UNIVERSIDADE FEDERAL DE UBERLÂNDIA
FACULDADE DE ENGENHARIA ELÉTRICA
ENGENHARIA ELETRÔNICA E DE TELECOMUNICAÇÕES

CAIO BORGES ZUCCOLOTTO

PROJETO DE ROTEIROS PRÁTICOS EM UM LABORATÓRIO DE REDES DE COMUNICAÇÕES PARA ENSINO NA ENGENHARIA

PATOS DE MINAS - MG
2024

UNIVERSIDADE FEDERAL DE UBERLÂNDIA
FACULDADE DE ENGENHARIA ELÉTRICA
ENGENHARIA ELETRÔNICA E DE TELECOMUNICAÇÕES

CAIO BORGES ZUCCOLOTTO

PROJETO DE ROTEIROS PRÁTICOS EM UM LABORATÓRIO DE REDES DE COMUNICAÇÕES PARA ENSINO NA ENGENHARIA

Trabalho apresentado à banca examinadora como para avaliação da disciplina de PFC2 da graduação em Engenharia Eletrônica e de Telecomunicações, da Faculdade de Engenharia Elétrica, da Universidade Federal de Uberlândia, Campus Patos de Minas.

Orientador: Prof. Dr Daniel Costa Ramos

PATOS DE MINAS - MG
2024

CAIO BORGES ZUCCOLOTTO

PROJETO DE ROTEIROS PRÁTICOS EM UM LABORATÓRIO DE REDES DE COMUNICAÇÕES PARA ENSINO NA ENGENHARIA

Trabalho apresentado à banca examinadora como para avaliação da disciplina de PFC2 da graduação em Engenharia Eletrônica e de Telecomunicações, da Faculdade de Engenharia Elétrica, da Universidade Federal de Uberlândia, Campus Patos de Minas.

Patos de Minas, 6 de dezembro de 2024

Banca Examinadora

_____

Prof. Dr. Daniel Costa Ramos – FEELT/UFU (Orientador)

_____

Prof. Dr. Rafael Augusto Silva – FEELT/UFU (Membro 1)

_____

Profª. Drª. Karine Carbonaro – FEELT/UFU (Membro 2)

AGRADECIMENTOS

Expresso minha gratidão a todos que fizeram parte da minha jornada acadêmica e estiveram ao meu lado durante a realização do meu Trabalho de Conclusão de Curso. Agradeço imensamente à minha família por seu constante apoio, encorajamento e amor incondicional, que foram fundamentais para alcançar meus objetivos. Também sou grato aos meus amigos, que compartilharam momentos de estudo intenso e incertezas, oferecendo apoio e sendo minha rede de suporte. Aos meus professores, agradeço sinceramente por suas orientações, conhecimentos transmitidos e dedicação, que contribuíram para meu crescimento pessoal.

Em conjunto, vocês formaram um suporte valioso para mim, tornando possível a conclusão deste importante capítulo em minha vida. Agradeço a todos por acreditarem em mim, me encorajarem e me motivarem a buscar sempre o meu melhor. Sem o apoio de vocês, não estaria celebrando essa conquista hoje. Embora minha jornada acadêmica tenha chegado ao fim, sei que posso contar com o apoio contínuo de cada um de vocês, independentemente do caminho que eu escolha seguir. Nossa conexão vai além da academia, e estou ansioso para compartilhar mais momentos preciosos juntos.

RESUMO

O projeto tem como objetivo a implementação de um conjunto de roteiros práticos para o ensino de redes de computadores e segurança da informação, a ser aplicado em um laboratório de redes de ensino superior. A proposta abrange etapas como a preparação de dispositivos, instalação de sistemas operacionais, monitoramento de tráfego, crimpagem de cabos, configuração de VLANs e controle de tráfego, utilizando equipamentos como *switches, hubs, patch panels* e raspberry pi. A execução dessas atividades visa proporcionar um aprendizado prático e eficaz, capacitando profissionais a gerenciar, otimizar e proteger redes em ambientes corporativos e experimentais. O objetivo foi concluído proporcionando um ambiente de aprendizado capaz de desenvolver habilidades técnicas, assim como habilidades de resolução de problemas e práticas de segurança, preparando os alunos para enfrentar desafios reais em infraestruturas de TI.

Palavras-chave: Redes de computadores. Segurança da informação. Aprendizado prático.

ABSTRACT

The project aims to implement a set of practical guides for teaching computer networks and information security, to be applied in a higher education network laboratory. The proposal encompasses stages such as device preparation, operating system installation, traffic monitoring, cable crimping, VLAN configuration, and traffic control, using equipment such as switches, hubs, patch panels and Raspberry Pi devices. The execution of these activities seeks to provide practical and effective learning, enabling professionals to manage, optimize, and secure networks in corporate and experimental environments. The goal was achieved by providing a learning environment capable of developing technical skills, as well as problem-solving abilities and security practices, preparing students to tackle real-world challenges in IT infrastructures.

Keywords: Computer networks. Information security. Practical learning.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

A**CL** - *Access Control List* (Lista de Controle de Acesso)

ACL IPv4 - *Access Control List* IPv4 (Lista de Controle de Acesso para IPv4)

ACL Number - *Access Control List Number* (Número da Lista de Controle de Acesso)

CAT6A - Categoria 6A

CAT5 - Categoria 5

CAT5e - Categoria 5e

CAT6 - Categoria 6

CAT7 - Categoria 7

CAT8 - Categoria 8

DARPA – Defense Advanced Research Projects Agency (Agência de Projetos de Pesquisa Avançada de Defesa)

DHCP - *Dynamic Host Configuration Protocol* (Protocolo de Configuração Dinâmica de Hosts)

DNS - *Domain Name System* (Sistema de Nomes de Domínio)

DLP - *Data Loss Prevention* (Prevenção contra Perda de Dados)

DPI - *Deep Packet Inspection* (Inspeção Profunda de Pacotes)

DSL - *Digital Subscriber Line* (Linha de Assinante Digital)

FTP - *File Transfer Protocol* (Protocolo de Transferência de Arquivos)

IP - *Internet Protocol* (Protocolo de Internet)

IoT - *Internet of Things* (Internet das Coisas)

ISPs - *Internet Service Providers* (Provedores de Serviços de Internet)

LAN - *Local Area Network* (Rede de Área Local)

LLC - *Logical Link Control* (Controle de Enlace Lógico)

MAC - *Media Access Control* (Controle de Acesso ao Meio)

MM - *Multimode* (Multimodo)

NAT - *Network Address Translation* (Tradução de Endereço de Rede)

NFC - *Near Field Communication* (Comunicação de Campo Próximo)

OSPF - *Open Shortest Path First* (Primeiro Caminho Mais Curto Aberto)

OSI - *Open Systems Interconnection* (Interconexão de Sistemas Abertos)

PDU - *Power Distribution Unit* (Unidade de Distribuição de Energia)

QoS - *Quality of Service* (Qualidade de Serviço)

SCADA - *Supervisory Control and Data Acquisition* (Aquisição de Dados e Controle Supervisório)

SM - *Single Mode* (Monomodo)

SNMP - *Simple Network Management Protocol* (Protocolo Simples de Gerenciamento de Rede)

SOHO - *Small Office Home Office* (Pequeno Escritório Escritório em Casa)

SFTP - *Secure File Transfer Protocol* (Protocolo de Transferência de Arquivos Seguro)

STP - *Shielded Twisted Pair* (Par Trançado Blindado)

TCP - *Transmission Control Protocol* (Protocolo de Controle de Transmissão)

TCP/IP - *Transmission Control Protocol/Internet Protocol* (Protocolo de Controle de Transmissão/Protocolo de Internet)

TI - *Information Technology* (Tecnologia da Informação)

UDP - *User Datagram Protocol* (Protocolo de Datagrama de Usuário)

UFU - Universidade Federal de Uberlândia

VLAN - *Virtual Local Area Network* (Rede de Área Local Virtual)

VPN - *Virtual Private Network* (Rede Virtual Privada)

WAN - *Wide Area Network* (Rede de Área Ampla)

Wi-Fi - *Wireless Fidelity* (Fidelidade Sem Fio)

WLAN - *Wireless Local Area Network* (Rede de Área Local Sem Fio)

SUMÁRIO

1 INTRODUÇÃO

A Internet é uma rede global de computadores interconectados que permite a troca de informações e comunicação em todo o mundo. Ela surgiu na década de 1960 como uma iniciativa da Agência de Projetos de Pesquisa Avançada de Defesa (DARPA) dos Estados Unidos para permitir a comunicação entre seus militares em caso de ataques nucleares. Com o tempo, a rede foi se expandindo e se popularizando até se tornar a rede mundial de computadores que conhecemos hoje (James; Ross, 2013).

A Internet é composta por milhões de dispositivos interconectados, incluindo computadores, servidores, dispositivos móveis, roteadores e outros dispositivos que utilizam uma variedade de tecnologias de comunicação, como cabos, fibra ótica, satélite e wireless. Através da Internet, os usuários podem acessar uma enorme quantidade de informações, serviços e aplicativos, além de se comunicar com outras pessoas em qualquer lugar do mundo em tempo real (James; Ross, 2013).

Atualmente, a Internet é uma das redes mais complexas e diversificadas do mundo, conectando bilhões de dispositivos em todo o planeta. Ela é composta por diversos protocolos de comunicação que trabalham juntos para permitir que os dados sejam transmitidos entre diferentes dispositivos de forma confiável e eficiente. No entanto, a diversidade de protocolos de comunicação e a complexidade da Internet também trazem desafios significativos para a segurança, escalabilidade e interoperabilidade. Gerenciar e manter essa rede global requer um grande esforço e cooperação entre diversos setores e organizações, desde empresas até governos e instituições acadêmicas (James; Ross, 2013).

A estrutura básica da Internet consiste em uma rede de redes interconectadas, que são compostas por hosts e ISPs (*Internet Service Providers*). Os hosts são os dispositivos finais que estão conectados à rede, como computadores, laptops, smartphones e tablets. Os ISPs, por outro lado, são as empresas que fornecem acesso à Internet aos usuários, incluindo serviços de banda larga, DSL (*Digital Subscriber Line*) e outros tipos de conexões. Para conectar esses hosts à Internet, é necessária a infraestrutura de rede que consiste em divisões de LAN (*Local Area Networks*) e WAN (*Wide Area Networks*). A LAN refere-se à rede local que conecta os dispositivos dentro de uma área limitada, como uma casa ou um escritório. A WAN, por outro lado, é uma rede que conecta várias LANs em diferentes locais geográficos. Juntos, esses componentes formam a estrutura básica da

Internet, que é capaz de fornecer acesso à informação e comunicação em escala global (Ross, 2013).

O uso de laboratórios de redes de computadores é fundamental para a formação de profissionais capacitados em tecnologia da informação (TI). A atuação profissional em laboratórios de redes exige habilidades técnicas específicas, treinamentos práticos, trabalho em equipe e atualização constante dos conhecimentos. É necessário capacitar os profissionais em conceitos e protocolos de rede, equipamentos e tecnologias, bem como permitir a experimentação, teste e aplicação de conhecimentos em um ambiente realístico.

A validação de conhecimentos com a prática de laboratório é uma etapa essencial para a aquisição e consolidação de conhecimentos em diversas áreas do conhecimento, especialmente em áreas técnicas, como engenharia, ciência da computação e tecnologia da informação.

A prática de laboratório permite que os alunos experimentem e apliquem teorias e conceitos aprendidos em sala de aula em ambientes controlados e realistas. Isso permite que os alunos se familiarizem com a tecnologia e os equipamentos, aprendam a solucionar problemas e erros comuns, bem como desenvolvam habilidades práticas que serão úteis em suas futuras carreiras. Além disso, a prática de laboratório também ajuda a desenvolver a capacidade de trabalho em equipe, bem como a habilidade de comunicação e colaboração, pois os alunos trabalham em grupos para realizar experimentos e projetos. Em resumo, a prática de laboratório é uma parte fundamental do processo de aprendizagem, permitindo que os alunos apliquem e consolidem os conhecimentos adquiridos na teoria, desenvolvam habilidades práticas e se preparem para suas carreiras profissionais.

1.1 TEMA DO PROJETO

Este trabalho tem como intuito mapear os equipamentos e contribuir com o laboratório de redes de comunicação por meio da elaboração de roteiros práticos a serem utilizados neste laboratório com os equipamentos já existentes.

1.2 PROBLEMATIZAÇÃO

O tema de redes de computadores é considerado por muitos como complexo e desafiador, envolvendo diversos conceitos teóricos e técnicos que podem ser difíceis de entender apenas com a teoria. Além disso, as redes de computadores estão em constante evolução, com novas tecnologias e padrões sendo introduzidos regularmente. Por esse

motivo, é importante que os estudantes tenham a oportunidade de aplicar os conceitos aprendidos em um ambiente prático, como um laboratório, para consolidar o conhecimento e desenvolver habilidades práticas. A prática de laboratório permite que os estudantes experimentem diferentes cenários e soluções de problemas em um ambiente controlado, onde podem aplicar e testar seus conhecimentos. Isso ajuda a tornar a aprendizagem mais efetiva e a preparar os estudantes para os desafios do mundo real em suas carreiras profissionais.

A prática de laboratório é uma ferramenta essencial para complementar o aprendizado teórico e ajudar a tornar o tema de redes de computadores mais acessível e compreensível. Essa afirmação foi confirmada no estudo realizado pela Baskent University (2012) (Emiroglu, Sahin, 2012)**,** onde é afirmado que a combinação de aplicações práticas juntamente com áreas teóricas de qualquer domínio disciplinar durante o processo de ensino superior de engenharia pode ajudar a aumentar o nível de qualidade do aprendizado dos estudantes.

A tecnologia de redes evolui rapidamente e é difícil acompanhar todas as mudanças. Novos protocolos, dispositivos e técnicas são desenvolvidos constantemente, tornando-se uma tarefa árdua para os profissionais de TI manterem-se atualizados sobre as mais recentes tendências em redes. As empresas precisam de profissionais que possam lidar com as complexidades de infraestruturas de rede cada vez maiores e mais diversas, capazes de lidar com questões como segurança, gerenciamento de rede e provisionamento de largura de banda.

Para manter-se atualizado, os profissionais precisam dedicar tempo e recursos para aprender as novas tecnologias e praticar suas habilidades em laboratórios de rede. Eles também precisam estar abertos a mudanças e aprender continuamente para garantir que suas habilidades estejam atualizadas e que possam fornecer soluções eficazes para as necessidades da organização.

No curso de engenharia eletrônica e de telecomunicações na UFU (Universidade Federal de Uberlândia) em Patos de Minas, é ofertada a disciplina de redes, que visa o aprendizado sobre o que é a internet, quais suas camadas e seus protocolos, e recentemente foi adicionada uma segunda disciplina sobre redes de computadores, que visa o aprendizado sobre gerenciamento e segurança das redes.

A implantação de roteiros práticos de redes, com roteiros adequados é fundamental para a aprendizagem dos profissionais que lidam com tecnologia. Com a rápida evolução das redes e a crescente demanda por conectividade, é necessário que os

estudantes tenham acesso a equipamentos que possibilitem simular casos reais, enfrentando desafios da tecnologia atual.

1.3 HIPÓTESE

A principal hipótese do trabalho é a possibilidade, frente aos desafios tecnológicos e financeiros, de se montar roteiros práticos de redes de computadores que sejam suficientemente adequados para realizar as demonstrações necessárias nas disciplinas de redes do curso de Engenharia Eletrônica e de Telecomunicações de Patos de Minas e por consequência, melhorar o aprendizado dos discentes do curso.

1.4 OBJETIVOS

1.4.1 Objetivos Gerais

Mapear as condições atuais do laboratório e desenvolver roteiros práticos adequados aos seus equipamentos atuais, para que o laboratório possa exercer o seu papel no ensino na Universidade Federal de Uberlândia em Patos de Minas.

1.4.2 Objetivos Específicos

Para alcançar o objetivo geral, é necessário cumprir os seguintes objetivos específicos:

- Estudar laboratórios de redes de computadores e suas aplicações;
- Verificar os equipamentos do laboratório na UFU Patos de Minas;
- Avaliar quais equipamentos seriam utilizados;
- Construir os roteiros práticos.

1.5 JUSTIFICATIVA

O desenvolvimento e planejamento de roteiros práticos para laboratórios de redes de comunicação emergem como um tópico de grande relevância acadêmica e prática, especialmente na última década. Estudos como o desenvolvimento de um laboratório que exemplifica tecnologias SOHO (Small Office Home Office) mostram a importância de experimentos práticos para o entendimento de tecnologias como SOHO *Router*/*Firewall*, Wi-Fi (*Wireless Fidelity*) LAN, e comunicação via *HomePlug Powerline* e *HomePNA Phoneline*. Esses roteiros práticos permitem que os estudantes experimentem e resolvam problemas em ambientes que simulam situações reais de rede, promovendo melhor compreensão dos princípios de comunicação de dados e redes (Sang, 2013).

O laboratório projetado visa aprimorar a educação dos alunos por meio de aprendizado cooperativo, utilizando equipamentos de rede SOHO de última geração.

Foi criado um conjunto de experimentos práticos em laboratório que permitem aos estudantes construir, experimentar e resolver problemas em infraestruturas de rede reais. Esses experimentos são adequados para cursos introdutórios de comunicação de dados e redes, bem como para educação continuada. Eles ajudam os alunos a adquirir experiência na configuração de redes SOHO e a compreender melhor os conceitos e princípios de rede. Testes realizados antes e depois dos experimentos mostraram um impacto significativo na aprendizagem dos alunos, que relataram alta confiança e interesse em estudos e trabalho adicionais na área de redes (Sang, 2013).

O trabalho desenvolvido por Mary Martin e Ka Ching Chan (2012), aborda o desenvolvimento de uma infraestrutura de rede virtual e física integrada para o Laboratório de Interconexão da Universidade La Trobe e destaca a importância da experiência prática em equipamentos físicos de rede para que os estudantes possam entender profundamente conceitos básicos e avançados de redes, como cabos, protocolos de roteamento e VLANs (Chan; Martin, 2012).

O currículo de TI inclui redes e segurança, tecnologias de plataforma, administração e manutenção de sistemas e sistemas e tecnologias web. A La Trobe University possui um Laboratório de Interconexão que faz parte dos cursos de TI e pode ser ministrado em um ambiente físico ou remoto, utilizando dispositivos físicos de rede ou dispositivos virtualizados. Ressalta-se que o termo "laboratório virtual de redes" não possui uma definição clara e pode se referir tanto a um ambiente virtual para ensino de redes quanto a um laboratório de redes que utiliza dispositivos de rede virtualizados (Chan; Martin, 2012).

Outro exemplo é o trabalho que aborda o Laboratório de Redes de Computadores da Universidade de Mendel em Brno, que tem como objetivo oferecer suporte a cursos especializados em redes de computadores, segurança de rede e sistemas operacionais, bem como fornece um ambiente experimental para teses finais e testes de rede ou segurança (Pokorný; Zach, 2013).

A rede de laboratório é usada para diferentes tipos de experimentos de rede e segurança e é um ambiente especial onde atividades perigosas podem ocorrer, mas que não afetam nenhum sistema ou rede de produção. É comum que os alunos tenham privilégios de administrador na rede, o que torna a segurança e manutenção geral da rede uma tarefa difícil. O artigo apresenta uma solução que define requisitos de usuário e regras de segurança para proteger a infraestrutura do laboratório, bem como a rede da

universidade externa e a Internet. O trabalho também descreve o *design* físico e topológico da rede e apresenta a inovação de virtualização de sistemas nos dispositivos host finais. O design do laboratório de rede pode ser usado como modelo para outros laboratórios educacionais de rede. O artigo é uma continuação de um artigo anterior que descreveu a ideia essencial da transição para computadores de mesa virtualizados e o equipamento adquirido em 2009 (Pokorný; Zach, 2013).

Existem também outras abordagens para projeto de laboratórios de redes, como a utilização de laboratórios virtuais e remotos. Alguns estudos apontam que os laboratórios tradicionais de rede têm limitações financeiras e exigem muitos recursos e pessoal qualificado para gerenciá-los. Desta forma, para superar essas limitações, foram criados laboratórios on-line, como os virtuais e remotos. Os laboratórios virtuais podem ser limitados pela falta de realismo, enquanto os remotos podem ser complicados para iniciantes em redes e exigir a escrita de programas/scripts. Além disso, as ferramentas de interface de usuário usadas em laboratórios na web podem ser exigentes em recursos e não adequadas para dispositivos com limitações de recursos (Cui et al., 2012).

Como exemplo de laboratório on-line, é indicado o WeFiLab, um laboratório on-line para estudantes universitários que se concentra em tecnologias de redes sem fio, permitindo experiência prática em experimentos em dispositivos reais. A plataforma é acessível por meio de uma interface gráfica na web e utiliza uma estrutura de operações de dois níveis para coordenar a comunicação entre clientes e dispositivos sem fio. O agendamento da plataforma é projetado para facilitar o uso eficiente desses dispositivos.

O WeFiLab foi implementado e avaliado em dois estudos de caso que envolveram 315 alunos de graduação em ciência da computação, sendo usado como complemento para o curso de Computação Móvel e Computação Pervasiva na City University de Hong Kong. O WeFiLab ajudou a melhorar a compreensão dos alunos sobre o WiFi e a identificar as áreas de conhecimento mais fracas para serem enfatizadas nas palestras do curso (Cui et al., 2012).

O desenvolvimento de roteiros práticos para laboratórios de redes é essencial para a formação de estudantes de engenharia e telecomunicações, promovendo um aprendizado ativo e relevante. Esses roteiros contribuem não só para a otimização dos recursos institucionais, mas também para a atração de novos estudantes e professores, consolidando a posição da universidade como uma referência no ensino de redes de comunicação.

1.6 CONSIDERAÇÕES FINAIS

Neste capítulo, foram definidos objetivos que visam resolver a problemática de um laboratório de redes de computadores que, embora possuam equipamentos, carece de roteiros práticos que otimizem o uso desses recursos e contribuam para aprimoramento das habilidades dos alunos no campus UFU Patos de Minas. A partir dessas diretrizes, será possível promover uma utilização mais eficaz do laboratório, possibilitando aos estudantes a aplicação prática dos conhecimentos adquiridos e o desenvolvimento de competências essenciais para suas futuras carreiras.

Nos capítulos seguintes, serão apresentados os métodos e materiais detalhados para a execução deste trabalho, visando alcançar os objetivos propostos de maneira eficiente e organizada.

2 REFERENCIAL TEÓRICO

A criação de um laboratório de redes de computadores requer uma compreensão sólida de uma série de conceitos teóricos que formam a base nas disciplinas de redes.

2.1 REDES DE COMPUTADORES

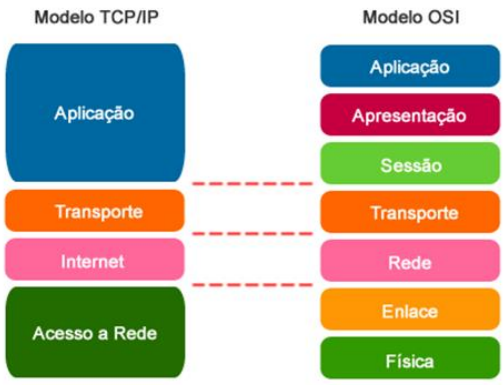
As redes de computadores desempenham um papel essencial na nossa era digital, conectando dispositivos e permitindo a troca de informações em todo o mundo. Elas são os alicerces da comunicação moderna, possibilitando desde o envio de um simples e-mail até o acesso a plataformas globais em tempo real.

Uma rede de computadores é um conjunto interconectado de dispositivos eletrônicos que compartilham recursos e transmite dados entre si. Essas redes podem ser locais, abrangendo uma pequena área, como uma residência ou um escritório, ou podem ser amplas, abrangendo todo o planeta. Elas operam com base em protocolos e padrões estabelecidos, garantindo a segurança, a eficiência e a confiabilidade das comunicações.

2.1.1 Modelo OSI e TCP/IP

O Modelo de Referência OSI (*Open Systems Interconnection*) é uma estrutura abstrata que descreve as camadas de comunicação entre sistemas abertos. Ele descreve como as informações são enviadas de um computador para outro em uma rede. O modelo OSI é composto por sete camadas como na Figura 1, cada uma com uma função específica (Alura, 2023).

Figura 1 - Camadas Modelos TCP/IP e OSI.



Fonte: Brenzink (2019, on-line)

A camada 1 é a física, é responsável por especificar os dispositivos, como *hubs*, e os meios de transmissão, como cabos de rede, que são usados para enviar os dados.

A camada 2 é a de enlace ou ligação, os dados recebidos da camada anterior são verificados para averiguar possíveis erros e corrigi-los. Esta camada é subdividida em duas, camada MAC (*Media Acess Control*) e camada LLC (*Logical Link Control*). A MAC é onde ocorre a interconexão de vários computadores em uma rede. Cada máquina na rede possui um endereço físico exclusivo, conhecido como endereço MAC (Alura, 2023).

O endereço MAC é o identificador físico do remetente do pacote. Isso significa que, à medida que o pacote passa por diferentes dispositivos (como roteadores, *switches* ou servidores), o endereço MAC é alterado durante o processo. Essa camada utiliza esse endereço para identificar e encaminhar os pacotes de dados.

A LLC é onde ocorre o gerenciamento do fluxo de dados na rede. É graças a essa camada que é possível ter vários protocolos da camada superior coexistindo em uma mesma rede.

A camada 3 é a de rede, onde são definidos os endereços IP de origem e destino, além disso, ela pode atribuir prioridades a determinados pacotes e tomar decisões sobre o caminho a ser seguido para enviar os dados, ou seja, essa camada é responsável pelo controle do roteamento entre a origem e o destino do pacote (Alura, 2023).

A camada 4 é a de transporte, que é responsável por garantir o envio e o recebimento dos pacotes provenientes da camada três. Ela gerencia o transporte dos pacotes, assegurando o sucesso na entrega e recebimento dos dados, garantindo que os dados sejam entregues com consistência, ou seja, sem erros ou duplicações (Alura, 2023).

A camada 5 é a sessão, que estabelece e encerra a conexão entre hosts, também possibilita o suporte, como registros de log e realização de tarefas de segurança (Alura, 2023).

A camada 6 é a apresentação, que é responsável pela tradução dos dados para as próximas camadas. E também é onde ocorre a conversão e compactação de dados, e também criptografia dos dados, caso necessário (Alura, 2023).

A camada 7 é a aplicação, que é responsável por consumir os dados. Nessa camada, encontramos os programas que possibilitam a interação entre humanos e máquinas. Por meio dela, é possível enviar e-mails, transferir arquivos, acessar websites e estabelecer conexões remotas com outras máquinas, entre outras funcionalidades (Alura, 2023).

Já o modelo TCP/IP (*Transmission Control Protocol/Internet Protocol*) é um conjunto de protocolos de comunicação de rede que permite a comunicação entre

dispositivos em uma rede. O TCP/IP também é composto por camadas, mas utiliza apenas quatro camadas (Avast, [s.d.]).

A camada de enlace de dados, é responsável pelo gerenciamento das partes físicas envolvidas no envio e recebimento de dados. Isso inclui o uso de cabos Ethernet, redes sem fio, placas de interface de rede e *drivers* de dispositivos nos computadores.

Acima da camada de enlace de dados está a camada de internet, também chamada de camada de rede. Essa camada controla o movimento dos pacotes pela rede, garantindo que eles sejam roteados corretamente de um dispositivo para outro. Ela desempenha um papel fundamental no estabelecimento e na manutenção da comunicação entre diferentes redes.

A camada de transporte, que estabelece uma conexão confiável de dados entre dois dispositivos. Essa camada divide os dados em pacotes, reconhece os pacotes recebidos do outro dispositivo e garante que o outro dispositivo também reconheça os pacotes recebidos. A camada de transporte é responsável pela entrega correta dos pacotes e lida com questões como controle de fluxo e correção de erros.

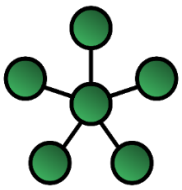
A camada de aplicação, composta por aplicativos que requerem comunicação em rede. Nessa camada, os usuários interagem com os aplicativos, como e-mails e mensagens. Os aplicativos na camada de aplicação não precisam se preocupar com os detalhes técnicos da comunicação, pois as camadas inferiores lidam com esses aspectos. Cada camada desempenha um papel específico e contribui para o funcionamento eficiente e confiável das redes de comunicação.

2.1.2 Topologia de Rede

A topologia de rede é o arranjo físico ou lógico dos dispositivos em uma rede. Há várias topologias de rede, incluindo estrela, barramento, anel e malha. Cada topologia tem suas próprias vantagens e desvantagens em termos de desempenho, escalabilidade e confiabilidade (International IT, 2021).

Topologia estrela, como mostrado na Figura 2 é a configuração mais comum. Nessa configuração, os nós da rede são conectados a um hub central, que atua como um servidor. O hub desempenha o papel de gerenciar a transmissão de dados pela rede (International IT, 2021).

Figura 2 - Topologia estrela.



Fonte: International IT (2021, on-line)

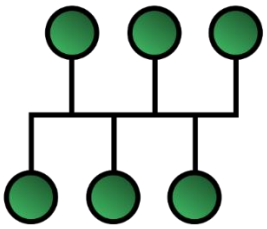
A configuração em estrela apresenta algumas vantagens significativas. Em primeiro lugar, permite um gerenciamento conveniente a partir de um local central. Com o hub central, é possível realizar o controle e gerenciamento da rede de forma prática e centralizada. Além disso, essa configuração garante a continuidade da rede mesmo em caso de falha de um nó. Como os demais nós estão conectados ao hub central, a rede continua funcionando mesmo que um dos nós apresente falhas. Outra vantagem é a facilidade de adição e remoção de dispositivos sem interromper a rede. É possível fazer alterações e expansões na rede sem causar interrupção no seu funcionamento.

A configuração em estrela também oferece uma facilidade na identificação e isolamento de problemas de desempenho. Como todos os dados passam pelo hub central, é mais fácil identificar e isolar problemas que possam afetar o desempenho da rede.

No entanto, essa configuração também possui algumas desvantagens a serem consideradas. Uma delas é a dependência do hub central. Se o hub central apresentar falhas, toda a rede será afetada e deixará de funcionar. Outra desvantagem é a limitação de desempenho e largura de banda imposta pelo hub central. A capacidade do hub central pode restringir o desempenho da rede, especialmente em casos de redes com muitos nós ou que exijam alta velocidade de transmissão. Além disso, é importante considerar que operar uma configuração em estrela pode envolver custos elevados, principalmente em relação ao hub central e sua manutenção.

A topologia em barramento, como mostrado na Figura 3 é caracterizada pela disposição dos dispositivos ao longo de um único cabo que percorre toda a extensão da rede. Os dados fluem ao longo do cabo, seguindo o seu trajeto até o destino pretendido (International IT, 2021).

Figura 3 - Topologia em barramento.

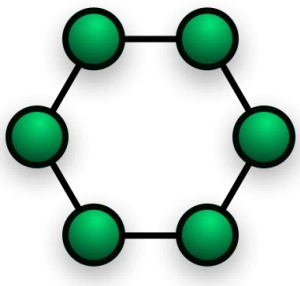


Fonte: International IT (2021, on-line)

Uma das vantagens dessa topologia é sua economia, sendo especialmente adequada para redes menores. Além disso, o layout é simples, com todos os dispositivos conectados através de um único cabo. Isso facilita a instalação e o gerenciamento da rede. Outro benefício é a capacidade de adicionar mais nós à rede ao simplesmente estender o cabo ao longo da linha, permitindo sua expansão conforme necessário. No entanto, também apresenta algumas desvantagens. A rede é vulnerável a falhas de cabo, pois qualquer problema ou interrupção no cabo pode afetar toda a rede, causando indisponibilidade dos serviços. Além disso, cada nó adicionado à linha reduz a velocidade de transmissão da rede, pois os dados precisam ser transmitidos em sequência e em uma única direção de cada vez. Isso pode resultar em um desempenho limitado quando muitos dispositivos estão conectados à rede.

A topologia em anel, como mostrado na Figura 4 é caracterizada pela configuração dos nós em um padrão circular, onde os dados viajam por cada dispositivo à medida que percorrem o anel. Em redes maiores, pode ser necessário utilizar repetidores para evitar perdas de pacotes durante a transmissão. Essas topologias podem ser implementadas como anel único (half-duplex) ou anel duplo (full-duplex), permitindo o fluxo de tráfego em ambas as direções simultaneamente (International IT, 2021).

Figura 4 - Topologia em anel.

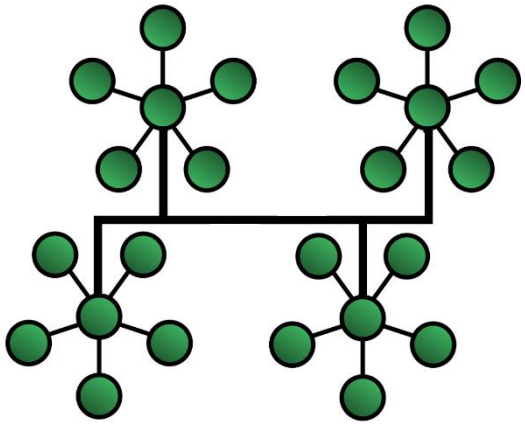


Fonte: International IT (2021, on-line)

Uma das vantagens da topologia em anel é o seu custo-benefício. Ela é uma opção econômica para instalação em redes, oferecendo uma maneira eficiente de conectar os dispositivos. Além disso, a topologia em anel facilita a identificação de problemas de desempenho, uma vez que os dados passam por cada nó, tornando mais fácil identificar possíveis gargalos ou falhas. No entanto, apresenta desvantagens a serem consideradas. Se um nó falhar, ele pode afetar vários nós ao longo do anel, causando interrupções na rede. Todos os dispositivos compartilham a largura de banda do anel, o que pode resultar em limitações na taxa de transferência de dados. Além disso, adicionar ou remover nós na rede requer tempo de inatividade para toda a rede, o que pode ser inconveniente em termos de disponibilidade dos serviços.

A topologia em árvore, como mostrado na Figura 5 é caracterizada por um nó central que conecta *hubs* secundários, estabelecendo uma relação hierárquica com os dispositivos. O nó central representa o tronco da árvore, onde os *hubs* secundários ou nós de controle estão localizados, e os dispositivos conectados são anexados aos ramos (International IT, 2021).

Figura 5 - Topologia em árvore.



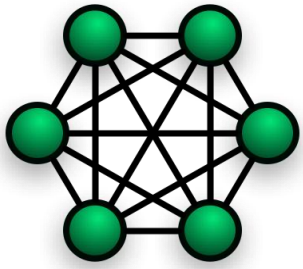
Fonte: International IT (2021, on-line)

Uma das principais vantagens da topologia em árvore é sua extrema flexibilidade e escalabilidade. Ela permite adicionar *hubs* secundários e dispositivos de forma fácil e eficiente, adaptando-se às necessidades de crescimento da rede. Além disso, a estrutura em árvore facilita a identificação de erros, pois cada ramo da rede pode ser diagnosticado individualmente, simplificando a resolução de problemas.

No entanto, também apresenta desvantagens a serem consideradas. Se o hub central falhar, os nós conectados a ele serão desconectados, embora os ramos possam continuar funcionando de forma independente. Isso pode levar a interrupções na comunicação e afetar a conectividade dos dispositivos. Além disso, a estrutura em árvore pode ser desafiadora de gerenciar de forma eficaz, especialmente em redes complexas com múltiplos ramos e dispositivos interconectados. Além disso, a topologia em árvore requer mais cabeamento em comparação com outros métodos devido à natureza hierárquica da conexão.

A topologia em malha, como mostrado na Figura 6 é caracterizada por uma rede de dispositivos interconectados. Existem dois tipos principais de topologia em malha: malha completa e malha parcial. Na malha completa, todos os dispositivos estão diretamente conectados uns aos outros, formando uma teia de conexões. Já na malha parcial, a maioria dos dispositivos está conectada diretamente, permitindo vários caminhos para a entrega de dados. Em ambas as configurações, os dados são transmitidos pelo caminho mais curto disponível.

Figura 6 - Topologia em malha.



Fonte: International IT (2021, on-line)

Uma das principais vantagens da topologia em malha é sua confiabilidade e estabilidade. Como os dispositivos estão interconectados, não há dependência de um único nó para a operação da rede. Mesmo que um dispositivo falhe, a rede continua funcionando por meio de outras rotas de comunicação disponíveis. No entanto, também apresenta desvantagens a serem consideradas. O grau de interconectividade entre os nós pode se tornar complexo, especialmente em redes maiores, exigindo um planejamento cuidadoso para a instalação e configuração adequadas. Além disso, a implementação de uma topologia em malha pode ser trabalhosa, pois requer a conexão direta de cada dispositivo com os demais. Isso implica em um maior uso de cabeamento em comparação

com outras topologias, aumentando os custos e a complexidade da infraestrutura física da rede.

2.1.3 Protocolos de Rede

Os protocolos de rede são conjuntos de regras que governam a comunicação entre dispositivos em uma rede. Existem muitos protocolos diferentes, como o Protocolo de Controle de Transmissão (TCP), Protocolo de Internet (IP), Protocolo de Datagrama de Usuário (UDP), Protocolo de Transferência de Arquivos (FTP) e Protocolo de Transferência de Arquivos Seguro (SFTP). Cada protocolo tem uma finalidade específica e é usado para diferentes tipos de comunicação (Tebaldi, 2019).

O Protocolo de Controle de Transmissão (TCP) oferece diversos serviços adicionais às aplicações. Primeiramente, e de maior importância, ele proporciona uma transferência confiável de dados.

Por meio do controle de fluxo, números de sequência, reconhecimentos e temporizadores, o protocolo garante que os dados sejam transmitidos corretamente e em ordem do processo remetente ao processo destinatário. Dessa forma, o TCP transforma o serviço não confiável do IP entre sistemas finais em um serviço confiável de transporte de dados entre processos. Além disso, o TCP também oferece controle de congestionamento, que não é tanto um serviço fornecido à aplicação solicitante, mas sim um serviço voltado para a Internet como um todo, visando o bem geral.

Em termos gerais, o controle de congestionamento do TCP impede que outras conexões TCP sobrecarreguem os links e roteadores entre os hosts comunicantes com um volume excessivo de tráfego. Em princípio, o TCP permite que as conexões TCP que trafegam por um link de rede congestionado compartilhem igualmente a largura de banda desse link. Isso é alcançado através do ajuste da taxa na qual o lado remetente do TCP pode enviar tráfego para a rede (James; Ross, 2013).

O Protocolo de Datagrama de Usuário (UDP) oferece um serviço não baseado em conexão para suas aplicações. É um serviço eficiente que garante segurança, mas sem controle de fluxo e congestionamento.

O Protocolo de Internet (IP) é um protocolo essencial para a comunicação na web. Ele permite a criação e o transporte de pacotes de dados, embora não garanta sua entrega. A identificação do destinatário é feita por meio de campos como o endereço IP, a máscara de sub-rede e o gateway padrão, que são fundamentais para o encaminhamento correto dos dados na rede (Tebaldi, 2019).

O endereço IP é o identificador utilizado no Protocolo de Internet. A versão mais comum desse protocolo é a versão 4, que possui um campo de endereço de 32 bits. Isso resulta em cerca de quatro bilhões de endereços disponíveis. Embora esse número seja considerável, está próximo de ser completamente utilizado. Por isso, a cada ano cresce a especulação em torno da adoção da versão 6 do protocolo. A versão 6, por sua vez, possui um campo de endereço de 128 bits, o que permite a inclusão de aproximadamente 340 undecilhões de dispositivos na Internet (Kurtz, 2020).

2.1.4 VLAN

Uma VLAN (*Virtual Area Network*) é uma técnica de rede que permite a divisão lógica de uma rede local em sub-redes virtuais, independentemente da localização física dos dispositivos. O principal objetivo de uma VLAN é criar segmentos lógicos em uma rede física, proporcionando isolamento e controle de tráfego (Perlman, 2000).

Uma das principais funções das VLANs é isolar o tráfego entre grupos de dispositivos. Essa separação melhora a segurança e a privacidade, uma vez que dispositivos pertencentes a uma VLAN não podem acessar diretamente dispositivos de outras VLANs, a menos que haja uma configuração específica permitindo essa comunicação e possibilitam o gerenciamento de tráfego. A segmentação baseada em VLAN permite a aplicação de políticas de *Qualidade de Serviço* (QoS), priorizando determinados tipos de tráfego e garantindo a qualidade adequada para serviços como voz, vídeo ou dados sensíveis.

A flexibilidade e escalabilidade são outras vantagens das VLANs. É possível adicionar, remover ou reconfigurar VLANs de maneira fácil e rápida, sem a necessidade de redesenhar fisicamente a infraestrutura de rede.

Além disso, elas auxiliam na organização e gestão da rede. Os dispositivos podem ser agrupados logicamente com base em departamentos, funções ou projetos, facilitando a aplicação de políticas de segurança, alocação de recursos, gerenciamento de acesso, além de permitir a convergência de serviços. Diferentes serviços podem compartilhar a mesma infraestrutura de rede física, por exemplo, uma VLAN para voz sobre IP (VoIP), outra para dados e outra para serviços de vídeo. Cada uma possui isolamento e priorização de tráfego adequados.

2.1.5 Segurança de Rede

A segurança de rede é um aspecto crítico de qualquer rede de computadores. É necessário proteger os dados e informações que são transmitidos através da rede contra ameaças externas. Existem diferentes tipos de medidas de segurança de rede, como

firewalls, segurança de e-mails, *software* antivírus e antimalware, segmentação de rede, controle de acesso, segurança de aplicações, análise do comportamento, prevenção contra perda de dados, sistemas de prevenção contra invasão, segurança de dispositivos móveis, segurança das informações e gerenciamento de eventos, VPN, segurança da web e segurança sem fio. Cada uma dessas medidas desempenha um papel específico na proteção da rede e dos dados (Cisco, [s.d.]).

Os *firewalls* atuam como uma proteção entre uma rede interna confiável e as redes externas não confiáveis, como a Internet. Eles são responsáveis por aplicar um conjunto de regras que determinam quais tipos de tráfego são permitidos ou bloqueados. Os *firewalls* podem ser implementados tanto em hardware quanto em *software*, e a Cisco oferece dispositivos de gerenciamento unificado de ameaças (UTM) e *firewalls* de próxima geração com foco em ameaças.

Essas soluções proporcionam uma defesa robusta contra ameaças em constante evolução. Além disso, o uso de *software* antivírus e antimalware é essencial para combater diferentes tipos de malware, como vírus, *worms*, *Trojans*, *ransomware* e *spyware*. Esses programas não apenas analisam o malware na entrada, mas também monitoram constantemente os arquivos em busca de anomalias, removendo o malware e corrigindo quaisquer danos.

A segmentação de rede, realizada por meio de *software*, classifica o tráfego de rede e facilita a aplicação de políticas de segurança. A segmentação baseada na identidade do dispositivo, em vez de apenas no endereço IP, permite a atribuição de direitos de acesso com base na função e localização, garantindo que apenas as pessoas autorizadas tenham acesso adequado à rede.

O controle de acesso à rede é fundamental para impedir que invasores acessem a rede. Ao reconhecer cada usuário e dispositivo, é possível aplicar políticas de segurança adequadas, bloqueando dispositivos não autorizados ou concedendo acesso limitado.

A análise do comportamento é uma técnica que permite detectar atividades anormais na rede, identificando indicadores de comprometimento e agindo rapidamente contra ameaças. Ferramentas de análise comportamental automatizam esse processo, distinguindo automaticamente as atividades que fogem do comportamento normal.

A prevenção contra perda de dados é essencial para evitar que informações confidenciais sejam enviadas de forma insegura para fora da rede. Tecnologias de DLP impedem o envio, encaminhamento ou impressão de informações importantes, garantindo a segurança dos dados.

Os sistemas de prevenção contra invasões analisam o tráfego de rede para bloquear ativamente ataques. Dispositivos de próxima geração, como os da Cisco, utilizam inteligência de ameaças global para bloquear atividades mal-intencionadas, monitorar a progressão de arquivos suspeitos na rede e prevenir a disseminação de ataques.

Redes virtuais privadas (VPNs) criptografam as conexões de *endpoints* para uma rede, geralmente pela Internet. VPNs de acesso remoto utilizam protocolos de segurança, como IPsec ou SSL, para autenticar a comunicação entre o dispositivo e a rede.

2.1.6 Gestão de Rede

A gestão de rede é a prática de gerenciar uma rede de computadores para garantir que ela funcione efetivamente e eficientemente. Isso envolve a monitorização e resolução de problemas em tempo real, bem como a implementação de políticas de segurança e atualizações de *software*. Muitas plataformas de gerenciamento de rede começaram como uma forma de controlar redes locais (LANs).

À medida que as redes corporativas se tornaram mais complexas e diversificadas, esses sistemas de gerenciamento expandiram suas capacidades para incluir SD-WAN, segurança e IoT (Internet of Things). As plataformas mais eficazes combinam dispositivos e sensores em uma única visualização do tráfego de rede, facilitando para a equipe de TI não apenas monitorar, mas também proteger e solucionar problemas de desempenho (Cisco, [s.d.]).

Os sistemas de gerenciamento de rede coletam dados em tempo real dos elementos de rede, como *switches*, roteadores, pontos de acesso, assim como dispositivos de *endpoint*, como telefones celulares, laptops e desktops. Essas informações são utilizadas para fornecer insights sobre o estado da rede.

Geralmente, os dados são coletados e enviados para o sistema de duas maneiras, SNMP (*Simple Network Management Protocol*): o Protocolo Simples de Gerenciamento de Rede é um padrão aberto amplamente suportado pela maioria dos fabricantes de elementos de rede desde a década de 1990. O SNMP faz consultas a cada elemento da rede e envia as respostas ao sistema de gerenciamento de rede e Telemetria em tempo real: um agente de *software* instalado em um elemento de rede permite a transmissão automática de indicadores-chave de desempenho em tempo real. A telemetria em tempo real está substituindo rapidamente o SNMP, pois é mais eficiente, capaz de gerar um maior número de pontos de dados e oferece maior escalabilidade. Além disso, padrões de

telemetria, como NETCONF/YANG, estão ganhando aceitação como formas de oferecer o mesmo suporte multifornecedor do SNMP (Cisco, [s.d.]).

Quando se trata de gerenciar uma rede complexa ou altamente distribuída, as três capacidades mais cruciais de uma ferramenta de gerenciamento de rede estão diretamente relacionadas à sua habilidade de unificar locais e trabalhadores remotos.

À medida que o número de dispositivos e aplicativos conectados às redes aumenta, as redes se tornam mais complexas. No entanto, uma rede complexa não requer necessariamente um sistema de gerenciamento de rede complexo de usar. Os sistemas de gerenciamento de rede atuais são abertos, expansíveis e orientados por *software*, o que ajuda a acelerar e simplificar as operações de rede, reduzir custos e diminuir riscos.

Impulsionados por inteligência avançada e segurança integrada, esses sistemas oferecem automação e garantia em toda a rede, independentemente de seu tamanho, resultando em maior eficiência e economia de custos, ao mesmo tempo em que fornecem visibilidade, automação e conhecimentos abrangentes.

No ambiente de trabalho híbrido atual, as organizações enfrentam uma variedade de desafios. Esses desafios incluem uma força de trabalho altamente distribuída e móvel, uma variedade inconsistente de opções de conectividade de qualidade e a necessidade de implementar rapidamente ferramentas de colaboração, suporte e continuidade dos negócios.

Consequentemente, os sistemas de gerenciamento de rede precisam ser ágeis, com inteligência e automação integradas para facilitar a tomada de decisões e reduzir erros. A segurança deve ser inerente e priorizada para garantir que as redes e os dispositivos conectados a elas estejam seguros desde o núcleo até a borda.

2.2 DISPOSITIVOS DE REDE

Os dispositivos de rede são hardware que é usado para conectar computadores e outros dispositivos em uma rede. Alguns exemplos de dispositivos de rede incluem roteadores, *switches*, *hubs* e placas de rede. Cada dispositivo tem uma função específica em uma rede e pode ser usado para otimizar a comunicação e a transferência de dados.

2.2.1 Switch

Um *switch*, como observado na Figura 7 é um dispositivo de rede utilizado para conectar vários dispositivos em uma rede local (LAN). Ele é projetado para direcionar o tráfego de rede de forma eficiente, enviando pacotes de dados para o destino correto (Spurgeon; Zimmerman, 2013).

Figura 7 - Switch 24 Portas Gigabit 10/100/1000 Tp-link TL-SG1024D.

Fonte: Amazon, ([s.d.], on-line)

O principal objetivo de um *switch* é criar uma rede de comunicação eficiente, permitindo que diferentes dispositivos (como computadores, impressoras, servidores, etc.) se comuniquem entre si. Ele desempenha a função de um intermediário inteligente, conectando dispositivos em uma rede local e garantindo que o tráfego seja direcionado apenas para os dispositivos relevantes (Spurgeon; Zimmerman, 2013).

Ao receber dados de um dispositivo, o *switch* examina o endereço MAC contido no pacote de dados para identificar o dispositivo de destino. Com base nessa informação, o *switch* encaminha o pacote de dados apenas para a porta conectada ao dispositivo de destino. Isso permite que os dados sejam enviados apenas para o dispositivo correto, minimizando o congestionamento da rede e melhorando o desempenho.

Os *switches* modernos também podem oferecer recursos avançados, como VLANs (*Virtual Local Area Networks*), priorização de tráfego QoS, monitoramento de rede, segurança de rede e outras funcionalidades adicionais.

2.2.2 Roteador

Um roteador, como o visto na Figura 8, é um dispositivo de rede responsável por encaminhar pacotes de dados entre diferentes redes. Sua função é tomar decisões inteligentes com base nos endereços IP de origem e destino contidos nos pacotes, determinando o melhor caminho para enviar esses pacotes.

Figura 8 - Roteador D-link DSL-2740M sem fio n300 adsl2.

Fonte: Alibaba.com ([s.d.], on-line)

O objetivo principal de um roteador é interconectar redes e direcionar o tráfego de forma eficiente. Ele desempenha um papel fundamental em redes de computadores, como a Internet, roteando pacotes de dados entre diferentes redes locais (LANs) ou entre uma rede local e a Internet (WAN - *Wide Area Network*) (Peterson; Davie, [s.d.]).

Um roteador possui diversas funções e usos importantes. Uma delas é o encaminhamento de pacotes, em que o roteador recebe pacotes de dados de uma rede e os envia para a rede correta com base nas informações do endereço IP de destino. Isso é feito por meio de tabelas de roteamento e protocolos de roteamento, como OSPF (*Open Shortest Path First*).

Muitos roteadores também possuem uma função de compartilhamento de conexão à Internet. Através da função de NAT (*Network Address Translation*), um único endereço IP externo é compartilhado entre vários dispositivos em uma rede local. O roteador atribui endereços IP locais aos dispositivos internos e traduz esses endereços para o endereço IP externo.

Além disso, os roteadores desempenham um papel importante na segurança de rede. Eles podem oferecer recursos como *firewalls* para proteger a rede contra ameaças externas. Os roteadores podem filtrar e inspecionar o tráfego de entrada e saída, implementar regras de segurança e fornecer proteção contra ataques cibernéticos.

2.2.3 Firewall

Um *firewall* é uma medida de segurança de rede que monitora e controla o tráfego com base em regras predefinidas. Ele tem como objetivo proteger a rede ou dispositivo contra ameaças externas, como ataques cibernéticos e malware. O *firewall* atua como uma barreira entre a rede interna e a rede externa, geralmente a Internet, controlando o tráfego que entra e sai da rede por meio da aplicação de regras de filtragem.

Ele examina os pacotes de dados com base em critérios como endereço IP de origem, endereço IP de destino, número de porta e protocolo, permitindo ou bloqueando o tráfego com base nessas informações para evitar o acesso não autorizado à rede (Stewart; Kinsey, 2020).

Outro recurso comum em *firewalls* é a tradução de endereços de rede (NAT), que permite que vários dispositivos internos compartilhem um único endereço IP público, protegendo a identidade e a estrutura da rede interna.

Alguns *firewalls* avançados realizam uma inspeção profunda de pacotes (DPI), que analisa não apenas os cabeçalhos, mas também o conteúdo dos pacotes. Isso possibilita identificar e bloquear ameaças baseadas em conteúdo, como ataques

específicos de aplicativos ou tráfego malicioso. Além disso, muitos *firewalls* oferecem recursos embutidos para criação e gerenciamento de conexões VPN (Rede Virtual Privada), que estabelecem túneis seguros para comunicação privada entre redes remotas. Essa função adiciona uma camada adicional de segurança à rede.

2.2.4 Rack

Um rack, como observado na Figura 9, também conhecido como gabinete ou bastidor, é uma estrutura física que tem como finalidade abrigar e organizar equipamentos eletrônicos em uma infraestrutura de rede ou data center. Ele consiste em uma estrutura metálica ou de plástico com prateleiras, painéis e acessórios que permitem a montagem e organização padronizada dos equipamentos (Woodward, 2014).

Figura 9 - Rack Servidor Fechado 44U x 570mm.

Fonte: Rackfort (2024, on-line)

Os racks são amplamente utilizados em ambientes de tecnologia da informação (TI) e redes para fornecer um local centralizado para a instalação e interconexão de vários componentes, como servidores, *switches*, roteadores, dispositivos de armazenamento, patch panels, unidades de distribuição de energia (PDUs) e outros dispositivos de rede.

2.2.5 Patch Panel

Um patch panel, como observado na Figura 10, também conhecido como painel de conexão ou painel de interligação, é um componente utilizado em redes de computadores para organizar e facilitar a conexão de cabos de rede. Ele é um painel montado em um rack ou gabinete e possui uma série de portas, geralmente RJ-45, onde os cabos de rede podem ser conectados (Woodward, 2014).

Figura 10 - Patch Panel 24 portas 5e.

Fonte: Free SVG ([s.d.], on-line)

A função principal de um patch panel é fornecer uma maneira organizada e flexível de gerenciar a interconexão dos cabos de rede. Aqui estão alguns dos principais usos e benefícios do patch panel:

O patch panel permite a organização dos cabos em um local centralizado e de fácil acesso. Os cabos são terminados nas portas do patch panel, facilitando a identificação e a manutenção dos cabos individuais. É possível reconfigurar ou adicionar conexões conforme necessário, sem precisar alterar a infraestrutura física da rede.

O patch panel também simplifica o gerenciamento das conexões de rede. Ao conectar os cabos ao patch panel, é possível alterar, adicionar ou remover conexões de forma rápida e fácil, sem a necessidade de mexer diretamente nos dispositivos finais.

2.2.6 Tipos de Cabo de Rede

Há uma variedade de cabos de rede que são empregados para estabelecer conexões e possibilitar a transferência de dados entre dispositivos. Cada tipo de cabo possui características específicas que o tornam adequado para diferentes necessidades e cenários. Neste texto, vamos explorar alguns dos cabos de rede mais comumente utilizados.

O cabo de par trançado é amplamente empregado em redes Ethernet. Composto por pares de fios de cobre entrelaçados, esse cabo ajuda a reduzir a interferência eletromagnética. Existem duas categorias principais de cabo de par trançado: UTP (*Unshielded Twisted Pair* - par trançado não blindado) e STP (*Shielded Twisted Pair* - par trançado blindado). O UTP é mais comum em redes domésticas e de escritórios, enquanto o STP possui uma camada adicional de blindagem metálica para uma proteção extra contra interferências externas.

Outro cabo comumente utilizado é o cabo coaxial, encontrado em sistemas de TV a cabo e redes de banda larga. Esse cabo consiste em um núcleo central condutor isolado por um material dielétrico, envolto por uma malha condutora externa. Essa configuração ajuda a minimizar a perda de sinal e a interferência externa, permitindo a transmissão de sinais de alta frequência com boa qualidade.

Para transmissões de dados de alta velocidade e alta capacidade, o cabo de fibra óptica é a opção ideal. Ele utiliza fibras de vidro ou plástico para transmitir pulsos de luz que carregam os dados. O núcleo interno do cabo é altamente reflexivo, o que possibilita a propagação do sinal óptico por longas distâncias com mínima perda de qualidade. Os cabos de fibra óptica são amplamente empregados em redes de longa distância, backbones de rede e aplicações que requerem altas taxas de transferência, como redes de data centers.

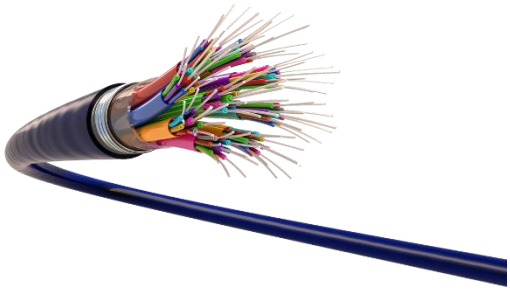
Existem também os cabos de par trançado blindado (FTP/STP), que são similares aos cabos de par trançado convencionais, mas possuem uma camada extra de blindagem para proteção contra interferências eletromagnéticas. Esses cabos são utilizados em ambientes onde há maior probabilidade de interferências, como locais com fiação elétrica densa ou exposição a campos magnéticos intensos.

É fundamental escolher o tipo adequado de cabo de rede com base nas necessidades específicas de cada situação. Cada cabo possui vantagens e limitações em termos de velocidade, distância máxima de transmissão e imunidade a interferências. Ao selecionar um cabo de rede, é crucial considerar a velocidade desejada da rede, a distância que os dados precisam percorrer, a interferência ambiental esperada e a infraestrutura existente.

Para suprir a demanda de um laboratório de redes de computadores será necessário o uso do cabo de fibra óptica.

Cabo de fibra óptica, como visto na Figura 11, utiliza fibras de vidro ou plástico para transmitir dados através de pulsos de luz. Os cabos de fibra óptica oferecem alta velocidade, largura de banda e imunidade a interferências eletromagnéticas. Eles são amplamente utilizados em redes de longa distância e em ambientes com alta demanda de largura de banda, como data centers. Existem diferentes tipos de cabos de fibra óptica, como MM (Multimodo) e SM (Monomodo) cada um adequado para diferentes aplicações e distâncias (Conway, 2019).

Figura 11 - Fibra Óptica.



Fonte: GratisPNG ([s.d.], on-line)

2.2.7 Categorias de Cabo Ethernet

Atualmente, existem dois tipos principais de cabos de rede com algumas variações. O cabo coaxial é usado principalmente para conexões de internet em redes locais, transmitindo dados a uma taxa máxima de 10 Megabits por segundo (Mbps). Ele é comumente encontrado em provedores de internet e é adequado para conexões

residenciais e pequenas redes locais. O cabo coaxial usa uma topologia de barramento, onde todos os dispositivos estão conectados ao mesmo cabo principal.

O cabo de par trançado é amplamente utilizado em redes locais e possui quatro pares de fios entrelaçados para melhorar a conexão e reduzir a interferência eletromagnética. Diferente do cabo coaxial, ele pode ser usado em diferentes topologias. É comumente utilizado para conectar equipamentos de rede, como *hubs* e *switches*. O cabo de par trançado usa conectores RJ-45, e diferentes configurações, conhecidas como cabo cruzado ou crossover, podem ser necessárias para conectar dispositivos semelhantes.

Existem várias categorias de cabos de par trançado, cada uma com diferentes velocidades e capacidades de transmissão. O CAT5 é um padrão mais antigo, com velocidade de cerca de 100 Mbps, e é raramente utilizado em redes domésticas atualmente. O CAT5e é uma versão aprimorada do CAT5, com velocidade de 1.000 Mbps (1 Gbps) e uma melhor qualidade de conexão. É uma opção popular em termos de custo-benefício (MORENTE, 2023).

O CAT 6 possui uma estrutura diferente do CAT5e, oferecendo velocidades de até 10 Gigabits (10 Gbps) e menor interferência de sinal. É menos comum em configurações domésticas, sendo mais adequado para redes corporativas que exigem altas velocidades de transferência de dados. O CAT6a é uma versão aprimorada do CAT6, com as mesmas velocidades e melhor desempenho em distâncias maiores (MORENTE, 2023).

O CAT7 é uma categoria de cabo de alto desempenho que suporta velocidades de até 10 Gbps em distâncias de até 100 metros. Ele possui uma blindagem mais robusta e conectores de metal para minimizar a interferência. O CAT7 é recomendado para ambientes onde o cabeamento passa próximo a fios condutores de eletricidade (MORENTE, 2023).

Por fim, o CAT8 oferece velocidades de transmissão de até 40 Gbps em distâncias de até 30 metros. É um cabo de rede de alta velocidade que se aproxima do desempenho da fibra óptica. No entanto, devido à sua limitação de distância, o CAT7 é geralmente preferido para cobrir áreas maiores (MORENTE, 2023).

2.2.8 Hosts

Os hosts, como computadores e servidores, desempenham um papel fundamental na troca de informações e recursos em uma rede. Eles possuem capacidade de armazenamento e processamento de dados, executando aplicativos, processando solicitações e fornecendo serviços aos dispositivos na rede (Peterson; Davie, [s.d.]).

Além disso, os hosts têm a capacidade de compartilhar recursos, como arquivos e impressoras, permitindo que outros dispositivos acessem e utilizem esses recursos na rede local.

Os hosts também facilitam o acesso dos usuários a serviços e recursos disponíveis na rede, como acesso à Internet, serviços de e-mail, streaming de mídia e acesso a bancos de dados, oferecidos por outros hosts na rede.

A comunicação e a troca de dados entre hosts são realizadas por meio da troca de informações, como mensagens, arquivos, solicitações e respostas, utilizando protocolos de comunicação, como o protocolo TCP/IP.

2.3 ATIVIDADES EM LABORATÓRIOS DE REDES

O laboratório de redes é crucial no campo da tecnologia da informação, permitindo que profissionais aprimorem suas habilidades e adquiram conhecimento sobre o funcionamento e administração de redes de comunicação.

Nesse ambiente controlado, estudantes, pesquisadores e profissionais podem experimentar diferentes configurações, protocolos e tecnologias de rede, realizando atividades práticas como configuração de dispositivos, estabelecimento de conexões, implementação de protocolos de roteamento, resolução de problemas e simulação de cenários complexos. Além disso, esses laboratórios também servem como espaços de pesquisa, onde cientistas e acadêmicos investigam novas tecnologias e desenvolvem soluções inovadoras para desafios emergentes, resultando em melhorias na eficiência, segurança e confiabilidade das redes.

2.3.1 Montagem e Configuração de Redes de Comunicação

Após a instalação física, é necessário configurar os dispositivos de rede, como roteadores, *switches* e pontos de acesso. Isso inclui atribuir endereços IP aos dispositivos, configurar interfaces de rede, estabelecer rotas de comunicação, definir políticas de segurança (como *firewalls* e autenticação) e configurar serviços de rede (como DHCP (*Dynamic Host Configuration Protocol*) e DNS (*Domain Name System*)).

Após a configuração inicial, é importante realizar testes para verificar se a rede está funcionando conforme o esperado. Isso envolve a verificação da conectividade entre os dispositivos, o teste de serviços de rede, a avaliação do desempenho e a identificação de possíveis problemas. Caso ocorram falhas ou problemas de conectividade, é necessário realizar diagnósticos para identificar a causa raiz e aplicar as correções apropriadas.

Após a rede estar em funcionamento, é essencial estabelecer um processo contínuo de monitoramento e manutenção. Isso inclui monitorar o desempenho da rede, detectar e solucionar problemas de conectividade, aplicar atualizações de segurança e firmware, realizar backups regulares e implementar políticas de gerenciamento de rede.

2.3.2 Monitoramento de Pacotes e Protocolos

O monitoramento de pacotes e protocolos é uma técnica utilizada para analisar o tráfego de rede em tempo real e obter informações detalhadas sobre o funcionamento dos protocolos de comunicação e o fluxo de dados entre os dispositivos da rede (Sanders, 2017).

Existem diversas ferramentas e *softwares* disponíveis para realizar o monitoramento de pacotes e protocolos, como o *Wireshark*, tcpdump e Microsoft Network Monitor. Essas ferramentas capturam os pacotes de dados que trafegam pela rede e exibem informações como endereços IP de origem e destino, portas utilizadas, tipos de protocolo, tamanho dos pacotes.

O monitoramento de pacotes permite analisar o tráfego de rede em diferentes níveis, desde o nível de enlace até o nível de aplicação. Ele permite identificar problemas de desempenho, anomalias de rede, erros de protocolo, tráfego indesejado e até mesmo atividades maliciosas na rede.

Além disso, o monitoramento de pacotes também é útil para analisar o desempenho da rede, identificar gargalos, otimizar a utilização dos recursos de rede e diagnosticar problemas de conectividade.

Ao utilizar essas ferramentas, os administradores de rede podem examinar e filtrar os pacotes de acordo com suas necessidades, visualizar as informações em formatos legíveis e realizar análises detalhadas para solucionar problemas ou otimizar a rede.

2.3.3 Redes de Comunicação sem Fio

Redes de comunicação sem fio, também conhecidas como redes wireless, são sistemas de comunicação que permitem a troca de informações entre dispositivos sem a necessidade de cabos físicos. Essas redes utilizam ondas eletromagnéticas, como ondas de rádio ou sinais de infravermelho, para transmitir dados entre os dispositivos (Rappaport, 2002).

O funcionamento básico envolve dispositivos sem fio, como smartphones, laptops, tablets e roteadores sem fio, equipados com interfaces sem fio, como Wi-Fi, Bluetooth ou 3G/4G/5G. Um ponto de acesso atua como um hub central para conectar dispositivos sem fio à rede, encaminhando dados para outros dispositivos e fornecendo

serviços de segurança, como autenticação e criptografia. O meio de transmissão é o espaço físico onde as ondas eletromagnéticas são propagadas, permitindo a comunicação entre dispositivos em diferentes locais dentro do alcance da rede. Protocolos de comunicação, como Wi-Fi, Bluetooth e redes móveis, garantem a eficiência da comunicação. A segurança é essencial, com técnicas de criptografia e autenticação sendo utilizadas para proteger a privacidade e a integridade dos dados transmitidos.

O alcance e a cobertura das redes sem fio variam dependendo da tecnologia, sendo importante considerar esses aspectos ao planejar e implementar redes sem fio. Essas redes podem ser implementadas em diferentes escalas, desde redes locais sem fio em ambientes residenciais ou empresariais até redes de longa distância, como redes móveis que abrangem grandes áreas geográficas.

2.3.4 Internet das Coisas

A Internet das Coisas (IoT) é um conceito que se refere à conexão de dispositivos do cotidiano à internet, permitindo que eles troquem informações e interajam entre si. Esses dispositivos podem ser objetos físicos, como eletrodomésticos, veículos, sensores, câmeras, entre outros, que são equipados com sensores, *software* e conectividade para coletar e compartilhar dados.

A ideia por trás da IoT é criar uma rede de dispositivos interconectados que possam coletar, transmitir e analisar dados de forma automatizada, tornando possível monitorar, controlar e otimizar esses dispositivos de maneira mais eficiente. A IoT permite que os objetos se comuniquem uns com os outros, sem intervenção humana direta, e tomem decisões com base nas informações coletadas (Kranz, 2016).

O funcionamento da IoT envolve três componentes principais: dispositivos, conectividade e plataforma de dados.

- Dispositivos: Os dispositivos IoT são equipados com sensores e atuadores que permitem coletar dados do ambiente e interagir com ele. Esses dispositivos podem variar em tamanho e complexidade, desde pequenos sensores até veículos autônomos. Eles coletam informações, como temperatura, umidade, localização, movimento, entre outros, e as transformam em dados digitais.
- Conectividade: A conectividade é essencial na IoT, permitindo que os dispositivos se comuniquem e transmitam os dados coletados. Isso é alcançado por meio de diferentes tecnologias de rede, como Wi-Fi, Bluetooth, Zigbee, NFC (Near Field Communication) e redes celulares, como 3G, 4G e 5G. A escolha da

tecnologia de conectividade depende do alcance, largura de banda, consumo de energia e outros requisitos específicos do dispositivo e da aplicação.

- Plataforma de dados: Os dados coletados pelos dispositivos são enviados para uma plataforma de dados, onde são armazenados, processados e analisados. Essa plataforma pode ser baseada em nuvem ou em servidores locais. Ela permite que os dados sejam acessados, gerenciados e utilizados para tomar decisões inteligentes. Algoritmos de análise de dados e inteligência artificial podem ser aplicados para extrair informações valiosas e insights dos dados coletados.

2.3.5 Comunicações Ópticas

A comunicação óptica é um método de transmissão de informações que utiliza sinais de luz para transmitir dados. Ela é baseada no uso de fibras ópticas, que são fios finos e transparentes feitos de material especial que permite que a luz seja transmitida ao longo de sua extensão (Conway, 2019).

No processo de comunicação óptica, os dados são convertidos em pulsos de luz, que são enviados através da fibra óptica. Esses pulsos de luz representam os bits de informação, sendo que a presença ou ausência de luz indica os valores binários 0 e 1, respectivamente.

Ao longo da fibra óptica, a luz se propaga através de reflexões internas totais. Isso ocorre devido ao fenômeno da reflexão total interna, onde a luz é refletida de volta para dentro da fibra quando atinge um ângulo crítico em relação à interface entre o núcleo da fibra e sua casca externa.

Para enviar os dados em uma fibra óptica, é necessário modular a intensidade da luz. Isso é feito por meio de um dispositivo chamado modulador óptico, que varia a intensidade da luz de acordo com os sinais elétricos que representam os dados a serem transmitidos. Na extremidade receptora, um dispositivo chamado fotodetector converte a luz em sinais elétricos novamente, permitindo a recuperação dos dados originais.

A comunicação óptica oferece vantagens em relação a outros métodos de transmissão, como maior largura de banda, menor perda de sinal e imunidade a interferências eletromagnéticas. Essas características tornam a comunicação óptica ideal para transmitir grandes volumes de dados em longas distâncias, como em redes de telecomunicações e sistemas de transmissão de internet de alta velocidade.

2.3.6 Redes Industriais

Uma rede industrial, ou rede de automação industrial, é um sistema de comunicação desenvolvido para interligar dispositivos e equipamentos em ambientes

industriais. Essas redes suportam a comunicação e o controle de processos, facilitando a troca de informações e o gerenciamento eficiente das operações. Os principais elementos de uma rede industrial incluem dispositivos como controladores lógicos programáveis (CLPs), sensores, atuadores e sistemas de monitoramento, que coletam e transmitem dados do processo industrial. Esses dispositivos monitoram e controlam variáveis críticas, como temperatura, pressão, nível e velocidade (Marshall; Rinaldi, 2017).

Essas redes utilizam protocolos especializados, como Profibus, Modbus, Ethernet/IP, Profinet e DeviceNet, que garantem a transmissão segura e confiável de dados, proporcionando comunicação em tempo real e sincronização precisa entre os dispositivos. Controladores, como os CLPs, desempenham papel essencial ao processar informações e tomar decisões baseadas em parâmetros predefinidos, enquanto sistemas de supervisão, como o SCADA, oferecem uma visão centralizada do processo industrial (Marshall; Rinaldi, 2017).

A segurança e confiabilidade são prioritárias, demandando medidas como *firewalls*, autenticação de dispositivos e criptografia de dados, além de técnicas de redundância, como duplicação de componentes críticos e caminhos de comunicação alternativos. Além disso, essas redes promovem a integração de diversos sistemas e dispositivos, coordenando a produção e otimizando a troca de informações entre eles. Assim, as redes industriais visam aumentar a eficiência, a produtividade e a segurança dos processos, proporcionando automação, monitoramento em tempo real e controle preciso das operações.

2.3.7 Simulação de Ataques em Redes de Comunicação

A simulação de ataques em redes de comunicação é uma prática essencial na segurança cibernética, pois permite testes realistas para identificar vulnerabilidades antes que sejam exploradas por agentes mal-intencionados. Esse processo avalia a capacidade de detecção de intrusões, a resposta a incidentes e a eficácia das medidas de segurança aplicadas, identificando pontos fracos e fornecendo insights sobre ameaças potenciais, o que contribui para aprimorar defesas e políticas de segurança.

Recentemente, a Guardicore aprimorou sua ferramenta Infection Monkey, utilizada para simular ataques e violações de segurança. Agora, a ferramenta conta com um novo relatório que oferece recomendações técnicas e medidas de mitigação com base no conhecimento da matriz MITRE ATT&CK, reconhecida por profissionais de segurança como uma referência abrangente de táticas e técnicas de ataques reais. Esse

relatório permite que equipes de segurança simulem ameaças persistentes avançadas e adotem medidas estratégicas para mitigá-las (Redação, [s.d.]).

Com a nova versão, o Infection Monkey possibilita a execução de testes com técnicas específicas do ATT&CK, fornecendo análises detalhadas sobre o uso dessas técnicas e oferecendo recomendações para a proteção da rede. Esses testes podem ser configurados facilmente, sendo executados de forma automatizada, com os resultados apresentados em relatórios de fácil interpretação. A ferramenta permite que profissionais de segurança avaliem automaticamente a defesa de rede, identificando violações de políticas e gerando recomendações que podem ser aplicadas sem necessidade de treinamento especializado, ajudando a identificar e corrigir deficiências nas defesas da rede (Redação, [s.d.]).

2.3.8 Configuração de VLANs

As VLANs são redes virtuais que permitem a segmentação de uma rede física em várias redes lógicas distintas, proporcionando flexibilidade e segurança no gerenciamento dos dispositivos. Cada VLAN atua como uma rede independente, com seus próprios endereços IP e configurações de rede (Perlman, 2000).

Diversas configurações podem ser utilizadas na implementação de VLANs, adaptando-se às necessidades e requisitos da rede. A primeira configuração comum é a VLAN baseada em porta, onde cada porta de um *switch* é atribuída a uma VLAN específica, agrupando os dispositivos conectados em uma mesma VLAN.

Outra configuração é a VLAN baseada em endereço MAC, em que os dispositivos são atribuídos a VLANs com base em seus endereços MAC. Isso possibilita que um dispositivo seja automaticamente designado a uma VLAN específica, independentemente da porta do *switch* a qual esteja conectado.

A VLAN baseada em sub-rede IP é outra opção, na qual os dispositivos são associados a VLANs de acordo com suas sub-redes IP. Dispositivos com endereços IP em uma determinada faixa são automaticamente incluídos na VLAN correspondente, permitindo a segmentação por departamentos ou grupos de trabalho.

A segmentação da rede também pode ocorrer por meio da VLAN baseada em protocolo, onde dispositivos que utilizam um protocolo específico, como VoIP ou vídeo, são agrupados em uma VLAN separada para priorizar e otimizar o desempenho desse tipo de tráfego.

Por fim, temos a VLAN baseada em políticas, onde elas são atribuídas com base em políticas de segurança ou requisitos de acesso. Por exemplo, dispositivos de

convidados podem ser colocados em uma VLAN separada com acesso restrito aos recursos internos da rede.

Essas configurações de VLANs oferecem uma segmentação mais refinada da rede, proporcionando maior controle, desempenho e segurança na troca de informações e recursos entre os dispositivos.

3 MATERIAIS E MÉTODOS

Nesta seção, serão apresentados os materiais e métodos necessários para o desenvolvimento dos roteiros práticos, com base no laboratório de redes de computadores da UFU Patos de minas.

3.1 MATERIAIS

Os materiais utilizados para realizar esse trabalho foram listados na tabela a seguir:

Tabela 1 - Lista de Materiais

Material	Descrição
Raspberry Pi 3	Microcomputador usado nos roteiros de configuração e monitoramento de rede.
Cartão SD (mín. 8GB, preferencialmente 16GB)	Armazenamento do sistema operacional para o Raspberry Pi.
Raspberry Pi Imager	*Software* para gravar sistemas operacionais no cartão SD.
Fonte de alimentação para Raspberry Pi	Alimentação elétrica para o Raspberry Pi.
Monitor	Exibição da interface do Raspberry Pi.
Teclado e mouse	Periféricos para controle do Raspberry Pi durante a configuração.
Cabo HDMI	Conexão do Raspberry Pi ao monitor.
Computador	Equipamento utilizado para configuração e monitoramento da rede.
Wireshark	*Software* de captura e análise de pacotes de rede.
Packet Sender	*Software* para envio de pacotes de rede durante os testes.

Acesso à internet	Necessário para baixar *softwares* e realizar algumas configurações online.
Conexão de rede Ethernet ou Wi-Fi	Meio de conexão para captura de pacotes e acesso à rede.
Arquivo de texto	Usado como referência para testes com Packet Sender.
Cabo de rede (Cat5e, Cat6, etc.)	Conexão de dispositivos em rede.
Conectores RJ-45	Terminais para crimpar cabos de rede.
Alicate de crimpagem	Ferramenta para crimpar cabos de rede.
Decapador de cabos	Ferramenta para remover o revestimento dos cabos de rede.
Tesoura ou cortador de cabos	Ferramenta para cortar cabos no comprimento desejado.
Testador de cabos de rede	Verifica a continuidade e integridade das conexões dos cabos.
Parafusadeira ou chave de fenda	Opcional, usada para ajustes durante a crimpagem e instalação do Patch Panel.
Patch Panel	Equipamento que organiza conexões de rede em um rack.
Rack de rede	Estrutura para montar equipamentos de rede.
Ferramenta *Punch Down*	Ferramenta para conectar cabos ao Patch Panel.
Fita de velcro	Organização de cabos no rack.
Switch HP 1910	Dispositivo para configuração de VLANs e bloqueio de portas em horários específicos.
Software PuTTY	Utilitário para acesso remoto via SSH.
Navegador	Acesso à interface web para configurar dispositivos de rede.
Acesso ao terminal ou CMD	Teste de conectividade e configuração em dispositivos de rede.

Fonte: O autor

Os materiais utilizados para as práticas de configuração de rede e monitoramento abrangem uma série de dispositivos e ferramentas que são essenciais para garantir uma rede funcional, configurável e testável. O *Raspberry Pi* 3 é uma plataforma de hardware

compacta e acessível, ideal para testes de rede e instalação de sistemas operacionais como OpenWrt. Ele permite a experimentação de redes Wi-Fi e configurações de roteamento em um ambiente controlado e de baixo custo. Para o funcionamento do *Raspberry Pi*, é necessário o cartão SD (preferencialmente de 16GB ou superior), que armazena o sistema operacional e os dados essenciais para as práticas, como configuração de rede e monitoramento de pacotes. A fonte de alimentação garante que o dispositivo funcione com estabilidade durante todo o processo de configuração, enquanto o monitor, teclado e mouse permitem interações diretas para realizar as configurações iniciais do sistema, sobretudo em situações em que o acesso remoto não foi configurado.

O *Raspberry Pi* Imager, que possibilita a gravação do sistema operacional no cartão SD, essencial para preparar o *Raspberry Pi* com o *software* necessário para cada prática. Em atividades que exigem captura e análise de pacotes de rede, o *Wireshark* desempenha papel central, pois permite a visualização detalhada dos dados que trafegam pela rede, proporcionando uma análise de segurança e desempenho. Em conjunto com o *Wireshark*, o *Packet Sender* permite o envio de pacotes de teste, útil para analisar o comportamento da rede em diferentes cenários. Para garantir o funcionamento adequado do *Wireshark*, ajustes de permissões de usuário são necessários em alguns sistemas, assegurando que o *software* tenha acesso irrestrito aos pacotes de rede.

O cabo de rede Ethernet e o computador são usados de forma recorrente para estabelecer a conexão entre os dispositivos, permitindo que as configurações sejam realizadas e testadas. Para práticas que envolvem a montagem física de cabos, como a crimpagem, são utilizados o cabo de rede (Cat5e, Cat6), os conectores RJ-45, alicate de crimpagem, decapador de cabos, e tesoura ou cortador de cabos. Esses materiais garantem que os cabos estejam montados de acordo com os padrões de rede, viabilizando conexões de alta qualidade e durabilidade. Após a montagem, o testador de cabos de rede é fundamental para verificar a continuidade e integridade das conexões, identificando possíveis problemas antes do uso.

No contexto de instalações mais complexas, como a configuração de um *Patch Panel*, são necessários materiais específicos, incluindo o próprio *Patch Panel*, rack de rede (para organizar e montar o equipamento), e a ferramenta *Punch Down*, que conecta os cabos ao *Patch Panel* com precisão. Fitas de velcro auxiliam na organização, prendendo os cabos no rack para uma disposição visualmente limpa e eficiente. A parafusadeira ou chave de fenda pode ser útil na fixação de dispositivos no rack, mantendo a estrutura de rede segura e acessível.

O *Switch* HP 1910 é amplamente utilizado em práticas avançadas de configuração de redes. Este *switch* permite configurações detalhadas de controle de tráfego e gerenciamento de acesso, possibilitando testes reais de políticas de QoS (Qualidade de serviços) e ACLs (Listas de controle de acesso). Para acessar a interface de configuração do *switch*, é utilizado um navegador com acesso ao IP e às credenciais do dispositivo, enquanto o PuTTY possibilita a conexão via SSH, necessária para configurações remotas mais avançadas. Por fim, o acesso a terminal ou CMD em computadores é essencial para a realização de testes de conectividade, como comandos de ping, que validam a comunicação entre dispositivos e a eficácia das configurações realizadas.

O conjunto desses materiais é fundamental para criar, configurar e testar redes em ambiente de laboratório. Cada ferramenta e dispositivo foi selecionado para fornecer ao aluno uma experiência prática completa, desde a montagem física e preparação de cabos até o monitoramento, segmentação e controle de tráfego de rede em ambientes simulados.

3.2 METODOLOGIA

Para a elaboração de roteiros práticos voltados ao ensino em um laboratório de redes de comunicação, a metodologia foi dividida em etapas estratégicas. O objetivo foi projetar um ambiente que atendesse às necessidades das disciplinas de redes de computadores.

A primeira etapa consistiu em uma revisão bibliográfica detalhada sobre as práticas e padrões atuais em laboratórios de redes de computadores. Nesta fase, foram analisados laboratórios de redes já estabelecidos em universidades e centros de pesquisa conceituados, com o objetivo de identificar as práticas e equipamentos comumente utilizados.

Em seguida, foi realizado um levantamento detalhado dos equipamentos disponíveis no campus Patos de Minas da UFU. Nesta fase, foi realizada a documentação dos dispositivos e acessórios de rede presentes.

O planejamento da infraestrutura física e lógica do laboratório foi desenvolvido com base na estrutura já existente, aproveitando o espaço físico e a disposição atual dos equipamentos. Foi realizado um estudo do cabeamento disponível, visando otimizar a organização e garantir uma padronização eficiente dentro das limitações estruturais.

Com a infraestrutura e os recursos planejados, foi iniciada a elaboração dos roteiros práticos para ensino. Os roteiros foram desenvolvidos para abarcar práticas como configuração de redes, monitoramento de tráfego e atividades específicas de telecomunicações.

Os roteiros práticos apresentados são fundamentais para a construção de habilidades essenciais em um laboratório de redes, abordando desde a segmentação de rede até a implementação de segurança e controle de tráfego. A configuração de VLANs, por exemplo, é crucial para a criação de redes lógicas dentro de uma infraestrutura física, permitindo um gerenciamento mais eficiente e seguro do tráfego. A segmentação de rede por VLANs não só melhora o desempenho, mas também oferece uma camada extra de segurança, isolando dispositivos e controlando o acesso entre diferentes partes da rede.

A configuração de Wi-Fi com OpenWRT utilizando um *Raspberry Pi* também oferece uma abordagem prática para a criação de redes sem fio seguras e personalizadas, um componente vital para qualquer ambiente de laboratório moderno, permitindo que estudantes e profissionais compreendam o gerenciamento de redes sem fio de forma prática e acessível.

Além disso, a configuração de QoS e ACLs para bloquear portas em horários específicos permite que os alunos explorem o controle de tráfego e a segurança em ambientes de rede mais complexos. Ao implementar essas políticas, é possível entender como diferentes mecanismos de controle de tráfego funcionam em conjunto para otimizar a rede e proteger contra acessos não autorizados.

Esses roteiros são essenciais em um laboratório de redes, pois não apenas ensinam a teoria por trás da configuração e gestão de redes, mas também preparam os alunos para lidar com situações reais que podem ocorrer em redes corporativas e de grande porte, tornando-os mais capacitados para enfrentar desafios do mundo real.

4 DESENVOLVIMENTO

Nesta seção, serão apresentados os equipamentos e estrutura do laboratório, assim como os roteiros práticos elaborados.

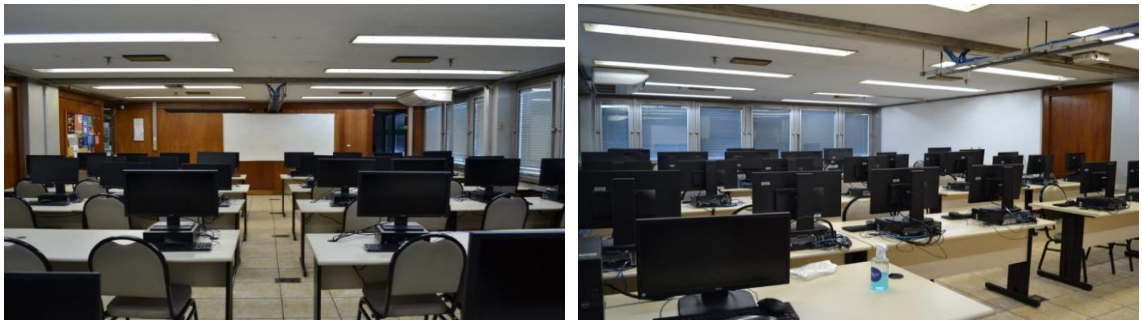
4.1 LABORATÓRIOS DE REDES DE COMUNICAÇÃO EXISTENTES

Nessa seção serão descritos os laboratórios de redes de computadores encontrados, que contenham descrição dos equipamentos utilizados e fotos do ambiente do laboratório.

4.1.1 Laboratório de redes de computadores no SENAI

O laboratório de redes de computadores no SENAI, como observado na Figura 12, tem como objetivo fornecer suporte ao desenvolvimento de atividades teóricas e práticas relacionadas a redes de computadores, sistemas de telecomunicações e áreas afins. Ele utiliza simuladores, *softwares* comerciais e equipamentos reais, como roteadores, suítes e *firewalls* (Senai, [s.d.]).

Figura 12 - Laboratório SENAI - Espaço para aulas com computadores.



Fonte: Senai ([s.d.], on-line)

Os estudantes têm a oportunidade de desenvolver habilidades por meio da infraestrutura e dos equipamentos disponíveis neste ambiente. Eles podem explorar a criação de topologias de redes de diferentes tamanhos, desde pequenas até grandes, realizando montagens, configurações e testes práticos (Senai, [s.d.]).

A estrutura do laboratório inclui as ferramentas e equipamentos necessários para criar e configurar uma rede de computadores, como *hubs*, *switches*, cabos, testadores e computadores. Isso permite que os alunos implementem e realizem testes práticos com base no conteúdo visto em sala de aula (Senai, [s.d.]).

Infraestrutura – recursos e equipamento, como podem ser visualizados na Figura 13:

- Computadores com monitor, mouse e teclado;
- Projetor Multimídia;
- Tela de projeção, branca, retrátil;
- Roteador CISCO 2600;
- *Switch* CISCO 2800, *Switch* CISCO 3560, *Switch* CISCO 2960, *Switch* CISCO 2950;
- *Switch* D-Link;
- Adaptive Security Appliances - ASA 5500;
- Controlador externo de ponto de acesso;
- Controlador de ponto de acesso para roteador CISCO 2800;
- Ponto de Acesso Wireless;
- Rack fechado de 44U, Rack fechado de 42U;
- Kit de ferramentas;
- Multímetro;
- Racks;
- Patch panel e
- Cabos retos, crossover, V.35, rollover, etc.

Figura 13 - Laboratório SENAI – Rack com equipamentos.

Fonte: Senai ([s.d.], on-line)

***Softwares* utilizados no laboratório:**

- Sistema operacional windows;
- Mozilla Firefox;
- Windows Internet Explorer;

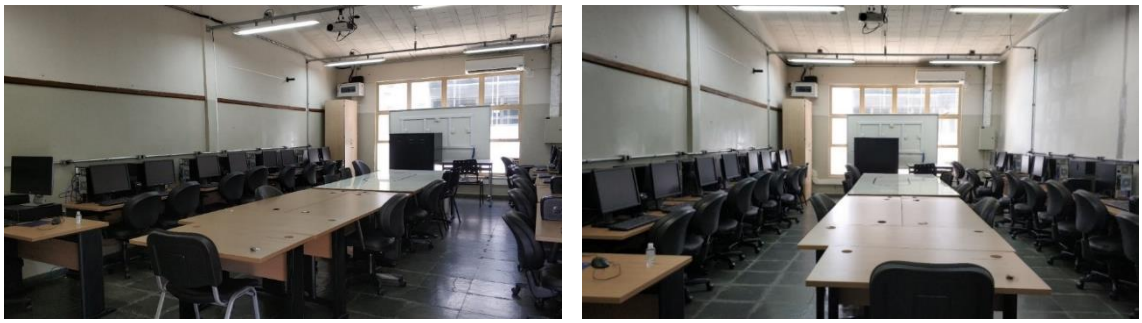
- CutePDF;
- *Wireshark*;
- WinPcap;
- Packet Tracer;
- Pacote Office Básico – Word, Excel e Power Point;
- Microsoft Visio;
- Microsoft Project;
- Acrobat Reader;
- VirtualBox;
- Cisco TFTP *Server* v1.1;
- Gns3;
- X-Lite e
- Quartus II.

4.1.2 Laboratório de Redes de Computadores no IFSULDEMINAS

O Laboratório de Redes de Computadores do IFSULDEMINAS, podendo ser visto na Figura 14, é um ambiente voltado para a realização de atividades práticas essenciais para as disciplinas de redes de computadores e áreas afins nos cursos de Ciência da Computação e Técnico em Informática Integrado ao Ensino Médio. Além de atender às necessidades de ensino, o laboratório apoia projetos de extensão, pesquisa e inovação, proporcionando aos estudantes a oportunidade de projetar, implementar, configurar e testar diferentes cenários de redes (IFSULDEMINAS, [s.d.]).

Assim, o laboratório possibilita a aplicação prática dos conceitos teóricos adquiridos nas disciplinas de redes. As atividades realizadas incluem o desenvolvimento de projetos de redes, configurações, segurança e testes em variados contextos (IFSULDEMINAS, [s.d.]).

Figura 14 - Laboratório IFSULDEMINAS – Espaço para aulas com computadores.



Fonte: IFSULDEMINAS ([s.d.], on-line)

Serviços e ações desenvolvidos:

Configuração de redes cabeadas e sem fio. Sistemas distribuídos. Simulação de redes de computadores. Suporte e apoio às atividades de pesquisa, ensino e extensão.

- Segurança Cibernética;
- Programação de Robótica e
- Redes de Computadores.

Equipamentos, podem ser visualizados nas Figuras 15, 16 e 17:

- Computador;
- Cabeamento;
- Kits utilizados na criação e manutenção de uma rede de computadores;
- Dispositivos utilizados na criação e manutenção de uma rede de computadores;
- Roteador;
- Armário;
- Escaninho alto e
- Kit de robótica.

Figura 15 - Laboratório IFSULDEMINAS – Dispositivos de redes de computadores.

Fonte: IFSULDEMINAS ([s.d.], on-line)

Figura 16 - Laboratório IFSULDEMINAS – Cabos e ferramentas.

Fonte: IFSULDEMINAS ([s.d.], on-line)

Figura 17 - Laboratório IFSULDEMINAS – Kits de robótica.

Fonte: IFSULDEMINAS ([s.d.], on-line)

4.1.3 Laboratórios do curso de redes de computadores da Unoeste

4.1.3.1 Laboratório de criação

O laboratório de redes de computadores da Unoeste, podendo ser visto na Figura 18, foi desenvolvido para oferecer aos alunos a chance de realizar diversas práticas acadêmicas e profissionais, utilizando equipamentos modernos e de alta performance, além de contar com internet de alta velocidade.

O espaço dispõe de oito mesas e quatro bancadas, dois projetores multimídia, telas de projeção, uma lousa branca, mesas para execução de projetos e uma divisória retrátil com isolamento acústico. Essa divisória permite que o ambiente seja configurado como duas salas separadas ou mantido como um único espaço amplo e integrado (Unoeste, [s.d.]).

Figura 18 - Laboratório Unoeste – Espaço para aulas com computador.

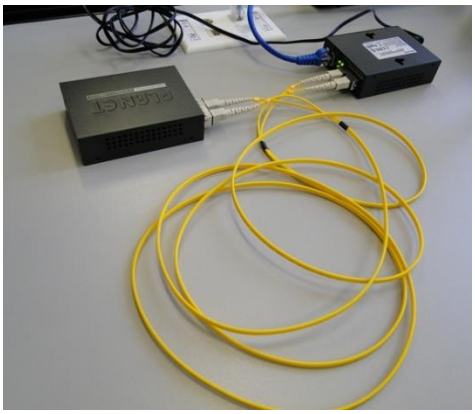
Fonte: Unoeste ([s.d.], on-line)

Os computadores dos Laboratórios de Criação 1 e 2 contam com configurações avançadas, sem gabinetes, e incluem monitores sensíveis ao toque de 23 polegadas em LED, com resolução full HD (1920 x 1080). Equipados com processadores Intel® Core™ i7-4790S de 4ª geração (3.2 GHz expansível até 4 GHz e 8 MB de cache), possuem 8 GB de SDRAM DDR3 a 1600 MHz, disco rígido de 1TB (SATA, 7200 RPM), placa de vídeo AMD Radeon™ R7 A265 de 2GB DDR3, além de um gravador de DVD/CD dual layer. Entre os diversos *softwares* disponíveis estão o Visual Studio 2013, Unity, Premiere Pro e 3D Max (Unoeste, [s.d.]).

4.1.3.2 Laboratório de redes

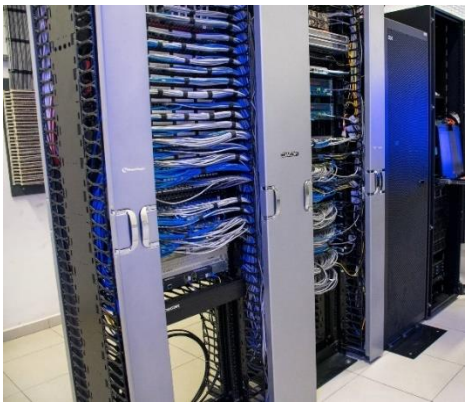
Esse laboratório permite que o aluno configure tanto *softwares* quanto equipamentos para a conexão de redes locais, redes de longa distância e redes sem fio, como podem ser vistos nas Figuras 19, 20,21 e 22. Cada mesa é equipada com quatro pontos de rede, possibilitando ao aluno realizar práticas com até quatro redes diferentes simultaneamente. O laboratório também dispõe de equipamentos variados, como roteadores Cisco, roteadores wireless, access points, *switches* de camadas 2 e 3, *hubs*, *transceivers* GBIC (para fibra óptica), thin clients, conversores de mídia e uma conexão de internet exclusiva. Além disso, um armário de telecomunicações organiza e armazena os equipamentos (Unoeste, [s.d.]).

Figura 19 - Laboratório Unoeste – Conversores de mídia fibra óptica/ethernet.



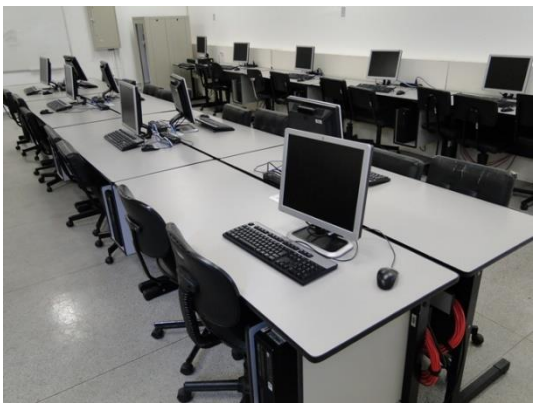
Fonte: Unoeste ([s.d.], on-line)

Figura 20 - Laboratório Unoeste – Data center.



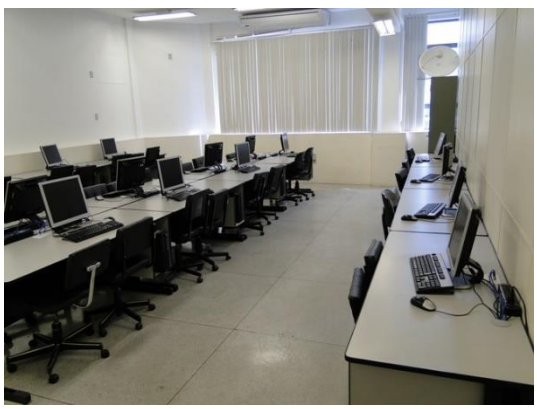
Fonte: Unoeste ([s.d.], on-line)

Figura 21 - Laboratório Unoeste - Vista Geral - Fundos



Fonte: Unoeste ([s.d.], on-line)

Figura 22 - Labortório Unoeste - Vista Geral - Frente



Fonte: Unoeste ([s.d.], on-line)

4.1.3.3 Laboratório de infraestrutura

O laboratório de infraestrutura pode ser visto nas Figuras 23 e 24, oferece aos alunos a oportunidade de implementar, na prática, todo o cabeamento estruturado, conforme as normas e padrões atuais. Os alunos são responsáveis por planejar e realizar a passagem dos cabos pelos dutos disponíveis, instalar conectores, utilizar equipamentos de teste e configuram os dispositivos, como podemos visualizar nas Figuras 25 e 26. No início das atividades, o laboratório não possui nenhuma infraestrutura de rede instalada. Ao concluir as práticas, os alunos deixam o ambiente completamente operacional, inclusive com acesso à Internet (Unoeste, [s.d.]).

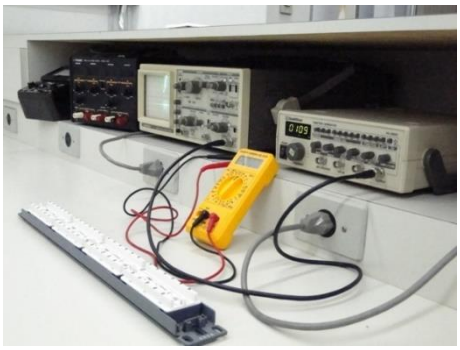
Figura 23 - Laboratório Unoeste – Vista geral.

Fonte: Unoeste ([s.d.], on-line)

Figura 24 - Laboratório Unoeste – Armários de telecomunicações.

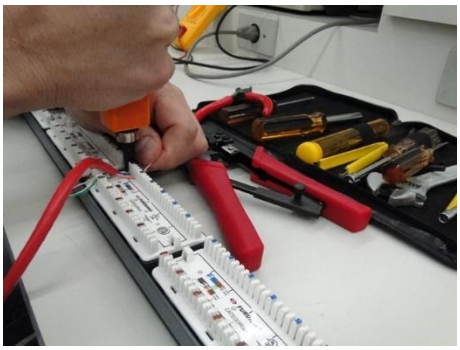
Fonte: Unoeste ([s.d.], on-line)

Figura 25 - Laboratório Unoeste – Equipamentos de eletrônica digital.



Fonte: Unoeste ([s.d.], on-line)

Figura 26 - Laboratório Unoeste – Ferramentas de crimpagem.



Fonte: Unoeste ([s.d.], on-line)

O laboratório conta com dutos para organização dos cabos e armários de telecomunicações onde os equipamentos de rede são instalados. Ele dispõe ainda de patch panels, multímetros, testadores de cabos UTP, certificadores de cabeamento, ferramentas

para conectorização, modems, distribuidores ópticos e materiais de consumo, como cabos e conectores (Unoeste, [s.d.]).

4.2 MAPEAMENTO DO LABORATÓRIO DA UFU

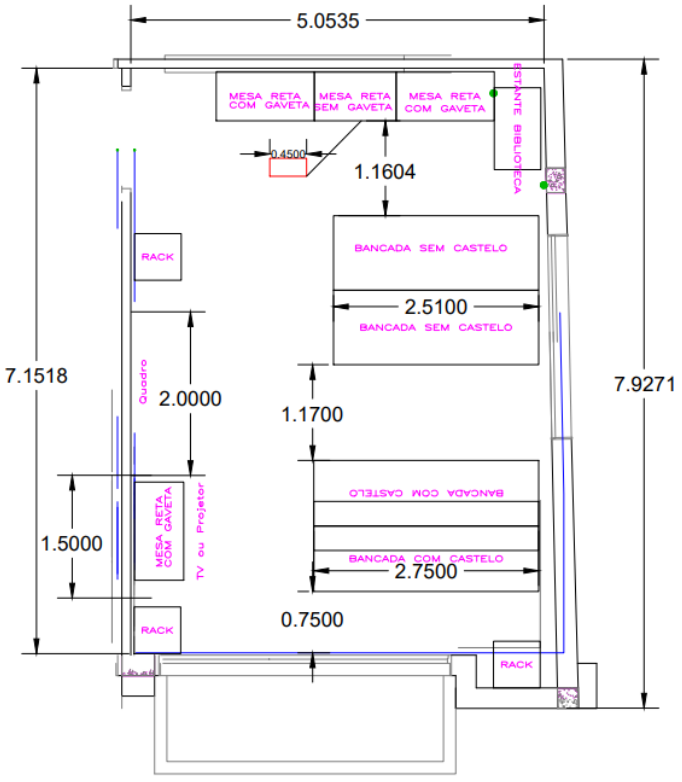
Nesta seção, foi realizado o mapeamento do laboratório de redes de comunicação da UFU Patos de minas, realizado em duas etapas, sendo elas, descrever a estrutura física do laboratório, e os equipamentos disponíveis.

4.2.1 Estrutura do Laboratório

A planta do laboratório visualizada na Figura 27, mostra como é a disposição das mesas, bancadas e racks no laboratório, além de também mostrar aproximadamente as medidas de paredes, bancadas e espaçamento entre as bancadas.

O laboratório conta com uma área de aproximadamente 35 m^2, e tem capacidade para aproximadamente 12 alunos sentados ao redor das bancadas.

Figura 27 - Planta do laboratório de redes de computadores da UFU Patos de minas



Fonte: O autor

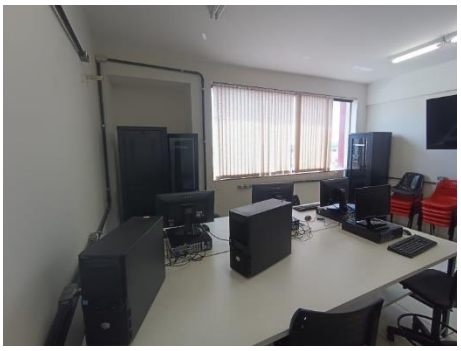
Como pode ser visto nas Figuras 27, 28, 29, 30 e 31, o laboratório conta com uma estrutura suficiente para realizar todos os roteiros práticos, de maneira que seja possível

atender por volta de doze alunos simultaneamente, com equipamentos adequados e possibilita também a expansão de atividades práticas.

Figura 28 - Laboratório UFU - Vista do laboratório ao entrar.

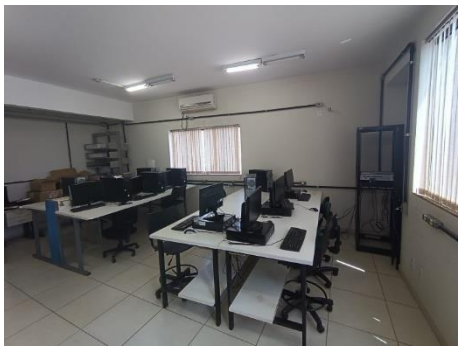
Fonte: O autor

Figura 29 - Laboratório UFU - Vista do lado direito do laboratório.



Fonte: O autor

Figura 30 - Laboratório de redes - Vista das bancadas do laboratório.



Fonte: O autor

Figura 31 - Laboratório de redes - Vista frontal do laboratório.

Fonte: O autor

4.2.2 Equipamentos do Laboratório

Neste capítulo, são apresentados os equipamentos do laboratório de redes de computadores da UFU Patos de minas

4.2.2.1 ALICATE CRIMPADOR RJ11/45

O Alicate Crimpador, visto na Figura 32, é uma ferramenta essencial no processo de conexão de cabos a conectores. Ele é utilizado para crimpar (fixar) terminais nos fios, criando uma conexão segura e eficiente. Este tipo de ferramenta é comumente utilizado em instalações de redes, eletrônica e telecomunicações, sendo fundamental para a criação de cabos de rede, sistemas de áudio e outros componentes eletrônicos.

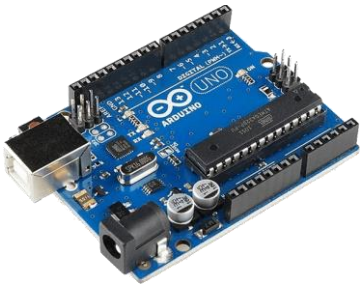
Figura 32 - Alicate crimpador RJ11/45.

Fonte: O autor

4.2.2.2 Arduino Uno

O Arduino Uno mostrado na Figura 33 é uma plataforma de prototipagem eletrônica popular, baseada em um microcontrolador que facilita a criação de projetos de automação, robótica e eletrônica em geral. Seu uso é bastante comum em educação e desenvolvimento de protótipos devido à sua simplicidade e grande comunidade de apoio. O Arduino Uno é utilizado para controlar sensores, motores e dispositivos, sendo amplamente aplicado em áreas como Internet das Coisas (IoT), automação residencial e sistemas embarcados.

Figura 33 - Arduino UNO.



Fonte: PNG Wing (2024, on-line)

4.2.2.3 Cabo de Rede Cat 6

O Cabo de Rede CAT 6, visto na Figura 34, é um tipo de cabo utilizado em redes de comunicação de alta velocidade. Ele oferece uma largura de banda maior que os cabos CAT 5e, sendo ideal para transmissões de dados em alta velocidade e em longas distâncias. Seu uso é predominante em instalações de redes de computadores, onde é necessário garantir uma comunicação rápida e estável, como em ambientes empresariais, centros de dados e sistemas domésticos de rede.

Figura 34 - Cabo de rede CAT6.

Fonte: Equipe 2000 (2024, on-line)

4.2.2.4 PLACA WIFI LORA ESP32

A placa wifi lora esp32 visualizada na Figura 35 é um dispositivo de comunicação sem fio baseado na tecnologia LoRa (*Long Range*). Ele permite a comunicação de dados a longas distâncias com baixo consumo de energia, sendo ideal para aplicações de IoT, como sensores remotos, redes de monitoramento e automação. Este módulo é usado em áreas como agricultura de precisão, monitoramento ambiental, cidades inteligentes e rastreamento de ativos, onde a comunicação a longa distância é necessária sem depender de redes celulares (OLIVEIRA, [s.d.]).

Figura 35 - LoRa 32.

Fonte: O autor

4.2.2.5 Raspberry Pi 3b+

O *Raspberry Pi* 3B+, visto na Figura 36, é um microcomputador que pode ser usado para uma ampla variedade de aplicações. Serve como plataforma para aprendizado de programação, prototipagem de projetos, automação e até mesmo para a criação de servidores pessoais. Sua versatilidade o torna popular em áreas como educação,

desenvolvimento de *software*, automação residencial, media centers, e até em sistemas de monitoramento e controle.

Figura 36 - Raspberry Pi 3 B+.

Fonte: O autor

4.2.2.6 Testador de cabos de rede Tozz

O Testador de Cabo, visto na Figura 37, é um dispositivo utilizado para verificar a continuidade e a qualidade de conexões de cabos de rede. Ele ajuda a garantir que os cabos estejam corretamente conectados e funcionais, identificando problemas como falhas em fios ou conectores. É utilizado por profissionais de redes, eletrônica e telecomunicações, sendo essencial para a instalação e manutenção de redes de dados e sistemas elétricos.

Figura 37 - Testador de cabos de rede Tozz.

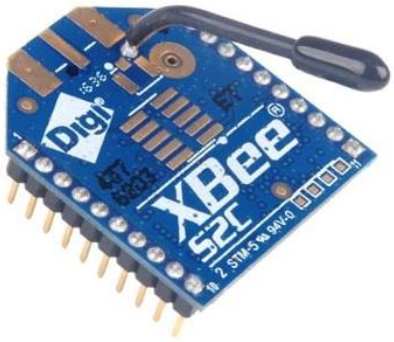
Fonte: Enterlight (2024, on-line)

4.2.2.7 XBee 52C

O XBee 52c, visto na Figura 38 é um módulo de comunicação sem fio que utiliza o padrão Zigbee para transmitir e receber dados em distâncias relativamente curtas. Ele é amplamente utilizado em redes de sensores sem fio, automação residencial e dispositivos

IoT, oferecendo comunicação confiável e de baixo consumo de energia. É particularmente útil em projetos que envolvem controle remoto de dispositivos, monitoramento de dados e redes mesh (Microcontrollers Lab, [s.d.]).

Figura 38 - XBee 52C.

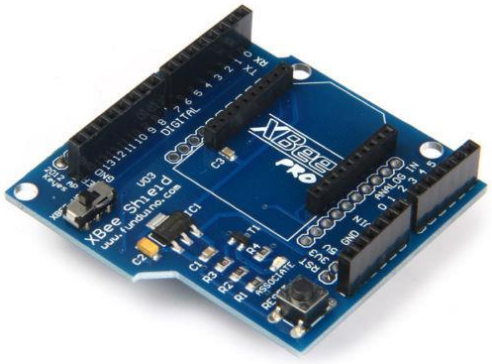


Fonte: Microcontrollers Lab (2024, on-line)

4.2.2.8 XBee PRO SHIELD

O XBee PRO SHIELD, visto na Figura 39, é um módulo de expansão para o Arduino que permite a comunicação sem fio de longo alcance entre dispositivos. Ele é usado principalmente em projetos de redes sem fio, automação e controle remoto de dispositivos. Sua aplicação é muito comum em sistemas de monitoramento remoto, onde é necessário transmitir dados a distâncias maiores do que os módulos XBee padrão, sendo ideal para projetos de longo alcance em áreas como agricultura inteligente, rastreamento e controle de sistemas remotos.

Figura 39 - XBee PRO SHIELD.



Fonte: Techsul Eletrônicos (2024, on-line)

4.2.2.9 Switches

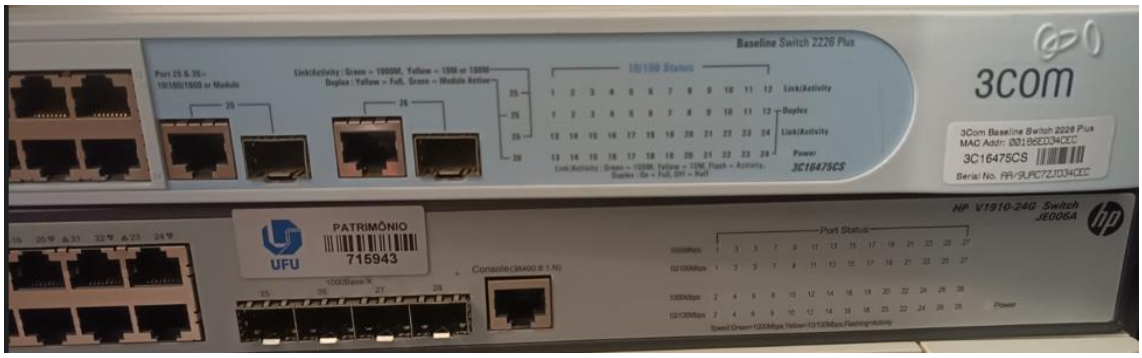
O *Switch* é um dispositivo de rede responsável por conectar múltiplos dispositivos, como computadores, servidores e impressoras, em uma mesma rede local (LAN). Ele

opera na camada de enlace (Camada 2) ou, em alguns casos, na camada de rede (Camada 3) do modelo OSI, permitindo a comunicação eficiente entre dispositivos ao direcionar os dados apenas para o destinatário correto, em vez de transmitir para todos os dispositivos na rede.

Baseline *Switch* 2226 Plus, visto na Figura40, este modelo é conhecido por ser um *switch* gerenciável voltado para pequenas e médias empresas. Ele suporta até 24 portas Ethernet de alta velocidade e duas portas adicionais para *uplinks*. Suas funcionalidades incluem a configuração de VLANs, priorização de tráfego (QoS) e monitoramento básico de rede. É uma escolha acessível para redes que precisam de desempenho estável e recursos básicos de gerenciamento.

Switch HP V1910-24G, visto na Figura40, é gerenciado com 24 portas Gigabit Ethernet. Este modelo suporta recursos avançados, como roteamento estático, suporte a IPv6, agregação de links e controle detalhado de QoS. Sua interface de gerenciamento baseada em web torna a configuração e o monitoramento mais acessíveis, mesmo para administradores com pouca experiência.

Figura 40 - Switches.

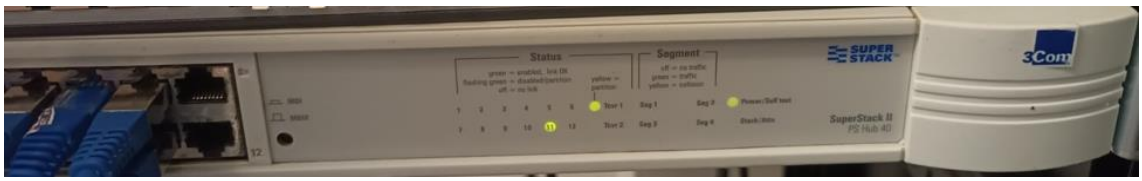


Fonte: O autor

4.2.2.10 Hub SuperStack II-PS Hub 40

Um hub, visualizado na Figura 41, é um dispositivo de rede utilizado para conectar múltiplos dispositivos dentro de uma mesma rede local (LAN). Ele opera na camada física do modelo OSI (Camada 1), funcionando como um ponto central para o tráfego de dados. Quando um dispositivo envia um dado para o hub, este replica o sinal para todas as portas, permitindo que os dispositivos conectados recebam a informação. No entanto, por não possuir inteligência para gerenciar o tráfego, o hub pode levar a colisões de dados em redes mais congestionadas.

Figura 41 - Hub SuperStack.



Fonte: O autor

O SuperStack II-OS Hub 40, da 3Com, é um dispositivo de rede projetado para conectar vários dispositivos em uma rede local (LAN) de maneira simples e eficiente. Operando na camada física do modelo OSI, ele replica os dados recebidos para todas as portas, permitindo a comunicação entre dispositivos conectados. Ideal para redes pequenas e ambientes com baixa complexidade, o hub oferece múltiplas portas Ethernet e capacidade de empilhamento, permitindo expandir a conectividade conforme necessário. Com LEDs indicadores para monitoramento básico e configuração plug-and-play, o SuperStack II-OS Hub 40 atende bem a redes básicas, embora não possua funcionalidades avançadas, como gerenciamento de tráfego ou segmentação de rede.

4.2.2.11 Patch Panel (24P CAT6 UTP)

O Patch Panel, visto nas Figuras 42 e 43, é um componente essencial em infraestruturas de rede estruturada, projetado para organizar e facilitar a conexão de cabos de comunicação. Este modelo específico conta com 24 portas compatíveis com cabos CAT6 UTP (Unshielded Twisted Pair), que oferecem alto desempenho em termos de transmissão de dados, suportando velocidades de até 10 Gbps em distâncias de até 55 metros.

O Patch Panel serve como um ponto central para a terminação de cabos que vêm de diferentes áreas da rede, permitindo que conexões sejam realizadas de forma prática, ordenada e flexível. Ele também facilita a manutenção e a expansão da rede, pois os cabos podem ser facilmente conectados, desconectados ou reconfigurados, minimizando o impacto no sistema geral. Ideal para ambientes empresariais, o Patch Panel é uma solução que garante eficiência e organização em redes de alta performance.

Figura 42 - Patch Panel 24P CAT6 UTP – Frontal.

Fonte: O autor

Figura 43 - Patch Panel 24P CAT6 UTP – Traseira.

Fonte: O autor

4.3 PREPARAÇÃO DOS ROTEIROS PRÁTICOS

Este capítulo tem como finalidade apresentar uma série de roteiros práticos que auxiliam o aluno no desenvolvimento de competências essenciais para atuar com redes de computadores, dispositivos embarcados e a configuração de infraestrutura de TI. Através da execução de cada roteiro, o estudante será capaz de realizar atividades práticas, como configurar sistemas operacionais em dispositivos como o Raspberry Pi, monitorar o tráfego de rede, instalar hardware de rede e configurar VLANs, além de outras tarefas fundamentais para a gestão eficiente e segura de redes.

Cada um desses roteiros foi cuidadosamente planejado para proporcionar não apenas uma base teórica robusta, mas também para possibilitar a aplicação dos conceitos em situações práticas, promovendo uma experiência significativa e realista. O aprendizado dessas atividades é de extrema importância, pois serve como base para a atuação em ambientes profissionais, nos quais o domínio das técnicas de configuração, diagnóstico e otimização de redes é crucial.

4.3.1 Roteiro Prático 1 – Preparação do Dispositivo e Gravação do Sistema Operacional

A preparação de dispositivos como o *Raspberry Pi* e a gravação de um sistema operacional são passos fundamentais para a utilização do hardware em projetos de redes e computação. Este roteiro prático destaca a importância de seguir procedimentos corretos para garantir que o *Raspberry Pi* esteja configurado de forma eficaz e segura. O *Raspberry Pi Imager* é a ferramenta ideal para este processo, facilitando a gravação do sistema operacional escolhido em um cartão SD. O aprendizado dessas etapas é essencial por vários motivos. Primeiramente, o *Raspberry Pi* é um dispositivo versátil amplamente utilizado em projetos de redes, como servidores DNS, monitoramento de tráfego, *firewalls* e até experimentos em redes distribuídas. Dominar a instalação do sistema operacional permite configurar o dispositivo para diferentes aplicações com eficiência.

A escolha do sistema operacional é igualmente crítica, pois cada opção, como Raspbian, Ubuntu MATE, OSMC e outros, atende a diferentes objetivos, desde

aplicações educacionais até multimídia ou servidores. Além disso, a capacidade do cartão SD influencia diretamente o desempenho do dispositivo, já que espaço insuficiente pode limitar as atualizações e o uso de recursos mais avançados. Outro ponto de destaque é a atualização do sistema operacional e seus pacotes. Manter o sistema atualizado não só melhora o desempenho como também garante maior segurança e compatibilidade com novos *softwares*. Isso é crucial para evitar vulnerabilidades em projetos voltados à segurança de redes. Por fim, aprender a configurar adequadamente o *Raspberry Pi* prepara o usuário para utilizar este microcomputador em ambientes reais, onde ele pode desempenhar um papel fundamental na infraestrutura de redes ou em soluções inovadoras de TI.

4.3.2 Roteiro Prático 2 – Monitoramento de Rede através do Wireshark utilizando Raspberry Pi

O monitoramento de redes é uma habilidade essencial em qualquer ambiente de TI, pois permite detectar e resolver problemas de conectividade, garantir a segurança da infraestrutura e otimizar o desempenho das comunicações. Neste roteiro prático, utilizaremos o *Wireshark*, uma das ferramentas mais poderosas e amplamente utilizadas para análise de tráfego de rede. Através do *Wireshark*, é possível capturar, visualizar e analisar pacotes de dados transmitidos em uma rede, possibilitando uma compreensão detalhada do funcionamento dos protocolos e a detecção de falhas ou comportamentos anômalos.

A instalação e a configuração do *Wireshark* em um *Raspberry Pi*, como abordado neste roteiro, são etapas cruciais para o aprendizado de redes e segurança. A configuração de permissões adequadas, por exemplo, permite que o usuário acesse as interfaces de rede e realize a captura de pacotes de maneira eficiente. Além disso, a utilização de ferramentas como o *Packet Sender* possibilita a criação de pacotes de rede para que possam ser monitorados e analisados em tempo real. Essa prática não só reforça o entendimento sobre o tráfego de rede, mas também permite identificar problemas específicos, como latência, perda de pacotes e tráfego suspeito.

Aprender a realizar o monitoramento de rede com o *Wireshark* tem diversas implicações práticas. O *Wireshark* é utilizado por profissionais de redes, administradores de sistemas e especialistas em segurança para solucionar problemas de conectividade, melhorar a performance de rede e identificar vulnerabilidades. A análise de pacotes é fundamental para entender o comportamento de protocolos como TCP, UDP, DNS, entre outros, e a ferramenta também pode ser utilizada para investigar falhas, ataques ou

problemas de desempenho. Para profissionais de segurança, é um recurso crucial para detectar atividades maliciosas, como tentativas de intrusão ou tráfego não autorizado.

Além disso, o aprendizado deste roteiro prático também prepara o usuário para realizar diagnósticos em redes reais e pode ser uma competência essencial para quem busca trabalhar em ambientes corporativos, acadêmicos ou de pesquisa em redes e segurança. Assim, o domínio do *Wireshark* não só expande as habilidades do profissional, mas também oferece uma compreensão profunda dos protocolos e da infraestrutura de redes.

4.3.3 Roteiro Prático 3 – Crimpar Cabo de Rede

A crimpagem de cabos de rede é uma habilidade essencial para profissionais que trabalham com redes de computadores. A capacidade de criar cabos de rede de alta qualidade, com conexões seguras e eficientes, é fundamental para garantir a estabilidade e a velocidade das redes. Este roteiro prático tem como objetivo guiar o aluno pelo processo de crimpagem, utilizando ferramentas específicas, como conectores RJ-45 e alicate de crimpagem, e garantir que o cabo resultante seja funcional e confiável para uso em ambientes de rede.

Dominar a crimpagem de cabos de rede é importante por diversas razões. Primeiro, em ambientes de redes, a qualidade da conexão depende de cabos bem montados. Um cabo mal crimpado pode resultar em falhas de comunicação, perda de pacotes ou desconexões frequentes, prejudicando a performance da rede. Além disso, a escolha correta do padrão de pinagem (T568A ou T568B) é essencial para garantir a compatibilidade com outros dispositivos e para que o cabo possa ser utilizado sem problemas em *switches*, roteadores, computadores e outros equipamentos.

O aprendizado desse processo proporciona uma base sólida para quem deseja trabalhar com montagem, manutenção e otimização de redes. Outro aspecto fundamental abordado neste roteiro é a utilização de ferramentas adequadas, como o alicate de crimpagem e o testador de cabos.

O uso correto dessas ferramentas é crucial para assegurar que a conexão entre os fios do cabo e os pinos do conector RJ-45 seja firme e eficiente. O testador de cabos, por exemplo, é um dispositivo essencial para garantir que as crimpagens foram feitas corretamente, permitindo detectar problemas como fios trocados, curtos-circuitos ou conexões mal feitas.

Ao concluir este roteiro, o aluno estará capacitado para criar cabos de rede personalizados, atendendo às necessidades de sua rede local, e será capaz de realizar testes

para garantir que os cabos estejam funcionando corretamente. Além disso, o aprendizado prático de crimpagem prepara o usuário para diagnosticar problemas de rede relacionados à conectividade, o que é uma habilidade valiosa tanto em ambientes corporativos quanto domésticos.

Portanto, aprender a crimpar cabos de rede não apenas proporciona uma competência técnica essencial para quem deseja trabalhar com infraestrutura de redes, mas também reforça a importância de realizar um trabalho cuidadoso e preciso. A crimpagem adequada é uma etapa crítica para garantir a estabilidade e a qualidade das conexões em redes de computadores, influenciando diretamente a performance e a segurança de toda a infraestrutura de TI.

4.3.4 Roteiro Prático 4 – Instalando um Patch Panel

A instalação de um Patch Panel é uma prática essencial para a organização e eficiência de redes de computadores, especialmente em ambientes corporativos e data centers. Este dispositivo permite a conexão centralizada de múltiplos cabos de rede, simplificando a gestão e manutenção das conexões. Ao invés de ligar cabos diretamente a *switches* ou *hubs*, o Patch Panel proporciona uma estrutura organizada para realizar essas conexões na parte traseira, facilitando o gerenciamento do cabeamento.

O aprendizado dessa prática é importante por vários motivos. Primeiramente, o uso de Patch Panels traz uma série de vantagens, como a escalabilidade da rede. À medida que novos dispositivos são adicionados, o Patch Panel facilita a expansão, sem a necessidade de realizar modificações complexas na infraestrutura existente. Além disso, o dispositivo contribui para a redução de desordem em racks, mantendo os cabos organizados e permitindo que o trabalho dos administradores de rede seja mais eficiente. Isso também resulta na diminuição dos custos de instalação e manutenção, uma vez que problemas podem ser localizados e corrigidos com mais facilidade, sem a necessidade de rastrear manualmente cada cabo.

Outro ponto importante é a versatilidade do Patch Panel, que além de ser utilizado para redes Ethernet, pode também ser adaptado para redes de fibra óptica. Isso amplia suas possibilidades de uso, atendendo a diferentes demandas de conectividade. Durante o processo de instalação, o aluno aprenderá a utilizar ferramentas específicas, como o alicate *Punch Down*, que são essenciais para garantir uma crimpagem precisa e a conformidade com os padrões de pinagem (T568A ou T568B), assegurando que as conexões sejam realizadas corretamente.

A prática também aborda a utilização de testadores de cabos, que são fundamentais para verificar se todas as conexões foram feitas de maneira adequada e se não há falhas nas crimpagens. O uso do testador permite verificar a continuidade dos fios e a integridade das conexões, garantindo que o Patch Panel esteja funcionando corretamente.

Ao concluir o aprendizado sobre a instalação do Patch Panel, o aluno será capaz de realizar uma instalação eficiente, organizando e gerenciando as conexões de rede com precisão. Esse conhecimento é essencial não apenas para quem trabalha com redes, mas também para quem busca otimizar e melhorar a infraestrutura de TI, proporcionando uma base sólida para a gestão de redes em ambientes corporativos, datacenters e redes domésticas.

Portanto, aprender a instalar e configurar um Patch Panel é fundamental para profissionais de redes, pois a correta organização e manutenção da infraestrutura de cabeamento são cruciais para o desempenho, a escalabilidade e a facilidade de manutenção de redes de computadores.

4.3.5 Roteiro Prático 5 – Criação e configuração de VLANs

A criação e configuração de VLANs é uma habilidade essencial para profissionais de redes, uma vez que permite segmentar o tráfego de rede de forma lógica, sem a necessidade de alterar a infraestrutura física. Este roteiro prático destaca como configurar VLANs em um *switch* HP 1910, atribuir portas, configurar trunking e testar a conectividade entre diferentes VLANs, promovendo uma rede mais eficiente, segura e de fácil gerenciamento.

O aprendizado sobre VLANs é crucial, pois elas oferecem maior controle sobre o tráfego de rede, separando diferentes tipos de dados em canais lógicos isolados. Isso não apenas melhora o desempenho, ao reduzir o tráfego desnecessário, mas também aumenta a segurança, limitando o acesso a informações sensíveis dentro de uma rede corporativa. Além disso, a criação de VLANs facilita o gerenciamento de redes complexas, onde diferentes departamentos ou grupos de usuários necessitam de níveis distintos de acesso e prioridade.

A prática de configurar VLANs também envolve o aprendizado de técnicas como trunking, onde múltiplas VLANs podem compartilhar o mesmo link físico entre *switches*. Essa configuração é fundamental para garantir que a comunicação entre VLANs diferentes ocorra de maneira fluida, sem comprometer a eficiência da rede. Assim, ao dominar esse procedimento, o profissional não apenas aprimora sua capacidade de

administrar redes locais, mas também ganha experiência prática com conceitos fundamentais de redes como VLAN ID, trunks e interfaces de rede.

Além disso, o conhecimento de como configurar corretamente as portas do *switch* e verificar a conectividade entre dispositivos em VLANs distintas, através de comandos como o "ping", é indispensável para assegurar que a implementação das VLANs seja bem-sucedida. Com essas habilidades, o usuário estará capacitado a realizar segmentações eficazes de rede, essenciais para ambientes de rede corporativa, data centers e redes distribuídas, otimizando tanto o desempenho quanto a segurança do tráfego de dados.

Esse roteiro prático proporciona um aprendizado que tem grande aplicabilidade em ambientes de rede profissional, sendo fundamental para quem deseja seguir carreira em redes, segurança de TI ou gerenciamento de infraestrutura de rede, já que a segmentação de rede é uma prática amplamente adotada em diversas soluções de rede modernas.

4.3.6 Roteiro Prático 6: Configuração de Wi-Fi Utilizando Raspberry Pi como roteador

A configuração de um *Raspberry Pi* como roteador Wi-Fi utilizando o sistema operacional *OpenWrt* é uma prática valiosa, especialmente para quem deseja aprender sobre redes e configurar soluções de conectividade em dispositivos de baixo custo e alta flexibilidade. O *OpenWrt* é um sistema operacional baseado em Linux que permite configurar e personalizar roteadores e dispositivos embarcados, como o *Raspberry Pi*, de maneira avançada. Ao usar o *OpenWrt*, o *Raspberry Pi* pode ser transformado em um roteador Wi-Fi com capacidades de controle de tráfego, gerenciamento de segurança e definição de redes virtuais (VLANs), entre outras funções. Este roteiro prático guia o usuário pelo processo de instalação e configuração do *OpenWrt*, desde a gravação do sistema operacional até a criação de uma rede sem fio funcional.

O aprendizado dessas etapas é essencial por várias razões. Primeiramente, a habilidade de configurar um roteador personalizado com *OpenWrt* oferece uma compreensão profunda de como os dispositivos de rede operam e como otimizar suas funcionalidades para atender a diferentes necessidades, como conectividade de baixo custo em ambientes domésticos ou projetos experimentais de redes. Além disso, o *Raspberry Pi*, como roteador, pode ser utilizado em várias aplicações práticas, como melhorar a cobertura de Wi-Fi em locais específicos, fornecer segurança adicional em redes domésticas ou até mesmo criar soluções de rede em ambientes corporativos com orçamento limitado.

A personalização do *OpenWrt* permite que o usuário configure sua rede de acordo com suas necessidades, incluindo criptografia Wi-Fi avançada (como WPA2-PSK), controle de interfaces de rede e gerenciamento de *firewall*. O conhecimento de como configurar as interfaces, o *firewall* e a segurança da rede Wi-Fi são cruciais para a criação de redes seguras e eficientes. Além disso, entender como o OpenWrt interage com o hardware do *Raspberry Pi*, e como ele pode ser integrado com outros dispositivos, amplia a capacidade do usuário de gerenciar e configurar redes em cenários reais. Ao finalizar este roteiro, o aluno não só será capaz de configurar um *Raspberry Pi* como um roteador Wi-Fi funcional, mas também terá uma compreensão sólida das melhores práticas de segurança e gerenciamento de redes, ferramentas essenciais no campo da administração de redes e infraestrutura de TI.

4.3.7 Roteiro Prático 7: Bloquear as Portas de Rede de um *Switch* em um Período Desejado

A configuração de controles de tráfego e segurança em redes é essencial para garantir um gerenciamento eficiente dos recursos, principalmente em ambientes corporativos onde a otimização e a proteção dos sistemas são prioridades. Neste roteiro prático, vamos aprender a configurar a funcionalidade de bloqueio de portas de um *Switch* HP V1910 em horários específicos, utilizando uma combinação de recursos como ACLs (Listas de Controle de Acesso), QoS (Qualidade de Serviço) e *Time Range*. A implementação dessas configurações permite um controle preciso sobre o tráfego de dados nas portas do *switch*, aumentando a segurança e evitando acessos não autorizados durante períodos determinados.

A aprendizagem dessas etapas é de extrema importância, principalmente em redes que demandam um controle rigoroso de acesso e proteção de dados. A função *Time Range*, por exemplo, permite configurar períodos de tempo em que determinadas portas serão desativadas, sendo uma ferramenta muito útil em situações onde se deseja garantir que o acesso à rede seja restrito a horários específicos.

O uso de ACLs e Classifiers, que permitem a filtragem do tráfego de rede de acordo com endereços IP ou outras características, contribui diretamente para a segurança, bloqueando tentativas de acesso indesejadas. Ao associar essas configurações a uma política de QoS e aplicar restrições de tráfego em portas específicas, garantimos não apenas o controle do acesso, mas também a integridade da rede.

A habilidade de configurar ACLs e policies, e aplicar essas regras em horários específicos, prepara o usuário para um cenário de gestão avançada de redes, onde as

políticas de segurança devem ser dinâmicas e adaptáveis. Em ambientes de TI corporativos, essa capacidade de configurar de forma precisa o controle do tráfego de rede contribui significativamente para evitar sobrecarga de tráfego indesejado e para otimizar os recursos de rede, protegendo a infraestrutura de ameaças externas.

A implementação dessa configuração também fortalece o controle de acesso a recursos críticos, prevenindo acessos não autorizados ou desnecessários. Assim, aprender a aplicar estas configurações é uma habilidade essencial para quem deseja gerenciar redes de forma eficaz e segura.

5 ROTEIROS PRÁTICOS

Este capítulo foi desenvolvido para apresentar os roteiros práticos realizados ao longo do estudo sobre configuração e gerenciamento de redes. Os roteiros abordam uma série de atividades essenciais para a administração eficiente de redes, incluindo a criação e configuração de VLANs, o uso do Raspberry Pi como roteador sem fio, e a implementação de políticas de controle de tráfego e segurança em *switches*.

Cada prática foi elaborada com o objetivo de aplicar conceitos teóricos em situações reais, permitindo aos participantes uma compreensão mais profunda dos processos envolvidos na criação, segmentação e gerenciamento de redes. As atividades envolvem a configuração de dispositivos como *switches* HP 1910 e a instalação de sistemas como OpenWrt em placas Raspberry Pi, visando não apenas otimizar o desempenho da rede, mas também garantir sua segurança e integridade.

Ao longo deste capítulo, será possível entender como diferentes ferramentas e protocolos, como VLANs, ACLs, QoS e outras políticas de segurança, podem ser configurados de maneira eficaz para controlar o tráfego de dados e o acesso à rede. A experiência prática adquirida através dessas atividades é fundamental para a formação de profissionais capazes de gerenciar redes de maneira eficiente e segura.

5.1 ROTEIRO PRÁTICO 1 – PREPARAÇÃO DO DISPOSITIVO E GRAVAÇÃO DO SISTEMA OPERACIONAL

O Roteiro Prático 1 aborda a configuração inicial do Raspberry Pi 3, com foco na gravação do sistema operacional e na preparação do dispositivo para projetos de redes de computadores. A prática é dividida em etapas detalhadas, incluindo a escolha e instalação do sistema operacional adequado (como Raspberry Pi OS, Ubuntu MATE, entre outros), além da atualização do sistema. Essa prática é essencial para garantir que o dispositivo funcione corretamente e esteja preparado para aplicações como servidores e monitoramento de rede.

5.1.1 Introdução

Nesta prática, você será guiado no processo de configuração de um *Raspberry Pi* 3, desde a instalação do sistema operacional até a atualização de *software*, com ênfase em redes de computadores. O propósito é ensinar como gravar o *Raspberry Pi* OS em um cartão SD e ajustar o hardware para assegurar o bom funcionamento do dispositivo.

O *Raspberry Pi* pode ser amplamente utilizado em redes para funções como servidor DNS, *firewall*, monitoramento de tráfego, servidor web e em experimentos com redes distribuídas. Essas aplicações fazem do *Raspberry Pi* uma ferramenta valiosa tanto para aprendizado quanto para a implementação de projetos práticos.

Seguir corretamente as etapas de instalação e manter o sistema e os pacotes sempre atualizados é crucial para garantir segurança, desempenho e compatibilidade, especialmente em projetos voltados para monitoramento e segurança de redes.

5.1.2 Sistemas Operacionais

Existem diversas opções de sistemas operacionais compatíveis com o *Raspberry Pi*, ideais para diferentes usos:

Raspbian: iniciantes no *Raspberry Pi*

O *Raspbian* é uma versão adaptada do Debian, uma popular distribuição Linux, projetada para rodar no *Raspberry Pi*. Ele é considerado o sistema operacional padrão do microcomputador. Completo, oferece *software* de escritório, navegação na Internet e ferramentas de configuração e desenvolvimento, sendo uma ótima escolha para quem está se familiarizando com o *Raspberry Pi*.

Ubuntu MATE: Ideal para "transformar" o *Raspberry Pi* em um PC

O Ubuntu é a distribuição Linux mais famosa e existe em várias versões compatíveis com o *Raspberry Pi*. A versão MATE, mais leve, roda bem no *Raspberry Pi* 2 e 3, oferecendo ferramentas como o LibreOffice e acesso a diversos aplicativos através dos repositórios da Canonical. Essa versão é ideal para quem quer utilizar o *Raspberry Pi* como um desktop tradicional.

OSMC: Transformar o *Raspberry Pi* em um media center

Diferente das opções mais generalistas, o OSMC é especializado em transformar o *Raspberry Pi* em um completo media center. Ele oferece acesso a canais de streaming via Internet e permite a reprodução de áudio e vídeo de alta qualidade, funcionando como uma Apple TV caseira.

Recalbox: Usar o *Raspberry Pi* como uma central de jogos

Recalbox é uma das opções mais fáceis para quem deseja transformar o *Raspberry Pi* em uma central de emulação de videogames antigos. Com suporte a uma ampla gama

de consoles clássicos, como Atari, Super Nintendo e Playstation, ele oferece uma interface amigável e menos complexa que o RetroPie, outra plataforma similar.

Pidora: para quem busca uma alternativa ao Ubuntu MATE

O Pidora é uma versão do Fedora adaptada para o *Raspberry Pi*, com acesso a aplicativos da Red Hat, como navegador e suíte de escritório. Um recurso interessante do Pidora é o modo Headless, que permite configurar e controlar o *Raspberry Pi* via rede, sem a necessidade de um monitor, facilitando o uso do dispositivo em projetos remotos.

5.1.3 Etapas para instalação do Rasbian

Siga corretamente os passos, para instalar de maneira correta o Rasbian.

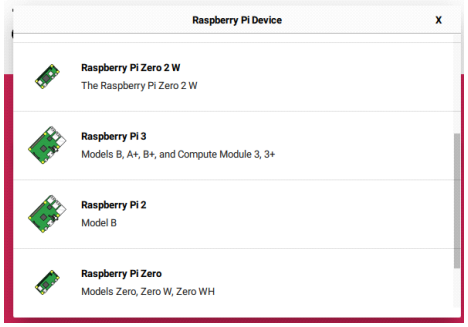
1. Acesse o site oficial da *Raspberry Pi* para baixar o *Raspberry Pi* Imager, podendo ser visualizado na Figura 44, através do link: https://www.raspberrypi.com/software/.

Figura 44 - Tela inicial Raspberry Pi Imager.

Fonte: O autor

2. Escolha o dispositivo que será utilizado, neste caso o Raspiberry Pi 3, como pode-se ver na Figura 45.

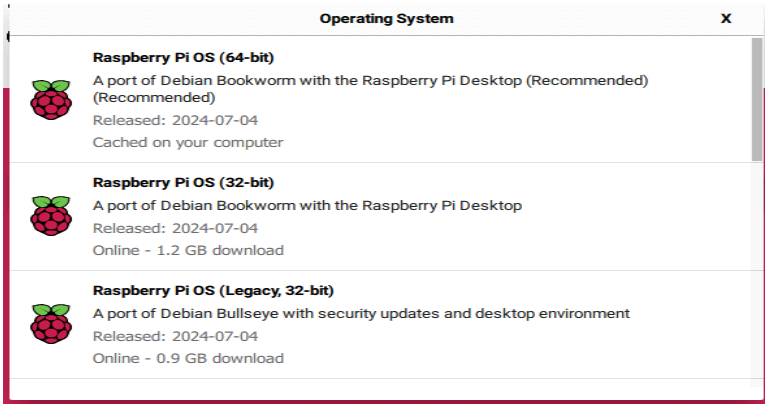
Figura 45 - Escolha do dispositivo no raspberry pi imager.



Fonte: O autor

3. Escolha o sistema operacional desejado, neste caso foi utilizado o Raspberry Pi OS (64-bit) como é mostrado na Figura 46.

Figura 46 - Escolhendo o sistema operacional no raspberry pi imager.



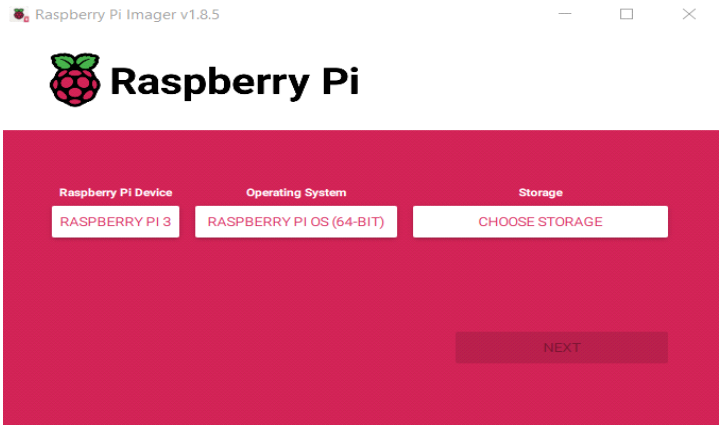
Fonte: O autor

4. Selecione o cartão SD correto para armazenar o sistema operacional, como visto na Figura 47. Certifique-se de que o cartão tenha espaço suficiente (mínimo de 8GB).

Figura 47 - Escolha do dispositivo de armazenamento no raspberry pi imager.

Fonte: O autor

Figura 48 - Raspberry Pi Imager.



Fonte: O autor

5. Após a gravação, insira o cartão SD na *Raspberry Pi*.

6. Conecte o hardware necessário (fonte de alimentação, monitor, teclado, mouse) e ligue a *Raspberry Pi.*

5.1.4 Etapas para atualização do sistema operacional

Siga corretamente os passos, para atualizar o sistema operacional e garantir a funcionalidade do dispositivo.

1. Abra o terminal na *Raspberry Pi.*

2. Execute o comando para atualizar a lista de pacotes:

sudo apt update

3. Em seguida, execute o comando para atualizar todos os pacotes existentes:

sudo apt upgrade

4. Se solicitado para continuar, digite "Y" e pressione **Enter** para confirmar a atualização.

5.2 ROTEIRO PRÁTICO 2 – MONITORAMENTO DE REDE ATRAVÉS DO WIRESHARK UTILIZANDO RASPBERRY PI

O Roteiro Prático 2 explora o uso do *Wireshark* no monitoramento de redes utilizando um *Raspberry Pi.* O *Wireshark* é uma ferramenta poderosa para análise de tráfego de rede, permitindo capturar, visualizar e investigar pacotes para identificar padrões, falhas e anomalias. A prática abrange a instalação e configuração do *Wireshark*, o envio de pacotes com o *Packet Sender*, e a análise desses pacotes para compreender os protocolos e comportamentos de rede.

5.2.1 Introdução

Nesta aula prática de monitoramento de rede, utilizaremos o *Wireshark*, uma das ferramentas mais poderosas e amplamente utilizadas para análise de tráfego de rede. Desenvolvido inicialmente em 1998 por Gerald Combs e mantido por uma comunidade global de especialistas, o *Wireshark* continua a ser atualizado para suportar novas tecnologias e protocolos de criptografia. Sua utilização é fundamental em diversos cenários, como solução de problemas de rede, segurança e ensino.

O *Wireshark* permite capturar, visualizar e analisar pacotes de dados que trafegam em uma rede, possibilitando a identificação de padrões de comunicação, detecção de falhas ou anomalias, e monitoramento de protocolos específicos, como TCP e DNS. A ferramenta é segura e utilizada por governos, empresas e instituições de ensino, sendo uma excelente plataforma para o aprendizado prático de redes.

É importante destacar a questão legal: o uso do *Wireshark* deve ser restrito a redes onde você tenha autorização para inspecionar o tráfego. Durante esta prática, vamos explorar como instalar e configurar o *Wireshark* em um *Raspberry Pi*, além de aprender a capturar e filtrar pacotes, permitindo uma análise detalhada do tráfego de rede local. Isso proporcionará uma compreensão mais profunda dos protocolos e da estrutura das redes de comunicação.

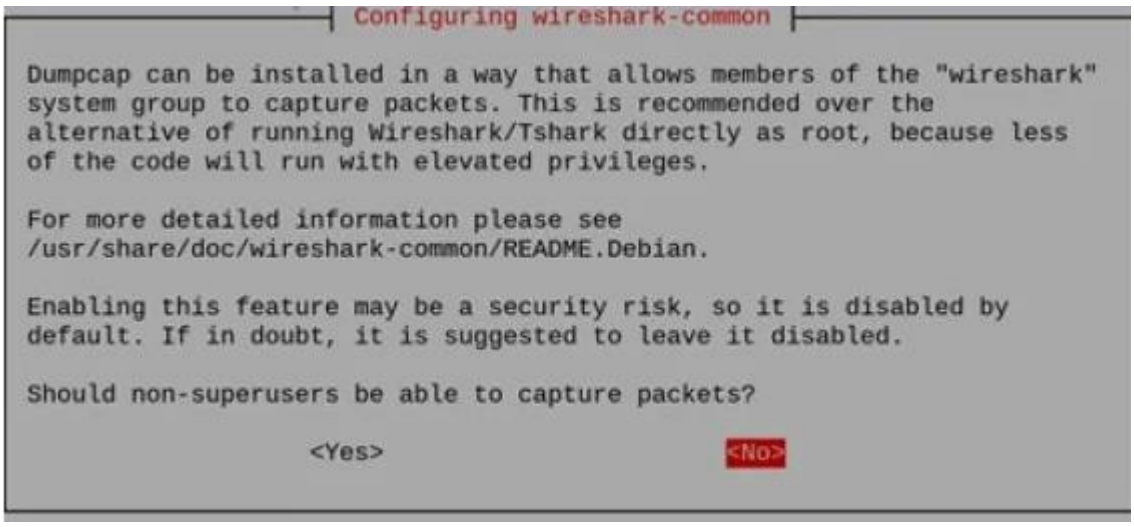
5.2.2 Etapas para a instalação do wireshark

1. No terminal, execute o seguinte comando para instalar o *Wireshark*:

sudo apt install wireshark

2. Durante a instalação, você será perguntado se deseja que o *Wireshark* seja acessível por usuários não root, como podemos visualizar na Figura 49. Use as setas para selecionar "<Yes>" e pressione Enter.

Figura 49 - Instalação do Wireshark.



Fonte: Unboxing Tomorrow (2024, on-line)

5.2.3 Etapas para configuração do wireshark

1. Adicione seu usuário ao grupo "*wireshark*" para que ele tenha acesso às interfaces de rede. Substitua "pi" pelo seu nome de usuário:

   sudo usermod -a -G wireshark pi

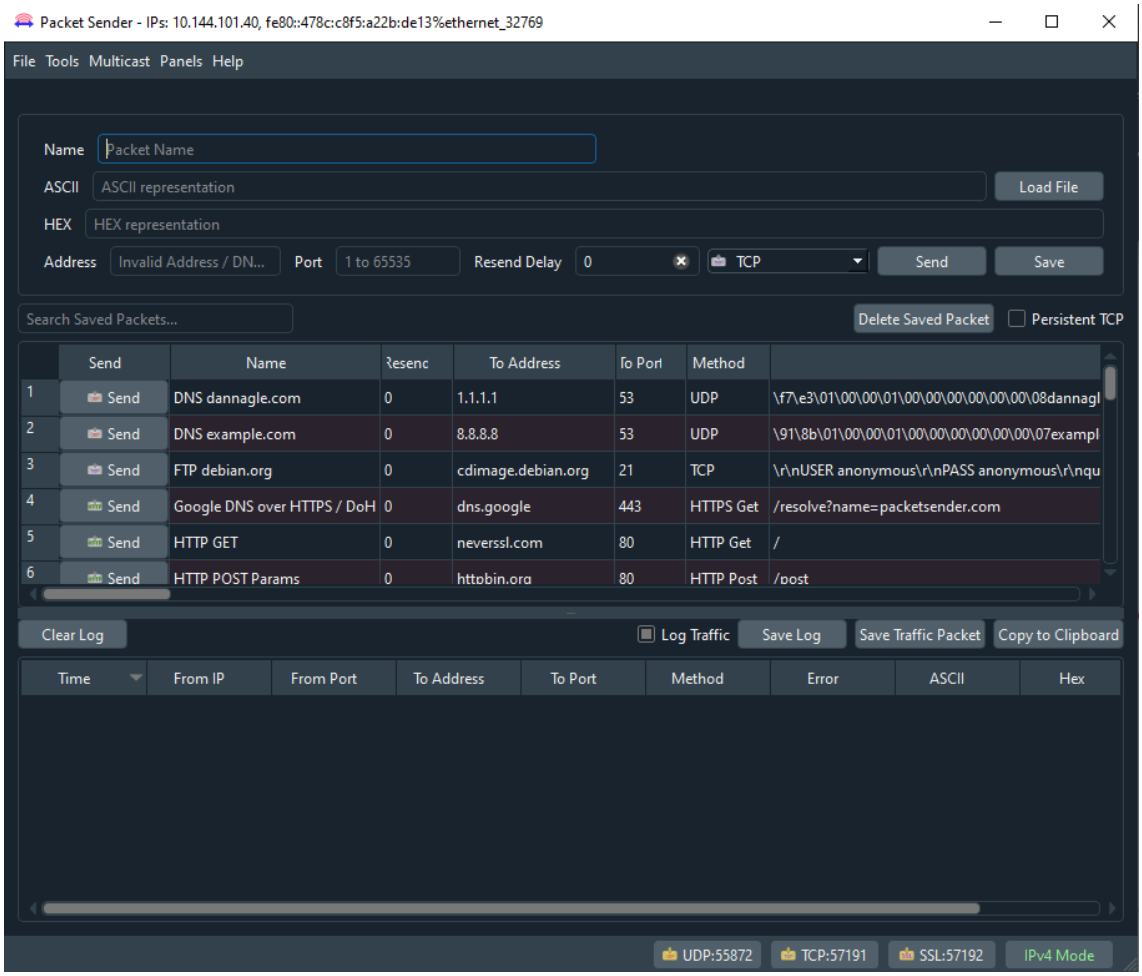
2. Reinicie a *Raspberry Pi* para aplicar as alterações de permissão:

   sudo reboot

5.2.4 Etapas para instalação e análise de pacotes em tempo real utilizando o packet sender

1. Vá até o link Packet Sender - Download e instale o *software*.
2. Após instalar, abra o *software*, a tela que você verá será a mostrada a seguir assim como na Figura 50.

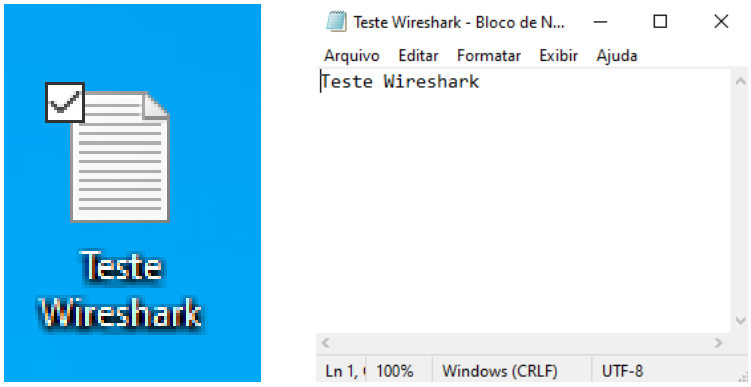
Figura 50 - Packet Sender.



Fonte: O autor

3. Crie um arquivo de texto e nomeie de acordo com sua preferência, dê o nome como **Teste *Wireshark*** e escreva algo nesse documento, neste caso escrevi Teste *Wireshark* também, como pode ser observado na Figura 51.

Figura 51 - Arquivo de texto.



Fonte: O autor

4. Escolha um nome para ser colocado no ***Packet Sender,*** como pode ser observado na Figura 52.

Figura 52 - Nome no Packet Sender.

Fonte: O autor

5. Vá até o **Load File** e escolha o arquivo criado por você, como pode ser visto na Figura 53.

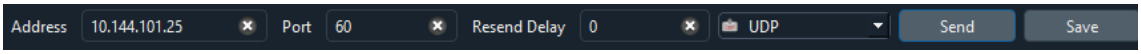
Figura 53 - Escolha do arquivo para carregar no packet sender.

Fonte: O autor

6. Escolha qual o endereço você quer enviar aquele pacote, qual porta quer utilizar e qual protocolo irá utilizar, como podemos ver na Figura 54.

Neste caso foi utilizado o ip de uma máquina do laboratório de redes, a porta 60 e o protocolo UDP.

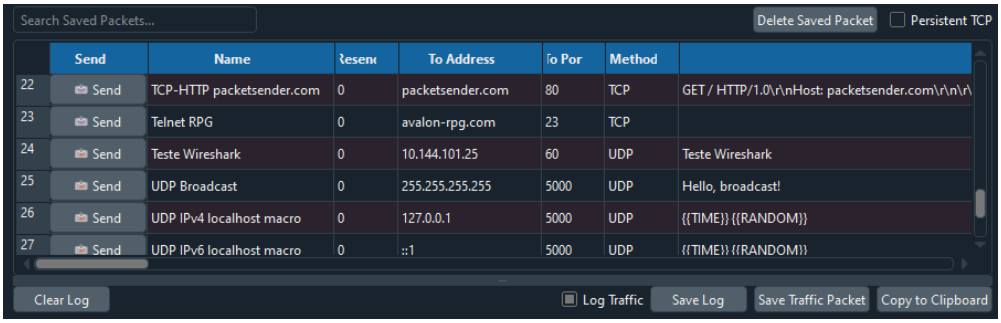
Figura 54 - Escolha da porta e protocolo utilizados.



Fonte: O autor

7. Após ter preenchido essas informações clique em **Save**, como pode ser visto na Figura 55.

Figura 55 - Log do packet sender.

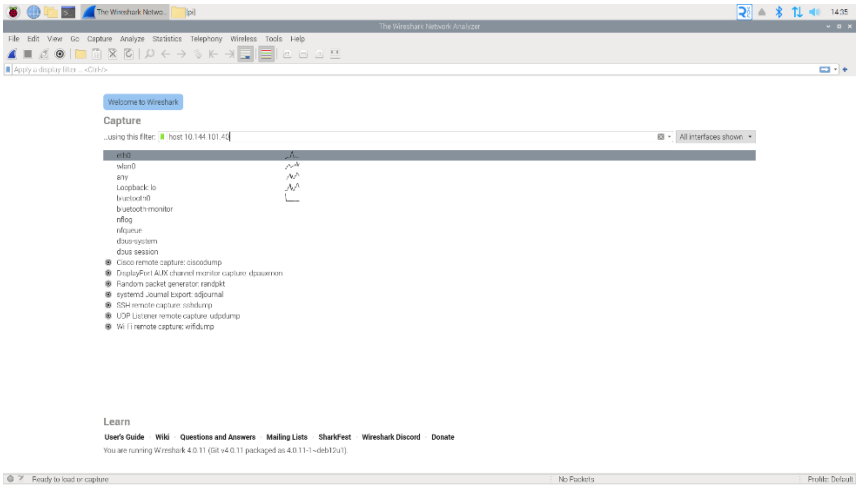


Fonte: O autor

8. Abra o ***wireshark*** instalado em sua *Raspberry Pi*, vá até o prompt de comando e digite *wireshark* e pressione **enter**.

9. Após a inicialização do *wireshark* clique uma vez em eth0, e digite host 10.144.101.40, sendo 10.144.101.40 o ip da máquina de onde será enviado o arquivo criado anteriormente, como pode ser visto na Figura 56.

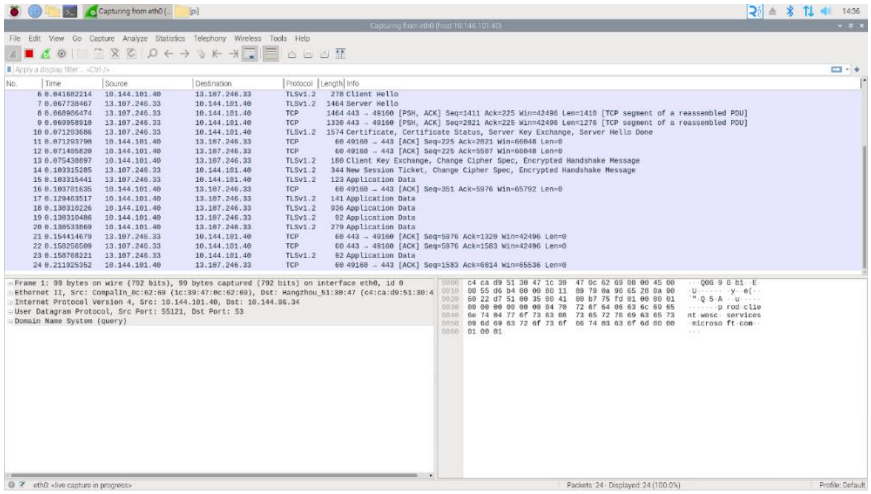
Figura 56 - Primeira Interface do Wireshark.



Fonte: O autor

10. Pressione enter, e então aparecerá uma tela semelhante à mostrada a seguir, como pode ser visto na Figura 57.

Figura 57 - Tela de monitoramento da rede no wireshark.



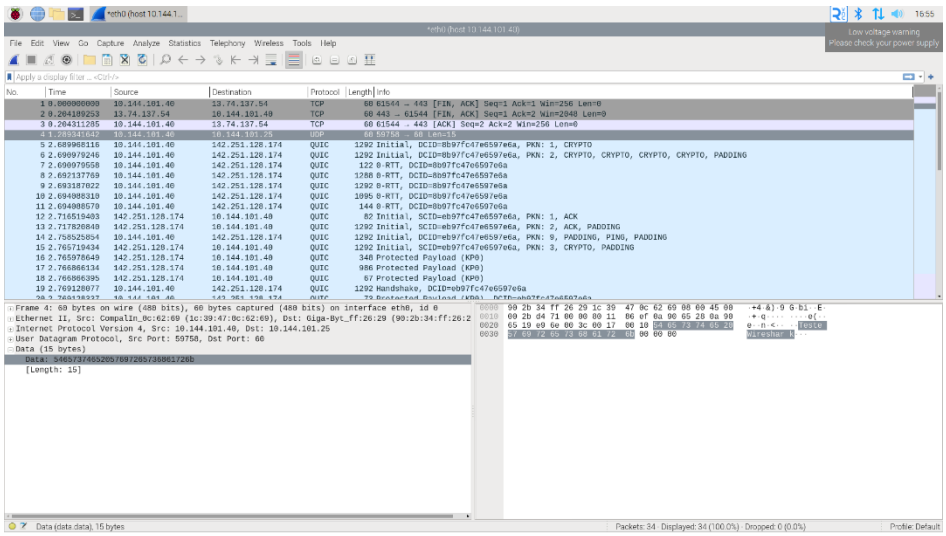
Fonte: O autor

11. Volte ao aplicativo ***Packet Sender*** e clique em send.

12. Após isso vá ao botão quadrado vermelho na aba do *wireshark* para pausar o monitoramento e averiguar o pacote enviado pelo *Packet Sender*.

13. Então procure o pacote que você enviou, observando a source (fonte) e Destination (destino) daquele pacote, como é mostrado na Figura 58.

Figura 58 - Verificação do pacote enviado no packet sender.

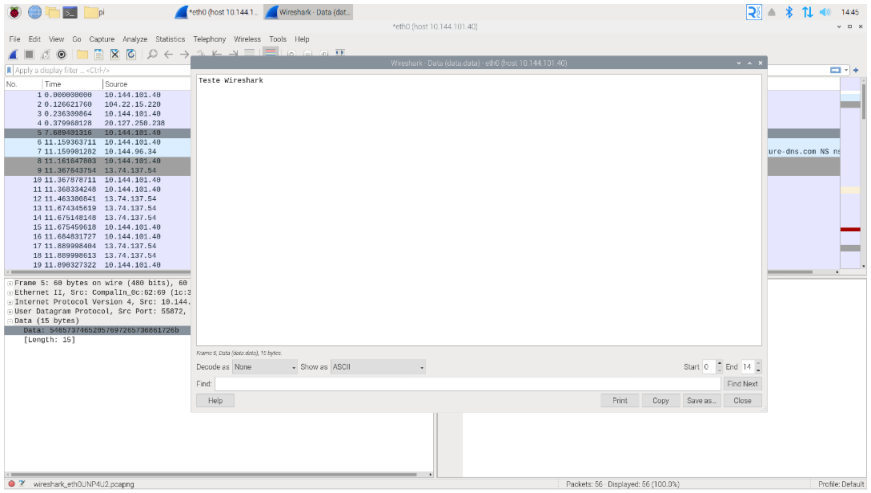


Fonte: O autor

14. A **source** como pode ser observado no print acima, é o ip da máquina que eu enviei o pacote, no caso 10.144.101.40 e Destination é o ip da máquina que recebeu esse pacote, no caso 10.144.101.25.

15. Vá até a aba **Analyze** e clique em Show Packet Bytes... e então aparecerá uma tela com o nome do arquivo enviado, como pode ser visualizado na Figura 59.

Figura 59 - Visualização do pacote enviado no packet sender.



Fonte: O autor

5.3 ROTEIRO PRÁTICO 3 – CRIMPAR CABO DE REDE

O Roteiro Prático 3 ensina como crimpar cabos de rede, uma habilidade fundamental para configurar conexões estáveis em redes de computadores. O processo envolve organizar os fios internos do cabo conforme os padrões T568A ou T568B, inserir os fios em conectores RJ-45, utilizar um alicate de crimpagem para fixá-los e testar a funcionalidade com um testador de cabos. A prática também aborda como identificar e corrigir falhas comuns, como fios desalinhados, má crimpagem e curtos-circuitos, garantindo a eficiência e durabilidade do cabo. Dicas e orientações ajudam a evitar erros e asseguram um trabalho preciso.

5.3.1 Introdução

Nesta aula prática, vamos aprender a crimpar um cabo de rede, um processo fundamental para quem trabalha com redes de computadores. O objetivo é criar um cabo de rede funcional, conectando dispositivos e garantindo uma boa transmissão de dados. Para isso, utilizaremos ferramentas específicas como conectores RJ-45, alicate de crimpagem e cabos de rede.

Entender como crimpar corretamente é essencial para garantir a eficiência de uma rede, evitando problemas de conexão causados por mau contato ou erros de pinagem. Durante esta atividade, você aprenderá a organizar os fios internos de acordo com os padrões de pinagem (T568A ou T568B), inserir corretamente os fios no conector e utilizar o alicate de crimpagem para garantir uma conexão sólida. Ao final, será possível testar o cabo para assegurar seu funcionamento, reforçando a importância de um trabalho cuidadoso e preciso.

Materiais Necessários:

- Cabo de rede (Cat5e, Cat6, etc.);
- Conectores RJ-45;
- Alicate de crimpagem;
- Decapador de cabos e
- Tesoura ou cortador de cabo.

5.3.2 Etapas para preparação do cabo

Essa etapa tem como principal objetivo, instruir como o cabo deve ser manuseado, para que a crimpagem seja um processo simples.

1. **Corte o cabo** no comprimento desejado usando o cortador de cabo.
2. **Retire a capa externa** do cabo com o decapador. Evite cortar os fios internos.
3. **Organização dos Fios:**

   • **Desdobre e alinhe os fios internos**. Normalmente, você verá 8 fios em cores diferentes, organizados em pares.

   • **Acomode os fios na ordem correta**. Dependendo do padrão que você está seguindo (T568A ou T568B), alinhe os fios conforme a pinagem escolhida como pode ser visto na Figura 60. Aqui estão as ordens de pinagem para ambos os padrões:

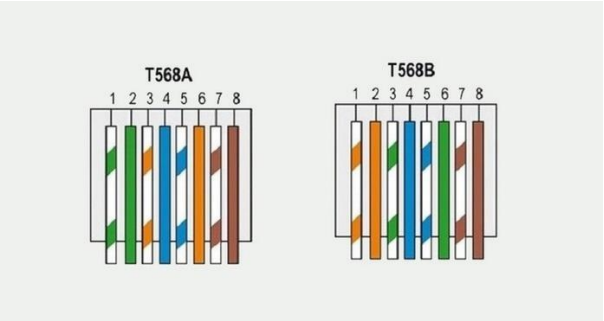
Tabela 2 - Padrões de organização

T568A	**T568B**
Branco/Verde	Branco/Laranja
Verde	Laranja
Branco/Laranja	Branco/Verde
Azul	Azul

Branco/Azul	Branco/Azul
Laranja	Verde
Branco/Marrom	Branco/Marrom
Marrom	Marrom

Fonte: O autor

Figura 60 - Padrões de organização.



Fonte: (Redação, 2017)

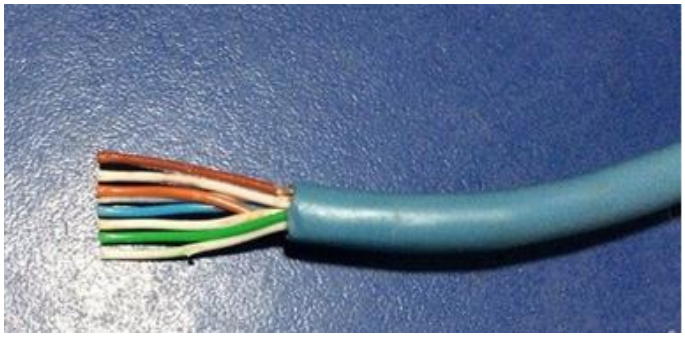
5.3.3 Etapas para crimpagem

Essa etapa tem como principal objetivo, instruir como a crimpagem deve ser feita, para que o cabo funcione adequadamente.

1. **Corte o Excesso:**

   Ajuste os fios para que todos tenham o mesmo comprimento e sejam curtos o suficiente para entrar no conector RJ-45 sem dobrarem, como pode ser visto na Figura 61.

Figura 61 - Cabo de rede pronto para colocar no conector RJ-45 seguindo o padrão T568A.



Fonte: Redação (2017, on-line)

2. **Inserção dos Fios no Conector:**

   Insira os fios cuidadosamente no conector RJ-45, certificando-se de que cada fio entre completamente em seu canal.

   Verifique se todos os fios estão alinhados e completamente inseridos até o final do conector, como pode ser visto na Figura 62.

Figura 62 - Cabo de rede crimpado.

Fonte: Redação (2017, on-line)

3. **Crimpagem:**

Coloque o conector RJ-45 no alicate de crimpagem.

Aperte o alicate firmemente para crimpar os pinos do conector nos fios. Isso garante que os fios fiquem presos e estabeleçam uma boa conexão com os contatos internos do conector.

5.3.4 Verificação de funcionamento

O testador de cabos de rede Tozz, visualizado na Figura 63, assim como outros modelos semelhantes, é um aparelho utilizado para conferir a continuidade, o alinhamento dos pinos e a integridade das conexões em cabos de rede, especialmente os cabos Ethernet. Sua função principal é verificar se o cabo está em boas condições de funcionamento e se as extremidades estão crimpadas corretamente, garantindo que as conexões foram feitas adequadamente.

Figura 63 - Testador de cabos de rede Tozz.

Fonte: Enterlight (2024, on-line)

5.3.4.1 Componentes do testador

Esses são os componentes do testador:

Unidade principal: Conta com LEDs que indicam o status do teste e portas onde o cabo é conectado. Em muitos casos, é onde o sinal é gerado.

Unidade remota: Utilizada para testar cabos mais extensos, é colocada na outra extremidade do cabo e recebe o sinal enviado pela unidade principal.

5.3.4.2 Como usar o testador de cabos de rede

É fundamental que o teste seja realizado corretamente e que seja compreendido em casa de funcionamento ou não funcionamento.

1. **Conecte o cabo**: Para cabos Ethernet (RJ45), insira uma extremidade na unidade principal e a outra na unidade remota.
2. **Execute o teste**: Ao ligar o testador, ele emite sinais elétricos pelos fios do cabo. Os LEDs em ambas as unidades começam a piscar ou acender em sequência.

5.3.4.3 Como ler os resultados

É necessário compreender a leitura dos resultados, para que seja possível corrigir erros em caso de falha durante a verificação.

Sequência correta (1 a 8): Se os LEDs acenderem em ordem numérica, o cabo está crimpado corretamente e as conexões estão boas.

Fios trocados: Se os LEDs acenderem em ordem diferente nas duas unidades (ex: LED 1 da unidade principal corresponde ao LED 2 da remota), há cruzamento de fios.

Fios em curto: Se algum LED não acender ou mais de um acender ao mesmo tempo, há curto-circuito entre os fios.

Fios partidos: Se um ou mais LEDs não acenderem, isso indica ruptura ou má crimpagem.

5.3.4.4 Funções

Essas são algumas das funções para o testador de cabos de redes.

Verificação de continuidade: Confirma a continuidade elétrica em todos os pinos do cabo.

Verificação de padrão: Identifica se o cabo segue o padrão correto (T568A ou T568B).

Detecção de curto: Detecta se há fios em curto-circuito.

5.3.4.5 Falhas comuns

Essas são as possibilidades de falhas ao realizar a crimpagem.

Desalinhamento dos fios: Inserir os fios na ordem errada de pinagem (T568A ou T568B) gera falhas de conexão entre dispositivos.

Fios mal inseridos: Se os fios não forem empurrados completamente no conector RJ-45, os pinos não fazem contato adequado, causando uma conexão instável.

Remoção excessiva da capa externa: Expor muito os fios internos pode deixá-los vulneráveis a danos e interferências.

Crimpagem insuficiente: Se o alicate não for apertado com firmeza, os contatos não perfuram corretamente o isolamento, prejudicando a conexão.

Conectores inadequados: Usar conectores de baixa qualidade ou incompatíveis com o cabo afeta a crimpagem e o desempenho.

Cabo mal posicionado: Um cabo mal inserido no conector pode se soltar com o tempo, causando falhas recorrentes.

5.3.4.6 Dicas adicionais

Essas são algumas dicas que podem ajudar a evitar problemas durante a realização do roteiro.

- Trabalhe com cuidado para evitar danificar os fios internos;
- Certifique-se de usar a ferramenta correta para crimpar para evitar problemas de conexão;
- Teste o cabo após a crimpagem para garantir que está funcionando corretamente.

5.4 ROTEIRO PRÁTICO 4 – INSTALANDO UM PATCH PANEL

O Roteiro Prático 4 aborda a instalação de um Patch Panel, dispositivo essencial para organizar e gerenciar conexões em redes. O Patch Panel centraliza cabos em um único painel, conectando-os a equipamentos como computadores e *switches*, promovendo escalabilidade, organização e facilidade de manutenção.

5.4.1 Introdução

Patch Panels são dispositivos de rede que possibilitam a conexão organizada de diversos equipamentos, como computadores e impressoras. Esses dispositivos possuem várias portas, e cada porta é conectada a um dispositivo por meio de cabos de rede, garantindo uma distribuição eficiente do tráfego de dados. Ao invés de ligar os cabos

diretamente em *switches* ou *hubs*, as conexões são realizadas na parte de trás do Patch Panel. Isso permite uma organização mais eficiente da rede. Além das redes Ethernet, os Patch Panels também podem conectar diferentes tipos de redes, como a de fibra óptica, oferecendo uma solução versátil para gerenciar múltiplas conexões de maneira prática e organizada.

O uso de Patch Panels traz uma série de vantagens para a gestão de redes. Um dos principais benefícios é a escalabilidade, já que facilita a expansão da rede, permitindo a adição de novos dispositivos de forma simples e eficiente. Além disso, ao consolidar todos os cabos em um único painel, os Patch Panels ajudam a reduzir a desordem nos racks e contribuem para a redução de custos de instalação e manutenção. Outro ponto positivo é a facilidade de manutenção, uma vez que problemas podem ser identificados e corrigidos rapidamente, sem a necessidade de rastrear manualmente cada cabo. Além da funcionalidade, um rack organizado com Patch Panels também melhora a aparência do ambiente e facilita o trabalho dos administradores de rede, tornando o gerenciamento da infraestrutura mais eficiente.

5.4.2 Etapas para instalação de um patch panel

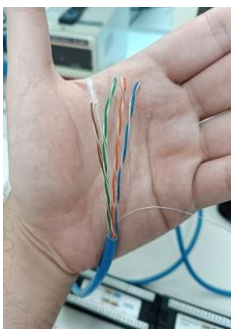
Siga corretamente esses passos, para garantir o funcionamento correto do patch panel.

1. Identifique o local apropriado para instalar o Patch Panel, geralmente em um rack de rede.
2. Prepare o rack, com uma parafusadeira ou chave de fenda, remova a placa de espelho do rack, caso exista.
3. Prepare os cabos, use um descascador de fios para remover cerca de 30 mm do isolamento de cada cabo de rede, como pode ser visto nas Figuras 64 e 65.

Figura 64 - Ilustração de um cabo de rede descascado.

Fonte: Nasatecnologia (2024, on-line)

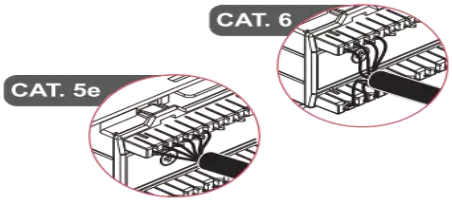
Figura 65 - Cabo de rede descascado.



Fonte: O autor

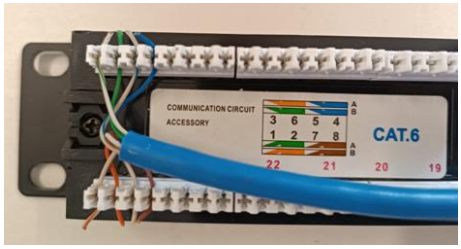
4. Conecte os fios ao Patch Panel, distribua os fios nos módulos RJ45 seguindo o padrão T568A ou T568B, indicado no verso de cada módulo, como pode ser visto nas Figuras 66 e 67.

Figura 66 - Ilustração da distribuição dos fios no patch panel.



Fonte: Nasatecnologia (2024, on-line)

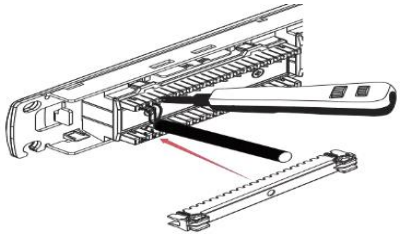
Figura 67 - Distribuição dos fios no patch panel.



Fonte: O autor

5. Utilize um alicate Punch Down, visto na Figura 68, ou um alicate específico para redes para fazer a conexão.

Figura 68 - Ilustração da utilização do alicate punch down para a crimpagem.



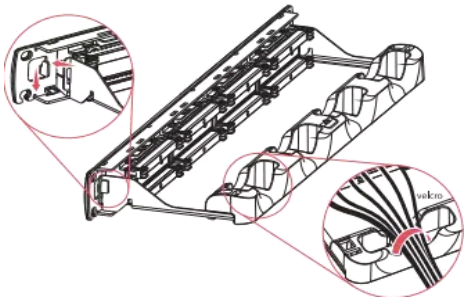
Fonte: Nasatecnologia (2024, on-line)

Figura 69 - Alicate punch down.

Fonte: O autor

6. Organize e fixe os cabos, prendendo os cabos de cada módulo ao suporte do Patch Panel usando fita de velcro para manter a organização.

Figura 70 - Ilustração de como fixar os cabos ao suporte do patch panel.



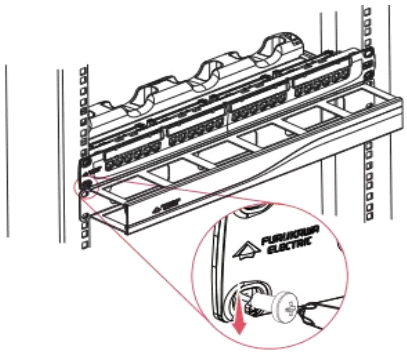
Fonte: Nasatecnologia (2024, on-line)

Figura 71 - Materiais para auxiliar na fixação dos cabos.

Fonte: O autor

7. Posicione o Patch Panel no rack e aperte os parafusos para fixá-lo.

Figura 72 - Ilustração do posicionamento do patch panel no rack.



Fonte: Nasatecnologia (2024, on-line)

Figura 73 - Local onde se coloca o parafuso no patch panel.

Fonte: O autor

5.4.3 Verificação

O testador de cabos de rede Tozz, visto na Figura 74, assim como outros modelos semelhantes, é um aparelho utilizado para conferir a continuidade, o alinhamento dos pinos e a integridade das conexões em cabos de rede, especialmente os cabos

Ethernet. Sua função principal é verificar se o cabo está em boas condições de funcionamento e se as extremidades estão crimpadas corretamente, garantindo que as conexões foram feitas adequadamente.

Figura 74 - Testador de cabos de rede Tozz.

Fonte: Enterlight (2024, on-line)

5.4.3.1 Componentes do testador

Esses são os componentes do testador

Unidade principal: Conta com LEDs que indicam o status do teste e portas onde o cabo é conectado. Em muitos casos, é onde o sinal é gerado.

Unidade remota: Utilizada para testar cabos mais extensos, é colocada na outra extremidade do cabo e recebe o sinal enviado pela unidade principal.

5.4.3.2 Como usar o testador de cabos

É fundamental que o teste seja realizado corretamente e que seja compreendido em casa de funcionamento ou não funcionamento.

Conecte o cabo: Para realizar o teste do patch panel com esse dispositivo, é necessário conectar um lado do cabo de ethernet na porta crimpada no patch panel e o outro lado do cabo na porta da unidade remota e conecte a outra ponta do cabo que está conectado ao patch panel na unidade principal.

Execute o teste: Ao ligar o testador, ele emite sinais elétricos pelos fios do cabo. Os LEDs em ambas as unidades começam a piscar ou acender em sequência.

5.4.3.3 Como ler os resultados

É necessário compreender a leitura dos resultados, para que seja possível corrigir erros em caso de falha durante a verificação.

Sequência correta (1 a 8): Se os LEDs acenderem em ordem numérica, o cabo está crimpado corretamente e as conexões estão boas.

Fios trocados: Se os LEDs acenderem em ordem diferente nas duas unidades (ex: LED 1 da unidade principal corresponde ao LED 2 da remota), há cruzamento de fios.

Fios em curto: Se algum LED não acender ou mais de um acender ao mesmo tempo, há curto-circuito entre os fios.

Fios partidos: Se um ou mais LEDs não acenderem, isso indica ruptura ou má crimpagem.

5.4.3.4 Funções

Essas são algumas das funções para o testador de cabos de redes.

Verificação de continuidade: Confirma a continuidade elétrica em todos os pinos do cabo.

Verificação de padrão: Identifica se o patch panel segue o padrão correto (T568A ou T568B).

Detecção de curto: Detecta se há fios em curto-circuito.

5.5 ROTEIRO PRÁTICO 5: CRIAÇÃO E CONFIGURAÇÃO DE VLANS

O Roteiro Prático 5 aborda o uso de VLANs como uma solução para segmentação lógica de redes, promovendo maior segurança, eficiência e controle no tráfego de dados. O exercício se concentra em configurar VLANs em um *Switch* HP 1910, atribuir portas a essas redes virtuais e configurar o *trunking* para permitir a comunicação entre VLANs diferentes.

5.5.1 Introdução

As VLANs são uma das principais ferramentas utilizadas em redes para segmentar o tráfego de forma lógica. Elas permitem a criação de múltiplas redes lógicas dentro de uma mesma infraestrutura de *switches*, oferecendo maior segurança, controle e eficiência no gerenciamento de tráfego.Já o SSH (Secure Shell) é um protocolo de rede criptografado amplamente utilizado para administração remota de sistemas e dispositivos em redes. Ele garante a comunicação segura entre cliente e servidor, permitindo acessar e gerenciar dispositivos como *switches*, roteadores e servidores de forma confiável. Combinando o uso de VLANs e SSH, é possível segmentar e proteger a rede, além de

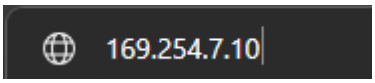
administrar seus componentes remotamente com segurança, mesmo em ambientes distribuídos.

5.5.2 Etapas para configuração de uma VLAN

Siga atentamente os passos descritos abaixo, para que a VLAN seja configurada corretamente.

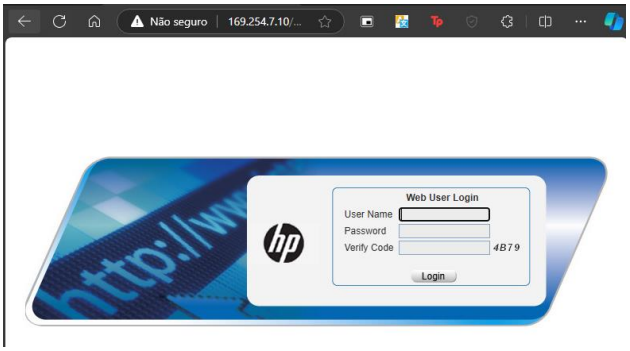
1. Conecte o cabo de rede no computador que será utilizado para fazer as configurações e no *Switch* HP 1910.
2. Entre no Link a seguir para fazer as configurações do *Switch* HP 1910: Web user login ou veja o ip de acesso ao *switch* na parte de trás e digite no navegador, como pode ser observado na Figura 75.

Figura 75 - Link para configurar o Switch HP 1910.



Fonte: O autor

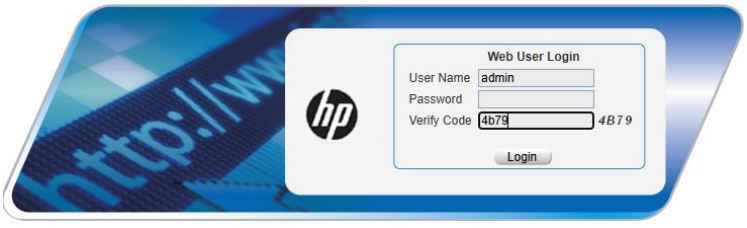
Figura 76 - Página de login do switch.



Fonte: O autor

3. Preencha os campos da seguinte maneira e clique em login, como pode ser observado na Figura 77.

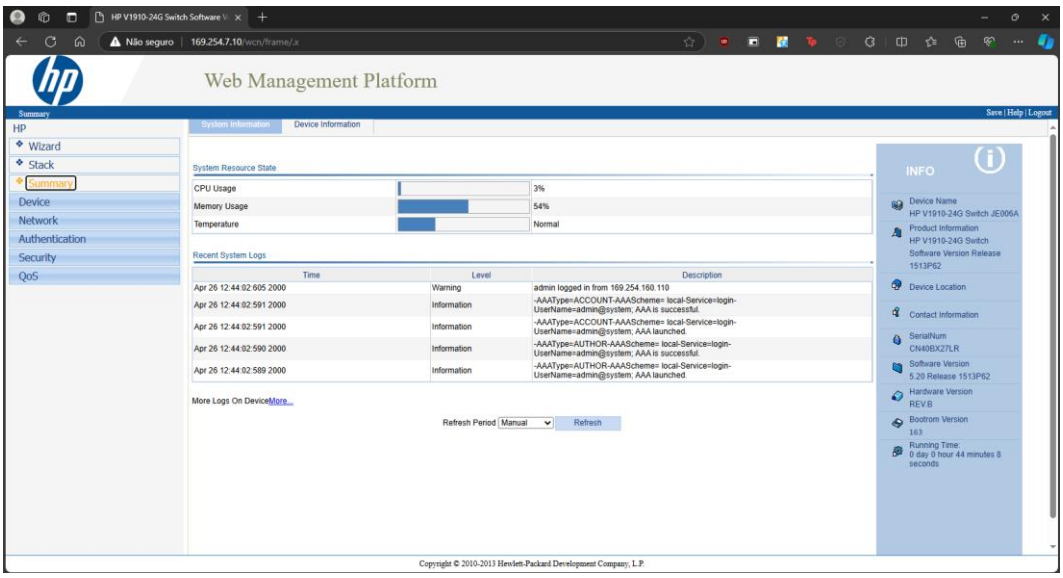
Figura 77 - Username para configurar o switch.



Fonte: O autor

4. Essa será a página inicial para configuração do *Switch*, como visto na Figura 78.

Figura 78 - Página inicial para configurações do switch.



Fonte: O autor

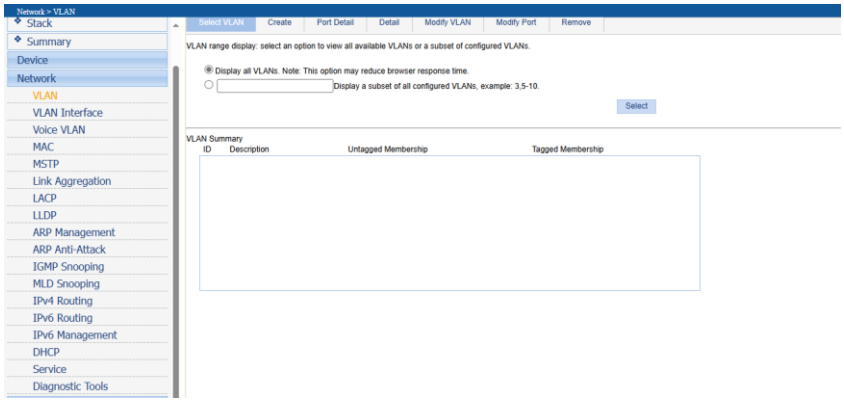
5. No lado esquerdo vá até **Network** e clique, como podemos observar na Figura 79.

Figura 79 - Menu de configuração Network.

Fonte: O autor

6. Vá até **VLAN**, como mostrado na Figura 80.

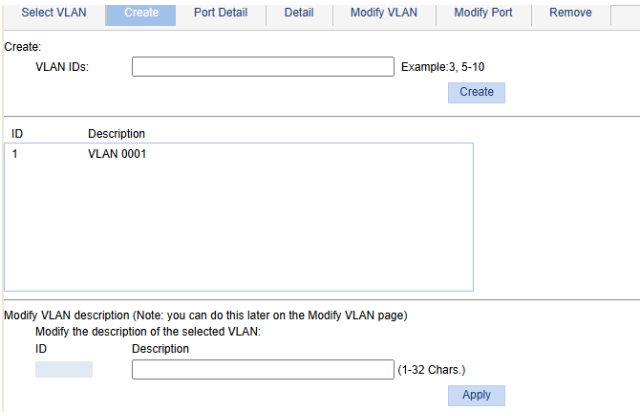
Figura 80 - Menu de configuração VLAN.



Fonte: O autor

7. Vá até **create** no canto superior, como mostrado na Figura 81.

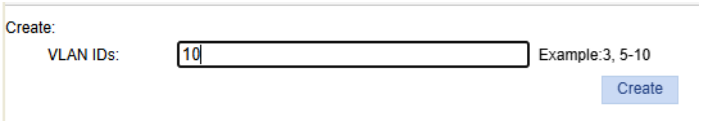
Figura 81 - Menu de criação de VLAN.



Fonte: O autor

8. Escolha **VLAN ID** que irá utilizar, com um número e clique em **create**, neste caso utilizei 10, como observado na Figura 82.

Figura 82 - Escolha do ID da VLAN.



Fonte: O autor

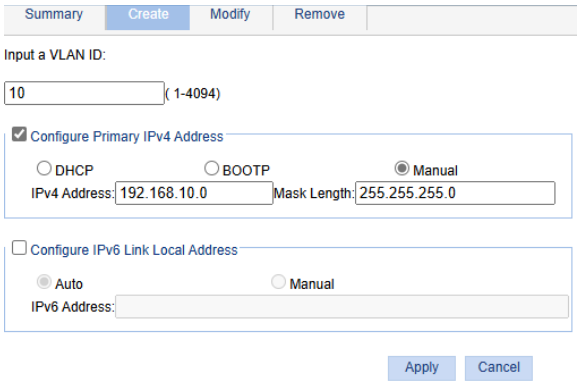
9. Após a criação da VLAN, vá até **VLAN Interface** no canto esquerdo, como observado na Figura 83.

Figura 83 - Menu VLAN Interface.

Fonte: O autor

10. Vá até **create** no canto superior e configure o ip da **VLAN** de maneira manual, como observado na Figura 84.

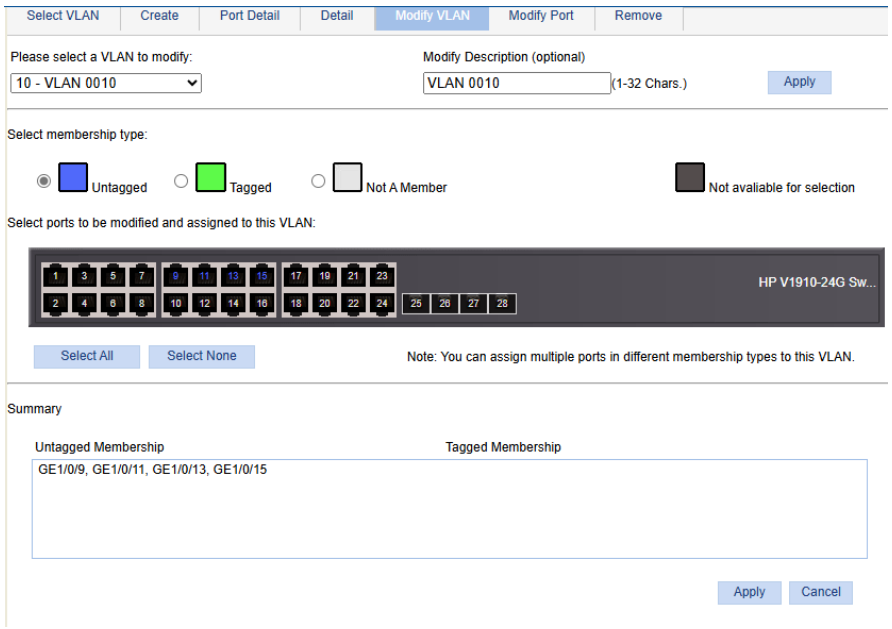
Figura 84 - Criação e configuração de uma VLAN.



Fonte: O autor

11. Retorne para VLAN e vá até **modify VLAN,** configure as portas da VLAN10 como Untagged. Basta selecionar a opção Untagged e clicar nas portas que deseja configurar, como observado na Figura 85.

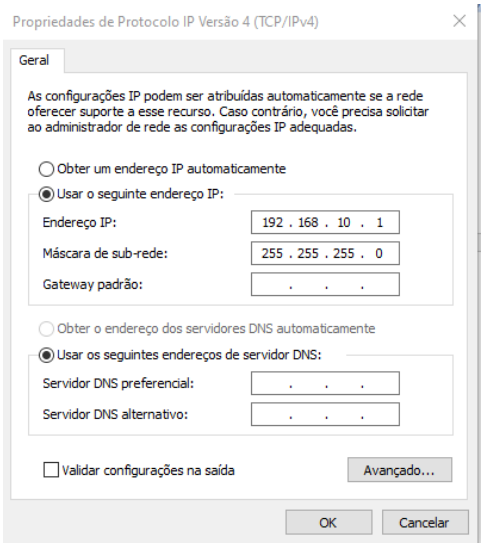
Figura 85 - Modificação das portas do switch.



Fonte: O autor

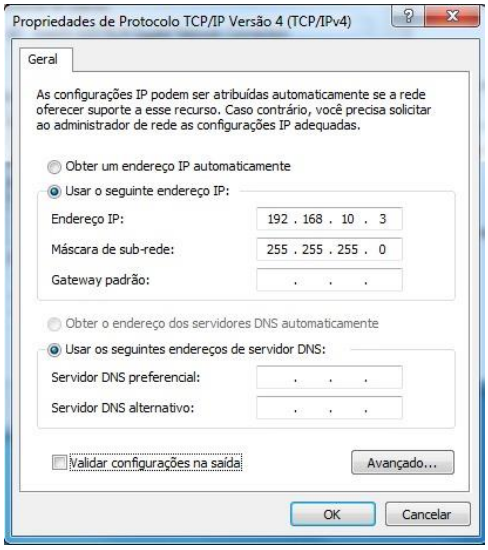
12. Após essa etapa, é necessário **configurar o ip** manualmente dos computadores conectados ao *switch*, como é possível ver nas Figuras 86 e 87.

Figura 86 - Configuração ip no computador 1.



Fonte: O autor

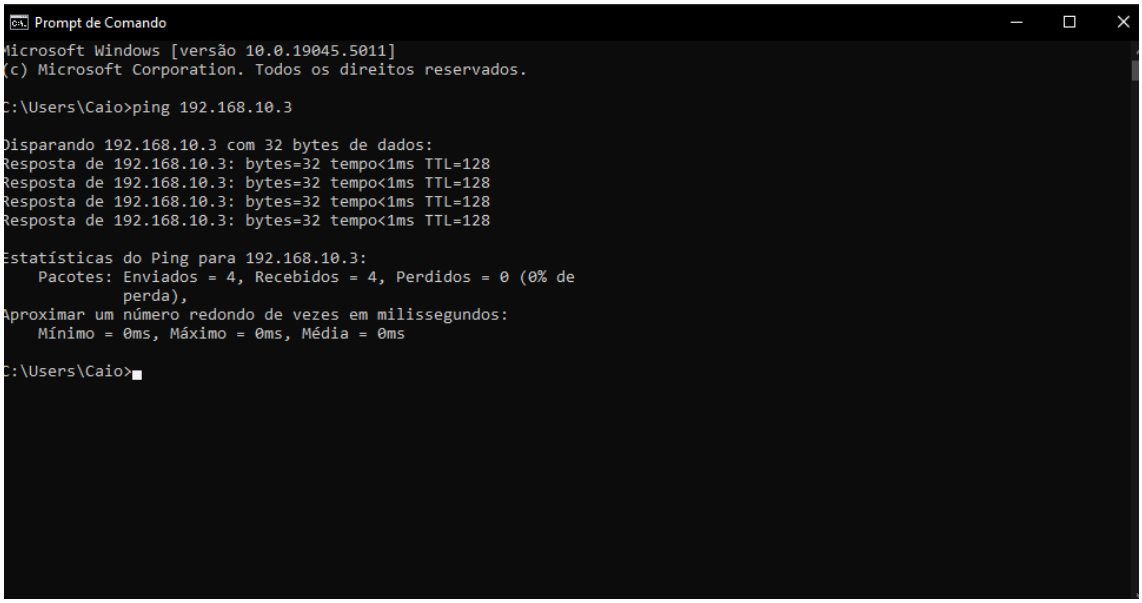
Figura 87 - Configuração ip no computador 2.



Fonte: O autor

13. Após essa alteração dos endereços IP, bastar fazer o teste no cmd, que consiste em utilizar o comando ping com o ip do outro computador e verificar que existe a conexão, como mostrado abaixo, sendo o primeiro print tirado em um computador pessoal e o outro em um computador do laboratório, ambos conectados no *switch*, como é visto nas Figuras 88 e 89.

Figura 88 - Teste ping no computador



Fonte: O autor

Figura 89 - Teste ping no computador 2.

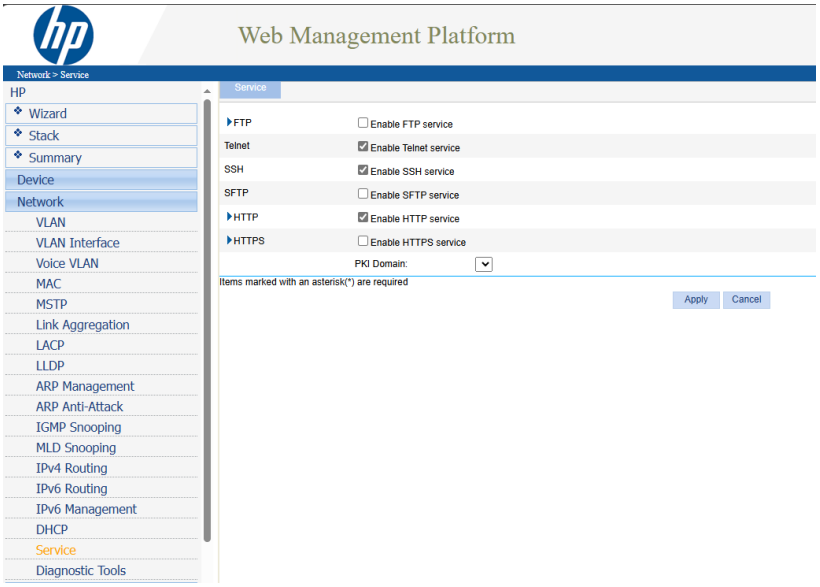
Fonte: O autor

5.5.3 Etapas para configuração de uma porta trunk

Siga as etapas com atenção, para que seja possível configurar corretamente a porta escolhida como porta trunk.

1. Habilite nas configurações do *switch* as opções a seguir para conseguir fazer as configurações via ssh utilizando o PuTTY, como é possível verificar na Figura 90.

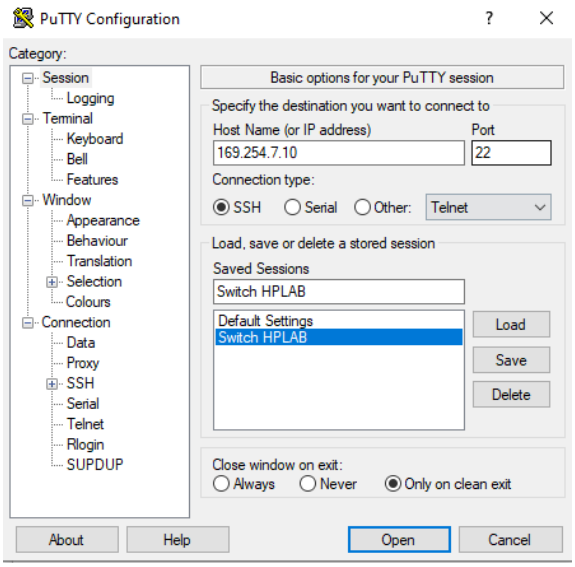
Figura 90 - Habilitando configuração via ssh.



Fonte: O autor

2. Utilizando **PuTTY,** conecte via ssh no *switch* para realizar as configurações, como podemos ver na Figura 91.

Figura 91 - PuTTY Configuration.



Fonte: O autor

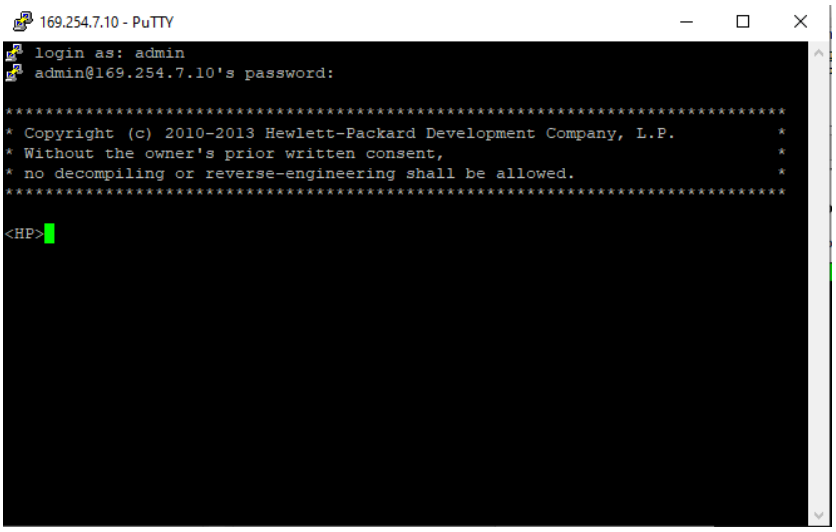
3. Após se conectar, aparecerá essa tela, como é visto na Figura 92.

Figura 92 - Prompt de configuração via ssh.

Fonte: O autor

4. Para acessar as configurações digite **admin**, clique em enter e após isso clique em enter, pois não existe senha configurada no dispositivo, como visto na Figura 93.

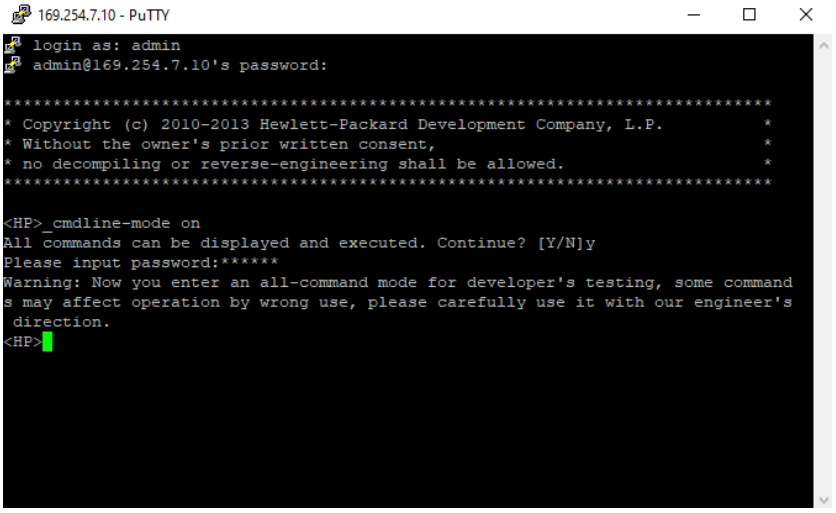
Figura 93 - Prompt de configuração via ssh.



Fonte: O autor

5. Para acessar as configurações digite **_cmdline-mode on** e pressione enter, após isso digite y e pressione enter novamente, após isso digite a senha **512900**, como podemos verificar na Figura 94.

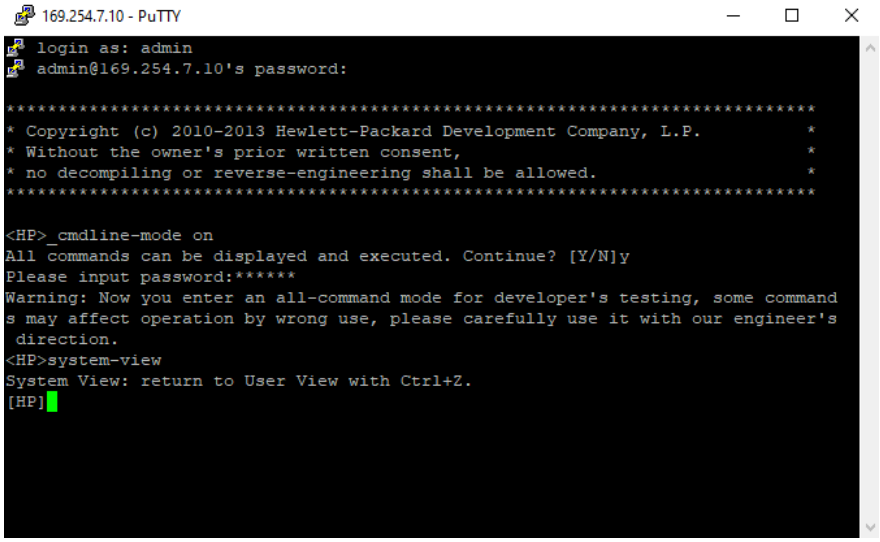
Figura 94 - Prompt de configuração via ssh.



Fonte: O autor

6. Digite **system-view** e clique em **enter**, como podemos verificar na Figura 95.

Figura 95 - Prompt de configuração via ssh.



Fonte: O autor

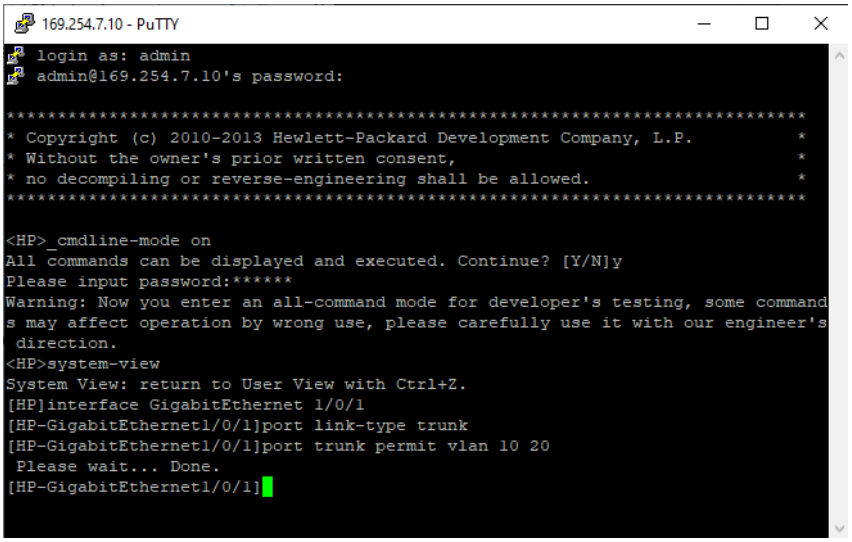
7. **Nesse caso, a porta escolhida para configuração é a 1, então utilize os seguintes comandos**, como é visto na Figura 96.

interface GigabitEthernet 1/0/1 - Esse conjunto de três números (1/0/1) refere-se à localização específica da interface no dispositivo. Primeiro número (1) – Slot do chassi, segundo número (0) – Subslot ou módulo, terceiro número (1) – Porta física.

port link-type trunk

port trunk permit vlan 10 20

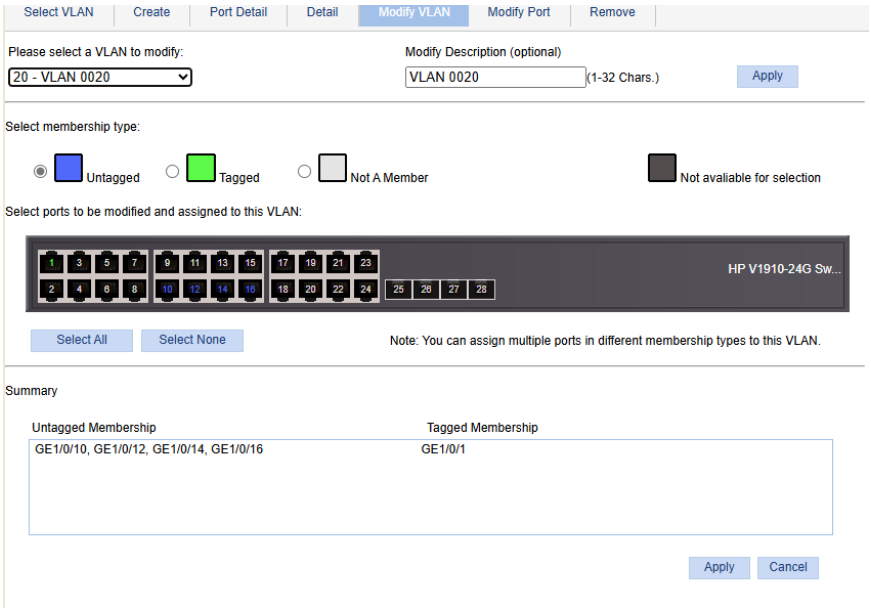
Figura 96 - Prompt de configuração via ssh.



Fonte: O autor

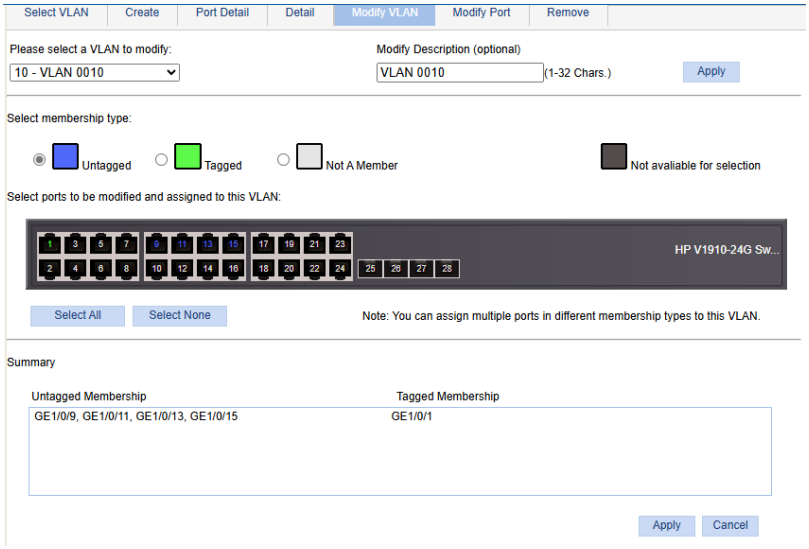
8. Para verificar se funcionou o trunk na porta 1, vá até o menu de configuração do *switch*, como deve ser observado nas Figuras 97 e 98.

Figura 97 - Verificação de configuração.



Fonte: O autor

Figura 98 - Verificação de configuração.



Fonte: O autor

5.6 ROTEIRO PRÁTICO 6 – CONFIGURAÇÃO DE WI-FI UTILIZANDO RASPBERRY PI COMO ROTEADOR

O Roteiro Prático 6 apresenta o uso do sistema operacional *OpenWrt* em um *Raspberry* Pi para transformá-lo em um roteador funcional. O *OpenWrt*, baseado em Linux, permite uma ampla personalização, oferecendo aos usuários a possibilidade de superar limitações dos firmwares tradicionais por meio de sua capacidade de instalação de pacotes personalizados.

5.6.1 Introdução

O OpenWrt é um sistema operacional baseado em Linux projetado para dispositivos embarcados. Ao invés de oferecer um firmware fixo e estático, ele disponibiliza um sistema de arquivos gravável com suporte a gerenciamento de pacotes, o que libera os usuários das limitações impostas pelas aplicações e configurações fornecidas pelos fabricantes. Isso possibilita uma ampla personalização dos dispositivos por meio de pacotes que podem ser instalados para diversas finalidades.

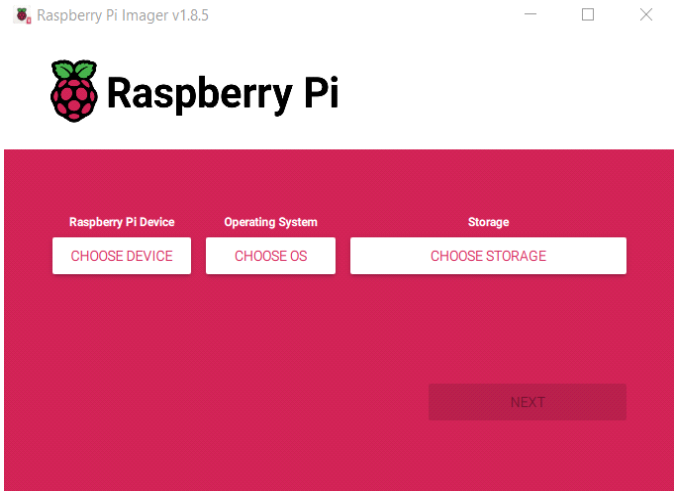
5.6.2 Etapas para instalação e configuração do OpenWrt

Siga atentamente essas etapas, para que a versão correta do openwrt seja instalado.

1. Acesse o site [OpenWrt Wiki] Raspberry Pi e selecione de acordo com seu dispositivo *Raspberry Pi*.
2. Baixe e instale a Factory image.

3. Acesse o site oficial da *Raspberry Pi* para baixar o *Raspberry Pi Imager*: https://www.raspberrypi.com/software/.

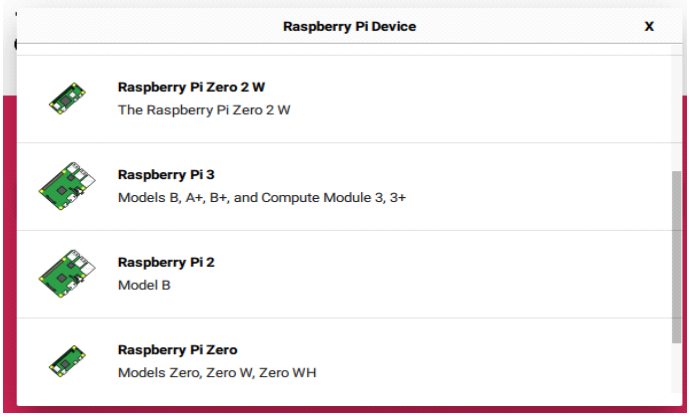
Figura 99 - Tela inicial Raspberry Pi Imager.



Fonte: O autor

4. Escolha o dispositivo que será utilizado, neste caso o Raspiberry Pi 3, como visto na Figura 100.

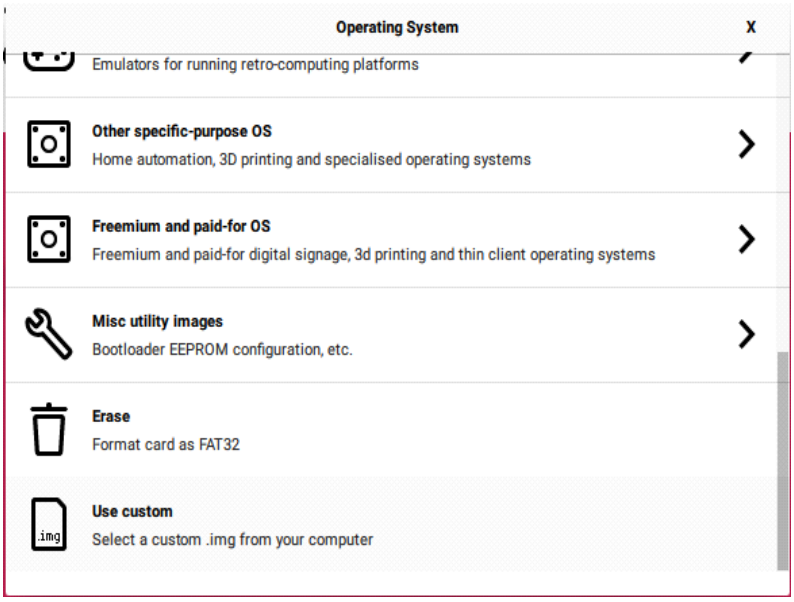
Figura 100 - Escolha do dispositivo no raspberry pi imager.



Fonte: O autor

5. Vá até “Use custom”, como visto na Figura 101 e selecione a o arquivo baixado no site [OpenWrt Wiki] Raspberry Pi.

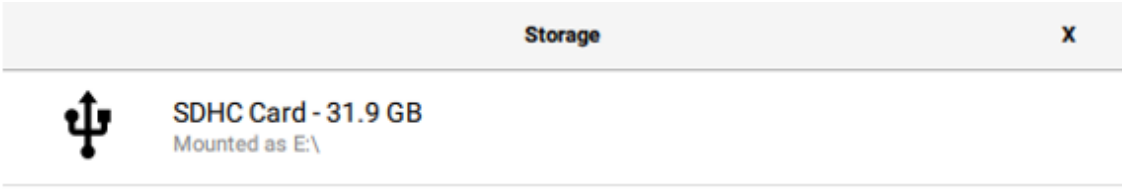
Figura 101 - Escolhendo o sistema operacional no raspberry pi imager.



Fonte - O autor

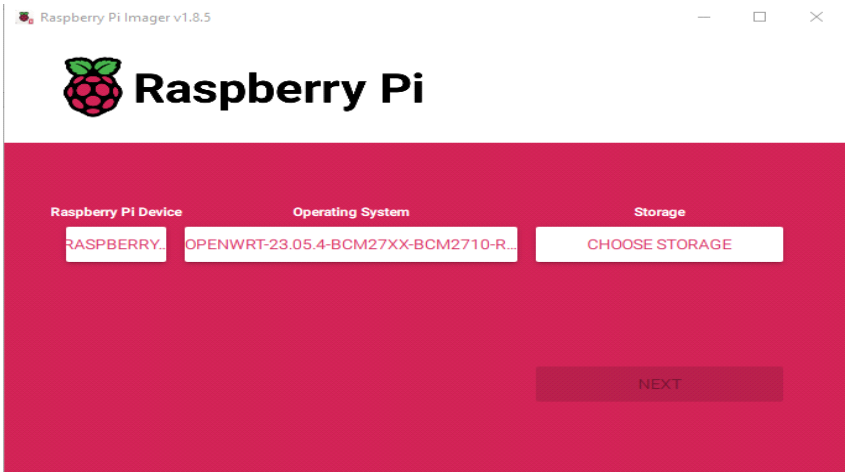
6. Selecione o cartão SD correto para armazenar o sistema operacional. Certifique-se de que o cartão tenha espaço suficiente (mínimo de 2GB), como observado na Figura 102.

Figura 102 - Escolha do dispositivo de armazenamento no raspberry pi imager.



Fonte: O autor

Figura 103 - Raspberry Pi Imager.



Fonte: O autor

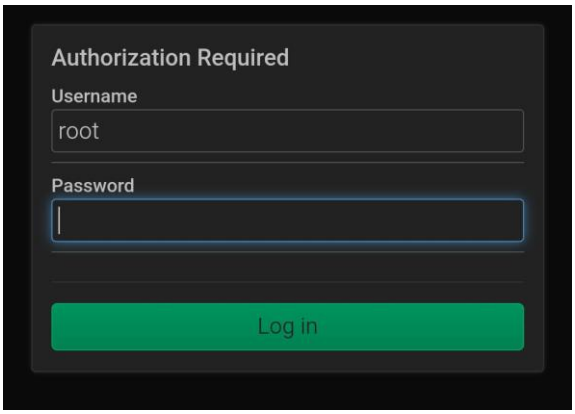
7. Após a gravação, insira o cartão SD na *Raspberry Pi*.

5.6.3 Etapas para configuração wireless utilizando o OpenWRT

É fundamental que todos esses passos sejam seguidos corretamente para que o dispositivo funcione da maneira correta.

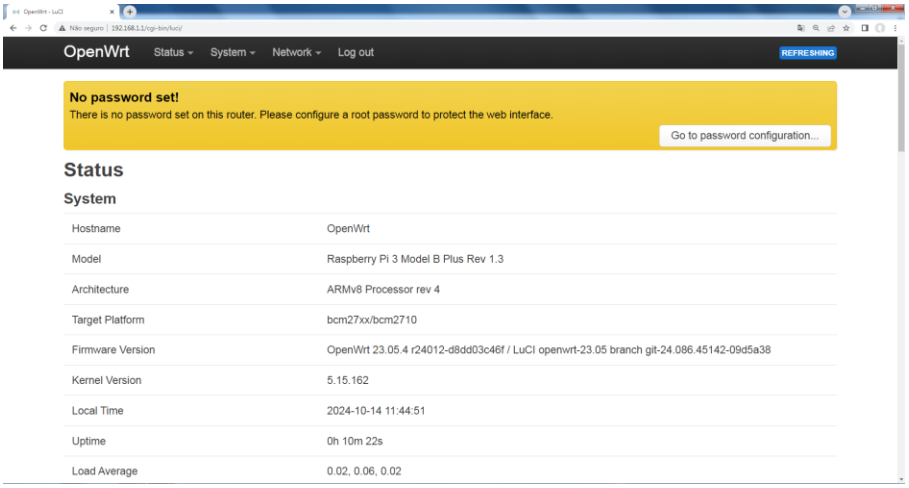
1. Conecte o cabo de rede na *Raspberry Pi* e no computador que será utilizado para fazer a configuração, siga os seguintes passos:
2. Acesse o IP padrão do *OpenWrt*: http://192.168.1.1 através do seu navegador.
3. A tela de login do *OpenWrt* será exibida. Não há senha configurada por padrão. Deixe o campo em branco e clique em **Login,** como é possível verificar na Figura 104.

Figura 104 - Tela de login OpenWrt.



Fonte: O autor

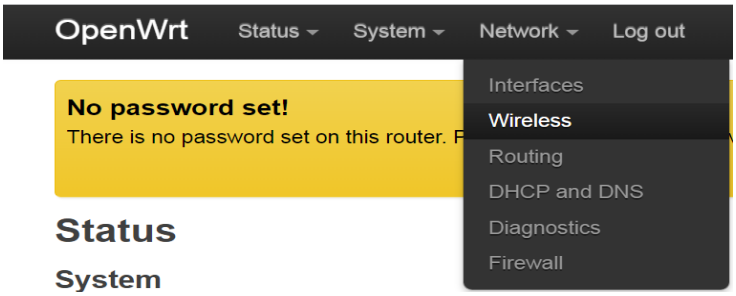
Figura 105 - Tela inicial do OpwnWrt.



Fonte: O autor

4. Vá até a aba Network e clique em **Wireless**, como indicado na Figura 106.

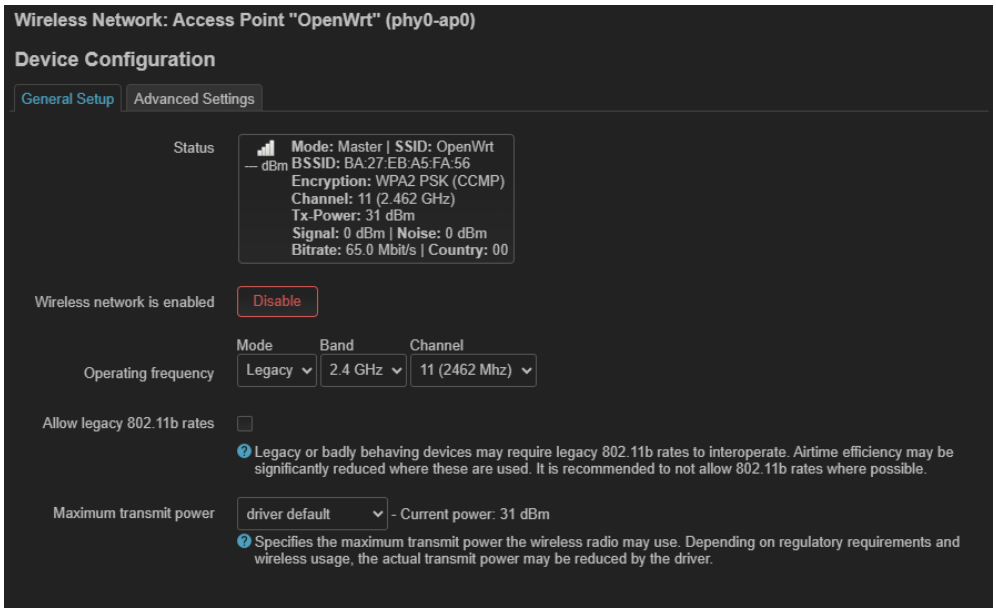
Figura 106 - Aba Network.



Fonte: O autor

5. Habilite o Wi-Fi clicando em **Enable** e vá em **edit** .

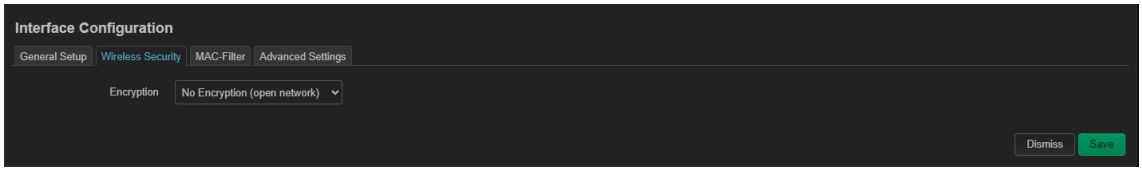
Figura 107 - Wireless Network.



Fonte: O autor

6. Na mesma página vá até **Interface Configuration** vá em **Wireless Security**, como indicado na Figura 108**.**

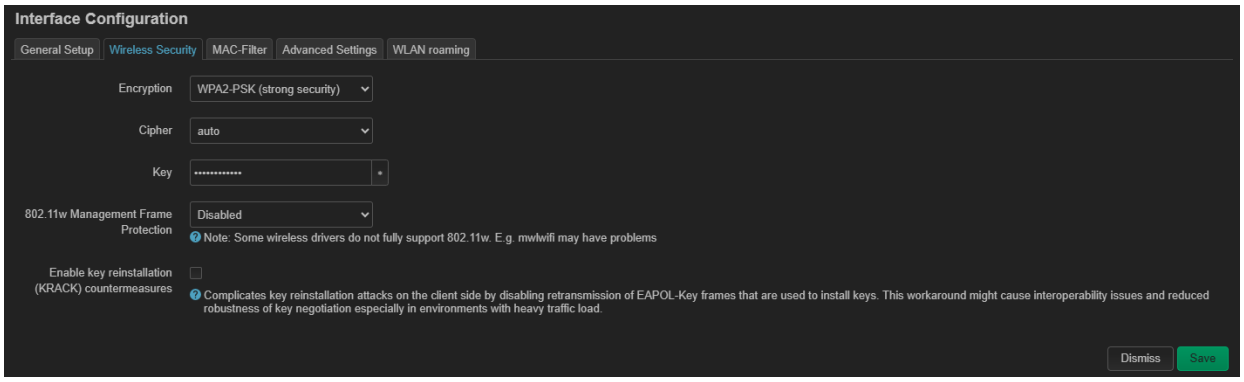
Figura 108 - Wireless Security.



Fonte: O autor

7. Altere de **No Encryption (open network)** para **WPA2-PSK (strong security)** e defina uma senha para a rede Wi-Fi OpenWrt, como visto na Figura 109.

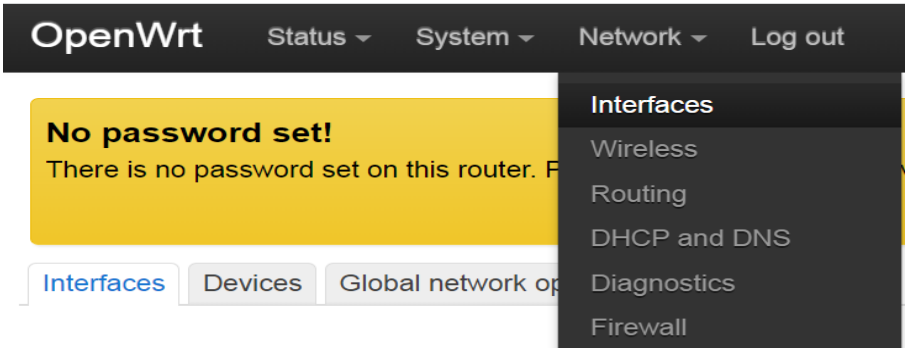
Figura 109 - Interface Configuration.



Fonte: O autor

8. Após fazer as configurações anteriores e após fazer as configurações clique em **save** e depois **Save & Apply**.
9. Se conecte ao Wi-Fi **OpenWRT.**
10. Vá até a aba Network e clique em **Interfaces**, como observado na Figura 110.

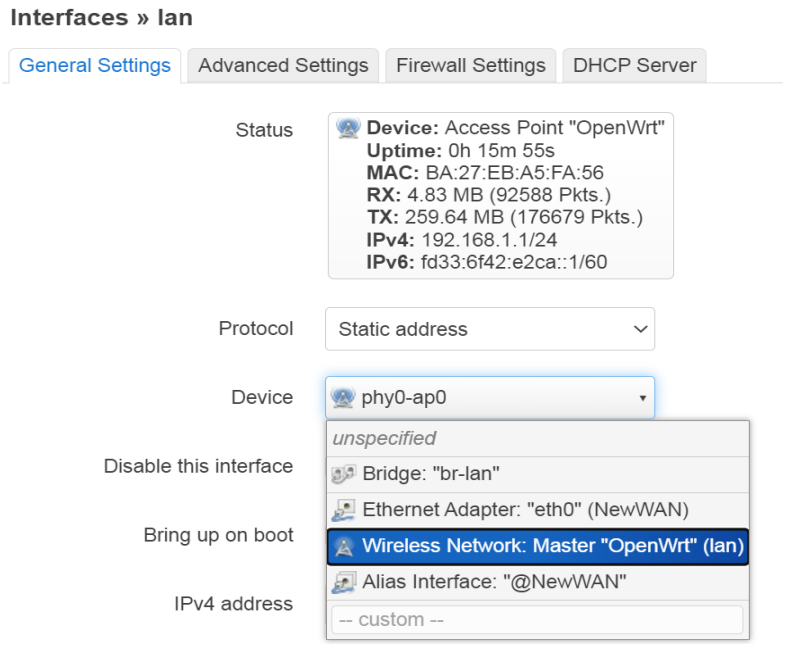
Figura 110 - Aba Interfaces.



Fonte: O autor

11. Vá até **edit** da lan existente, modifique **device** de **br-lan** para **Wireless Network: Master,** clique em **save** e depois em **Save & Apply**, como pode ser observado na Figura 111.

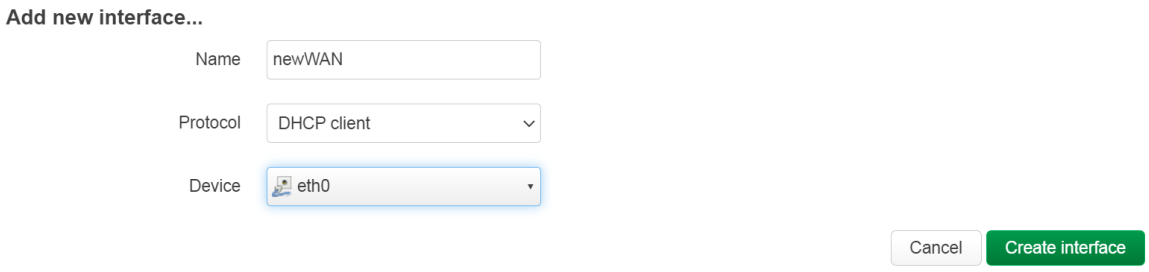
Figura 111 - Interfaces >> lan.



Fonte: O autor

12. Vá até **Add new interface.**
13. Coloque o nome na nova interface, selecione em protocol **DHCP client**, em device coloque **eth0**, clique em **Create interface**, clique em **save** depois em **Save & Apply**, como é visto na Figura 112.

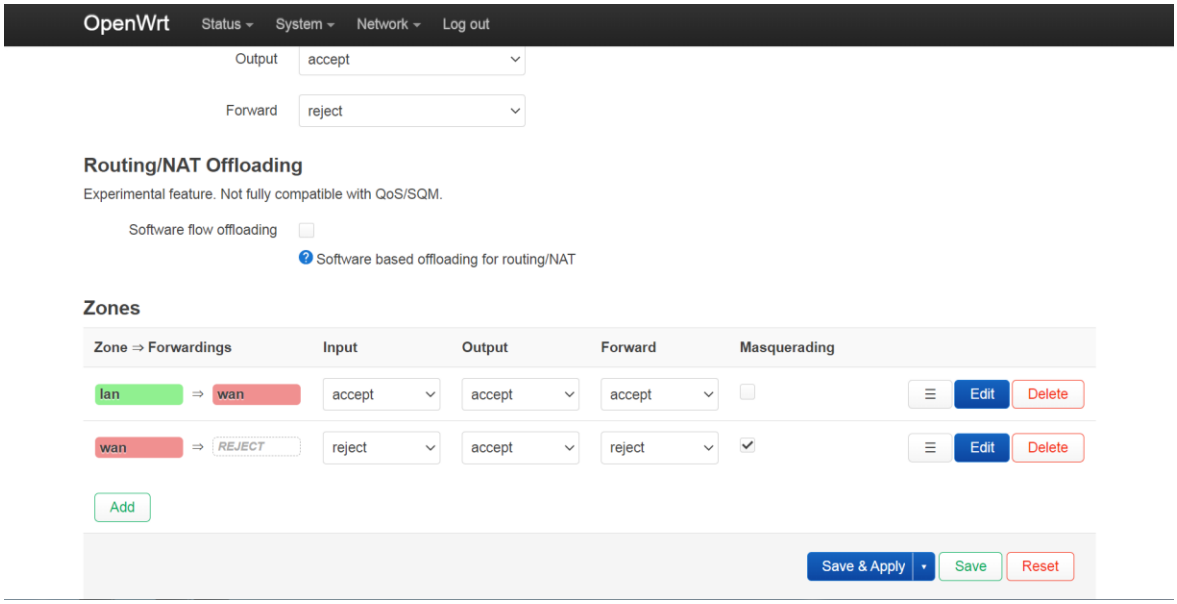
Figura 112 - Add new interface.



Fonte: O autor

14. Vá até a aba Network e clique em ***Firewall***, como é visto na Figura 113.

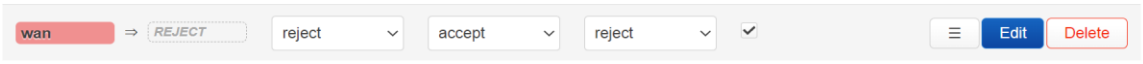
Figura 113 - Firewall.



Fonte: O autor

15. Vá até **edit** e altere **Covered networks** para **NewWAN**, clique em **save** e depois em **Save & Apply**, como podemos observar nas Figuras 114 e 115.

Figura 114 - Configuração NewWAN



Fonte: O autor

Figura 115 - Covered networks.

Fonte: O autor

16. Conecte o cabo de rede que está conectado na *Raspberry* no roteador.

17. Realize um teste de velocidade, para verificar se a conexão está funcionando, como podemos observar na Figura 116.

Figura 116 - Teste de velocidade.

Fonte: O autor

5.7 ROTEIRO PRÁTICA 7: BLOQUEAR AS PORTAS DE REDE DE UM SWITCH EM UM PERÍODO DESEJADO

O Roteiro Prático 7 aborda a configuração de políticas de controle de acesso e tráfego em *switches* utilizando recursos como QoS e ACLs (Listas de Controle de Acesso). O objetivo é criar regras que bloqueiem o tráfego em portas específicas do *switch* durante intervalos de tempo determinados, otimizando a segurança e a gestão de redes.

5.7.1 Introdução

Nesta aula prática, vamos aprender a configurar políticas de controle de tráfego e gerenciamento de acesso em um *switch* HP V1910, focando no uso de QoS (Qualidade de Serviço) e ACLs. O propósito é criar regras que bloqueiem determinadas portas do *switch* em horários específicos, otimizando o controle do tráfego de rede e aumentando a segurança.

Para isso, começaremos configurando o recurso *Time Range*, que permite definir intervalos de tempo nos quais as portas serão bloqueadas. Com essa funcionalidade, podemos programar horários precisos para ativar ou desativar as regras de controle. Em seguida, criaremos uma ACL básica. A ACL é uma ferramenta que filtra o tráfego de rede com base em critérios como endereços IP, protocolos ou portas específicas. Neste caso, usaremos uma ACL configurada com a ação deny, que bloqueará o tráfego que corresponder às condições definidas na regra.

Além disso, configuraremos um Classifier (Classificador), que serve para definir critérios ou condições que classificam o tráfego da rede. Quando os pacotes de dados atendem a esses critérios, são tratados de acordo com as regras configuradas. O classificador será vinculado à ACL criada, permitindo que o tráfego identificado por essa

lista de controle seja bloqueado. Em seguida, definiremos um *Behavior* (Comportamento), que especifica as ações a serem tomadas quando o tráfego cumpre os critérios do classificador. Nesse caso, a ação será bloquear o tráfego (Deny).

Após isso, criaremos uma *QoS Policy* (Política de Qualidade de Serviço), que combina o classificador e o comportamento configurados, formando uma política de controle de tráfego que será aplicada a portas específicas. A *Port Policy* (Política de Porta) é a última etapa, na qual a política de QoS será associada a determinadas portas do *switch*, definindo em quais portas e horários as regras serão aplicadas.

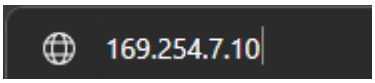
Essa prática permitirá que você veja na prática como diferentes elementos, como ACLs, classificadores e políticas de QoS, trabalham em conjunto para gerenciar o acesso e o fluxo de tráfego na rede, garantindo segurança e controle em horários determinados.

5.7.2 Etapas para configuração do switch

Com atenção siga os passos a seguir, para configurar o switch corretamente, para a aplicação proposta funcione.

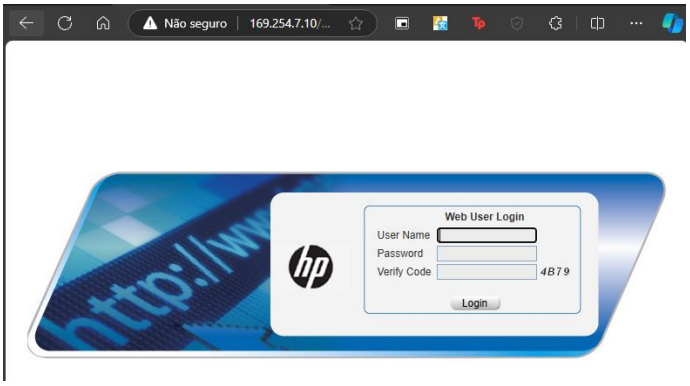
1. Conecte o cabo de rede no computador que será utilizado para fazer as configurações e no *Switch* HP 1910.
2. Entre no Link a seguir para fazer as configurações do *Switch* HP 1910: Web user login ou veja o ip de acesso ao *switch* na parte de trás e digite no navegador, como é visto na Figura 117.

Figura 117 - Link para configurar o Switch HP 1910.



Fonte: O autor

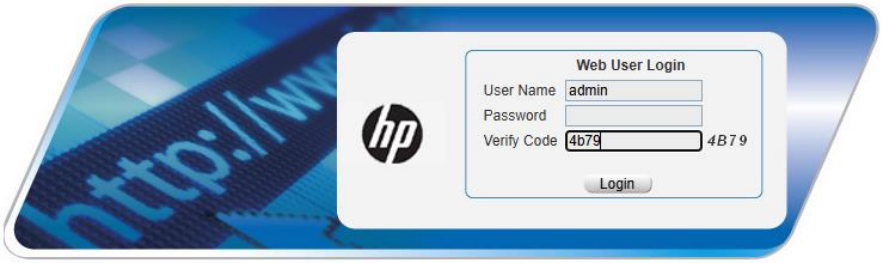
Figura 118 - Página de login do switch.



Fonte: O autor

3. Preencha os campos da seguinte maneira e clique em login, como é visto na Figura 119.

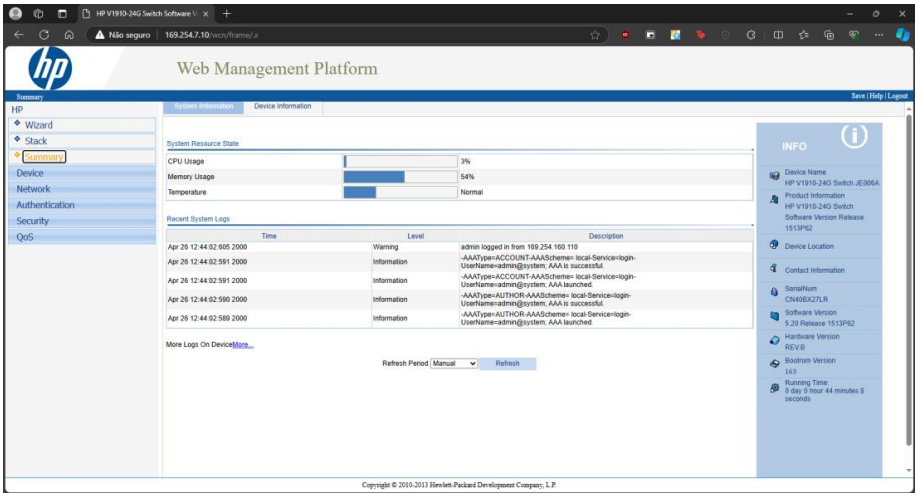
Figura 119 - Username para configurar o switch.



Fonte: O autor

4. Essa será a página inicial para configuração do *Switch*, assim como na Figura 120.

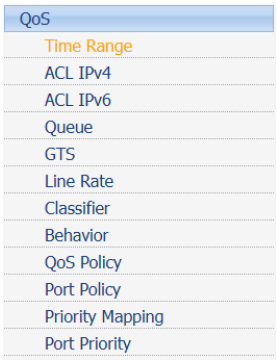
Figura 120 - Página inicial para configurações no switch.



Fonte: O autor

5. Vá até o menu **QoS** no canto esquerdo e entre na aba ***Time Range***, como mostrado na Figura 121, para configurar o horário de bloqueio das portas.

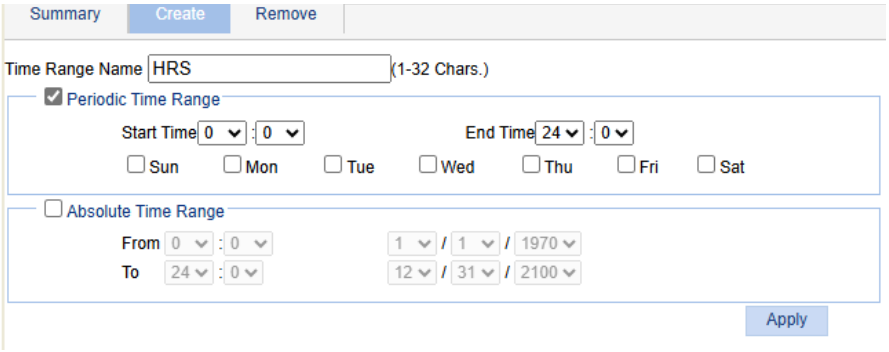
Figura 121 - Time range no menu QoS.



Fonte: O autor

6. Vá até **create** para criar um espaço de tempo, quando as portas serão desabilitadas e clique em **apply**, como mostrado na Figura 122.

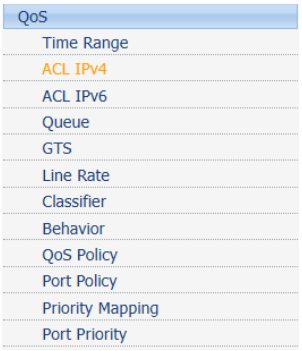
Figura 122 - Criação do time range.



Fonte: O autor

7. Vá até o menu **QoS** no canto esquerdo e entre na aba **ACL IPv4**, como mostrado na Figura123.

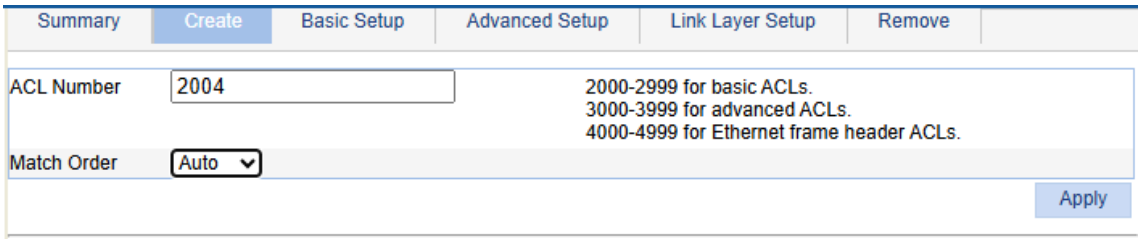
Figura 123 - ACL IPv4 no menu QoS.



Fonte: O autor

8. Vá até **create**, crie uma basic ACLs, ou seja, a **ACL Number** com uma numeração de 2000 até 2999 e coloque **Match Order** como **Auto**, como é mostrado na Figura 124.

Figura 124 - Criação da ACL.

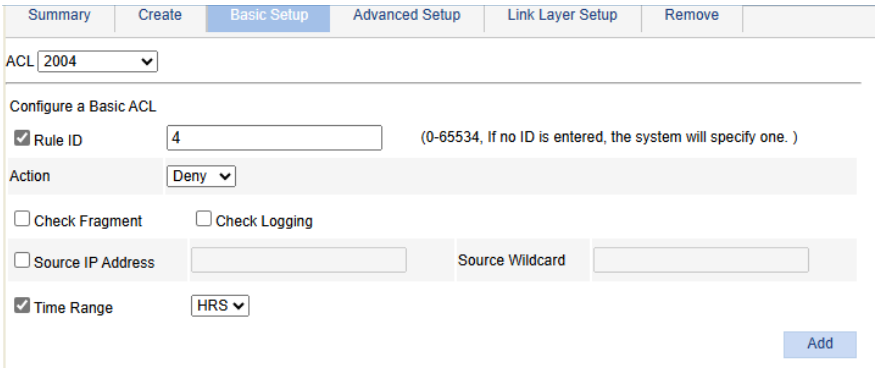


Fonte: O autor

9. Vá até ***Basic Setup*** e selecione a **ACL** criada anteriormente, marque a caixa em frente ao ***Rule ID***, selecione ***Deny*** como ***Action*** e coloque o ID específico e marque a caixa

em frente ao ***Time Range***, selecionando o criado por você anteriormente e após efetuar todas as configurações clique em **Add**, como é visto na Figura 125.

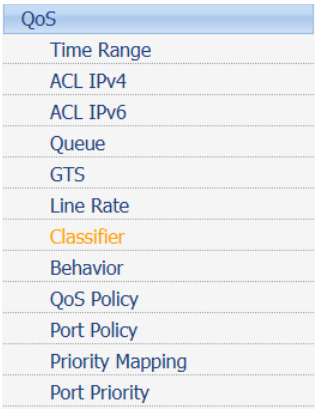
Figura 125 - ACL Basic setup.



Fonte: O autor

10. Vá até o menu **QoS** no canto esquerdo e entre na aba **Classifier**, como é visto na Figura 126.

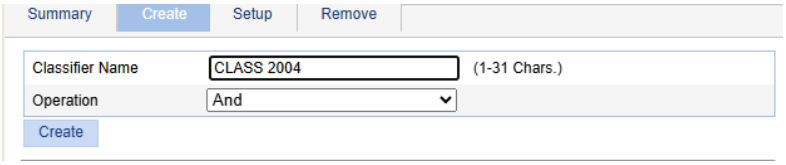
Figura 126 - Classifier no menu QoS.



Fonte: O autor

11. Vá até **create**, escolha um **Classifier Name** e **Operation** como **And**, como é visto na Figura 127.

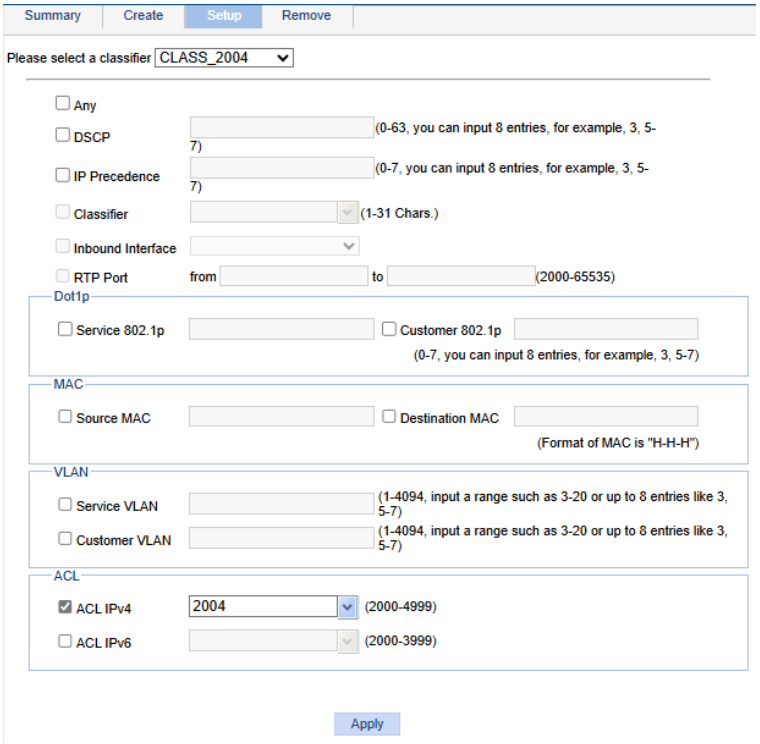
Figura 127 - Criação de um Classifier.



Fonte: O autor

12. Em ***Setup*** selecione a classifier criada anteriormente, ative **ACL IPv4** e selecione a ACL criada anteriormente, como é visto na Figura 128.

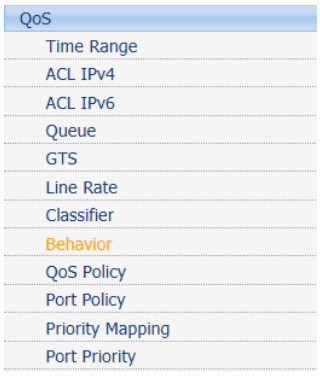
Figura 128 - Setup do Classifier criado.



Fonte: O autor

13. Vá até o menu **QoS** no canto esquerdo e entre na aba **Behavior**, como é observado na Figura 129.

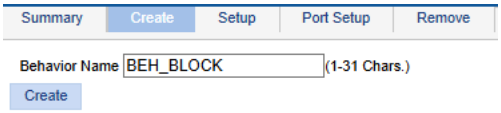
Figura 129 - Behavior no menu QoS.



Fonte: O autor

14. Vá até **Create**, escolha um nome e clique em **create**, de acordo com a Figura 130.

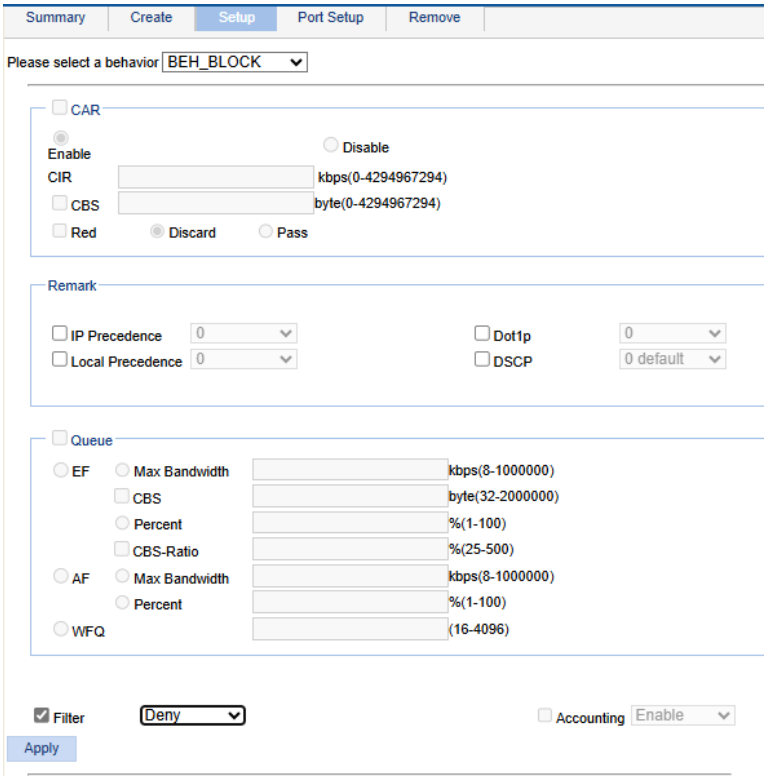
Figura 130 - Criação do behavior.



Fonte: O autor

15. Vá até *Setup* selecione o ***Beahavior*** criado e após isso habilite o **Filter** e selecione **Deny**, como pode ser visto na Figura 131.

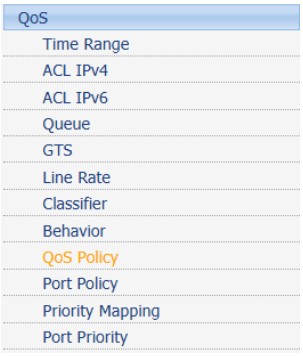
Figura 131 - Setup do behavior criado.



Fonte: O autor

16. Vá até o menu **QoS** no canto esquerdo e entre na aba ***QoS Policy***, como pode ser visto na Figura 132.

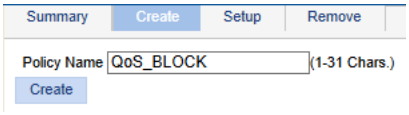
Figura 132 - QoS Policy no menu QoS.



Fonte: O autor

17. Vá até **Create** para criar uma ***QoS Policy*** e escolha o ***Policy Name*** e clique em **Create**, como pode ser visto na Figura 133.

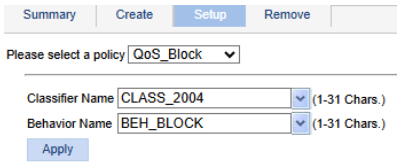
Figura 133 - Criação do QoS Policy.



Fonte: O autor

18. Vá até *Setup* e selecione ***QoS Policy***, ***Classifier Name*** e ***Behavior Name*** criados anteriormente, como mostrado na Figura 134.

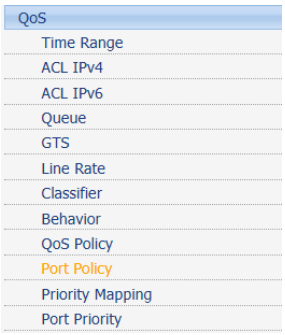
Figura 134 - Setup da QoS policy criada.



Fonte: O autor

19. Vá até o menu **QoS** no canto esquerdo e entre na aba ***Port Policy***, como podemos ver na Figura 135.

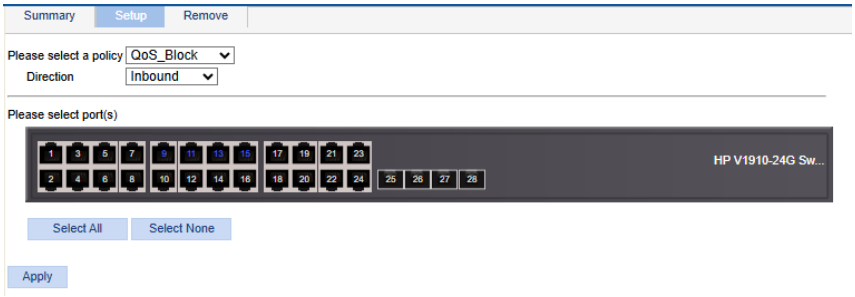
Figura 135 - Port Policy no menu QoS.



Fonte: O autor

20. Vá até ***Setup*** e selecione a ***QoS policy*** criada anteriormente, ***Direction*** como ***Inbound*** e após isso selecione as portas que deseja bloquear nos dias e horários determinados, como pode ser observado na Figura 136.

Figura 136 - Setup da Port Policy criada.



Fonte: O autor

21. Para verificar se as portas estão realmente bloqueadas, basta tentar acessar o link para configuração do *switch* com o computador conectado a porta bloqueada, e então perceba que não é possível acessar o menu de configuração do *switch*.

6 DISCUSSÃO DOS RESULTADOS

No campo de redes de computadores e segurança da informação, a prática e o conhecimento de técnicas avançadas são fundamentais para a criação, manutenção e segurança das infraestruturas de TI. Os roteiros práticos apresentados abordam desde a preparação de dispositivos, como o *Raspberry Pi*, até a configuração de VLANs e controles de tráfego em *switches*, oferecendo uma visão abrangente de habilidades essenciais para profissionais da área de redes.

Estes roteiros cobrem tópicos como instalação e configuração de sistemas operacionais, monitoramento de redes, crimpagem de cabos, gestão de tráfego e segurança, e a criação de soluções personalizadas utilizando o *Raspberry Pi*. Cada um desses processos tem implicações diretas na otimização e segurança de redes locais, corporativas e experimentais.

6.1 RELAÇÃO ENTRE OS ROTEIROS PRÁTICOS

Os roteiros práticos estão interligados e oferecem uma abordagem progressiva para configurar, monitorar e gerenciar redes. Partindo da preparação do Raspberry Pi, que serve como base para diversas aplicações, cada etapa complementa a anterior, avançando para práticas como monitoramento de tráfego, configuração de VLANs e controle de acesso. Essa integração permite ao leitor aplicar os conhecimentos de forma prática e eficiente, criando redes robustas, seguras e adaptadas a diferentes necessidades.

1. **Preparação do *Raspberry Pi* e Gravação do Sistema Operacional**

O primeiro roteiro prático foca na preparação do *Raspberry Pi*, um dispositivo versátil amplamente utilizado em projetos de redes e computação. A instalação e configuração do sistema operacional adequado são cruciais para garantir que o dispositivo funcione corretamente em aplicações como servidores DNS, monitoramento de tráfego, *firewalls* e redes distribuídas. Este processo conecta-se diretamente com outros roteiros, pois fornece a base para o uso de ferramentas como o *Wireshark* para monitoramento de redes e a criação de soluções de rede personalizadas.

2. **Monitoramento de Rede com Wireshark**

O segundo roteiro destaca a utilização do *Wireshark* no *Raspberry Pi* para monitorar e analisar o tráfego de redes. O aprendizado de como capturar e analisar pacotes é vital para identificar problemas de conectividade, otimizar o desempenho da rede e

aumentar a segurança. Esta habilidade complementa a configuração do *Raspberry Pi* (do primeiro roteiro), pois permite que o dispositivo seja utilizado não só para servir, mas também para monitorar e proteger a infraestrutura de rede.

3. Criação de Cabos de Rede e Instalação de Patch Panels

A crimpagem de cabos de rede e a instalação de Patch Panels são habilidades fundamentais para qualquer profissional de redes. Essas práticas garantem que a infraestrutura física de uma rede seja robusta e confiável, evitando falhas de comunicação e melhorando a performance geral. Esses roteiros se conectam com os anteriores ao proporcionar a infraestrutura necessária para a criação de redes eficazes, que podem ser posteriormente monitoradas com ferramentas como o *Wireshark*, ou até mesmo segmentadas com VLANs.

4. Criação e Configuração de VLANs

O gerenciamento de tráfego e a segurança das redes são aprimorados com o aprendizado de como criar e configurar VLANs. As VLANs segmentam o tráfego de rede, aumentando a segurança e a eficiência ao separar diferentes tipos de dados. A configuração de VLANs está diretamente relacionada aos roteiros anteriores, pois otimiza as redes criadas com o *Raspberry Pi* e a infraestrutura de cabeamento, além de garantir maior controle sobre a rede, que pode ser monitorada e protegida com as ferramentas adequadas.

5. Configuração de Roteador Wi-Fi com Raspberry Pi

O *Raspberry Pi*, configurado como roteador Wi-Fi, pode ser uma solução econômica e personalizada para diversos cenários, seja para melhorar a conectividade em áreas domésticas ou para otimizar redes em ambientes corporativos. Este roteiro está relacionado ao uso de tecnologias como o *OpenWrt* e conecta-se com o aprendizado sobre VLANs e monitoramento de redes, pois permite que os profissionais configurem e otimizem as redes Wi-Fi de acordo com as necessidades específicas de segurança e conectividade.

6. Controle de Acesso em Switches (Bloqueio de Portas de Rede)

O último roteiro prático aborda como aplicar controles de tráfego em um *switch*, permitindo o bloqueio de portas em horários específicos. Esse controle é essencial em ambientes corporativos onde a segurança e a gestão eficiente de recursos são prioritárias.

O uso de ACLs, QoS e *Time Range* para gerenciar o tráfego de rede se conecta com todos os roteiros anteriores, pois assegura que as redes e dispositivos configurados (como os *Raspberry Pi* e os cabos de rede) operem de forma segura e eficiente.

O impacto esperado desses roteiros práticos vai além do aprendizado técnico, promovendo competências diretamente aplicáveis a cenários reais em TI. Com abordagens detalhadas, os profissionais são capacitados a lidar com alguns desafios e a implementar soluções eficazes em diferentes contextos, como os que serão descritos abaixo.

A configuração de VLANs e Patch Panels é essencial para a gestão eficiente de grandes redes corporativas, permitindo segmentação de dados e segurança aprimorada ao isolar informações sensíveis. A prática de bloquear portas de rede em horários específicos protege a infraestrutura contra acessos não autorizados.

Utilizar um Raspberry Pi como roteador Wi-Fi, combinado com sistemas como OpenWrt, possibilita a criação de redes sob medida e com custos reduzidos. Essas soluções são ideais para cenários domésticos ou projetos experimentais.

Softwares como Wireshark e conceitos como VLANs são indispensáveis para profissionais de segurança, pois permitem identificar tráfego anômalo, proteger dados e garantir a eficiência na comunicação da rede. Paralelamente, práticas como crimpagem de cabos e instalação de Patch Panels fortalecem a infraestrutura física.

O conhecimento a respeito de crimpagem de cabos e o uso de testadores asseguram uma infraestrutura confiável, simplificando o diagnóstico e a resolução de falhas. Além disso, ferramentas como Wireshark capacitam os profissionais a realizar análises em redes, detectando e corrigindo problemas de forma rápida e precisa.

7 CONCLUSÃO

Os roteiros práticos apresentados oferecem uma formação abrangente e detalhada para profissionais e estudantes da área de redes e segurança de TI. Eles cobrem aspectos essenciais, desde a configuração de dispositivos, passando pela criação de soluções de rede personalizadas, até o gerenciamento de tráfego e segurança de redes corporativas.

Os objetivos propostos para este trabalho foram atingidos de maneira integral, demonstrando a eficácia do planejamento e execução. O primeiro deles, voltado ao estudo de laboratórios de redes de computadores, foi concretizado com destaque para instituições como o SENAI, IFSULDEMINAS e Unoeste. Essas organizações oferecem infraestrutura e metodologias de ensino que promovem uma formação teórica e prática robusta, essencial para a área de redes e segurança de TI.

No que se refere ao segundo objetivo, a análise dos equipamentos no laboratório da UFU proporcionou uma avaliação criteriosa. Foi possível confirmar que os recursos disponíveis atendem plenamente às demandas das atividades práticas, garantindo condições ideais para o desenvolvimento das propostas.

Já a meta de avaliar os equipamentos para a construção dos roteiros práticos foi igualmente concluída. A escolha criteriosa de dispositivos e ferramentas assegurou a execução de atividades alinhadas com as necessidades reais do aprendizado, promovendo experiências didáticas eficazes.

Por fim, a elaboração dos roteiros práticos, etapa final deste trabalho, resultou em um conjunto de atividades abrangentes e bem estruturadas. Ao dominar essas práticas, os profissionais estarão aptos a enfrentar desafios reais e contribuir de maneira significativa para a construção e manutenção de infraestruturas de TI robustas, seguras e eficientes.

Apesar dos resultados positivos, há espaço para melhorias no trabalho desenvolvido. A implementação de mais testes para serem desenvolvidos no *wireshark* por exemplo, aprimoraria ainda mais as possibilidades de aprendizado. Além disso, existe a possibilidade de explorar ainda mais as possibilidades de uso do *raspberry pi*, assim como as possibilidades de configurações do *Switch* HP V1910-24G.

REFERÊNCIA

Alibaba. **D-link Dsl-2740m Roteador Sem Fio N300 Adsl2 + Modem, 4x 10/100 Portas Lan de Ethernet Rápido Pk Tp-link.** Alibaba.com, [s.d.]. Disponível em: https://portuguese.alibaba.com/product-detail/D-Link-DSL-2740M-Wireless-N300-62280319823.html. Acesso em: 13 nov. 2024.

Alura**. Modelo OSI e suas 7 camadas - Protocolos de rede.** Alura, 2023. Disponível em: https://www.alura.com.br/artigos/conhecendo-o-modelo-osi. Acesso em: 9 jun. 2023.

Amazon**. Switch 24 Portas Gigabit 10/100/1000 Tp-link TL-SG1024D.** Amazon.com.br, [s.d.]. Disponível em: https://www.amazon.com.br/Switch-Portas-Gigabit-Tp-link-TL-SG1024D/dp/B07MQ22QWY. Acesso em: 13 nov. 2024.

AWS**. O que é CIDR? - Explicação de blocos e notação CIDR.** AWS, [s.d.]. Disponível em: https://aws.amazon.com/pt/what-is/cidr/. Acesso em: 7 out. 2024.

BRENZINK, Marcelo**. Qual a diferença entre o modelo OSI e o modelo TCP/IP?.** DLtec, [s.d.]. Disponível em: https://www.dltec.com.br/blog/redes/diferenca-entre-modelo-osi-e-tcp-ip/. Acesso em: 13 nov. 2024.

CHAN, Ka Ching; MARTIN, Mary. **An integrated virtual and physical network infrastructure for a networking laboratory.** In: 2012 7th International Conference on Computer Science & Education (ICCSE). [s.l.: s.n.], 2012, p. 1433–1436.

CISCO**. O que é segurança de rede?** Cisco, [s.d.]. Disponível em: https://www.cisco.com/c/pt_br/products/security/what-is-network-security.html. Acesso em: 13 nov. 2024.

CISCO. **What Is Network Management?** Cisco, [s.d.]. Disponível em: https://www.cisco.com/c/en/us/solutions/enterprise-networks/what-is-network-management.html. Acesso em: 13 nov. 2024.

CONWAY, Edwin. **Optical Fiber Communications Principles and Practice.** [s.l.]: Scientific e-Resources, 2019.

CUI, Lin; TSO, Fung Po; YAO, Di, et al. **WeFiLab: A Web-Based WiFi Laboratory Platform for Wireless Networking Education.** IEEE Transactions on Learning Technologies, v. 5, n. 4, p. 291–303, 2012.

CURTI, Luiz**. NASATECNOLOGIA. Tudo sobre Patch Panel: o que é, como instalar e mais.** Disponível em: https://nasatecnologia.com.br/tudo-sobre-patch-panel-o-que-e-como-instalar-e-mais/. Acesso em: 10 out. 2024.

ENTERLIGHT. **Testador de Cabo de Rede UTP Padrão RJ TOZZ 1881.** Disponível em: https://www.enterlight.com.br/testador-de-cabo-de-rede-utp-padrao-rj-tozz-1881/p. Acesso em: 15 out. 2024.

EQUIPE 2000. **Cabo de Rede Patch Cord CAT6 Blindado 5m Azul**. Disponível em: https://www.equipe2000.com.br/cabo-de-rede-patch-cord-cat6-blindado-5m-azul. Acesso em: 15 nov. 2024.

ESCOLA SUPERIOR DE REDES. **Entenda a diferença dos protocolos RIP e OSPF em 10 passos.** ESR, [s.d.]. Disponível em: https://esr.rnp.br/administracao-e-projeto-de-redes/diferenca-protocolos-rip-ospf/. Acesso em: 7 out. 2024.

FISHER, Sharonon**. O que é um TCP/IP e como ele funciona?** Avast, 2019. Disponível em: https://www.avast.com/pt-br/c-what-is-tcp-ip. Acesso em: 13 nov. 2024.

GRATISPNG. **Fibra óptica, Cabo De Fibra óptica, Cabo Elétrico png transparente grátis.** GratisPNG, [s.d.]. Disponível em: https://www.gratispng.com/png-jfshq3/. Acesso em: 22 jun. 2023.

INTEGRA; IFSULDEMINAS. **Laboratório de Redes de Computadores | Integra IFSULDEMINAS.** IFSULDEMINAS, [s.d.]. Disponível em: https://integra.ifsuldeminas.edu.br/portfolio/laboratorios/laboratorio-de-redes-de-computadores-campus-passos-46. Acesso em: 13 nov. 2024.

IT, International**, Topologia de Rede: Conheça os principais tipos."** International IT, 2021. Disponível em: https://www.internationalit.com/post/topologia-de-rede-conheça-os-principais-tipos. Acesso em: 13 nov. 2024.

JAMES, F.; ROSS, Keith W. **Redes de Computadores e a Internet: Uma Abordagem Top-Down.** 6. ed. São Paulo: Pearson Education, 2013.

KRANZ, Maciej. **Building the Internet of Things: Implement New Business Models, Disrupt Competitors, Transform Your Industry.** [s.l.]: John Wiley & Sons, 2016.

KURTZ, Julia**. IPv4 e IPv6: saiba tudo sobre os protocolos de internet. TechTudo, 2020.** Disponível em: **https://www.techtudo.com.br/noticias/2020/10/ipv4-e-ipv6-saiba-tudo-sobre-os-protocolos-de-internet.ghtml.** Acesso em: 21 nov. 2024.

MARSHALL, Perry S.; RINALDI, John S. **Industrial Ethernet.** [s.l.]: ISA, 2017.

MICROCONTROLLERS LAB. **XBee S2C Module Pinout, Applications, Programming & Datasheet**. Disponível em: https://microcontrollerslab.com/xbee-s2c-module-pinout-applications-programming-datasheet/. Acesso em: 13 nov. 2024.

MORENTE, IGOR. **Quais são os principais cabos de rede e suas indicações de uso.** Olhar Digital, 2023. Disponível em: https://olhardigital.com.br/2023/11/03/dicas-e-

tutoriais/quais-sao-os-principais-cabos-de-rede-e-suas-indicacoes-de-uso/#h-cat8. Acesso em: 21 nov. 2024.

OLHAR TEC DIGITAL. **O que é: Subnet.** Olhar Tec Digital, [s.d.]. Disponível em: https://olhartecdigital.com/glossario/o-que-e-subnet/. Acesso em: 7 out. 2024.

OLIVEIRA, Euler. **Conhecendo a placa WiFi LoRa ESP32 433MHz 868MHz 915MHz.** Blog MASTERWALKER SHOP, [s.d.]. Disponível em: https://blogmasterwalkershop.com.br/embarcados/esp32/conhecendo-a-placa-wifi-lora-esp32-433mhz-868mhz-915mhz. Acesso em: 21 nov. 2024.

OPENCLIPART. **24p patch panel.** Free SVG, [s.d.]. Disponível em: https://freesvg.org/24p-patch-panel. Acesso em: 13 nov. 2024.

PERLMAN, Radia. **Interconnections: Bridges, Routers, Switches, and Internetworking Protocols.** [s.l.]: Addison-Wesley Professional, 2000.

PETERSON, Larry L.; DAVIE, Bruce S. **Computer Networks: A Systems Approach.** 5. ed. [s.l.]: Morgan Kaufmann, [s.d.].

PNG WING. **Free PNG: Download Transparent Images**. Disponível em: https://www.pngwing.com/en/free-png-cgxyu/download. Acesso em: 15 nov. 2024.

POKORNÝ, Martin; ZACH, Petr. **Design, implementation and security of a typical educational laboratory computer network.** Acta Universitatis Agriculturae et Silviculturae Mendelianae Brunensis, v. 61, n. 4, p. 1077–1087, 2013. Disponível em: http://acta.mendelu.cz/doi/10.11118/actaun201361041077.html. Acesso em: 13 nov. 2024.

PROGRAMAE. **SOFTWARE. O que é NAT (Network Address Translation) e para que serve?.** Programaê, [s.d.]. Disponível em: https://programae.org.br/termos/glossario/o-que-e-nat-network-address-translation-e-para-que-serve/. Acesso em: 7 out. 2024.

RACKFORT. **Rack servidor fechado 44U x 570mm**. Disponível em: https://www.rackfort.com.br/rack-fechado/rack-servidor-fechado-44u-x-570mm. Acesso em: 18 nov. 2024.

RAPPAPORT, Theodore S. **Wireless Communications: Principles and Practice.** [s.l.]: Prentice Hall PTR, 2002.

REDAÇÃO. **Cinco sistemas operacionais para usar no Raspberry Pi.** TechTudo, 2016. Disponível em: https://www.techtudo.com.br/noticias/2016/09/cinco-sistemas-operacionais-para-usar-no-raspberry-pi.ghtml. Acesso em: 29 out. 2024.

REDAÇÃO. **Como crimpar um cabo de rede Ethernet Cat6 com o alicate RJ-45.** TechTudo, 2017. Disponível em: https://www.techtudo.com.br/noticias/2017/03/como-crimpar-um-cabo-ethernet-de-qualquer-comprimento.ghtml. Acesso em: 29 out. 2024.

REDAÇÃO. **Ferramenta que simula ataques ajuda a identificar vulnerabilidades na rede.** Security Report, 2020. Disponível em: https://www.securityreport.com.br/ferramenta-que-simula-ataques-ajuda-a-identificar-vulnerabilidades-na-rede/. Acesso em: 21 jun. 2023.

SANDERS, Chris. **Practical Packet Analysis, 3rd Edition: Using Wireshark to Solve Real-World Network Problems.** [s.l.]: No Starch Press, 2017.

SANG, Janche. **Hands-on laboratory experiments with SOHO networking technologies: HANDS-ON NETWORKING EXPERIMENTS.** Computer Applications in Engineering Education, v. 21, n. 4, p. 586–595, 2013. Disponível em: https://onlinelibrary.wiley.com/doi/10.1002/cae.20503. Acesso em: 13 nov. 2024.

SENAI**. Laboratório de Redes de Computadores."** Senai, [s.d.]. Disponível em: https://www.senairs.org.br/laboratorio-de-redes-de-computadores. Acesso em: 21 jun. 2023.

SPURGEON, Charles E.; ZIMMERMAN, Joann. **Ethernet Switches.** [s.l.]: O'Reilly Media, Inc., 2013.

STEWART, J. Michael; KINSEY, Denise. **Network Security, Firewalls, and VPNs.** [s.l.]: Jones & Bartlett Learning, 2020.

TANENBAUM, Andrew; FEAMSTER, Nick; WETHERALL, David. **Redes de Computadores.** [s.l.]: Bookman Editora, 2021.

TEBALDI, Pedro. **Protocolos de Rede | Conheça os principais protocolos e suas aplicações!.** OP Services, 2019. Disponível em: https://www.opservices.com.br/protocolos-de-rede/. Acesso em: 13 nov. 2024.

TECHSUL ELETRÔNICOS. **XBee Pro Shield para Arduino**. Disponível em: https://techsuleletronicos.com.br/product/xbee-pro-shield-para-arduino/. Acesso em: 13 nov. 2024.

TORRES, Gabriel. **Redes Wi-Fi.** 2. ed. [s.l.]: Clube do Hardware, [s.d.].

UNBOXING TOMORROW. **Project: Installing Wireshark on Raspberry Pi.** Disponível em: https://unboxing-tomorrow.com/project-installing-wireshark-on-raspberry-pi/. Acesso em: 13 nov. 2024.

UNOESTE**. Laboratórios - Redes de Computadores - Unoeste.** Unoeste, [s.d.]. Disponível em: https://www.unoeste.br/graduacao/faculdade-de-redes-computadores/laboratorios. Acesso em: 13 nov. 2024.

WOODWARD, Bill. **Cabling: The Complete Guide to Copper and Fiber-Optic Networking.** [s.l.]: John Wiley & Sons, 2014.