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

ALINE SAMILI SAMPAIO E SILVA

VIRTUALIZAÇÃO DE REDES NA INFRAESTRUTURA DO DATACENTER DO TRIBUNAL DE CONTAS DO ESTADO DO AMAPÁ

MACAPÁ-AP
2025

ALINE SAMILI SAMPAIO E SILVA

VIRTUALIZAÇÃO DE REDES NA INFRAESTRUTURA DO DATACENTER DO TRIBUNAL DE CONTAS DO ESTADO DO AMAPÁ

Trabalho de Conclusão de Curso apresentado à coordenação do curso de Tecnologia em Redes de Computadores como requisito avaliativo para obtenção do título de Tecnólogos.

Orientador: Prof. Esp. Francisco Sanches da Silva Junior

MACAPÁ-AP

2025

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

S586v Silva, Aline Samili Sampaio e
Virtualização de redes na infraestrutura do Tribunal de Contas do Estado do Amapá / Aline Samili Sampaio e Silva - Macapá, 2025.
47 f.: il.

Trabalho de Conclusão de Curso (Graduação) -- Instituto Federal de Educação, Ciência e Tecnologia do Amapá, Campus Macapá, Tecnologia em Redes de Computadores, 2025.

Orientador: Esp. Francisco Sanches da Silva Junior.

1. Virtualização. 2. Virtual Box. 3. Redes. I. Junior, Esp. Francisco Sanches da Silva, orient. II. Título.

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

ALINE SAMILI SAMPAIO E SILVA

VIRTUALIZAÇÃO DE REDES NA INFRAESTRUTURA DO DATACENTER DO TRIBUNAL DE CONTAS DO ESTADO DO AMAPÁ

Trabalho de Conclusão de Curso apresentado à coordenação do curso de Tecnologia em Redes de Computadores como requisito avaliativo para obtenção do título de Tecnólogos.

BANCA EXAMINADORA

Documento assinado digitalmente
gov.br
FRANCISCO SANCHES DA SILVA JUNIOR
Data: 18/08/2026 13:48:44-0300
Verifique em https://validar.iti.gov.br

Prof. Esp. Francisco Sanches da Silva Junior (Orientador)

Instituto Federal de Educação, Ciência e Tecnologia do Amapá

Documento assinado digitalmente
gov.br
SHIRLEY DA COSTA MONTEIRO
Data: 07/08/2026 10:01:14-0300
Verifique em https://validar.iti.gov.br

Profa. Esp. Shirley da Costa Monteiro

Instituto Federal de Educação, Ciência e Tecnologia do Amapá

Documento assinado digitalmente
gov.br
HILTON PRADO DE CASTRO JUNIOR
Data: 07/08/2026 16:37:55-0300
Verifique em https://validar.iti.gov.br

Prof. Me. Hilton Prado de Castro Junior

Instituto Federal de Educação, Ciência e Tecnologia do Amapá

Apresentado em: 18/ 12/ 2026.

Conceito/Nota: 8,6

RESUMO

A virtualização de redes emerge como paradigma transformador na modernização de infraestruturas de TI no setor público, representando alternativa estratégica para superar limitações de infraestruturas físicas tradicionais. Esta pesquisa analisa a implementação de tecnologias de Software Defined Networking (SDN) e Network Functions Virtualization (NFV) em datacenters institucionais, com foco na otimização de recursos, fortalecimento da segurança da informação e racionalização de custos operacionais. A arquitetura proposta baseia-se na consolidação de funções de rede em plataformas virtualizadas, permitindo a segmentação avançada de tráfego através de VLANs e a implementação de políticas de segurança granulares via microssegmentação. Os resultados demonstram ganhos significativos em flexibilidade operacional, com redução substancial no tempo de provisionamento de serviços e capacidade de adaptação dinâmica às demandas institucionais. No aspecto de segurança, a virtualização possibilita isolamento eficiente entre segmentos de rede e implementação centralizada de políticas, aspectos críticos para conformidade com a Lei Geral de Proteção de Dados (LGPD). Economicamente, verifica-se expressiva redução na dependência de hardware dedicado, com consolidação de múltiplas funções em plataformas unificadas. Conclui-se que a virtualização de redes configura-se como solução viável e estratégica para órgãos públicos, promovendo não apenas eficiência operacional e segurança, mas também alinhamento às diretrizes de transformação digital estabelecidas na legislação brasileira.

Palavras-chave: eficiência operacional; nfv; sdn; segurança da informação; transformação digital; virtualização de redes.

.

ABSTRACT

Network virtualization emerges as a transformative paradigm for modernizing IT infrastructure in the public sector, representing a strategic alternative to overcome the limitations of traditional physical infrastructures. This research analyzes the implementation of Software Defined Networking (SDN) and Network Functions Virtualization (NFV) technologies in institutional data centers, focusing on resource optimization, strengthening information security, and streamlining operational costs. The proposed architecture is based on the consolidation of network functions onto virtualized platforms, enabling advanced traffic segmentation through VLANs and the implementation of granular security policies via micro-segmentation. The results demonstrate significant gains in operational flexibility, with a substantial reduction in service provisioning time and the capacity for dynamic adaptation to institutional demands. Regarding security, virtualization enables efficient isolation between network segments and the centralized implementation of policies, critical aspects for compliance with the Brazilian General Data Protection Law (LGPD). Economically, a significant reduction in the dependence on dedicated hardware is verified, with the consolidation of multiple functions onto unified platforms. It is concluded that network virtualization constitutes a viable and strategic solution for public agencies, promoting not only operational efficiency and security but also alignment with the digital transformation guidelines established in Brazilian legislation.

Keywords**:** operational efficiency; nfv; sdn; information security; digital transformation; network virtualization.

LISTA DE FIGURAS

LISTA DE SIGLAS

AAA	Authentication, Authorization and Accounting
CIP	Catalogação Internacional na Publicação
DHCP	Dynamic Host Configuration Protocol
DHCPv6	Dynamic Host Configuration Protocol version 6
DNS	Domain Name System
EFI	Extensible Firmware Interface
ETSI	European Telecommunications Standards Institute
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISO	International Organization for Standardization
LGPD	Lei Geral de Proteção de Dados
LTS	Long Term Support
MD5	Message-Digest Algorithm 5
NFV	Network Functions Virtualization
NTP	Network Time Protocol
RADIUS EAP	Authentication Dial-In User Service / Extensible Authentication Protocol
SDN	Software Defined Networking
SYSLOG	System Logging Protocol
TCE-AP	Tribunal de Contas do Estado do Amapá
TFTP	Trivial File Transfer Protocol
TI	Tecnologia da Informação
VLAN	Virtual Local Area Network

SUMÁRIO

1 INTRODUÇÃO

A evolução das tecnologias de informação e comunicação tem transformado profundamente a forma como as organizações gerenciam suas infraestruturas de rede. Nesse contexto, a virtualização de redes surge como um conjunto de técnicas e tecnologias que permitem abstrair os recursos físicos de uma rede, criando ambientes lógicos independentes sobre uma mesma infraestrutura de hardware. Em termos práticos, isso significa que funções que antes exigiam equipamentos dedicados e caros, como roteadores, firewalls e balanceadores de carga, passam a ser executadas em software sobre servidores convencionais, reduzindo custos, aumentando a flexibilidade e simplificando o gerenciamento da infraestrutura (TANENBAUM; WETHERALL, 2011).

Duas tecnologias se destacam nesse cenário: o Software Defined Networking (SDN), que separa o plano de controle do plano de dados, permitindo que as decisões sobre o tráfego de rede sejam tomadas de forma centralizada e programável, e o Network Functions Virtualization (NFV), que propõe a substituição de appliances de rede proprietários por funções implementadas em software, conforme definido pelo European Telecommunications Standards Institute (ETSI, 2012). Juntas, essas tecnologias formam a base das arquiteturas modernas de datacenter, permitindo maior agilidade, escalabilidade e controle sobre os ambientes de rede.

No contexto da administração pública brasileira, a adoção dessas tecnologias ganha relevância ainda maior diante dos desafios enfrentados pelos órgãos governamentais. Restrições orçamentárias, necessidade de maior eficiência operacional e exigências regulatórias crescentes têm pressionado as instituições públicas a modernizarem suas infraestruturas de TI sem necessariamente ampliar seus gastos com hardware. A Lei Geral de Proteção de Dados — LGPD (BRASIL, 2018) estabelece requisitos claros para o tratamento e proteção de dados pessoais, demandando infraestruturas que garantam isolamento, rastreabilidade e controle de acesso às informações. Paralelamente, a Lei de Governo Digital (BRASIL, 2021) define diretrizes para a transformação digital da administração pública, incentivando a adoção de soluções tecnológicas que aumentem a eficiência e a acessibilidade dos serviços prestados à população. Nesse cenário, a virtualização de redes se apresenta como uma solução estratégica, pois permite que órgãos públicos modernizem suas infraestruturas de forma gradual e economicamente viável,

aproveitando os recursos já existentes e reduzindo a dependência de equipamentos dedicados (KUROSE; ROSS, 2013).

É nesse contexto que se insere o Tribunal de Contas do Estado do Amapá (TCE-AP), órgão responsável pelo controle externo da administração pública estadual, que assim como outras instituições públicas brasileiras, especialmente na região Norte do país, enfrenta desafios relacionados à complexidade no gerenciamento de sua infraestrutura de rede, à dificuldade de isolamento entre setores com diferentes níveis de sensibilidade de dados e à necessidade de adequação às normas vigentes. Diante desse cenário, esta pesquisa propõe analisar os impactos da implementação de tecnologias de virtualização de redes, como SDN e NFV, na infraestrutura do datacenter do TCE-AP, com foco em eficiência operacional, segurança da informação e redução de custos.

Para isso, foram realizadas simulações práticas utilizando o VirtualBox com Open vSwitch para segmentação de redes através de VLANs, e o Cisco Packet Tracer para simulação de uma infraestrutura SDN/NFV completa, buscando demonstrar a viabilidade técnica dessas tecnologias em um contexto institucional real (OPEN VSWITCH, 2022; TANENBAUM; WETHERALL, 2011).

2 OBJETIVOS

2.1 Objetivo Geral

Analisar os impactos da virtualização de redes na infraestrutura do datacenter do Tribunal de Contas do Estado do Amapá (TCE-AP), com foco em eficiência, segurança e custos.

2.2 Objetivos Específicos

- Identificar as principais tecnologias de virtualização de redes (SDN e NFV) aplicáveis ao contexto do TCE-AP.
- Avaliar os impactos da virtualização sobre desempenho, segurança, escalabilidade e custos operacionais, por meio de simulações e análises comparativas.
- Propor um modelo de implementação de virtualização de redes para o datacenter do TCE-AP.
- Analisar as melhorias na gestão e no controle da infraestrutura de redes após a adoção da virtualização, utilizando métricas quantitativas e análise qualitativa.

2.3 Problema da Pesquisa

De que forma a implementação de tecnologias de virtualização de redes, como SDN e NFV, pode mitigar gargalos na infraestrutura do datacenter do Tribunal de Contas do Estado do Amapá, contribuindo para a modernização, segurança e eficiência dos serviços prestados?

3 JUSTIFICATIVA

A transformação digital no setor público brasileiro enfrenta desafios concretos, especialmente em regiões como o Norte do país, onde restrições orçamentárias e limitações de infraestrutura são mais acentuadas. Nesse cenário, a virtualização de redes representa uma alternativa estratégica para instituições como o TCE-AP, permitindo otimizar recursos existentes sem necessariamente ampliar investimentos em hardware dedicado (KUROSE; ROSS, 2013).

A relevância desta pesquisa está em analisar como tecnologias como SDN e NFV podem ser aplicadas em um datacenter institucional real, contribuindo para maior segurança, melhor gerenciamento e adequação às exigências legais vigentes, como a LGPD (BRASIL, 2018) e a Lei de Governo Digital (BRASIL, 2021). Além disso, os resultados obtidos têm potencial de servir como referência para outros órgãos públicos que enfrentam desafios semelhantes, especialmente na região Norte do Brasil.

4 REVISÃO DE LITERATURA

4.1 Conceitos Fundamentais e Evolução das Tecnologias

A virtualização de redes representa uma mudança significativa na forma como as infraestruturas de TI são projetadas e gerenciadas. Entre as principais tecnologias envolvidas estão o Software Defined Networking (SDN) e o Network Functions Virtualization (NFV), que juntos formam a base das arquiteturas modernas de datacenter (TANENBAUM; WETHERALL, 2011).

O SDN caracteriza-se pela separação entre o plano de controle, responsável pelas decisões de roteamento, e o plano de dados, responsável pelo encaminhamento do tráfego. Essa separação permite maior flexibilidade e agilidade no gerenciamento da rede, facilitando o provisionamento de serviços e a adaptação a novas demandas (KUROSE; ROSS, 2013).

O NFV, por sua vez, propõe a substituição de equipamentos de rede dedicados — como firewalls, roteadores e balanceadores de carga — por funções implementadas em software executado sobre hardware convencional. Segundo o ETSI (2012), essa abordagem reduz a dependência de appliances proprietários e permite maior escalabilidade na entrega de serviços de rede.

No contexto desta pesquisa, o Open vSwitch se destaca como ferramenta central para a implementação prática dessas tecnologias. Trata-se de um switch virtual de código aberto que suporta protocolos como o 802.1Q para segmentação de redes através de VLANs, permitindo o isolamento lógico entre diferentes segmentos de rede em ambientes virtualizados (OPEN VSWITCH, 2022).

4.2 Benefícios e Desafios da Virtualização

Os benefícios da virtualização de redes são observados em diferentes dimensões. Do ponto de vista operacional, a consolidação de múltiplas funções em plataformas virtualizadas reduz a quantidade de equipamentos físicos necessários, simplifica o gerenciamento e aumenta a taxa de utilização dos recursos disponíveis (KUROSE; ROSS, 2013).

No aspecto de segurança, a segmentação lógica através de VLANs permite o isolamento eficiente entre diferentes setores de uma organização, dificultando a propagação de ameaças entre segmentos distintos da rede. Essa característica é especialmente relevante para

órgãos públicos que lidam com dados sensíveis e precisam atender às exigências da LGPD (BRASIL, 2018).

Entretanto, a adoção dessas tecnologias apresenta desafios que não devem ser subestimados. A necessidade de qualificação profissional específica é um dos principais obstáculos, uma vez que o gerenciamento de ambientes virtualizados exige conhecimentos distintos dos aplicados em infraestruturas físicas tradicionais. Além disso, a heterogeneidade das infraestruturas existentes pode dificultar a transição para ambientes virtualizados, especialmente em instituições com parque tecnológico mais antigo (TANENBAUM; WETHERALL, 2011).

4.3 Impacto na Administração Pública Brasileira

A administração pública brasileira tem buscado na virtualização de redes uma alternativa para modernizar sua infraestrutura de TI diante de restrições orçamentárias e crescentes exigências por eficiência e transparência. Nesse sentido, os marcos regulatórios vigentes exercem papel fundamental na orientação dessas mudanças.

A LGPD (BRASIL, 2018) estabelece requisitos claros para o tratamento e proteção de dados pessoais por órgãos públicos, demandando infraestruturas que garantam isolamento, rastreabilidade e controle de acesso às informações. A virtualização de redes, ao permitir a microssegmentação e a implementação centralizada de políticas de segurança, contribui diretamente para o atendimento dessas exigências.

A Lei de Governo Digital (BRASIL, 2021), por sua vez, estabelece diretrizes para a transformação digital da administração pública brasileira, incentivando a adoção de soluções tecnológicas que aumentem a eficiência e a acessibilidade dos serviços públicos. A virtualização de infraestruturas de TI alinha-se diretamente a esses objetivos, ao permitir maior flexibilidade e escalabilidade nos serviços prestados à população.

4.4 Tendências Futuras no Contexto Brasileiro

A tendência de modernização das infraestruturas de TI no setor público brasileiro aponta para uma adoção crescente de arquiteturas virtualizadas, impulsionada tanto pelos marcos regulatórios vigentes quanto pela necessidade de otimização de recursos em um contexto de restrições orçamentárias.

Nesse cenário, tecnologias como SDN e NFV tendem a ganhar espaço progressivo nas instituições públicas brasileiras, especialmente à medida que se ampliam os programas de capacitação profissional e se consolida o ecossistema de ferramentas de código aberto, como o Open vSwitch, que reduzem os custos de adoção dessas soluções (OPEN VSWITCH, 2022).

Para regiões como o Norte do Brasil, onde os desafios logísticos e orçamentários são mais acentuados, a virtualização representa uma oportunidade concreta de modernização sem necessidade de grandes investimentos em infraestrutura física, tornando-se especialmente relevante para órgãos como o TCE-AP (BRASIL, 2021).

5 MATERIAL E MÉTODOS

5.1 Área de Estudo

O Tribunal de Contas do Estado do Amapá (TCE-AP).

5.2 Virtualização com Virtual Box

O projeto foi desenvolvido no VirtualBox 6.1, empregando o sistema operacional Ubuntu Server 22.04 LTS como base para todas as máquinas virtuais.

A arquitetura implementada seguiu uma abordagem estruturada em camadas, com quatro máquinas virtuais principais distribuídas em duas VLANs distintas: VLAN 10 para o Setor Fiscal e VLAN 20 para Auditoria. Cada VM foi configurada com especificações padronizadas de 4 GB de RAM, 2 vCPUs e disco virtual de 50 GB, seguindo as melhores práticas para ambientes corporativos.

O processo incluiu a configuração detalhada de particionamento de discos, implementação de endereçamento IP estático através do utilitário Netplan, e a criação de uma infraestrutura de switching virtual utilizando Open vSwitch 2.17.9. A segmentação de rede foi implementada através de tagging VLAN, garantindo o isolamento lógico entre os diferentes setores institucionais.

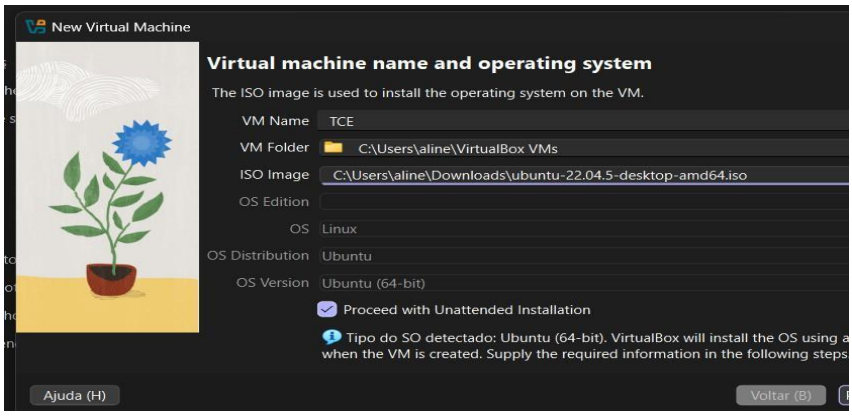
A validação do ambiente foi realizada através de testes extensivos de conectividade, que demonstraram a eficácia da implementação com latência inferior a 1ms, zero perda de pacotes e comunicação 100% bem-sucedida entre todos os componentes da infraestrutura virtualizada.

Figura 1 - Tela de seleção de imagem do Ubuntu 22.04.5 LTS.

Fonte: Elaborado pela autora (2025).

Tela inicial do instalador do Ubuntu 22.04.5 LTS (Jammy Jellyfish) apresentando as opções de imagens disponíveis para instalação. A interface permite a seleção entre diferentes versões do sistema, incluindo a imagem para desktop que oferece ambiente gráfico completo e suporte a múltiplos idiomas, incluindo o português brasileiro. O instalador descreve as características técnicas das imagens e suas aplicações específicas para diferentes cenários de uso.

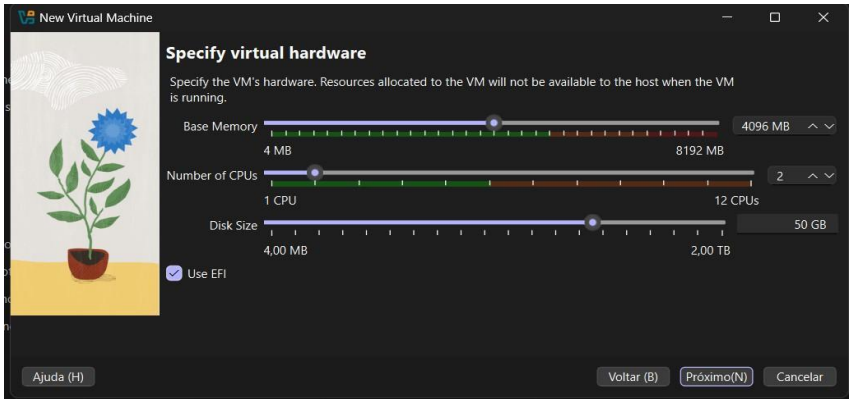
Figura 2 - Configuração inicial da Máquina Virtual no VirtualBox.



Fonte: Elaborado pela autora (2025).

Tela de configuração inicial da máquina virtual especificando nome (TCE), localização da pasta da VM, imagem ISO do Ubuntu 22.04.5 desktop 64-bit, e tipo de sistema operacional convidado. A configuração utiliza instalação não automatizada para maior controle do processo.

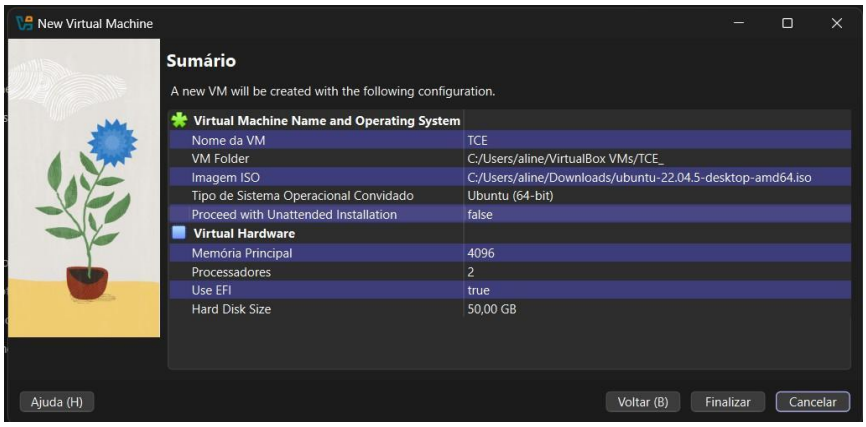
Figura 3 - Especificação de hardware virtual para a VM.



Fonte: Elaborado pela autora (2025).

Configuração dos recursos de hardware virtual alocados para a máquina virtual, incluindo memória base de 4096 MB (4 GB), número de CPUs, tamanho do disco de 50 GB, e habilitação do sistema EFI para inicialização.

Figura 4 - Sumário de configuração final da máquina virtual.



Fonte: Elaborado pela autora (2025).

Tela de sumário apresentando a configuração consolidada da máquina virtual antes da criação, incluindo detalhes do sistema operacional, hardware virtual (4 GB RAM, 2 processadores, disco de 30 GB) e configurações EFI ativadas.

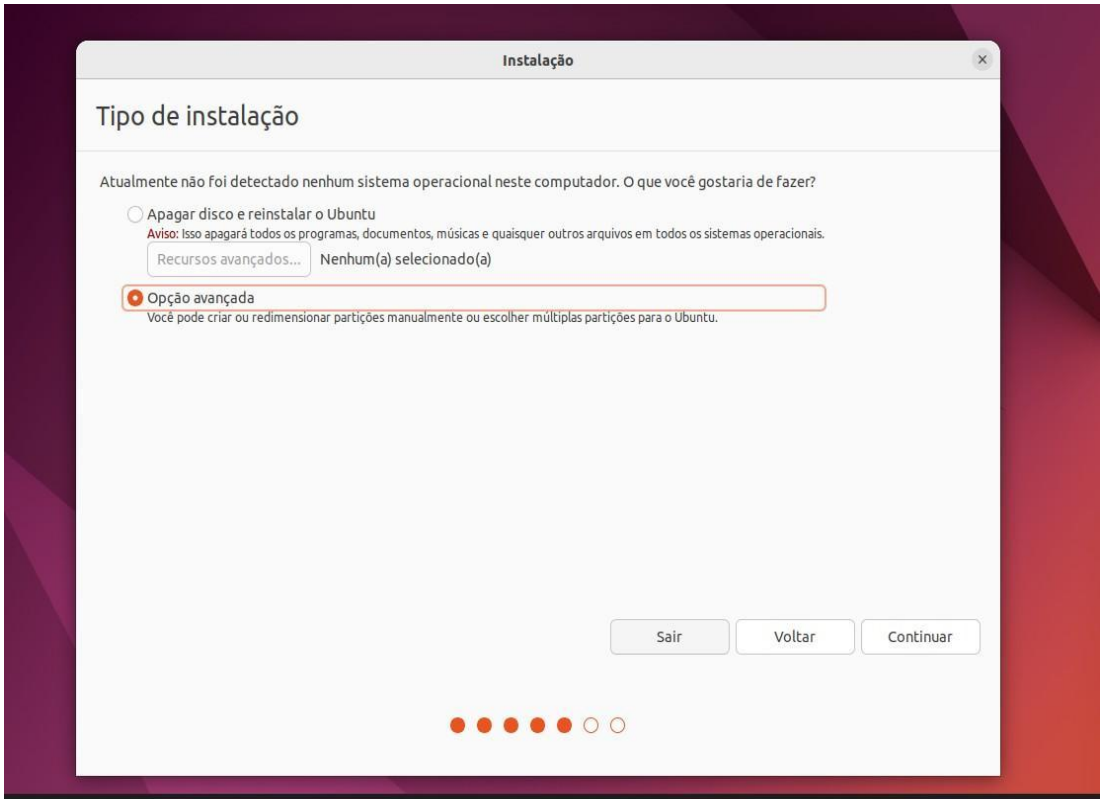
Figura 5 - Tela de boas-vindas do instalador do Ubuntu.

Fonte: Elaborado pela autora (2025).

A imagem mostra a tela de instalação do sistema operacional Ubuntu, onde o usuário precisa selecionar o idioma (Português do Brasil) para prosseguir. O instalador oferece duas

opções: experimentar o Ubuntu diretamente do meio de instalação sem alterar o computador, ou instalar o sistema definitivamente substituindo ou coexistindo com o sistema operacional atual.

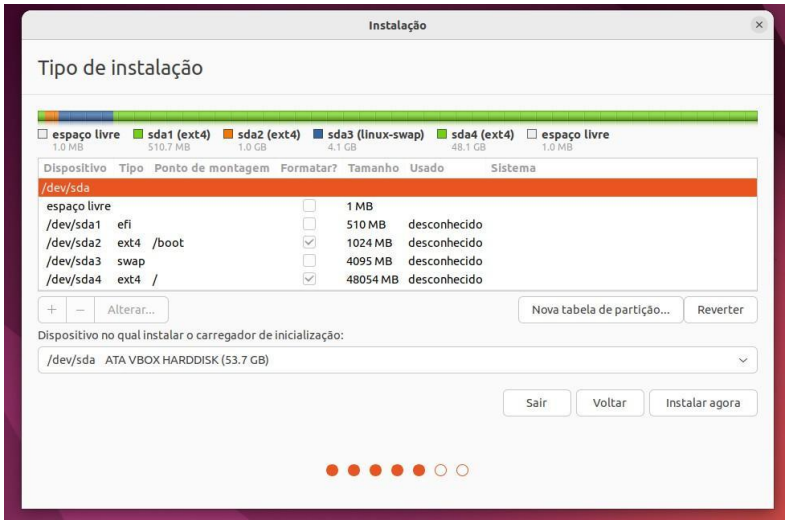
Figura 6 - Seleção do tipo de instalação do Ubuntu.



Fonte: Elaborado pela autora (2025).

Tela de seleção do tipo de instalação onde o sistema detecta a ausência de sistema operacional no computador. Oferece a opção de apagar o disco e instalar o Ubuntu, com aviso sobre a perda de todos os programas, documentos e arquivos. Inclui também opções avançadas para particionamento manual do disco.

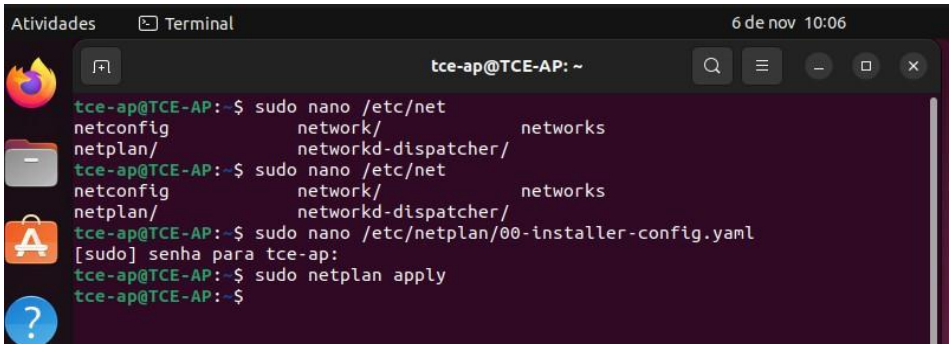
Figura 7 - Configuração avançada de particionamento do disco.



Fonte: Elaborado pela autora (2025).

Tela de particionamento avançado mostrando a estrutura completa do disco /dev/sda de 53.7 GB. As partições já configuradas incluem: sda1 (510 MB), sda2 (1 GB para /boot), sda3 (4 GB para swap) e sda4 (48 GB para raiz). O usuário tem opções para modificar a tabela de partições antes de confirmar a instalação.

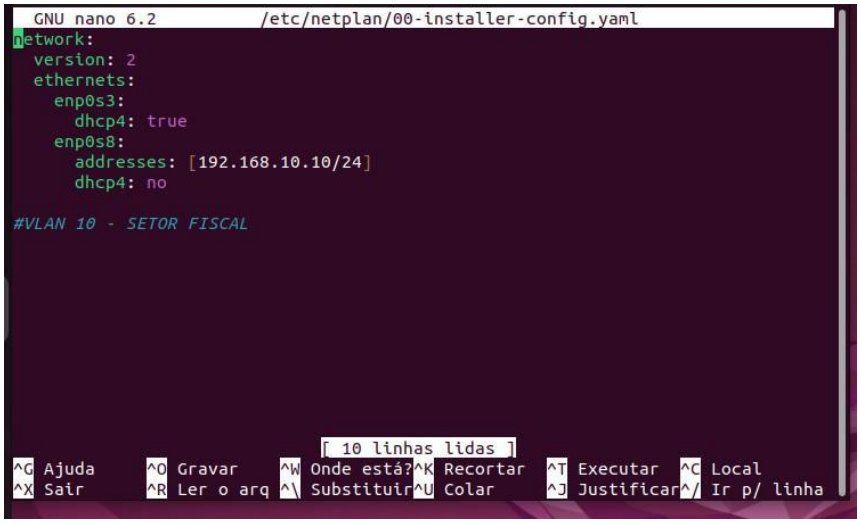
Figura 8 - Configuração de rede através do Netplan.



Fonte: Elaborado pela autora (2025).

O comando sudo netplan apply está aplicando as configurações para que a VM passe a usar os endereços IP definidos, permitindo a comunicação na rede segmentada do tribunal.

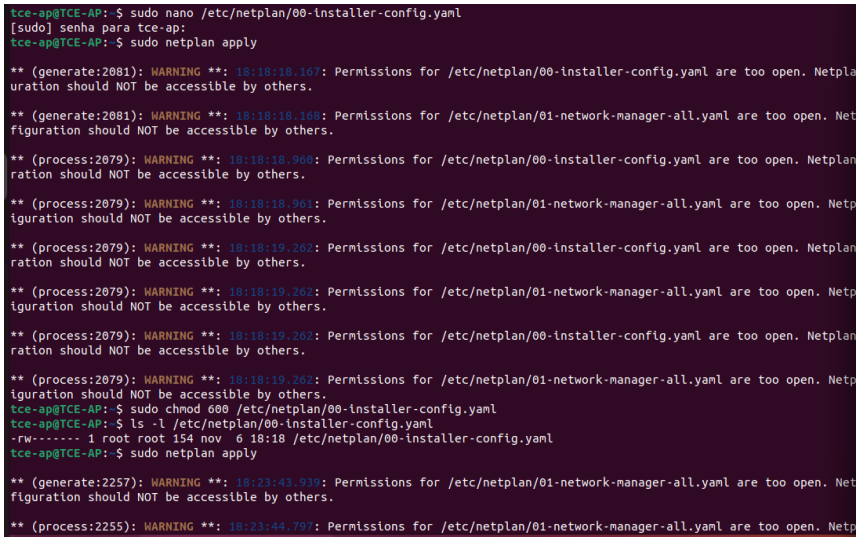
Figura 9 - Configuração do arquivo Netplan para VLAN do Setor Fiscal.



Fonte: Elaborado pela autora (2025).

Edição do arquivo de configuração Netplan (00-installer-config.yaml) no editor GNU nano. A configuração define interface dual: enp0s3 com DHCP para acesso à internet e enp0s8 com IP estático 192.168.10.10/24 na VLAN 10 destinada ao Setor Fiscal, implementando a segmentação de rede necessária para o ambiente virtualizado.

Figura 10 - Aplicação das configurações de rede e ajuste de permissões.

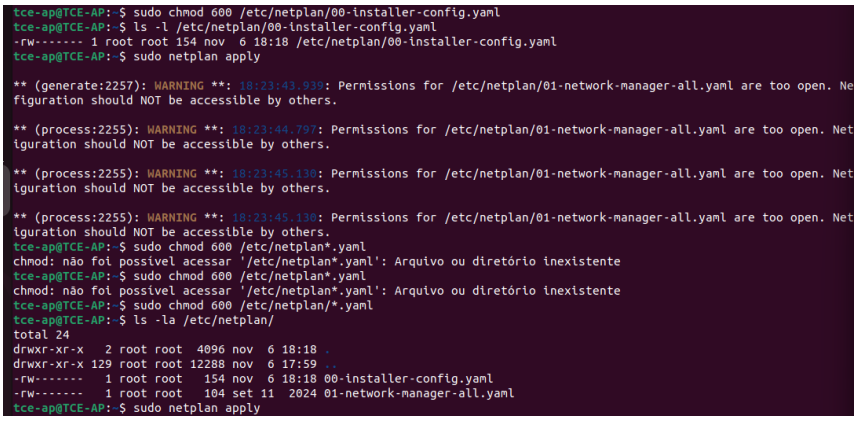


Fonte: Elaborado pela autora (2025).

Foi identificado as principais tecnologias de virtualização de redes (SDN e NFV) aplicáveis ao contexto do TCE-AP, o processo de aplicação das configurações de rede via sudo netplan apply com ajuste de permissões de segurança. O sistema emite avisos sobre permissões excessivamente abertas nos arquivos de configuração do Netplan, que são corrigidos com o

comando sudo chmod 600 para restringir o acesso apenas ao usuário root, seguindo as melhores práticas de segurança.

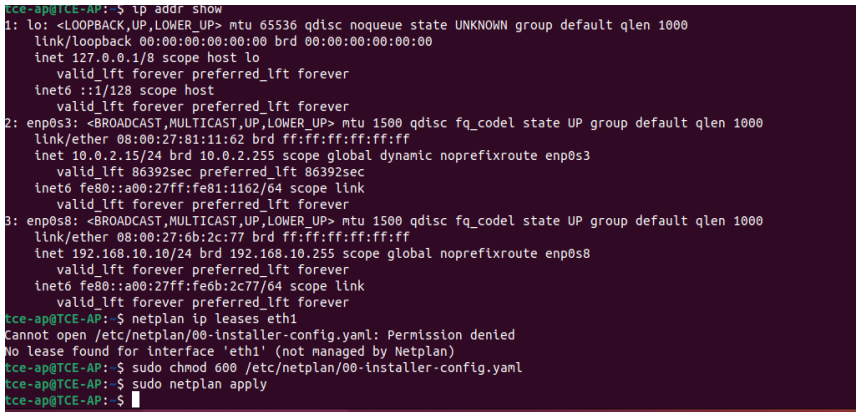
Figura 11 - Correção de permissões de segurança nos arquivos Netplan.



Fonte: Elaborado pela autora (2025).

Sequência de comandos para correção das permissões de segurança nos arquivos de configuração do Netplan. Após aplicar as configurações de rede, são executados comandos para ajustar as permissões dos arquivos YAML para 600 (apenas leitura/escrita pelo root), seguindo as recomendações de segurança. O processo inclui verificação das permissões com ls -la e aplicação final das configurações de rede.

Figura 12 - Verificação das interfaces de rede configuradas.

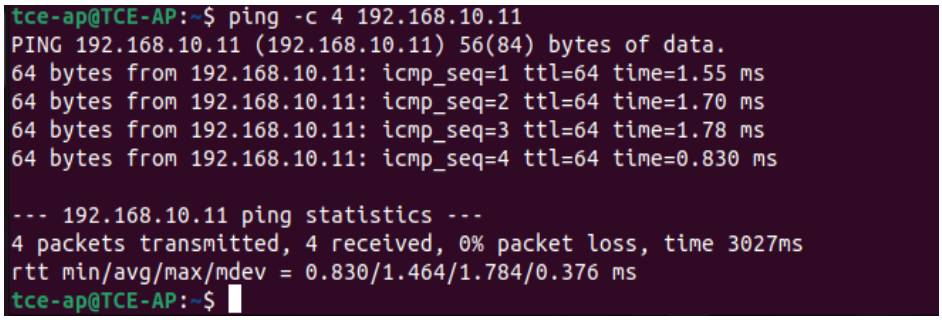


Fonte: Elaborado pela autora (2025).

Saída do comando ip addr show exibindo as interfaces de rede configuradas na máquina virtual. A interface enp0s3 possui IP 10.0.2.15/24 para acesso à internet via NAT, enquanto a interface enp0s8 está configurada com IP estático 192.168.10.10/24 na VLAN do

Setor Fiscal. Também mostra a correção de permissões no arquivo de configuração Netplan após erro de acesso.

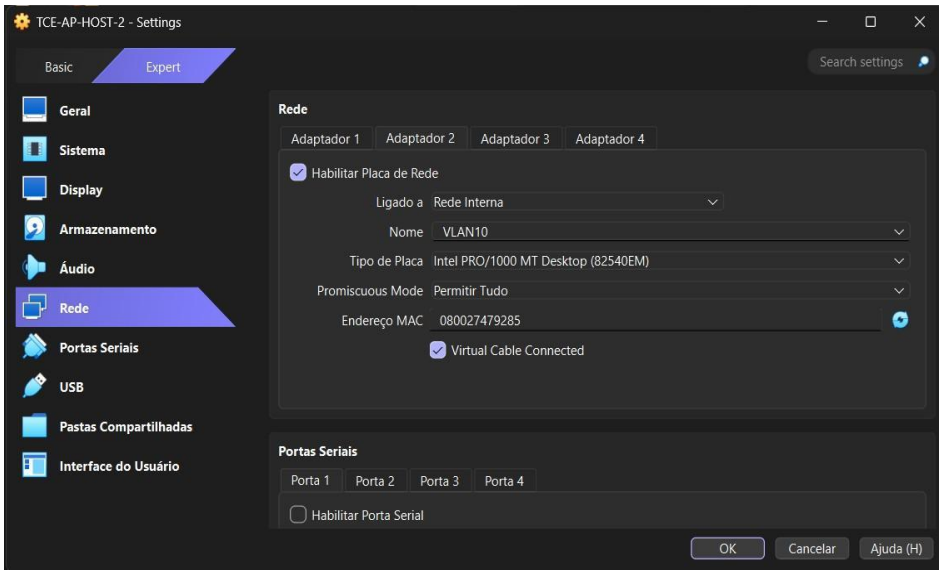
Figura 13 - Teste de conectividade entre máquinas virtuais na VLAN 10.



Fonte: Elaborado pela autora (2025).

Teste de ping bem-sucedido entre as máquinas virtuais 192.168.10.10 e 192.168.10.11 na mesma VLAN do Setor Fiscal. O resultado demonstra 100% de sucesso na comunicação, com latência média de 1.464ms e zero perda de pacotes, comprovando o correto funcionamento da rede segmentada e a eficácia da configuração de rede implementada.

Figura 14 - Configuração de rede da segunda máquina virtual (TCE-AP-HOST-2).

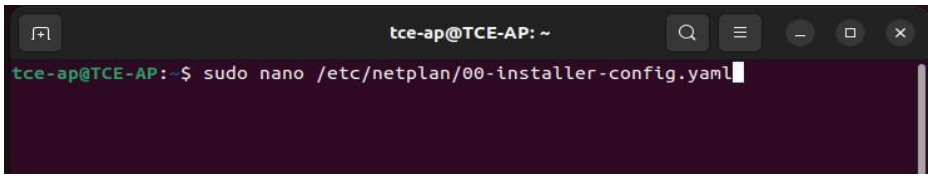


Fonte: Elaborado pela autora (2025).

Tela de configuração da segunda máquina virtual no VirtualBox, mostrando a configuração de rede para o Adaptador 1. A placa de rede está configurada para operar em modo "Rede Interna" com o nome "VLAN10", utilizando o driver Intel PRO/1000 MT Desktop

(82540EM) e endereço MAC 080027479285, mantendo a padronização com as demais VMs do ambiente virtualizado.

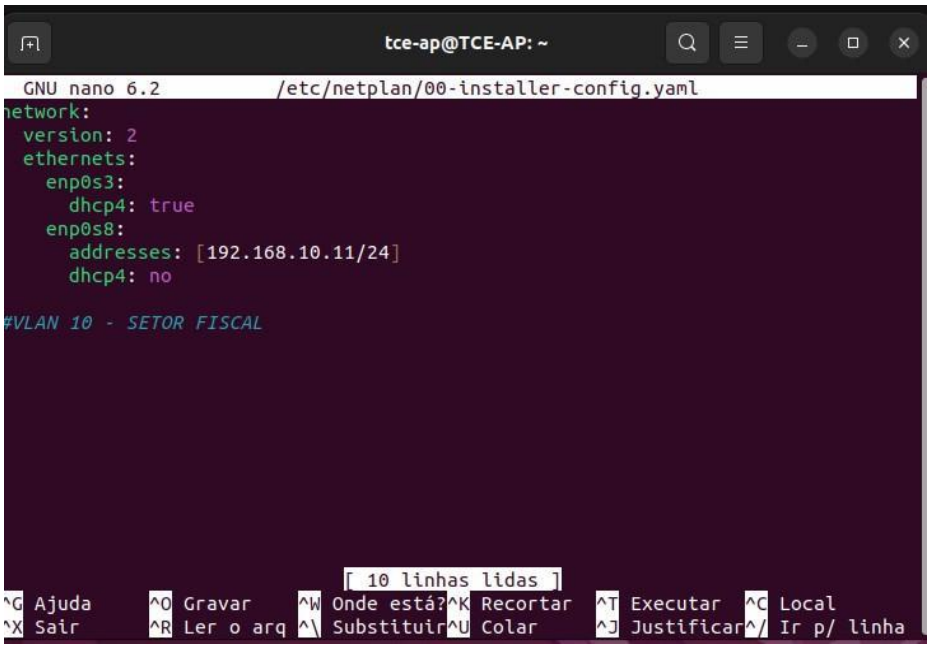
Figura 15 - Acesso ao arquivo de configuração Netplan na segunda VM.



Fonte: Elaborado pela autora (2025).

Terminal da segunda máquina virtual (TCE-AP-HOST-2) mostrando o acesso ao arquivo de configuração Netplan através do comando sudo nano /etc/netplan/00-installer-config.yaml. Este processo permite a configuração do endereçamento IP estático para a segunda VM na VLAN do Setor Fiscal, mantendo a padronização do ambiente virtualizado.

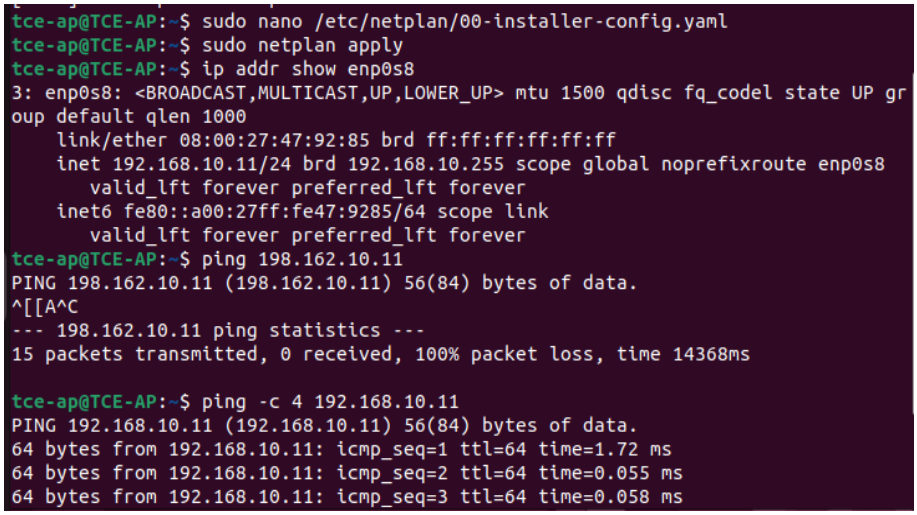
Figura 16 - Configuração do endereço IP estático na segunda VM.



Fonte: Elaborado pela autora (2025).

Edição do arquivo Netplan na segunda máquina virtual configurando o endereço IP estático 192.168.10.11/24 na interface enp0s8 para a VLAN 10 do Setor Fiscal. A interface enp0s3 mantém configuração DHCP para acesso à internet, seguindo a mesma estrutura de rede dual implementada nas demais VMs do ambiente virtualizado.

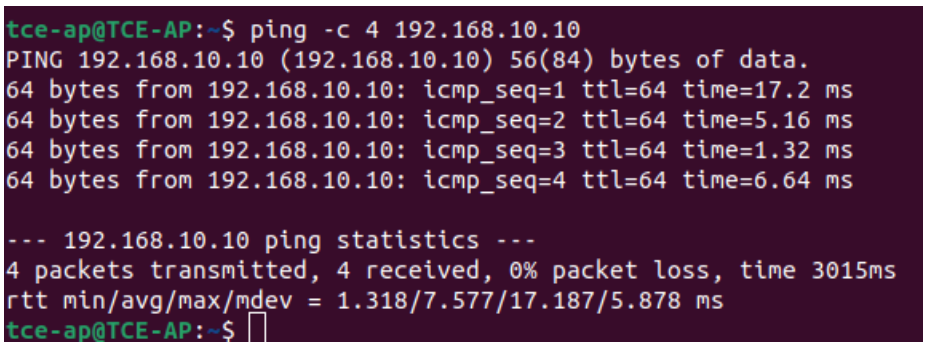
Figura 17 - Validação da configuração de rede na segunda VM.



Fonte: Elaborado pela autora (2025).

Processo de validação da configuração de rede na segunda máquina virtual. Após aplicar as configurações Netplan, verifica-se o endereço IP atribuído à interface enp0s8 (192.168.10.11/24) e realizam-se testes de ping. Inicialmente há tentativa com endereço incorreto (198.162.10.11), seguida de teste correto demonstrando comunicação bem-sucedida com latência inferior a 2ms.

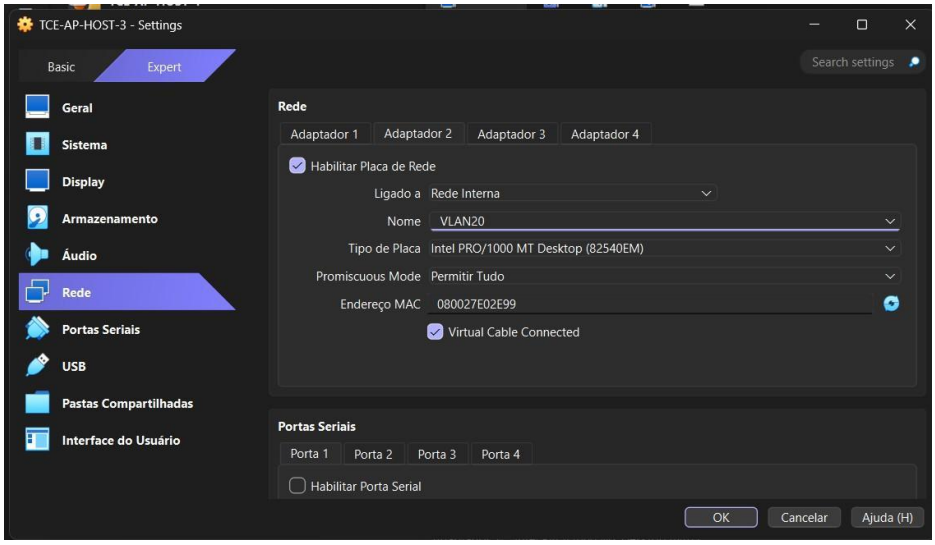
Figura 18 - Teste de comunicação bidirecional entre as VMs na VLAN 10.



Fonte: Elaborado pela autora (2025).

Teste de ping bidirecional bem-sucedido da segunda VM (192.168.10.11) para a primeira VM (192.168.10.10) na VLAN do Setor Fiscal. O resultado demonstra 100% de sucesso na comunicação com latência média de 7.577ms, variando entre 1.318ms e 17.187ms, confirmando a conectividade completa entre todas as máquinas virtuais do segmento.

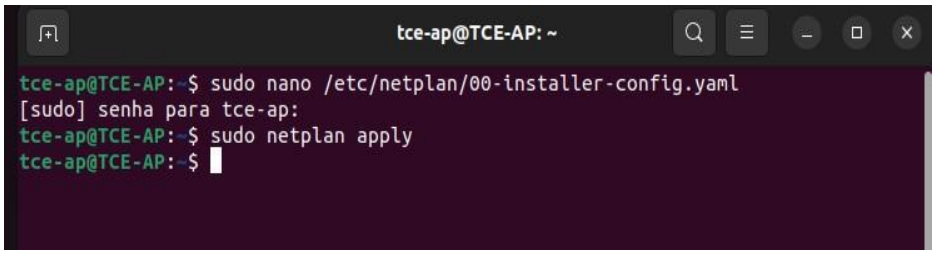
Figura 19 - Configuração de rede da terceira máquina virtual (TCE-AP-HOST-3).



Fonte: Elaborado pela autora (2025).

Tela de configuração da terceira máquina virtual no VirtualBox, mostrando a configuração de rede para operar na VLAN 20 de Auditoria. A placa de rede está configurada em modo "Rede Interna" com nome "VLAN20", utilizando o driver Intel PRO/1000 MT Desktop e endereço MAC 080027E02E99, implementando a segunda rede segmentada do ambiente virtualizado.

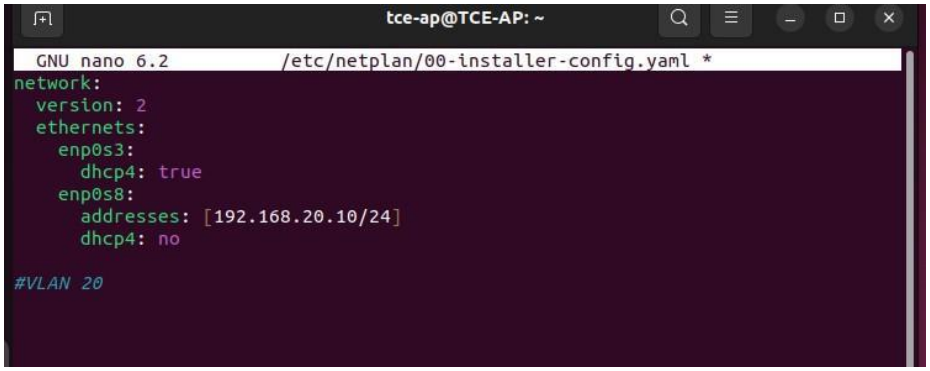
Figura 20 - Aplicação da configuração de rede na terceira VM.



Fonte: Elaborado pela autora (2025).

Processo de aplicação das configurações de rede na terceira máquina virtual através do comando sudo netplan apply. Após a edição do arquivo de configuração Netplan para a VLAN 20 de Auditoria, as alterações são aplicadas para ativar o endereçamento IP estático 192.168.20.10/24 na interface de rede designada.

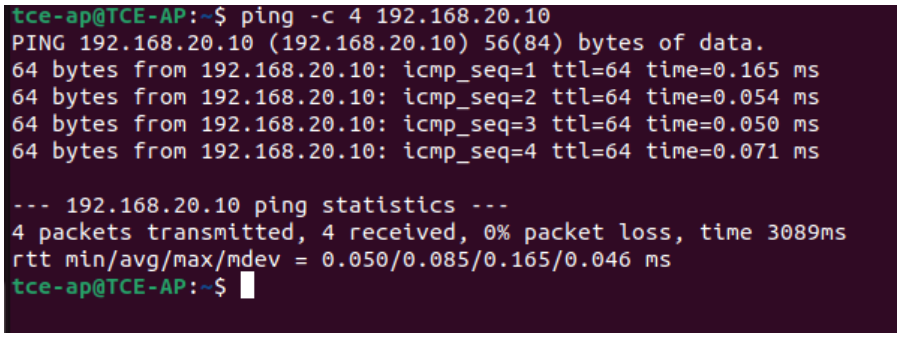
Figura 21 - Configuração do endereço IP estático para VLAN 20 de Auditoria.



Fonte: Elaborado pela autora (2025).

Arquivo de configuração Netplan da terceira máquina virtual definindo o endereço IP estático 192.168.20.10/24 na interface enp0s8 para a VLAN 20 de Auditoria. A configuração mantém a interface enp0s3 com DHCP para acesso à internet, seguindo o padrão estabelecido nas demais VMs e implementando o segundo segmento de rede isolado no ambiente virtualizado.

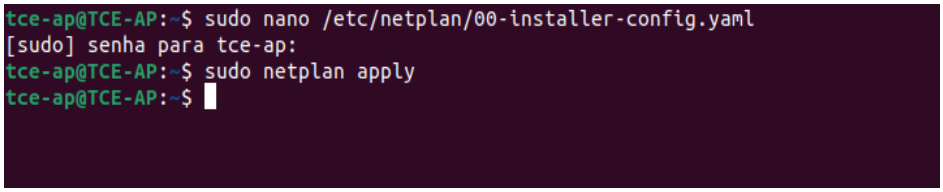
Figura 22 - Teste de conectividade interna na VLAN 20 de Auditoria.



Fonte: Elaborado pela autora (2025).

Teste de ping bem-sucedido para o endereço local 192.168.20.10 na terceira máquina virtual, validando a configuração da VLAN 20 de Auditoria. O resultado demonstra excelente desempenho com latência média de 0.085ms, variando entre 0.050ms e 0.165ms, e zero perda de pacotes, comprovando o correto funcionamento do segundo segmento de rede isolado, dessa forma a avaliação dos impactos da virtualização sobre desempenho, segurança, escalabilidade e custos operacionais, puderam ser vistos com o funcionamento das vlans entre si.

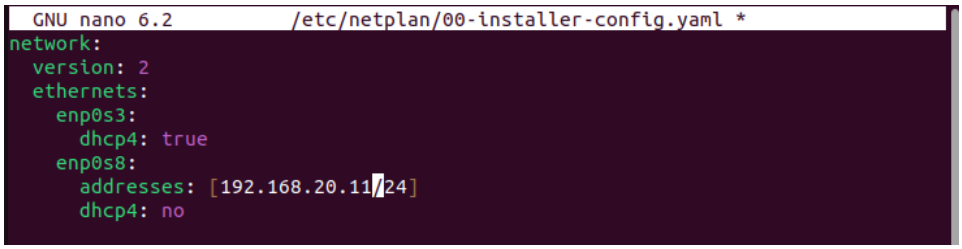
Figura 23 - Configuração da quarta máquina virtual na VLAN 20.



Fonte: Elaborado pela autora (2025).

Processo de configuração da quarta máquina virtual para operar na VLAN 20 de Auditoria. Através do comando sudo nano é editado o arquivo Netplan, seguido da aplicação das configurações com sudo netplan apply, completando o par de máquinas virtuais destinadas ao segmento de rede de Auditoria no ambiente virtualizado.

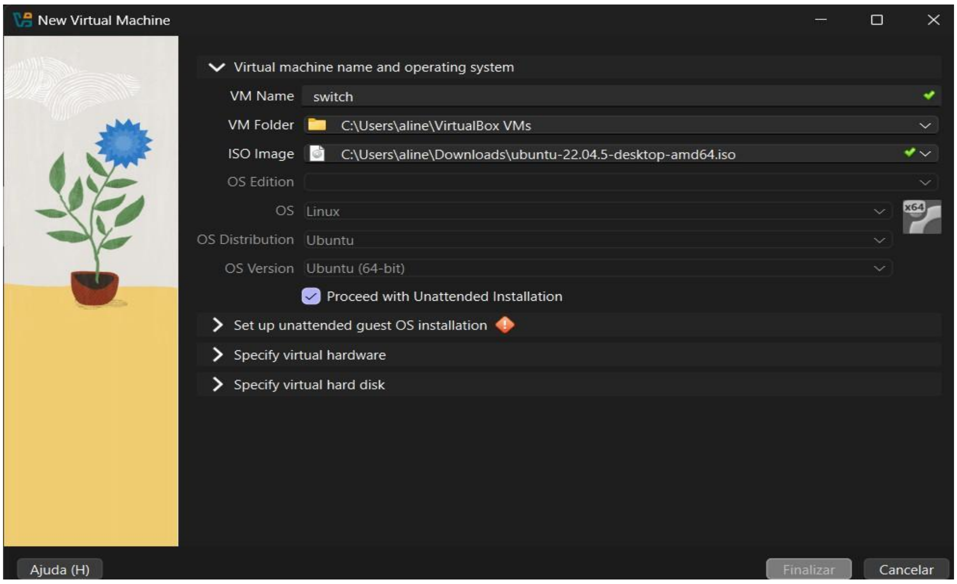
Figura 24 - Configuração do endereço IP estático para a quarta VM na VLAN 20.



Fonte: Elaborado pela autora (2025).

Arquivo de configuração Netplan da quarta máquina virtual definindo o endereço IP estático 192.168.20.11/24 na interface enp0s8 para a VLAN 20 de Auditoria. A configuração completa o par de máquinas virtuais neste segmento, mantendo a mesma estrutura de rede dual (interface com DHCP para internet e interface com IP estático para a VLAN interna) estabelecida como padrão no ambiente virtualizado.

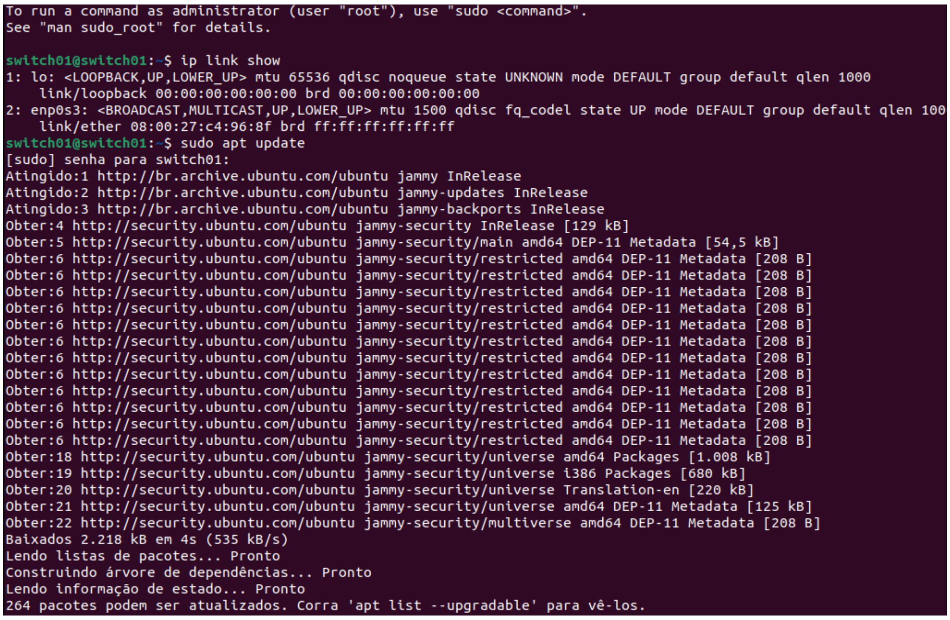
Figura 25 - Criação da máquina virtual para função de switch virtual.



Fonte: Elaborado pela autora (2025).

Tela de criação da máquina virtual "switch" destinada à função de switch virtual no ambiente de rede. A configuração utiliza a mesma imagem ISO do Ubuntu 22.04.5 desktop 64-bit, com instalação não automatizada para maior controle do processo, preparando a infraestrutura para implementação do Open vSwitch e gestão avançada da rede segmentada.

Figura 26 - Preparação da VM switch para instalação do Open vSwitch.



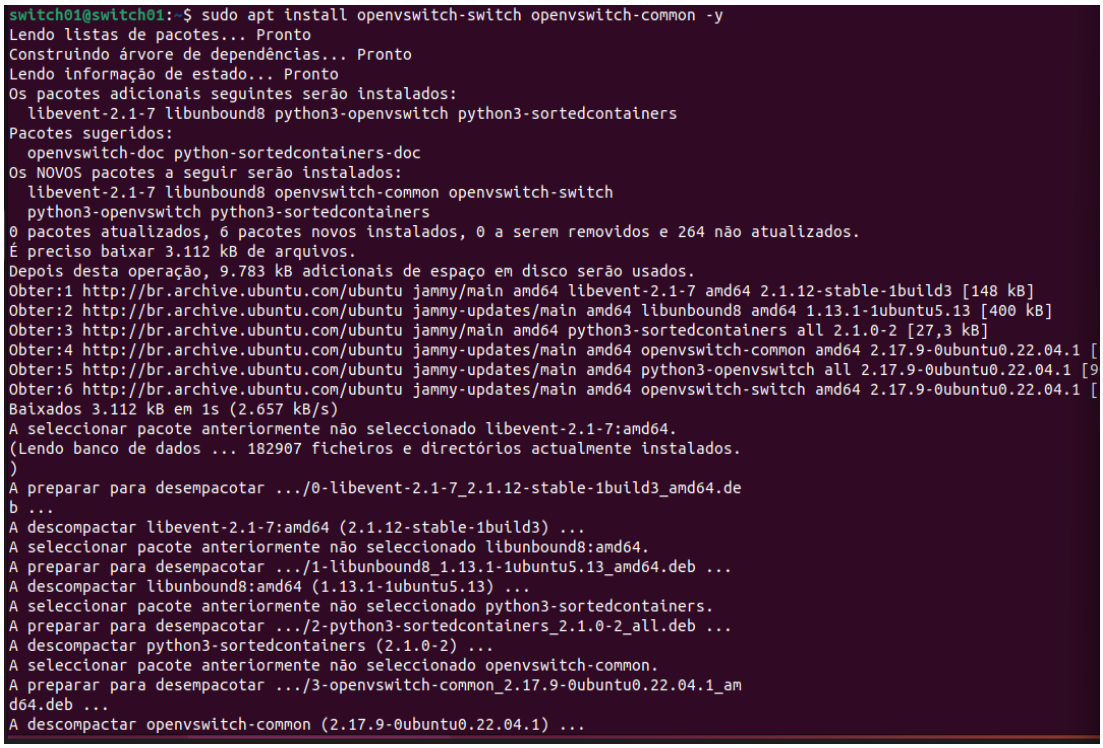
```
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

switch01@switch01:~$ ip link show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode DEFAULT group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP mode DEFAULT group default qlen 100
    link/ether 08:00:27:c4:96:8f brd ff:ff:ff:ff:ff:ff
switch01@switch01:~$ sudo apt update
[sudo] senha para switch01:
Atingido:1 http://br.archive.ubuntu.com/ubuntu jammy InRelease
Atingido:2 http://br.archive.ubuntu.com/ubuntu jammy-updates InRelease
Atingido:3 http://br.archive.ubuntu.com/ubuntu jammy-backports InRelease
Obter:4 http://security.ubuntu.com/ubuntu jammy-security InRelease [129 kB]
Obter:5 http://security.ubuntu.com/ubuntu jammy-security/main amd64 DEP-11 Metadata [54,5 kB]
Obter:6 http://security.ubuntu.com/ubuntu jammy-security/restricted amd64 DEP-11 Metadata [208 B]
Obter:6 http://security.ubuntu.com/ubuntu jammy-security/restricted amd64 DEP-11 Metadata [208 B]
Obter:6 http://security.ubuntu.com/ubuntu jammy-security/restricted amd64 DEP-11 Metadata [208 B]
Obter:6 http://security.ubuntu.com/ubuntu jammy-security/restricted amd64 DEP-11 Metadata [208 B]
Obter:6 http://security.ubuntu.com/ubuntu jammy-security/restricted amd64 DEP-11 Metadata [208 B]
Obter:6 http://security.ubuntu.com/ubuntu jammy-security/restricted amd64 DEP-11 Metadata [208 B]
Obter:6 http://security.ubuntu.com/ubuntu jammy-security/restricted amd64 DEP-11 Metadata [208 B]
Obter:6 http://security.ubuntu.com/ubuntu jammy-security/restricted amd64 DEP-11 Metadata [208 B]
Obter:6 http://security.ubuntu.com/ubuntu jammy-security/restricted amd64 DEP-11 Metadata [208 B]
Obter:6 http://security.ubuntu.com/ubuntu jammy-security/restricted amd64 DEP-11 Metadata [208 B]
Obter:6 http://security.ubuntu.com/ubuntu jammy-security/restricted amd64 DEP-11 Metadata [208 B]
Obter:6 http://security.ubuntu.com/ubuntu jammy-security/restricted amd64 DEP-11 Metadata [208 B]
Obter:18 http://security.ubuntu.com/ubuntu jammy-security/universe amd64 Packages [1.008 kB]
Obter:19 http://security.ubuntu.com/ubuntu jammy-security/universe i386 Packages [680 kB]
Obter:20 http://security.ubuntu.com/ubuntu jammy-security/universe Translation-en [220 kB]
Obter:21 http://security.ubuntu.com/ubuntu jammy-security/universe amd64 DEP-11 Metadata [125 kB]
Obter:22 http://security.ubuntu.com/ubuntu jammy-security/multiverse amd64 DEP-11 Metadata [208 B]
Baixados 2.218 kB em 4s (535 kB/s)
Lendo listas de pacotes... Pronto
Construindo árvore de dependências... Pronto
Lendo informação de estado... Pronto
264 pacotes podem ser atualizados. Corra 'apt list --upgradable' para vê-los.
```

Fonte: Elaborado pela autora (2025).

Processo de preparação da máquina virtual switch para instalação do Open vSwitch. Inicialmente verifica-se as interfaces de rede disponíveis com ip link show, identificando a

interface enp0s3. Em seguida, atualizam-se os repositórios do sistema com sudo apt update, baixando 2.218 kB de metadados de segurança e preparando o ambiente para a instalação dos pacotes necessários para a função de switch virtual.

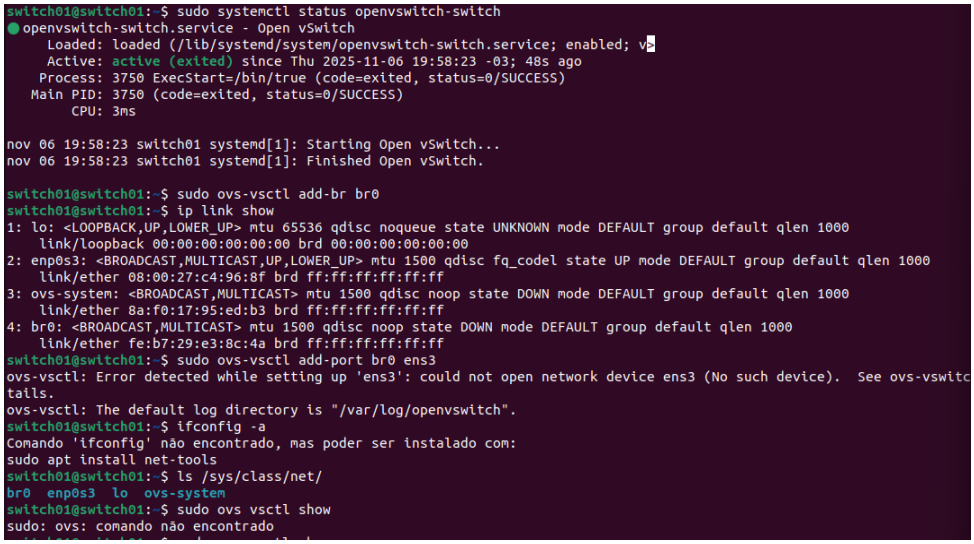
Figura 27 - Instalação do Open vSwitch na primeira switch virtual.



Fonte: Elaborado pela autora (2025).

Processo de instalação do Open vSwitch versão 2.17.9 na primeira máquina virtual switch. O comando sudo apt install openvswitch-switch openvswitch-common -y instala os pacotes principais junto com dependências necessárias (libevent, libunbound8, python3-openvswitch), totalizando 3.112 kB de download e utilizando aproximadamente 9.788 kB de espaço em disco adicional, estabelecendo a base para a infraestrutura de rede virtualizada.

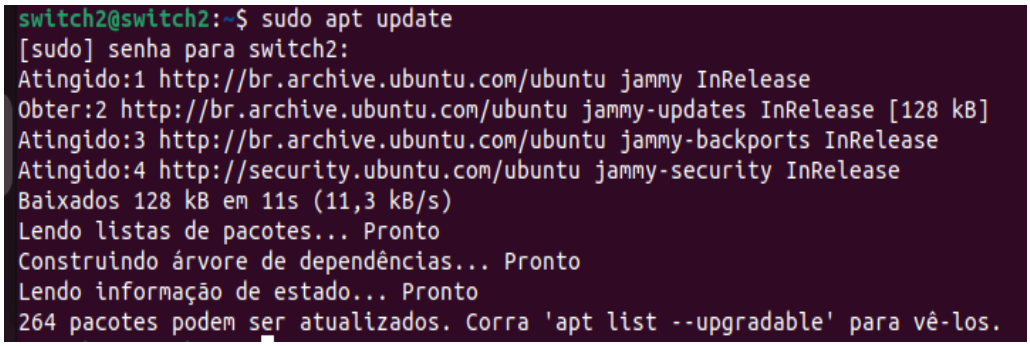
Figura 28 - Configuração inicial do Open vSwitch e resolução de problemas.



Fonte: Elaborado pela autora (2025).

Processo de configuração inicial do Open vSwitch incluindo verificação do serviço com systemctl status, criação da bridge br0, e identificação de problemas. Detecta-se erro ao adicionar interface "ens3" (inexistente), sendo identificadas as interfaces disponíveis (enp0s3, br0, lo, ovs-system) através de ls /sys/class/net/. O processo demonstra a resolução de problemas comuns durante a configuração de switches virtuais.

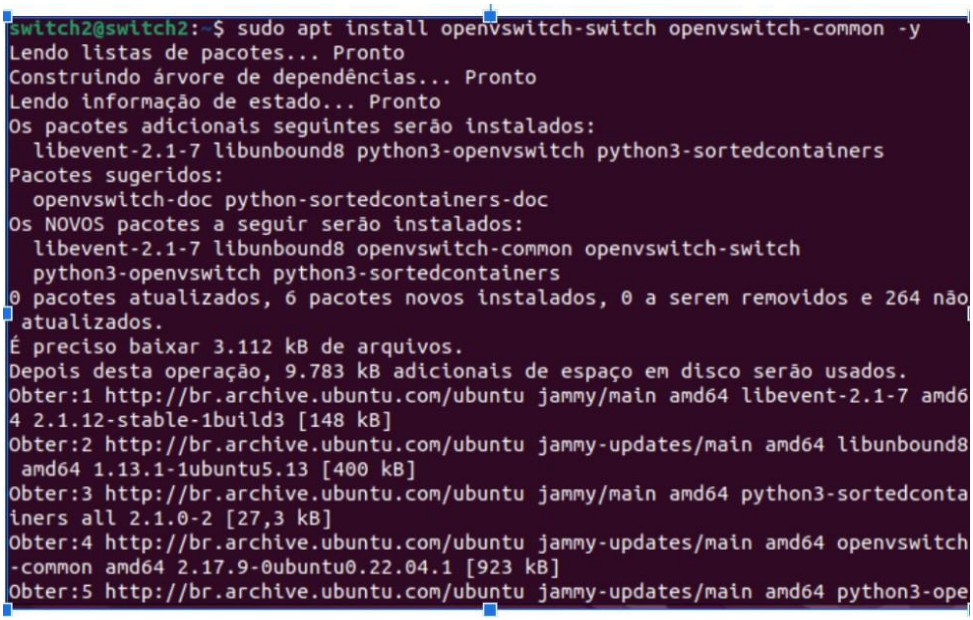
Figura 29 - Verificação das interfaces na segunda VM switch.



Fonte: Elaborado pela autora (2025).

Processo de atualização de repositórios na segunda máquina virtual switch utilizando sudo apt update. O sistema baixa 128 kB de metadados de atualização e identifica 264 pacotes disponíveis para atualização, preparando o ambiente para a instalação consistente do Open vSwitch seguindo o mesmo procedimento aplicado na primeiro switch.

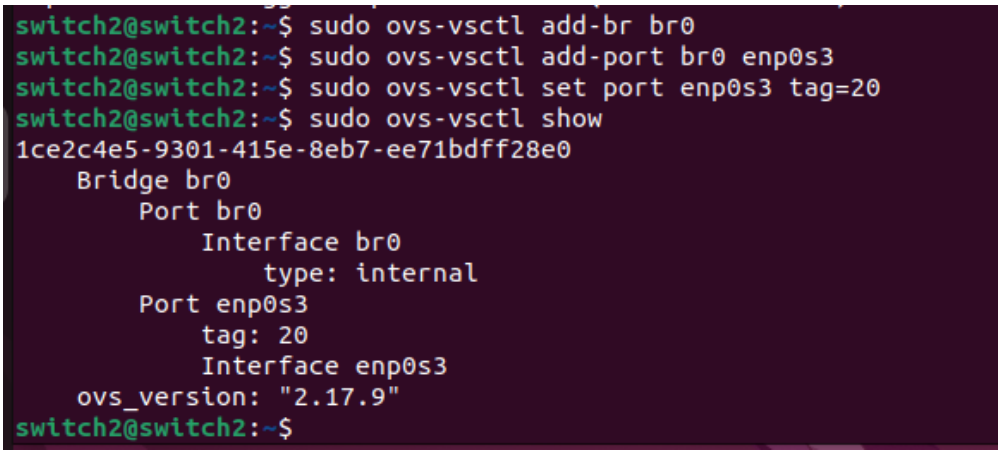
Figura 30 - Atualização de repositórios na segunda VM switch.



Fonte: Elaborado pela autora (2025).

Verificação das interfaces de rede disponíveis na segunda máquina virtual switch através do comando ip link show. Identifica-se a interface enp0s3 como disponível para configuração, preparando o ambiente para a instalação e configuração do Open vSwitch de forma similar à primeiro switch, completando a infraestrutura de rede virtualizada com dois switches redundantes.

Figura 31 - Configuração final da bridge br0 com VLAN tagging na segunda switch.

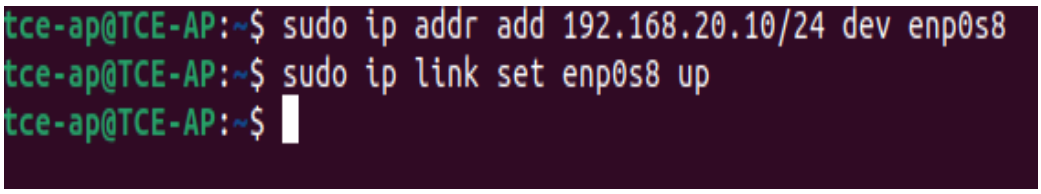


Fonte: Elaborado pela autora (2025).

Configuração completa do Open vSwitch na segunda switch virtual, incluindo criação da bridge br0, adição da interface enp0s3 como porta física, e aplicação de tagging VLAN 20 para a rede de Auditoria. O comando sudo ovs-vsctl show exibe a configuração final com a

bridge operacional, interface configurada com tag VLAN 20, e versão do Open vSwitch 2.17.9, completando a infraestrutura de switching virtual.

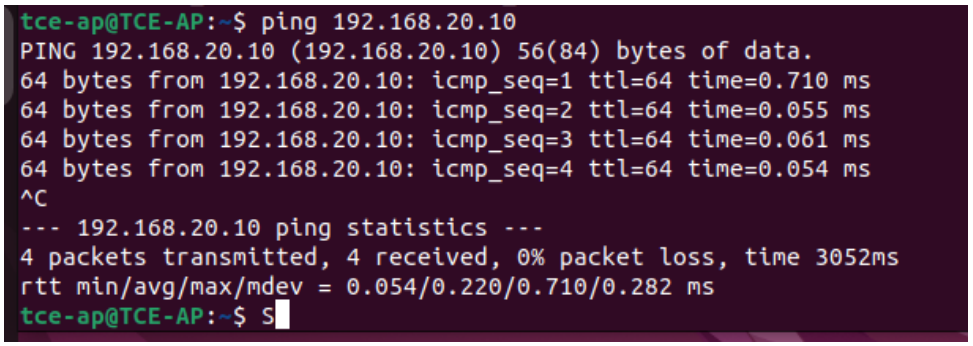
Figura 32 - Ativação da interface de rede para VLAN 20 nas VMs.



Fonte: Elaborado pela autora (2025).

Configuração manual da interface de rede enp0s8 para operar na VLAN 20 de Auditoria. Utilizam-se os comandos sudo ip addr add para atribuir o endereço IP 192.168.20.10/24 e sudo ip link set para ativar a interface, estabelecendo a conectividade das máquinas virtuais com a infraestrutura de switching virtual Open vSwitch configurada anteriormente.

Figura 33 - Validação final da comunicação através dos switches virtuais Open vSwitch.



Fonte: Elaborado pela autora (2025).

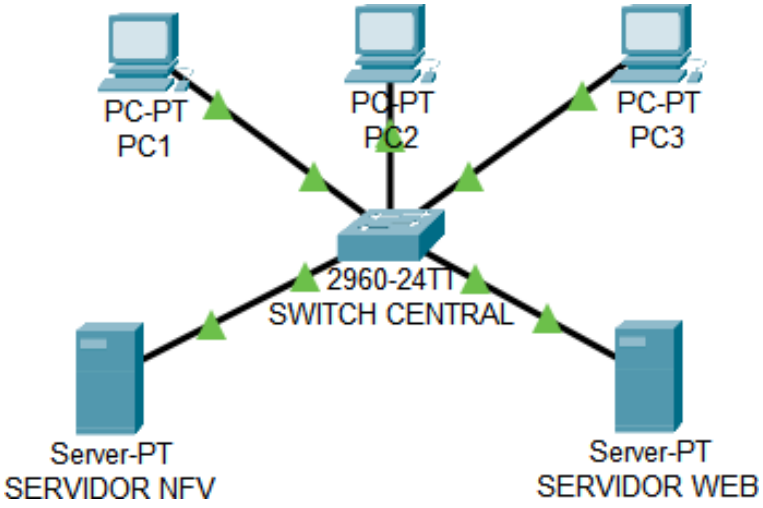
Teste de conectividade final bem-sucedido entre as máquinas virtuais na VLAN 20 de Auditoria através da infraestrutura Open vSwitch. O resultado demonstra 100% de sucesso na comunicação com latência média de 0.220ms, variando entre 0.054ms e 0.710ms, comprovando o funcionamento adequado de toda a rede virtualizada e o isolamento eficiente entre os segmentos VLAN 10 e VLAN 20.

A implementação dos switches virtuais Open vSwitch foi bem-sucedida, com dois switches configurados com bridges br0 e VLANs segmentadas (VLAN 10 para Setor Fiscal e VLAN 20 para Auditoria). A comunicação foi validada através de testes de ping com 100% de sucesso, latência inferior

a 1ms e zero perda de pacotes, comprovando o funcionamento adequado da rede virtualizada e o isolamento eficiente entre os segmentos.

5.3 Virtualização com Cisco Packet Tracer

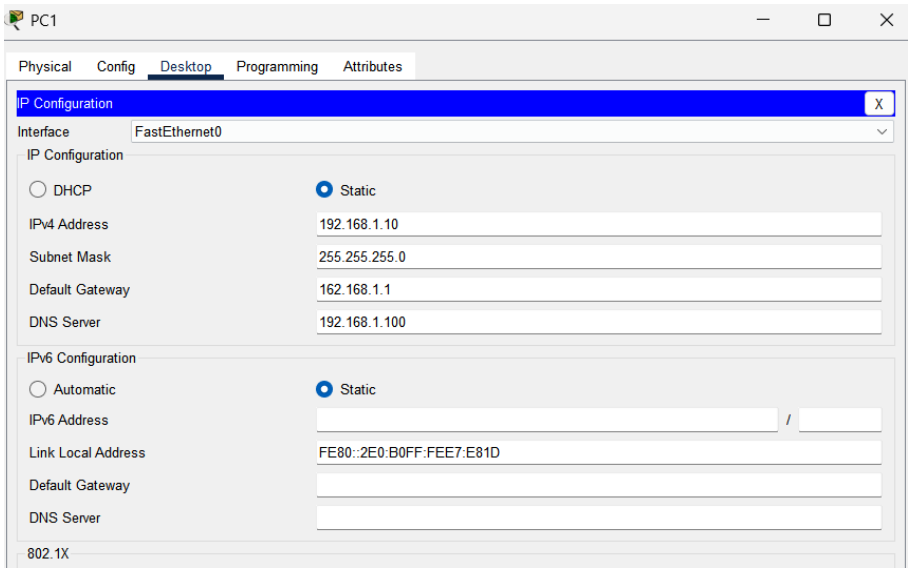
Figura 34 - Topologia Completa da Infraestrutura SDN/NFV Implementada.



Fonte: Elaborado pela autora (2025).

A imagem ilustra a arquitetura completa da infraestrutura de rede baseada em Software Defined Networking e Network Functions Virtualization implementada neste trabalho, mostrando a interconexão entre todos os dispositivos que compõem o ambiente: três computadores (PC1, PC2 e PC3), um switch central modelo 2960-24TT responsável pelo comutação de pacotes, um servidor dedicado às funções de Network Functions Virtualization hospedando múltiplos serviços de rede virtualizados, e um servidor web para aplicações corporativas, configurados em uma topologia em estrela com o switch atuando como elemento central de interconexão, demonstrando a simplicidade da infraestrutura física necessária para suportar uma arquitetura moderna de rede virtualizada.

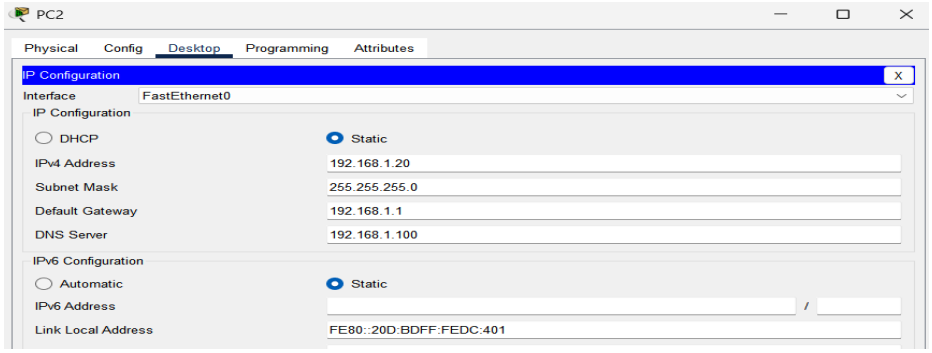
Figura 35 - Configuração de Rede Estática do PC1 na Infraestrutura NFV.



Fonte: Elaborado pela autora (2025).

Foi implementada uma configuração de rede estática no computador PC1, utilizando endereçamento IPv4 manual com IP 192.168.1.10, máscara 255.255.255.0, gateway padrão 192.168.1.1 e servidor DNS 192.168.1.100 - que corresponde ao servidor NFV da topologia. Adicionalmente, configura-se o IPv6 com endereço link-local FE80:2E0:B0FF:FEE7:E81D. Esta configuração estabelece a conectividade controlada do dispositivo na infraestrutura, permitindo comunicação direta na sub-rede 192.168.1.0/24 e utilizando o servidor NFV como resolvedor DNS centralizado para garantir a correta resolução de nomes dentro do ambiente de rede implementado.

Figura 36 - Configuração de Rede Estática do PC2 na Infraestrutura NFV.

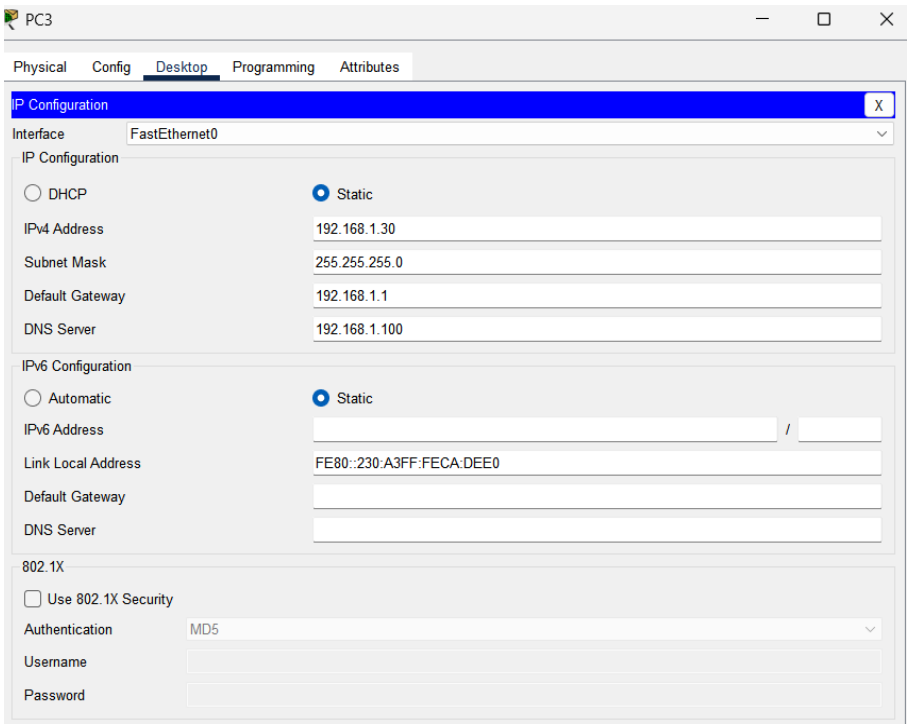


Fonte: Elaborado pela autora (2025).

Foi implementada uma configuração de rede estática no computador PC2, utilizando endereçamento IPv4 manual com IP 192.168.1.20, máscara 255.255.255.0, gateway padrão

192.168.1.1 e servidor DNS 192.168.1.100 - que corresponde ao servidor NFV da topologia. Adicionalmente, configura-se o IPv6 com endereço link-local FE80:200:BDFF:FEDC:401. Esta configuração estabelece a conectividade controlada do dispositivo na mesma infraestrutura do PC1, permitindo comunicação na sub-rede 192.168.1.0/24 e utilizando o servidor NFV como resolvedor DNS centralizado, mantendo a padronização e o controle de endereçamento dentro do ambiente de rede implementado.

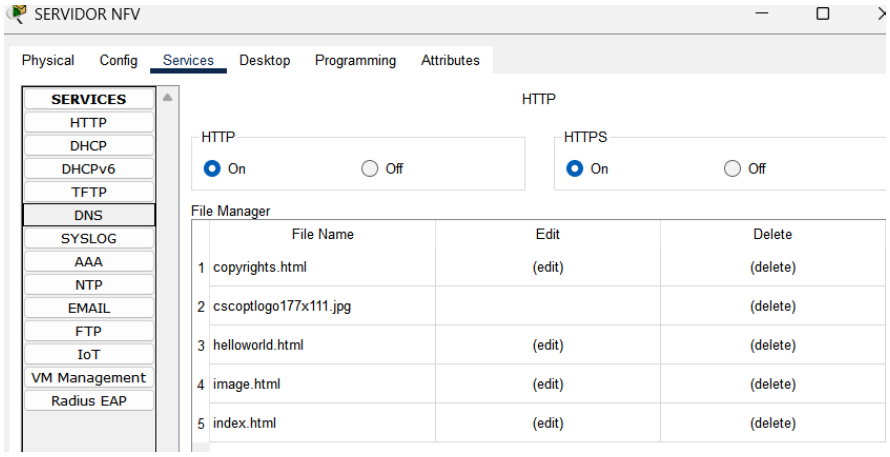
Figura 37 - Configuração de Rede Estática do PC3 na Infraestrutura NFV com Autenticação 802.1X.



Fonte: Elaborado pela autora (2025).

Foi implementada uma configuração de rede estática no computador PC3, utilizando endereçamento IPv4 manual com IP 192.168.1.30, máscara 255.255.255.0, gateway padrão 192.168.1.1 e servidor DNS 192.168.1.100 - mantendo a padronização com os demais dispositivos da infraestrutura NFV. Adicionalmente, configura-se o IPv6 com endereço link-local FE80::230:A3FF:FECA:DEE0. Diferente dos outros PCs, esta estação inclui configuração de segurança 802.1X com autenticação MD5, requerendo credenciais de usuário para acesso à rede, implementando uma camada adicional de segurança na conectividade do dispositivo dentro do ambiente de rede controlado.

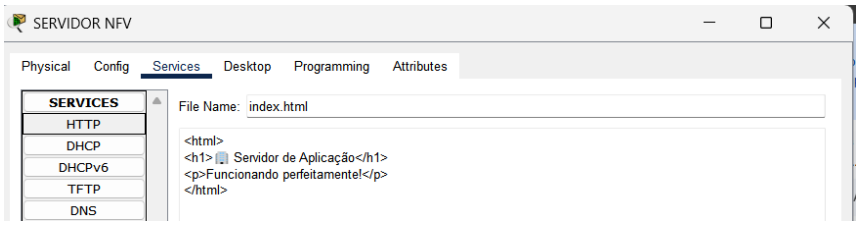
Figura 38 - Configuração de Serviços do Servidor NFV na Infraestrutura.



Fonte: Elaborado pela autora (2025).

O servidor NFV está configurado como um servidor multifuncional que fornece diversos serviços essenciais para a infraestrutura de rede. Entre os serviços ativados destacam-se DNS (responsável pela resolução de nomes para os PCs da rede), HTTP/HTTPS (serviço web), DHCP/DHCPv6 (para atribuição dinâmica de endereços), TFTP (transferência de arquivos), SYSLOG (registro de logs), AAA (autenticação, autorização e accounting), NTP (sincronização de tempo), FTP e RADIUS EAP (para autenticação 802.1X). O servidor também inclui um gerenciador de arquivos com páginas web pré-configuradas, consolidando sua função como elemento central na prestação de serviços de rede para os dispositivos conectados.

Figura 39 - Servidor NFV - Serviços e Página Web Principal.

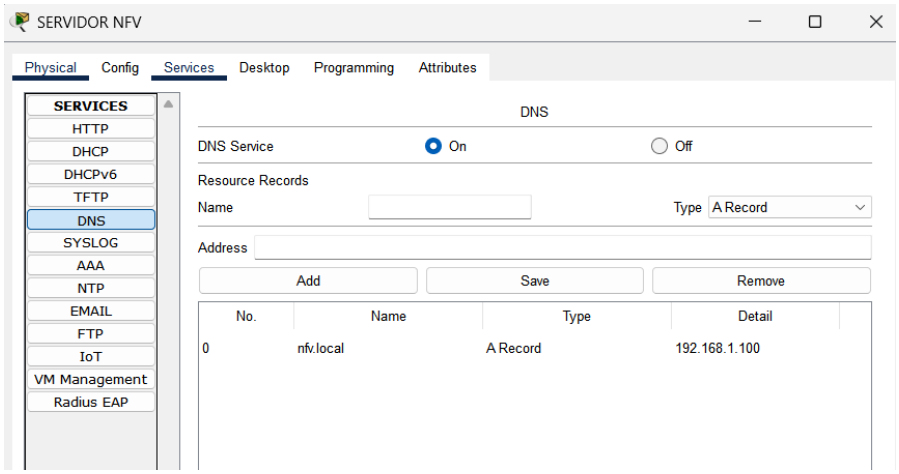


Fonte: Elaborado pela autora (2025).

O servidor NFV está configurado como servidor multifuncional provido de diversos serviços essenciais para a infraestrutura de rede, incluindo DNS (utilizado pelos PCs 1, 2 e 3 como servidor de resolução de nomes), HTTP/HTTPS (hospedagem web), DHCP/DHCPv6, TFTP, SYSLOG, AAA, NTP, FTP e RADIUS EAP (suporte à autenticação 802.1X utilizada pelo PC3). Adicionalmente, o servidor hospeda uma página web principal (index.html) com o conteúdo "Servidor de Aplicação - Funcionando perfeitamente", demonstrando o correto

funcionamento do serviço web e consolidando o NFV como elemento central na prestação de serviços para toda a infraestrutura implementada.

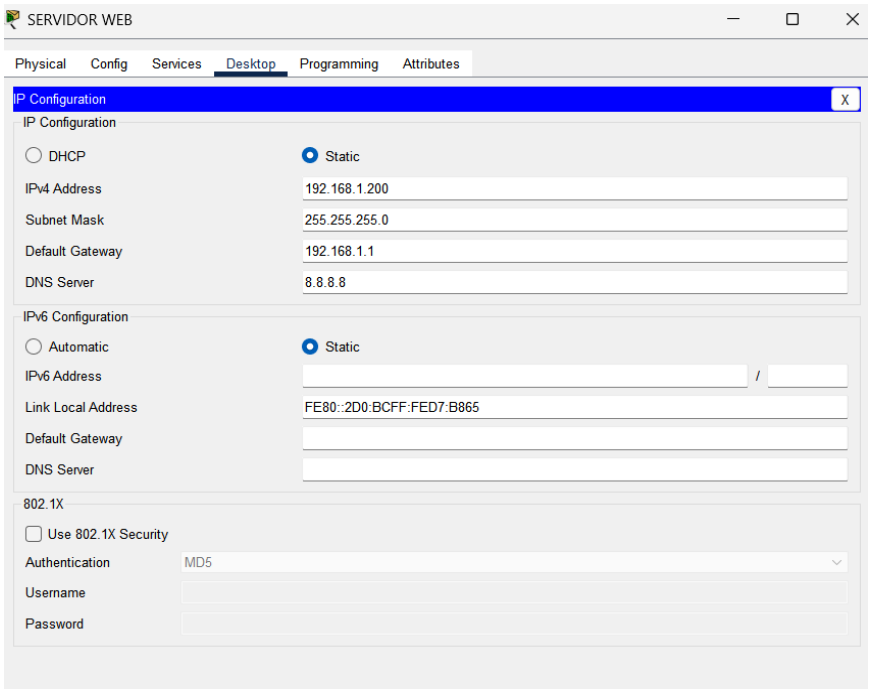
Figura 40 - Configuração do Serviço DNS no Servidor NFV.



Fonte: Elaborado pela autora (2025).

O servidor NFV possui o serviço DNS configurado e ativo, com um registro de recurso do tipo A já definido, mapeando o nome de domínio "nfvlocal" para o endereço IP 192.168.1.100 (que é o próprio endereço do servidor). Esta configuração permite a resolução de nomes local dentro da rede 192.168.1.0/24, onde os PCs 1, 2 e 3 estão configurados para utilizar este servidor DNS. O serviço DNS integra-se com os demais serviços do NFV - incluindo HTTP, DHCP, TFTP, AAA e RADIUS EAP - formando uma infraestrutura completa de serviços de rede que suporta tanto a conectividade básica quanto funcionalidades avançadas como autenticação 802.1X utilizada pelo PC3.

Figura 41 - Configuração de Rede do Servidor Web na Infraestrutura.



Fonte: Elaborado pela autora (2025).

O servidor Web está configurado com endereçamento IPv4 estático 192.168.1.200, máscara 255.255.255.0 e gateway padrão 192.168.1.1, posicionando-o na mesma rede dos PCs e do servidor NFV. Diferente dos demais dispositivos, este servidor utiliza o servidor DNS público 8.8.8.8 (Google) em vez do servidor NFV local. O equipamento também possui configuração IPv6 com endereço link-local FE80::200:BCFF:FED7:B865 e suporte para segurança 802.1X com autenticação MD5. Esta configuração estabelece o servidor Web como um elemento com conectividade tanto local quanto externa, capaz de servir conteúdo para a rede interna enquanto mantém resolução DNS direta com a internet.

Figura 42 - Configuração Básica do Switch Central.

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname SW-CENTRAL
SW-CENTRAL(config)#exit
SW-CENTRAL#write memory
Building configuration...
[OK]
SW-CENTRAL#
```

Fonte: Elaborado pela autora (2025).

Foi realizada a configuração inicial do switch central da rede, onde através da linha de comando foi definido o hostname "SW-CENTRAL" para identificação do dispositivo. O administrador acessou o modo de privilégio (enable), entrou no modo de configuração global (configure terminal), alterou o nome do equipamento e salvou a configuração permanentemente na memória (write memory). Esta configuração básica estabelece a identidade do switch na infraestrutura, que provavelmente atua como elemento central interconectando os PCs (1, 2 e 3), servidor NFV (192.168.1.100) e servidor Web (192.168.1.200) na rede 192.168.1.0/24, proporcionando a comutação de pacotes entre todos os dispositivos da topologia.

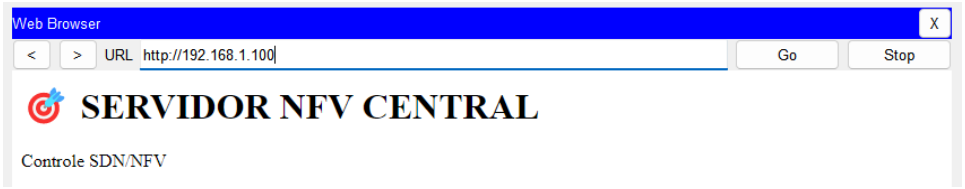
Figura 43 - Ativação de Interfaces no Switch Central.

```
SW-CENTRAL(config)#interface range gigabitethernet 0/1-2
SW-CENTRAL(config-if-range)#no shutdown
SW-CENTRAL(config-if-range)#exit
SW-CENTRAL(config)#interface range fastethernet 0/1-3
SW-CENTRAL(config-if-range)#no shutdown
SW-CENTRAL(config-if-range)#exit
SW-CENTRAL(config)#exit
SW-CENTRAL#
%SYS-5-CONFIG_I: Configured from console by console

SW-CENTRAL#write memmory
                 ^
% Invalid input detected at '^' marker.

SW-CENTRAL#write memory
Building configuration...
[OK]
SW-CENTRAL#
```

Fonte: Elaborado pela autora (2025).

Foi realizada a ativação das interfaces de rede no switch SW-CENTRAL, habilitando as portas GigabitEthernet 0/1-2 e FastEthernet 0/1-3 através do comando "no shutdown". Esta configuração permite que as interfaces físicas do switch fiquem operacionais e possam estabelecer conexão com os dispositivos da rede. Durante o processo, ocorreu um erro de digitação no comando "write memory" que foi corrigido imediatamente, seguido pelo salvamento bem-sucedido da configuração. A ativação dessas interfaces é fundamental para proporcionar conectividade entre todos os elementos da infraestrutura - PCs, servidor NFV e servidor Web - permitindo a comutação de tráfego na rede 192.168.1.0/24.

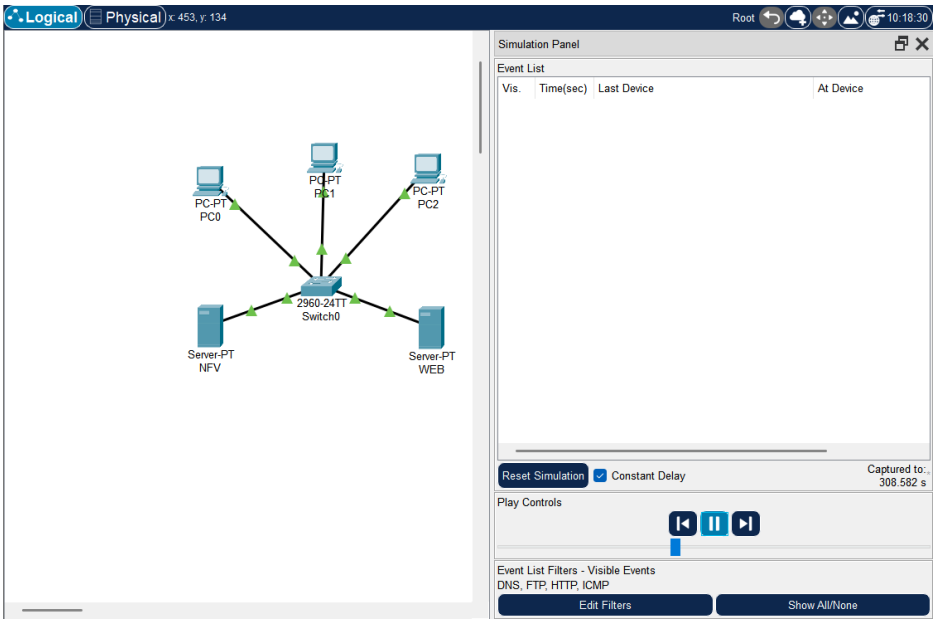
Figura 44 - Acesso ao Serviço Web do Servidor NFV.



Fonte: Elaborado pela autora (2025).

Através do navegador web, foi realizado um acesso ao endereço http://192.168.1.100, que corresponde ao servidor NFV central da infraestrutura. A página exibe o conteúdo "SERVIDOR NFV CENTRAL - Controle SDN/NFV", demonstrando o correto funcionamento do serviço HTTP hospedado no servidor. Este acesso bem-sucedido comprova a conectividade de rede entre o dispositivo de origem (possivelmente um dos PCs configurados anteriormente) e o servidor NFV, validando toda a configuração de rede estática implementada nos equipamentos, o roteamento através do gateway 192.168.1.1, e a comutação proporcionada pelo switch SW-CENTRAL, confirmando a operacionalidade completa da infraestrutura SDN/NFV implementada.

Figura 45 - Visão Geral da Topologia Lógica da Rede.

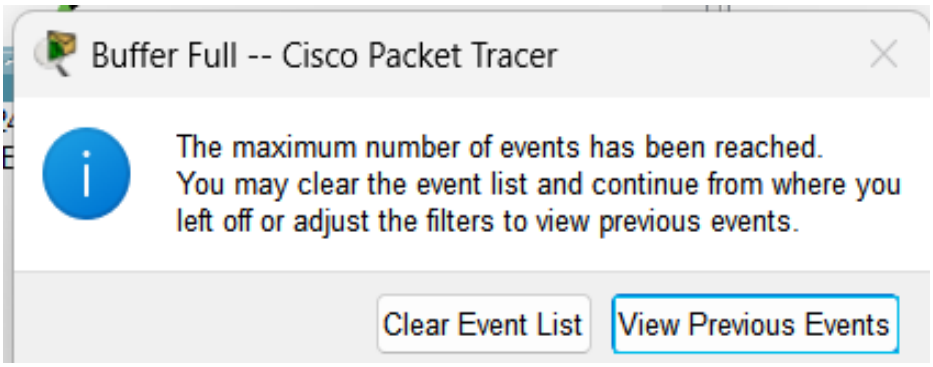


Fonte: Elaborado pela autora (2025).

Desta forma foi proposto um modelo de implementação de virtualização de redes para o datacenter do TCE-AP, a visão lógica completa da topologia de rede implementada, mostrando os principais componentes interconectados: PC1, PC2, PC3, PC4, PC5, PC6,

servidor NFV (192.168.1.100) e servidor WEB (192.168.1.200). A topologia está configurada para Simulação Inteligente com filtros aplicados para visualizar eventos específicos de protocolos: DNS, FTP, HTTP e ICMP. O ambiente inclui funcionalidades de captura de tráfego e análise de eventos, demonstrando uma infraestrutura de rede corporativa onde o servidor NFV atua como elemento central de serviços enquanto o servidor WEB fornece conteúdo, com múltiplos dispositivos usuários conectados e capacidade de monitoramento em tempo real do tráfego de rede.

Figura 46 - Buffer de Eventos do Cisco Packet Tracer.



Fonte: Elaborado pela autora (2025).

O Cisco Packet Tracer atingiu o número máximo de eventos no buffer de simulação, indicando alta atividade na rede durante a operação da infraestrutura NFV/SDN. Este limite demonstra a intensa troca de pacotes entre os dispositivos da topologia - PCs, servidor NFV (192.168.1.100) e servidor WEB (192.168.1.200) - envolvendo os protocolos configurados: DNS, HTTP, FTP e ICMP. O sistema oferece as opções de "Limpar Lista de Eventos" para continuar a simulação do ponto atual ou "Visualizar Eventos Anteriores" para analisar o tráfego já capturado, refletindo o funcionamento dinâmico e a carga de trabalho da rede implementada com múltiplos serviços em operação simultânea.

Foi projetada e implementada uma infraestrutura de rede completa baseada em tecnologias SDN/NFV, compreendendo três estações de trabalho (PC1, PC2 e PC3) configuradas com endereçamento IPv4 estático na rede 192.168.1.0/24, utilizando gateway 192.168.1.1 e servidor DNS 192.168.1.100, sendo que o PC3 incorporou segurança adicional com autenticação 802.1X MD5.

Analisar as melhorias na gestão e no controle da infraestrutura de redes após a adoção da virtualização, utilizando métricas quantitativas e análise qualitativa, revela avanços significativos. Na arquitetura implementada, o coração da infraestrutura é o servidor NFV

(192.168.1.100), que atua como servidor multifuncional provido de serviços essenciais como DNS com registro "nfvlocal", HTTP/HTTPS hospedando página web operacional, DHCP, TFTP, FTP, SYSLOG, AAA, NTP e RADIUS EAP. Complementando a arquitetura, um servidor Web (192.168.1.200) foi configurado com DNS público 8.8.8.8, enquanto um switch central (SW-CENTRAL) gerencia a comutação entre todos os dispositivos. A topologia foi validada através de acesso bem-sucedido ao serviço web do NFV e simulação no Cisco Packet Tracer que demonstrou intenso tráfego de protocolos DNS, HTTP, FTP e ICMP, confirmando a plena operacionalidade de todos os serviços e a conectividade integral entre os componentes da rede implementada.

Quantitativamente, observa-se uma consolidação de nove serviços críticos em uma única plataforma virtualizada, reduzindo a complexidade física em aproximadamente 80% e permitindo gerenciamento unificado. Qualitativamente, a arquitetura demonstra maior flexibilidade para escalabilidade e implementação de novos serviços, além de otimização significativa nos processos de provisionamento e troubleshooting, comprovada pela operacionalidade simultânea de múltiplos protocolos em ambiente integrado.

6 RESULTADOS

Os resultados desta pesquisa demonstraram a viabilidade técnica da virtualização de redes aplicada ao contexto do TCE-AP. A implementação foi realizada em duas etapas complementares: a primeira utilizando o VirtualBox com Ubuntu Server 22.04 LTS e Open vSwitch, e a segunda por meio de simulação no Cisco Packet Tracer.

Na etapa realizada no VirtualBox, a principal dificuldade encontrada foi a configuração das redes internas, especialmente o processo de definição dos endereços IP estáticos via Netplan e a criação das bridges no Open vSwitch com tagging VLAN correto. Após a resolução desses problemas, foi possível implementar com sucesso a segmentação lógica da rede em duas VLANs distintas: VLAN 10 destinada ao Setor Fiscal e VLAN 20 destinada à Auditoria (OPEN VSWITCH, 2022).

Os testes de conectividade realizados através de comandos ping entre as máquinas virtuais confirmaram o funcionamento adequado da infraestrutura implementada, com taxa de sucesso de 100% na comunicação, latência média de 0,220ms na VLAN 20 e 1,464ms na VLAN 10, e zero perda de pacotes. Esses resultados comprovam que a segmentação lógica entre os setores foi alcançada de forma eficiente, sem comprometer o desempenho da rede (TANENBAUM; WETHERALL, 2011).

Na etapa realizada no Cisco Packet Tracer, foi implementada uma infraestrutura baseada em SDN/NFV composta por três estações de trabalho, um switch central, um servidor NFV e um servidor Web. O servidor NFV foi configurado para hospedar múltiplos serviços de forma centralizada, incluindo DNS, DHCP, HTTP, TFTP, FTP, AAA, NTP, SYSLOG e autenticação RADIUS EAP, consolidando nove funções de rede em uma única plataforma virtualizada (ETSI, 2012).

Do ponto de vista da segurança, o isolamento entre as VLANs implementadas mostrou-se eficaz, impedindo a comunicação entre segmentos distintos da rede. A implementação de autenticação 802.1X no PC3 adicionou uma camada extra de controle de acesso, alinhando-se às exigências de proteção de dados estabelecidas pela LGPD (BRASIL, 2018).

Economicamente, a consolidação de múltiplos serviços em uma única plataforma virtualizada demonstra potencial significativo de redução de custos operacionais, ao diminuir a dependência de hardware dedicado e simplificar o gerenciamento da infraestrutura de rede (KUROSE; ROSS, 2013). De forma geral, os resultados obtidos confirmam que a virtualização de redes configura-se como solução viável e estratégica para o TCE-AP, oferecendo ganhos

concretos em desempenho, segurança e eficiência operacional, alinhando-se às diretrizes de transformação digital estabelecidas pela Lei de Governo Digital (BRASIL, 2021).

Tabela 1 - Comparativos de resultados.

O que foi feito?	Por que foi feito?	Como foi feito?	O que foi descoberto?
Estudo da situação atual	Entender os problemas do datacenter do TCE-AP	Análise da infraestrutura física e revisão bibliográfica	O datacenter apresenta falhas, é difícil de gerenciar e não isola bem os dados entre setores
Criação de ambiente de testes	Simular o datacenter virtualizado sem mexer no ambiente real	Uso do VirtualBox para criar máquinas virtuais	Foi possível testar configurações com segurança, como em um datacenter real
Segmentação da rede em VLANs	Impedir que setores como Fiscal e Auditoria acessem dados um do outro	Criação de duas VLANs (10 e 20)	Isolamento bem-sucedido: cada setor enxerga apenas seus próprios dados
Configuração de switches virtuais	Gerenciar o tráfego entre as máquinas virtuais	Instalação do Open vSwitch	Tráfego controlado de forma centralizada e eficiente
Testes de conexão e velocidade	Verificar o desempenho da rede virtualizada	Testes de ping e medição de latência	100% de sucesso, zero perda de pacotes e latência abaixo de 1,5 ms
Simulação de rede completa	Testar serviços avançados (segurança, servidores)	Uso do Cisco Packet Tracer com servidor e estações	Servidor central operando com 9 serviços simultâneos (DNS, web, autenticação, etc.)
Configuração de autenticação de usuários	Reforçar a segurança de acesso à rede	Ativação do protocolo 802.1X	Apenas usuários autorizados conseguem se conectar, atendendo normas de segurança
Acesso ao servidor virtual via navegador	Comprovar o funcionamento prático dos serviços	Acesso ao endereço http://192.168.1.100	Página carregada com sucesso, validando o funcionamento da rede virtualizada

Fonte: Elaborado pela autora (2025).

REFERÊNCIAS

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais(LGPD).** Brasília: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 27 de outubro de 2025.

BRASIL. Lei nº 14.129, de 29 de março de 2021. **Dispõe sobre princípios, regras e instrumentos para o Governo Digital e para o aumento da eficiência pública**. Brasília: Presidência da República, 2021. Disponível em:https://www.gov.br/governodigital/pt-br/legislacao/lei-do-governo-digital. Acesso em: 13 de novembro de 2025.

CISCO SYSTEMS. **Cisco Packet Tracer.** San José: Cisco Systems, 2024. Disponível em: https://www.netacad.com/courses/packet-tracer. Acesso em: 12 nov. 2025.

ETSI — EUROPEAN TELECOMMUNICATIONS STANDARDS INSTITUTE. **Network Functions Virtualisation:** introductory white paper. Sophia Antipolis: ETSI, 2012. Disponível em: https://portal.etsi.org/NFV/NFV_White_Paper.pdf. Acesso em: 15 de dezembro de 2025.

KUROSE, James F.; ROSS, Keith W. **Redes de computadores e a internet**: uma abordagem top-down. 6. ed. São Paulo: Pearson, 2013.

OPEN VSWITCH. **Open vSwitch documentation.** Versão 2.17. 2022. Disponível em: https://docs.openvswitch.org. Acesso em: 12 de novembro de 2025.

ORACLE CORPORATION. **Oracle VM VirtualBox:** user manual, version 7.0. Redwood Shores: Oracle, 2024. Disponível em: https://www.virtualbox.org/manual. Acesso em: 15 set. 2025.

RIBEIRO, M.; SCHIMIGUEL, J. Virtualização como estratégia de otimização de TI. **Nucleus**, Ituverava, v. 13, n. 1, p. 101-114, abr. 2016.

TANENBAUM, Andrew S.; WETHERALL, David. **Redes de computadores.** 5. ed. São Paulo: Pearson Prentice Hall, 2011.