INSTITUTO DE ENSINO SUPERIOR - FACULDADE LABORO
TECNÓLOGO EM REDES DE COMPUTADORES

THOMAS DHOWSEPHT OLIVEIRA SALES

IMPLANTAÇÃO DE INFRAESTRUTURA DE REDE

Ambiente de laboratório informatizado para instituição de ensino

TRABALHO DE CONCLUSÃO DE CURSO

SÃO LUÍS – MA
2019

THOMAS DHOWSEPHT OLIVEIRA SALES

IMPLANTAÇÃO DE INFRAESTRUTURA DE REDE

Ambiente de laboratório informatizado para instituição de ensino

Trabalho de Conclusão de Curso apresentado ao Curso Tecnólogo em Redes de Computadores da Faculdade Laboro, para obtenção do título de Tecnólogo em Redes de Computadores.

Orientador: Prof. Esp. Carlos Rayllan Lima Sousa

SÃO LUÍS - MA
2019

THOMAS DHOWSEPHT OLIVEIRA SALES

Trabalho de Conclusão de Curso apresentado ao Curso Tecnólogo em Redes de Computadores da Faculdade Laboro, para obtenção do título de Tecnólogo em Redes de Computadores.

Aprovado em: / /

BANCA EXAMINADORA

_____

Prof. Esp. Carlos Rayllan Lima Sousa (Orientador)

_____

Prof. Ms. Milson Louseiro Lima

_____

Prof. Ms. Yanna Leidy Ketley Fernandes Cruz

AGRADECIMENTOS

Agradeço ao meu orientador Prof. Esp. Carlos Rayllan Lima Sousa, pela sabedoria e paciência com que me guiou nesta trajetória. A instituição, pelo auxílio e resolução das dúvidas. Aos meus colegas de trabalho na área e sala de aula, que percorreram juntos comigo esse longo caminho de desafios, mas também de muita ajuda mútua e incentivo. Gostaria de deixar mencionado também, o meu reconhecimento à minha família. Sendo assim, portanto fica registrado meus agradecimentos a todos os que contribuíram das mais diversas maneiras para a realização desta pesquisa.

“Os computadores são incrivelmente rápidos, precisos e burros; os homens são incrivelmente lentos, imprecisos e brilhantes; juntos, seus poderes ultrapassam os limites da imaginação.”

(Albert Einstein)

RESUMO

OLIVEIRA, Thomas Dhowsepht. **Implantação de infraestrutura de rede:** Ambiente de laboratório informatizado para instituição de ensino. 2019. 20 f. Trabalho de Conclusão de Curso (Graduação) – Tecnólogo em Redes de Computadores. Instituto de Ensino Superior – Faculdade Laboro. São Luís - MA, 2019.

Hoje em dia desde grandes, médias e pequenas empresas, instituições do governo, de ensino, lugares públicos como shoppings, aeroportos, bares, até as casas das pessoas comuns, as redes de computadores permitem que dispositivos se comuniquem com outros próximos, ou outros há milhares de km de distância, com cada vez mais velocidade e alta capacidade de transmissão de dados, de forma transparente ao usuário. Aliados a dispositivos finais com cada vez mais capacidade de processamento, todos estamos acostumados a estarmos conectados, gerando, disponibilizando e consumindo conteúdo com cada vez mais praticidade e rapidez, por meio dessa tecnologia que está presente fortemente em nossa vida. Citando a própria internet como um exemplo maior, que é um resultado das muitíssimas redes que se conectam entre si, devemos lembrar e ressaltar que por trás de tudo isso existe uma necessidade da existência de uma infraestrutura de rede, possibilitando o uso das funcionalidades de rede que tanto conhecemos e estamos habituados a usar, como e-mail, redes sociais, streaming de vídeo, jogos online, etc. E como a área de redes de computadores faz parte das ciências exatas, há uma série de padrões, métodos e tecnologias a serem seguidas na hora de se implantar uma infraestrutura desse tipo. Portanto este trabalho ressalta a importância deste tipo de conteúdo, trazendo uma visão geral para melhor compreensão de como implantar uma infraestrutura de rede de computadores em um laboratório de informática em uma instituição de ensino, provendo serviços de rede e compartilhamento de recursos com finalidade educacional para uso de seus alunos e professores, atendendo os padrões, requisitos, boas práticas e recomendações para se montar uma rede que atenda este propósito, sendo confiável.

Palavras-chave: Redes de computadores. Dispositivos. Internet. Infraestrutura de rede. Tecnologias.

ABSTRACT

OLIVEIRA, Thomas Dhowsepht. **Network Infrastructure Deployment:** Computer Labs for Education. 2019. 20 f. Trabalho de Conclusão de Curso (Graduação) – Tecnólogo em Redes de Computadores. Instituto de Ensino Superior – Faculdade Laboro. São Luís - MA, 2019.

Today, from large, medium and small businesses, government institutions, schools, public places such as shopping malls, airports, bars, to people's homes, computer networks allow devices to communicate with others nearby, or others. Thousands of kilometers away, with ever-increasing speed and high data transmission capacity, transparently to the user. Coupled with end-to-end processing devices, we are all used to being connected, generating, making available and consuming content more and more quickly and easily through this technology that is strongly present in our lives. Citing the Internet itself as a larger example, which is a result of the many networks that connect to each other, we must remember and point out that behind all this there is a need for a network infrastructure, enabling the use of network functionality. that we know so much about and are used to, such as email, social networking, video streaming, online games, etc. And because computer networking is part of the exact sciences, there are a number of standards, methods, and technologies to follow when deploying such an infrastructure. Therefore this paper underscores the importance of this type of content, providing an overview for a better understanding of how to deploy a computer network infrastructure in a computer lab in an educational institution, providing educational networking and resource sharing services for use of its students and teachers, meeting the standards, requirements, good practices and recommendations to build a network that serves this purpose and is reliable..

Keywords: Network. Internet. Devices. Infrastructure. Services.

LISTA DE FIGURAS E ILUSTRAÇÕES

LISTA DE ABREVIATURA E SIGLAS

LAN – Local Area Network

TI – Tecnologia da Informação

EAD – Ensino a Distância

MAN – Metropolitan Area Network

WAN – Wide Area Network

PAN – Personal Area Network

CAN – Campus Area Network

ISP – Internet Service Provider

FDDI – Fiber Distributed Data Interface

ATM – Asynchronous Transfer Mode

Gbps – Gigabit por Segundo

OSI – Open System Interconnection

UTP – Unshielded Twisted Pair

FTP – Foiled Twisted Pair

STP – Shielded Twisted Pair

SSTP – Screened Shielded Twisted Pair

EIA – Electronics Industries Alliance

TIA – Telecomunications Industry Association

WLAN – Wireless LAN

LED – Light Emitter Diode

POE – Power Over Ethernet

IEEE – Institute of Electrical and Electronic Engineers

WI-FI – Wireless Fidelity

BSS – Basic Service Set

SSID – Service Set ID

ESS – Extended Service Set

MAC – Media Acess Control

WEP – Wired Equivalent Privacy

WPA – Wi-fi Protected Acess

TKIP – Temporal Key Integrity Protocol

WPA2 – Wi-fi Protected Acess 2

AES – Advanced Encryption Standard

RADIUS – Remote Authentication Dial In User Service

GHz – Gigahertz

MHz – Megahertz

MIMO – Multiple Input Multiple Output

WPS – Wi-fi Protected Setup

PIN – Personal Identification Number

DHCP – Dynamic Host Configuration Protocol

QOS – Quality of Service

NTP – Network Time Protocol

IPV4 – Internet Protocol Version 4

SUMÁRIO

1 INTRODUÇÃO

Hoje nós vivemos na era da informação. Não se depende mais somente da tv ou do rádio como veículo de informação. Com a existência das redes de computadores, ou melhor...redes de dispositivos, que conectados formam a tão conhecida internet, qualquer um pode ter uma informação na palma da mão, buscando-a onde quer que ela esteja, em praticamente qualquer lugar.

Empresas, instituições, casas, aeroportos, bares, etc. em quase todos os lugares existe uma rede que oferece acesso a serviços e recursos tão usados pela população, resultado de muita demanda por essa tecnologia. Começando pelo acesso massificado aos computadores, passando por smartphones cada vez mais poderosos, com maior capacidade de processamento, até a eletrodomésticos com capacidade de se comunicarem com servidores na internet, buscando e exibindo informações em tempo real.

Adota-se e demanda-se cada vez mais por essa tecnologia, pois descobriu-se já há um bom tempo o potencial que ela traz. Podendo ser usada para diversos fins, desde uma loja que além de venda física também aumenta o faturamento no fim do mês com vendas virtuais por conta de um site próprio na internet, ou um bar que atrai mais clientes por conta de uma boa conexão de internet e reserva de mesas por meio de um aplicativo, até uma instituição de ensino que tenha mais matrículas em detrimento de outra concorrente, por ter um sistema moderno e eficiente de ensino a distância que esteja disponível 24 horas por dia sem quedas e instabilidades, a serviço de seus alunos e professores.

Isso são só alguns simples exemplos, não precisando de muitos deles para que todos possam concordar que essa tecnologia se faz cada vez mais necessária na vida da sociedade. E, portanto, a demanda e dependência por ela só aumenta. E com a expansão das redes de computadores, mais dispositivos conectados, mais complexas essas redes ficam. Com dispositivos finais cada vez mais poderosos, mais inteligentes, aplicações cada vez mais complexas e exigentes, arquivos de dados cada vez mais maiores, a necessidade por redes robustas, eficientes e seguras se faz cada vez mais presente para suportar toda essa demanda, pois a tendência é cada vez mais crescimento.

E por trás de uma rede com tais características, existe toda uma infraestrutura necessária. Desde o cuidado com a escolha dos elementos passivos, mais simples, como cabo, conectores, tomadas, até a escolha dos elementos ativos da rede, como os switchs, roteadores, modens, de acordo com o cenário e das tecnologias contidas nos mesmos, além das corretas configurações desses equipamentos para se extrair melhor operação e eficiência.

Este trabalho traz uma visão geral de uma implementação de uma infraestrutura de rede LAN (Local Area Network) cabeada e sem fio, em um laboratório de informática situado no prédio de uma faculdade X. O objetivo é servir como material de referência e de boas práticas para estudantes e profissionais da área de redes em tecnologia da informação, para posteriores consultas. Também servirá como um guia para quem estiver começando na área de infraestrutura de TI (Tecnologia da Informação), mostrando em detalhes os materiais, equipamentos e principais configurações necessárias para se montar uma rede de computadores pequena e torná-la operacional e eficiente, minimizando-se os eventuais problemas.

1.1 Problema

A Faculdade X precisa de uma infraestrutura de rede para implementação de um laboratório de informática, para realização de tarefas como: pesquisa de conteúdo na internet, acesso ao sistema de notas e ambiente EAD (Ensino a Distância) da instituição, atividades de simulação usando softwares de rede, downloads de softwares, compartilhamento de arquivos, etc. Esses laboratórios serão usados para aulas, cursos, exercícios e testes na área de redes de computadores, devendo fornecer uma rede cabeada e wireless (sem fio) que suporte a demanda de tráfego de todos os dispositivos dos alunos e professores, e que ofereça uma internet de qualidade, com banda e velocidade final suficiente para atender as necessidades dos alunos e professores no laboratório.

1.2 Justificativa

Onde há uma rede, existe uma infraestrutura física e lógica montada e configurada para possibilitar a comunicação e compartilhamento de recursos. Desde grandes, médias e pequenas empresas, instituições do governo, de ensino, locais públicos, até as casas das pessoas comuns, existem essas redes que oferecem muitos recursos e possibilitam uma infinidade de funções necessárias nos ambientes de nosso dia-a-dia. Todos estão dependentes delas, porque no mundo de hoje se depende muito de acesso e compartilhamento de dados informatizados. Por tudo que foi citado acima, há a importância e necessidade do aprendizado de como se implementar uma boa infraestrutura de rede, seguindo padrões, métodos e técnicas conhecidas.

1.2.1 Viabilidade

O projeto é totalmente viável pois a instituição necessita deste novo laboratório de informática com mais espaço e capacidade para atender melhor seus alunos e professores, garantindo mais satisfação aos mesmos. Além da sala estar vazia, com acabamento e instalações elétricas finalizadas, somente à espera do início do projeto.

1.2.2 Importância

O projeto tem sua importância justificada pelo fato do prédio da instituição de ensino ser da área de redes de computadores, exigindo-se assim que o mesmo ofereça um laboratório de qualidade para exercícios práticos, testes e pesquisas, para melhor aprendizado e qualidade de ensino de seus alunos e professores

1.3 OBJETIVOS

1.3.1 Geral

O objetivo deste projeto consiste em entregar uma infraestrutura de rede em um laboratório de informática no mesmo prédio para a faculdade X, considerando-se que a sala esteja finalizada, com todo acabamento e instalação elétrica pronta. Considerando-se que todo o material necessário para completa realização deste trabalho foi comprado e entregue, estando à disposição para o início do serviço. Incluindo também todos os 30 computadores, com seus respectivos periféricos e acessórios necessários, previamente comprados e entregues pela instituição, com seus sistemas operacionais e licenças previamente instalados pelo fabricante. Sendo assim limitando este trabalho a descrição dos métodos para implantação da infraestrutura de rede nos laboratórios e configuração do roteador e computadores, assim resultando em uma LAN totalmente funcional.

Executando-se as boas práticas na área de TI, e cumprindo com os requisitos estipulados pela instituição, almeja-se que a rede local seja de fácil e baixa necessidade de manutenção, assim como o seu cabeamento de grande vida útil. Também é esperado que a rede suporte alta capacidade de tráfego, sendo robusta, livre de interferências, segura, eficiente e escalável. Entregando uma rede local com todas essas características, podemos assim considerar que o produto final atende as necessidades do cenário proposto, sendo cumprido o propósito deste trabalho.

1.3.2 Específicos

- Abordar teoricamente as redes de computadores, dando ênfase na tecnologia padrão de arquitetura física e topologia de rede que foram usadas neste trabalho.

- Descrever os materiais que foram usados, recomendações a respeito dos mesmos, assim como técnicas de instalações desses materiais, equipamentos usados que auxiliam o profissional da área, além de noções de cabeamento estruturado e sua importância.

- Abordar teoricamente a importância e necessidade do surgimento e uso das redes sem fio, fazendo uma comparação com as redes cabeadas, e de maneira simples, conceitos conhecidos e tão importantes neste tipo de rede, como criptografia, frequências e padrões.

- Descrever passo-a-passo, fazendo uso de capturas de tela, as configurações aplicadas na criação da rede sem fio para o ambiente do laboratório, além de recomendações para aumento de desempenho e segurança da mesma.

- Descrever passo-a-passo, fazendo uso de capturas de tela, as principais configurações de rede aplicadas no sistema operacional Windows 10, instalado nos computadores de mesa do laboratório.

1.4 Hipótese

Fazendo um correto dimensionamento da rede, implementando uma infraestrutura de rede que atenda os 30 computadores de mesa no ambiente do laboratório, com 40 pontos de rede levando-se já em conta uma margem de escalabilidade, seguindo as boas práticas, com cabeamento categoria 6A de um bom fabricante, tomadas e conectores de qualidade, switch gigabit de 48 portas, e um roteador que trabalhe no padrão 802.11 AC + 802.11 N simultaneamente para dispositivos sem fio dos alunos e professores, instalado de forma centralizada no ambiente de cada sala do laboratório, espera-se que seja suficiente para atender de forma satisfatória os usuários da rede, cumprindo com o propósito deste trabalho.

1.5 Estrutura do texto

Este trabalho apresenta-se dividido em 6 capítulos. Onde há uma introdução que alega a importância cada vez maior das redes de computadores e internet nas vidas das pessoas, causando cada vez maior demanda, justificando a necessidade de infraestrutura de rede para sustentar essas redes, para continuidade dos recursos e serviços tão demandados pela sociedade. Além de apresentar o problema a ser discutido no trabalho, a justificativa que permite a existência do mesmo e os objetivos gerais e específicos almejados.

O Capítulo 2 apresenta uma visão geral das redes de computadores, internet e sua indiscutível importância, além dos tipos de redes mais comuns classificas por área de abrangência, somado há conceitos embasados através de referencial teórico construído a partir de obras de autores consagrados e renomados na área.

O Capítulo 3 destina-se as redes cabeadas, dando uma visão geral sobre a arquitetura e topologia mais usada em uma rede local, noções de cabeamento estruturado, além dos detalhes na escolha de materiais, métodos e técnicas empregadas para instalação dos equipamentos e manuseio dos equipamentos.

O Capítulo 4 destina-se as redes sem fio, dando uma visão geral sobre elas, sua importância, padrões adotados e conhecidos, além das principais configurações adotadas em um roteador sem fio.

O Capítulo 5 destina-se as principais configurações de rede adotadas nos computadores de mesa, usando sistema operacional Windows 10.

O Capítulo 6 apresenta as conclusões e resultados esperados ao se seguir os passos e recomendações dos capítulos anteriores.

2 REDES DE COMPUTADORES: VISÃO GERAL

2.1 REDES DE COMPUTADORES E A INTERNET

As redes de computadores foram pensadas para cumprir o objetivo de possibilitar que dispositivos pudessem se comunicar entre si, gerando também o compartilhamento de recursos. Essas redes evoluíram muito ao longo das décadas, e atestaram o seu valor e importância já há bastante tempo. Hoje em dia seja nas organizações, instituições, casas, e lugares públicos, as redes com acesso à internet estão presentes, pois “à medida que cresce nossa capacidade de colher, processar e distribuir informações, torna-se ainda maior a demanda por formas mais sofisticadas de processamento de informação.” (TANENBAUM, 2011, p. 1)

Resultado da maior expansão e crescimento a nível mundial das redes e internet, estamos mais que acostumados a usufruir de seus benefícios, através de seus recursos, serviços e aplicações por meio de uma variedade de dispositivos finais diferentes, não somente computadores.

> A Internet é uma rede de computadores que interconecta centenas de milhões de dispositivos de computação ao redor do mundo. Há pouco tempo, esses dispositivos eram basicamente PCs de mesa, estações de trabalho Linux, e os assim chamados servidores que armazenam e transmitem informações, como páginas da Web e mensagens de e-mail. No entanto, cada vez mais sistemas finais modernos da Internet, como TVs, laptops, consoles para jogos, telefones celulares, webcams, automóveis, dispositivos de sensoriamento ambiental, quadros de imagens, e sistemas internos elétricos e de segurança, estão sendo conectados à rede. Na verdade, o termo rede de computadores está começando a soar um tanto desatualizado, dados os muitos equipamentos não tradicionais que estão sendo ligados à Internet. No jargão da rede, todos esses equipamentos são denominados hospedeiros ou sistemas finais. (KUROSE, ROSS, 2013, p. 3)

As redes estão tão presentes hoje em dia em nossas vidas e nas atividades do cotidiano, que muitas vezes nem mesmos percebemos quando estamos diante de uma delas.

> Mesmo fora do ambiente da explícito da informática, todos nós temos contato com algum tipo de rede em maior ou menor grau. Caixas eletrônicos de bancos são o maior exemplo: cada terminal não passa de um computador ligado a um computador central que armazena as informações de sua conta. Quem vive nos grandes centros se depara com redes de computadores em supermercados, farmácias e inúmeros outros lugares – na maioria das vezes nem mesmo percebendo que está diante de uma rede de computadores.
>
> (TORRES, 2016, p. 4)

Dispositivos trocam dados com outros dispositivos constantemente, de maneira até transparente para os usuários, sempre enviando e recebendo dados.

> Na internet, então, essa troca de informações armazenadas remotamente é levada ao extremo: acessamos dados armazenados nos locais mais remotos e, na maioria das vezes, o local onde os dados estão fisicamente armazenados não tem a menor importância para o usuário.
>
> (TORRES, 2016, p. 5)

Cada vez mais os dispositivos são projetados e fabricados para funcionarem conectados. A internet das coisas é um grande exemplo que atesta que as redes estão enraizadas na vida em sociedade.

2.1.1 TIPOS DE REDE E ÁREAS DE ABRANGÊNCIA

E para sustentar tudo isso, existem redes de muitos modelos, tamanhos e tecnologias distintas. Redes podem ser classificadas de diversas formas diferentes. Mas uma forma geral de classifica-las é de acordo com o tamanho da área geográfica que elas abrangem, como a LAN (Local Area Network), MAN (Metropolitan Area Network) e WAN (Wide Area Network). Existem outras classificações, como PAN (Personal Area Network – Rede de Area Pessoal), CAN (Campus Area Network – Rede de campo), consideradas por outros autores da área. Mas este trabalho vai focar nestas três abaixo, que são as principais e consideradas em todas as obras na área.

> Uma rede local (LAN – Local Area Network) geralmente é uma propriedade privada e conecta alguns hosts em um único escritório, prédio ou campus. Dependendo das necessidades de uma organização, uma LAN pode ser simples com apenas dois computadores e uma impressora no escritório da casa de alguém, ou pode se estender por toda a empresa e incluir dispositivos de áudio e vídeo. Cada host em uma LAN possui um identificador, ou seja, um endereço que o define de forma unívoca na LAN.
>
> (FOROUZAN, MOSHARRAF, 2013, p. 2)

Dando prosseguimento, as redes MAN (Metropolitan Area Network) são redes que se estendem e abrangem uma área metropolitana como de uma cidade. Para melhor entendimento, pode-se citar como exemplo, o de uma empresa em que sua matriz se localiza na mesma cidade de suas filiais, e se comunica com elas. Pode-se considerar esse tipo de rede como uma interligação de várias redes LAN distintas em lugares diferentes dentro de uma grande área.

> MAN (Metropolitan Area Network): rede metropolitana, uma rede maior do que a rede de campo, podendo até abranger uma cidade inteira. Na rede de campo os prédios que fazem parte da rede estão relativamente próximos uns dos outros e o cabeamento entre eles é normalmente feito pela própria empresa. No caso das redes metropolitanas, os prédios podem estar distantes uns dos outros – em bairros diferentes, por exemplo. Tradicionalmente a conexão entre as redes locais ou de campo que compõe uma rede metropolitana é feita contratando-se uma concessionária de telecomunicações [...] (TORRES, 2016, p. 7)

Já as redes WAN (Wide Area Network) são redes de alcance e abrangência global, tendo como melhor exemplo a internet. São formadas por uma interconexão de várias redes MAN, e dispositivos de conexão como roteadores, switches e modens

que operam no núcleo das redes de cada ISP (Internet Service Provider), que são conectados uns aos outros e espalhados por todo o globo.

Essas redes são interligadas para formar uma rede maior, a internet, que é o maior exemplo que se pode dar da interconexão de diferentes tipos de redes.

> Uma rede de longa distância (WAN – Wide Area Network) é também uma interligação de dispositivos capazes de se comunicar. No entanto, existem algumas diferenças entre uma LAN e uma WAN. A LAN normalmente tem tamanho limitado, estendendo-se por um escritório, edifício ou campus, enquanto uma WAN tem uma extensão geográfica maior, abrangendo uma cidade, um estado, um país, ou mesmo o mundo. Uma LAN interliga hosts; uma WAN interliga dispositivos de conexão como switches, roteadores ou modems. Uma LAN normalmente é propriedade privada da organização que a utiliza; uma WAN, por sua vez, costuma ser criada e operada por empresas de comunicação e alugada por uma organização que a utiliza.
>
> (FOROUZAN, MOSHARRAF, 2013, p. 33)

O foco deste trabalho será na rede do tipo LAN (Local Area Network), pois a infraestrutura de nossa rede estará limitada somente ao prédio da faculdade X. Sendo assim, vamos entrar em detalhes sobre o que é necessário para se formar uma LAN, usando a arquitetura ethernet e a topologia estrela, que são mais populares e de uso mais comum.

3 REDE CABEADA DO LABORATÓRIO: CONCEITOS E PRÁTICA

3.1 ARQUITETURA ETHERNET

Em primeiro lugar, deve-se mencionar e explicar resumidamente a arquitetura e topologia da rede. Como já citado, a arquitetura mais popular de uso massificado nas redes locais hoje é a arquitetura ethernet.

A ethernet é um padrão de rede local, surgido dentro de um laboratório de desenvolvimento da empresa XEROX, de nome PARC. Fruto do trabalho de dois pesquisadores, de nome Bob Metcalfe e David Boggs, usava cabos coaxiais para conectar os computadores e assim formar uma rede, tornando possível a comunicação entre eles, embora a uma baixa velocidade.

Em 1973 foi feito o primeiro teste de transmissão de dados usando o padrão ethernet. Sua velocidade era de apenas 2.94 megabits.

> A tecnologia de LAN Ethernet foi desenvolvida em 1970 por Robert Metcalfe e David Boggs. Desde então, ela passou por quatro gerações: Ethernet Padrão (10 Mbps), Fast Ethernet (100 Mbps), Ethernet Gigabit (1 Gbps) e 10 Gibabit Ethernet (10 Gbps). (FOROUZAN, MOSHARRAF, 2013, p. 422)

Na história da evolução do padrão ethernet, houve muitos outros padrões de rede local concorrentes na sua história, como token ring, FDDI e ATM. Para evitar uma derrota para esses padrões, o padrão ethernet sempre evoluía e crescia em velocidade. Dos 2.94 mbps (megabits por segundo) do primeiro teste em 1973, até na casa dos Gbps (gigabits por segundo), como é possível nos dias de hoje. Além disso, houve outros motivos que também foram responsáveis pela sua permanência no mercado e justificativa da adoção do padrão frente a seus concorrentes.

> Há muitas razões para o sucesso da Ethernet. Primeiro, ela foi a primeira LAN de alta velocidade amplamente disseminada. Como foi disponibilizada cedo, os administradores de rede ficaram bastante familiarizados com a Ethernet — com suas maravilhas e sutilezas — e relutaram em mudar para outras tecnologias LAN quando estas apareceram em cena. Segundo, token ring, FDDI e ATM são tecnologias mais complexas e mais caras do que a Ethernet, o que desencorajou ainda mais os administradores na questão da mudança. Terceiro, a razão mais atraente para mudar para uma outra tecnologia LAN (como FDDI e ATM) era em geral a velocidade mais alta da nova tecnologia; contudo, a Ethernet sempre se defendeu produzindo versões que funcionavam a velocidades iguais, ou mais altas. E, também, a Ethernet comutada foi introduzida no início da década de 1990, o que aumentou ainda mais suas velocidades efetivas de dados. Por fim, como se tornou muito popular, o hardware para Ethernet (em particular, adaptadores e comutadores) passou a ser mercadoria comum, de custo muito baixo.
>
> (KUROSE, ROSS, 2013, p. 348)

> Exceto pela Ethernet, quase todas as tecnologias de LAN desapareceram do mercado porque a Ethernet foi capaz de se atualizar para atender as necessidades de cada época. Várias razões para esse sucesso são mencionadas na literatura, mas acreditamos que o protocolo Ethernet foi projetado para que ele fosse capaz de evoluir com a demanda por maiores taxas de transmissão. É natural que uma organização que usava uma LAN Ethernet no passado e agora precisava de uma taxa de dados mais elevada preferisse fazer a atualização para a nova geração em vez de migrar para outra tecnologia, algo que pode envolver maiores custos.
>
> (FOROUZAN, MOSHARRAF, 2013, p. 422)

3.2 TOPOLOGIAS DE REDE

Uma topologia de rede descreve como uma rede está disposta fisicamente, além de como o fluxo de dados nela trafega. Existem dois tipos de topologias; a física e a lógica. Uma rede pode ter uma topologia lógica que difere de sua topologia física.

A topologia física diz respeito a como a rede está organizada, estruturada, em como ela se parece fisicamente. Ou seja, refere-se ao seu layout físico. Já a topologia lógica diz respeito a como a rede trafega seu fluxo de dados internamente.

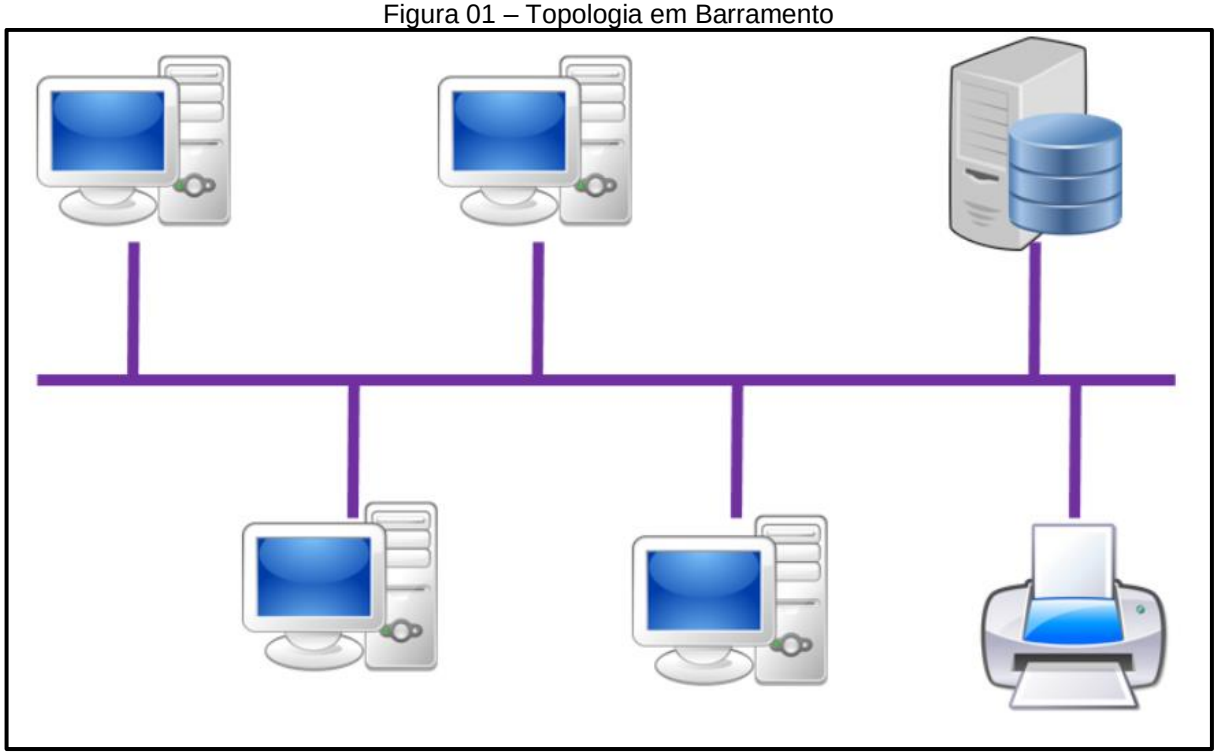
O tipo de topologia usada em uma rede impacta no tipo de hardware usado, nas possibilidades de expansão futura dessa rede, além de seu gerenciamento.

Abaixo estão listadas as principais topologias de rede, acompanhadas de uma breve explicação sobre elas.

3.2.1 TOPOLOGIA BARRAMENTO

É uma topologia antiga, usada nos primórdios das redes de computadores. Consiste em um único meio de transmissão dos dados, que se dá por meio de um cabo que liga todos os dispositivos pertencentes a uma rede. Suas maiores desvantagens são gerar broadcast desnecessário toda vez que um dispositivo envia um dado para outro, pois todos os outros dispositivos também recebem esses dados, além de que se houver um rompimento no cabo, que é o único meio de transmissão e recepção de dados na rede, toda a rede cai. Com o surgimento de outras topologias melhores, essa topologia caiu em desuso.

Figura 01 – Topologia em Barramento

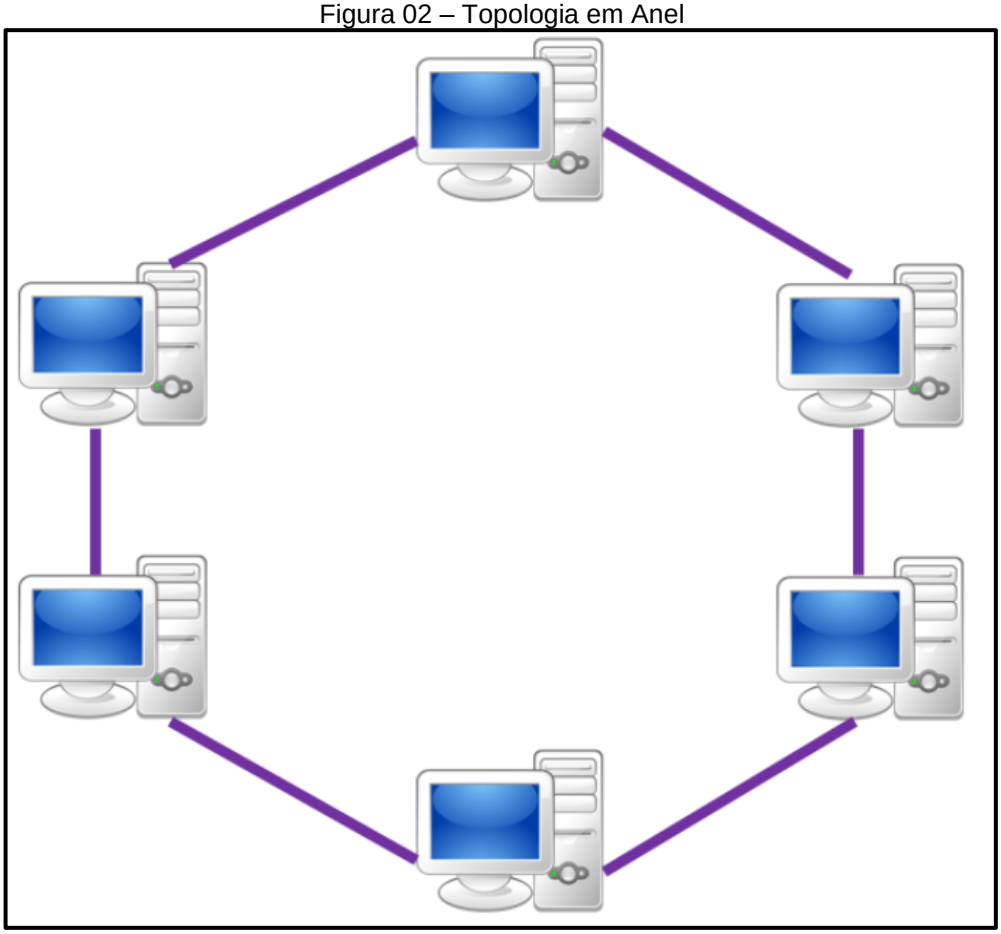


Fonte: bosontreinamentos.com.br (2016)

3.2.2 TOPOLOGIA EM ANEL

Também é uma topologia antiga, que pode ser encontrada em uso em redes legadas. O exemplo mais famoso de redes que empregam essa topologia são as redes Token Ring, da IBM. Nessa topologia os dispositivos são conectados em série, formando um circuito fechado. Uma mensagem enviada por um dispositivo trafega pelo anel e passa por outros dispositivos que retransmitem o sinal até chegar ao dispositivo de destino. Essa topologia trabalha com o conceito de token, o que significa na prática que quem estiver de posse do token está responsável pela transmissão. As mensagens podem trafegar pelos dois sentidos dentro do anel, pois se uma ligação do anel cair, o sentido da comunicação pode ser invertido.

Figura 02 – Topologia em Anel



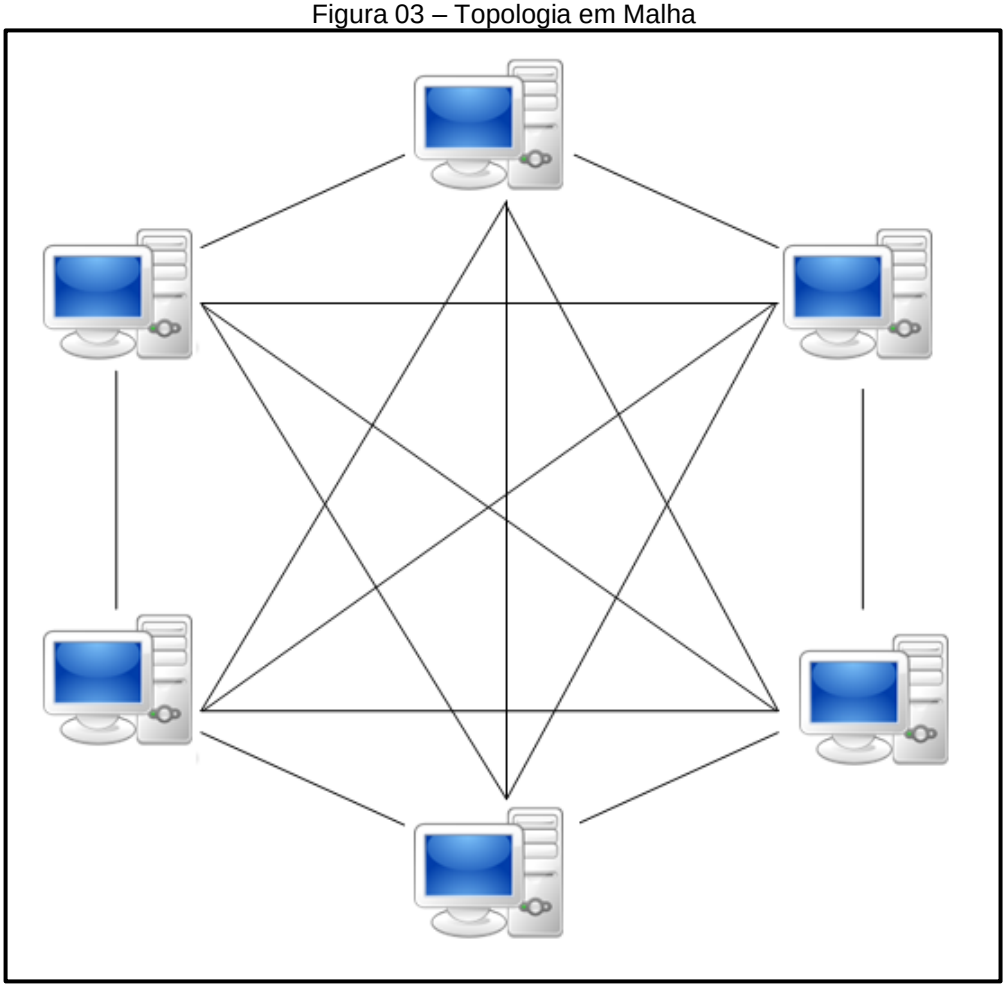
Fonte: bosontreinamentos.com.br (2016)

3.2.3 TOPOLOGIA EM MALHA

Uma topologia em malha possui múltiplas conexões para cada um de seus dispositivos. Essa topologia se divide em Malha Totalmente Conectada e Malha

Parcialmente Conectada. De modo que na Malha Totalmente Conectada, cada dispositivo esteja conectado diretamente a cada outro dispositivo da rede. E na Malha Parcialmente Conectada cada dispositivo estará conectado diretamente somente a alguns dos outros dispositivos da rede, sendo que para haver comunicação com o restante, tem de passar por outros dispositivos primeiro, não havendo a comunicação direta. Esse tipo de topologia tem como vantagem oferecer alto nível de redundância, embora seja mais cara para se implementar e gerenciar, devido ao número excessivo de conexões.

Figura 03 – Topologia em Malha



Fonte: wikiwand.com (2019)

3.2.4 TOPOLOGIA EM ESTRELA

Assim como o padrão ethernet é o mais popular adotado em redes locais hoje em dia, a topologia mais popular usada nesse tipo de arquitetura é a topologia tipo estrela. Nesse sempre foi assim, pois só depois de 1995, que o padrão abandonou a topologia em barramento para adotar a topologia em estrela. E só no começo dos

anos 2000 que a ethernet passou a usar o switch como dispositivo concentrador, tornando assim o funcionando de toda topologia, tanto física como lógica, efetivamente estrela.

Na topologia em estrela, os dispositivos finais da rede são ligados pelos cabos a um dispositivo que atua como concentrador. Sendo ele responsável por conectar os hosts da rede, fornecendo acesso ao meio e gerenciando as comunicações entre esses hosts. É importante salientar que uma rede só terá topologia estrela em nível de funcionamento, se um switch estiver sendo utilizado. Pois mesmo que os cabos individuais de cada host da rede estejam concentrados e ligados a um dispositivo concentrador, se ele for um hub, haverá somente um domínio de colisão, consequentemente gerando broadcast para todas as máquinas da rede toda vez que uma delas for se comunicar com a outra. Pois um hub trabalha somente na camada 1 do modelo OSI (Open System Interconnection), que é a física, retransmitindo tudo que chega em uma porta para todas as outras portas, causando tráfego desnecessário e lentidão na rede. Fazendo assim, a rede funcionar como nas redes antigas com topologia em barramento.

Para reforçar a compreensão do assunto, segundo Torres:

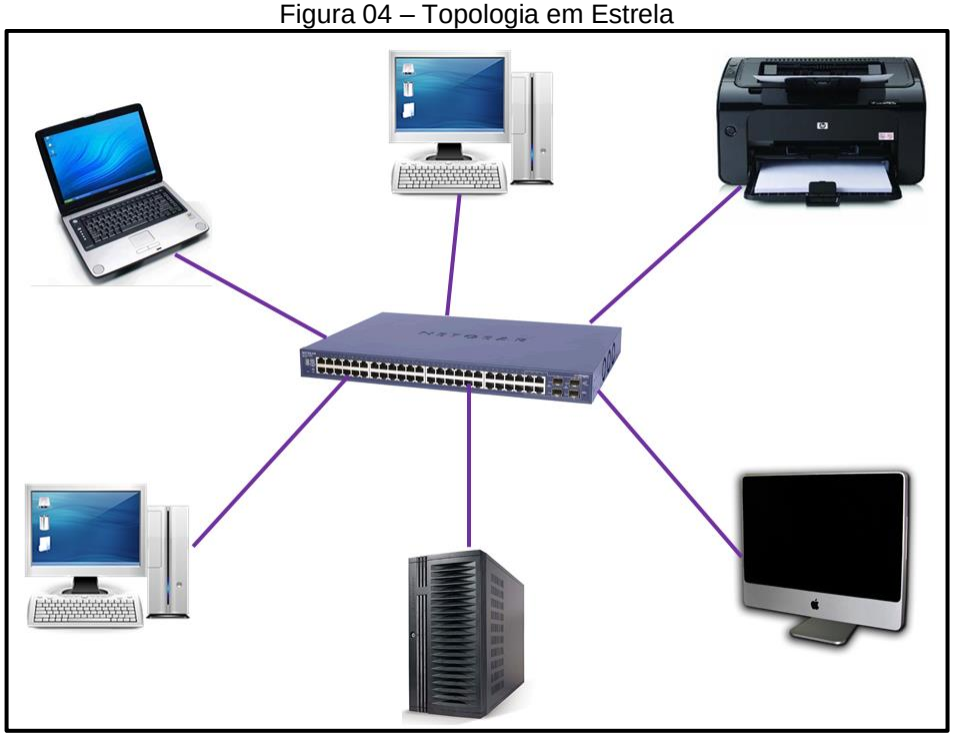
"Quando hubs são usados, apenas um domínio de colisão existe. Isto é, todas as máquinas funcionam como se estivessem conectadas a um mesmo cabo (barramento linear), disputando seu uso." (TORRES, 2016, p. 465)

Por esses e outros motivos hubs caíram em desuso, não sendo mais usados. As redes hoje em dia usam os switchs como concentradores, por suas inúmeras vantagens frente aos hubs.

> Já os switches criam domínios de colisão separados: cada porta do switch será um domínio de colisão separado. Com isso, quando um computador quer transmitir dados, as chances são que ele encontrará seu cabo desocupado quase sempre, ao contrário do que ocorre quando um hub é usado. (TORRES, 2016, p. 465)

> Outra diferença entre hubs e switches é que hubs só operam no modo half-duplex, enquanto que switches permitem a operação da rede no modo full-duplex, que em teoria dobra a largura de banda disponível (em outras palavras, aumenta o desempenho da rede). (TORRES, 2016, p.465)

Figura 04 – Topologia em Estrela



Fonte: bosontreinamentos.com.br (2016)

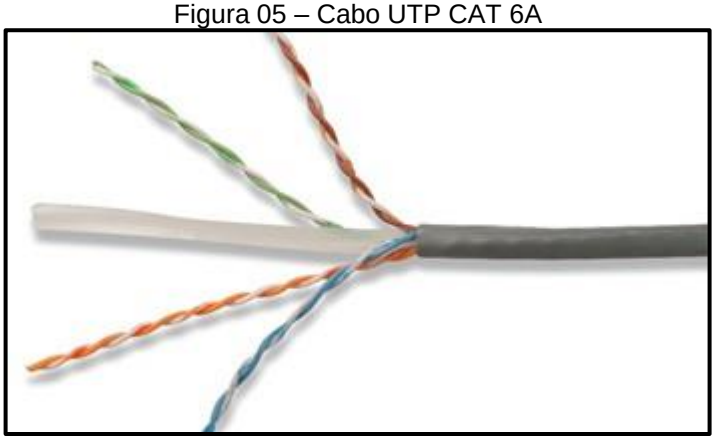
3.3 CABOS E CONECTORES

Como foi dada uma breve explicação sobre o tipo de arquitetura padrão e topologia usada hoje em dia em uma LAN, este trabalho dará prosseguimento através da explicação sobre os diversos tipos de materiais e procedimentos necessários para instalá-los, formando parte da estrutura da rede. Os materiais citados fazem parte da parte física da rede, responsável por conduzir os sinais elétricos entre os dispositivos finais, passando pelos dispositivos que controlam essas comunicações, como os switchs.

Na arquitetura ethernet, é mais comum serem empregados cabos de cobre, ou seja, cabos metálicos, do tipo par trançado, composto por 8 fios. Esse tipo de cabo é relativamente barato, flexível, e oferece velocidades de transmissão hoje na casa dos gigabits, sendo o padrão em redes LAN. Já tendo passado por muitas revisões, esse tipo de cabo para uso em redes locais se encontra na categoria 6A. Cada categoria indica a qualidade do cabo, frequência de operação, velocidade de transmissão máxima suportada, e consiste em um conjunto de características e normais técnicas, que precisam ser seguidas pelos fabricantes na hora da fabricação desse tipo de cabo.

Porém esses cabos de rede transmitem sinais elétricos, e por isso são suscetíveis a interferências externas e próximas, até mesmo dos fios vizinhos do mesmo cabo, efeito chamado de crosstalk. Para minimizar esse fato, esses cabos trazem de fábrica os fios trançados de ponta a ponta, criando uma proteção eletromagnética contra interferência externa e interna dos pares de fios vizinhos, sem recorrer a qualquer espécie de blindagem. Daí o nome cabo UTP (Unshielded Twisted Pair – Par Trançado Não Blindado).

Figura 05 – Cabo UTP CAT 6A

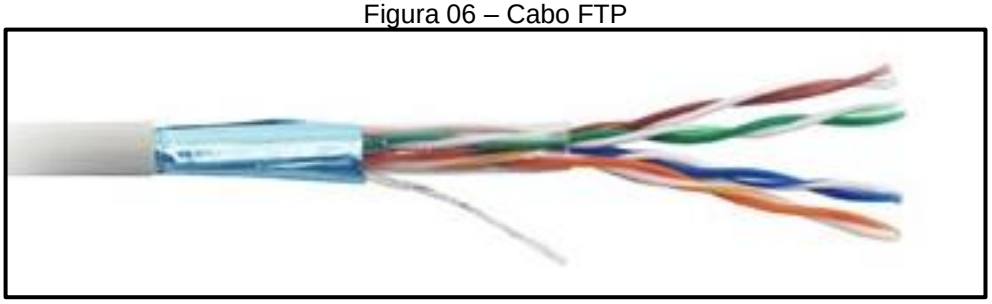


Fonte: hardware.com.br (2008)

Esses cabos são vendidos originalmente em caixas de 305 metros, e sua distância de propagação de sinal foi definida como sendo de 100 metros. Embora na prática podemos ver casos de um cabo com comprimento maior funcionar sem problemas, ele estará fora do padrão recomendado, que foi definido por meio da garantia que o sinal percorrerá até 100 metros dentro do cabo, sem problemas, considerando um cenário livre de interferência sobre o cabo.

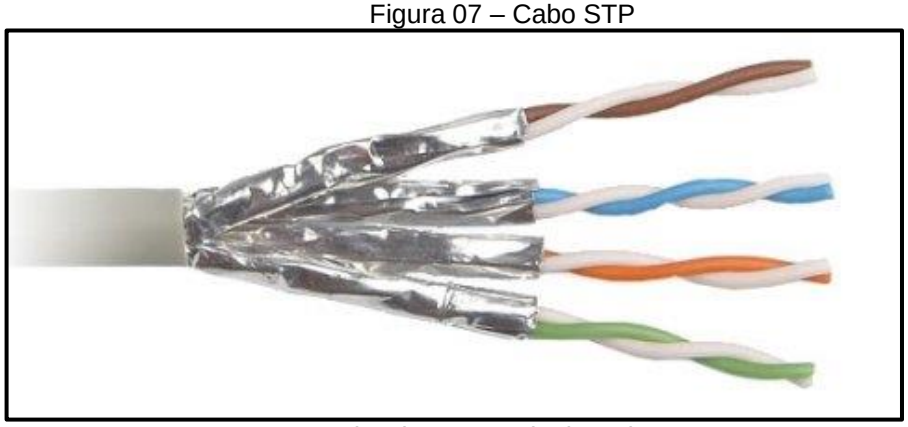
Continuando, existem não só cabos UTP que não são blindados, como também cabos blindados, que podem ser FTP (Foiled Twisted Pair), STP (Shielded Twisted Pair – Par Trançado Blindado) e SSTP (Screened Shielded Twisted Pair).

Figura 06 – Cabo FTP



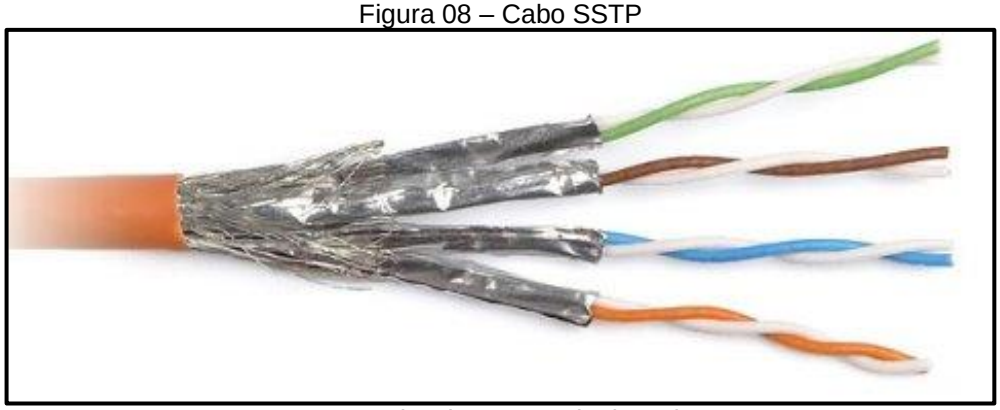
Fonte: hardware.com.br (2008)

Figura 07 – Cabo STP



Fonte: hardware.com.br (2008)

Figura 08 – Cabo SSTP



Fonte: hardware.com.br (2008)

Importante citar que o fato de existir um nível de blindagem não tem relação direta com a categoria do cabo.

> Os cabos sem blindagem são mais baratos, mais flexíveis e mais fáceis de crimpar e por isso são de longe os mais populares, mas os cabos blindados podem prestar bons serviços em ambientes com forte interferência eletromagnética, como grandes motores elétricos ou grandes antenas de transmissão muito próximas. (MORIMOTO, 2011, p. 58)

Assim como no caso dos cabos, existem também conectores blindados e não blindados. Os conectores blindados protegem a parte destrançada dos fios que se localizam dentro do conector, evitando que eles sejam a parte fraca do cabeamento, por não dispor de proteção. Porém os conectores não blindados é que são os populares.

Figura 09 – Conector RJ45 Blindado

Fonte: hardware.com.br (2008)

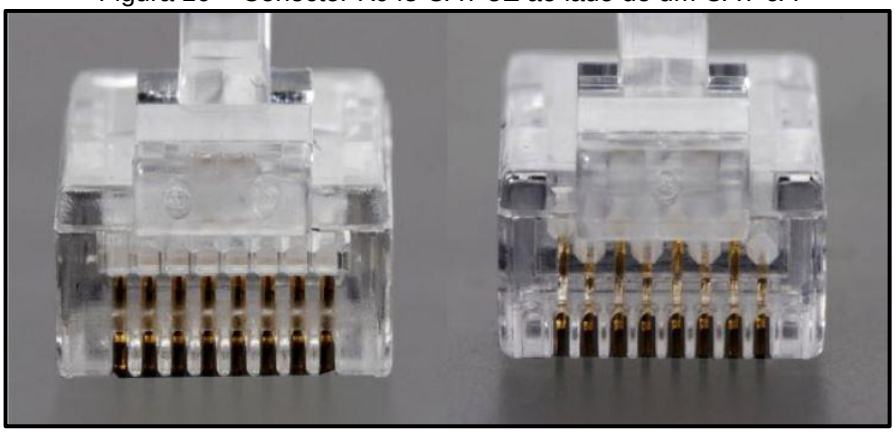
Deve-se ter atenção ao se comprar os conectores certos para a categoria de cabo usado, porque mesmo usando-se um cabeamento de categoria 6, mas com conectores para cabos de categoria 5, o cabeamento será considerado categoria 5.

Como neste trabalho foram usados cabos 6A, foi consequentemente comprado conectores RJ-45 feitos para cabos categoria 6. Esses conectores embora a uma primeira vista sejam externamente quase iguais aos conectores RJ-45 para cabos 5, internamente são facilmente identificáveis através de um olhar atento, ao padrão de distribuição dos fios do cabo, que são dispostos em zig-zag dentro do conector, ao invés do padrão de distribuição dos fios em paralelos em linha reta, como no conector para cabos de categoria 5.

Outras diferenças de um conector RJ-45 para cabo de categoria 6 e um conector RJ45 para cabo de categoria 5, segundo Morimoto:

> “Embora o formato e a aparência seja a mesma, os conectores RJ-45 destinados a cabos cat 6 e cat 6A utilizam novos materiais, suportam frequências mais altas e introduzem muito menos ruído no sinal”. (MORIMOTO, 2011, p. 57)

Figura 10 – Conector RJ45 CAT 5E ao lado de um CAT 6A



Fonte: hardware.com.br (2008)

3.4 PASSAGEM DE CABOS

De posse dos cabos, chega o momento de passá-los através de algum meio que os proteja, não os deixando exposto, de forma a minimizar o contraste com o visual do ambiente. O objetivo sempre é oferecer proteção aos cabos, mas também escondê-los sempre que for possível. Para isso se utiliza dos mais diferentes materiais que podem ser colados ou parafusados na parede, ou no teto. Como por exemplo, perfis de plástico com divisão, canaletas, eletrocalhas, conduítes, etc

É muito importante saber de antemão que cabos de rede não podem dividir o mesmo espaço juntamente com cabos de rede elétrica, usando os mesmos dutos e tubulações para os dois, pois:

> Cabos de rede podem ser passados junto com cabos de telefone e de TV a cabo sem problemas, mas não juntamente com cabos da rede elétrica. O problema com relação a eles é que o campo eletromagnético gerado pelos cabos elétricos (devido ao uso de corrente alternada) induz corrente nos cabos de rede, o que gera interferência na transmissão, causando corrupção de dados. (MORIMOTO, 2011, p. 95)

Entretanto

> Graças ao sistema de checagem e retransmissão usados pelas placas de rede, raramente dados serão perdidos, mas as retransmissões irão reduzir a taxa de transferência e aumentar a latência da rede, como resultados variados. A interferência é maior em redes elétricas sem aterramento adequado ou em circuitos com cargas pesadas, como os usados por chuveiros e motores elétricos. (MORIMOTO, 2011, p. 95)

Passando-se os cabos de rede através de conduítes separados de cabos de rede elétrica já existentes no prédio, se eliminará a chance de que o cabeamento da rede sofra com essa fonte de interferência, que são os cabos da rede elétrica. Contribuindo assim para uma rede com menos perdas de pacotes, retransmissões e latência.

3.5 NOÇÕES DE CABEAMENTO ESTRUTURADO

Ao se falar sobre a passagem dos cabos e preparação das tomadas, deve-se ter em mente que todo profissional da área tenha pelo menos noção do que é cabeamento estruturado.

> Montar uma rede doméstica é bem diferente de montar uma rede local de 100 pontos em uma empresa de médio porte. Não apenas porque o trabalho é mais complexo, mas também porque existem normas mais estritas a cumprir. O padrão para instalação de redes locais em prédios é o ANSI/TIA/EIA-568-B, que especifica normas para instalação do cabeamento, topologia da rede e outros quesitos, que chamamos genericamente de cabeamento estruturado. No Brasil termos a norma NBR 14565, publicada pela ABNT em 2001.
>
> (MORIMOTO, 2011, p.98)

> A ideia central do cabeamento estruturado é cabear todo o prédio de forma a colocar pontos de rede em todos os pontos em que eles possam ser necessários. Todos os cabos vão para um ponto central, onde ficam os switchs e outros equipamentos da rede. Os pontos não precisam ficar necessariamente ativados, mas a instalação fica pronta para quando precisar ser usada. A ideia é que a longo prazo é mais barato instalar todo o cabeamento de uma vez, de preferência antes do local ser ocupado, do que ficar fazendo modificações cada vez que for preciso adicionar um novo ponto de rede. (MORIMOTO, 2011, p. 98)

Toda a estrutura da rede começa pela sala de equipamentos, que é a sala responsável por abrigar os servidores, os switchs e roteadores principais. Essa é a parte central da rede. Essa sala deve ser de acesso restrito, e os equipamentos de rede contidos nela devem ser protegidos de qualquer acesso não autorizado.

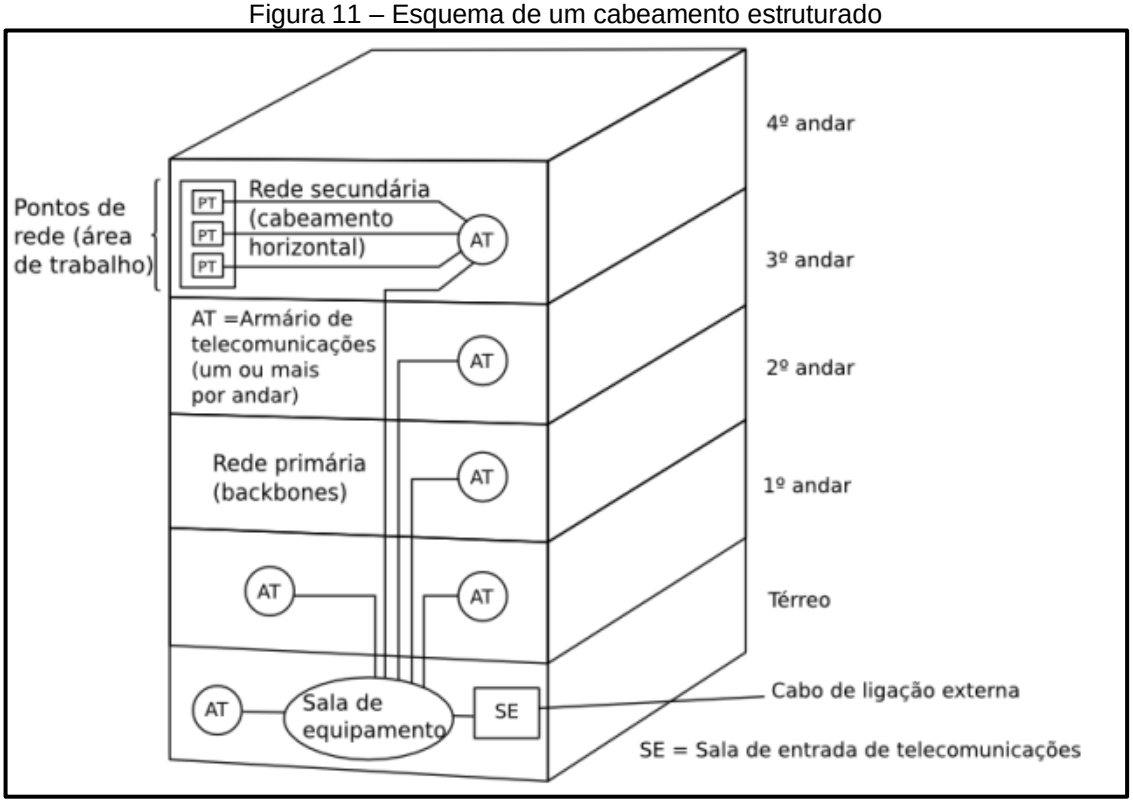
Considerando o exemplo de um prédio de 3 andares, seria inviável puxar um cabo da sala de equipamentos até cada tomada de rede presente nas salas, no restante dos andares do prédio. Para isso existe um segundo nível hierárquico, que é o armário de telecomunicações. O papel desse armário é concentrar todo o cabeamento horizontal presente no andar. Sendo assim, o cabeamento dos pontos de rede acaba se concentrando em um armário com um ou mais switchs e patch panels em cada andar. Esses armários de telecomunicações são pontos de distribuição na rede. Muitas vezes na prática esses armários são representados por um rack fixado na parede, trancado, de acesso restrito, abrigando um ou mais switchs e patch panels devidamente parafusados em sua estrutura interna. Esses switchs e patch panels recebem o cabeamento fixo que vem dos pontos de rede individuais nas áreas de trabalho.

Para prover acesso a rede para os dispositivos que são conectados nos pontos de rede, os armários de telecomunicações precisam se unir ao restante da rede. Para isso são conectados com outros cabos que percorrem verticalmente o prédio, que são cabos que vem da sala de equipamentos, chamados de backbone. Normalmente o backbone é composto por cabos de fibra óptica, por necessidade de se trafegar dados em grande velocidade. São cabos que vem dos roteadores e switchs principais na sala de telecomunicações. Se houver um backbone de fibra óptica na rede do prédio, deve existir também switchs que tenham portas que recebam fibra óptica. Porém, dependendo da distância e tamanho da rede, cabos de rede par trançado podem ser usados normalmente como backbone da rede.

De uma forma resumida, podemos numerar os componentes de um cabeamento estruturado:

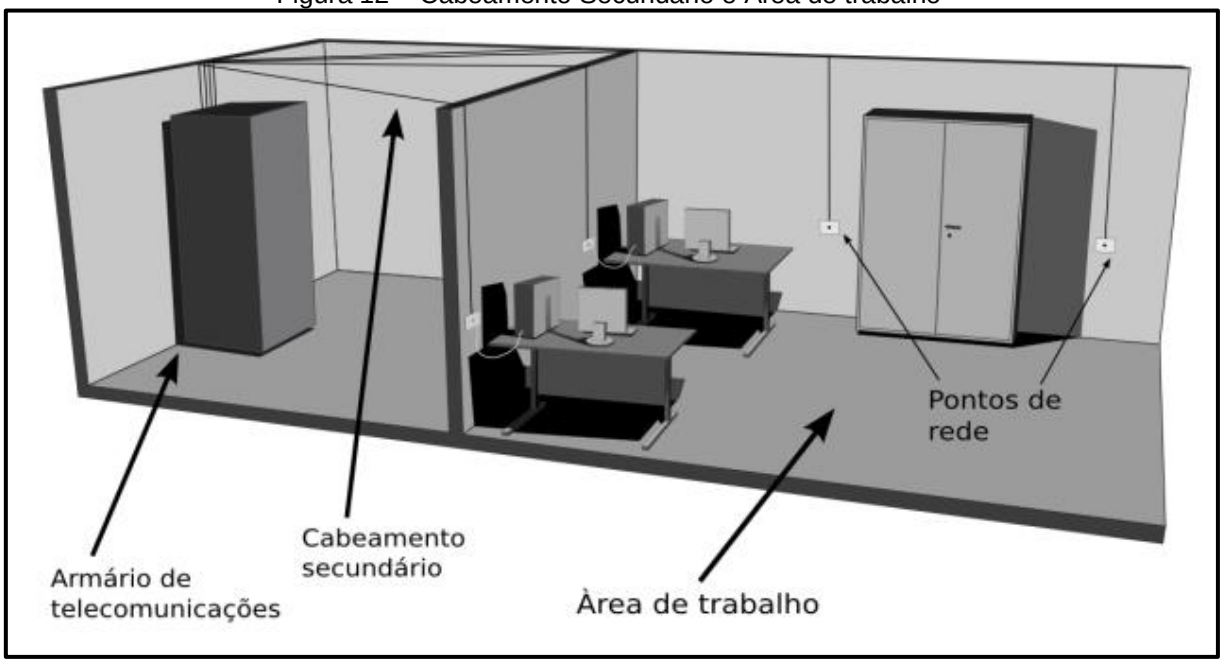
1. Sala de equipamentos
2. Cabeamento vertical (Rede primária)
3. Cabeamento horizontal (Rede secundária)
4. Armário de telecomunicações
5. Áreas de trabalho
6. Estações de trabalho

Figura 11 – Esquema de um cabeamento estruturado



Fonte: hardware.com.br (2008)

Figura 12 – Cabeamento Secundário e Área de trabalho



Fonte: hardware.com.br (2008)

Como fica claro no cenário deste trabalho, não foi feito antes um cabeamento estruturado no prédio, pensado para suportar um laboratório de informática, eliminando a necessidade de uma infraestrutura de cabeamento extra para isso.

Mas mesmo que este trabalho não trate de um ambiente com um cabeamento estruturado, pode-se mesmo assim aplicar-se noções e padrões pertencentes a ele, para melhor estruturar e prover escalabilidade a rede.

Como por exemplo, o padrão que determina que o cabo entre o ponto de rede ou ponto de telecomunicação, vulgo tomada de rede, e o patch panel (painel de conexão), não pode exceder 90 metros. Pois como se sabe, cabos de rede foram feitos para terem 100 metros de comprimento sem atenuação de sinal. Então esses 90 metros da tomada ao patch panel no armário de telecomunicações, se somam aos 6 metros do cabo da tomada a estação de trabalho, que é computador, e mais 3 metros do patch cord que vai do patch panel ao switch. Obviamente o padrão permite uma flexibilidade, pois se não for necessários 90 metros de cabo da tomada até o patchpanel, poderia se usar um cabo maior que 6 metros para ligar um computador a tomada. O que é regra é não exceder o total de 100 metros permitidos.

3.6 TOMADAS E INSTALAÇÕES, CABOS E CRIMPAGEM

Tomadas e instalação

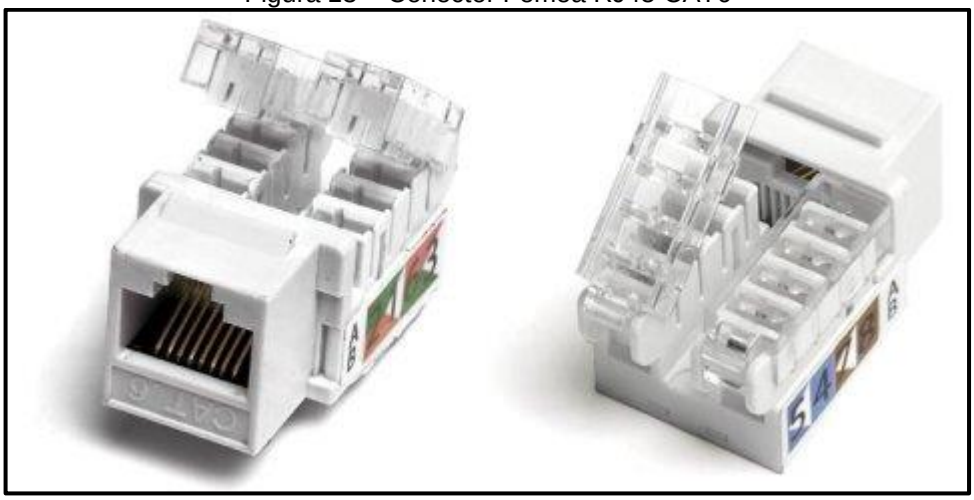
Depois da passagem dos cabos respeitando algumas noções de cabeamento estruturado, o passo seguinte é o preparo das tomadas para receber os cabos vindo dos dispositivos da rede. Dando um acabamento mais profissional a rede, a finalidade delas é atuar como ponto fixo para conexão de um novo dispositivo a rede, dando flexibilidade para a conexão de cabos de variados tamanhos, e possibilidade de substituição desses cabos, conforme necessário. Essas tomadas podem ser únicas ou dupla, agregando dois conectores RJ-45 fêmea em uma só tomada, possibilitando mais de um dispositivo conectado por tomada. Obviamente, para uma tomada ser dupla ela também precisa de mais de um cabo de rede conectada a ela. Neste trabalho, essas tomadas foram implementadas na parede, para conexão dos

computadores das bancadas dos laboratórios, e outras bem perto do quadro e mesa do professor.

Para se montar uma tomada destas, usando como exemplo sua instalação em uma parede, deve-se atentar para os seguintes passos e detalhes.

Primeiramente, passando a ponta do cabo para dentro da caixa sobrepor, e em seguida parafusando a mesma na parede. A ponta do cabo que vem da parede, e se encontra no interior da caixa de sobrepor, precisa ser decapada sem que nenhum fio seja também cortado no processo. Com os fios da ponta do cabo intactos, destrança-se todos os fios e analisa-se a demarcação em cores dos padrões criados pela EIA (Electronics Industries Alliance) e TIA (Telecomunications Industry Association), que são o EIA/TIA T568A e EIA/TIA T568B do conector RJ-45 fêmea, também conhecido como keystone. Cada tomada tem o seu padrão de ordem dos fios. E o ideal é usar o mesmo modelo de tomada para toda a rede.

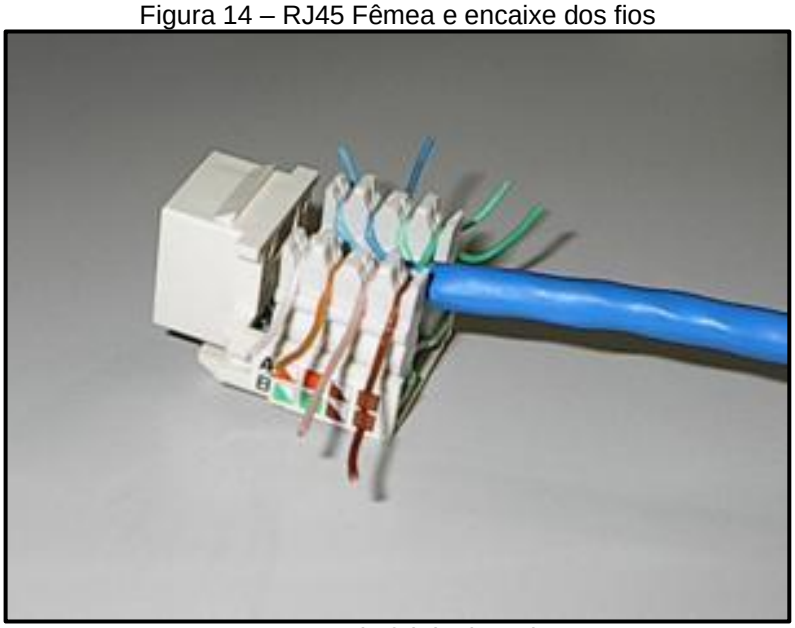
Figura 13 – Conector Fêmea RJ45 CAT6



Fonte: hardware.com.br (2008)

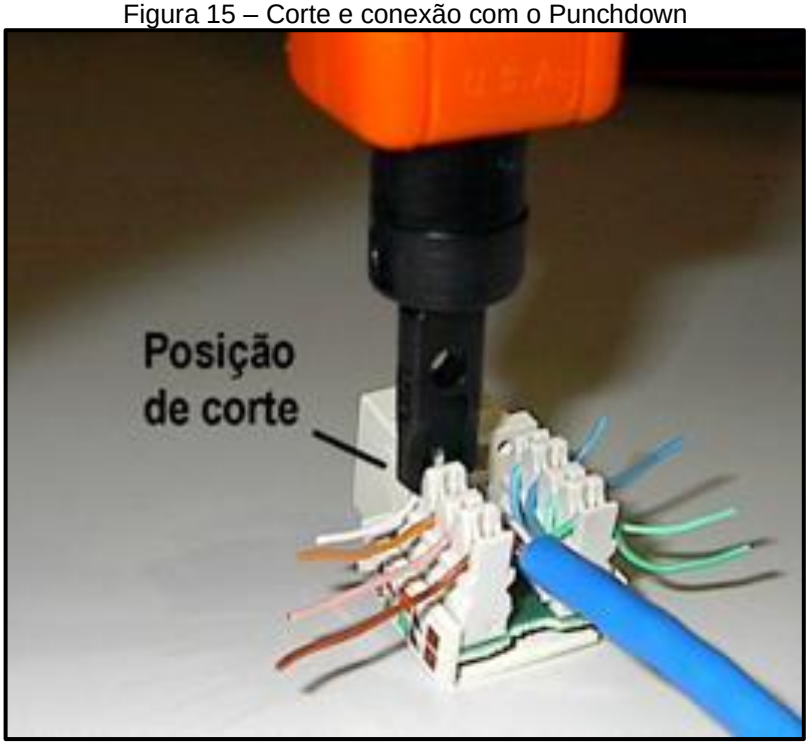
Com os fios destrançados, é só colocar o cabo com os fios no centro do conector RJ-45 fêmea, até aproximadamente a metade da profundidade do conector, e em seguida separar, direcionar e encaixar cada fio a sua fresta de marcação de cor correspondente, de acordo com o padrão EIA/TIA T568A ou EIA/TIA T568B, dependendo do caso. Por fim, finalizando com o uso da ferramenta chamada punch down, que é um alicate de pressão, que pressiona os fios contra as lâminas no fim de cada fresta do conector, criando o contato e ao mesmo tempo cortando o excesso de fios que sobra pra fora do conector.

Figura 14 – RJ45 Fêmea e encaixe dos fios



Fonte: nti.ufpb.br (2019)

Figura 15 – Corte e conexão com o Punchdown

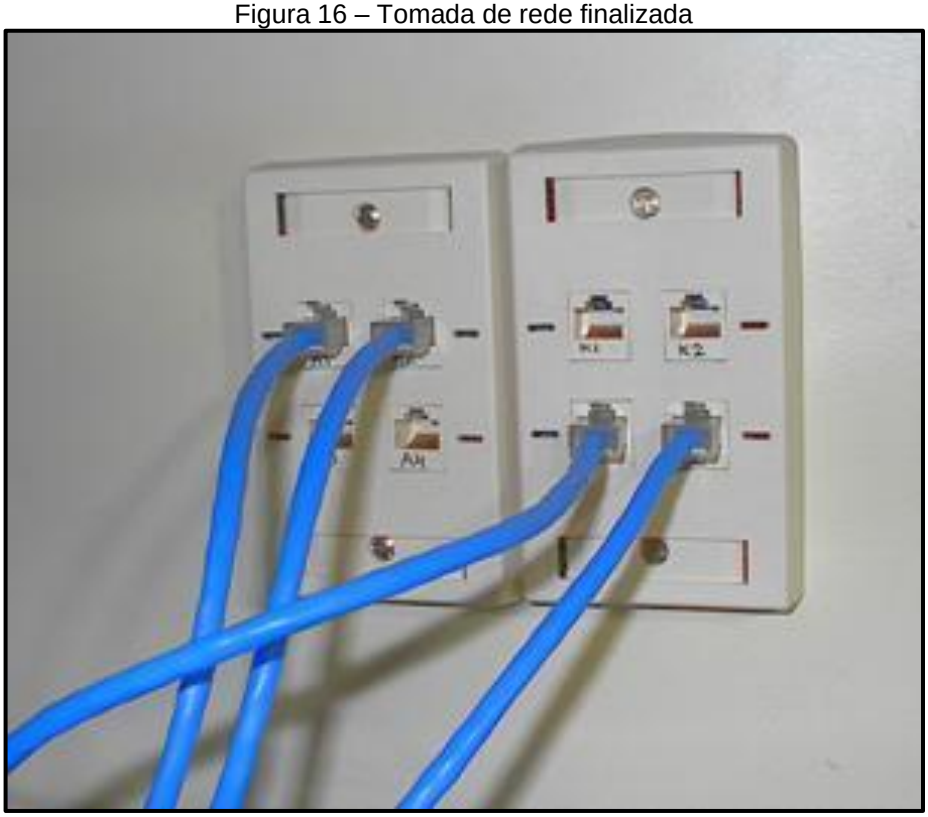


Fonte: nti.ufpb.br (2019)

Com isso o resultado é o cabo conectado ao conector RJ-45 fêmea, o que já possibilita conexão. Porém para se ter uma tomada propriamente dita, ainda é necessário encaixar o conector ao resto das peças que compõe a moldura, e então juntar a moldura que é a frente da tomada, com a caixa sobrepor que é a parte de trás dela, através de parafusos que já acompanham a tomada. Neste momento, deve-se enrolar e empurrar a sobra do cabo para dentro da caixa sobrepor, para que tudo fique

acomodado dentro da estrutura da tomada, assim permitindo parafusar a frente da tomada sem maiores problemas.

Figura 16 – Tomada de rede finalizada



Fonte: nti.ufpb.br (2019)

Continuando, todo cabo de rede precisa de um par de conectores em suas pontas para prover uma correta conexão física, assim entregando os sinais elétricos junto de seus bits. Se tratando desse tipo de cabo, o conector que o acompanha leva o nome de RJ-45.

Cabos e crimpagem

O alicate de crimpagem é a ferramenta usada para se crimpar cabos de rede. Normalmente um alicate de crimpagem pode crimpar cabos com conectores RJ45 e RJ11 também. O RJ11 é usado em redes de telefonia.

O principal papel do alicate de crimpagem é pressionar o conector contra o cabo, fazendo as facas-contatos perfurarem a cobertura plástica que envolve os fios, provocando por meio disso, o contato entre o conector e os fios. Além disso, o alicate de crimpagem pode ser usado para cortar e decapar o cabo.

Existem alicates de crimpagem de todos os preços. Mas é recomendável que todo profissional compre um de valor mais elevado. Por terem mais qualidade, são fortes e precisos, além de sua vida útil ser maior. Já os alicates baratos demais, com o tempo não funcionam adequadamente, pois suas lâminas de corte ficam cegas rapidamente, além de sofrerem de outros problemas.

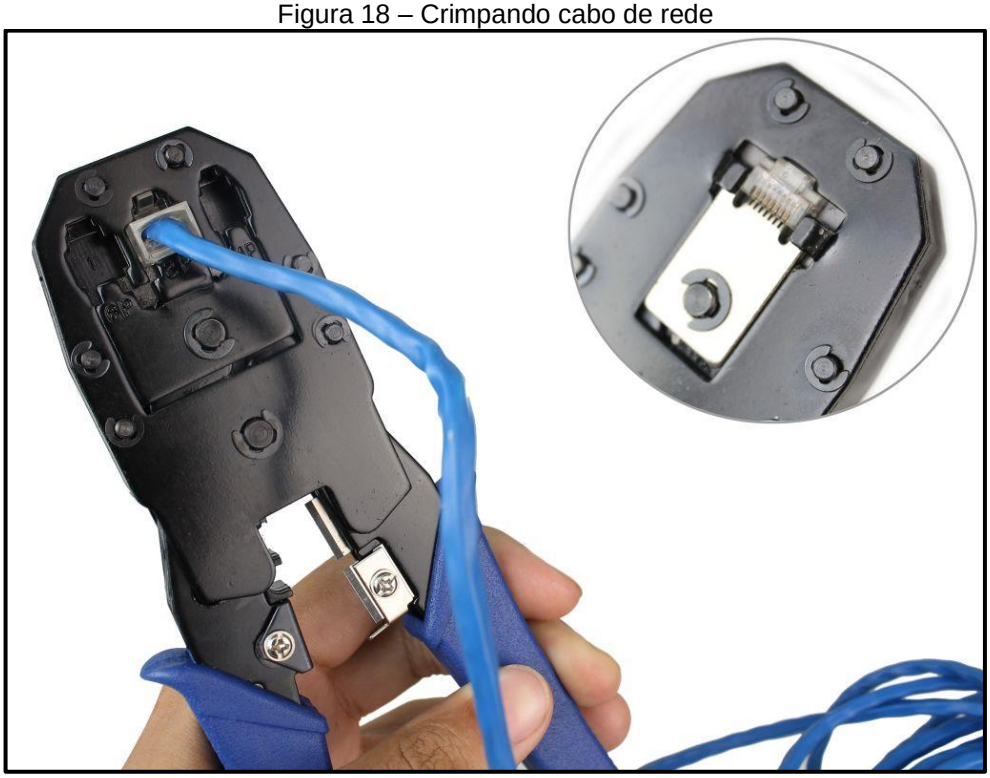
Figura 17 – Alicate de Crimpagem

Fonte: hikariferramentas.com.br (2019)

A sequência de procedimentos para crimpar um cabo de rede, consiste em decapar o cabo, isto é, eliminar a capa externa, tornando possível a manipulação dos fios individualmente. Em seguida destrança-se todos os fios e os separa-se pelas suas cores. Com os fios separados e retos, corta-se os fios para ficarem do tamanho adequado para inserção no conector. Aqui deve-se ter cuidado para não deixar os fios longos demais, ocasionando em um cabo passível de mal contato e até rompimento. Por isso existe uma recomendação que determina que deve-se cortar o excesso de fios, de modo que sobre 1,27 cm para inserção dentro do conector RJ-45. Em seguida, com o conector com a trava virada para baixo em uma mão, e na outra com o cabo e os fios separados e alinhados, insere-se os fios junto com o cabo dentro do conector. Tomando-se cuidado para que os fios estejam na ordem correta e cheguem todos até a extremidade do fim do conector.

E por fim, utiliza-se o alicate de crimpagem, apertando-o contra o conector com o cabo já inserido em seu interior. Fazendo assim com que os pinos do conector, que tem formato de lâmina, possam perfurar a proteção plástica que envolve os fios, e chegar nos fios, criando o contato.

Figura 18 – Crimpando cabo de rede

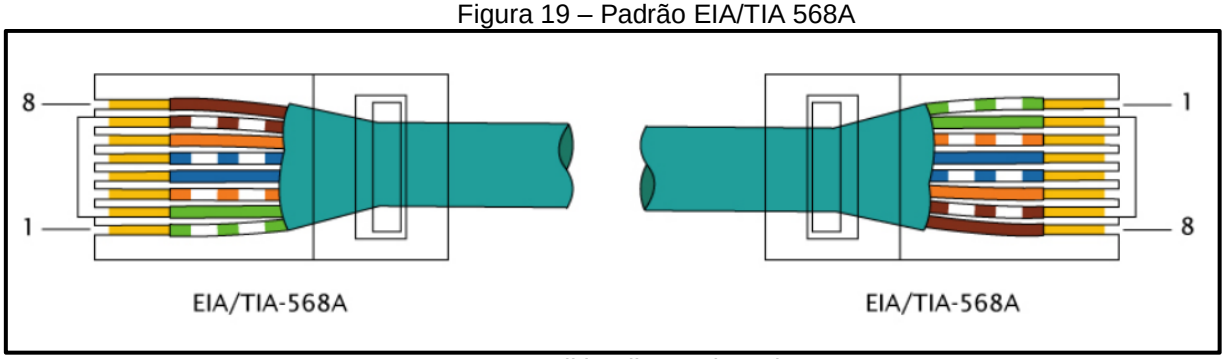


Fonte: usinainfo.com.br (2018)

Para crimpar um cabo de rede, além do fato de se ter certificado de ter escolhido um cabo, conector e alicate de qualidade, deve-se escolher um padrão de ordem dos fios para inserção no conector, dependendo dos dispositivos que vão ser conectados por meio desse cabo. Existem dois padrões: o EIA/TIA 568A e o EIA/TIA 568B. A diferença entre esses dois padrões é que a posição do par verde e par laranja é invertida dentro do conector.

O padrão mais usado é o EIA/TIA T568A. Nesse padrão os fios ficam dispostos assim:

Figura 19 – Padrão EIA/TIA 568A

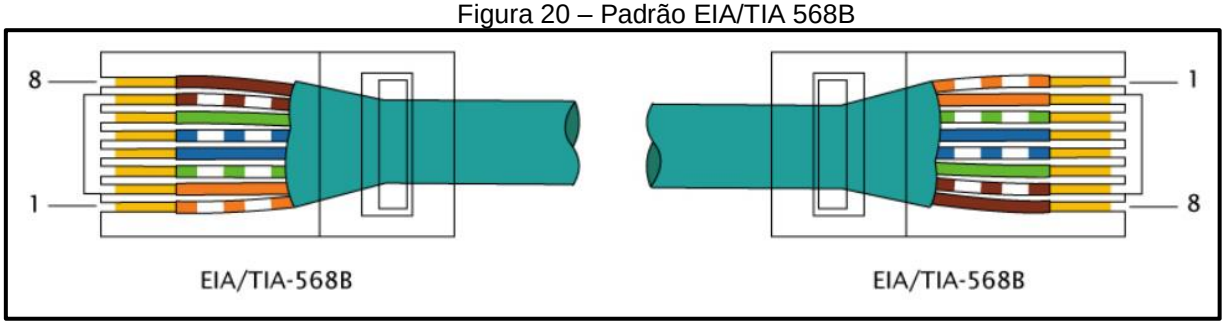


Fonte: et.wikipedia.org (2019)

1. Branco com verde
2. Verde
3. Branco com laranja
4. Azul
5. Branco com azul
6. Laranja
7. Branco com marrom
8. Marrom

E no padrão EIA/TIA T568B, ficam:

Figura 20 – Padrão EIA/TIA 568B



Fonte: et.wikipedia.org (2019)

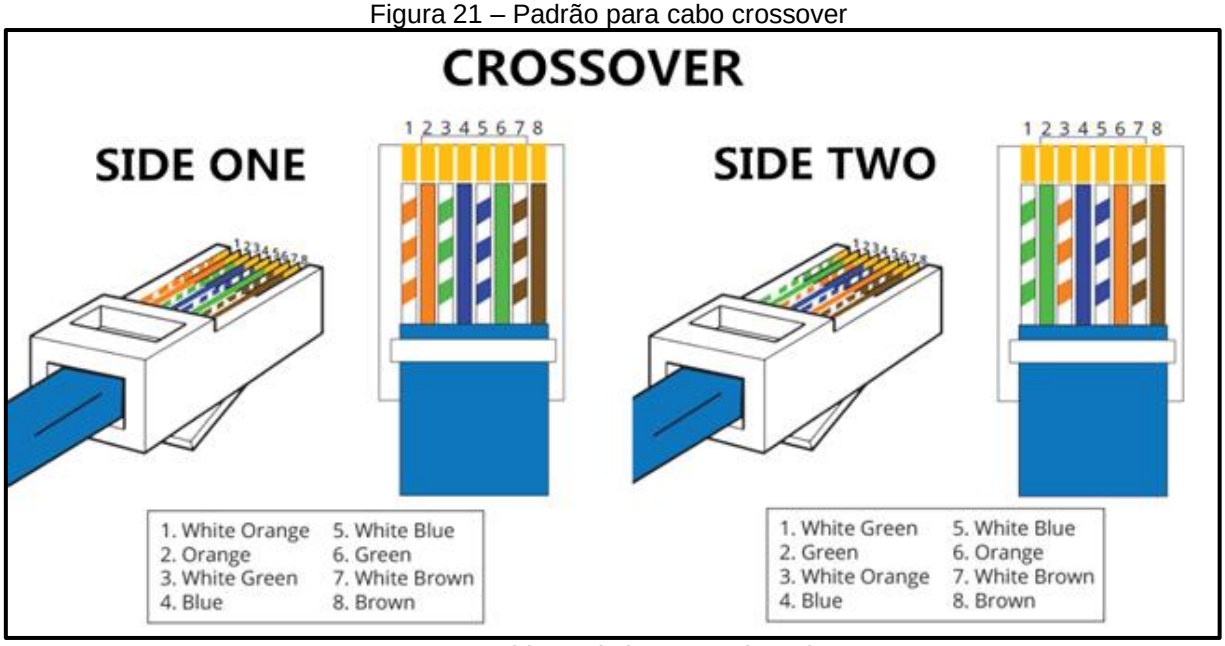
1. Branco com laranja
2. Laranja
3. Branco com verde
4. Azul
5. Branco com azul
6. Verde
7. Branco com marrom
8. Marrom

Além desses dois padrões, existem ainda os tipos de cabo paralelo e crossover (cabo cruzado). O cabo crimpado com o mesmo padrão nas duas pontas é chamado de cabo paralelo. Esse é o tipo de cabo mais comum, por ligar diferentes tipos de dispositivos na rede, como um computador ao switch. Já o cabo que foi crimpado usando um padrão diferente em cada ponta, é chamado de cabo crossover. Este serve para ligar dois dispositivos iguais sem necessidade de um dispositivo intermediador no meio. Como por exemplo, ligar dois computadores sem necessidade de um switch.

> É importante enfatizar que este cabo é geralmente necessário apenas ao interligar equipamentos antigos, pois a grande maioria dos switchs e também placas gigabit atuais são capazes de cruzar o cabo automaticamente, aceitando serem ligadas diretamente com um cabo 568B ou 568A straight. Isso ocorre quando os transmissores são capazes de ajustar a transmissão via software, recurso chamado de Auto-MDI/MDI-X.
>
> (MORIMOTO, 2011, p. 87)

Abaixo vemos uma imagem ilustrativa de um cabo crossover, que em cada ponta tem um padrão diferente.

Figura 21 – Padrão para cabo crossover



Fonte: cables-solutions.com (2016)

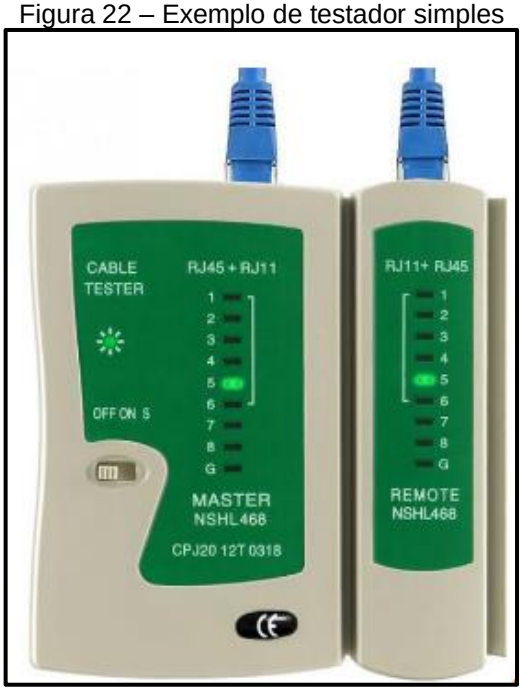
Testadores

Depois da crimpagem do cabo, pode-se testá-lo logo na prática conectando-o aos dispositivos da rede para ver se há comunicação. O que gera perda de tempo, se

o cabo estiver com problema por conta de algum rompimento interno ou má crimpagem. Por isso o recomendado é testar antes por meio de ferramentas próprias para essa finalidade, chamadas de testadores. Essas ferramentas geralmente consistem de duas unidades, uma principal e uma remota, em que uma ponta do cabo é conectado a cada uma delas. Em seguida ao se pressionar o botão de teste do equipamento, um grupo de LED (Light Emitter Diode) acende e um bip ocorre indicando se há contato com todos os fios nas duas pontas do cabo. Dependendo do modelo de testador, o estado do cabo pode ser indicado por LEDs acendendo em intervalos alternados ou acendendo de uma só vez, junto de outro LED que sinaliza o resultado.

Existem diversos modelos de testadores de cabo, com enorme variedade de funções, qualidade e preço. Desde testadores simples de marcas chinesas e brasileiras, custando poucas dezenas de reais e não sendo muito confiáveis, até testadores profissionais que custam milhares de reais. Testadores simples são simples porque somente fazem teste de continuidade em um cabo. Eles não dispõem de nenhuma tela para maiores informações sobre o cabo, mas sim somente de LEDs com suas respectivas legendas. É através da atividade ou não desses LEDs, além de sinais sonoros, que o profissional sabe quando há problema no cabo testado, mas não exatamente qual o problema e nem onde ele está exatamente localizado no cabo.

Figura 22 – Exemplo de testador simples



Fonte: cpeletronicos.com.br (2019)

Já os testadores profissionais são muito sofisticados, dispõe de telas com iluminação própria, sistema embarcado que exibe as funções e configurações possíveis. Exibem também é claro, informações sobre o cabo testado, sendo por exemplo capazes de detectar o comprimento de um cabo, detectar se o cabo está rompido e em que parte do cabo está o rompimento, detectar se o cabo está conectado a uma fonte POE (Power Over Ethernet), entre outras funções.

Figura 23 – Exemplo de testador profissional

Fonte: pt.flukenetworks.com (2019)

Figura 24 – Kit completo

Fonte: pt.flukenetworks.com (2019)

Como mostrado até aqui, há diversos tipos de testadores. Desde tipos muito simples a profissionais, que tem preços proibitivos para a imensa maioria dos profissionais, sendo mais comum serem comprados por grandes empresas para uso de seus profissionais de TI para trabalhos de certificação. Na prática para os profissionais da área de redes de computadores, um testador de continuidade simples, porém não muito barato, já é o suficiente. Pois já atende a finalidade principal que é identificar se todos os fios de um cabo estão conduzindo os sinais elétricos de uma ponta à outra, sem mal contato junto aos conectores ou rompimento interno no cabo. Além de possibilitarem testar não só cabo de rede, como também cabo de telefone e cabo coaxial, em alguns modelos.

Usando um bom material, ferramentas adequadas, e seguindo-se os padrões e recomendações da área, uma rede dificilmente terá problemas de ordem física. Os próprios cabos de rede depois de fabricados, oferecem bastante resistência mecânica e oferecem flexibilidade para passar por dentro de tubulações. Fisicamente, a infraestrutura de uma boa rede dura muitos anos sem necessidade de troca de algum componente material, como tomadas, cabos, conectores, conduítes, por parte dos profissionais de TI responsáveis.

Considerando que a parte física da rede está pronta e instalada, este trabalho dará prosseguimento avançando para a parte de configurações dos equipamentos. Abordando somente o roteador e os computadores de mesa usados, já que os switchs não vão ser gerenciáveis.

4 REDES SEM FIO

4.1 VISÃO GERAL E APLICABILIDADE DAS REDES SEM FIO

Redes cabeadas são a forma mais rápida de se transmitir dados. Por usar meio guiado, como cabos, para transmissão dos bits, uma rede desse tipo é mais veloz, sofre menos interferência e tem latência menor em comparação a uma rede sem fio, ou rede WI-FI.

Porém no mundo das redes de computadores, não há solução perfeita. Redes cabeadas são ótimas para computadores que ficam fixos em cima de uma mesa, estações de trabalho que só ficam no mesmo lugar, a disposição diária dos funcionários de uma empresa, sempre no mesmo lugar ou sala. Mas em contrapartida são inadequadas para dispositivos portáteis, como smartphones, tablets e até notebooks, desses mesmos funcionários. Redes cabeadas também podem ser bem caras.

Existem LANs do tamanho de uma simples sala de escritório, o que não exige mais do que poucos metros de cabo, assim como existem LANs do tamanho de um campus inteiro de uma universidade, o que exige uma grande estrutura de cabeamento. Então, além do desafio de implantar cabos em uma área não adequada para tal, o fator custo pode pesar, a depender do tamanho da rede.

Por conta da óbvia necessidade de se transmitir e receber dados em lugares em que não se poderia pensar na existência de cabos, as redes sem fio surgiram.

> Rede sem fio é um conjunto de equipamentos de rede conectados por ondas eletromagnéticas. O meio de comunicação é o ar, ao invés de fios. Uma rede sem fio dispensa cabeamento, tomadas, conectores, dutos, calhas etc. Também conhecida por WLAN (ou Wireless LAN).
>
> (ELIAS, LOBATO, 2013, p. 44)

Também conhecida como WLAN (Wireless LAN – LAN sem fio), esse tipo de rede teve suas especificações definidas pelo IEEE (Institute of Electrical and Electronic Engineers), sob a recomendação IEEE 802.11.

As redes sem fio evoluíram muito ao longo de sua história. Hoje em dia redes sem fio não servem só para ligar dispositivos próximos. Assim como as redes cabeadas que possibilitam conexões e transmissão de dados a dezenas de km, usando fibra óptica, uma rede sem fio possibilita o mesmo através do enlace entre rádios e antenas poderosas em pontos distantes.

É inegável que as redes sem fio flexibilizaram as redes de computadores. Através de sua existência e evolução, elas ajudaram e foram responsáveis pela entrada no mundo das redes e conexão massiva de dispositivos finais dos usuários, como smartphones, tablets, notebooks, smart tvs, na internet. Sendo hoje, a forma preferida de conexão a uma rede com internet.

Dentre as vantagens e motivações que levam as redes sem fio a serem usadas, podemos citar; mobilidade, confiabilidade, facilidade de instalação, custo e escalabilidade.

Porém, as redes fios não substituem completamente as redes cabeadas, por uma série de motivos. Elas são mais lentas, sofrem com mais interferências, tem latência bem maiores, além de serem menos seguras que as redes cabeadas. Em contrapartida hoje em dia elas oferecem velocidade suficiente para a maioria das tarefas requeridas, além de estarem cada vez mais seguras, através do surgimento de novos protocolos de criptografia.

Como podemos perceber, cada tipo de rede tem o seu uso dependendo da situação e tipo de dispositivo final que vai se conectar a ela. Cada cenário pede um tipo de rede, ou mesmo os dois tipos, como é comum hoje em dia.

Visto que uma variedade grande dispositivos finais coexistem entre si nos mesmos ambientes, como nas casas das pessoas, empresas, escolas, lugares públicos, se dá a necessidade de uma rede cabeada também ter um segmento de rede sem fio, por assim dizer. Essas duas redes usam a mesma arquitetura, que é a ethernet. Portanto elas trabalham perfeitamente bem uma com a outra. Facilmente pode-se ligar um novo roteador sem fio em uma rede cabeada, bastando apenas

conectá-lo a um cabo de rede que venha de um switch, por exemplo. Inclusive muitas vezes nem mesmo precisa-se de uma tomada próxima como fonte de energia separada, pois o mesmo cabo que transmite os dados para o roteado, também lhe fornecerá energia, se o mesmo for compatível com a tecnologia para isso, chamada POE (Power Over Ethernet).

Diante dessas informações, e sabendo que o cenário deste trabalho é um laboratório de informática, o mesmo precisará que uma rede sem fio coexista com uma rede cabeada, diante da necessidade de possibilitar conexão à internet e compartilhamento de recursos com os dispositivos proprietários dos alunos e professores. Na verdade, uma parte da rede cabeada vai ser transformada em rede sem fio, através da conexão de um cabo de rede ao roteador, vindo de um switch. Por isso se dá a necessidade da existência deste capítulo, que fornece uma visão geral sobre as redes sem fio, além de fornecer detalhes sobre a configuração de um roteador sem fio.

4.2 PADRÃO IEEE 802.11

Dentre as informações mais importantes que devemos saber sobre as redes sem fio, é a evolução do seu padrão, o IEEE 802.11.

Antes deste trabalho explanar sobre o padrão IEEE 802.11, é importante esclarecer que por mais que as redes sem fio sejam chamadas de redes WI-FI (Wireless Fidelity), elas são coisas diferentes.

Segundo TORRES:

> Existem várias tecnologias para se montar uma rede sem fio, sendo o padrão IEEE 802.11 o mais popular. Este padrão é também conhecido como Wi-fi, mas é importante saber que Wi-fi e IEEE 802.11 não são a mesma coisa. Wi-fi é uma marca registrada da Aliança Wi-fi, um grupo formado por diversos fabricantes. Para um equipamento ter o direito de ser chamado Wi-fi ele tem de ter passado pelo processo de certificação desse grupo. Sendo assim, todo equipamento Wi-fi é IEEE 802.11, mas nem todo equipamento IEEE 802.11 é Wi-fi. (TORRES, 2016, p. 96)

Modos de funcionamento

Há 3 modos modos de funcionamento em uma rede IEEE 802.11

Ad-hoc: Que era utilizado para se conectar dispositivos sem fio que estivessem próximos, sem a necessidade de um dispositivo gerenciando a conexão, como o AP (Acess Point – Ponto de acesso).

BSS (Basic Service Set): Modo de funcionamento mais comum, sendo muito usado. Consiste em um dispositivo chamado ponto de acesso, que conecta os dispositivos próximos, tornando possível a comunicação entre eles e a internet. Para conexão com a internet, o ponto de acesso precisa estar conectar ao restante da rede. Geralmente o ponto de acesso é chamado de roteador. O roteador cria a rede sem fio, atribuindo um nome a ela (SSID – Service Set ID), que é visto por todos os dispositivos próximos.

ESS (Extended Service Set): Nesse modo de funcionamento, uma rede sem fio é formada por vários pontos de acesso com o mesmo SSID, ou seja, o mesmo nome de rede, formando assim, uma rede única. Isso permite que um usuário mantenha-se conectado à rede, mesmo que saia do alcance de um ponto de acesso. Pois ao sair ou estar longe de um ponto de acesso ao qual estava conectado, automaticamente se conecta a outro ponto de acesso que ofereça um sinal mais forte. Ou seja, o usuário pode transitar pelo ambiente que automaticamente vai se conectar a vários pontos de acesso, dependendo da distância em que esteja de um para o outro, de forma transparente.

É importante destacar que para uma rede sem fio ser ESS, ela precisa que os pontos de acesso estejam configurados da mesma maneira, com o SSID e senha em comum, além de ter pelo menos 10% de interseção entre a área de cobertura de um ponto de acesso ao outro.

4.2.1 CRIPTOGRAFIA E PROTOCOLOS

Assim como nas redes cabeadas, as redes sem fio também dispõem de uma camada de controle de acesso ao meio (MAC – Media Acess Control). Mas diferente destas, os dados precisam ser protegidos contra leitura de terceiros, pois eles trafegam no ar, que é um meio não guiado. Sendo assim, o uso de um protocolo de criptografia na rede é essencial, pois embaralha os dados que trafegam no ar. Mesmo

que um hacker tenha acesso aos pacotes por meio de captura, ele não conseguirá ler os dados, pois estarão todos criptografados, o que torna seu conteúdo ilegível.

Os algoritmos de criptografia fazem uso de dois tipos de chaves, a pública e a privada. Quando uma estação quer se comunicar com outra estação na rede, ela criptografa os dados usando uma chave pública da estação de destino, e os envia pela rede. E assim que a estação de destino recebe a mensagem, ela usa sua chave privada para descriptografar a mensagem para poder ler seu conteúdo.

Como fica evidente, alguém só poderá ler os dados se tiver a chave privada. Se alguém roubar a chave pública de uma estação da rede, ainda assim não terá como descriptografar as mensagens endereçadas a ela, pois a chave pública só serve para criptografar os dados.

Além disso, as chaves criptográficas nunca circulam na rede. Elas são negociadas individualmente entre o ponto de acesso e as estações. Quando uma estação quer se conectar a uma rede, ela envia um quadro de autenticação para o ponto de acesso, que responde enviando um quadro de autenticação com um texto de verificação para a estação. A estação então tem que codificar esse texto com a chave específica que foi configurada, e enviar de volta para o ponto de acesso usando um quadro de autenticação. O ponto de acesso decodifica o texto, obtendo um resultado. Esse resultado então é comparado com o resultado que ele obteria com o uso da chave que foi previamente configurada. Se os resultados forem os mesmos, o ponto de acesso permite a autenticação e conexão da estação a rede sem fio, através do envio de um quadro de autenticação de resposta.

Por meio deste mecanismo, em nenhum momento as chaves circulam na rede. A estação tem que saber previamente qual a chave criptográfica configurada no ponto de acesso, para assim adentrar na rede.

A chave criptográfica é criada a partir de uma senha que é configurada no ponto de acesso. Mas essa senha não é a chave usada. A chave é criada por meio da senha, usando um algoritmo matemático.

Protocolos de criptografia

Existem três versões de protocolo de criptografia criados para uso em uma rede sem fio. São eles, o WEP, WPA e WPA2.

WEP (Wired Equivalent Privacy): Faz uso de um algoritmo chamado RC4, que é um codificador de fluxo. Em teoria a chave de criptografia teria de estar em constante mudança. Em sua chave de criptografia, se faz presente dois componentes: Uma chave que pode ter tamanho de 40, 104 ou 128 bits, chamada de chave raiz. E o outro componente é um vetor de inicialização de 24 bits, que muda a cada nova transmissão, e que circula junto com os dados codificados contidos no quadro. A fraqueza e vulnerabilidade contida neste protocolo de criptografia, é o tamanho de seu vetor de inicialização, que contém somente 24 bits.

> O problema do WEP é que o vetor de inicialização é muito curto, com apenas 24 bits, o que faz com que o seu valor seja repetido de tempos em tempos (a cada 2^{24} quadros transmitidos). Isto permite vários tipos de ataque analisando-se o tráfego da rede, e existem vários programas disponíveis na internet com esta finalidade. Dependendo do tráfego da rede é possível quebrar esta criptografia em poucos minutos. (TORRES, 2016, p. 117)

Embora ainda suportado por pontos de aceso e estações, o uso desse protocolo caiu em desuso.

WPA (Wi-fi Protected Acess): O WPA foi criado para substituir o WEP, tendo como objetivo central não ser vulnerável como o mesmo. O WPA usa o mesmo algoritmo RC4 do WEP, mas adotou o uso de um novo protocolo para gerar chaves criptográficas, de nome TKIP (Temporal Key Integrity Protocol – Protocolo de Integridade por Chave Temporal).

No WPA, o vetor de inicialização também está presente, e seu tamanho foi aumentado para 48 bits. Esse vetor de inicialização é usado para numerar os quadros, minimizando o risco de ataques do tipo replay, onde um quadro é capturado e retransmitido para a rede. Além disso o WPA possui outras diferenças e melhorias em relação ao WEP, como a maneira em que a chave de criptografia é usada pelo algoritmo RC4.

WPA2 (Wi-fi Protected Acess 2): Protocolo de criptografia mais seguro, de uso comum hoje em dia. Em uma rede sem fio, é sempre recomendado o uso deste protocolo em detrimento do WPA e do WEP. Usa um novo algoritmo para criptografia dos dados, de nome AES (Advanced Encryption Standard), além de uma negociação de quatro vias para a troca de chaves. Também pode-se usar um servidor RADIUS (Remote Authentication Dial In User Service) para autenticação, entre outros recursos.

Segundo Torres (2014), o protocolo WPA2 é muito mais seguro que o WPA e o WEP, devendo a razão disso por fazer uso do processo de autenticação em quatro vias e pela forma como as chaves são geradas.

4.2.2 FREQUÊNCIAS

Redes sem fio trabalham transmitindo e recebendo ondas de rádio. Atualmente duas frequências são usadas, 2.4 e 5 GHz (Gigahertz). Elas são liberadas para uso, pois não dependem de autorização especial do governo. Dependendo do ambiente e cenário, há de se optar pelo uso de uma ou outra, ou até mesmo as duas.

2.4 GHz

A frequência de 2.4 GHz (Gigahertz) é amplamente usada, sendo a mais comum. Por isso a mesma está saturada em muitos ambientes, pois vários dispositivos completamente diferentes de um ponto de acesso trabalham operando nesta frequência, o que gera bastante interferência.

Esta frequência faz uso de 14 canais, divididos por uma pequena faixa de frequência que começa de 2.401 MHz (Megahertz) até a frequência de 2.483,5 MHz no Brasil e na maioria dos países do mundo (2.473 MHz nos Estados Unidos). Os canais 1 a 12 estão separados por um espaço de 5 MHz entre eles, enquanto os canais 13 e 14 estão com 12 MHz de espaço. É importante citar que dependendo do país, um ou mais canais não podem ser usados. No Brasil por exemplo, só é permitido o uso dos canais de 1 ao 11.

Por conter comente 5 MHz de espaço entre a maioria dos canais, na prática acontece que se for usado pontos de acesso configurados para usar canais próximos, como 1 e 4, acaba ocorrendo sobreposição, pois um canal invade a faixa de outro. Pois no padrão IEEE 802.11 a largura do canal pode ser de 20 ou 40 MHz, provocando sobreposição entre canais próximos. Aqui no Brasil por exemplo, somente os canais 1, 6 e 9 tem espaço suficiente para possibilitar seu uso entre roteadores próximos, sem que ocorra sobreposição de canais.

5 GHz

A faixa de frequência de 5 GHz é bem menos usada que a de 2.4 GHz. Sendo assim, um dos motivos que possibilita na prática maiores taxas de transferência. Começa de 5.150 MHz e vai até 5.350 MHz e depois de 5.725 MHz indo até 5.835

MHz. É dividida em 3 bandas: Banda inferior (5.150 MHz até 5.250 MHz), Banda central (5.250 MHz até 5.350 MHz) e Banda superior (5.725 MHz até 5.825 MHz). A banda inferior e a banda superior são somente para uso em ambiente interno. Já a banda central pode ser de uso interno como externo.

No IEEE 802.11, a faixa de frequência de 5 GHz é dividida em 13 canais que não se sobrepõem, pois o espaço entre cada canal é de 20 Mhz. Em redes sem fio operando nessa faixa de frequência, pode-se alcançar no padrão 802.11ac, velocidade acima dos 1000 Mbps (Megabits por segundo), em contraste com a faixa de frequência dos 2.4 GHz.

A desvantagem de usar essa frequência em uma rede sem fio, é que o sinal é abrange uma curta distância. Além disso, o sinal é atenuado por obstáculos mais facilmente do que numa rede 2.4 GHz. Por isso, o ideal é se usar um roteador sem fio que trabalhe com as duas frequências simultaneamente, servindo dispositivos que estão por perto e trabalhem com 5 GHz, assim como dispositivos que só trabalhem com 2.4 GHz ou estejam mais afastados para usufruir do 5 GHz.

4.2.3 IEEE 802.11n e IEEE 802.11ac

Estes protocolos entre outras coisas, ditam a velocidade máxima da rede. Começando desde o IEEE 802.11 original em 1997 que possibilitava alcançar somente 2 Mbps, e usava a frequência de 2.4 GHz.

Desde então esses padrões evoluíram muito, incorporando aumento da velocidade máxima e uso da frequência de 5 GHz. Indo do 802.11 até o 802.11 ac, que possibilita velocidade máxima acima de 1000 Mbps.

Figura 25 – Evolução do padrão IEEE 802.11

Standard	Frequency Band	Bandwidth	Modulation Scheme	Channel Arch.	Maximum Data Rate
802.11	2.4 GHz	20 MHz	BPSK to 256-QAM	DSSS, FHSS	2 Mbps
b	2.4 GHz	21 MHz	BPSK to 256-QAM	CCK, DSSS	11 Mbps
a	5 GHz	22 MHz	BPSK to 256-QAM	OFDM	54 Mbps
g	2.4 GHz	23 MHz	BPSK to 256-QAM	DSSS, OFDM	54 Mbps
n	2.4 GHz, 5 GHz	24 MHz and 40 MHz	BPSK to 256-QAM	OFDM	600 Mbps
ac	5 GHz	20, 40, 80, 80+80= 160 MHz	BPSK to 256-QAM	OFDM	6.93 Gbps

Fonte: mwrf.com (2015)

802.11n

Este padrão foi pensado para se atingir velocidade acima de 100 Mbps na prática. O grande diferencial deste padrão em relação a seus antecessores está no uso da técnica MIMO (Multiple Input, Multiple Output – Múltipla Entrada, Múltipla Saída), em que se combina o uso de várias antenas no roteador sem fio, operando independentemente uma da outra, enviando e recebendo dados, para se conseguir maior taxa de transferência prática.

No 802.11n pode-se optar por usar 2.4 GHz ou 5 GHz, com canais de 20 ou 40 MHz, havendo sobreposição entre eles. A taxa de transferência prática pode variar muito, porque depende de uma série de fatores, como: número de antenas usadas, tamanho do canal, intervalo de guarda, modulação e taxa de codificação. Por isso é incorreto delimitar uma velocidade somente pelo roteador e estação ser 802.11n. Um fato que corrobora isso, é que os fabricantes de equipamentos de rede por exemplo, lançam equipamentos que trabalham no padrão 802.11n, mas que suportam diferentes velocidades entre si, dependendo se é um equipamento entrada, intermediário ou topo de linha.

802.11ac

Se o padrão 802.11n foi desenvolvido para oferecer velocidades acima de 100 Mbps, o padrão 802.11ac foi desenvolvido para oferecer velocidade na faixa dos Gbps. Sendo assim, trazendo a velocidade das redes cabeadas gigabit ethernet para o mundo das redes sem fio.

Este padrão só opera na faixa de frequência de 5 GHz, é compatível com o padrão 802.11n e também faz uso da técnica MIMO, permitindo configurações com variado número de antenas. Possibilita uso de canais com largura de 80 MHz ou 160 MHz.

Equipamentos que trabalham com este padrão já são comuns hoje em dia. Porém geralmente os mesmos possuem outro transmissor embutido que trabalha também com o padrão 802.11n, de 2.4 GHz, por conta do curto alcance da frequência 5GHz.

É importante lembrar que alcance do sinal e velocidade de transferência tem uma relação em comum, pois quanto mais distante do ponto de acesso, menor a velocidade obtida. E quanto mais perto, maior a velocidade. Toda rede sem fio tem um alcance que pode variar na prática, por conta do ambiente ter ou não muitos obstáculos, fontes de interferências próximas, entre outros fatores, resultando em uma taxa de transferência que pode variar muito na prática.

4.3 ROTEADOR SEM FIO E CONFIGURAÇÕES DE REDE APLICADAS

Hoje em dia os roteadores sem fio domésticos trabalham com o padrão 802.11n, além do 802.11ac. Inclusive com os dois padrões ao mesmo tempo, criando uma rede de 2.4 GHz e uma outra de 5 GHz. O padrão 802.11ac oferece velocidades acima de 1000 Mbps, o que é um grande avanço se tratando de redes sem fio. Já os demais padrões antes do 802.11n, caíram em desuso com o tempo, devido suas baixas velocidades.

Como é de conhecimento comum na área, a frequência de 2.4 GHz na maioria dos cenários está saturada, sendo comum sofrer de interferência por outros dispositivos próximos que trabalham nessa mesma frequência, como o micro-ondas, telefone sem fio, etc. Além disso muitos dispositivos hoje em dia já são fabricados

para trabalhar na frequência de 5 GHz, como muitos smartphones por exemplo, diminuindo um pouco a necessidade de sempre se usar essa frequência em redes sem fio.

Dado estes fatos, devemos configurar o roteador para trabalhar com essas duas frequências, por meio de duas redes. Pois assim os dispositivos que tiverem suporte a 5 GHz, irão se conectar na rede 5 GHz.

Outra evolução das redes sem fio diz respeito à segurança, especificamente aos protocolos de criptografia. Primeiro com o WEP, que logo se provou falho e inseguro. Em seguida com o WPA, e depois com o WPA2 que é a versão que usamos hoje em dia.

Diante da explanação dessas informações acerca das redes sem fio e roteadores, este trabalho mostrará como foi feita a configuração do roteador usado no laboratório de informática.

Atualização de Firmware: Ignorado por muitos administradores de rede, mas de muita importância. A atualização de firmware minimiza a chance de ataques automatizados contra os dispositivos de rede, incluindo-se o roteador. Por isso é importante verificar periodicamente se existe um firmware mais atualizado. Pois o mesmo geralmente traz correção de bugs, brechas e vulnerabilidades. A lista de firmware para um modelo de roteador é encontrada no site de seu fabricante, geralmente na parte destinada a downloads.

Deve-se atentar para alguns detalhes antes da atualização, como estar sempre conectado ao roteador por meio de cabo, e também atentar-se para a versão do roteador. Um mesmo modelo de roteador pode ter diferentes versões, como é o caso deste modelo Archer C9 usado neste trabalho. Por isso essa informação deve ser checada, de preferência por meio de acesso físico ao roteador, olhando-se a etiqueta contida na parte inferior do mesmo. Esses detalhes são importantes pois uma atualização de firmware malsucedida pode até inutilizar um equipamento.

MODELO: Archer c9
VERSÃO: v2.0
VERSÃO DO FIRMWARE (INSTALADO): 4.0.0
VERSÃO DO FIRWARE (ATUAL): 4.0.0

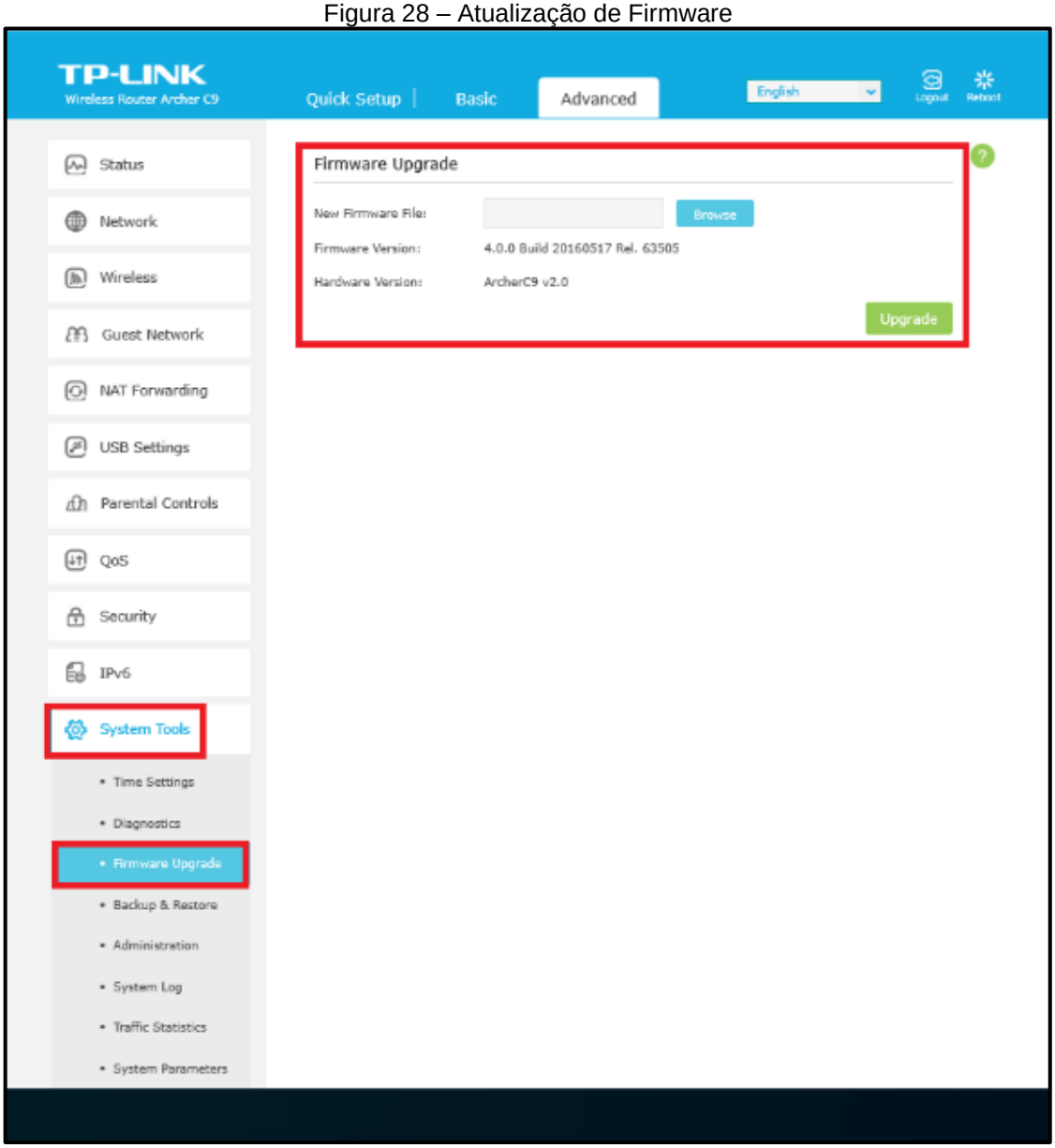
Figura 26 – Roteador Archer C9: Visão frontal

Fonte: tp-link.com (2019)

Figura 27 – Roteador Archer C9: Visão traseira

Fonte: tp-link.com (2019)

Figura 28 – Atualização de Firmware



Fonte: Autoria Própria (2019)

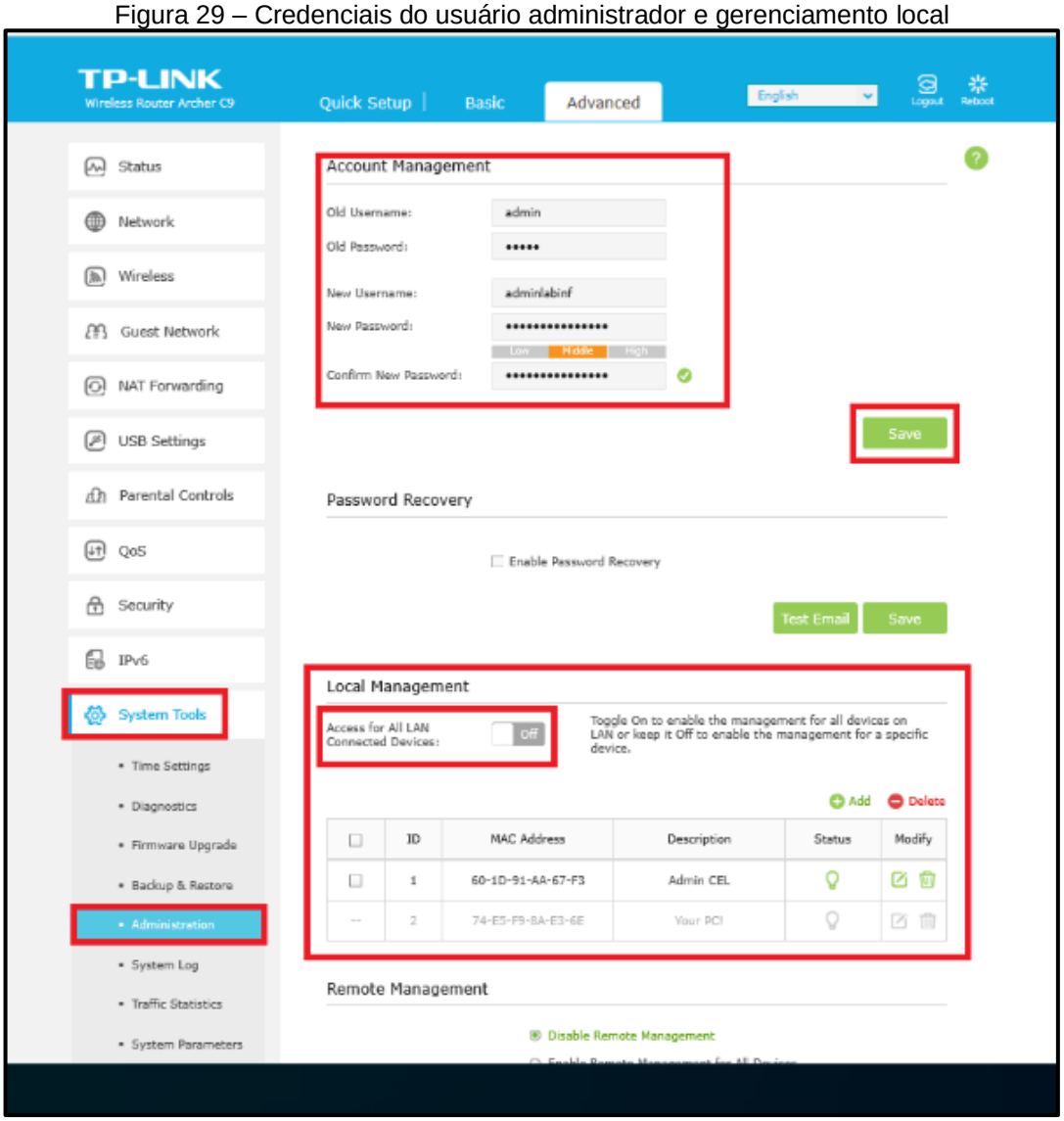
Nome e senha do usuário administrador: De nada adianta se configurar bem um roteador, se não se muda a senha e usuário padrão. Em alguns dispositivos mais baratos, o firmware não permite que o nome do usuário administrador seja trocado, somente sua senha. Mas no modelo de roteador usado neste trabalho, pode-se alterar livremente o nome e a senha do usuário administrador. Isso impede que algum usuário da rede com acesso ao usuário e senha padrão fornecido pelo fabricante, desconfigure o roteador e comprometa sua segurança, deixando em risco os dispositivos da rede.

Recomenda-se que a senha seja complexa, o que envolve uso de caractere especial e número pelo menos. Isso para não ficar semelhante a nenhuma senha padrão fornecida pelos fabricantes de dispositivos de rede.

USUÁRIO: adminlabinf

SENHA: #@adminlab@#2019

Figura 29 – Credenciais do usuário administrador e gerenciamento local



Fonte: Autoria Própria (2019)

Gerenciamento local do roteador: Refere-se à administração do roteador, podendo o administrador de rede permitir que qualquer dispositivo conectado à rede local possa acessar a página de login para configuração do roteador, ou somente um ou mais determinados dispositivos cadastrados possam acessar a página de configuração do roteador.

Neste cenário, a opção que permite que todos os dispositivos da LAN possam acessar a página de configuração do roteador, foi desativada para oferecer maior segurança. E em seguida foram cadastrados os dispositivos pertencentes ao administrador da rede, por meio do fornecimento do endereço MAC da placa rede

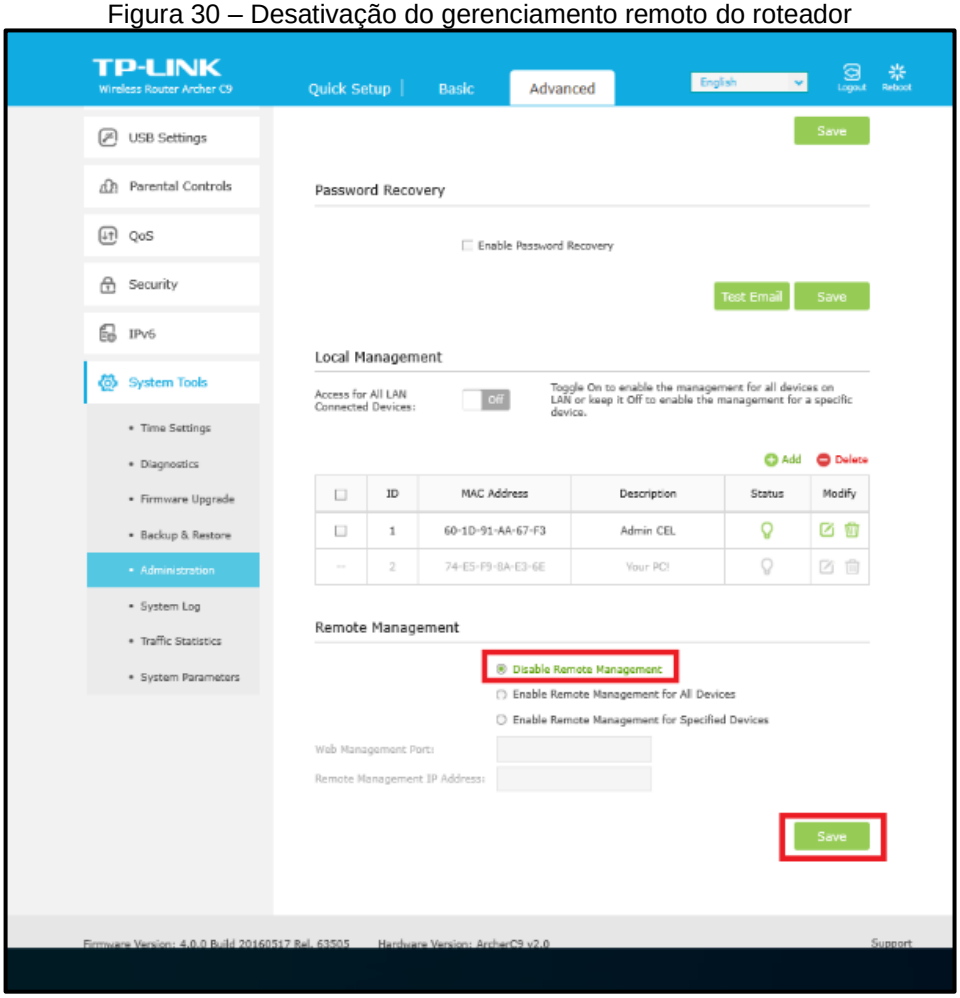
cabeada ou sem fio, e descrição do dispositivo para ajudar o administrador a identificá-lo.

Gerenciamento remoto do roteador: Refere-se à administração remota do roteador, ou seja, de fora da rede local. Essa opção é interessante, pois permite que se possa acessar o roteador mesmo em outra rede, permitindo flexibilidade ao administrador da rede. Este modelo de roteador permite que seja definido se o acesso a página de login por meio do IP do roteador se dará a qualquer dispositivo ou a um dispositivo específico. Similar ao que acontece na opção de gerenciamento local.

Neste cenário essa opção foi desabilitada, devido a não necessidade de um suporte remoto, levando-se em conta que o prédio da faculdade X já dispõe de uma equipe que presta suporte técnico em todos os dias de funcionamento do mesmo.

Além de minimizar a chance de ataques direcionados ao roteador, pôr não o expor a internet.

Figura 30 – Desativação do gerenciamento remoto do roteador



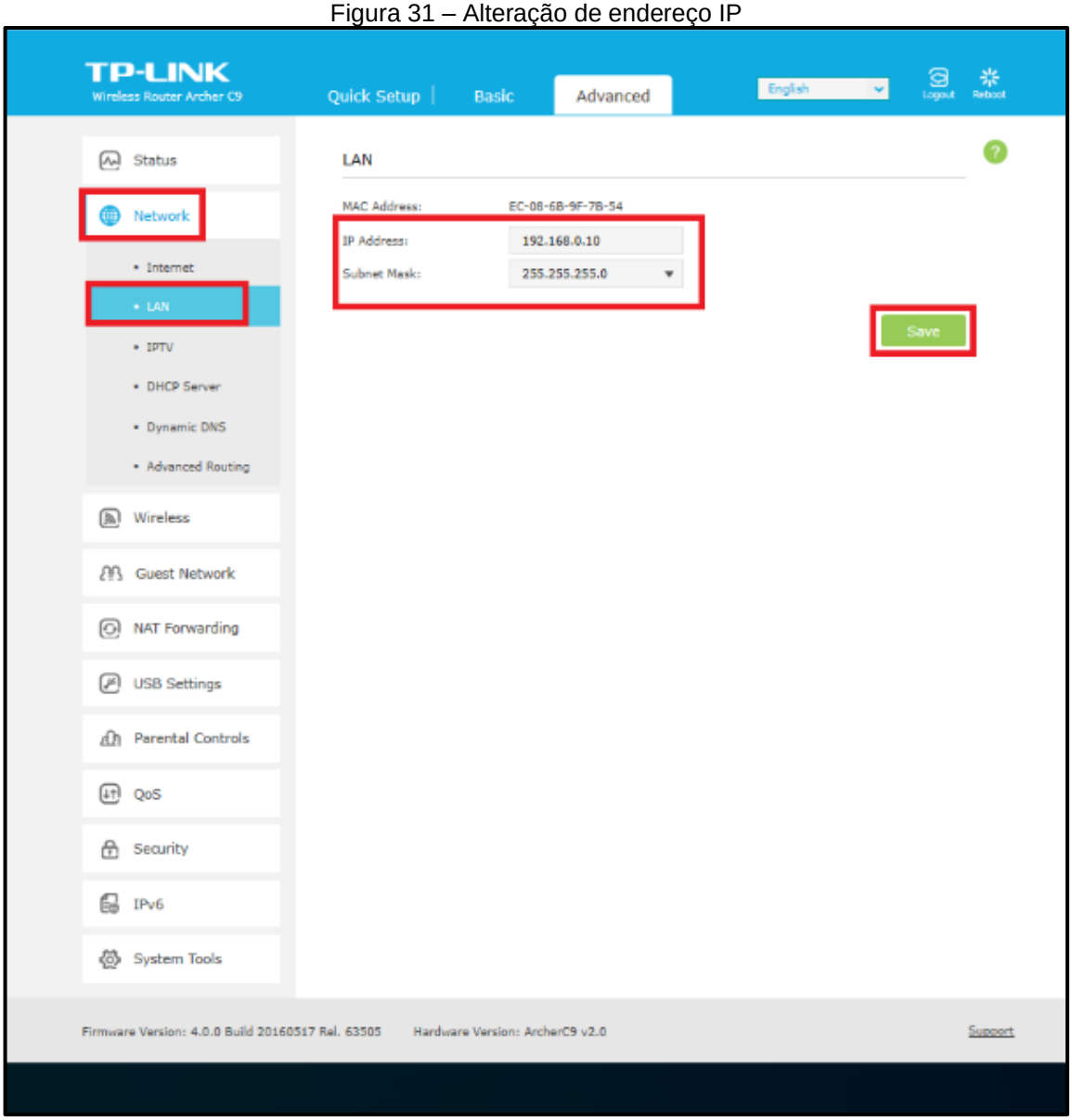
Fonte: Autoria Própria (2019)

IP fixo para o roteador: O roteador como atua como um dispositivo que servirá aos demais dispositivos sem fio da rede, precisa de um IP fixo dentro da rede local já existente no prédio, para se comunicar com os demais dispositivos da rede, incluindo o gateway.

IP: 192.168.0.10

MÁSCARA DE SUBREDE: 255.255.255.0

Figura 31 – Alteração de endereço IP



Fonte: Autoria Própria (2019)

Redes sem fio: Aqui se encontra uma série de configurações destinadas a(as) rede(s) sem fio. Onde foi definido as seguintes configurações por rede.

REGIÃO: Brasil

REDE 2.4 Ghz

SSID (NOME DA REDE): LAB_INFORMATICA_2.4GHZ

SEGURANÇA: WPA2 (Personal)

VERSÃO: WPA2-PSK

ENCRIPTAÇÃO: AES

SENHA DA REDE: 2019l@binf2019

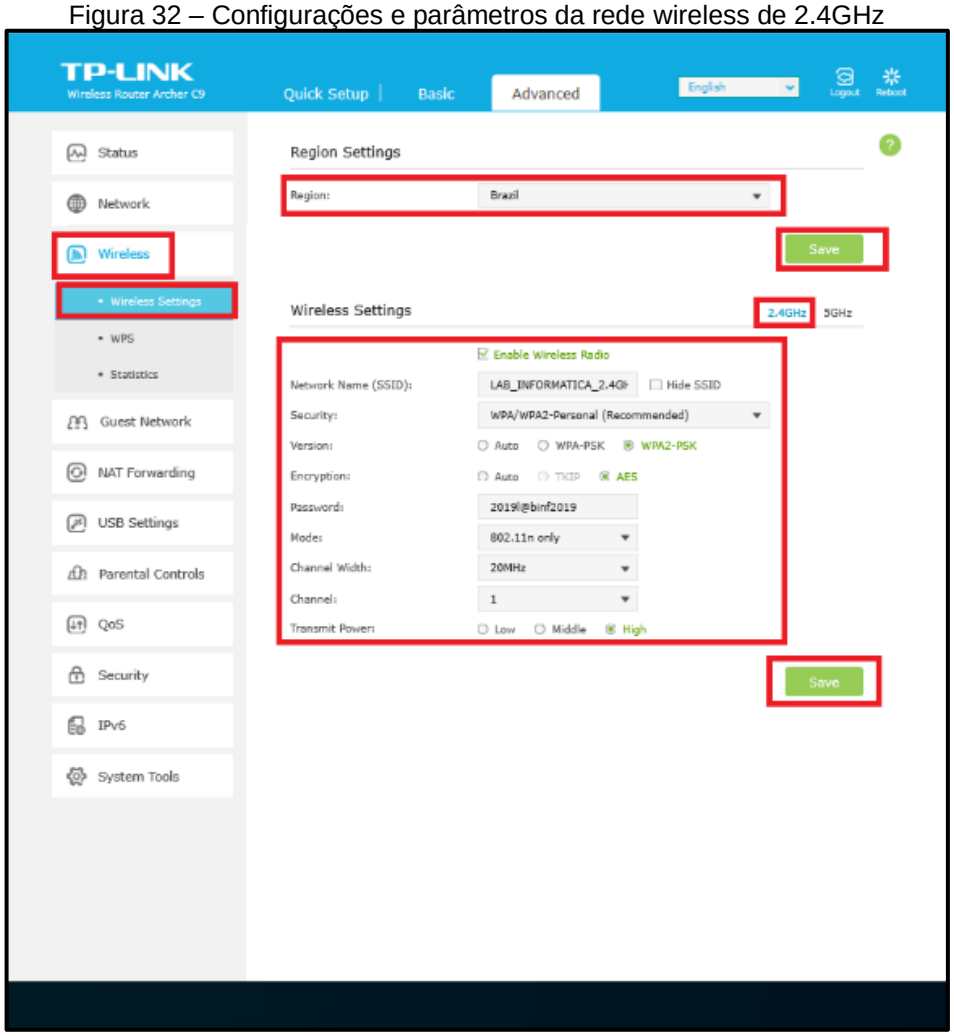
MODO: Somente 802.11n

LARGURA DO CANAL: 20 Mhz

CANAL: 1

PODER DE TRANSMISSÃO: Alto

Figura 32 – Configurações e parâmetros da rede wireless de 2.4GHz



Fonte: Autoria Própria (2019)

REDE 5 Ghz

SSID (NOME DA REDE): LAB_INFORMATICA_5GHZ

SEGURANÇA: WPA2 (Personal)

VERSÃO: WPA2-PSK

ENCRIPTAÇÃO: AES

SENHA DA REDE: 2019labinf_2019

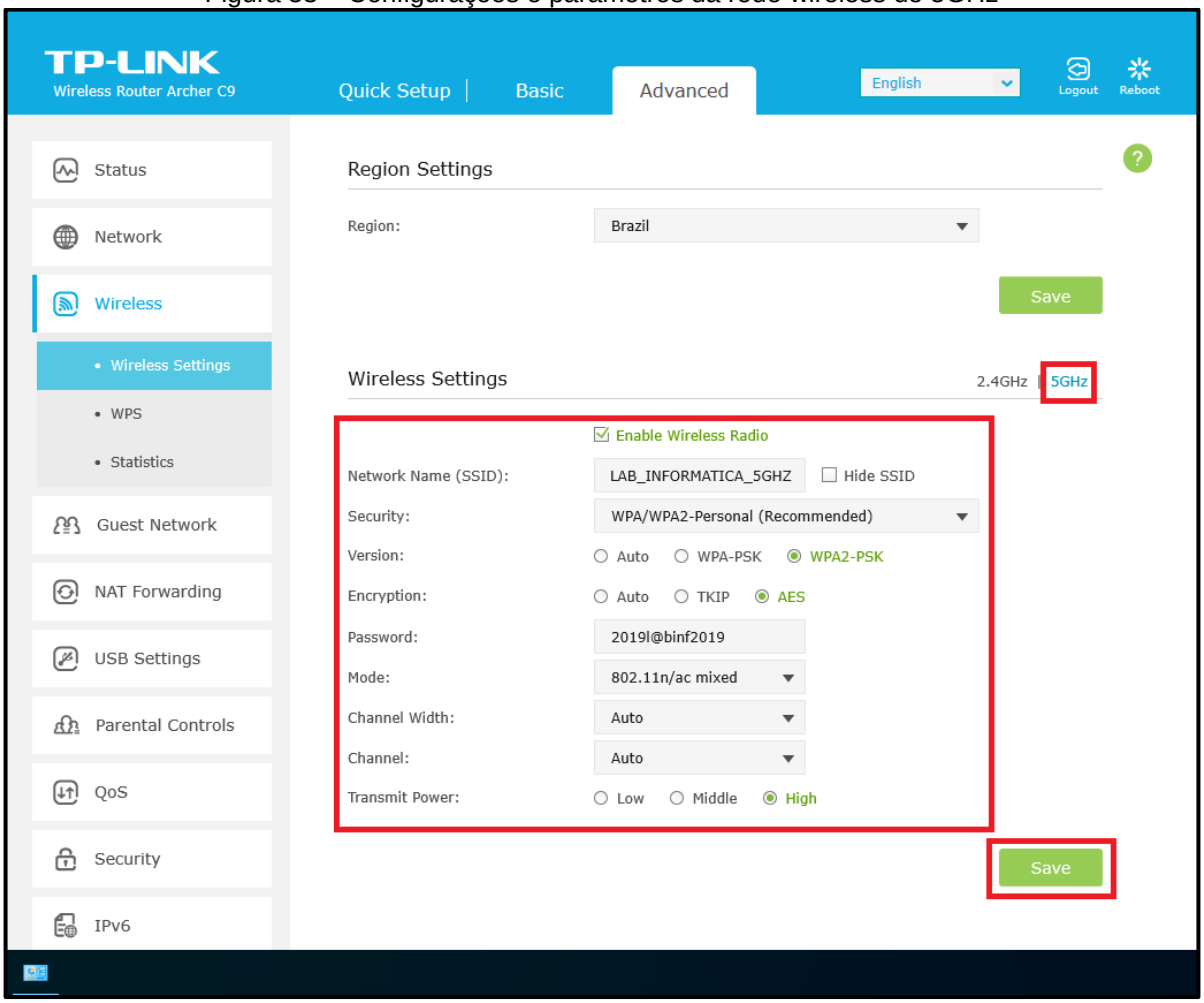
MODO: Misto 802.11n/ac

LARGURA DO CANAL: Automático

CANAL: Automático

PODER DE TRANSMISSÃO: Alto

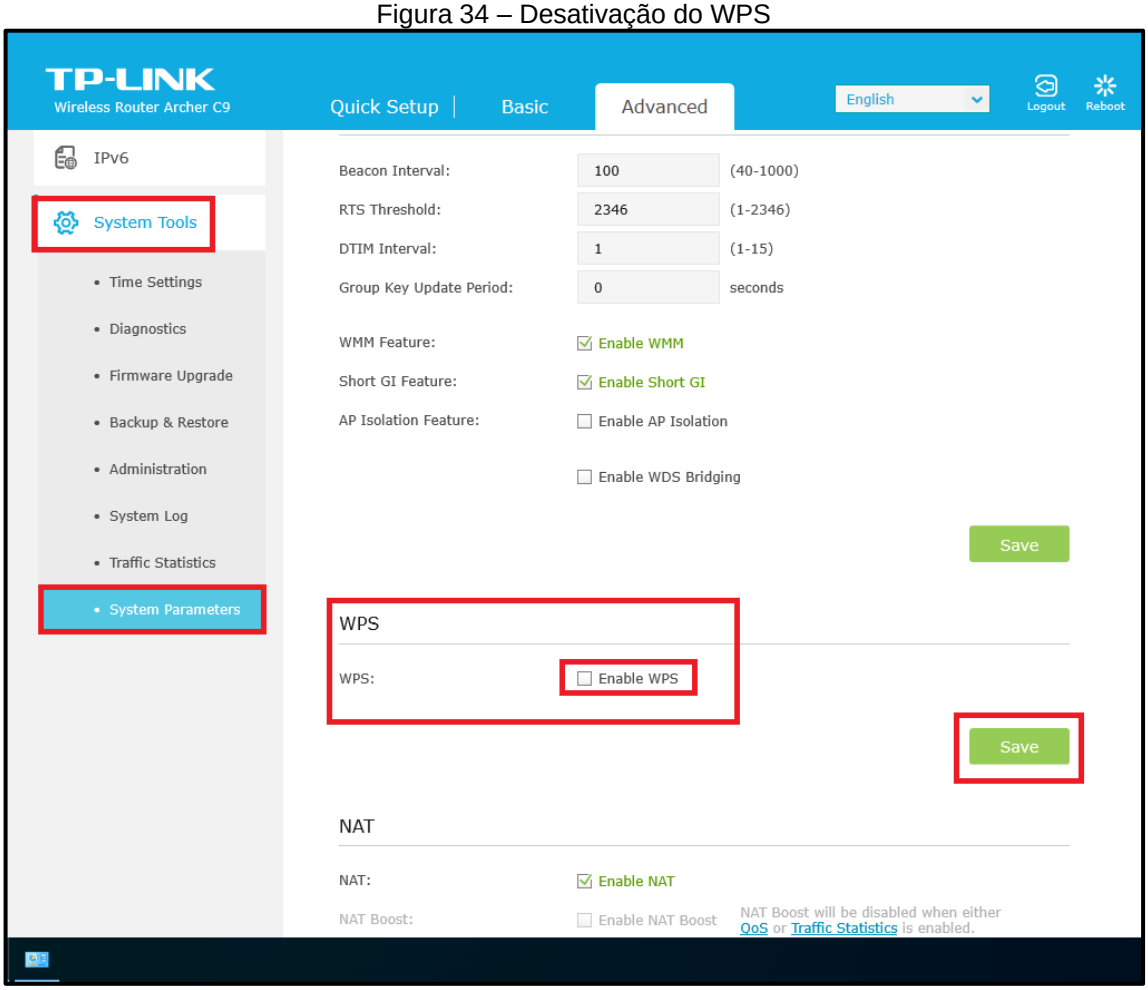
Figura 33 – Configurações e parâmetros da rede wireless de 5GHz



Fonte: Autoria Própria (2019)

WPS (Wi-fi Protected Setup): O protocolo WPS simplifica o acesso de um dispositivo a rede, por meio do acesso a ela pressionando-se o botão WPS existente no roteador e em seguida no dispositivo, ou por meio de um PIN (Personal Identification Number). Mas em contrapartida este protocolo é inseguro e viabiliza tentativas de ataques por meio da quebra do pin configurado no roteador. Diante disso, o WPS caiu em desuso e é sempre recomendado que se desative o recurso em qualquer roteador sem fio existente em uma rede.

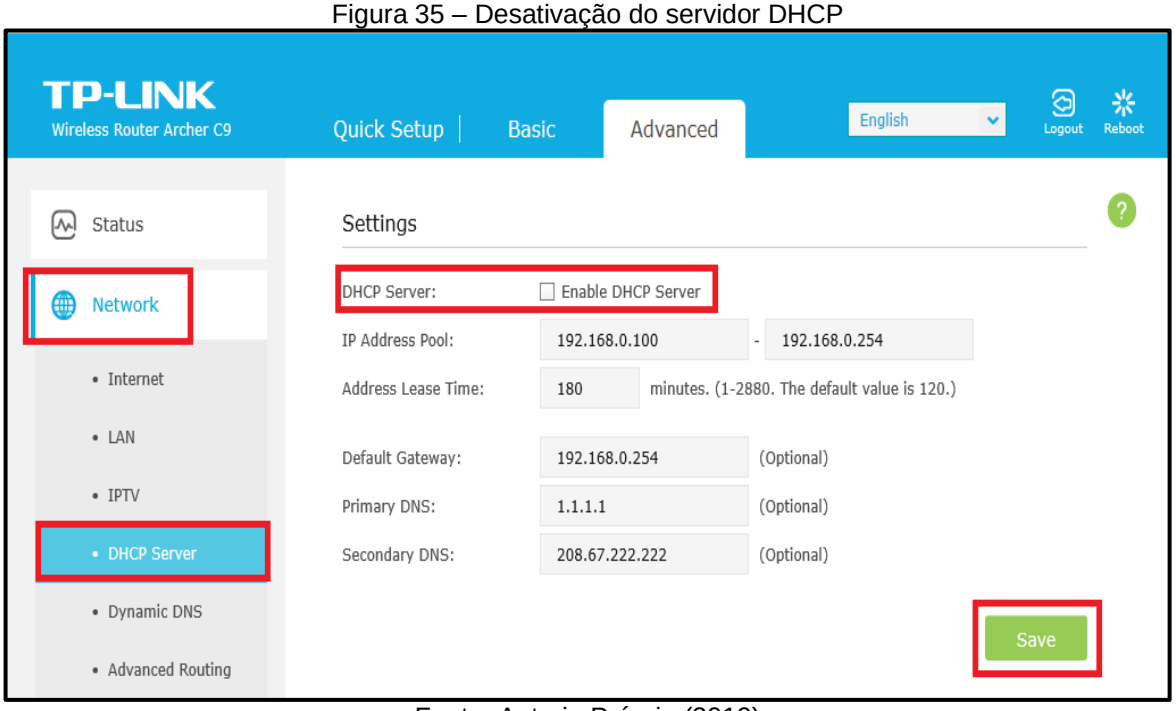
Figura 34 – Desativação do WPS



Fonte: Autoria Própria (2019)

DHCP (Dynamic Host Configuration Protocol) e Modo Bridge: Nessa parte se desativa o servidor DHCP do roteador, pois o mesmo irá funcionar em bridge. O modo bridge é uma ponte. Isto significa que o roteador só repassará as informações de IP, Máscara de sub-rede, Gateway e DNS (Dynamic Host Configuration Protocol) vindos do firewall existente na rede, toda vez que um dispositivo desejar se conectar à rede e precisar dessas informações. O firewall existente na rede é o PFSENSE.

Figura 35 – Desativação do servidor DHCP



Fonte: Autoria Própria (2019)

QOS (Quality of Service): O QOS serve para definição de uma prioridade de acesso à internet na rede para os dispositivos cadastrados. No cenário deste trabalho, que é um laboratório de informática, foi cadastrado o primeiro computador, e posteriormente os demais computadores de mesa pertencentes ao laboratório. Isso significa que esses computadores terão prioridade ao se conectarem na internet, em detrimento dos outros dispositivos de uso pessoal dos alunos e professores, como smartphones e notebooks.

Isso evita que algum aluno por exemplo esteja fazendo um download de um arquivo pesado na rede, que não tenha nada a ver com o conteúdo ministrado em questão, ocasionando lentidão de acesso a internet para o resto dos dispositivos que precisam de uma banda mínima para conclusão de suas tarefas, como: download de softwares usados nas aulas, acesso a sites de consulta, etc.

Foi medido primeiramente a velocidade de download e upload existente na prática em um horário onde a rede estava ociosa, para a partir dessas informações o QOS fazer a correta reserva de prioridade.

UPLOAD: 30 Mbps

DOWNLOAD: 100 Mbps

Após isso, foi definido por meio de porcentagem os valores de cada categoria de prioridade:

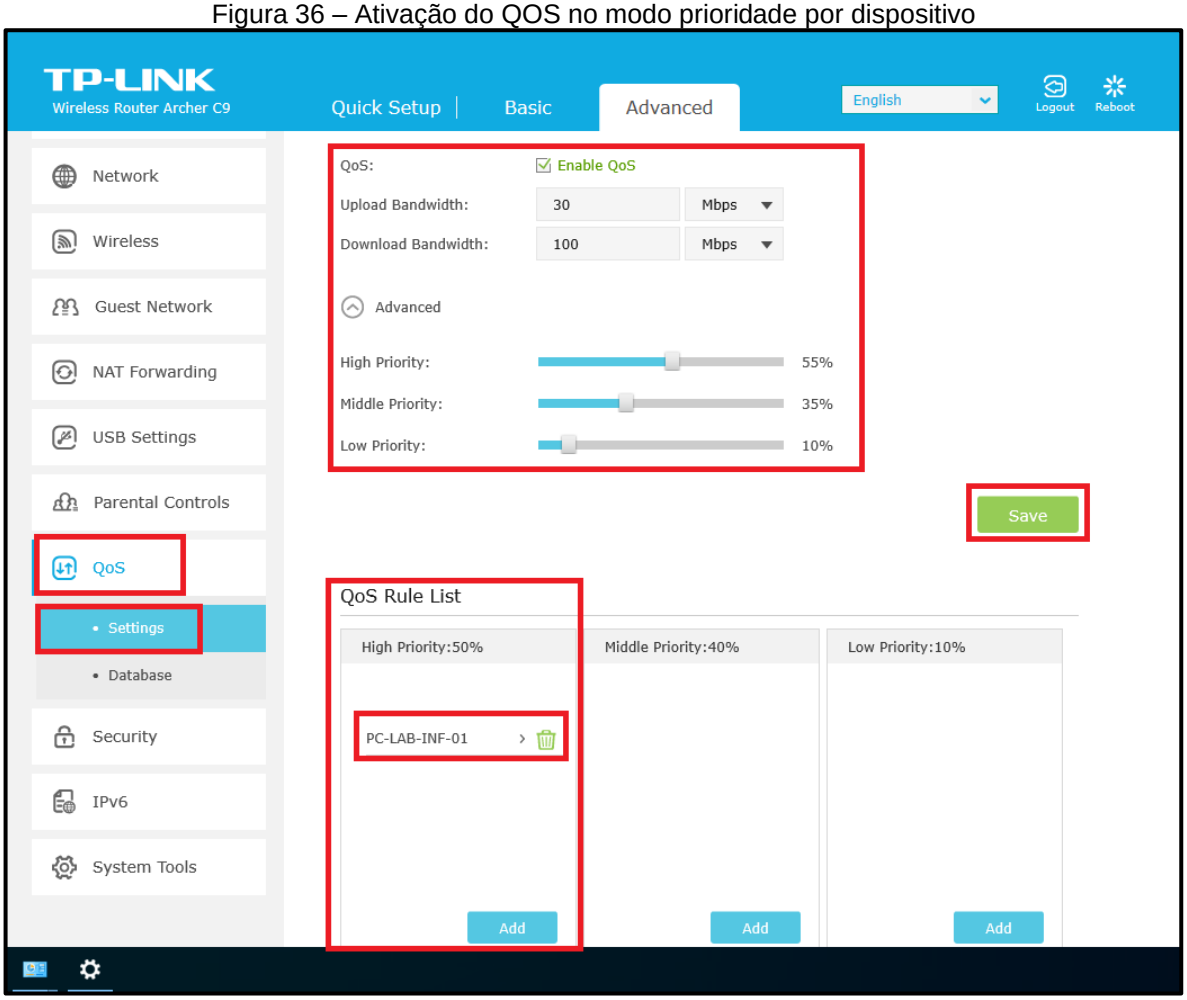
ALTA PRIORIDADE: 55%

MÉDIA PRIORIDADE: 35%

BAIXA PRIORIDADE: 10%

Em seguida foi incluído na lista de alta prioridade os computadores de mesa pertencentes ao laboratório. Essa inclusão não se deu por tipo de aplicação, e sim pela seleção da opção por dispositivo, pelo fornecimento do nome de cada computador e endereço MAC da placa de rede cabeada.

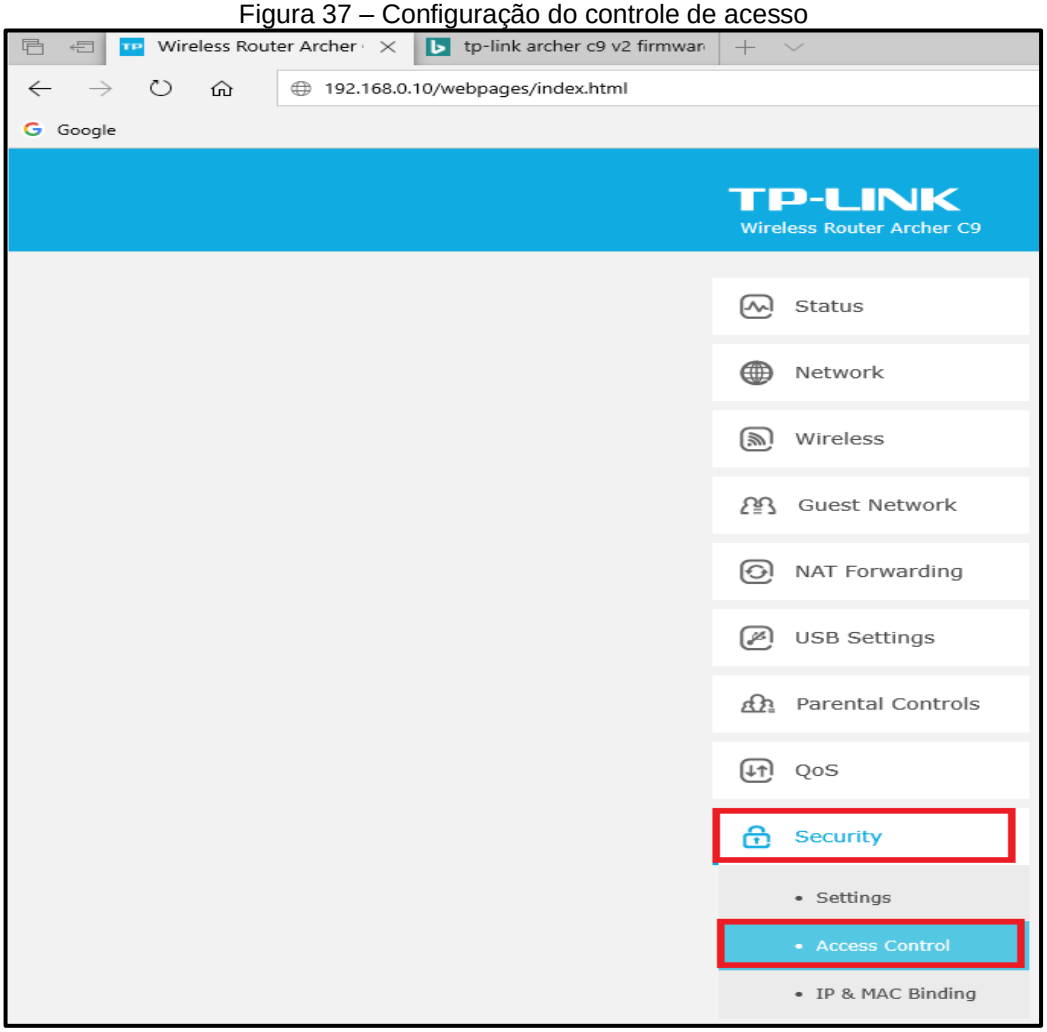
Figura 36 – Ativação do QOS no modo prioridade por dispositivo



Fonte: Autoria Própria (2019)

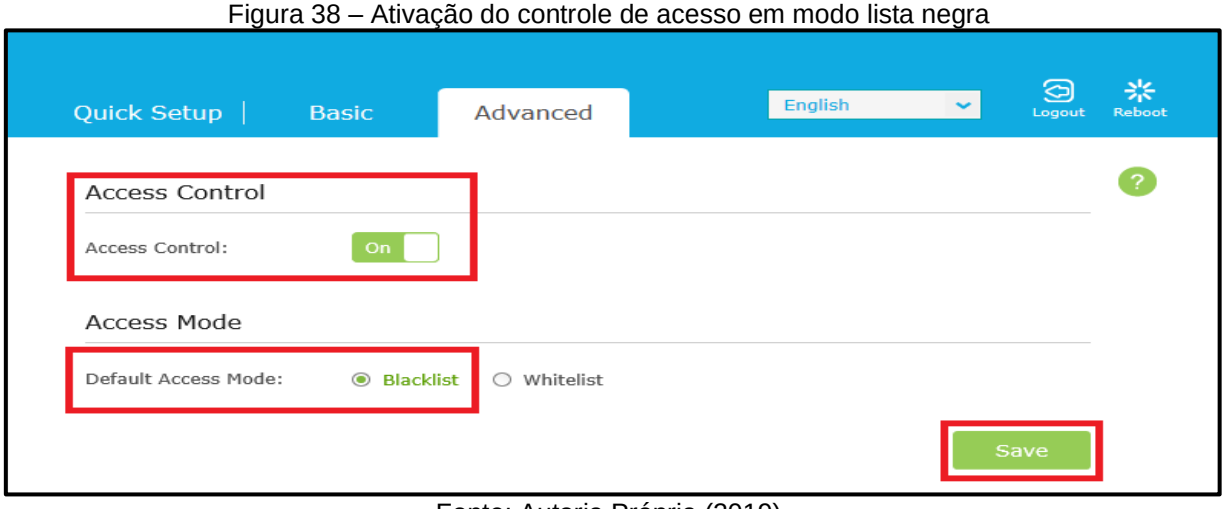
Controle de acesso: O controle de acesso permite bloquear rapidamente o acesso de um ou mais dispositivos na rede, por meio de uma blacklist (lista negra), assim como só permitir o acesso de determinados dispositivos na rede, por meio de uma whitelist (lista branca). Os dispositivos conectados são listados, permitindo ao administrador da rede bloquear cada um com apenas um clique. É recomendado deixar essa opção habilitada, para posteriormente bloquear rapidamente um dispositivo indesejado na rede.

Figura 37 – Configuração do controle de acesso



Fonte: Autoria Própria (2019)

Figura 38 – Ativação do controle de acesso em modo lista negra



Fonte: Autoria Própria (2019)

Região, data e hora, e idioma: Essas opções são importantes para as consultas do registro dos eventos presentes nos logs do sistema, pois permitem fornecer corretamente as informações de data e hora exata em que os eventos ocorreram. Através da escolha de um servidor NTP (Network Time Protocol), o roteador estará sempre configurado com o horário correto.

Foi configurado de acordo com o país e região de localização do roteador.

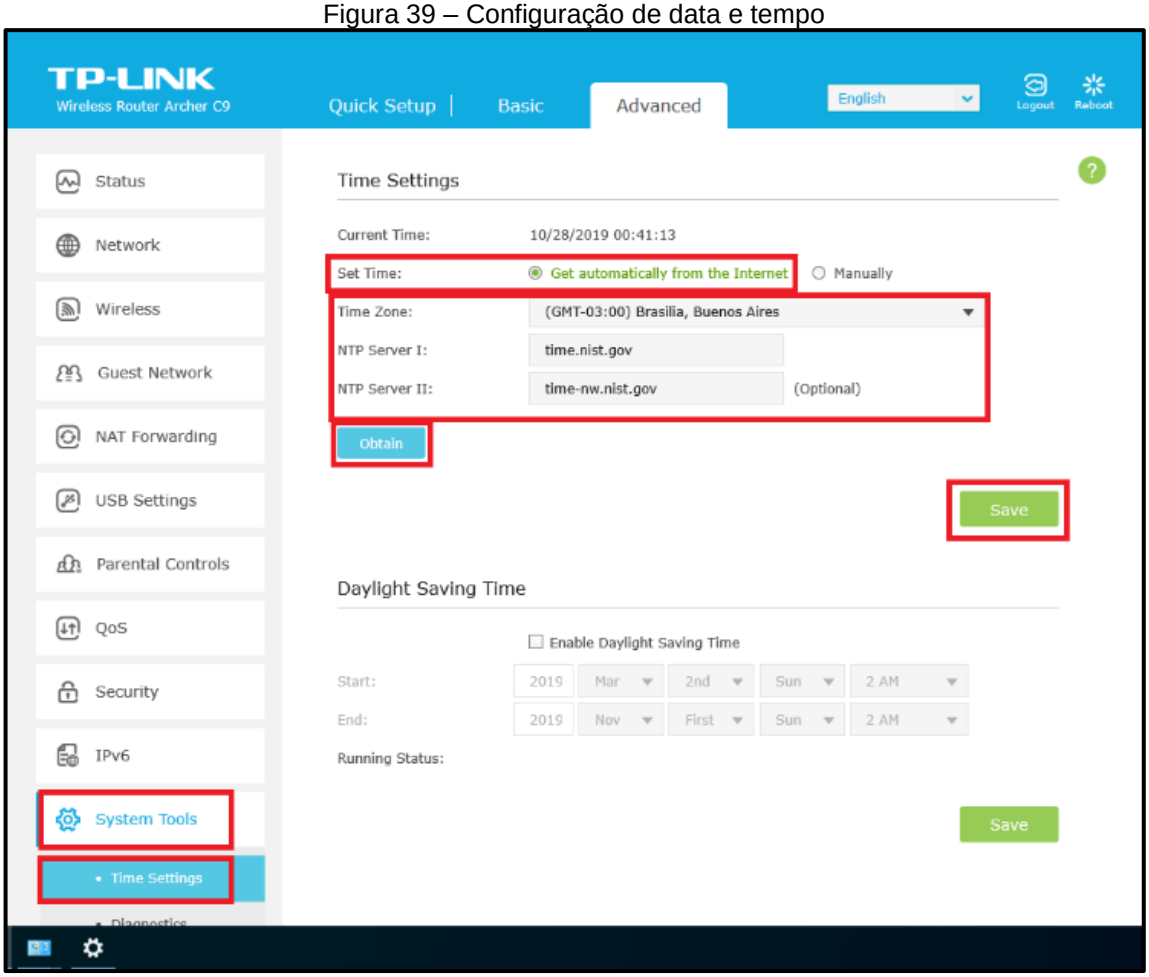
TEMPO: Obter automaticamente a partir da internet

FUSO HORÁRIO: (GMT-03:00) Brasília

SERVIDOR NTP I: time.nist.gov

SERVIDOR NTP II: time.nist.gov

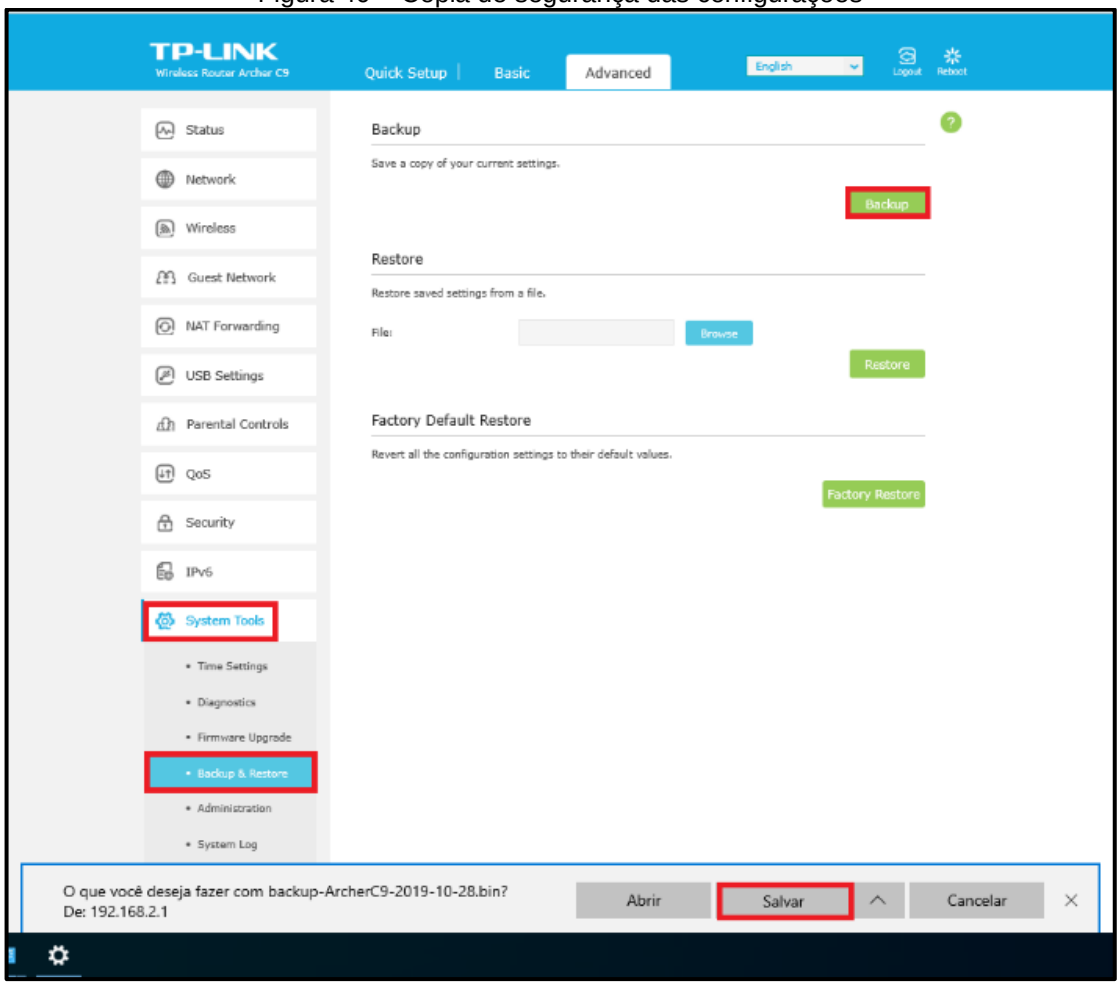
Figura 39 – Configuração de data e tempo



Fonte: Autoria Própria (2019)

Backup: Após a finalização das configurações, é muito importante sempre fazer o backup. O backup neste caso nada mais é que uma cópia de segurança de tudo que foi configurado. Pois no caso de algum problema, é só restaurar todas as configurações por meio do arquivo do backup, geralmente no salvo no formato .bin

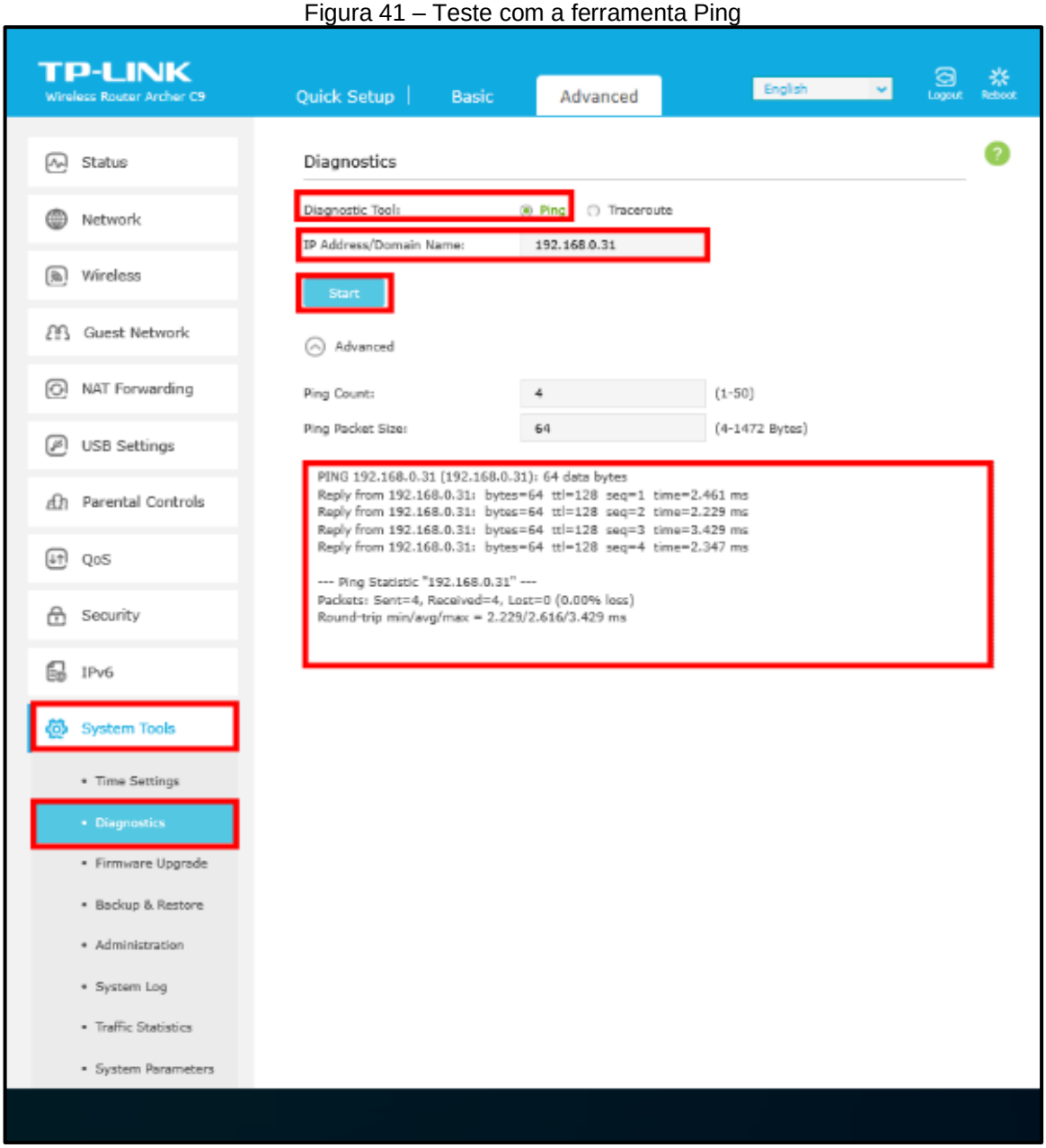
Figura 40 – Cópia de segurança das configurações



Fonte: Autoria Própria (2019)

Ping e Traceroute: Por último, foi feito um simples teste de comunicação e latência usando as ferramentas ping e traceroute presentes no próprio firmware do roteador. A ferramenta ping testa a comunicação entre outros dispositivos na rede local, enquanto a ferramenta traceroute traça o caminho até determinado domínio na internet. Por meio delas verifica-se há comunicação, tempo de latência entre a origem e o destino, perdas ou não de pacotes, etc. certificando-se se tudo está dentro do esperado.

Figura 41 – Teste com a ferramenta Ping



Fonte: Autoria Própria (2019)

Figura 42 – Teste com a ferramenta Traceroute

Fonte: Autoria Própria (2019)

Para finalizar este capítulo, abaixo estão listadas o resumo das configurações feitas no roteador sem fio do laboratório.

- Verificação da existência de firmware mais recente no site do fabricante;
- Configuração do nome e senha do usuário administrador;
- Habilitação do gerenciamento local do roteador somente para dispositivos específicos usados pelo administrador da rede;
- Desativação do gerenciamento remoto do roteador;
- Configuração de IP fixo dentro da faixa de rede local já existente e máscara de subrede usada na rede local;
- Configuração da rede 2.4 GHz;
- Configuração da rede 5 GHz;
- Desativação do protocolo WPS;
- Desativação do servidor DHCP, roteador em modo de funcionamento bridge;
- Habilitação do QOS por dispositivo, reservando alta prioridade para os pacotes de origem e destino provenientes dos computadores de mesa do laboratório;
- Habilitação do controle de acesso;
- Configuração dos parâmetros de região, data e hora;
- Backup de todas as configurações;
- Testes de diagnóstico, utilizando as ferramentas ping e traceroute presentes no firmware do roteador.

Após todas as configurações feitas e salvas, basta posicionar o roteador no centro do ambiente para melhor distribuição do sinal sem fio. Esse posicionamento leva em consideração a altura também. O roteador preciso estar acima dos demais objetos do ambiente, preferencialmente próximo ao teto.

Após todos esses passos o equipamento está apto para trabalhar da melhor forma, contribuindo com o bom desempenho da rede e proporcionando uma boa experiência aos usuários da rede sem fio.

5 COMPUTADORES DO LABORATÓRIO: CONFIGURAÇÕES

5.1 COMPUTADORES E CONFIGURAÇÕES DE REDE APLICADAS

Este trabalho não estaria completo se não houvesse uma visão geral das principais configurações de rede básicas adotadas no Windows 10, para o cenário deste trabalho.

Em geral computadores de mesa não precisam de nenhum método avançado para se conectarem a uma rede, especialmente se for por cabo, como é o cenário deste trabalho. É só conectar o cabo e automaticamente o computador estará munido de todas as configurações necessárias para se conectar à internet. Isso acontece pelo mesmo ser servido dos parâmetros necessários para conexão pela existência e resposta do servidor DHCP da rede, que neste caso é o firewall PFSENSE.

Porém é importante que alguns parâmetros sejam configurados para fins de uma melhor organização da rede.

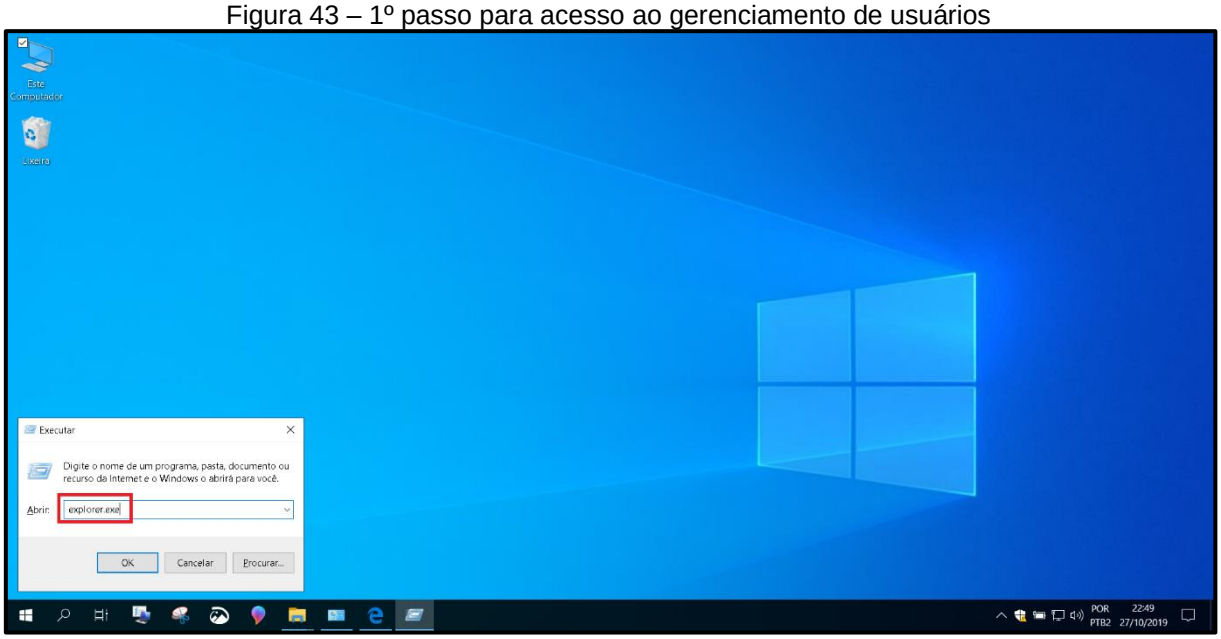
Alguns desses parâmetros são:

- Criação de conta com nome e senha padrão para todos os computadores, além da ativação e definição de senha do usuário administrador
- Nome e descrição padronizada de cada computador do laboratório
- Inserção de todos os computadores no grupo de trabalho já existente na rede local
- Endereço IP Fixo, Máscara de subrede, gateway e servidores DNS primário e secundário para cada computador do laboratório
- Definição do tipo de rede como rede particular no Windows 10, em cada computador do laboratório
- Nas propriedades de compartilhamento, no perfil “particular”, ativação da descoberta de rede, configuração automática dos dispositivos conectados à rede e ativação do compartilhamento de arquivo e impressora
- Nas propriedades de compartilhamento, no perfil “convidado ou público”, desativação da descoberta de rede e compartilhamento de arquivo e impressora
- Nas propriedades de compartilhamento, no perfil “todas as redes”, desativação do compartilhamento de pasta pública e habilitação do uso de criptografia de 128 bits

Os passos para se efetuar essas configurações descritas acima, são:

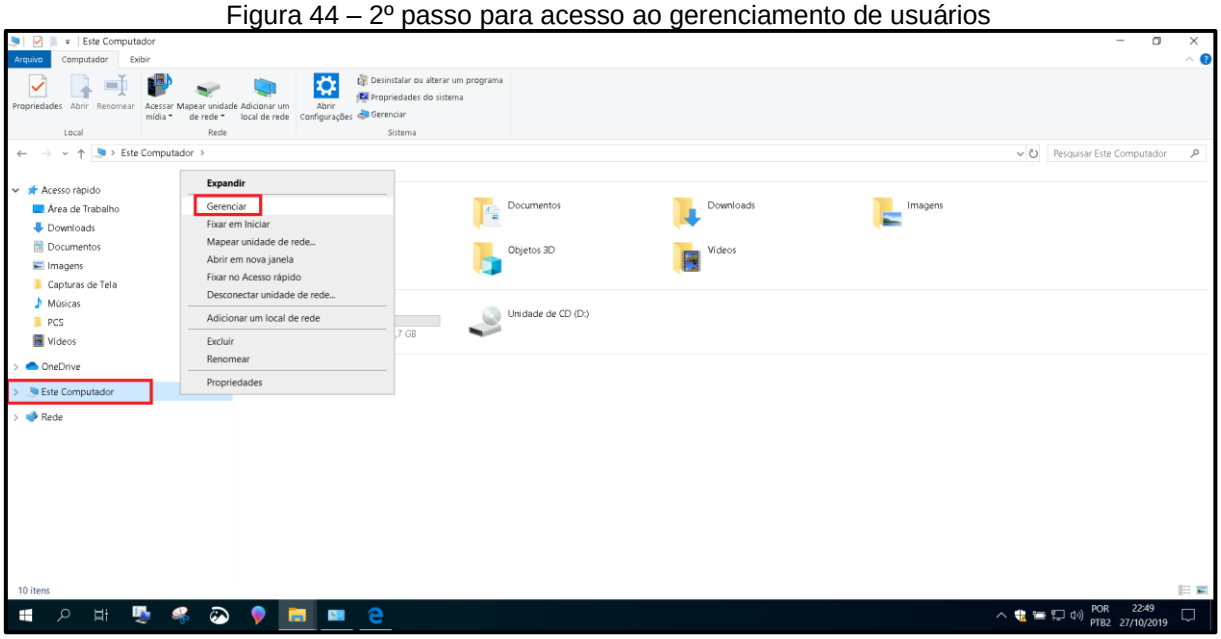
Conta de usuário e conta administrador: Pressionar as teclas “WINDOWS + R” > digitar “explorer.exe” > A esquerda, selecionar “Este Computador” > Clicar com botão direito do mouse em “Gerenciar” > Usuários e Grupos Locais > Usuários > Administrador > Definir senha > Prosseguir

Figura 43 – 1º passo para acesso ao gerenciamento de usuários



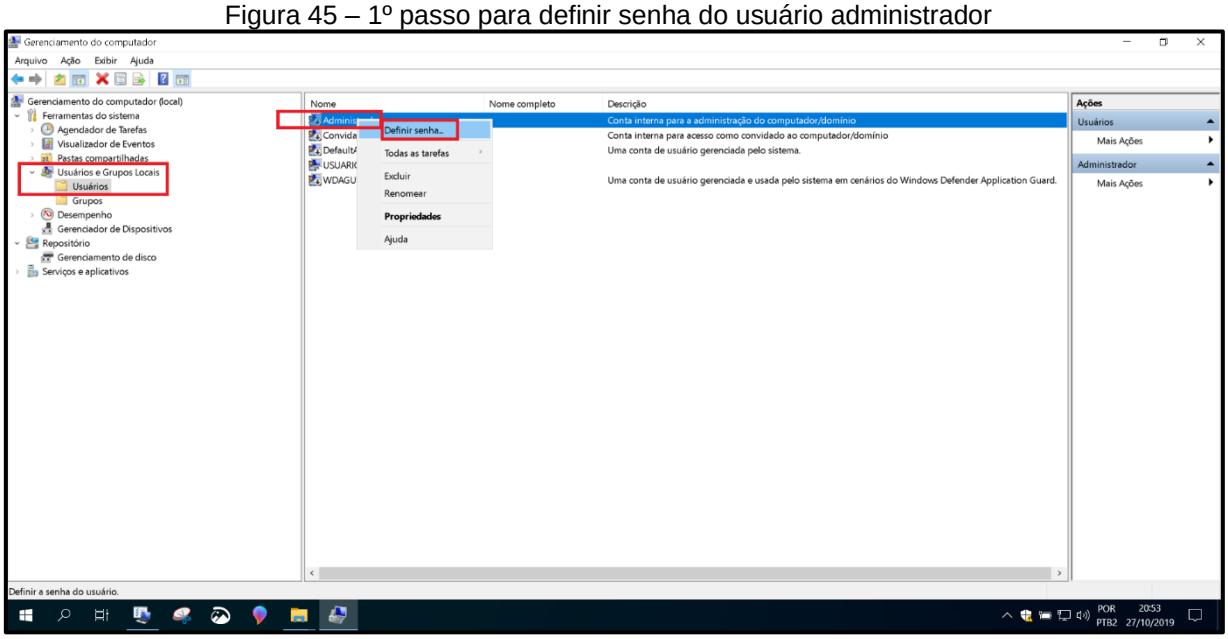
Fonte: Autoria Própria (2019)

Figura 44 – 2º passo para acesso ao gerenciamento de usuários



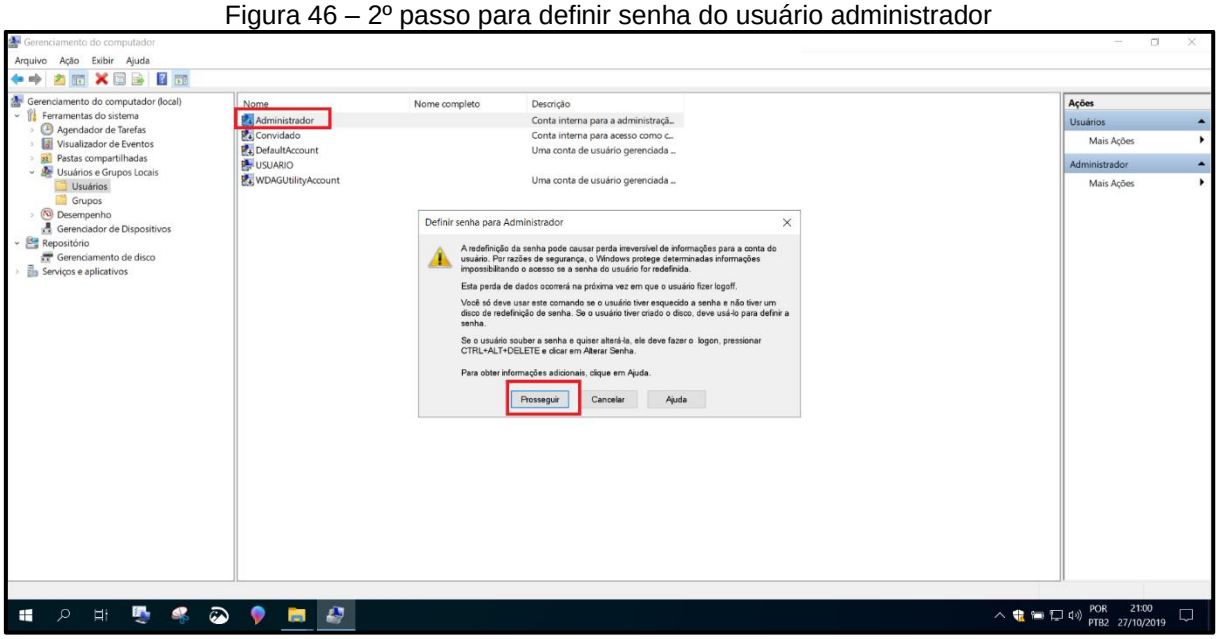
Fonte: Autoria Própria (2019)

Figura 45 – 1º passo para definir senha do usuário administrador



Fonte: Autoria Própria (2019)

Figura 46 – 2º passo para definir senha do usuário administrador



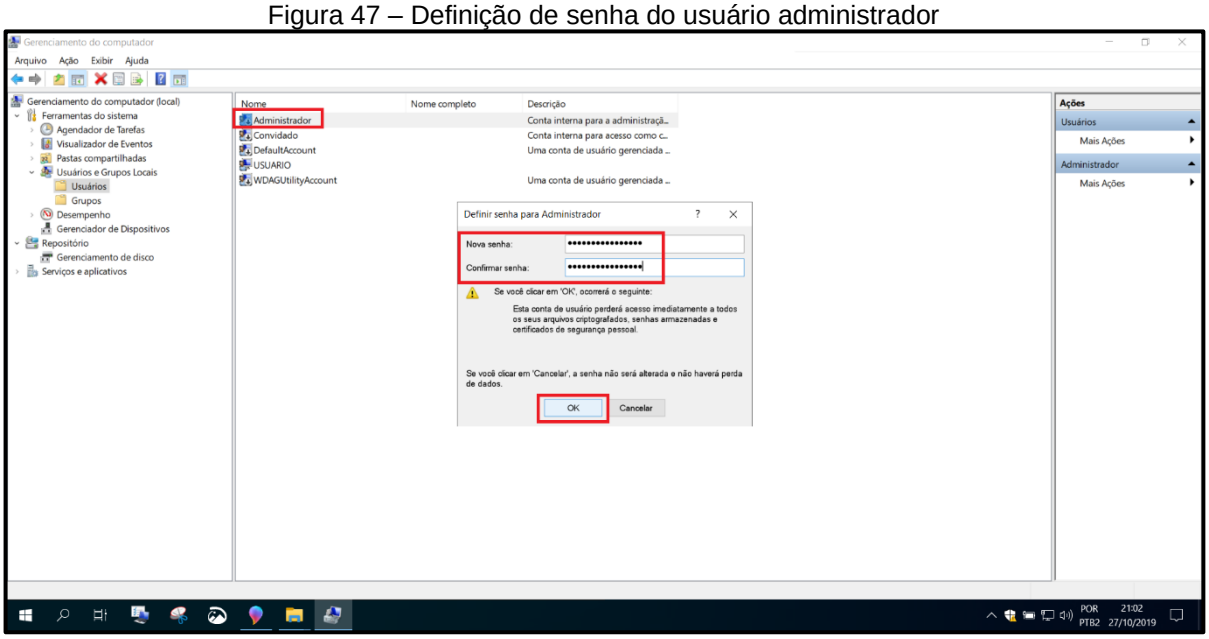
Fonte: Autoria Própria (2019)

Administrador

Nova senha: @dminlabinf2019

Confirmar senha: @dminlabinf2019

Figura 47 – Definição de senha do usuário administrador

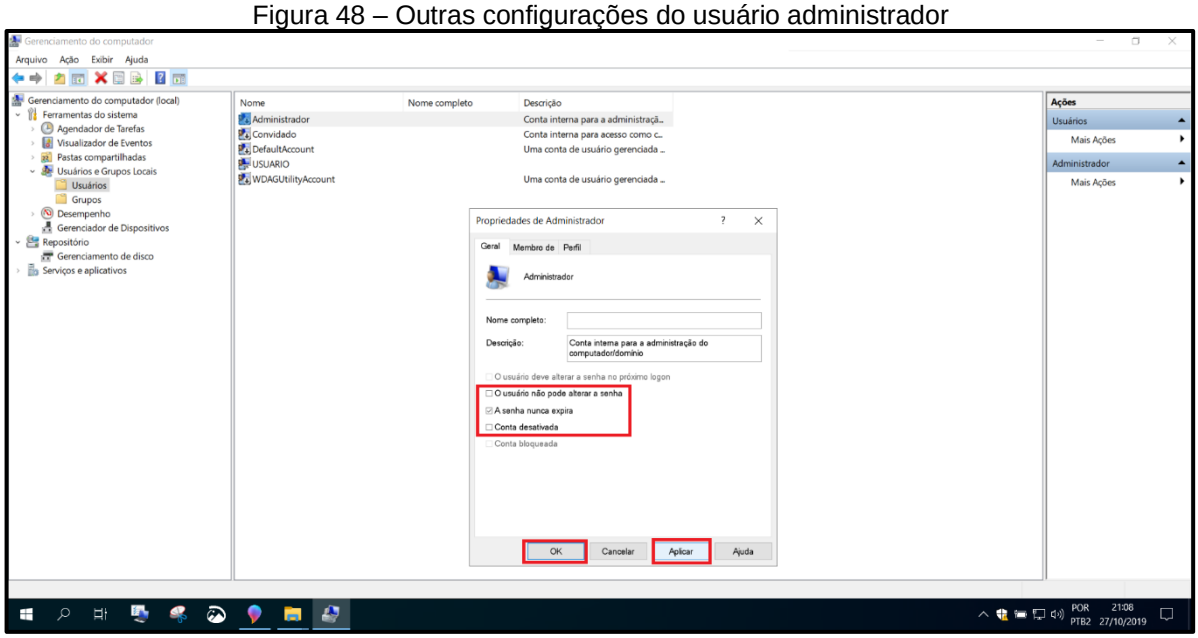


Fonte: Autoria Própria (2019)

Selecionar “Administrador” > Clicar com botão direito do mouse > Propriedades

- ☐ A senha nunca expira (Marcado)
- ☐ Conta Desativada (Desmarcado)

Figura 48 – Outras configurações do usuário administrador



Fonte: Autoria Própria (2019)

Em seguida clicar com o botão direito em qualquer ponto da área em branco > Novo usuário

Nome de usuário: USUARIOLAB

Descrição: Conta de usuário padrão usada pelos alunos nos computadores do laboratório.

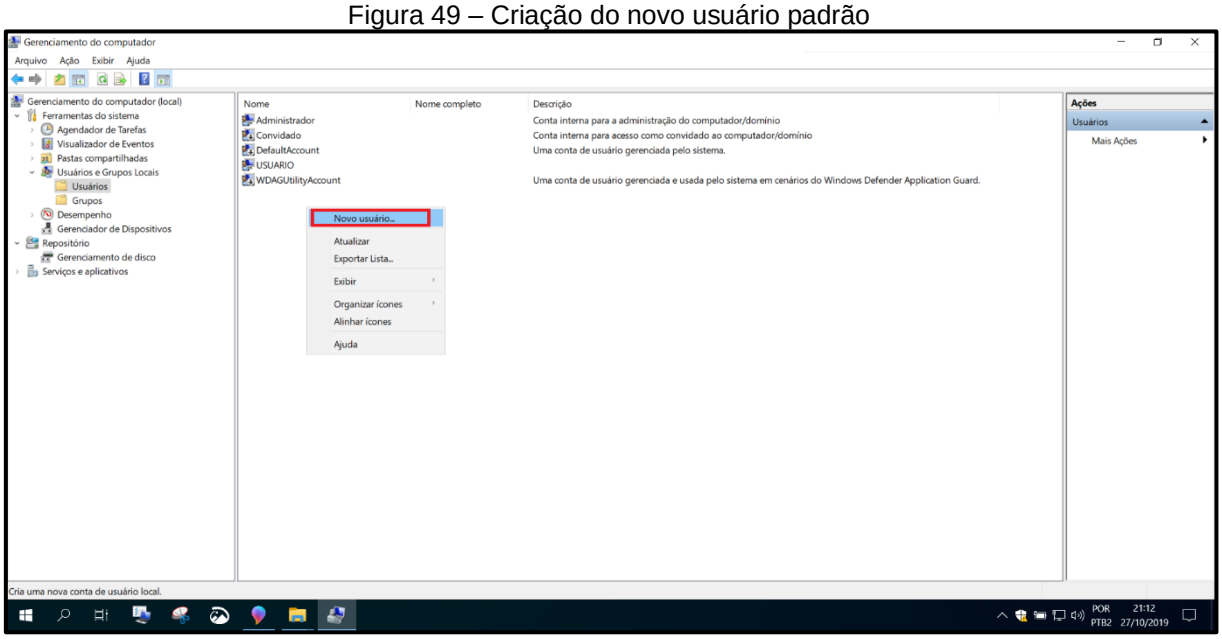
Senha: userlab

Confirmar senha: userlab

- ☐ O usuário deve alterar a senha no próximo logon (Desmarcado)
- ☐ O usuário não pode alterar a senha (Marcado)
- ☐ A senha nunca expira (Marcado)
- ☐ Conta Desativada (Desmarcado)

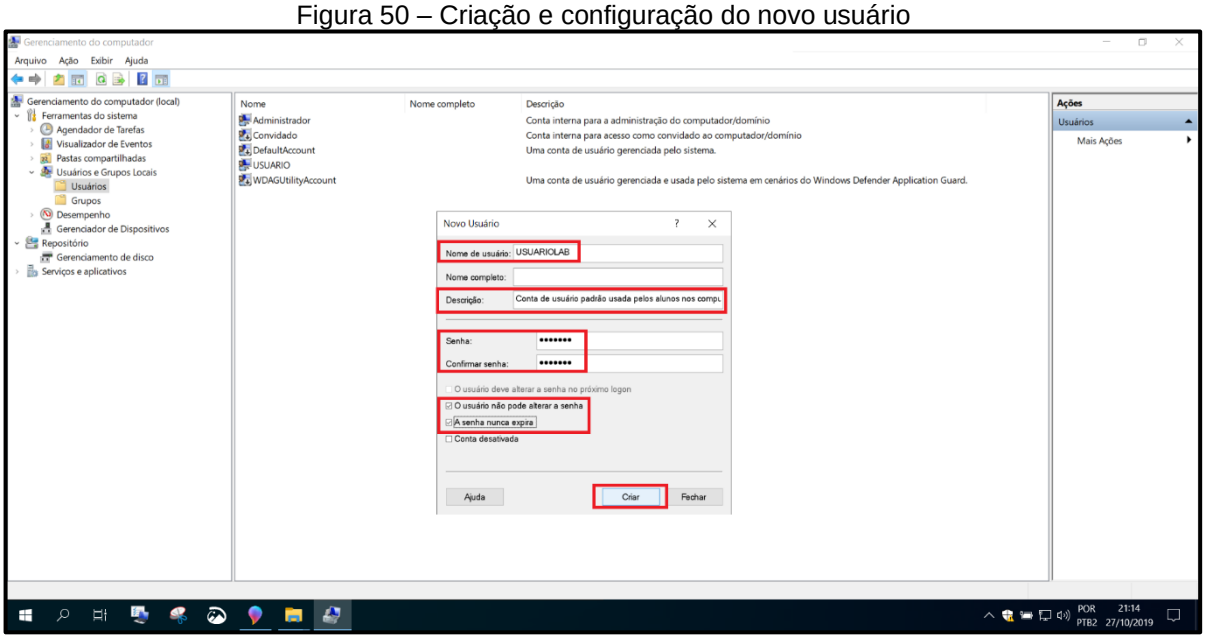
Em seguida clicar em “Criar”.

Figura 49 – Criação do novo usuário padrão



Fonte: Autoria Própria (2019)

Figura 50 – Criação e configuração do novo usuário



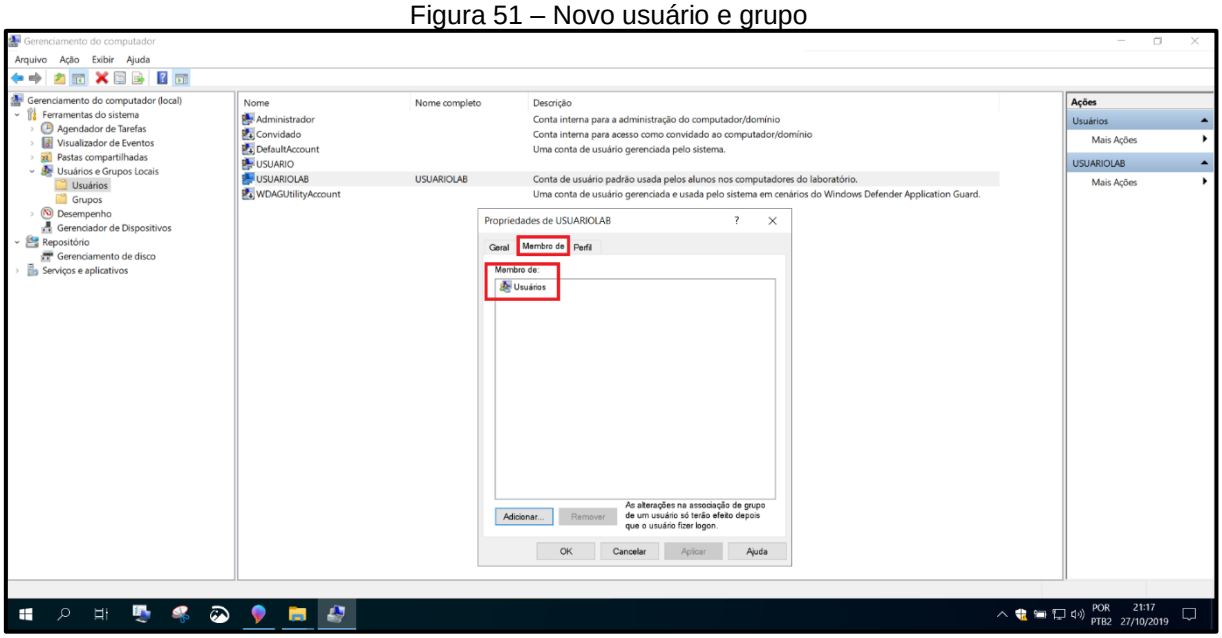
Fonte: Autoria Própria (2019)

Logo após, selecionar o “USUARIOLAB” > clicar com o botão direito do mouse > Propriedades > Aba “Membro de”

Membro de:

Usuários

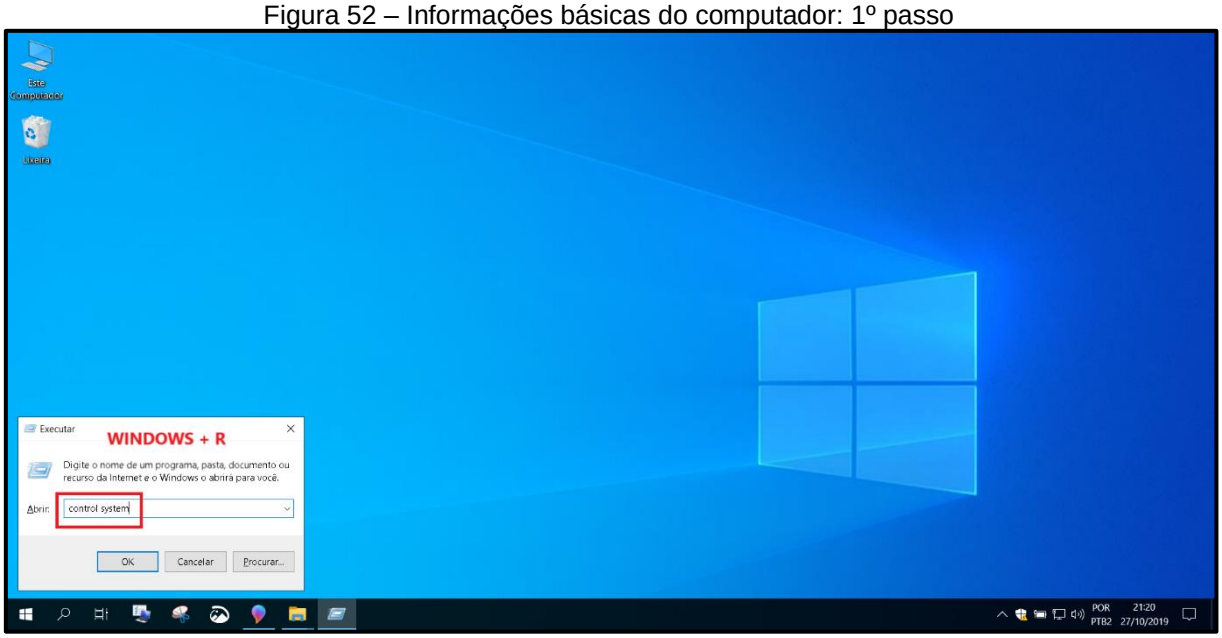
Figura 51 – Novo usuário e grupo



Fonte: Autoria Própria (2019)

Nome, descrição e grupo de trabalho: Os seguintes passos abaixo mostram como trocar o nome do computador e a descrição que o ajuda a identificar. Depois do sistema operacional ter iniciado e carregado por completo, pressiona-se WINDOWS + R > control system > À direita, clicar em “Alterar configurações” > Aba “Nome do computador”

Figura 52 – Informações básicas do computador: 1º passo



Fonte: Autoria Própria (2019)

Descrição do computador: Pc pertencente ao laboratório de informática da instituição.

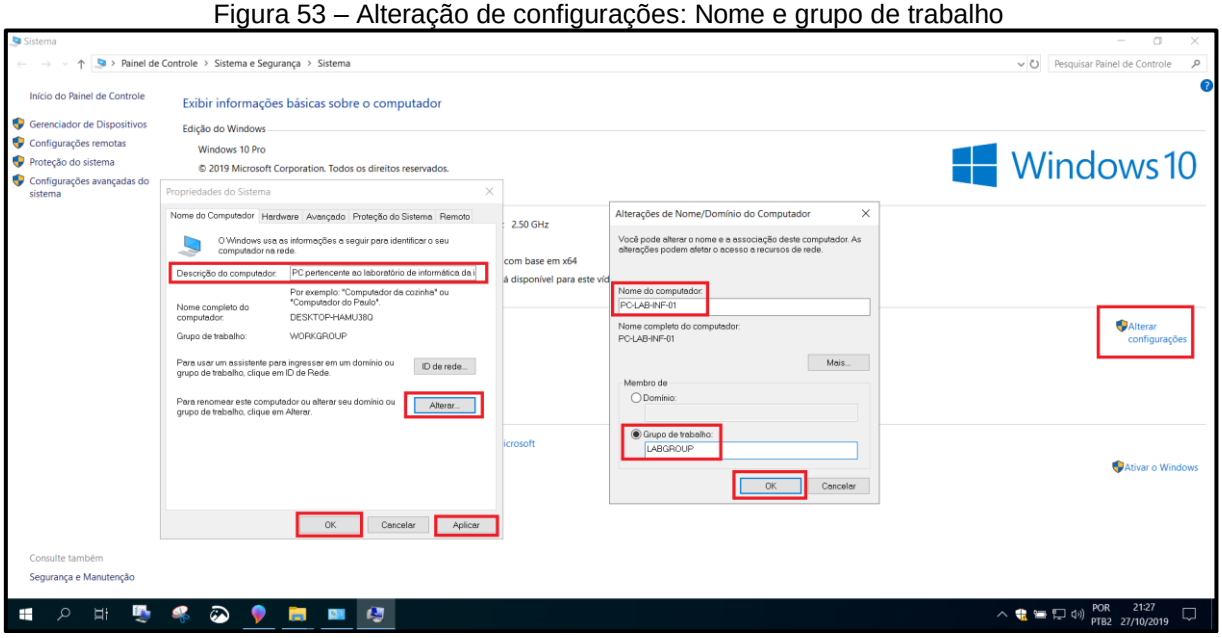
Em seguida, clicar em “Alterar”

Nome do computador: PC-LAB-INF-01

Grupo de Trabalho: LABGROUP

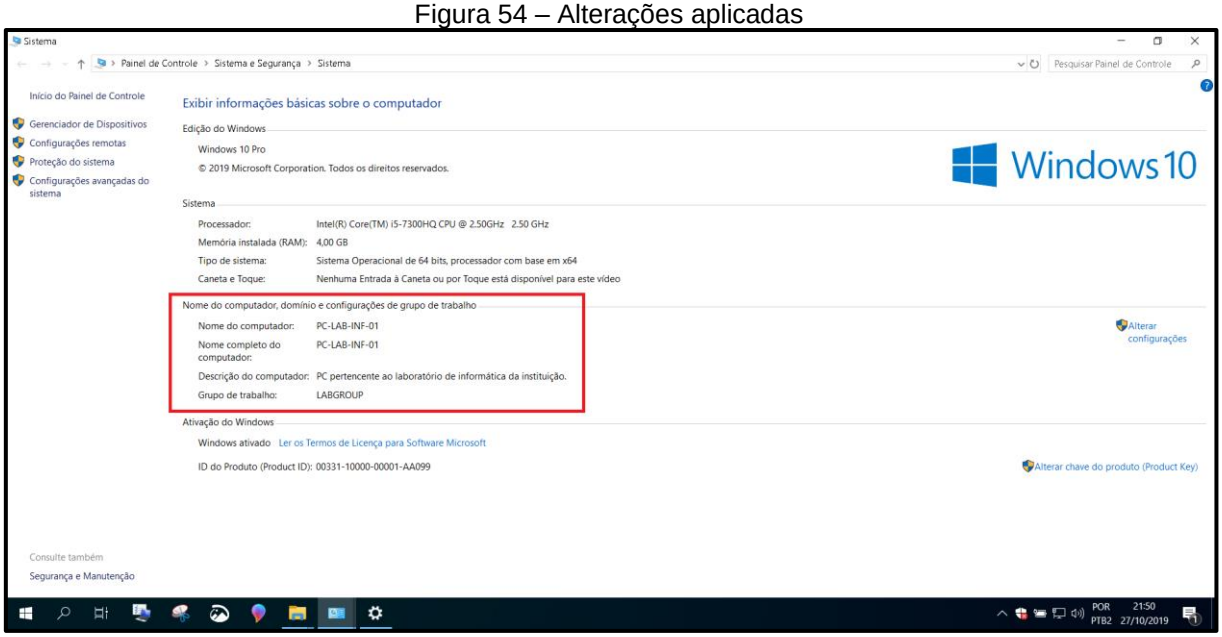
Com as informações alteradas, é só clicar em OK e reiniciar o computador para aplicar a configuração.

Figura 53 – Alteração de configurações: Nome e grupo de trabalho



Fonte: Autoria Própria (2019)

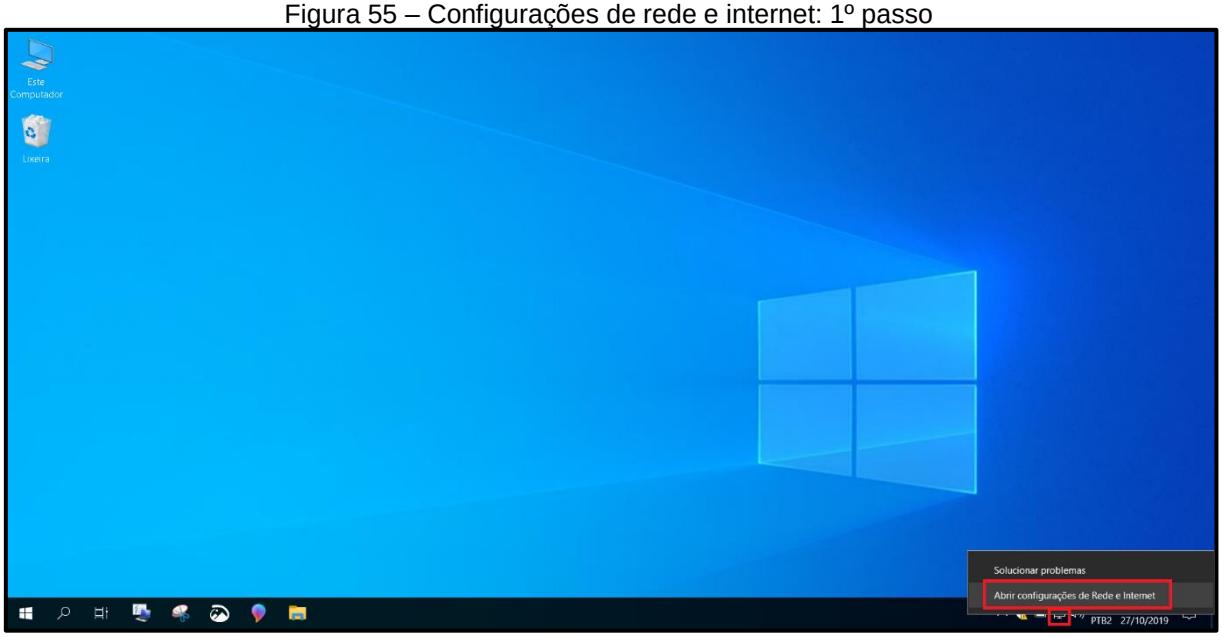
Figura 54 – Alterações aplicadas



Fonte: Autoria Própria (2019)

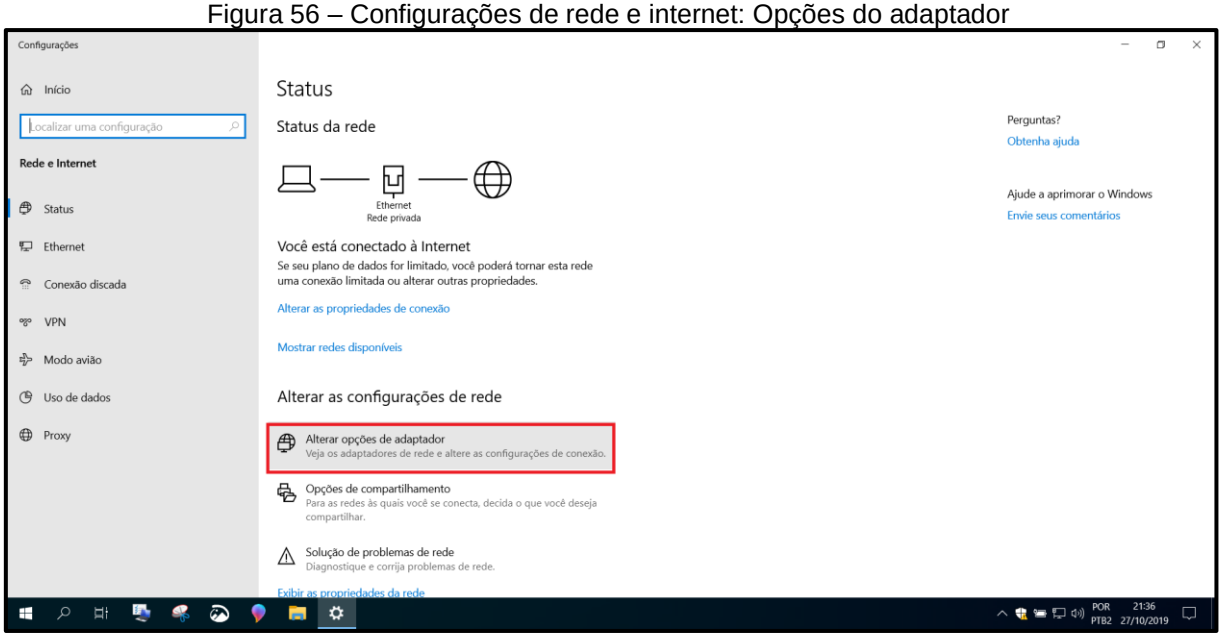
Endereçamento Fixo IPV4 (Internet Protocol Version 4) e DNS: Na barra de tarefas clicar no ícone de rede com o botão direito do mouse > Alterar configurações de Rede e Internet > Status > Alterar opções do adaptador > Clicar no adaptador de nome “Ethernet” com o botão direito do mouse > Propriedades > Selecionar “Protocolo IP Versão 4 (TCP /IPv4)” > Propriedades > Aba “Geral”

Figura 55 – Configurações de rede e internet: 1º passo



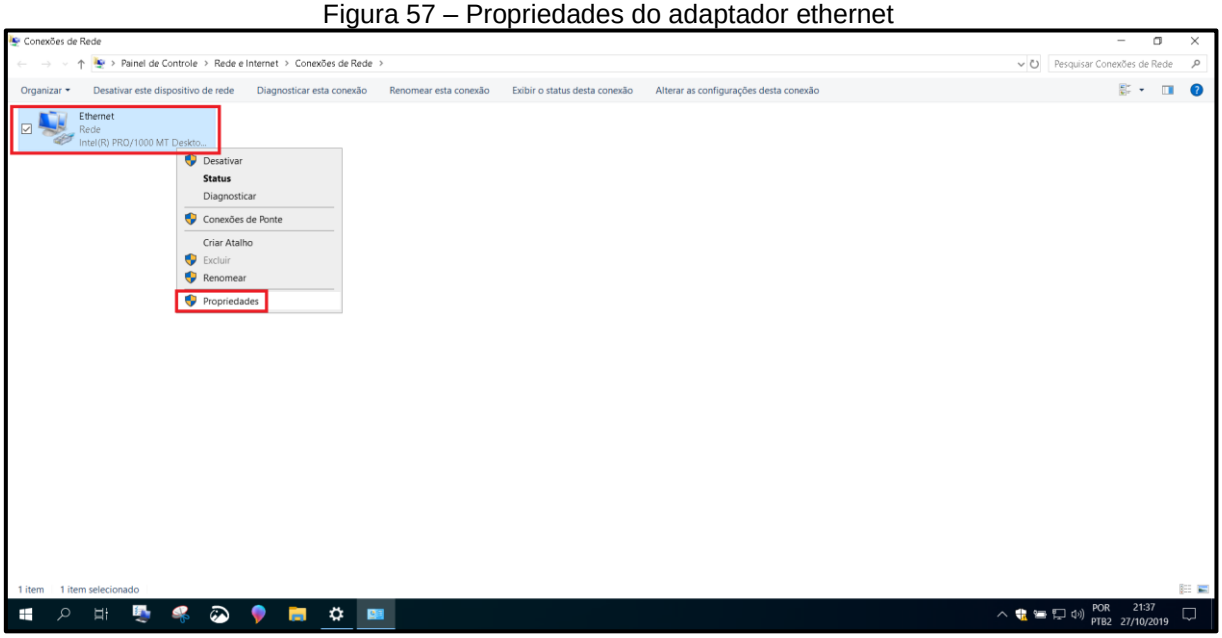
Fonte: Autoria Própria (2019)

Figura 56 – Configurações de rede e internet: Opções do adaptador



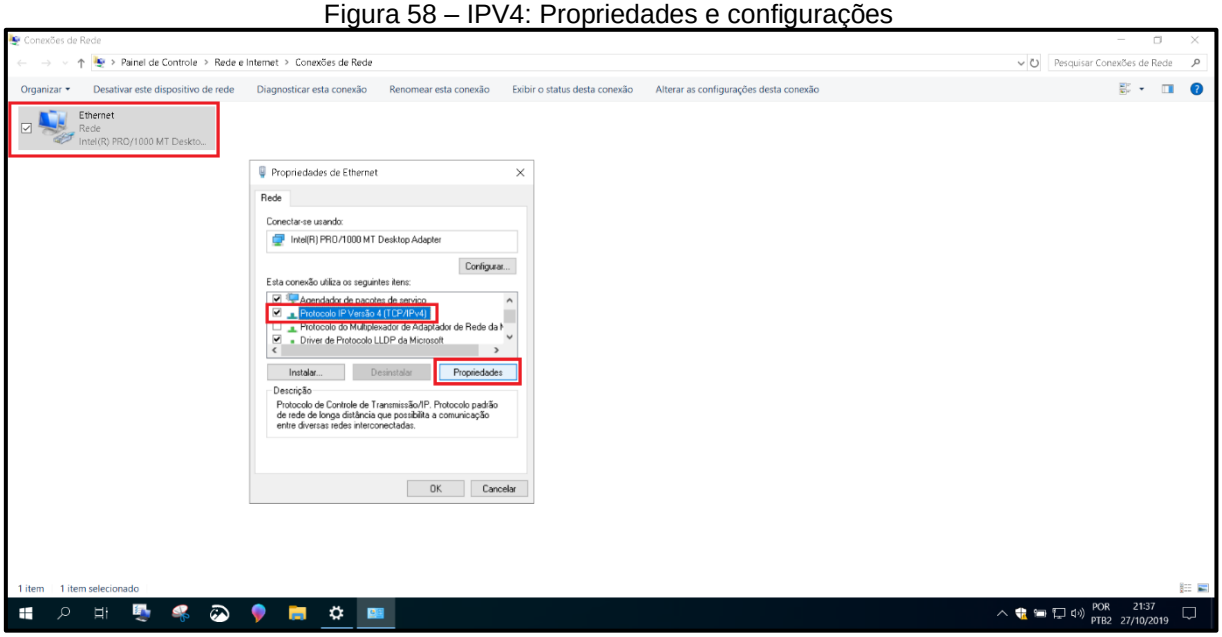
Fonte: Autoria Própria (2019)

Figura 57 – Propriedades do adaptador ethernet



Fonte: Autoria Própria (2019)

Figura 58 – IPV4: Propriedades e configurações



Fonte: Autoria Própria (2019)

Usar o seguinte endereço IP:

Endereço IP: 192.168.0.31

Máscara de sub-rede: 255.255.255.0

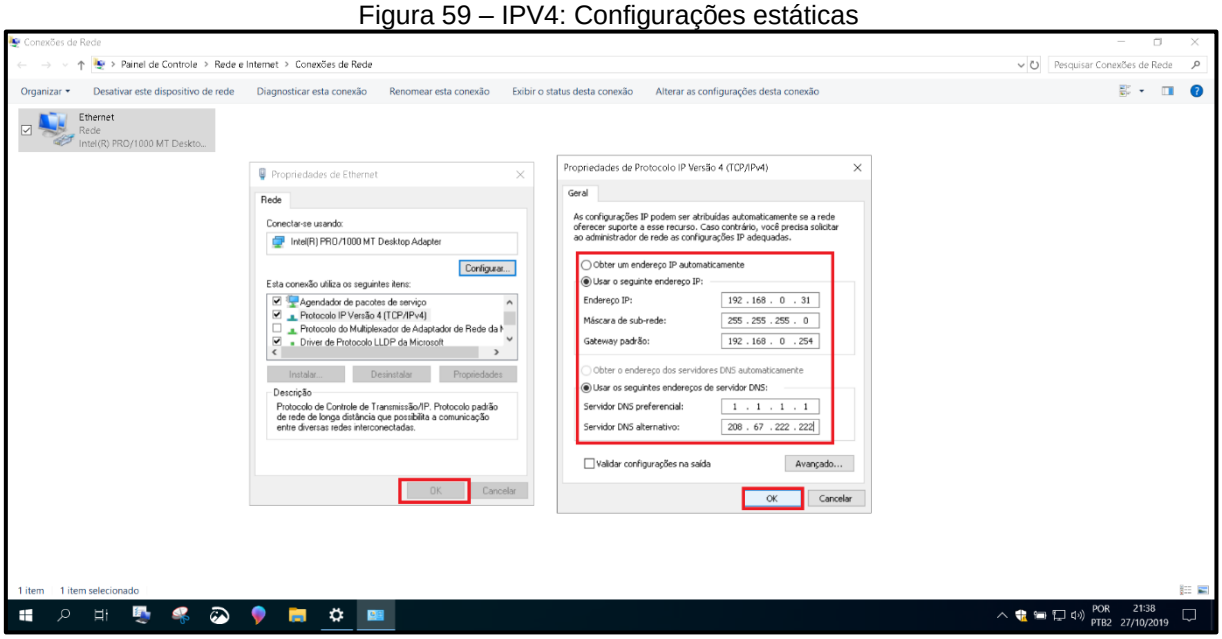
Gateway Padrão: 192.168.0.254

Usar os seguintes endereços de servidor DNS:

Servidor DNS preferencial: 1.1.1.1

Servidor DNS alternativo: 208.67.222.222

Figura 59 – IPV4: Configurações estáticas

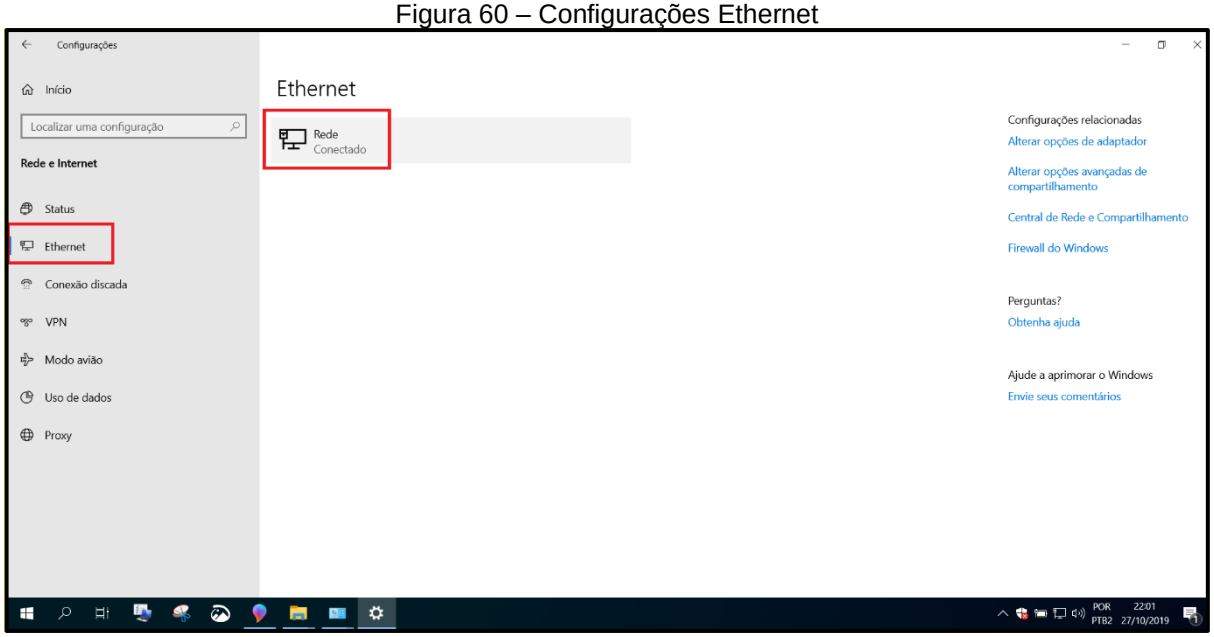


Fonte: Autoria Própria (2019)

Em seguida clicar em “OK” e “OK” novamente.

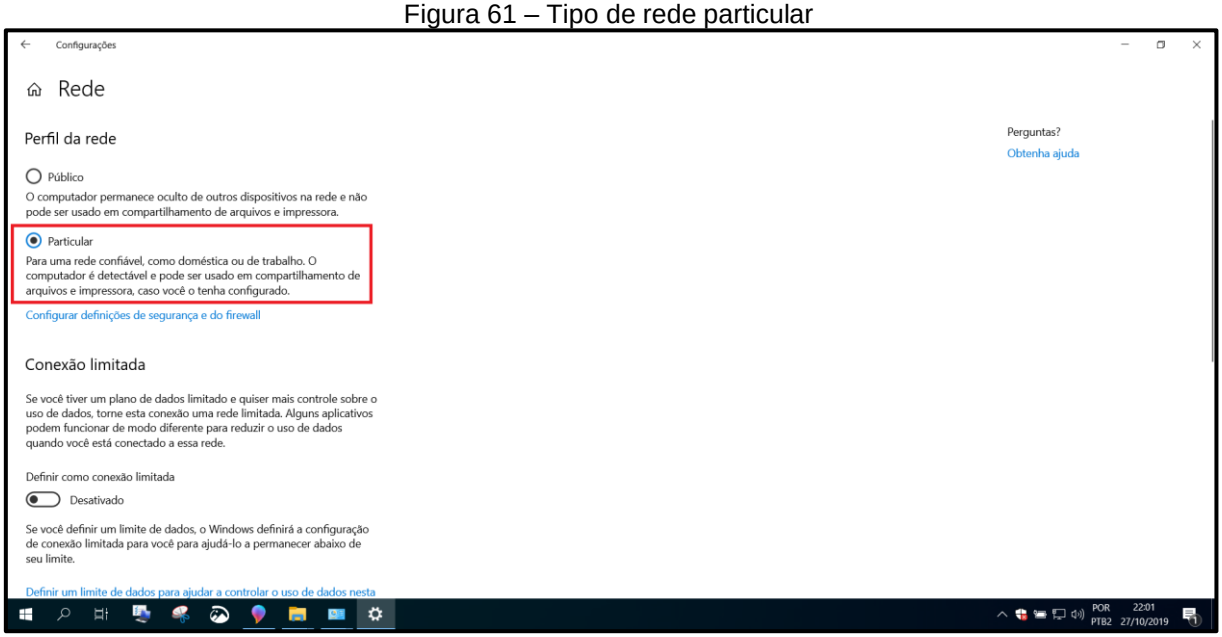
Perfil da rede e Opções de compartilhamento: Na barra de tarefas clicar no ícone de rede com o botão direito do mouse > Alterar configurações de Rede e Internet > Ethernet > Rede > Perfil da rede > Particular

Figura 60 – Configurações Ethernet



Fonte: Autoria Própria (2019)

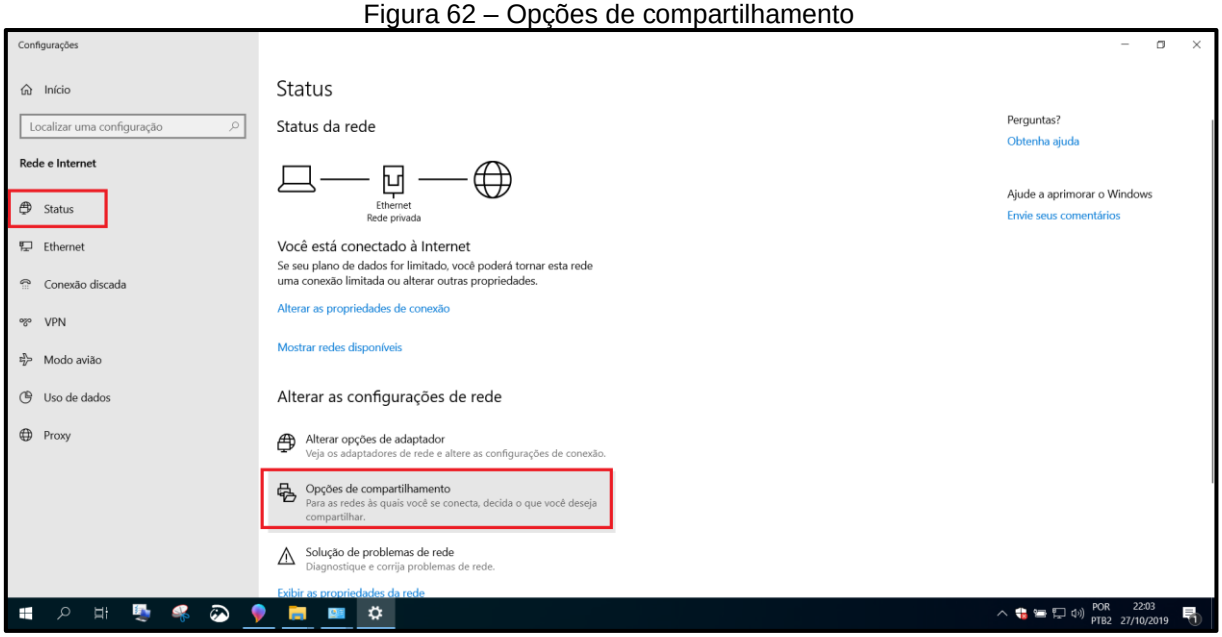
Figura 61 – Tipo de rede particular



Fonte: Autoria Própria (2019)

Em seguida clicar em “Status” > Opções de compartilhamento

Figura 62 – Opções de compartilhamento

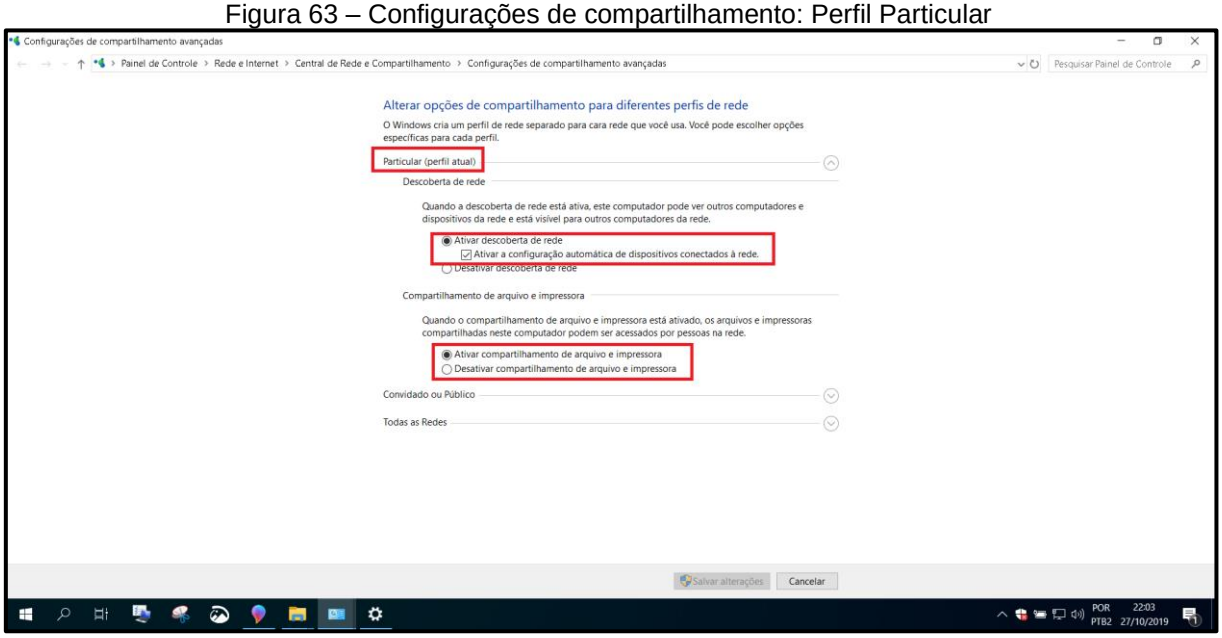


Fonte: Autoria Própria (2019)

Em “Particular (perfil atual)”:

- ☐ Ativar descoberta de rede (Marcado)
- ☐ Ativar a configuração automática de dispositivos conectados à rede (Marcado)
- ☐ Ativar compartilhamento de arquivo e impressora (Marcado)

Figura 63 – Configurações de compartilhamento: Perfil Particular

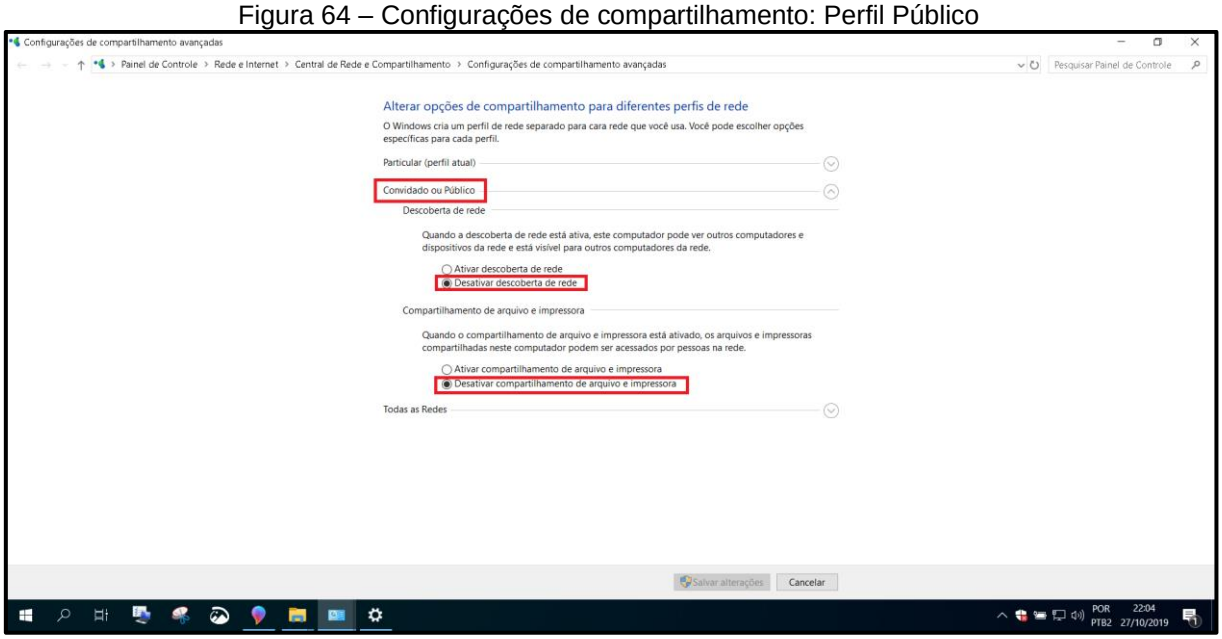


Fonte: Autoria Própria (2019)

Em perfil “Convidado ou Público”:

- ☐ Desativar descoberta de rede (Marcado)
- ☐ Desativar compartilhamento de arquivo e impressora (Marcado)

Figura 64 – Configurações de compartilhamento: Perfil Público

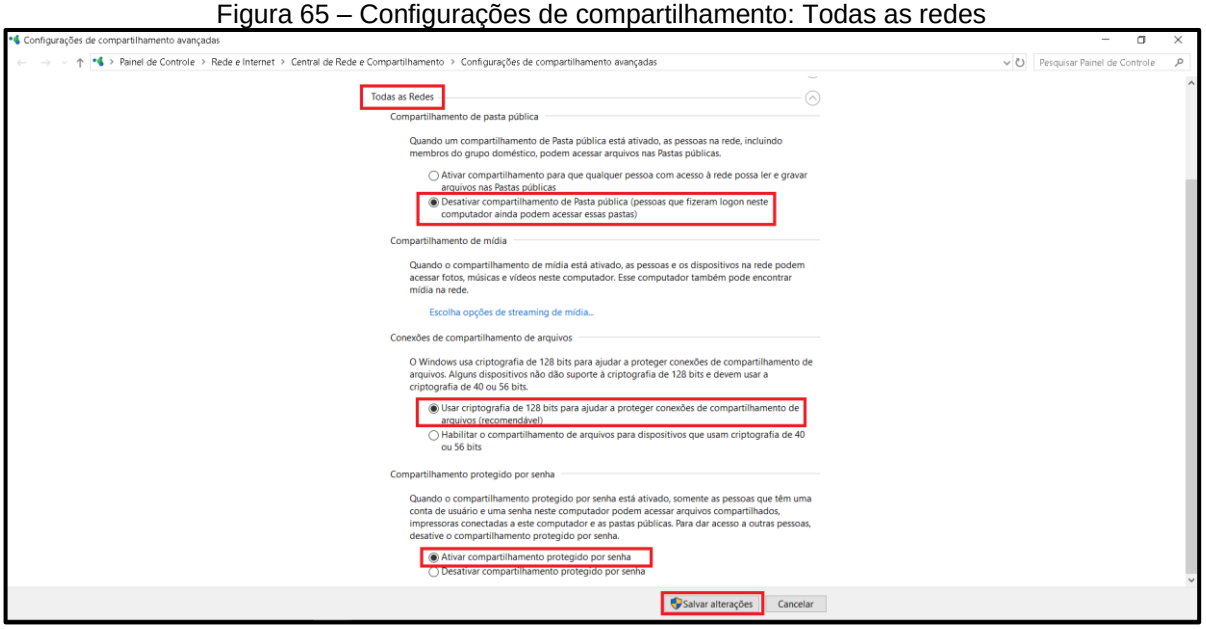


Fonte: Autoria Própria (2019)

Em perfil “Todas as Redes”:

- ☐ Desativar compartilhamento de Pasta Pública (Marcado)
- ☐ Usar criptografia de 128 bits para ajudar a proteger conexões de compartilhamento de arquivos (Marcado)
- ☐ Ativar compartilhamento protegido por senha (Marcado)

Figura 65 – Configurações de compartilhamento: Todas as redes



Fonte: Autoria Própria (2019)

Depois da aplicação de todas essas configurações em todos os computadores de mesa pertencentes ao laboratório, os computadores estarão melhor identificados na rede, se enxergando entre si e prontos para trabalhar com compartilhamento de pastas na rede. O uso de configurações padronizadas adotadas nas máquinas da rede, facilita o gerenciamento por parte do administrador da rede.

6 CONSIDERAÇÕES FINAIS

Este trabalho teve início apresentando uma visão geral sobre as redes de computadores e sua importância. Além de enfatizar a necessidade de investimento em infraestrutura de rede para que as redes possam continuar crescendo e se expandindo, oferecendo recursos e serviços tão usados e demandados pela sociedade, com maior rapidez e qualidade. Dividido em 5 capítulos, o presente trabalho se propôs a explorar e detalhar um pouco do universo que compõe uma rede de computadores LAN. Através de um exemplo de implantação de um laboratório de informática, o trabalho foi desenvolvido com foco nesse tipo de rede, devido ao cenário deste trabalho ser limitado geograficamente a uma sala pertencente a um prédio de uma instituição de ensino superior. Através deste caso de implantação, foi possível abordar desde os conceitos básicos sobre as redes cabeadas e sem fio, arquitetura e topologia mais usada, padrões existentes, tipos de materiais, técnicas e recomendações utilizadas na implantação de cada uma, além das configurações padrões em roteadores e computadores da rede.

Diferindo de tantas outras obras na área, este trabalho não trata de protocolos e nem de modelos de rede, tendo em vista a quantidade bastante expressiva de obras já existentes sobre esses assuntos. Devido a sua natureza, o seu foco é mais prático, fazendo parte da área de infraestrutura de redes, mas sem esquecer o referencial teórico que o sustenta.

Sendo assim, o presente trabalho teve como objetivo implantar com sucesso uma rede que atendesse um laboratório de informática, sendo ela robusta, eficiente, livre de interferências e com cabeamento de grande vida útil, atendendo bem a demandas dos dispositivos da instituição somado aos dispositivos pessoais dos alunos e professores. Este objetivo envolveu diversos procedimentos e passos necessários para ser cumprido.

Fica claro assim que o presente trabalho visa ter uma parcela de contribuição para estudantes e profissionais da área de infraestrutura em redes de computadores, servindo como fonte de referência aos mesmos, ajudando a transmitir um conhecimento suficiente que possibilite implantar ou expandir uma rede de computadores, seguindo as boas práticas da área.

REFERÊNCIAS

FOROUZAN, Behrouz A. **Comunicação de Dados e Redes de Computadores**. 4ª ed. Porto Alegre: AMGH, 2010.

TANENBAUM, Andrew S.; WETHERALL, David. **Redes de Computadores.** 5ª ed. São Paulo: Pearson Education do Brasil, 2011.

MORIMOTO, Carlos E. **Redes, Guia Prático:** Ampliada e Atualizada. 2ª ed. Porto Alegre: Sul Editores, 2011.

FOROUZAN, Behrouz A.; MOSHARRAF, Firouz. **Redes de Computadores**: Uma abordagem Top-Down. Porto Alegre: AMGH, 2013.

KUROSE, James F.; ROSS, Keith W. **Redes de Computadores e a Internet**: Uma abordagem top-down. 6ª ed. São Paulo: Pearson Education do Brasil, 2013.

ELIAS, Glêdson; LOBATO, Luiz Carlos. **Arquitetura e Protocolos de Rede TCP-IP**. 2ª Ed. Rio de Janeiro: Escola Superior de Redes, 2013.

TORRES, Gabriel. **Redes de Computadores:** Versão Revisada e Atualizada. 2ª ed. Rio de Janeiro: Nova Terra, 2016.