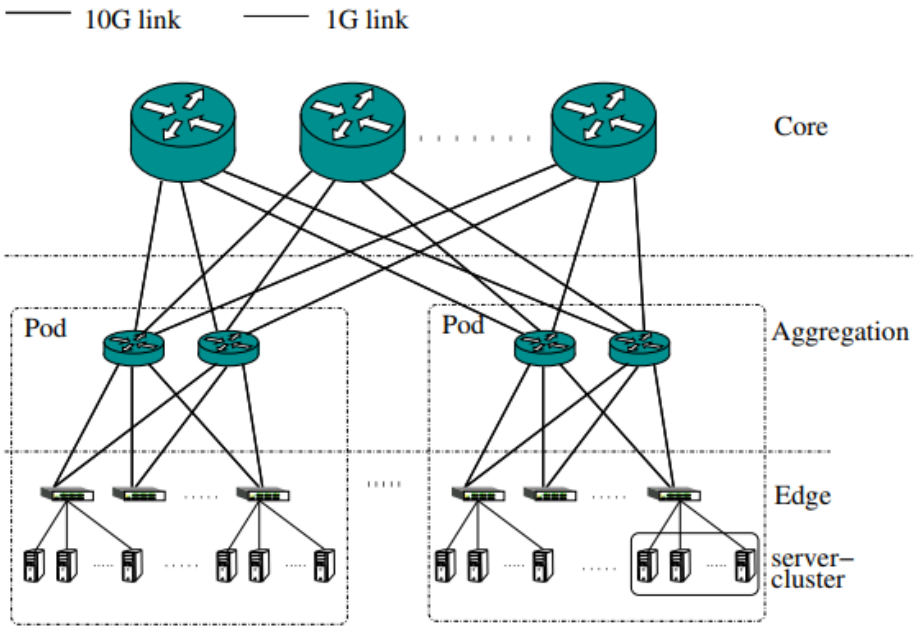

Figura 2.9: Arquitetura hierárquica *three-tier* para redes de *datacenter* [26]

Para definir um conjunto de servidores ligados ao mesmo *edge switch*, utiliza-se o termo *server-cluster*. Desta forma, se um *virtual datacenter* inteiro puder ser estruturado num único *server-cluster*, em termos de recursos de rede, isso significa que o *datacenter* vai utilizar apenas os *links* de um único *switch* - o *edge switch* que interliga o *server-cluster* - para comunicação entre as suas VMs. Esta arquitetura permite encaminhamento multicaminho, embora também possa estar sujeita a sobrecargas entre diferentes níveis: isto significa que quando os servidores tentam comunicar com toda a sua capacidade, pode acontecer congestionamento nos *edge switches* ou nos *switches* de agregação [26].

A Figura 2.10 representa a arquitetura *spine-leaf*, uma arquitetura de rede moderna que surgiu como alternativa às arquiteturas tradicionais, que se caracterizavam pela divisão em camadas.

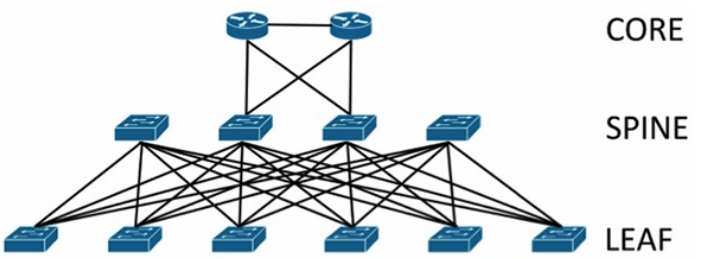

Figura 2.10: Arquitetura moderna *spine-leaf* para redes de *datacenter* [25]

A camada de acesso é constituída por um conjunto de *switches leaf*, que são totalmente interligados a uma série de*switches spine*. A malha garante que os *switches* da camada de acesso não estejam a mais de um *hop* de distância uns dos outros, minimizando assim a latência e a probabilidade de congestionamentos entre os *switches* da camada de acesso.

As arquiteturas *spine-leaf* podem ser definidas nos níveis 2 ou 3 do modelo OSI. Independentemente do projeto, todas as ligações estão a encaminhar tráfego, ou seja, nenhuma das ligações estará bloqueada, uma vez que o STP é substituído por outro tipo de protocolos.

Numa arquitetura *spine-leaf* da camada 2, a *spanning-tree* é geralmente substituída por uma versão do Transparent Interconnection of Lots of Links (Trill) ou do Shortest Path Bridging (SPB). Tanto o Trill quanto o SPB aprendem onde todos os *hosts* estão ligados à malha e fornecem um caminho livre de *loop* para os seus endereços *MAC Ethernet* através do cálculo do

caminho mais curto.

Caso estejamos na presença de uma arquitetura *leaf-spine* de nível 3, cada *link* representa uma ligação utilizada no encaminhamento de dados. O protocolo de encaminhamento *Open Shortest Path First* é frequentemente utilizado para calcular os caminhos entre os *switches leaf* e *spine*. Uma rede *leaf-spine* de camada 3 funciona de forma eficaz quando as redes locais virtuais são isoladas em *switches leaf* individuais ou quando é utilizada uma rede de sobreposição (rede de *overlay*).

As sobreposições de rede, como a VXLAN (que será desenvolvida no tópico seguinte), são comuns em ambientes altamente virtualizados e com vários utilizadores, como os encontrados em redes pertencentes a fornecedores de serviços [25].

A arquitetura *leaf-spine* apresenta algumas limitações topológicas:

- Os dispositivos pertencentes à mesma camada não podem ter ligações entre si;
- Se existirem *border leaf switches*, cada *spine switch* deve ter conexões com todos os *border leaf switches*;
- Se não existirem *border leaf switches*, cada *spine switch* deve ter ligações a todos os dispositivos Datacenter Gateway (DCGW) ou um par ou mais de *leaf switches* podem não só ligar-se aos servidores mas também a todos os DCGWs;
- Cada *leaf switch* tem de ter ligações a todos os *spine switches*;
- Deve haver pelo menos dois *leaf switches* por *rack*;
- Os servidores devem ter metade das suas portas ligadas ao primeiro *leaf switch* do seu *rack* e a outra metade conectada ao segundo *leaf switch*.

Estas restrições topológicas têm impacto no dimensionamento do *hardware*, uma vez que as ligações e os dispositivos têm de ser corretamente aprovisionados de modo a respeitar as restrições que regem a topologia baseada na arquitetura *spine-leaf* [27].

A infraestrutura hiperconvergente, Hyper Converged Infrastructure (HCI), é construída por blocos de construção de *software*, em detrimento do *hardware*. Na arquitetura hiperconvergente a computação e o armazenamento são combinados numa única solução e têm um único plano de controlo, enquanto a rede continua a ser fisicamente discreta e tem um plano de gestão separado. O aspeto fulcral de uma HCI é o armazenamento partilhado.

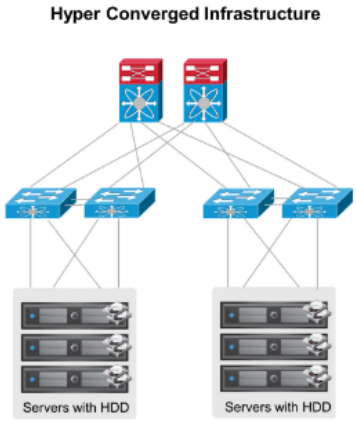

Figura 2.11: Arquitetura *Hyper Converged Infrastructure (HCI)* para redes de *datacenter*

[28]

Embora os discos estejam diretamente ligados a cada servidor, são partilhados entre vários servidores de forma dispersa. Em algumas soluções, os controladores de *software* estão ligados a uma Storage Area Network (SAN). Importa notar que a capacidade indicada no disco nem sempre é a capacidade disponível, dado que o sistema mantém várias réplicas de dados com base num fator de replicação pré-configurado, para que seja possível a recuperação de desastres e para permitir uma elevada disponibilidade em caso de falha de qualquer nó ou disco.

A HCI baseia-se em *hardware* que pode ser facilmente substituído e, dado que é uma solução definida por *software*, soluciona o problema da dependência de fornecedores, geralmente apresentado pelas soluções de infraestrutura convergente. Manter o armazenamento próximo do processamento e distribuir o seu acesso pelo grupo de servidores de processamento, não só mantém a latência Input/Output (I/O) do armazenamento controlada, como também aumenta a utilização do armazenamento.

Além disso, verifica-se uma maior flexibilidade de adicionar *hardware* de qualquer fornecedor, e também uma gestão simples, aliada a uma implementação muito mais rápida.

A infraestrutura é escalável de forma linear, bastando adicionar um novo nó (computador e armazenamento) ao *cluster* existente. Porém, o redimensionamento horizontal é bastante dispendioso, uma vez que se mostra necessário adicionar um novo nó, mesmo que se pretenda aumentar apenas a capacidade de computação ou de armazenamento. Dado que coexistem bastantes *softwares* de gestão, as soluções hiper convergentes apresentam um consumo excessivo de recursos [29].

No que respeita à última arquitetura ilustrada na Figura 2.7, o tópico 2.8: Tendências em Redes Definidas por *Software*, descreve em pormenor

esta abordagem para estruturar redes de *datacenter*.

De referir que existem outras tipologias de arquitetura, embora este estudo se tenha focado nas duas arquiteturas acima apresentadas.

A finalizar, convém referir que se podem identificar vários tipos de *datacenters* e modelos de serviços disponíveis, que se distinguem pelo facto de serem (ou não) propriedade de uma ou mais organizações, pela forma como se enquadram na topologia de outros *datacenters* (caso se enquadrem), das tecnologias a que recorrem para computação e armazenamento e, não menos importante, pelo seu grau de eficiência energética. Nesse sentido, identificam-se quatro tipos principais de *datacenters*:

- ***datacenters* empresariais:** são construídos, pertencem e são geridos por empresas, com especial foco na otimização direcionada ao utilizador final. Em grande parte dos casos, estão alojados nas instalações da própria empresa a que pertencem;
- ***datacenters* de serviços geridos:** a sua gestão é efetuada por terceiros em nome de uma empresa. A empresa aluga o equipamento e a infraestrutura, em detrimento de efetuar a sua compra;
- ***datacenters* de colocação:** uma empresa aluga espaço num *datacenter* pertencente a terceiros e localizado fora das instalações da empresa. Este tipo de *datacenter* é responsável por facultar a infraestrutura (edifício, refrigeração, largura de banda, segurança, entre outros), enquanto a empresa fornece e gere os componentes, como por exemplo servidores, armazenamento e *firewalls*;
- ***Cloud datacenters*:** esta tipologia caracteriza-se por alojar os dados e as aplicações num fornecedor de serviços em *cloud*, como a *Amazon Web Services (AWS)*, a Microsoft (Azure), a IBM *Cloud* ou outro fornecedor de *cloud* pública [20].

2.7 Redes de *Overlay*

As redes de *overlay* são projetadas para criar camadas adicionais de funcionalidade sobre infraestruturas de rede existentes. Essas camadas adicionais acarretam uma série de benefícios, tais como a segmentação de tráfego, a conexão de redes geograficamente dispersas, o isolamento de serviços e a implementação de políticas de segurança mais detalhadas.

A principal característica desta tipologia de rede é a capacidade de fornecer soluções flexíveis e escaláveis, independentemente da infraestrutura subjacente.

Com a capacidade de criar ambientes de rede personalizados e adaptáveis, as redes de *overlay* desempenham um papel crítico na criação de

arquiteturas de rede ágeis, eficientes e capazes de se ajustar às necessidades dinâmicas das organizações.

O conceito base caracteriza-se por configurar redes em camadas superiores, utilizando os recursos proporcionados pelas camadas subjacentes. Dado que não exigem a atualização de toda a infraestrutura de rede, ou seja, podem ser implantadas de forma incremental, têm sido utilizadas para acrescentar facilmente novos serviços ou funcionalidades às redes existentes. A sua constituição inclui vários elementos independentes que funcionam de forma colaborativa, nomeadamente:

- ***Underlay:*** a camada inferior da rede, composta por *routers* que ligam os *endpoints* da sobreposição. Trata-se normalmente de uma rede IP simples.
- ***Overlay:*** a camada superior da rede. Os seus *routers* adicionam e removem os cabeçalhos utilizados na rede subjacente (normalmente conhecidos como *routers* de encapsulamento ou desencapsulamento, respetivamente).
- ***Overlay endpoints:*** conjunto de *hosts* que interagem com a camada *overlay*, ou seja, não têm conhecimento da existência da camada *underlay*.
- ***Mapping system:*** servidor de base de dados que mantém os mapeamentos dos *endpoints* da camada *overlay* com os *routers* da camada *underlay*. De ressalvar que o *mapping system* é um componente opcional[30].

A Figura 2.12 ilustra esses diversos elementos e a forma como se interligam.

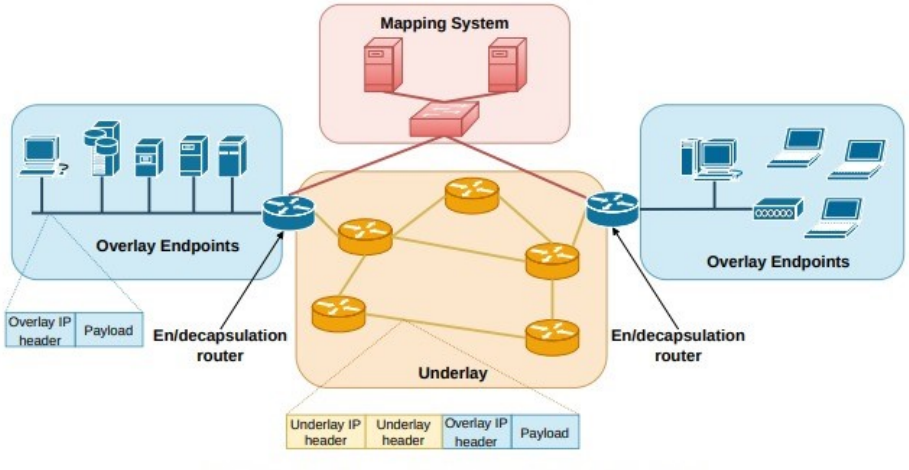

Figura 2.12: Arquitectura de referência para redes de *overlay* [30]

No contexto das redes de *overlay*, podem-se identificar alguns protocolos usados regularmente:

- ***Network Virtualization using Generic Routing Encapsulation (NVGRE):*** Semelhante ao VXLAN, que será abordado de seguida mais aprofundadamente, é usado para estender redes virtuais em ambientes como o *Microsoft Hyper-V*.
- ***Generic Routing Encapsulation (GRE):*** Usado para criar túneis e ligar redes geograficamente dispersas, frequentemente implementado em redes WAN.
- ***Multiprotocol Label Switching (MPLS):*** Permite a criação de redes de *overlay* e a diferenciação de tráfego com base em rótulos, comum em redes de operador e fornecedores de serviços.
- ***Stateless Transport Tunneling (STT):*** Focado na simplicidade e em baixar a carga de tráfego na rede, é usado em ambientes de virtualização.
- ***Layer 2 Tunneling Protocol (L2TP):*** Usado para estender redes privadas virtuais sobre a rede pública, maioritariamente em ligações VPN.
- ***Internet Protocol Security (IPsec):*** Protocolo focado na segurança, sendo usado para criar túneis seguros e estabelecer ligações VPN em redes de *overlay*.

- ***Ethernet Virtual Private Network (EVPN):*** Importante em ambientes de *datacenter* e redes de fornecedores de serviços, facilita a virtualização de LANs, dando suporte a situações como a interconexão de *datacenters*, mobilidade de VM e serviços VPN baseados em *Ethernet*. No capítulo três, este protocolo será abordado em detalhe.

- ***Virtual eXtensible Local Area Network (VXLAN):*** Amplamente utilizado para criar redes de *overlay* em ambientes de *datacenters*, permitindo a segmentação de tráfego e a ligação de redes virtuais numa rede física.

Tendo em conta os objetivos da dissertação, é importante aprofundar dois destes protocolos: EVPN (abordado no capítulo três) e VXLAN.

Numa rede VXLAN cada dispositivo constrói a sua própria base de dados, contendo informações correspondentes às VMs ligadas localmente. Os pacotes são transmitidos através de um túnel virtual, denominado segmento VXLAN, identificado por um campo específico de 24 *bits*, designado *Virtual Network Identifier (VNI)*, onde cada VNI garante o isolamento do tráfego associado a um segmento VXLAN.

O processo de encapsulamento do cabeçalho VXLAN pode definir um esquema de túneis da camada de ligação de dados sobre uma infraestrutura da camada de rede, sendo cada extremidade do túnel lógico designada genericamente por *Virtual Tunnel Endpoint (VTEP)* [31].

Esta é uma tecnologia que permite a sobreposição de uma rede da camada 2 (L2) sobre uma rede da camada 3 (L3) com a utilização de qualquer protocolo de encaminhamento IP, além de recorrer à utilização do encapsulamento MAC-in-UDP.

A VXLAN vem solucionar três problemas principais:

- proporciona 16M de VNIs (domínios de *broadcast*) contra os 4K oferecidos pelas
  VLANs tradicionais;

- Permite que o L2 seja estendido a qualquer lugar numa rede IP;

- *Flooding* [1] otimizado [33].

Em suma, os protocolos VXLAN e EVPN desempenham um papel altamente relevante na implementação de redes de *overlay* modernas.

[1] O flooding é uma forma de distribuir rapidamente as atualizações dos protocolos de encaminhamento a todos os nós de uma grande rede. Exemplos desses protocolos incluem o Open Shortest Path First (OSPF) e o *Distance Vetor Multicast Routing Protocol*.

Este evento ocorre quando um *router* utiliza um algoritmo de encaminhamento não adaptativo para enviar um pacote de entrada para todas as ligações de saída, exceto para o nó onde o pacote chegou [32].

O primeiro fornece a capacidade para estender redes virtuais sobre uma infraestrutura física, permitindo segmentação de tráfego, escalabilidade e isolamento de serviços em ambientes de *datacenter*.

Por outro lado, o EVPN emerge como uma solução robusta para virtualização de LANs, interconexão de *datacenters* e serviços baseados em *Ethernet*, mostrando-se essencial em redes corporativas e de fornecedores de serviços.

Ambos os protocolos permitem que as organizações possam alcançar uma infraestrutura de rede mais ágil e eficiente, atendendo às necessidades de conectividade flexível num cenário de constante evolução.

2.8 Tendências em Redes Definidas por *Software* (SDN)

A abordagem Software Defined Network (SDN) é revolucionária e tem transformado, de forma vincada, a forma como as redes são projetadas, geridas e operadas.

No passado e ainda atualmente, as redes de computadores são caracterizadas por infraestruturas rígidas e com configurações centralizadas, uma realidade que limita a agilidade e a capacidade de adaptação necessárias para atender às crescentes necessidades das aplicações e serviços modernos.

No entanto, com a ascensão do SDN, as redes tornam-se mais flexíveis e programáveis, permitindo que o controlo de rede seja baseado em *software*, criando uma distinção em diferentes planos consoante as funções específicas desempenhadas por cada um. Assim, podemos considerar que o *Data Plane* é uma rede constituída por um conjunto de switches que é responsável pelo transporte de dados, estando os sistemas terminais, como os computadores, ligados a esse plano. A gestão deste conjunto de switches é efetuada a partir de um controlador centralizado, que se situa no *Control Plane*, e que gere os recursos de rede. A "inteligência"necessária para que a rede funcione como pretendido é responsabilidade de aplicações de controlo que constituem o *Application Plane*"[34].

A Figura 2.13 representa os planos de uma rede definida por *software*.

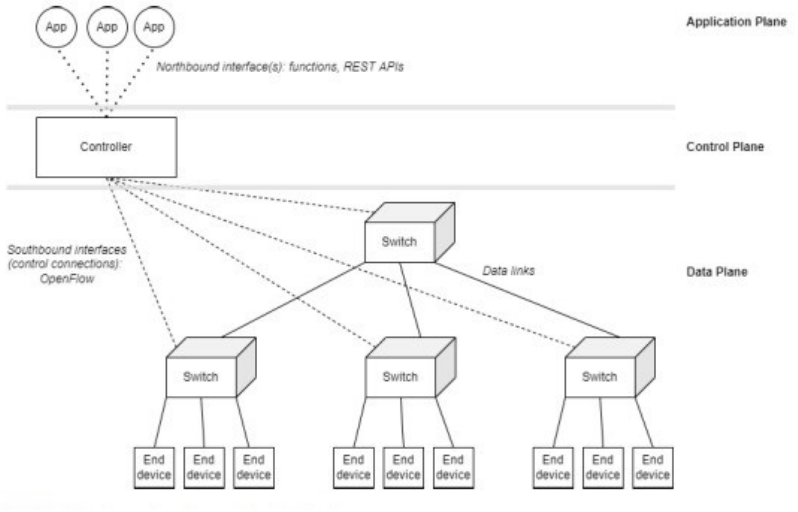

Figura 2.13: Planos de uma rede definida por *software* [34]

De uma forma mais detalhada, constata-se que a arquitetura de rede SDN permite dissociar os planos de controlo e de dados. Os *routers* e os *switches* tornam-se simples dispositivos de encaminhamento, devido ao facto da lógica de controlo ser transferida para um dispositivo lógico central, designado por controlador SDN, que apresenta duas interfaces: *Southbound* e *Northbound*.

A interface *Southbound* é padronizada e é responsável por controlar o plano de dados na rede. A interface *Northbound* é estipulada para serviços sob a forma de aplicações no topo do controlador SDN. Estas aplicações são independentes da infraestrutura e dos dispositivos de rede.

Em geral, a arquitetura SDN simplifica a conceção da rede e permite dispositivos de rede independentes do fornecedor, procurando nunca descurar a procura por uma melhor gestão das redes *wireless* [35].

Quando comparada com as redes convencionais, a capacidade de programação e monitorização centralizada das SDN tém inúmeras vantagens: recorrendo aos protocolos certos, o gestor de rede não tem de implementar políticas e funções de rede em cada um dos *switches*, sendo capaz de administrar toda a rede a partir de um controlador centralizado, o que possibilita a existência de uma visão global da rede e do seu estado.

As redes de interligação de *datacenters* são um excelente mote para a implementação dos conceitos de SDN, uma vez que, normalmente, são muito regulares, altamente centralizadas e, como a comunicação é interna à empresa, não se mostra necessário estar de acordo com os *standards*, isto se a comunicação não for efetuada com dispositivos externos [34].

Para além disso, as SDNs desempenham um papel fundamental na evolução e eficiência dos *datacenters* modernos. Neste contexto, a flexibilidade,

a escalabilidade e a capacidade de resposta são essenciais, pelo que este tipo de rede permite que os administradores de *datacenters* possam gerir as redes de forma mais dinâmica, reconfigurando os recursos de rede e o tráfego de uma maneira ágil, sem a necessidade de intervenção manual em dispositivos de *hardware* individuais. Este processo mostra-se essencial para suportar as crescentes necessidades das organizações em termos de *cloud computing*, virtualização e implantação de aplicações de alto desempenho. Assim, verifica-se uma melhor utilização dos recursos de rede, redução de tempo de inatividade, disponibilização mais rápida de serviços e maior capacidade de adaptação a mudanças impostas pela enorme quantidade de tráfego.

2.9 Integração com tecnologias emergentes

Nesta secção, serão abordadas algumas tecnologias de vanguarda para as redes de *datacenter* que estão a moldar o presente e o futuro das infraestruturas e dos serviços proporcionados. Frequentemente, recorre-se à interligação de várias tecnologias, por forma a aproveitar as vantagens que cada uma pode oferecer.

A integração de SDN com a tecnologia VXLAN está a revolucionar a gestão de redes de *datacenter*, promovendo níveis de flexibilidade e automação notáveis para a gestão de recursos: o SDN constituirá o plano de controlo, com o plano de dados a recorrer à estrutura de rede VXLAN.

Desta forma, é introduzida a separação entre os dois planos e, tirando partido da visão global e das funcionalidades programáveis, torna-se possível efetuar um controlo centralizado das redes VXLAN, além de melhorar significativamente o desempenho da rede e otimizar o mecanismo VXLAN. Na referência [36], os autores apresentam uma rede *cloud computing* baseada em VXLAN que depende da estrutura leaf-*spine*, na qual os *gateways* e os *switches* funcionam como *spines* e VxLAN Tunnel End Point (VTEP), respetivamente.

A Figura 2.14 ilustra a integração de SDN com VXLAN.

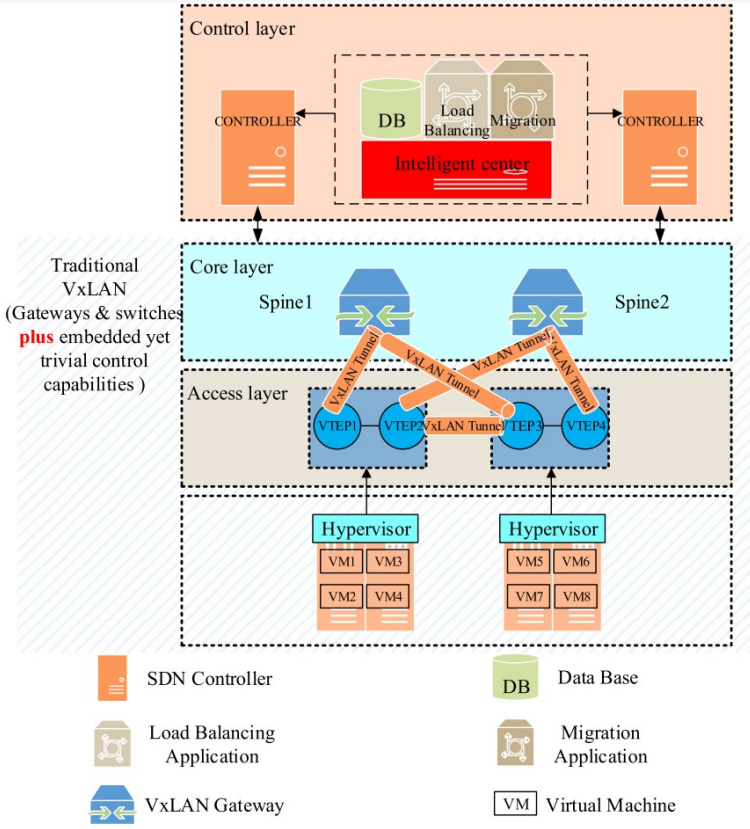

Figura 2.14: Integração SDN com VXLAN [36]

Em particular, a camada *core* onde estão localizados os routers *spine*permite que as VM se liguem a diferentes sub-redes e encaminhem o tráfego de/para os servidores na rede distante. A VXLAN utiliza a tecnologia de túnel para transmitir dados.

A arquitetura de rede distribuída evita potenciais estrangulamentos, mais propícios a um esquema centralizado. Para atingir este objetivo, a VXLAN utiliza *edge switches* (ou VTEP, na terminologia exata) na camada de acesso para encapsular e decapsular mensagens VXLAN. Por outras palavras, o túnel VXLAN é um canal lógico ou virtual entre dois VTEP e é responsável pela transmissão das mensagens VXLAN encapsuladas. Além disso, as VMs com VNIs diferentes sob o mesmo VTEP já não precisam de passar pela coluna vertebral para concluir a ligação, uma vez que o próprio VTEP pode concluir o trabalho.

Na rede VXLAN tradicional, tanto os *spines* como os VTEPs possuem uma capacidade de controlo limitada e são responsáveis de forma independente pelo encaminhamento do tráfego com base nas suas próprias informações locais.

A Virtualização de Funções de Rede (NFV) nos *datacenters*, uma tendência que recorre à virtualização de funções de rede tradicionalmente baseadas em *hardware*, promove uma economia de custos e uma maior agilidade operacional.

Um serviço de rede pode subdividir-se num conjunto de funções de rede, que posteriormente são virtualizadas e executadas em servidores de utilização geral ou em VMs. Desta forma, é possível atingir um maior nível de flexibilidade, já que as NFVs podem ser ativadas, realocadas ou destruídas de uma forma dinâmica, sem a necessidade de adquirir ou configurar *hardware* novo ou específico.

Esta tecnologia revolucionou a forma como os serviços de rede são disponibilizados, em comparação com os métodos tradicionais. De forma resumida, as principais diferenças são as seguintes:

- **Segmentação entre software e hardware:** Uma vez que o elemento de rede já não é o agregado de entidades integradas de *hardware* e *software*, a evolução de ambos é independente um do outro, o que viabiliza evoluções a ritmos distintos.

- **Implementação flexível das funções de rede:** A separação entre o *software* e o *hardware* permite a distribuição flexível das funções de rede, já que auxilia a reatribuição e partilha dos recursos da infraestrutura, pelo que, em conjunto, o *hardware* e o *software* podem desempenhar diferentes funções em vários momentos. A instanciação efetiva do *software* de rede pode tornar-se mais automatizada, tirando partido das diferentes tecnologias de *cloud* e de rede atualmente disponíveis. Para além disso, ajuda os operadores a implementar novos serviços de rede mais rapidamente na mesma plataforma física.

- **Escalonamento dinâmico:** A dissociação da funcionalidade da função de rede em componentes de *software* instanciáveis proporciona uma maior flexibilidade para escalar o desempenho efetivo da NFV de uma forma mais dinâmica e com uma melhor adaptação ao tráfego real [37].

A implementação de NFV em *datacenters* transfere funções de rede para *hardware* Commercial-Off-The-Shelf (COTS)[2], em vez de dispositivos especializados, o que viabiliza a padronização do *hardware* e permite que os fornecedores de serviços reduzam os custos e ganhem flexibilidade económica [39].

A Inteligência Artificial e o *Machine Learning* (IA/ML) podem ser usados na manutenção preditiva, otimização de recursos e segurança das redes de *datacenters*.

[2]Um produto de software e/ou hardware comercialmente pronto e disponível para venda, leasing ou licenciamento ao público em geral.[38].

A implementação de SDN na rede e a sua inerente capacidade de programação, possibilita a realização de operações de gestão otimizadas baseadas em Machine Learning (ML) em tempo real. A aplicação de ML com SDN é de grande interesse para lidar com várias tarefas de gestão da rede, como gestão e alocação de recursos, controlo e classificação do tráfego, previsão de QoS e Quality of Experience (QoE), otimização de encaminhamento e segurança. Para além disso, têm também potencial para maximizar a utilização dos recursos, recorrendo principalmente a algoritmos de *Reinforcement Learning*[3].

Na previsão de QoS e QoE são usadas operações de controlo proativas e de planeamento. Na otimização de encaminhamento com ML e SDN, os mecanismos mais eficientes levam em consideração o tráfego de rede e a otimização do consumo de energia.

2.10 Eficiência energética e sustentabilidade

A eficiência energética e a sustentabilidade são, cada vez mais, uma prioridade da área das telecomunicações. Com o crescente volume de dados e número de dispositivos interligados, o consumo de energia por parte das infraestruturas de rede também aumenta. Com o intuito de superar esse desafio, as operadoras e fornecedores de serviços optam por adotar medidas direcionadas para a redução do consumo de energia, como a implementação de tecnologias mais eficientes, a otimização de *Datacenters* e/ou a utilização de fontes de energia renovável. Estas iniciativas não contribuem apenas para a redução das emissões de Gases com Efeito de Estufa (GEE), mas também resultam numa atenuação significativa dos custos operacionais, tornando as redes mais sustentáveis e economicamente viáveis a longo prazo.

Segundo a referência [41], o maior consumo de energia atual na área das Tecnologias de Informação e Comunicação (TIC) é proveniente das instalações informáticas e das comunicações móveis. Os *Datacenters* assumem uma posição de destaque no que toca à contribuição para as emissões de GEE, uma vez que, em 2020 representavam 45% das emissões originadas por equipamentos da área das TIC. Contudo, o autor refere que, apesar dos valores de consumo continuarem a aumentar, as emissões de GEE têm diminuído, devido ao facto de se recorrer a energias sustentáveis para alimentar estes equipamentos.

Dada uma Energy-Harvesting Wireless Sensor Network (EH-WSN) (uma rede composta por nós alimentados pelo ambiente) e a energia disponível em cada nó, uma *workload* é energeticamente sustentável se o esforço necessário

[3] *Reinforcement learning* é um método de formação ML baseado na recompensa de comportamentos desejados e na punição de comportamentos indesejados. De uma forma geral, um sistema de ensino por reforço. A entidade que está a ser treinada é capaz de perceber e interpretar o seu ambiente, tomar medidas e aprender por tentativa e erro [40].

em cada nó para processar os pacotes de dados e encaminhá-los for completamente sustentado pela energia recolhida do ambiente [42].

Em síntese, a procura pela eficiência energética e sustentabilidade nas redes já se pode considerar uma realidade. À medida que as telecomunicações continuam a desempenhar um papel central no nosso quotidiano e na economia global, é fundamental que as redes sejam concebidas e aplicadas de uma maneira ambientalmente responsável. A otimização do consumo de energia, a transição para fontes renováveis e a redução das emissões de GEE não representam apenas preocupações ecológicas, mas também podem ser identificadas como vantagens económicas e operacionais significativas. Assim, a eficiência energética e a sustentabilidade deixam de ser uma temática apenas relacionada com questões ambientais, e passam a ser uma obrigatoriedade no que diz respeito ao futuro das redes de telecomunicações.

2.11 Segurança em redes de *Datacenter*

O tópico da segurança em contextos como os *datacenters* assume uma especial importância, devido à elevada quantidade de dados que circulam ou são armazenados e que os torna alvos atrativos para ameaças cibernéticas, bem como pela suscetibilidade que apresentam pelo facto de atualmente serem cada vez mais virtualizados, o que culmina numa maior vulnerabilidade a ataques.

Existem diversos tópicos que devem ser tidos em conta no contexto da segurança em *datacenters*:

- **Políticas de Segurança:** Para mitigar os desafios impostos pela natureza dos *datacenters*, estes exigem a implementação de políticas de segurança bastante rigorosas, incluindo políticas de acesso que especificam quem pode aceder aos recursos do *datacenter*, bem como políticas de controlo de identidade que garantem que apenas utilizadores autorizados podem aceder. A autenticação e autorização desempenham um papel fundamental na regulação de quem tem acesso aos diferentes recursos.

- **Deteção e Prevenção de Intrusões:** A detecção e prevenção de intrusões são elementos essenciais da segurança de *datacenters*. Os sistemas de deteção de intrusões (Intrusion Detection System (IDS)) monitorizam o tráfego à procura de atividades suspeitas e emitem alertas quando são identificadas ameaças.

  No caso dos Network-based Intrusion Detection System (NIDS), os dados são recolhidos diretamente da rede através de uma inspeção dos pacotes em circulação. No entanto, os IDS tradicionais analisam cada pacote, o que deteriora o desempenho da rede e resulta num aumento do atraso da rede e numa sobrecarga adicional de processamento na

infraestrutura, devido ao grande volume de dados [43]. Os sistemas de prevenção de intrusões (Intrusion Protection System (IPS)) têm a capacidade adicional de bloquear o tráfego malicioso para impedir ataques e, após detetar algum incidente suspeito, guardam informação relevante sobre o evento, como o horário em que foi descoberto o ataque, os IPs de origem e destino. Este sistema recorre a uma base de dados que contém as assinaturas de ataques detetados previamente, analisando o tráfego de forma reconhecer uma dessas assinaturas. É de extrema importância manter esta base de dados atualizada, para que seja possível detetar o maior número de ataques e os mais recentes [44].

- **Segurança de Rede:** A segurança de rede é uma preocupação fulcral, pelo que a segmentação de rede é implementada para isolar diferentes partes da infraestrutura. O recurso a *firewalls* e VPNs é feito com o intuito de proteger o tráfego sensível, de forma a garantir que a comunicação seja segura e que os dados confidenciais permanecem protegidos.

- **Proteção de Dados:** A proteção de dados é fundamental para garantir a continuidade dos negócios. Os *datacenters* implementam estratégias de *backup* e recuperação de calamidades para garantir que os dados críticos possam ser restaurados em caso de falhas ou incidentes, o que assegura que as operações possam continuar sem interrupção.

  Os *datacenters* devem cumprir regulamentações específicas, como Regulamento Geral sobre a Proteção de Dados (GDPR) ou Lei de Portabilidade e Responsabilidade do Seguro de Saúde (HIPAA). A conformidade regulamentar tem um caráter essencial uma vez que envolve medidas rigorosas para proteger informações sensíveis e garantir a privacidade dos dados.

- **Gestão de Identidade e Acesso:** A gestão de identidade e acesso desempenha um papel vital, uma vez que é responsável por garantir que apenas utilizadores autorizados têm acesso aos recursos e informações críticas e é fundamental para prevenir acessos não autorizados e proteger contra violações de segurança. O sistema Identity and Access Management (IAM) garante a segurança das identidades e dos atributos dos utilizadores da *cloud*, assegurando que apenas os utilizadores certos são autorizados a entrar nos sistemas de *cloud computing*. O IAM auxilia na gestão dos direitos de acesso através da verificação das permissões dos utilizadores que tentam aceder às informações que estão armazenadas nos sistemas de *cloud computing*. Atualmente, muitas organizações utilizam estes sistemas para proporcionar contextos mais seguros, além de uma melhor proteção das informações sensíveis que estão armazenadas na *cloud* [45].

- **Integração com Tecnologias Emergentes em Segurança:** De forma a aprimorar a deteção de ameaças e a resposta a incidentes, é fundamental promover a integração com tecnologias emergentes, o que permite a criação de uma abordagem mais proativa à segurança cibernética. A IA e o ML têm a capacidade para identificar padrões e comportamentos maliciosos com maior precisão, tendo um papel indispensável na proteção contra ameaças cada vez mais perigosas.

Mesmo tendo em consideração todos estes factos, há situações em que as redes não estão protegidas devido a diversos fatores.

A *cloud computing* tornou-se uma opção popular para fornecer serviços escaláveis através de VMs. No entanto, embora as capacidades de processamento sejam atribuídas às VMs, o recurso de rede é partilhado entre os diferentes utilizadores, o que torna o serviço vulnerável a ataques.

Um dos tipos de ataques que pode ocorrer são ataques direcionados ao Transmission Control Protocol (TCP), amplamente utilizado na *cloud computing*. Um tipo de ataque específico é o Pulsing Denial of Service (PDOs), que provoca *timeouts* nas ligações TCP dos seus alvos. Este tipo de ataque é difícil de detetar, o que o torna mais impactante [46].

Em suma, a segurança em *datacenters* é um aspeto essencial para garantir a integridade, a confidencialidade e a disponibilidade dos dados e serviços críticos que aí se encontrem hospedados. A implementação de políticas rigorosas, deteção e prevenção de intrusões, segurança de rede e proteção de dados é fundamental para proteger a infraestrutura contra ameaças. Para além disso, a integração de tecnologias emergentes, como a IA e o ML, proporciona oportunidades para melhorar a eficácia das metodologias de segurança e para adotar uma abordagem dinâmica na deteção de ameaças. À medida que a complexidade dos *datacenters* continua a crescer, a segurança permanece uma prioridade para garantir operações ininterruptas e proteção dos ativos digitais.

2.12 Redes de *Datacenter* e a era da IA

No atual contexto de constante evolução, começa a verificar-se a convergência entre as redes de *Datacenter* e a utilização de IA. A interação sinérgica entre estas duas áreas não transforma apenas a forma como os *Datacenters* são concebidos, mas redefine a capacidade dessas infraestruturas em dar resposta às exigências crescentes e complexas dos ambientes digitais contemporâneos.

A rápida ascensão da IA, com foco na melhoria da aprendizagem automatizada, processamento avançado e análise de dados massivos, desafia as normas convencionais das redes de *Datacenter*. No âmago desta transformação, surge a necessidade premente de adaptar as redes de *Datacenter* no sentido de dar suporte a quantidades massivas de dados e a cargas de

trabalho intensivas relacionadas com algoritmos complexos. A flexibilidade, escalabilidade e capacidade de resposta tornam-se critérios cruciais para estas infraestruturas, sendo a IA uma força propulsora para a sua redefinição.

Além disso, assiste-se à emergência de duas categorias distintas de *Datacenters*: as Fábricas de IA, concebidas para lidar com fluxos de trabalho em grande escala e desenvolvimento de modelos de IA avançados, e as *clouds* de IA, que sustentam aplicações geradoras de IA.

O *NVIDIA*, *Quantum-2*, *InfiniBand* e o *NVIDIA Spectrum-X* são plataformas de rede concebidas especificamente para enfrentar os desafios dos *Datacenters* de IA. A tecnologia *InfiniBand*, com latências extremamente baixas e funcionalidades otimizadas, representa uma escolha eficiente para as Fábricas de IA. Integrando tecnologias como o *Scalable Hierarchical Aggregation and Reduction Protocol* (SHARP) da *NVIDIA*, otimiza o seu desempenho. O encaminhamento adaptativo e a Arquitetura de Controlo de Congestionamento da *InfiniBand* contribuem para a utilização eficaz de recursos e garantem uma largura de banda e latência determinísticas, satisfazendo as exigências das aplicações de IA [47].

Capítulo 3

Implementação prática

Por forma a compreender o funcionamento do protocolo VXLAN, foi elaborado um primeiro cenário de rede que a seguir se apresenta e analisa.

3.1 Construção de uma rede baseada na tecnologia VXLAN

A implementação da virtualização de servidores tem originado novas necessidades na infraestrutura de rede física. Isto verifica-se devido ao facto de, com a virtualização de servidores, um servidor físico ser fragmentado em várias VMs, cada uma a operar o seu próprio sistema operativo e a correr as suas aplicações, e cada uma possuindo um endereço *Media Access Control* (MAC) único. Isso implica a necessidade de tabelas de endereços MAC mais extensas na rede *Ethernet*, devido à possibilidade de ligação e comunicação entre centenas de milhares de VMs.

No cenário em que as VMs num *datacenter* são categorizadas com base na sua VLAN, pode tornar-se imperativo ter um número expressivo de VLANs para segmentar o tráfego conforme o grupo específico ao qual cada VM está atribuída. O atual limite de 4094 VLANs revela-se insuficiente em contextos de tal magnitude.

Uma condição essencial para ambientes virtualizados que empregam uma infraestrutura física de Camada 2 é a necessidade de escalar a rede de Camada 2 para todo o *datacenter*, ou mesmo entre *datacenters*, visando uma alocação eficiente de recursos de computação, rede e armazenamento. Em tais contextos, a utilização de abordagens convencionais, como o STP, para garantir uma topologia livre de *loops*, pode acarretar um elevado número de ligações desativadas. [48]

Estes cenários conduzem à necessidade de criar redes de sobreposição. Esta sobreposição é utilizada para transportar o tráfego Ethernet das VMs individuais num formato encapsulado através de um "túnel"lógico.

Conforme mencionado na secção 2.7, o protocolo VXLAN representa

uma solução de sobreposição de rede amplamente utilizada em ambientes de *datacenter* com o propósito de facilitar a comunicação entre máquinas virtuais em redes virtuais extensíveis. Aliás, o VXLAN é frequentemente adotado em ambientes de *datacenter* para superar as limitações convencionais das VLANs. Nas configurações de rede de grandes *datacenters*, a escassez de identificadores de VLAN e os desafios relacionados com a mobilidade de máquinas virtuais tornam as VLANs inadequadas.

A criação de um cenário envolvendo o protocolo VXLAN tem como objetivo principal a simulação e compreensão do funcionamento das redes VXLAN num ambiente controlado, nomeadamente: estudo de redes virtuais extensíveis, a configuração de *routers Provider Edge* (PE), a compreensão do encaminhamento, a realização de testes de conectividade, a exploração de diferentes cenários de configuração e, por último, a identificação e resolução de problemas (*troubleshooting*).

Numa primeira fase foi elaborada uma rede constituída por dois PE *routers*, PE1-1 e PE2-1, um *router* denominado Core, dois *Ethernet switch* e quatro VPCS, sendo que o PC1 e o PC3 pertencem à mesma VLAN (VLAN 2) e o PC2 e o PC4 também pertencem à mesma VLAN (VLAN 3). A título exemplificativo, considera-se a existência de apenas duas VLANs. A Figura 3.1 apresenta a rede que foi elaborada no *software* GNS3 para estudo do protocolo VXLAN.

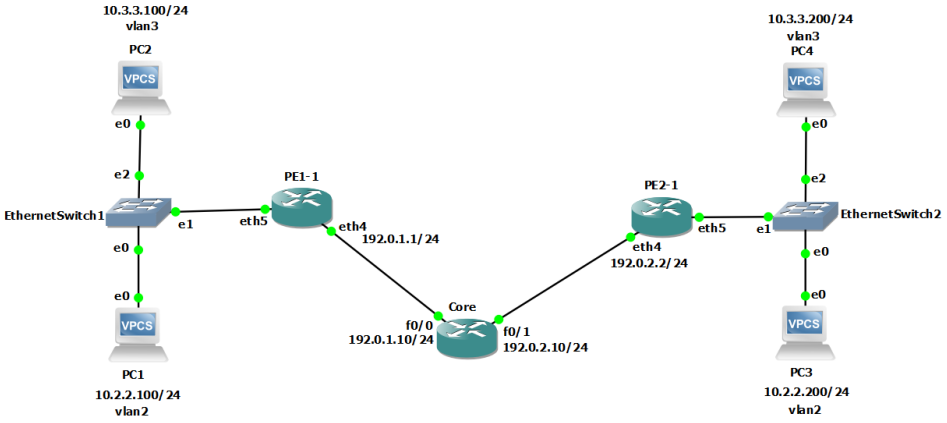

Figura 3.1: Rede elaborada no GNS3 para aplicação da tecnologia VXLAN

De realçar que o *router* Core é um dispositivo Cisco, ao passo que os *routers* PE1-1 e PE2-1 são dispositivos VyOS, uma vez que os IOS dos routers Cisco não suportam VXLAN. Numa fase inicial, foi efetuada a configuração de todos os endereços IPV4 e do protocolo *Open Shortest Path First* (OSPF) em todas as redes ligadas ao *router* Core. Note-se que no *router*

PE1-1 se configurou a interface *ethernet* eth4 com o endereço IP 192.0.1.1 e uma máscara de sub-rede de 24 bits e, posteriormente, configurou-se o protocolo OSPF para anunciar a rede 192.0.1.0/24 na área 0.

Este cenário é típico de ambientes de fornecedores de serviços, onde os PE *routers* estão ligados a clientes ou a outras redes. O protocolo OSPF assegura a conectividade na infraestrutura.

Na Figura 3.2 é possível observar as configurações efetuadas no dispositivo VyOs PE1-1.

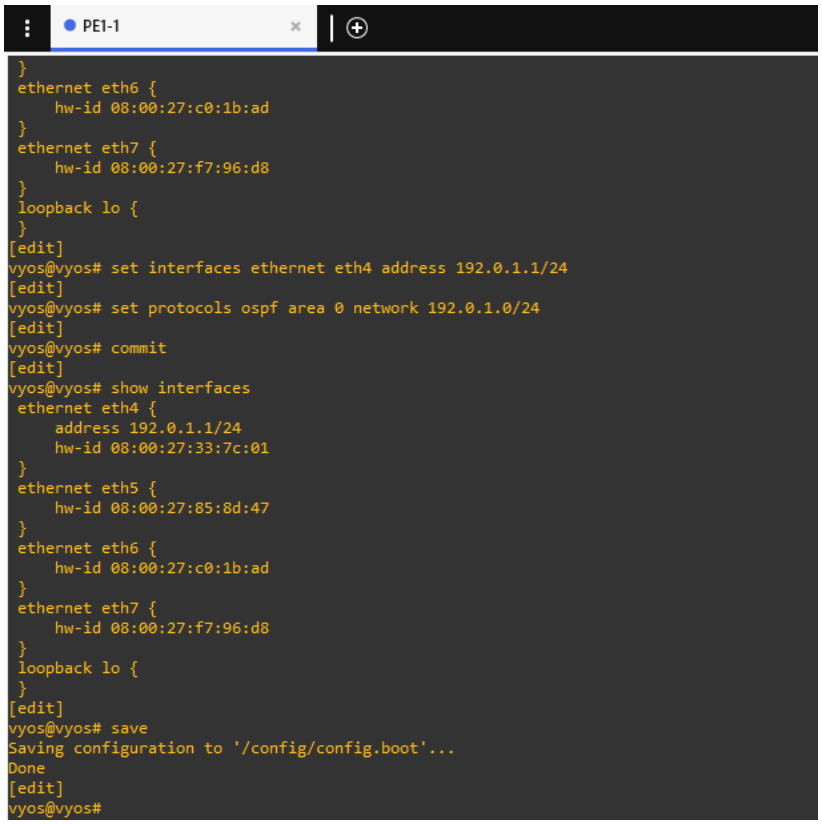

Figura 3.2: Configuração inicial do *Provider Edge router* PE1-1

De forma análoga, no PE2-1 foi atribuído o endereço IP 192.0.2.2/24 à interface *ethernet* eth4 e foi configurado o protocolo OSPF para anunciar a rede 192.0.2.0/24 na área 0, como é possível analisar através da Figura 3.3.

Figura 3.3: Configuração inicial do *Provider Edge router* PE2-1

Ao executar o comando *show ip route* em PE1-1, confirma-se que a rede 192.0.1.0/24 está diretamente ligada através da interface eth4, tal como se pode constatar na Figura 3.4.

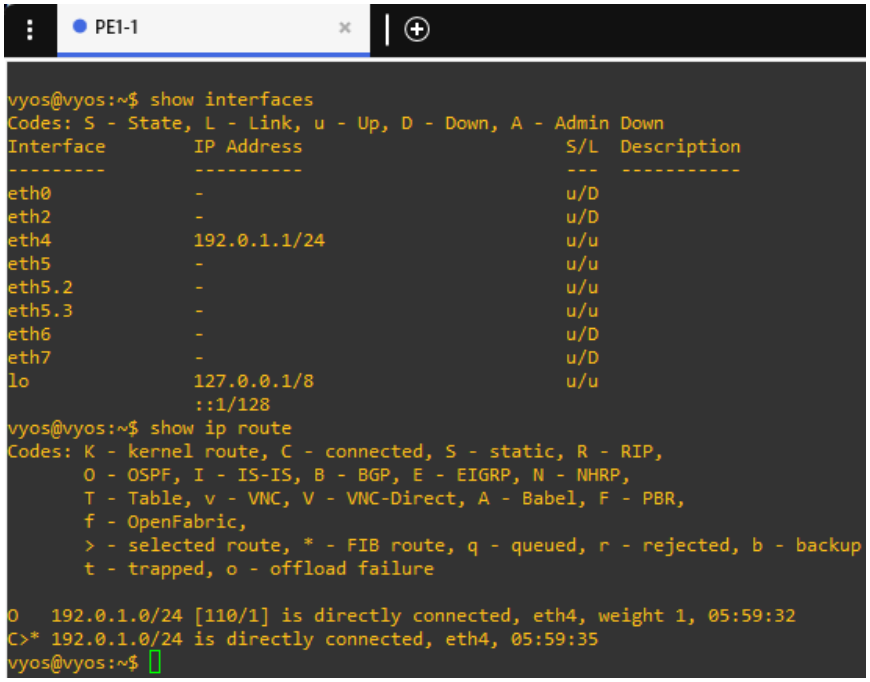

Figura 3.4: Tabela de encaminhamento IP do *router* PE1-1

O próximo passo consistiu em configurar os VPCS (sem *gateway*) e os *switches Layer* 2. Os PCs 1 e 3 foram atribuídos à VLAN 2, enquanto os PCs 2 e 4 foram atribuídos à VLAN 3. As ligações entre os *switches Layer* 2 e as PE routers foram configuradas como *trunks*. Nos *routers* PE foram configuradas sub-interfaces para cada VLAN, como é possível observar na Figura 3.5.

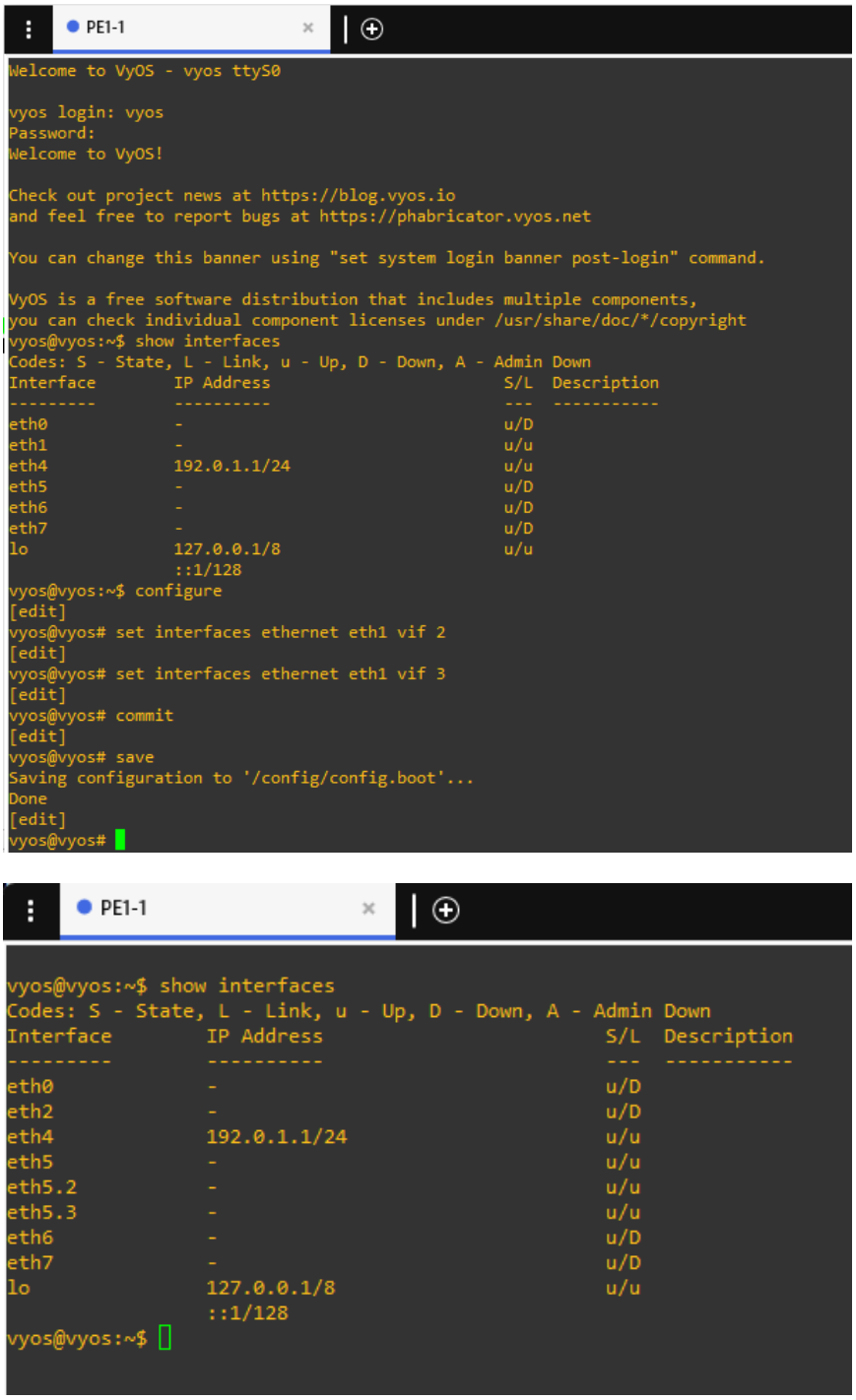

Figura 3.5: Configuração de sub-interfaces para cada VLAN em PE1-1

De seguida, foram criadas duas ligações VXLAN entre o PE1-1 e PE2-1, como é apresentado na Figura 3.6.

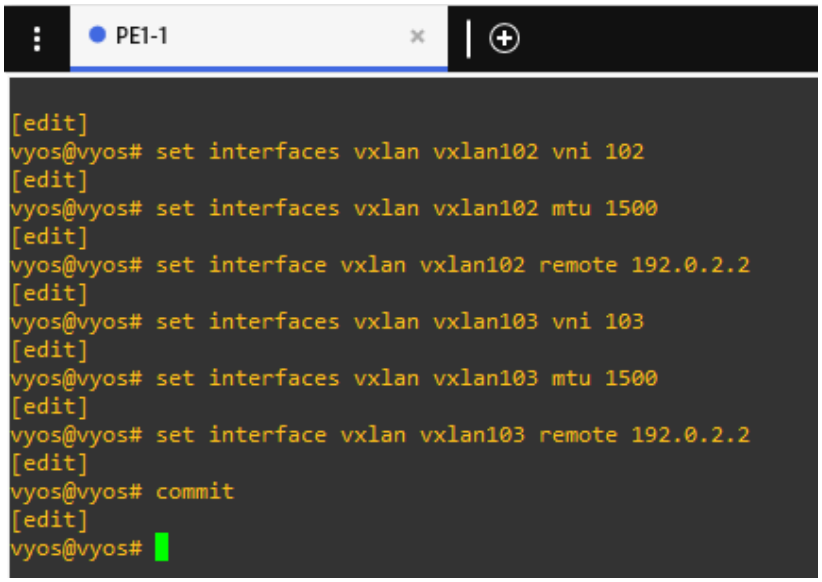

Figura 3.6: Criação de ligações VXLAN entre os Provider Edge routers

Por último, foram criadas duas pontes virtuais e adicionou-se a cada uma delas a respetiva interface VXLAN e sub-interface Ethernet, como é possível observar pela Figura 3.7.

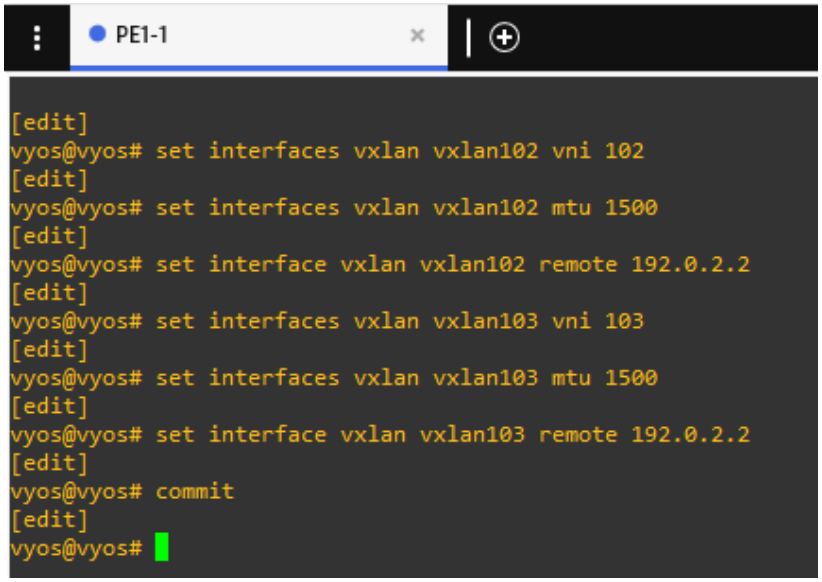

Figura 3.7: Criação de ligações VXLAN entre os Provider Edge routers

Tendo em conta a experiência realizada, é possível retirar algumas conclusões acerca do funcionamento da rede VXLAN como tecnologia adequada para redes de *datacenter*:

- **Configuração do protocolo de encaminhamento interno OSPF:** Neste cenário, ambos os *routers* PE1-1 e PE2-1 estão configurados com o protocolo OSPF, permitindo a construção das respetivas tabelas de encaminhamento. Qualquer protocolo de encaminhamento interno poderia ter sido utilizado, no sentido de garantir a conectividade e o encaminhamento de pacotes VXLAN.

- **Configuração de VXLANs:** Neste exemplo prático foram configuradas duas VXLANs (vxlan102 e vxlan103) em ambos os *routers* PE. Cada VXLAN está associada a um *Virtual Network Identifier* (VNI) específico (102 e 103), o que corresponde à criação de redes virtuais separadas dentro da infraestrutura VXLAN.

- **Criação de Pontes Virtuais:** As pontes virtuais foram configuradas associando interfaces físicas, interfaces VXLAN e membros de VLANs específicas, promovendo a integração de VXLANs com VLANs tradicionais de forma a permitir a comunicação entre dispositivos localizados em diferentes segmentos.

- **Configuração de Interfaces Virtual Interface (VIF):** Foram configuradas interfaces VIF para representar membros de VLANs específicas. Essas interfaces são associadas às VXLANs e às pontes virtuais, por forma a permitir o tráfego entre VXLANs e VLANs.

- **Comunicação Bidirecional entre PE1-1 e PE2-1:** A configuração remota das VXLANs em ambas as extremidades (PE1-1 e PE2-1) e o encaminhamento interno promovido pelo protocolo OSPF permitiu uma comunicação bidirecional. Cada *router* comunica com o endereço IP remoto do outro *router*.

- **Segmentação de Redes Virtuais:** A associação de VNIs distintos para cada VXLAN promove a segmentação de tráfego entre redes virtuais independentes, característica fundamental do VXLAN em ambientes de sobreposição de redes.

- **Isolamento de Tráfego:** A configuração de VXLANs e a associação com interfaces físicas e pontes virtuais ajudam a isolar o tráfego entre diferentes VXLANs, contribuindo para um ambiente de *datacenter* mais seguro.

- **Topologia Multi-nível:** A combinação de configurações OSPF e VXLAN sugere a criação de uma topologia multi-nível, onde o encaminhamento dinâmico é usado em conjunto com VXLANs para criar uma rede escalável.

Em suma, estas configurações proporcionam a criação de um cenário de rede eficiente para um *datacenter* com comunicação "segura"entre VXLANs e isolamento de tráfego em segmentos virtuais distintos.

3.2 Construção de uma rede com a tecnologia L2VPN/EVPN com transporte VXLAN

A secção 3.1 forneceu uma análise detalhada do desempenho de uma rede baseada no protocolo VXLAN, destacando as suas vantagens, aplicações e desafios específicos. Nesta secção avalia-se a integração L2VPN/EVPN, procurando desta forma uma gestão mais dinâmica e eficiente das redes de camada 2, essencial para ambientes complexos de *Datacenter*. Ganha-se amplitude na definição das políticas de rede, permitindo uma segmentação mais refinada e o controlo de tráfego.

A capacidade de fundir camadas, integrando a camada 2 com a camada 3, proporciona uma gestão mais holística e otimizada dos serviços de VPN. Além disso, a integração com VXLAN no contexto L2VPN/EVPNN oferece suporte a *multicast*, fundamental para transmissões eficientes em ambientes distribuídos.

Explorar L2VPN/EVPN implica adotar uma abordagem padronizada, facilitando a interoperabilidade entre diferentes equipamentos e fornecedores. Nesta secção será implementada uma rede L2VPN/EVPN com transporte VXLAN, sendo avaliado o seu desempenho e alguns aspetos operacionais, abordando desafios e estratégias para otimizar o funcionamento da rede num ambiente de *Datacenter*.

Numa primeira fase foi elaborada uma rede constituída por três *routers* PE - PE1-1, PE2-1 e PE3-1, um *router* de Core, seis *Ethernet switch* e seis VPCS. A Figura 3.8 apresenta a rede que foi elaborada no software GNS3 com o objetivo de explorar os mecanismos L2VPN/EVPN com transporte VXLAN.

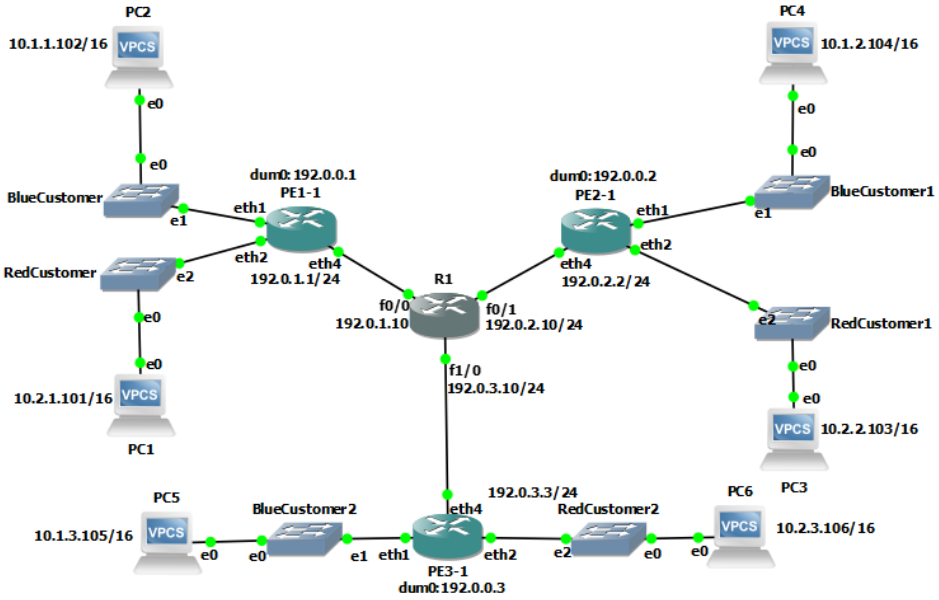

Figura 3.8: Rede elaborada no GNS3 para aplicação da tecnologia L2VPN/EVPN com transporte VXLAN

Após a construção da rede, foi necessário configurar todos os endereços IPv4 ilustrados na Figura 3.8. De seguida, procedeu-se à configuração do protocolo OSPF nas ligações associadas ao *router* Core.

No PE1-1, a configuração teve início com a atribuição do endereço IP 192.0.0.1/32 à interface *loopback* (dum0) e com a configuração do endereço IP 192.0.1.1/24 na interface *Ethernet* eth4. A configuração do OSPF prosseguiu associando as redes 192.0.0.1/32 (representando a interface de *loopback*) e 192.0.1.0/24 (eth4), ambas pertencentes à área OSPF 0. Além disso, o parâmetro *router-id* foi definido como 192.0.0.1, constituindo a identificação do router dentro do processo OSPF. Esta configuração pode ser visualizada na Figura 3.9.

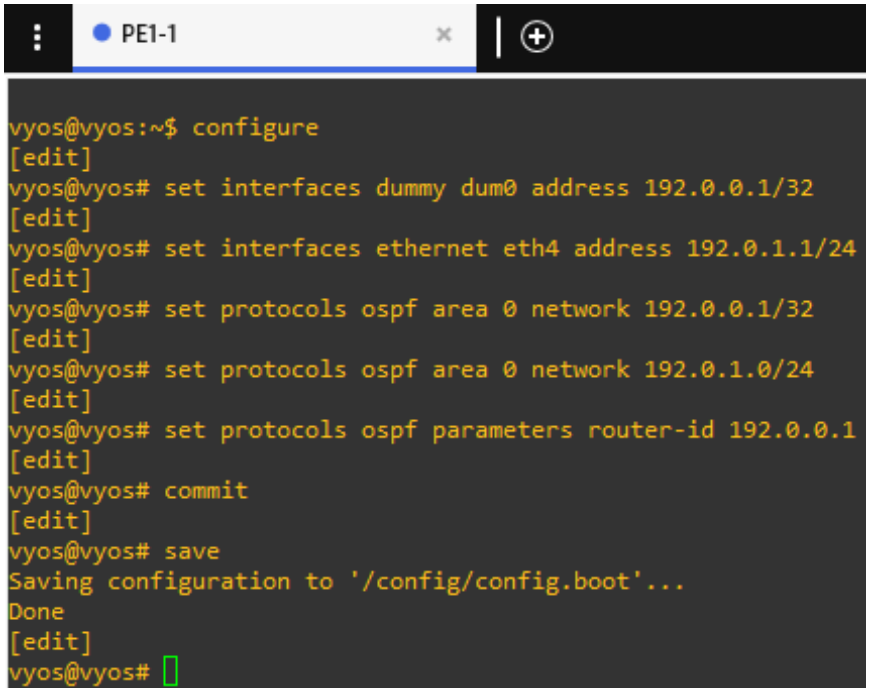

Figura 3.9: Configuração endereços IPV4 e OSPF no PE1-1

Os comandos "*show interfaces*"e "*show ip route*"permitem verificar se as configurações foram executadas com sucesso, conforme pode ser observado na Figura 3.10.

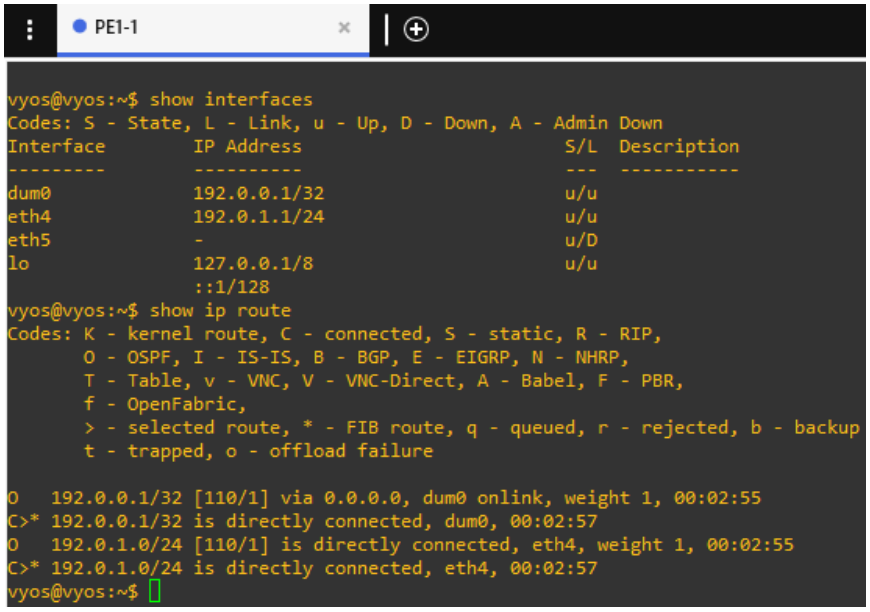

Figura 3.10: Verificação da configuração dos endereços IPV4 e OSPF no PE1-1

A configuração dos routers PE2-1 e PE3-1 foi feita de forma análoga, com a diferença apenas nos endereços atribuídos, seguindo o padrão apresentado na figura 3.8.

Posteriormente, foi configurada uma VPN de camada 2 entre as redes dos clientes para ambas as partes, utilizando o BGP EVPN com transporte VXLAN. Adicionalmente, implementou-se uma topologia *Spine-Leaf* entre os *routers* PE, onde o PE1-1 desempenha o papel de *Spine*. Este cenário levou em consideração as relações BGP internas dentro do mesmo *Autonomous System* (AS), empregando *Route Reflector*s. A configuração realizada no PE1-1 pode ser visualizada na Figura 3.9.

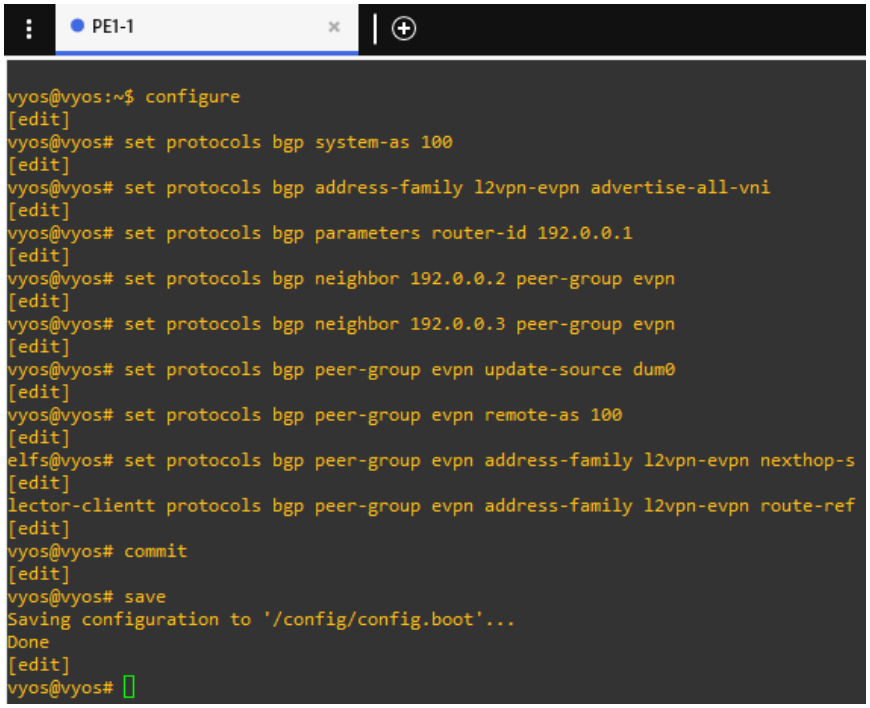

Figura 3.11: Configuração do Spine-Route Reflector em PE1-1

De seguida, foram realizados passos semelhantes para configurar PE2-1 e PE3-1, diferindo os endereços de rede, bem como a questão do PE1-1 ser *spine-route reflector* e PE2-1 e PE3-1 serem *leaf-route reflector clients*. A configuração do BGP para L2VPN/EVPN é uma parte essencial ao implementar uma solução de rede que envolve serviços de VPN de camada 2 (L2VPN) e Ethernet VPN (EVPN).

Procuremos agora analisar em detalhe a configuração efetuada. O comando "*set protocols bgp system-as 100*"simplesmente define o número do AS para o processo BGP. Como sabemos, um AS corresponde a um conjunto de *routers* e redes sob a administração de uma única entidade e que partilha uma política de encaminhamento comum. Sequidamente, o comando "*set protocols bgp address-family l2vpn-evpn advertise-all-vni*"ativa a família de endereços *L2VPN-EVPN* para o BGP. Esta configuração especifica que o BGP será utilizado para anunciar informações sobre VPNs de camada 2 e Ethernet VPN.

Com "*set protocols bgp parameters router-id 192.0.0.1*", configura-se o *ID* do *router* BGP. O *Router ID* é uma identificação única associada a um *router* BGP. As linhas "*set protocols bgp neighbor 192.0.0.2 peer-group evpn*"e "*set protocols bgp neighbor 192.0.0.3 peer-group evpn*"definem vizinhos BGP com endereços IP específicos e associam-nos ao grupo de pares EVPN.

O comando "*set protocols bgp peer-group evpn update-source dum0*"define

a interface *dum0* como a fonte para as atualizações BGP, especificando que interface será usada para troca de informações BGP.

Com "*set protocols bgp peer-group evpn remote-as 100*", configura-se o número do AS remoto para o grupo de pares EVPN, ao passo que o comando "*set protocols bgp peer-group evpn address-family l2vpn-evpn nexthop-self*"garante que o *router* local é o próximo salto (nexthop) para as rotas anunciadas no grupo de pares (EVPN).

Por fim, o comando "*set protocols bgp peer-group evpn address-family l2vpn-evpn route-reflector-client*"indica que os *routers* no grupo de pares (EVPN) atuam como clientes *Route Reflector*, o que é útil para escalabilidade em redes grandes.

Esta configuração é fundamental para estabelecer e manter a comunicação entre *routers* BGP, permitindo a troca eficiente de informações sobre redes de camada 2 e VPNs Ethernet.

Na última etapa, foram configurados o VXLAN e interfaces de ponte para cada cliente. Seguidamente, apresenta-se a configuração específica para o PE1-1.

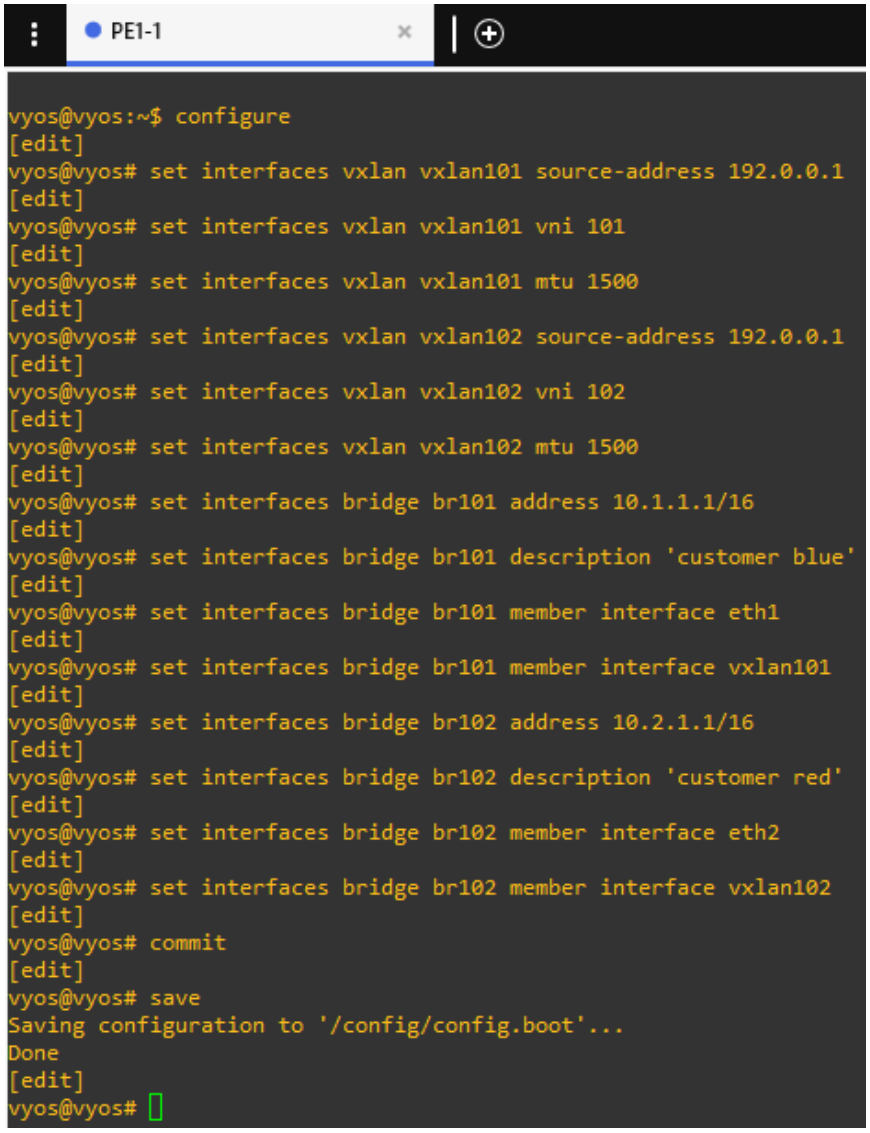

Figura 3.12: Configuração do VXLAN e de interfaces de ponte em PE1-1

A configuração apresentada para uma rede L2VPN/EVPN com transporte VXLAN oferece uma solução eficiente para conectividade em ambientes de *Datacenter*, especialmente projetada para serviços de VPN de camada 2 e Ethernet VPN.

Ao adotar a topologia *Spine-Leaf*, em que PE1-1 atua como *Spine* e PE2-1/PE3-1 atuam como *Leaf*, a arquitetura visa proporcionar escalabilidade e eficiência. A utilização do protocolo VXLAN como método de transporte destaca-se por superar as limitações tradicionais das VLANs, permitindo a extensão de redes L2 num ambiente totalmente IP.

A segmentação do tráfego é alcançada por meio da criação de interfaces

de ponte associadas a clientes específicos, isolando as redes de clientes, como exemplificado pelas interfaces br101 ("*customer blue*") e br102 ("*customer red*").

A configuração do BGP é crucial, destacando PE1-1 como um *route reflector*. Essa escolha contribui para a escalabilidade em redes maiores, facilitando a comunicação eficiente entre os routers BGP.

A identificação única de cada *router* BGP é garantida pelo uso do parâmetro *router-id*. Além disso, a configuração inclui o anúncio de todos os VNI, assegurando a disseminação de informações relevantes sobre VPNs de camada 2 e Ethernet VPN.

A estratégia de configurar o *router* local como o próximo salto (*nexthop*) para as rotas anunciadas no grupo de pares EVPN, denominada "*nexthop-self*", promove eficiência na troca de informações.

Por fim, a indicação de que os *routers* no grupo de pares EVPN atuam como clientes de refletores de rota é uma abordagem adotada para otimizar a escalabilidade em redes de maior dimensão.

Essas considerações ressaltam a robustez e a adequação da configuração para ambientes de *Datacenter* modernos, oferecendo uma solução escalável e eficiente para redes L2VPN/EVPN com VXLAN.

3.3 Integração do protocolo EVPN-VXLAN numa rede empresarial

Após a implementação de uma rede VXLAN na secção 3.1 e da criação de uma rede L2VPN/EVPN com transporte VXLAN na secção 3.2, o foco volta-se agora para as implicações práticas e os benefícios observados ao aplicar a tecnologia EVPN-VXLAN num cenário empresarial.

"Porque razão é necessário recorrer ao protocolo EVPN?"A resposta reside nos desafios enfrentados pelas tecnologias L2VPN tradicionais.

A tecnologia *Virtual Private LAN Service* (VPLS) permite ilustrar os desafios encontrados pelas tecnologias convencionais. A VPLS, sendo uma das primeiras tecnologias VPN MPLS, foi extensivamente utilizada em cenários de interligação de *Datacenters*, proporcionando serviços Ethernet multiponto-a-multiponto a utilizadores empresariais. No entanto, a VPLS apresenta várias limitações que a impedem de responder aos requisitos de *Datacenters* complexos e de grande escala.

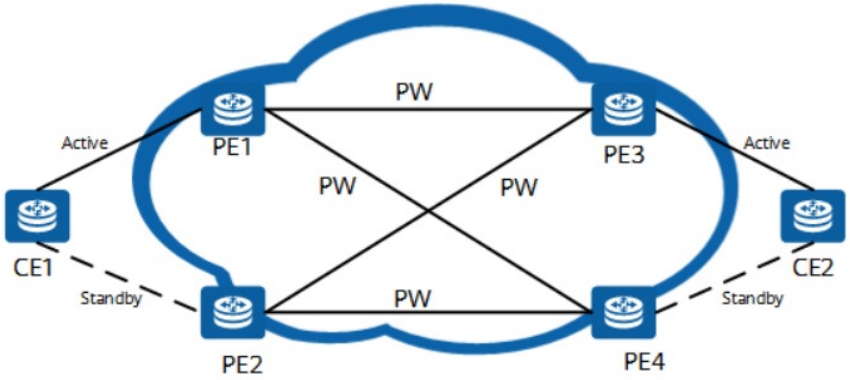

Figura 3.13: Implementação tradicional de L2VPN numa rede *datacenter Interconnect*

[49]

A implementação tradicional de L2VPN numa rede *Data Center Interconnect* (DCI) é desafiante devido a vários fatores. Os PEs precisam de conhecer os endereços MAC de todos os *Customers Edge* (CEs), no entanto, as suas tabelas de endereços MAC têm capacidade limitada. Além disso, as configurações dos PEs tornam-se complexas, o que dificulta a implementação da rede.

Outro problema está relacionado com a escalabilidade da rede. O uso do VPLS requer o estabelecimento de conexões completas entre os PEs, o que não é adequado para redes de grande dimensão. Além disso, o VPLS não possui um plano de controlo eficiente, resultando numa convergência deficiente quando ocorrem alterações nos endereços MAC ou falhas.

A baixa utilização da largura de banda da ligação também representa um desafio. Os PEs precisam de funcionar em modo ativo único para evitar a formação de *loops* entre eles e os CEs, o que resulta numa eficiência reduzida na utilização da largura de banda.

A tecnologia EVPN resolve os problemas anteriores ao utilizar extensões do BGP para mover a aprendizagem e anúncio de endereços MAC entre redes da Camada 2. Isso permite que os dispositivos possam gerir endereços MAC da mesma forma que gerem rotas, possibilitando a implementação de um equilíbrio de carga entre rotas EVPN com o mesmo endereço MAC de destino.

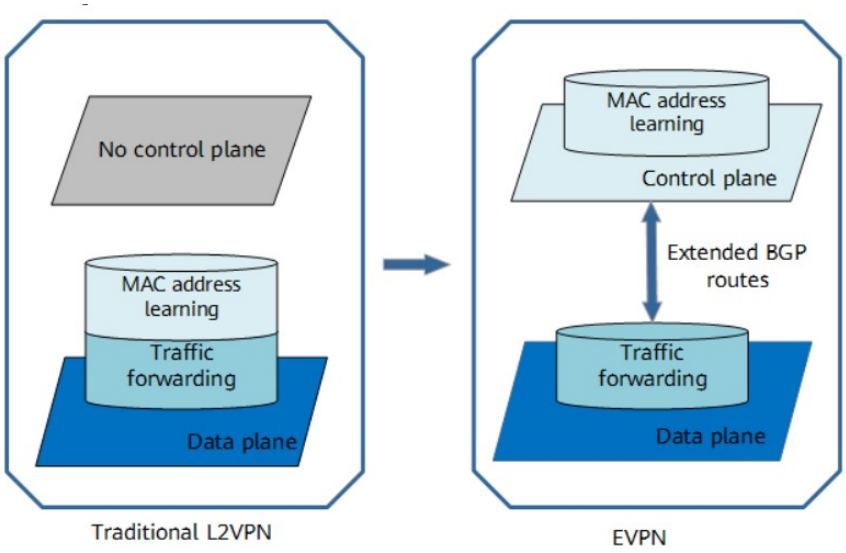

Figura 3.14: Comparação entre EVPN e L2VPN tradicional [49]

Além disso, a EVPN elimina a necessidade de estabelecer ligações completas entre os PEs, pois estes comunicam através do BGP, funcionando como *route reflectors*. Isso reduz a complexidade da rede e a quantidade de mensagens de sinalização. A EVPN também permite que os PEs aprendam endereços MAC locais através do ARP e endereços MAC e IP remotos através de rotas de anúncio MAC/IP. Isto reduz o consumo de recursos da rede, uma vez que os PEs já não necessitam de enviar pedidos ARP para outros PEs. Seguidamente, será analisado o funcionamento da EVPN.

Um *Ethernet Segment* (ES) é formado quando um dispositivo *Customer Edge* (CE) se liga a dois ou mais dispositivos *Provider Edge* (PE) através de ligações *Ethernet*. Essa ligação resulta num ES, identificado por um Ethernet Segment Identifier (ESI). Quando um CE se conecta a apenas um PE, o ESI assume o valor zero.

Para garantir que o CE seja reconhecido como uma única entidade pelo PE, é essencial que todos os PEs ligados ao mesmo CE usem o mesmo ESI nas respetivas interfaces.

Além disso, cada instância do protocolo EVPN é referida como uma EVPN Instance (EVI). De forma análoga a uma Virtual Switching Instance (VSI) no contexto do VPLS, a EVI é usada para identificar um cliente VPN. Cada PE pode suportar várias EVIs, uma vez que a EVPN é um tipo de VPN flexível e escalável.

Para o armazenamento dos endereços MAC adquiridos por uma EVI, é utilizado um MAC-VRF (MAC Virtual Routing and Forwarding). Cada EVI possui o seu próprio MAC-VRF, que armazena exclusivamente os endereços MAC associados a essa instância.

Na Figura 3.15, é possível observar a representação de uma rede EVPN.

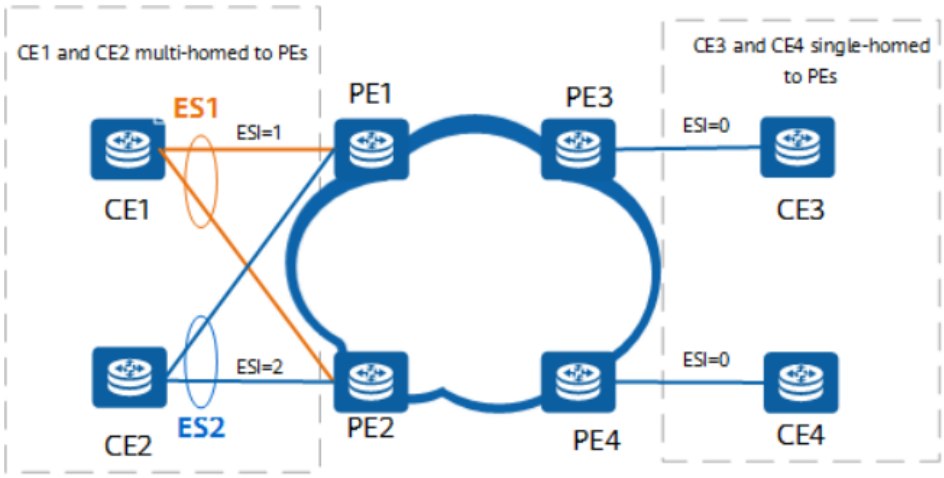

Figura 3.15: Rede EVPN
[49]

A necessidade de usar VXLAN é fundamentada na crescente tendência de virtualização de servidores, que por sua vez promove a migração dinâmica de VMs. Durante essa migração, é crucial manter inalterados os endereços IP e MAC das VMs, garantindo a continuidade dos serviços. Além disso, à medida que o número de clientes em redes virtualizadas aumenta, torna-se essencial ter um isolamento eficiente na rede.

A migração dinâmica das VMs tornou-se uma prática comum, acompanhando a tendência generalizada da virtualização de servidores. Para assegurar que a transição ocorra sem problemas, é imperativo que os endereços IP e o estado das VMs permaneçam inalterados. No entanto, esta necessidade limita a migração dentro do mesmo domínio da Camada 2.

A arquitetura tradicional de rede de três camadas, por sua vez, impõe restrições adicionais à migração dinâmica das VMs. Para permitir uma migração abrangente, é necessário que todos os servidores estejam dentro de um único e amplo domínio da Camada 2.

Foi com base nessa necessidade de migração das VMs e na procura pela implementação num domínio de Camada 2 estendido que surgiu o conceito da VXLAN. A VXLAN cria um túnel virtual na rede IP que viabiliza a comunicação entre os nós de origem e destino, independentemente da estrutura de rede subjacente. A VXLAN efetivamente virtualiza a infraestrutura de rede num vasto "*switch* virtual da Camada 2", permitindo que os servidores se liguem a esse *switch* virtual. Isso significa que as VMs não precisam alterar os seus endereços IP quando são movidas entre "portas".

Adicionalmente, a VXLAN satisfaz a necessidade de isolamento da rede em ambientes com um grande número de clientes. Introduz um identificador

de rede (VNI) no cabeçalho VXLAN, tornando possível a criação de até 16 milhões de segmentos VXLAN, possibilitando a identificação e isolamento eficiente de um grande número de clientes.

3.4 Recolha de informações relativas ao desempenho das redes

Um aspeto crucial a reter da implementação da rede L2VPN/EVPN com transporte VXLAN são as alterações nos prefixos EVPN tipo 3 e tipo 2. Essas modificações desempenham um papel fundamental, conferindo à rede benefícios significativos em termos de eficiência, escalabilidade e operacionalidade. Essas alterações apresentam grande importância:

- **Controlo de Encaminhamento Dinâmico:**
  - **Tipo 3:** Os prefixos EVPN tipo 3 são responsáveis por anunciar informações de sub-redes específicas dentro de uma mesma rede (intra-subnet). Isso permite um controlo dinâmico do encaminhamento entre os dispositivos da mesma sub-rede, otimizando a comunicação local.
  - **Tipo 2:** Os prefixos EVPN tipo 2 lidam com informações de encaminhamento entre sub-redes diferentes. Eles desempenham um papel fundamental ao estender a conectividade de camada 2 entre sub-redes distintas, possibilitando comunicação eficiente em ambientes distribuídos.
- **Escalabilidade:**
  - **Tipo 3:** Ao permitir a comunicação eficiente dentro de uma sub-rede, os prefixos EVPN tipo 3 contribuem para uma escalabilidade otimizada. O encaminhamento dinâmico intra-subnet elimina a necessidade de configurações manuais extensas, facilitando a adição de novos dispositivos à rede.
  - **Tipo 2:** A extensão da conectividade de camada 2 entre sub-redes diferentes por meio de prefixos EVPN tipo 2 mantém a escalabilidade mesmo em ambientes mais amplos, evitando a criação de redes complexas e isoladas.
- **Flexibilidade na Adição de Dispositivos:**
  - **Tipo 3:** Facilita a adição de novos dispositivos na mesma sub-rede sem a necessidade de configurações manuais extensivas. O encaminhamento dinâmico intra-subnet simplifica a integração de novos equipamentos.

  - **Tipo 2:** Simplifica a expansão da rede, permitindo a incorporação de novas sub-redes sem comprometer a conectividade de camada 2. Isso é fundamental para ambientes onde o crescimento é uma constante.

- **Gestão Eficaz de Tráfego:**
  - **Tipo 3:** Contribui para uma gestão mais eficaz do tráfego local, garantindo que os dispositivos na mesma sub-rede comuniquem de maneira eficiente e direta.
  - **Tipo 2:** Permite a comunicação de dispositivos em sub-redes diferentes como se estivessem na mesma rede local, otimizando o tráfego e proporcionando uma experiência de rede unificada.

- **Redução do Overhead de Configuração:**
  - **Tipo 3:** A automação proporcionada pelo encaminhamento dinâmico intra-subnet reduz o overhead de configuração, tornando a manutenção da rede mais simples e menos propensa a erros humanos.
  - **Tipo 2:** A capacidade de estender a conectividade de camada 2 entre sub-redes diferentes sem configurações manuais extensas simplifica a gestão da rede.

Em resumo, as alterações nos prefixos EVPN tipo 3 e tipo 2 são fundamentais para criar redes L2VPN/EVPN com transporte VXLAN eficientes, escaláveis e flexíveis, proporcionando uma base robusta para ambientes de *Datacenter* e redes distribuídas. Essas alterações são essenciais para alcançar um alto desempenho, uma administração simplificada e uma resposta dinâmica à procura no crescimento e evolução da rede.

A seguir, será explicado como os prefixos EVPN tipo 3 e tipo 2 são alterados, recorrendo para o efeito a uma captura de pacotes realizada na ligação Core relativa ao PE1-1.

3.5 Comparação dos dados recolhidos

No decurso da secção 3.1, procedeu-se a uma análise abrangente do desempenho de uma rede baseada no protocolo VXLAN. Um dos principais objetivos foi compreender a transmissão de pacotes entre os routers PE1-1 e PE2-1, concluindo que o protocolo *User Datagram Protocol* (UDP) desempenha um papel central nessa comunicação.

O VXLAN é uma tecnologia destinada a criar uma rede de *overlay* sobre uma infraestrutura existente. Nesse cenário, a escolha do protocolo UDP para encapsular os pacotes VXLAN facilita a comunicação entre os dispositivos VXLAN: o cabeçalho UDP desempenha um papel crucial ao encapsular os pacotes VXLAN, proporcionando um meio eficaz de comunicação entre os *routers* PE1-1 e PE2-1. A utilização do UDP emerge como uma característica distintiva do VXLAN, possibilitando o transporte eficiente dos pacotes VXLAN sobre a rede subjacente.

Outro aspeto fundamental é a identificação da VLAN de origem na ligação VXLAN, que é efetuada através do VXLAN *header* e, mais concretamente, do parâmetro VXLAN *Network ID*. Ao ser transmitido pela rede, o pacote VXLAN com o VXLAN *Network ID* permite que os dispositivos VXLAN nos extremos da comunicação reconheçam a VLAN de origem associada ao pacote. Ou seja, a identificação eficiente da VLAN é facilitada pelo VXLAN, garantindo a integridade e o correto encaminhamento do tráfego entre as redes virtuais.

Por fim, foram exploradas as limitações que surgem na ligação VXLAN quando há mais de dois locais remotos. A restrição observada está relacionada com o aumento do número de VLANs, resultando na necessidade de criar mais túneis. Essa complexidade adicional pode ser um desafio operacional, uma vez que cada VLAN exige a implementação de um túnel VXLAN dedicado. Além disso, surge a preocupação com a propagação de *broadcasts*. À medida que mais túneis VXLAN são estabelecidos para acomodar diversas VLANs, os *broadcasts* têm o potencial de se disseminar por todas essas VLANs. Essa disseminação generalizada de *broadcasts* pode levar a um aumento indesejado do tráfego, impactando negativamente o desempenho global da rede.

Em síntese, este estudo do VXLAN proporcionou uma compreensão das suas aplicações, vantagens e desafios em ambientes de *Datacenter*.

Na secção 3.2, foram extraídas conclusões essenciais sobre a arquitetura BGP *Spine-Leaf* com *Route Reflectors* em comparação com uma configuração completa de BGP *mesh*. Uma das descobertas fundamentais é a vantagem intrínseca do modelo *Spine-Leaf* na simplificação do processo de expansão da rede. Ao adotar uma abordagem *Spine-Leaf*, a adição de novos *routers* à rede é notavelmente facilitada. A necessidade de configurar a vizinhança apenas com o(s) *route reflectors* simplifica substancialmente o procedimento, proporcionando também uma conectividade total entre os

dispositivos. Essa abordagem elimina a complexidade inerente à configuração de todas as possíveis vizinhanças, como seria exigido numa configuração completa de BGP *mesh*.

A principal vantagem evidenciada nesse contexto é a escalabilidade e a eficiência operacional oferecidas pela arquitetura *Spine-Leaf*. À medida que a rede cresce, a adição de novos *routers* torna-se um processo mais ágil e menos propenso a erros, pois a configuração é simplificada e centralizada nos *route reflectors*. Essa simplificação não apenas acelera a implementação, mas também reduz a probabilidade de configurações incorretas, contribuindo para uma administração mais eficaz da rede.

Em conclusão, a escolha da arquitetura BGP *Spine-Leaf* com *route reflectors* não apenas oferece uma solução escalável mas simplifica também significativamente as operações de rede, especialmente quando comparada com uma configuração completa de BGP *mesh*.

3.6 Conclusões

O estudo das tecnologias de redes de *Datacenter* foi feito de forma progressiva, partindo da implementação de uma rede utilizando o protocolo VXLAN, passando pela criação de uma rede L2VPN/EVPN com transporte VXLAN e culminando na análise da integração do EVPN-VXLAN numa infraestrutura empresarial.

A transição para a tecnologia VXLAN marca uma evolução substancial, destacando-se pela capacidade de criar redes virtualmente segmentadas e altamente escaláveis. Por outro lado, a implementação da rede L2VPN/EVPN com transporte VXLAN evidencia-se pela eficiência operacional e flexibilidade, permitindo estender a conectividade de camada 2 entre diferentes sub-redes, facilitando a criação de ambientes dinâmicos distribuídos.

Ao integrar o protocolo EVPN-VXLAN numa infraestrutura empresarial, observam-se impactos positivos nos processos operacionais, na escalabilidade e na eficiência global da rede. Destaca-se o controlo dinâmico do encaminhamento e a automação melhorada, simplificando a gestão da rede e reduzindo a necessidade de configurações manuais extensas.

A combinação de EVPN-VXLAN traz ganhos notáveis em escalabilidade, permitindo comunicação eficiente dentro de uma sub-rede (Tipo 3) e estendendo a conectividade de camada 2 entre sub-redes distintas (Tipo 2). Essa abordagem contribui para ambientes distribuídos e proporciona uma unificação eficaz, permitindo uma comunicação eficiente entre dispositivos localizados em sub-redes diferentes.

A simplicidade na adição de novos dispositivos e a expansão da rede são aspectos destacados pelos tipos 3 e 2, simplificando a integração de novos equipamentos e facilitando o crescimento contínuo. A gestão eficaz do tráfego, tanto local quanto entre sub-redes, é crucial para garantir uma

experiência de rede otimizada.

As tecnologias VXLAN, L2VPN/EVPN e EVPN-VXLAN emergem assim como soluções robustas e eficazes para redes de *Datacenter*, abrangendo desde ambientes virtualmente segmentados até redes empresariais distribuídas, oferecendo respostas adaptáveis e eficientes para diferentes cenários.

Capítulo 4

Conclusão

Neste capítulo é feita uma reflexão sobre os resultados do estudo efetuado. Para além disso, são identificados os obstáculos encontrados durante o desenvolvimento da dissertação e são identificados os contributos do trabalho que foi desenvolvido. Finalmente, são explanadas algumas perspetivas de trabalho futuro.

Da realização deste estudo foi possível, antes de mais, aprofundar o conhecimento em várias áreas ligadas às redes de *Datacenter*: o mecanismo EVPN, o protocolo VXLAN e a arquitetura SDN. Estas áreas desempenham um papel crucial na evolução do desempenho destas redes, sendo fundamentais para as suas operações atuais e futuras.

A dissertação teve como objetivo principal investigar os conceitos relacionados com as tecnologias para redes de *datacenter*, um tópico extremamente atual devido à crescente quantidade de dados e tráfego, que implica a necessidade de aumentar a capacidade de resposta destas infraestruturas.

Assim, o trabalho começou por um enquadramento teórico abrangente que abordou diversos tópicos fundamentais para compreender o contexto das redes e tecnologias de *Datacenter*. Foram abordados os desafios inerentes à escala e eficiência das redes de comunicações, que se foram tornando cada vez mais relevantes à medida que as redes se expandiram e se tornaram mais complexas.

Seguidamente, abordou-se a evolução das LANs, destacando a sua importância nas infraestruturas de comunicação corporativas. Também se analisou a necessidade de segmentação das redes, incluindo a implementação de VLANs e estratégias de isolamento lógico.

Concretamente no contexto dos *Datacenters*, examinou-se a arquitetura das redes e a sua evolução ao longo do tempo, tendo em consideração as crescentes exigências de capacidade e desempenho. Nesse sentido, foram abordadas as redes de *overlay*, incluindo o protocolo VXLAN, que desempenha um papel fundamental na criação de ambientes virtuais nos *Datacenters*.

Seguidamente, considerou-se a integração com tecnologias emergentes,

identificando tendências e inovações que estão a moldar o futuro destas redes, com foco nas SDN. Para além disso, refletiu-se sobre a importância da eficiência energética e sustentabilidade nas operações de *Datacenter*, bem como as considerações de segurança fundamentais para proteger essas infraestruturas críticas. Por último, explorou-se a temática das redes de *Datacenter* na era da IA, considerando o potencial transformador que esta tecnologia poderá ter na manutenção, otimização e segurança dessas redes.

Este estudo teórico proporcionou uma base sólida para o desenvolvimento do estudo prático, permitindo a compreensão das tecnologias e conceitos que estão a moldar as atuais redes de *Datacenter*. No capítulo 3, procedeu-se à implementação de duas redes, utilizando protocolos previamente discutidos, nomeadamente o VXLAN e o EVPN. Na secção 3.3, foi estudada a integração destes protocolos com o objetivo de discutir o seu funcionamento e potenciais vantagens. Durante a implementação foram recolhidas informações relevantes para análise posterior, levada a cabo essencialmente no capítulo 4. Em concreto, as tecnologias EVPN-VXLAN revelaram-se cruciais nas redes de *Datacenter* empresariais.

4.1 Limitações do estudo

Durante a execução do estudo, foi encontrada uma limitação significativa: a impossibilidade de realizar simulações e procedimentos práticos no computador pessoal. Restrições de espaço de armazenamento tornaram impraticável a implementação no GNS3, uma ferramenta crucial para a execução das redes emuladas. Adicionalmente, foram enfrentados desafios ao iniciar as máquinas virtuais necessárias para as simulações.

Para contornar essas limitações, recorreu-se a um computador disponibilizado pela Universidade num dos laboratórios de redes, com as inerentes limitações de horário, dada a necessidade de compatibilizar o trabalho com as aulas que habitualmente decorrem nesse espaço.

4.2 Perspetivas de trabalho futuro

Tendo por base o estudo realizado, sugere-se uma abordagem mais aprofundada em trabalhos futuros, com especial ênfase na otimização do desempenho da rede. Essa otimização poderá ser alcançada através de ajustes nas configurações existentes, bem como pela avaliação minuciosa da viabilidade de eventuais atualizações de *hardware*, visando aprimorar a eficiência e a capacidade da infraestrutura.

De forma complementar, torna-se imperativo proceder a uma análise mais exaustiva dos custos inerentes à implementação e manutenção destas tecnologias, especialmente para as organizações que equacionam a sua adoção. Aprofundar a investigação sobre a resiliência da rede, ponderar estra-

tégias de redundância e realizar avaliações detalhadas de cenários de falha surgem como aspetos cruciais para garantir uma disponibilidade contínua e eficaz. Este aspeto reveste-se de particular importância em ambientes de *Datacenter* reais, onde a continuidade operacional é vital para a sustentabilidade e desempenho da infraestrutura tecnológica.

No âmbito da segurança, destaca-se a importância de incorporar medidas robustas, como criptografia e controlo de acessos, para reforçar a proteção dos dados e dos equipamentos. A pesquisa e integração de tecnologias emergentes também se revelam essenciais, no sentido de identificar soluções que complementem ou aprimorem as já implementadas.

Adicionalmente, estudos de caso práticos que demonstrem a aplicação real destas tecnologias em ambientes específicos de *Datacenter* proporcionariam uma compreensão mais profunda dos benefícios práticos. Uma descrição mais detalhada, incluindo procedimentos de configuração e manutenção, não só facilitaria a replicação do ambiente, como também contribuiria para uma eficaz disseminação de conhecimento.

Bibliografia

[1] Chester L. Meek. Encyclopedia of computer science. *Discrete Mathematics*, page 1068, 2003.

[2] Pat Jackman. The evolution of telecommunications. *IEEE*, 2000.

[3] Somayya Madakam, R. Ramaswamy, and Siddharth Tripathi. Internet of things (iot): A literature review. *Journal of Computer and Communications*, 2015.

[4] IT Insights. Tráfego de dados na europa continua a atingir recordes, 2020. `https://www.itinsight.pt/news/operacao/trafego-de-dados-na-europa-continua-a-atingir-recordes`.

[5] Saurabh Shukla, Mohd Fadzil Hassan, Duc Chung Tran, Rehan Akbar, and Irving Vitra Paputungan. Improving latency in internet-of-things and cloud computing for real-time data transmission: a systematic literature review (slr). *Cluster Computing*, 2021.

[6] ANACOM. Factos & números. Technical report, ANACOM, 2023. `https://www.anacom.pt/render.jsp?contentId=1749673`.

[7] Mah-Rukh Fida and Mahesh K. Marina. Impact of device diversity on crowdsourced mobile coverage maps. pages 348–352, 2018.

[8] Nasr Almurisi and Srinivasulu Tadisetty. Cloud-based virtualization environment for iot-based wsn: solutions, approaches and challenges. *Journal of Ambient Intelligence and Humanized Computing*, 2022.

[9] CHIEN-CHANG Liu and LI-DER CHOU. 5g/b5g network slice management via staged reinforcement learning. *IEEE*, 2023.

[10] NGMN Alliance. Ngmn 5g white paper. 2015.

[11] Ons Aouedi, Kandaraj Piamrat, and Benoît Parrein. Intelligent traffic management in next-generation networks. *Future Internet*, 2022.

[12] Juliana Akemi Nakamura. Evolução das redes de telecomunicação e o multiprotocol label switching (mpls), 2009.

[13] Adrien. Qu'est ce qu'un vlan ?, 2018. https://apprendrelereseau.fr/quest-ce-quun-vlan/.

[14] D.D. Clark, K.T. Pogran, and D.P. Reed. An introduction to local area networks. *Proceedings of the IEEE*, 66(11):1497–1517, 1978.

[15] Neal Wagner, Cem Ş. Şahin, Michael Winterrose, James Riordan, Jaime Pena, Diana Hanson, and William W. Streilein. Towards automated cyber decision support: A case study on network segmentation for security. In *2016 IEEE Symposium Series on Computational Intelligence (SSCI)*, pages 1–10, 2016.

[16] CISCO. What is network segmentation? https://www.cisco.com/c/en/us/products/security/what-is-network-segmentation.html.

[17] Manisha Barse and Rodney Manuel. Evolution of vlan. *International Journal of Innovations in Engineering Research and Technology*, pages 1–9, 2015.

[18] Faisal Shahriar and Jiancun Fan. Performance analysis of fhrp in a vlan network with stp. In *2020 IEEE 3rd International Conference on Electronics Technology (ICET)*, pages 814–818, 2020.

[19] Kashif Bilal, Saif Ur Rehman Malik, Samee U. Khan, and Albert Y. Zomaya. Trends and challenges in cloud datacenters. *IEEE Cloud Computing*, 1(1):10–20, 2014.

[20] CISCO. What is a data center?, 2023. https://www.cisco.com/c/en/us/solutions/data-center-virtualization/what-is-a-data-center.html?dtid=osscdc000283.

[21] Paul Kirvan. Cluster. 09 2022. https://www.techtarget.com/whatis/definition/cluster.

[22] Raj Jain. Data center network topologies, 2013. https://www.cse.wustl.edu/~jain/cse570-13/ftp/m_03dct.pdf.

[23] Sneha Mishra. Comprehensive guide to data center network architectures, 2023. https://go4hosting.com/blog/data-centers/comprehensive-guide-to-data-center-network-architectures/.

[24] Md. Faizul Bari, Raouf Boutaba, Rafael Esteves, Lisandro Zambenedetti Granville, Maxim Podlesny, Md Golam Rabbani, Qi Zhang, and Mohamed Faten Zhani. Data center network virtualization: A survey. *IEEE COMMUNICATIONS SURVEYS TUTORIALS*, 15(2), 2015. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6308765.

[25] Ethan Banks. Data center network design moves from tree to leaf, 2013. https://www.techtarget.com/searchdatacenter/feature/Data-center-network-design-moves-from-tree-to-leaf.

[26] Dinil Mon Divakaran, Tho Le, and Mohan Gurusamy. An online integrated resource allocator for guaranteed performance in data centers. *Parallel and Distributed Systems, IEEE Transactions on*, 25:1382–1392, 06 2014.

[27] Miguel Quinteiro Ribeiro. Micro-services based application for data center dimensioning. pages 9–16, 10 2023.

[28] Shahzad Khan. Hyperconverged infrastructure, 2018. https://www.vmantra.in/hyperconverged-infrastructure/.

[29] Abhishek Jayakar Shetty and Ganashree K. C. Comprehensive review of datacenter architecture evolution. *International Research Journal of Engineering and Technology (IRJET)*, 07:5–6, 05 2020. https://d1wqtxts1xzle7.cloudfront.net/64616588/IRJET-V7I51396-libre.pdf?1602063642=&response-content-disposition=inline%3B+filename%3DIRJET_Comprehensive_review_of_datacenter.pdf&Expires=1700155058&Signature=eL8ktxnvIcOs36l5K~NFgvQiFXOMRqM-AI2CYt9Zjuvw~p98~mdM5WYHKtNt9F-YUQggNHuXvbX20sa_&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA.

[30] Jordi Paillissé Vilanova. Next generation overlay networks : security, trust, and deployment challenges, 2021.

[31] Adriana-Elena Rădoi and Cristian-Iulian Rîncu. Integration of data center network technologies vxlan, bgp, evpn. *IEEE Xplore*, 2022.

[32] Katie Terrell Hanna. flooding (network). 2021. https://www.techtarget.com/searchnetworking/definition/flooding.

[33] CISCO. Configure vxlan. 2022. https://www.cisco.com/c/en/us/support/docs/switches/nexus-9000-series-switches/118978-config-vxlan-00.html?dtid=osscdc000283#anc6.

[34] JOSE MIGUEL-ALONSO. A research review of openflow for datacenter networking. *IEEE Access*, 2022. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=10004580.

[35] Kristián Košt'ál, Rastislav Bencel, Michal Ries, and Ivan Kotuliak. Performance evaluation of sdn wlan architecture. pages 1–7, 2018.

[36] ZHIFENG ZHAO, FENG HONG, and RONGPENG LI. Sdn based vxlan optimization in cloud computing networks. *IEEE Access*, 2017.

[37] JOÃO MANUEL ALVES DE MESQUITA BACELO. Integração de funções de rede virtualizadas e funções de rede físicas, 2021.

[38] National Institute of Standards and Technology. Information technology laboratory - computer security resource center. https://csrc.nist.gov/glossary/term/commercial_off_the_shelf.

[39] RAFAEL SOUZA, KELVIN DIAS, and STÊNIO FERNANDES. Nfv data centers: A systematic review. *IEEE Access*, 2019.

[40] Cameron Hashemi-Pour. reinforcement learning. 2023. https://www.techtarget.com/searchenterpriseai/definition/reinforcement-learning.

[41] Neda Shalavi, Giovanni Perin, Andrea Zanella, and Michele Rossi. Energy efficient deployment and orchestration of computing resources at the network edge: a survey on algorithms, trends and open challenges, 2022. https://arxiv.org/pdf/2209.14141.pdf.

[42] Energetic sustainability of routing algorithms for energy-harvesting wireless sensor networks. *Computer Communications*, 30(14):2976–2986, 2007. Network Coverage and Routing Schemes for Wireless Sensor Networks.

[43] Quentin Schueller, Kashinath Basu, Muhammad Younas, Mohit Patel, and Frank Ball. A hierarchical intrusion detection system using support vector machine for sdn network in cloud data center. *IEEE Access*, 2018.

[44] Sarah Abdulrezzak and Firas A. Sabir. Enhancing intrusion prevention in snort system. *IEEE Access*, 2023.

[45] I. Indu, P.M. Rubesh Anand, and Vidhyacharan Bhaskar. Identity and access management in cloud environment: Mechanisms and challenges. *Engineering Science and Technology, an International Journal*, 21(4):574–588, 2018. https://www.sciencedirect.com/science/article/pii/S2215098617316750.

[46] Zhenqian Feng, Haitao Wu, and Jinshu Su. Exploring potential vulnerabilities in data center network. 2019. https://dl.acm.org/doi/pdf/10.1145/1921206.1921219.

[47] Brian Sparks. Networking for data centers and the era of ai. https://developer.nvidia.com/blog/networking-for-data-centers-and-the-era-of-ai/.

[48] K. Duda P. Agarwal L. Kreeger T. Sridhar M. Bursell C. Wright M. Mahalingam, D. Dutt. Virtual extensible local area network (vxlan): A framework for overlaying virtualized layer 2 networks over layer

3 networks. 08 2014. https://www.rfc-editor.org/rfc/pdfrfc/rfc7348.txt.pdf.

[49] Chen Li and Wang Shengnan. Information technology laboratory - computer security resource center, 2023. https://info.support.huawei.com/info-finder/encyclopedia/en/EVPN.html.