INSTITUTO SUPERIOR POLITÉCNICO PRIVADO DA CATEPA

(Aprovado por Decreto nº 132/17 de 19 de Junho)

Departamento de Investigação Científica e Pós-graduação

IMPLEMENTAÇÃO DE UMA REDE LAN PARA LIGAÇÃO REMOTA DOS SERVIÇOS DE PRODUÇÃO COM OS SERVIÇOS DE MONITORAMENTO E REABASTECIMENTO: Um estudo realizado no Bar Mednet-Malanje

Autor: Mendes Domingos Francisco

Orientador: Buco António Albino Golambole Lic.

Malanje, 2023

Mendes Domingos Francisco

IMPLEMENTAÇÃO DE UMA REDE LAN PARA LIGAÇÃO REMOTA DOS SERVIÇOS DE PRODUÇÃO COM OS SERVIÇOS DE MONITORAMENTO E REABASTECIMENTO: Um estudo realizado no Bar Mednet-Malanje

Monografia apresentada ao Departamento de Investigação Científica em Graduação e Pós-graduação do Instituto Superior Privado da Catepa. "I.S.C.A.T", como requisito parcial para a obtenção do grau de Licenciatura em Engenharia Informática.

Orientador: Buco António Albino Golambole, Lic.

Malanje, 2023

FICHA DE CATLOGRÁFICA

Instituto Superior Politécnico Privado da Catepa – ISCAT

Director Geral: Lola Ndofusu, PhD

Director Geral Adjunto para Área Científica: José Domingos Fazenda, Phd
Coordenador do Curso de Engenharia Informática: Mateus Mulula Lic.

FICHA CATALOGRÁFICA

Mendes Domingos Francisco

IMPLEMENTAÇÃO DE UMA REDE LAN PARA LIGAÇÃO REMOTA DOS SERVIÇOS DE PRODUÇÃO COM OS SERVIÇOS DE MONITORAMENTO E REABASTECIMENTO: Um estudo realizado no Bar Mednet-Malanje**.**

Orientador: Buco António Albino Golambole, Lic.

Monografia – Iinstituto Superior Politécnico Privado da Catepa Licenciatura em Engenharia Informática.

ISBN:
Implementação;redes;lan.

1 – Francisco**,** Mendes, Domingos, **Nascido: 11 de Novembro de 1986.**

FICHA DE APROVAÇÃO

Mendes Domingos Francisco

IMPLEMENTAÇÃO DE UMA REDE LAN PARA LIGAÇÃO REMOTA DOS SERVIÇOS DE PRODUÇÃO COM OS SERVIÇOS DE MONITORAMENTO E REABASTECIMENTO: Um estudo realizado no Bar Mednet-Malanje**.**

Monografia apresentada ao Instituto Superior Politécnico Privado da Catepa,

como requisito para a obtenção do grau de Licenciatura em Engenharia Informática

COMISSÃO JULGADORA

Presidente do corpo de júri:

Primeiro arguente:

Segundo arguente:

Malanje, aos_____ de _____de 2023

DECLARAÇÃO

Nome:

Mendes Domingos Francisco

BI/Passaporte

002418912ME036

Telemóvel

922300197

Correio Electrónico

mendesdomingosfrancisco@live.com.pt

Título da Monografia

IMPLEMENTAÇÃO DE UMA REDE LAN PARA LIGAÇÃO REMOTA DOS SERVIÇOS DE PRODUÇÃO COM OS SERVIÇOS DE MONITORAMENTO E REABASTECIMENTO: Um estudo realizado no Bar Mednet-Malanje**.**

Nome do Orientador

Buco António Albino Golambole, Lic.

Ano de Conclusão

2023

Designação do Ramo de Conhecimento

Engenharia Informática.

Declara-se sobre compromisso de honra que a monografia agora entregue corresponde à que foi aprovada pelo Conselho Científico do Instituto Superior Politécnico Privado da Catepa (ISCAT).

Declara-se ainda que seja concedida ao ISCAT uma licença não exclusiva para arquivar e tornar acessível, nomeadamente através da sua biblioteca, nas condições abaixo indicadas, a monografia em suporte impresso e em suporte digital, sendo a autorização concedida a título gratuito.

Declara-se que, ao enviar-se o material em suporte impresso e digital, autoriza-se ao ISCAT um exemplar, que se remete em anexo, ou o exemplar que possui nas suas bibliotecas. Retendo todos os direitos de autora relativos à monografia, e o direito de usá-la em trabalhos futuros (como artigos ou livros).

Concorda-se que a monografia seja colocada na biblioteca do ISCAT.

Malanje, aos _____/_____/_____

O declarante

_____

Mendes Domingos Francisco

DEDICATÓRIA

Dedico a presente monografia a minha família, por tudo que fizeram e têm feito por mim.

AGRADECIMENTOS

Agradeço a Deus pai todo poderoso pela vida, e por tudo que tem feito e tudo que fará por mim, pela força e coragem para levar a bom porto o desenvolvimento e conclusão deste trabalho.

São muitas as pessoas a quem devo agradecer, por fazerem, em algum momento, parte do meu percurso académico a este nível.

Nesta instituição de ensino, tive a oportunidade de conhecer professores maravilhosos, com os quais muito aprendi e aos quais sou profundamente grato pelos ensinamentos valiosos que de forma directa ou indirecta contribuíram com os seus ensinamentos.

Este trabalho não seria possível sem a orientação do admirado professor Buco António Albino Golambole, um professor extremamente inteligente, claro nos seus ensinamentos e um orientador ímpar pela sua paciência e sugestões tão valiosas que enriqueceram este trabalho.

É necessário ainda agradecer a MEDNET LDA, por responder as perguntas relativas ao meu tema, propiciando a realização do estudo prático, o que me deixa muito orgulhoso e grato por ter participado desse momento de aprendizado e de aperfeiçoamento profissional.

EPÍGRAFE

“Não importa o que aconteça, continue a nadar”

-Walter Graham.

RESUMO

O presente trabalho, apresenta uma solução tecnológica para interligação da MEDNET e MEDNET-Filial utilizando técnicas para garantir o compartilhamento de serviços e recursos, mas sempre garantindo a segurança das informações trocadas entre esses pontos. O estudo visou responder a seguinte pergunta de partida: Como melhorar o reabastecimento e monitoramento da área de produção da Mednet através de um sistema informático? Para responder a pergunta de partida, elaborou-se os seguintes Objectivo geral; Implementar uma rede local para melhorar o reabastecimento e monitoramento da área de produção da Mednet. Objectivo específicos: Fundamentar teoricamente sobre implementação de rede locais e ligação remota; Avaliar o processo actual de reabastecimento e monitoramento da área de produção da Mednet; Criar e configurar uma rede local; Investigar as formas de conexão, protocolos e métodos de gestão dos equipamentos utilizados. Para o êxito desta investigação, utilizou-se uma abordagem qualitativa, foi realizada uma pesquisa bibliográfica. Como técnica de análise de dados utilizamos a análise de conteúdo, e a técnica de colecta de dados aplicadas foi a entrevista dirigida aos funcionários da empresa Mednet-Malanje. Tivemos como participantes desasseis (16) indivíduos, onde extraímos cinco (5) indivíduos que fizeram parte da pesquisa, dos participantes três (3) são do sexo masculino e dois (2) do sexo feminino, como critério de seleção da amostra usou-se a amostragem aleatória simples (probabilística). O presente estudo é sustentada na abordagem de Petter. De acordo com Petter (2011) “Uma rede lan é um grupo de computadores e outros dispositivos interligados através de uma linha de comunicação, formada por cabos ou links sem fio, com propósito de compartilhar recursos, dados ou serviços dentro de um ambiente controlado” (p.46).

Palavras Chaves: Implementação; rede; lan.

ABSTRACT

This work presents a technological solution for interconnecting MEDNET and MEDNET-Branch using techniques to guarantee the sharing of services and resources, but always guaranteeing the security of information exchanged between these points. The study aimed to answer the following starting question: How to improve the replenishment and monitoring of Mednet's production area through a computer system? To answer the starting question, the following general objective was developed; Implement a local network to improve replenishment and monitoring of Mednet's production area. Specific objectives: Provide theoretical foundations on the implementation of local networks and remote connections; Evaluate the current process of replenishment and monitoring of Mednet's production area; Create and configure a local network; Investigate connection methods, protocols and management methods for the equipment used. For the success of this investigation, a qualitative approach was used and a bibliographical research was carried out. As a data analysis technique, we used content analysis, and the data collection technique applied was the interview directed to employees of the company Mednet-Malanje. We had sixteen (16) individuals as participants, where we extracted five (5) individuals who took part in the research, of the participants, three (3) were male and two (2) were female, as a sample selection criterion we used simple random sampling (probability). The present study is based on Petter's approach. According to Petter (2011) “A LAN network is a group of computers and other devices interconnected through a communication line, formed by cables or wireless links, with the purpose of sharing resources, data or services within a controlled environment” (p.46).

Keywords: Implementation; network; lan.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE SIGLAS

AH: Authentication Header

ARP: Address Resolution Protocol

DMVPN: Dynamic Multipoint Virtual Private Network

ESP: Encapsulating Security Payload

EIGRP: Enhanced Interior Gateway Routing Protocol

IGRP: Interior Gateway Routing Protocol

IGP: Intern Gateway Protocol

ISP: Internet Service Provider

IPSec: Internet Protocol Security

IP: Internet Protocol

VOIP: Voice over Internet Protocol

HTTP: HyperText Transfer Protocol

FTP: File Transfer Protocol

FTPS: File Transfer Protocol over SSL

SSL: Secure Shell

SFTP: Secure File Transfer Protocol

IKE: Internet Key Exchange

ISAKMP: Internet Security Association and Key Management Protocol

SA: Security Association

MAC: Media Access Control

NHRP: Next Hop Resolutions Protocol

PC: Personal Computer

RFC: Request for Comments

RF: Radio Frequência

SA: Security Association

TDD: Time Division Duplexing

FDD: Frequency Division Duplexing

MAC: Media access control

LLC: logical link control

FTP: Protocolo de Transferência de Arquivos

HTTP: Protocolo de transferência de Hipertexto

POP: Protocolo Post Office

IP: Internet Protocol

ARP: Address Resolution Protocol

ICMP: Internet Control Message Protocol

IGMP: Internet Group Management Protocol

EBCDIC: Extend Binary Coded Decimal Interchange Code

ASCII: American Standard Code for Information Interchange

OSI: Open System Interconnection

SNA: Systems Network Architecture

VPN: Virtual Private Network

MGRE: Multipoint Generic Routing Encapsulations

LAN: Local Area Network

VLAN: Virtual Local Area Network

WAN: Wide Area Network

DNS: Domain Name System

DHCP: Dynamic Host Configuration Protocol

NIS: Network Information Service

PAP: Password Authentication Protocol

CHAP: Challenge Handshake Authentication Protocol

DV: Distance Vector

PDM: Product Data Management

PDA: Personal Digital Assistants

FDDI: Fiber Distributed Data Interface

OSPF: Open Shortest Path First

NBMA: Non-Broadcast Multiple Access

SMDS: Switched Multimegabit Data Service

ATM: Asynchronous Transfer Mode

VFR: Virtual routing and forwarding

QoS: Quality of Service

NAT: Network Address Translation

IPX: Internetwork Packet Exchange

UTP: Unshielded Twisted Pair

EMI: Electromagnetic Interference

STP: Shielded Twisted Pair

RFI: Radio Frequency Interference

LED: Light Emitting Diodes

INE: Instituto Nacional de Estatística

AGT: Administração Geral Tributária

ITA: Internet Technologies de Angola

GNS3: Graphical Network Simulator-3

VMWARE: Virtual Machine Ware

PBX: Private Branch Exchange

SIP: Session Initiation Protocol

IAX: Inter-Asterisk eXchange

ODU: Outdoor Unit

IDU: Indoor Unit

Wi-Fi: Wireless Fidelity

4G: Fourth Generation

VPC: virtual private cloud

RAM: Random Access Memory

CPE: Customer Premises Equipament

IEEE: The Institute of Electrical and Electronics Engineers

ÍNDICE

INTRODUÇÃO

A comunicação é uma das necessidades primárias do ser humano. Com a evolução e introdução dos sistemas de informação, a comunicação foi sendo aprimorada e usada em diferentes setores e para diferentes situações.

Século XVIII foi a época dos grandes sistemas mecânicos que acompanharam a Revolução Industrial. O Século XIX foi a era das máquinas a vapor. As principais conquistas tecnológicas do Século XX se deram no campo da aquisição, do processamento e da distribuição de informações. Entre outros desenvolvimentos, tem-se a instalação das redes de telefonia em escala mundial, a invenção do rádio e da televisão, o nascimento e o crescimento sem precedentes da indústria de Informática e o lançamento dos satélites de comunicação (Tanembaum, 2003, p.103).

Como resultado do rápido progresso tecnológico, essas áreas estão convergindo rapidamente e são cada vez menores as diferenças entre coleta, transporte, armazenamento e processamento de informações. Organizações com centenas de escritórios dispersos por uma extensa área geográfica podem, com um simples apertar de um botão, examinar o *status* atual de suas filiais mais remotas (Tanembaum, 2003, p. 112).

Esta organização estrutural fez com que a troca de dados, processos, controle e administração de informações, deixassem de ser realizados por computadores isolados, agora passando a ter os recursos físicos e lógicos compartilhados. Seguindo critérios de segurança, as informações são visíveis apenas por seus respectivos responsáveis.

Os recursos físicos como impressoras, scanners e outros que não necessitam ser de uso privado, podem ser colocados em rede e compartilhados, muitas vezes gerando economia para a empresa. Além de compartilhar recursos físicos a troca de informações se tornou mais rápida, fácil e eficiente, por exemplo, através de comunicadores, e-mails, service desk, VoIp e outros.

Este trabalho descreve o projeto de uma rede estruturada e também a estrutura de um ambiente de rede de computadores, tipos e modelos de 15 equipamentos, *softwares* de gerenciamento e cabeamento estruturado, usados na empresa em que o estudo de caso foi realizado. Será demonstrado como configurar uma rede empresarial explicando o uso de equipamentos de distribuição, segurança e armazenamento.

Na semelhança de outras, a nossa empresa também tem vivido situações não boas ligadas ao monitoramento e reabastecimento em tempo oportuno da área de produção, face ao

grande fluxo de encomendas e de pedido dos clientes, facto que tem trago descontentamento por parte de clientes que têm de esperar muito para obter o produto desejado.

Formulação do Problema

Existe uma carência de conectividade entre a MEDNET e a MEDNET-Filial, o facto que torna certos processos morosos e burocráticos. A falta de interconexão entre sites, a ausência de serviços de voz sobre IP, Servidores desabilitados, ausência de DNS, vasto número de equipamentos inoperativos, foram os principais problemas encontrados na MEDNET e MEDNET-Filial, e consequentemente os clientes e a própria produção da empresa são prejudicadas pelo atraso nos serviços.

Dado aos constrangimentos causados pelas dificuldades de serviços, elaborou-se a seguinte pergunta de partida:

Como melhorar o reabastecimento e monitoramento da área de produção da Mednet através de um sistema informático?

Tendo em conta a pergunta apresentada, traçou-se os seguintes objectivos:

Objectivo geral

Implementar uma rede local para melhorar o reabastecimento e monitoramento da área de produção da Mednet.

Objectivo específicos:

- Fundamentar teoricamente sobre implementação de rede locais e ligação remota dos equipamentos.
- Avaliar o processo actual de reabastecimento e monitoramento da área de produção da Mednet.
- Criar e configurar uma rede local.
- Ligar remotamente os componentes dos edifícios pertencentes a rede.
- Investigar as formas de conexão, protocolos e métodos de gestão dos equipamentos utilizados.

Teoria de suporte

A presente pesquisa é sustentada na abordagem de Petter. De acordo com Petter (2011) "Uma rede lan é um grupo de computadores e outros dispositivos interligados através de uma linha de comunicação, formada por cabos ou links sem fio, com propósito de compartilhar recursos, dados ou serviços dentro de um ambiente controlado" (p.46).

Metodologias/ Métodos/ Técnicas de investigação

O trabalho possui uma abordagem qualitativa e caracteriza-se por uma pesquisa descritiva, com dados colectados por meio de observações e entrevistas na instituição na qual versa o mesmo, que segundo Bogdan e Biklen(1994), citado por Benjamim (2015), envolve a obtenção de dados descritivos através do contacto directo do pesquisador com a situação estudada, enfatiza mais o processo do que o produto e se preocupa em retratar a perspectiva dos participantes.

Justificativa

Face ao constante avanço tecnológico, alguns objetivos tornam-se essenciais para o desenvolvimento de uma corporação. Desempenho, confiabilidade, segurança e custo são aspectos relevantes que devem ser levados em consideração para determinar o sucesso de uma empresa. Este projeto visa direcionar a implementação de sistemas e equipamentos, de forma a atender ao máximo às necessidades da empresa, com a finalidade de proporcioná-la maior vantagem competitiva no mercado, conscientização ambiental e a preocupação econômica, utilizando para tanto uma rede loca LAN com ligação remota de sistemas.

Descrição dos capítulos

O presente estudo, está constituído por três capítulos. No capítulo I, definem-se os principais termos e conceitos e são apresentados também, os principais contributos dos autores sobre a temática em estudo. Já no capítulo II, descreve-se a caracterização do campo de estudo, assim como as metodologias, técnicas e instrumentos utilizados no estudo, os participantes do estudo, bem como os procedimentos e dificuldades encontradas. Por fim, o Capítulo III, encontramos a apresentação, interpretação e análise dos dados recolhidos por meio de observações e entrevistas, que permitiram finalmente chegar as considerações finais e sugestões referentes ao estudo.

CAPÍTULO I – ENQUADRAMENTO CONCEPTUAL/TEÓRICO

1.1 Definição de termos e conceitos

Neste capítulo abordaremos sobres os conceitos e teorias aplicadas ao presente trabalho.

1.1.1 Implementação

Segundo Dicionário Integral de Língua portuguesa a implementação é uma palavra de origem latim, que significa pôr em prática.

Segundo Richard (2015) A implementação é a fase de um ciclo de vida de um sistema no contexto de sistema de informação que corresponde a elaboração e preparação dos módulos necessários à sua execução.

No nosso ponto de vista, tecnicamente a implementação é a fase final de um processo que começa com a análise de um problema cujo o objetivo é utilizar ferramentas/tecnologias, para solucionar o problema em questão.

1.1.2 Redes de computador

Para Guller (2012) A fusão dos computadores e das comunicações e telecomunicações influenciaram diretamente na forma como os computadores são atualmente organizados.

Pinheiro (2003) descreve o objetivo de uma rede: “Independente do tamanho e do grau de complexidade, o objetivo básico de uma rede é garantir que todos os recursos disponíveis sejam compartilhados rapidamente, com segurança e de forma confiável. Para tanto, uma rede de computadores deve possuir regras básicas e mecanismos capazes de garantir o transporte seguro das informações entre os elementos constituintes” (p.26).

Uma rede de computadores é a forma de conectarmos equipamentos a fim de que possamos estabelecer uma comunicação entre os mesmos fazendo com que eles troquem dados, informações e serviços. (Duarte, 2006, p.19).

Segundo Sousa (129) “rede de computadores é um conjunto de equipamentos interligados de maneira a trocarem informações e compartilharem recursos, como arquivos de dados gravados, impressoras, modems, softwares e outros equipamentos” (p.20).

1.1.2.1 Classificação das redes

As redes de computadores são classificadas de acordo com a dimensão geográfica que ocupam e todas elas são concebidas de forma que possam se comunicar com outras redes. Assim, as redes podem ser classificadas em:

- LAN (Local Area Network – Rede de Área Local);
- MAN (Metropolitan Area Network – Rede de Área Metropolitana) e
- WAN (Wide Area Network – Rede de Área Extensa).

Com o advento das novas tecnologias de redes wireless (sem fio), novas classificações foram adotadas tais como:

- WPAN (Wireless Personal Area Network – Rede sem Fio de Área Pessoal);
- WLAN (Wireless Local Area Network – Rede sem Fio de Área Local);
- WMAN (Wireless Metropolitan Area Network – Rede sem Fio de Área Metropolitana);
- WWAN (Wireless Wide Area Network – Rede sem Fio de Área Extensa).

Para o nosso caso falaremos apenas da rede local ou LAN (Local Area Network) que é o nosso foco. Uso das redes de computadores.

As redes de computadores são empregadas para potencializar diversas atividades cotidianas. Abaixo abordaremos as finalidades comerciais e a necessidade de mobilidade.

Finalidades comerciais

O advento das redes de computadores proporcionou a exploração de novos nichos de mercado, pois as mesmas possibilitaram solucionar desafios existentes no modelo tradicional de comércio. Antes do surgimento das tecnologias em redes, um dos modelos mais empregados em transações comerciais se baseava na dependência de um local físico para atender os clientes e disponibilizar os produtos e/ou serviços. Com o surgimento das redes de computadores, muitos empresários visionários identificaram a oportunidade de quebrar este paradigma. As tecnologias de redes possibilitaram a flexibilização em relação à dependência de um local físico. Por meio desta inovação as empresas poderiam, por exemplo, oferecer seus produtos e serviços através da rede, proporcionando um gerenciamento mais eficiente dos produtos em estoque e aumentando a disponibilidade de atendimento aos clientes. A identificação deste potencial contribuiu para investimentos consideráveis para criação de uma infraestrutura de rede em escala global capaz de disponibilizar plataformas de comércio eletrônico.

Mobilidade

Os usuários dos sistemas construídos para operar sob as redes de computadores geralmente permanecem interessados em acessar seus dispositivos para executar as mais variadas atividades. Como resultado, a indústria constantemente provê e aprimora dispositivos

e tecnologias para comunicação sem fio. Ao usar este arcabouço de soluções, os usuários poderiam manter-se em movimento enquanto realizavam atividades de computação, abrindo portas para uma nova área relacionada com a área de redes de computadores, a mobilidade.

Essa nova área despertou a atenção do mercado das redes celulares e da indústria militar. Muitas empresas de telefonia celular se interessaram em atuar como provedores de uma infraestrutura capaz de servir usuários móveis, ao explorar a infraestrutura de antenas já existentes e até então usadas apenas para comunicação de tráfego de áudio de ligações. Entrando nesse novo nicho de mercado, as antenas poderiam incluir a prestação de serviços de dados com objetivos de aumentar suas receitas. As tecnologias tais como 3G, 4G e 5G surgiram como soluções para suprir essa demanda e atualmente estão presentes no cotidiano de grande parte das pessoas. A indústria militar também demostrou grande interesse no conceito de mobilidade. Um tema largamente pesquisado neste contexto consiste na criação de redes de sensores sem fio. A ideia central desta abordagem compreende a criação de uma infraestrutura de rede de comunicação sem fio, onde existem diversos sensores capazes de coletar informações sobre um ambiente e armazenar os resultados em uma base de dados. Podemos imaginar os benefícios de uma rede como essa ao supor a aplicação de uma rede de sensores em uma área onde manobras militares são executadas e as informações coletadas sobre essa área fossem atualizadas em tempo real. Essas informações poderiam ser utilizadas na tomada de decisões antes da execução de manobras militares, podendo compreender uma vantagem tecnológica significativa.

1.1.2.2 Topologias de redes

Segundo SOARES et. al. (1995), a topologia de uma rede refere-se à forma como os enlaces físicos e os nós de comutação estão organizados, determinando os caminhos físicos existentes e utilizáveis entre quaisquer pares de estações conectadas a essa rede.

A topologia de uma rede descreve como o é o layout do meio através do qual há o tráfego de informações, e também como os dispositivos estão conectados a ele. São várias as topologias existentes, podemos citar a Topologia em Barramento, Estrela, Anel, Malha e Topologias Híbridas.

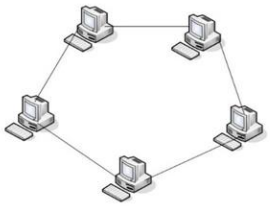
- **Topologia em anel**

Nessa topologia, procura-se diminuir ao máximo o número de ligações no sistema. As estações são ligadas ponto a ponto e operam em um único sentido de transmissão, como pode

ser visto na sua representação. Uma mensagem deverá circular pelo anel até que chegue ao módulo de destino, sendo passada de estação em estação (SOARES et. al., 1995).

Tal topologia apresenta limitações de velocidade e confiabilidade. Caso uma rede distribuída aumente consideravelmente o número de estações, isso significa um aumento intolerável no tempo de transmissão. Outro fator limitante refere-se à inexistência de caminhos alternativos para o tráfego de informações. Se porventura um segmento do anel for cortado, toda a rede fica comprometida.

Figura 1: Topologia em anel.

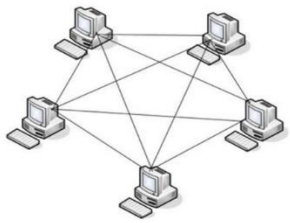


Fonte: Dados da pesquisa

- **Topologia em malha**

Nesta topologia todos os nós estão conectados a todos os outros nós, como se estivessem entrelaçados. Já que são vários os caminhos possíveis por onde a informação pode fluir da origem até o destino, este tipo de rede está menos sujeito a erros de transmissão, o tempo de espera é reduzido, e eventuais problemas não interrompem o funcionamento da rede. Um problema encontrado é com relação às interfaces de rede, já que para cada segmento de rede seria necessário instalar, numa mesma estação, um número equivalente de placas de rede. Como este tipo de topologia traz uma série de desvantagens para a maioria das instalações, raramente é usado.

Figura 2: Topologia em malha.



Fonte: Dados da pesquisa

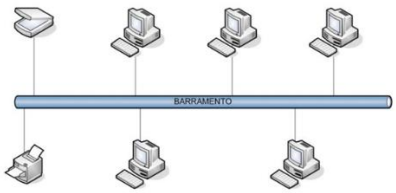
❖ **Topologia em barramento**

Na topologia em barramento, todas as estações compartilham um mesmo cabo. A barra é geralmente compartilhada em tempo e frequência, permitindo transmissão de informação.

Esta topologia é caracterizada por uma linha única de dados (o fluxo é serial), finalizada por dois terminadores (casamento de impedância), na qual cada nó é conectado de tal forma que toda mensagem enviada passa por todas as estações, sendo reconhecida somente por aquela que está cumprindo o papel de destinatário (estação endereçada).

O desempenho de um sistema que usa topologia barramento é determinado pelo meio de transmissão, número de estações conectadas, controle de acesso, tipos de tráfego, entre outros (SOARES et. al., 1995).

Figura 3: Topologia em barramento.



Fonte: Dados da pesquisa

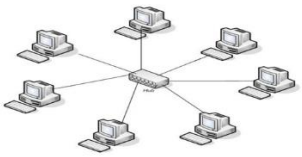
❖ **Topologia em estrela**

A topologia estrela, é caracterizada por um elemento central que gerência o fluxo de dados da rede, estando diretamente conectado (ponto-aponto) a cada nó, daí surgiu a designação "Estrela". Toda informação enviada de um nó para outro deverá obrigatoriamente passar pelo ponto central, ou concentrador, tornando o processo muito mais eficaz, já que os dados não irão passar por todas as estações. O concentrador encarrega-se de rotear o sinal para as estações solicitadas, economizando tempo.

Redes em estrela podem atuar por difusão (broadcasting) ou não. Em redes de difusão, todas as informações são enviadas ao nó central, que é responsável por distribui-las a todos os nós da rede (SOARES et. al., 1995).

Uma vez que o sinal sempre será conduzido para um elemento central, e a partir deste para o seu destino, as informações trafegam rapidamente, sendo assim, as mais indicadas para redes em que imperam o uso de informações "pesadas", como a troca de registros de uma grande base de dados compartilhada, som, gráficos de alta resolução e vídeo.

Figura 4: Topologia em estrela.

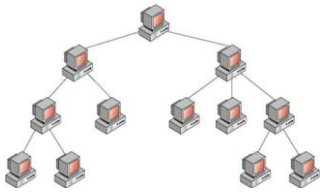


Fonte: Dados da pesquisa

- **Topologia em árvore**

Esta topologia é composta por vários níveis hierárquicos, assumindo o meio físico uma estrutura arborescente com vários níveis. Pode ser vista como resultante da interligação hierarquizada de várias topologias em estrela.

Figura 5: Topologia em árvore.



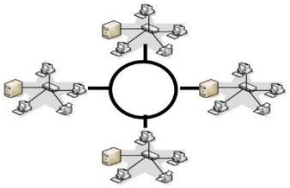
Fonte: Dados da pesquisa

- **Topologia mista**

A topologia mista resulta da combinação de várias topologias simples. Em cada nível hierárquico do sistema de cablagem, adopta-se a topologia mais adequada.

Com esta topologia, procura-se explorar as melhores características das topologias envolvidas. Alguns exemplos são, as topologias de estrelas conectadas em anel e árvores conectadas em barramento. A figura abaixo ilustra uma topologia mista que conecta várias topologias em estrela utilizando uma topologia em anel.

Figura 6: Topologia mista.



Fonte: Dados da pesquisa

1.1.2.3 Comunicação nas redes

A comunicação nas redes de computadores é feita através da ligação de um ponto com o outro, e essa ligação é feita através de meios físicos guiados e meios não guiados.

Transmissão Simplex

Neste método, os dados seguem apenas uma direção, ou seja, um dispositivo transmite e o outro recebe, e esta ordem não pode ser invertida. Como exemplo, podemos citar as transmissões de televisão: o transmissor envia o sinal e não espera por resposta.

Transmissão Semi duplex

Neste método, os dados podem seguir nas duas direções, porém, somente um dispositivo pode enviar dados de cada vez, ou seja, quando um dispositivo está transmitindo o outro dispositivo fica recebendo. Como exemplo, podemos citar o rádio amador que pode ser usado como transmissor ou receptor.

Transmissão Duplex

Neste método, os dados podem seguir em ambas direções, em transmissões separadas, mas paralelas, ocorrendo simultaneamente. Este tipo de transmissão pode ser vista como duas transmissões Simplex: uma em cada direção trabalhando simultaneamente. Esta transmissão divide-se em:

- **TDD** (Time Division Duplexing)

  A duplexação por divisão de tempo usa o tempo para fornecer um enlace direto e um reverso, ou seja, vários usuários compartilham o mesmo canal alternando somente o tempo. Na TDD, cada canal duplex possui um espaço de tempo direto e um reverso, assim, os usuários podem acessar individualmente o canal no espaço de tempo atribuído. Se este espaço de tempo for pequeno, não será perceptível aos usuários.
- **FDD** (Frequency Division Duplexing)

  A duplexação por divisão de frequência fornece duas bandas de frequências distintas para cada usuário. Na FDD, cada canal duplex consiste de dois canais simplex (um direto e um reverso) e um duplexador que permite a transmissão e a recepção simultaneamente nos par de canais simplex.

  Comparando as técnicas FDD e TDD, alguns fatores influenciam na escolha entre as técnicas. A FDD é usada em sistemas de comunicação de rádio, que

alocam frequências individuais para cada usuário e, pelo fato de transmitir e receber simultaneamente os sinais de rádio que podem variar por mais de 100db, a alocação da frequência deve ser coordenada dentro do transceptor (dispositivo que transmite e recebe).

A TDD permite que o transceptor funcione tanto como transmissor quanto receptor usando a mesma frequência, não precisando ter bandas direta e reversa separadas, mas a TDD possui uma latência de tempo, pois precisa de espaços de tempo para transmitir e receber, esta latência cria sensibilidades inerentes a atrasos de propagação dos usuários, devido a estes espaços de tempo exigidos, esta técnica geralmente é limitada a telefone sem fio ou acesso portátil em curta distância.

1.1.2.4 Modelos OSI e TCP/IP

Para realizar uma comunicação entre redes, o computador executa requisições para um servidor. Podemos pensar nessa requisição como se fosse uma carta enviada pelos correios: tem um remetente, uma mensagem e um destinatário, e essa carta passa por algumas etapas até chegar ao destinatário. No caso do computador, temos diferentes modelos de protocolos (que são as etapas da carta).

Protocolos: São regras de comunicação usadas para conectar dois ou mais dispositivos em rede.

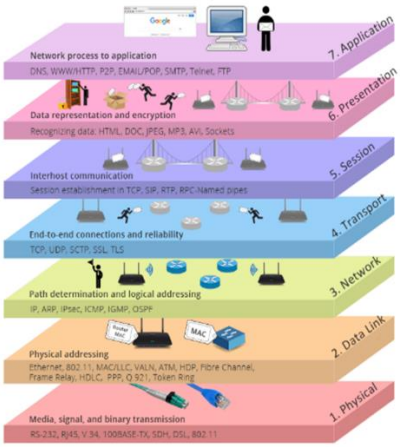
1.1.2.4.1 Modelo OSI

A ISO é uma organização para definição de padrões de arquiteturas abertas. O modelo de referência OSI foi criado pela ISO, sendo um modelo teórico que os fabricantes devem seguir para que sistemas diferentes possam trocar informações.

Segundo Spurgeon (2000), o modelo de referência OSI é o método para descrever como os conjuntos interconectados de hardware e software de rede podem ser organizados para que trabalhem concomitantemente no mundo das redes. Com efeito, o modelo OSI oferece um modo de dividir arbitrariamente a tarefa da rede em pedaços separados, que estão sujeitos ao processo formal de padronização.

Para fazer isso, o modelo de referência OSI descreve sete camadas de funções de rede que são: **Aplicação, Apresentação, Sessão, Transporte, Rede, Enlace de Dados e Física.**

Figura 7: Camadas do modelo OSI.



Fonte: Dados da pesquisa.

Camadas do modelo OSI

Camada Física

É a primeira camada do modelo OSI. Nela estão os caminhos que a informação vai percorrer, ou seja, são os meios de transmissão, por exemplo o cabo de rede, cabos de fibra óptica, entre outros.

Camada de Enlace Dados ou Ligação

É a segubda camada que fiscaliza as informações e controla o fluxo do envio, ou seja, transferência entre nós. Ela é dividida em duas subcamadas: camada MAC (media access control) e camada LLC (logical link control).

- **Subcamada MAC** – Faz o controlo de acesso dos meios da camada. Ela possibilita a conexão de vários computadores em uma única rede. Ela é conhecida como o endereço físico da máquina, que é utilizada para a sua identificação e para o envio de pacotes.
- **Subcamada LLC** – Faz o controlo das ligação lógicas. Ela realiza o controlo do fluxo dos dados que acontecem na rede, através da encapsulação dos protocolos. Assim, ela possibilita rodar vários protocolos em uma mesma rede.

Camada de Rede

Podemos entender como **rede** “um meio para o qual muitos nós podem ser ligados” (Iperius backup, p.04). Nessa leitura, cada nó corresponde a um endereço.

Esta camada lê os endereços IP de origem (nó origem) e de destino (nó destino), e faz a priorização dos pacotes, e decide também os caminhos de envio. O endereço de IP identifica a máquina na rede, e não sofre alteração conforme passa por diferentes dispositivos (roteadores, switches, etc), ao contrário do endereço MAC.

Camada de Transporte

Esta camada controla o envio e recebimento dos pacotes (que vieram da camada Rede). Ela é responsável por garantir a qualidade e integridade dos dados, ou seja, consistentes e sem erros e duplicações.

Camada de Sessão

Responsável pela comunicação entre máquinas, ou seja, ela estabelece e encerra conexão entre os hosts. Além disso, ela realiza a autenticação e autorização da comunicação.

Camada de Apresentação

É a camada responsável por traduzir os dados, ou seja, ela converte os textos codificados, no formato EBCDIC (Extend Binary Coded Decimal Interchange Code) em caracteres - texto codificado ASCII (American Standard Code for Information Interchange).

Camada de Aplicação

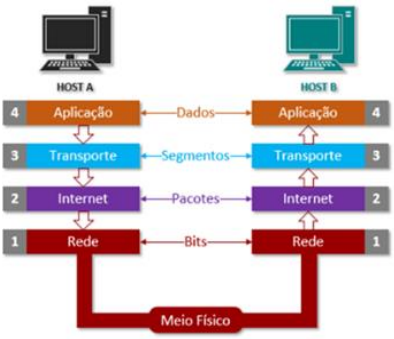
É a última camada responsável pelo consumo dos dados, que executa a interação humano-máquina. É através dela que conseguimos acessar páginas na internet, redes sociais, enviar e receber e-mails, entre outras atividades do nosso dia-a-dia.

Nela estão os protocolos para aplicações finais como: DNS (Sistema de Nome de Domínio), FTP (Protocolo de Transferência de Arquivos), HTTP (Protocolo de transferência de Hipertexto), POP (Protocolo Post Office), entre outros.

1.1.2.4.2 Modelo TCP/IP

Segundo Dantas (2002), o modelo de referência mais conhecido é o TCP/IP (Transmisson Control Protocol/Internet Protocol). O modelo TCP/IP foi projetado em quatro camadas, conforme mostra a figura abaixo.

Figura 8: Camadas do modelo TCP/IP.



Fonte: Dados da pesquisa

Camadas do modelo TCP/IP

Camada de aplicação

Esta camada é responsável por garantir às aplicações acesso a serviços das demais camadas, através de protocolos como HTTP, FTP, SMTP, entre outros.

Camada de transporte

Esta camada controla a comunicação host-a-host, permitindo assim a comunicação entre as aplicações. Nesta camada são usados dois protocolos: TCP (Transport Control Protocol) e UDP (Datagram Protocol). Através do protocolo TCP é garantido o controle de erros, de fluxo, além do controle de acesso. Já com o protocolo UDP, é garantido somente a multiplexação do acesso a internet.

Camada de Internet

É responsável por endereçar o destinatário, por empacotar e por funções para encaminhamento. Os principais protocolos dessa camada são:

- **IP** (Internet Protocol) - Protocolo responsável pelo endereço IP;
- **ARP** (Address Resolution Protocol) - Responsável em descobrir o endereço de acesso à rede;
- **ICMP** (Internet Control Message Protocol) - Fornece as funções que realizam o diagnóstico dos pacotes, e indicam os erros de entrega;
- **IGMP** (Internet Group Management Protocol) - Realiza a gestão de IP multidestino.

Camada de Acesso à Rede

É responsável pela inserção de pacotes TCP/IP no caminho, e também por receber os pacotes fora dele. Dessa forma é conhecida também por ser responsável pela interface da rede, que compatibiliza a tecnologia com o protocolo IP.

1.1.3 Rede local (LAN)

As LANs desenvolveram-se a partir de meados da década de 1970, com o objectivo de satisfazer as necessidades de comunicação de dados em empresas.

- As soluções então disponíveis em WANs não eram adequadas para ambiente LAN
- Era possível explorar soluções alternativas, na altura não viáveis em WANs

As LANs ligam uma grande diversidade de sistemas informáticos de uma mesma organização (computadores, workstations, computadores pessoais, servidores, periféricos, etc.)

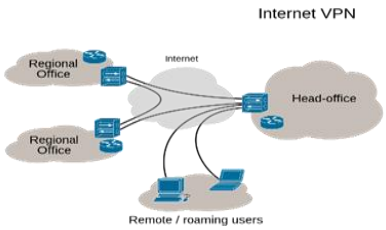
1.1.4. VPN- Virtual Private Network Ou Rede Virtual Privativa

VPN é a extensão de redes dedicadas sobre a infraestrutura da rede pública. No ponto de vista dos usuários da rede privada é como os seus dispositivos de computação estivessem conectados diretamente. (Gil, 2009, p. 61,).

A necessidade de utilizar a tecnologia VPN pode ser explicada pelo seguinte cenário. Empresas distribuídas geograficamente precisam de um acesso seguro para troca de informações. Contudo, é muito dispendioso para as empresas construir toda infraestrutura de telecomunicações. Para reduzir gastos, utiliza a infraestrutura da rede pública. No entanto, nesse tipo de rede é necessário certificar que os dados da empresa serão mantidos em segurança.

Basicamente, uma VPN é uma rede que para casos específicos, usa a Internet para conectar sites remotos ou usuários ao invés de usar uma conexão física, como uma linha dedicada, criando conexões virtuais direccionadas via Internet ligando a rede privada corporativa a outro escritório ou a um funcionário que trabalha à distância. [3]

Figura 9: Comunicação entre redes privadas através de um túnel público.



Fonte: Dados da pesquisa

A criação de uma VPN envolve um cliente, que inicia a ligação, e um Servidor que recebe o pedido do cliente. O dispositivo onde é implementado o Servidor é geralmente designado por concentrador de VPN.

O estabelecimento de um VPN envolve diversas tecnologias, dentre elas: O Encapsulamento, Autenticação, Mecanismos de hashing e Cifragem.

a) **Encapsulamento** ("Tunneling"), que permite a ligação entre as redes (privadas) nos extremos do túnel e consiste, basicamente, em encapsular um pacote original num outro que é transmitido pela rede pública, tornando opaco o pacote original. O túnel é caracterizado pela identificação dos respectivos extremos (endereços IP) e pelo protocolo de encapsulamento utilizado;
b) **Autenticação** para a verificação da identidade dos utilizadores e dos dispositivos envolvidos. A autenticação pode ser suportada por mecanismos mais simples baseados em username e password (PAP, CHAP, RADIUS) ou mais complexos, com recurso a uma infraestrutura de chaves públicas X.509.
c) **Mecanismos de "hashing"** para garantir a integridade das mensagens durante a travessia da rede pública.
d) **Cifragem** para garantir a confidencialidade da informação transmitida no túnel.

1.1.4.1. Tipos de VPN

Neste ponto faremos apenas referência de alguns tipos de VPN que são: O IPSec VPN, Site to Site VPN, Remote access VPN e DMVPN.

a) **IPsec VPN** (O Internet Protocol Security ou IPSec é usado para proteger a comunicação da Internet em uma rede IP. Ele faz a autenticação da sessão e criptografa cada pacote de dados durante a conexão).
b) **Site to Site VPN** (VPN ponto-a-ponto) também é chamada de VPN "roteador a roteador" e é usada principalmente a nível empresarial. As empresas usam esta

tecnologia para conectar matriz a escritórios em diferentes localizações geográficas.

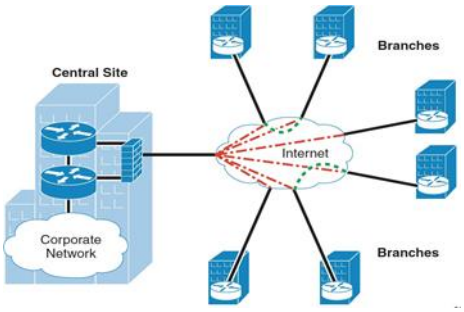
c) **Remote access VPN** (Rede Virtual Privativa de Acesso Remoto): A VPN de acesso remoto permite que um usuário se conecte a uma rede e acesse seus serviços e recursos remotamente. A conexão é segura e privada e ocorre através da Internet.

d) **DMVPN** (Redes Privativas Virtuais Dinâmicas e Multiponto): A DMVPN, permite a implementação de redes virtuais privadas (VPNs) de pequeno, médio ou mesmo de grande porte, de forma simples e rápida, por meio da combinação de tunelamento GRE, IPSec e NHRP (Next Hop Resolution Protocol).

1.2. DMVPN

Uma rede privada virtual dinâmica e multiponto (DMVPN) é uma rede segura que troca dados entre sites/roteadores sem passar tráfego pelo servidor ou roteador de rede virtual privada (VPN) de uma organização, localizado em sua sede. Uma DMVPN permite que as organizações construam uma rede VPN com vários sites, sem a necessidade de configurar dispositivos estaticamente. [2]

Figura 10: Comunicação entre Hub e Spokes

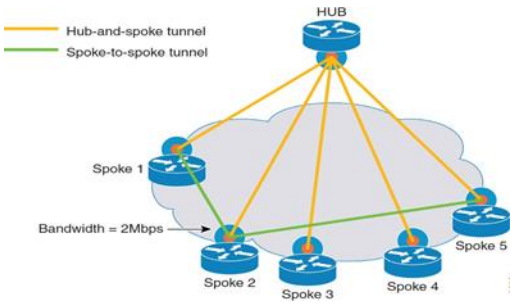


Fonte: Dados da pesquisa

Na DMVPN criamos Hub and Spokes, onde os hubs são chamados servidores e os spokes são chamados de clientes. Quando o cliente inicializa, ele se regista com o servidor. Quando alguém quer se comunicar com outros, um túnel dinâmico é criado entre dois spokes automaticamente. Após a comunicação, o túnel é destruído. Esta solução é mais gerenciável e escalável.

É uma tecnologia VPN que usa túnel dinâmico assente sobre a topologia ponto multiponto sem aprovisionamento do provedor.

Figura 11: Representação dos túneis em uma DMVPN



Fonte: Dados da pesquisa

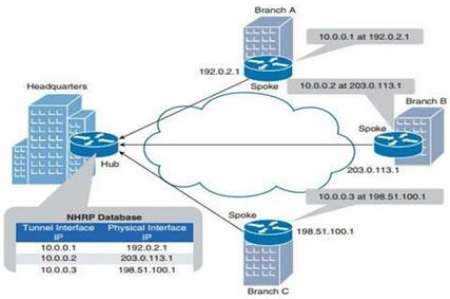
1.2.1. Principais Tecnologias de Uma DMVPN

Neste ponto faremos menção de algumas das principais tecnologias de uma DMVPN, nomeadamente: NHRP, Multipoint GRE, EIGRP e IPSec.

1.2.1.1. NHRP

O NHRP (Next Hop Resulutions Protocol), em português protocolo de resolução do próximo salto é na verdade a grande definição de DMVPN trabalha na camada 2 e com estrutura servidor cliente, tem como responsabilidade manter na base de dados à tabela de roteamento a fim de poder disponibilizar quando pedido assim é configurando para o HUB a instância NHRP Servidor e para as filias a gerente instância NHRP Cliente. Quando um Spoke fica on-line, informa ao Hub não só de um endereço físico IP (atribuído à sua interface física) quanto a um endereço IP lógico (atribuído à sua interface túnel virtual) que será utilizado para os seus túneis.

Figura 12: NHRP map e data base [2]



Fonte: Dados da pesquisa

1.2.1.2. Multipoint GRE

O Multipoint GRE (Multipoint Generic Routing Encapsulations), em portugueses encapsulamentos genéricos de roteamento multiponto. É um protocolo da camada 3 que possui recursos para suportar túnel IPsec múltiplo em uma única interface.

A escalabilidade oferecida pela DMVPN é possível, em parte, pelo Multipoint GRE (mGRE), que permite que um roteador suporte múltiplos túneis GRE em uma única interface GRE. Algumas das características do mGRE são como se segue: Como o GRE tradicional, mGRE pode transportar uma ampla variedade de protocolos (por exemplo, IP unicast, multicast Broadcast). Em uma topologia hub-and-spoke, um roteador hub pode ter uma única interface mGRE, e vários túneis podem usar essa interface única.

Uma interface configurada para mGRE é capaz de formar um túnel GRE dinamicamente usando Next Hop Resolution Protocol (NHRP) para descobrir o endereço IP do destino na outra extremidade do túnel. Você pode implantar o mGRE em uma topologia hub-and-spoke ou uma topologia spoke-to-spoke.

1.2.1.3. EIGRP

O EIGRP ("Enhanced Interior Gateway Routing Protocol", ou seja, Protocolo de Encaminhamento de Gateway Interior Aprimorado), é um protocolo de roteamento híbrido proprietário da Cisco que contém recursos de protocolos de roteamento de vetor de distância e estado de link. Algumas de suas características são:

a) **Convergência rápida**.

O EIGRP usa o algoritmo de atualização de difusão (DUAL) para obter uma convergência rápida. O DUAL não apenas calcula as melhores rotas sem loop, mas também calcula rotas de backup com antecedência antes que elas sejam realmente necessárias. Um roteador EIGRP armazena todas as rotas de backup disponíveis para reagir rapidamente a alterações na topologia da rede. Se nenhuma rota de backup existir na tabela de roteamento, um roteador EIGRP consultará seus vizinhos até que uma rota alternativa seja encontrada.

b) **Uso reduzido da largura de banda**.

O EIGRP não envia atualizações periódicas como nos protocolos DV. Ele envia atualizações parciais sobre as alterações de informações de rota (por exemplo: caminho, métrica). Além disso, a atualização é propagada apenas para roteadores que a requerem, em vez de todos os roteadores dentro de uma área, como nos protocolos de roteamento LS.

c) **Suporte a vários protocolos roteados**.

O EIGRP foi estendido do IGRP para ser independente da camada de rede. Ele suporta IP, IPX e AppleTalk com módulos dependentes de protocolo (PDMs), que são responsáveis pelos

requisitos de protocolo específicos dos protocolos roteados correspondentes. O EIGRP oferece desempenho e estabilidade superiores quando implementado em redes IPX e AppleTalk.

O EIGRP mantém uma tabela de vizinhos, uma tabela de topologia e uma tabela de roteamento para cada protocolo roteado (PDMs) em execução.

d) **Suporta todos os protocolos e topologias de link de dados LAN e WAN**.

O EIGRP não requer configuração especial em nenhum protocolo L2. OSPF requer diferentes configurações para diferentes protocolos L2, por exemplo: Ethernet e Frame Relay. O EIGRP foi projetado para operar com eficiência em ambientes LAN e WAN. O EIGRP suporta todas as redes multiacesso, por exemplo: Ethernet, Token Ring, FDDI e todas as topologias WAN linhas alugadas, links ponto a ponto e topologias multiacesso não broadcast (NBMA), por exemplo: X.25, SMDS, ATM e Frame Relay. EIGRP tem suas raízes como um protocolo de roteamento de vetor de distância (EIGRP é baseado em IGRP).

É considerado um protocolo de roteamento DV avançado com recursos DV tradicionais, por exemplo: sumarização automática, fácil configuração; e recursos LS, por exemplo: descoberta dinâmica de vizinhos. Outra regra do vetor de distância é que, se um vizinho está anunciando um destino, ele também deve estar usando essa rota para encaminhar pacotes para o destino específico.

O EIGRP (Enhanced IGRP) oferece muitos recursos de aprimoramento sobre o IGRP, um protocolo de roteamento DV tradicional, principalmente nas propriedades de convergência e eficiência operacional. Os protocolos de roteamento DV tradicionais enviam atualizações completas periódicas de roteamento, que consomem largura de banda desnecessária.

O EIGRP utiliza apenas multicasts e unicasts; transmissões não estão sendo usadas. Como resultado, os sistemas finais não serão afetados pelas atualizações e consultas de roteamento. - EIGRP é um protocolo de camada de transporte que se baseia em pacotes IP para entregar suas informações de roteamento. Os pacotes EIGRP são encapsulados em pacotes IP com o valor do campo Protocol Number 88 (0x58) no cabeçalho IP. Alguns pacotes EIGRP são enviados como multicasts (endereço IP de destino 224.0.0.10), enquanto outros são enviados como unicasts.

Uma vantagem significativa do EIGRP (e IGRP) sobre outros protocolos de roteamento é o suporte para balanceamento de carga de custo desigual. - O EIGRP executa a sumarização

automática por padrão, mas esse comportamento pode ser desabilitado com o subcomando no roteador de resumo automático.

1.2.1.4. IPSec

O IPSec Security Architecture enquadra um conjunto de normas destinadas a proporcionar comunicações privadas seguras sobre redes IP, através da utilização de serviços de autenticação e encriptação. A segurança em uma DMVPN é fornecida pelo IPSec. As seguintes características de segurança são oferecidas pelo IPSec:

a) Confidencialidade

A confidencialidade dos dados é fornecida por meio de criptografia de dados. Sem um terceiro interceptar dos dados criptografados, o mesmo não seria capaz de interpretar os dados.

b) Integridade

Integridade de dados assegura que os dados não são modificados em trânsito. Por exemplo, os roteadores em cada extremidade de um túnel podem calcular um valor de checksum (verificação da soma) ou um valor de hash para dados, e se ambos os roteadores calcularem o mesmo valor, os dos muito provavelmente não foram modificados em trânsito.

c) Autenticação

A autenticação de dados permite que as partes envolvidas em uma conversa verifiquem que a outra parte é a parte que afirma ser.

d) Anti-replay

O IPsec usa proteção anti-relay para garantir que os pacotes enviados não são pacotes duplicados. Por exemplo, um invasor pode capturar pacotes que compõem um login válido para um host e tentar reproduzir esses pacotes de volta, para que ele possa ter acesso ao host.

No entanto, o IPSec utiliza números de sequência para determinar se um pacote deve ser considerado um pacote duplicado, e quaisquer pacotes duplicados não são transmitidos. Destes serviços do IPSec, criptografia e autenticação são particularmente úteis em uma rede DMVPN. Por exemplo a criptografia pode ajudar a proteger o tráfego que flui entre sites (quer através da Internet ou através da nuvem de um Provedor de serviços). Além disso, a autenticação pode certificar-se que os túneis GRE não são ajustados dinamicamente com spokes indesejáveis.

O IPSec usa uma coleção de protocolos para fornecer suas características. Um dos protocolos primário utilizados pelo IPSec é o protocolo IKE (“Internet KEy Exchange”), ou

seja, troca de chaves de Internet. Especificamente, o IPSec pode fornecer criptografia entre pares autenticados usando chaves de criptografia, que são trocados periodicamente. IKE, no entanto, permite que um administrador configure chaves manualmente.

1.2.2. Fases da DMVPN

Fase 1

Quando implantamos o **DMVPN com a fase 1**, o cliente inicializará e registrar-se-á com o servidor. Um túnel permanente é criado entre Hub e Spoke. Quando um Spoke quer se comunicar com outro tráfego de Spoke, o tráfego passa por hub. Túnel dinâmico não é criado entre Spokes.

Fase 2

Quando implantamos o **DMVPN com a fase 2**, o cliente inicializará e registrar-se-á com o servidor. Um túnel permanente é criado entre Hub e Spoke. Quando um Spoke quer se comunicar com outro Spoke, um túnel dinâmico é criado entre os spokes.

Fase 3

Na **fase 3 da DMVPN**, a Cisco adicionou alguns comandos para melhorar a resposta da consulta NHRP. Esses comandos são:

IP nhrp Redirected que é implementado no hub;

IP nhrp shortcut que é implementado em Spokes.

Quando implantamos o DMVPN com fase 3, o cliente irá registrar-se com o servidor. Um túnel permanente é criado entre Hub e Spoke. Quando um Spoke quer se comunicar com outro Spoke, um túnel dinâmico é criado entre Spokes.

Devido aos comandos extras mencionados acima, quando um Spoke irá fazer uma consulta para um agregado NBMA no Hub. O Hub não dará resposta a essa consulta, o Hub redirecionará a consulta para o Spoke para quem a consulta é gerada.

1.2.3. Vantagens da DMVPN

1. Redução da complexidade da configuração.
2. Suporta roteamento Unicast e Multicast.
3. Suporta roteamento dinâmico com a ajuda do mGRE.
4. Suporta o endereçamento IP dinâmico no lado do Spoke.

5. Suporta Spoke por trás de NAT dinâmico e servidor por trás do NAT estático.
6. Suporta o túnel dinâmico de Spoke to Spoke para conectividade de malha completa.
7. Pode ser usado com ou sem criptografia IPsec.
8. Suporta roteamento virtual e encaminhamento (VFR).
9. Suporta qualidade de serviço (Qos).
10. Escalável com a rede como a configuração é feita somente no novo Spoke. Configuração zero- touch no lado Hub ou Spokes velhos.

1.3. Componentes físicos de uma rede

Segundo [1], há vários dispositivos que podem ser usados em uma rede para fornecer conectividade. O dispositivo usado dependerá de quantos dispositivos você estiver conectando do tipo de conexões que estes dispositivos usam e da velocidade na qual os dispositivos usam e da velocidade na qual os dispositivos operam. Estes são os tipos mais comuns de dispositivos em uma rede:

- Computadores;
- Hubs;
- Switches;
- Roteadores;
- Pontos de acesso sem fio;
- Antenas.

Os componentes físicos de uma rede são necessários para mover os dados entre esses dispositivos. As características do meio determinam onde e como os componentes são usados. Esses são os tipos mais comuns de meios usados em infraestruturas de redes:

- Par torcido;
- Fibra óptica;
- Ondas de rádio.

1.3.1. Dispositivos de rede

Para tornar a transmissão de dados mais extensível e eficiente do que ocorre em uma rede simples ponto-a-ponto, os desenvolvedores de rede usam dispositivos de rede especializados, como hubs, switches, roteadores, antenas e pontos de acesso com fios e sem fios, para enviar dados entre os dispositivos.

HUB

Hub é um dispositivo que tem a função de interligar computadores de uma rede local. A sua forma de trabalho é mais simples comparado com o switch e ao router: O hub recebe dados vindo do computador e transmite às outras máquinas. O instante em que isso ocorre, nenhum outro computador consegue enviar sinal. A sua libertação acontece após o sinal anterior ter sido completamente distribuído.

Switch

A funcionalidade básica de um switch de rede é conectar dispositivos em sua rede de computadores. Switches de rede estão disponíveis com diferentes quantidades de portas e recursos para atender às necessidades e exigências do seu projeto

Existem dois tipos de switches: Não gerenciáveis e gerenciáveis.

Entre eles, switches gerenciáveis são subdivididos em subcategorias. Simplificando, switches gerenciáveis apresentam controles de rede que permitem personalizar, gerenciar e monitorar sua rede. Por outro lado, switches não gerenciáveis é uma solução concebida apenas para aumentar a densidade de portas e não podem ser configurados.

Os switches não gerenciáveis e gerenciáveis (Camada 2 / Camada 2+ e Web Smart). Hoje em dia, não há muita diferença entre switches Camada 2 e Web Smart; ambos os switches dispõem de uma interface gráfica do usuário (GUI), no entanto, apenas switches Camada 2 oferecem uma interface de comando de linha (CLI). [3].

Roteador

O Roteador conecta e permite a comunicação entre duas redes, além de determinar o melhor caminho para que os dados viajem através dessas redes conectadas.

Os roteadores precisam do IOS (“Internetwork Operating System”, ou seja, Sistema Operacional de Interconexão de Redes) para executar as funções definidas nos arquivos de configuração.

Os arquivos de configuração contêm as instruções e os parâmetros que controlam o fluxo de tráfego que entra e sai dos roteadores. Os roteadores são os dispositivos que compõem o backbone das grandes intranets e da Internet. Eles operam na camada 3 do modelo OSI, tomando decisões com base nos endereços de rede.

Pontos de acesso sem fios

Os pontos de acesso sem fios fornecem um acesso de rede a dispositivos sem fios, como laptops e PDA´s ("Personal Digital Assistants", ou seja, Assistentes Digitais Pessoais). O ponto de acesso sem fios usa ondas de rádio para se comunicar com rádios em computadores, PDA´s e outros pontos de acesso sem fios. Um ponto de acesso tem uma faixa limitada de cobertura. Redes grandes requerem vários pontos de acesso para fornecer uma cobertura sem fios adequada.

Antenas

Para Korth (2001) "As antenas podem ser utilizadas para emitir ou receber sinas eletromagnéticos, uma corrente elétrica variável é produzida no transmissor e esse tipo de corrente tem sua intensidade variando em função do tempo" (p.83).

De acordo com a função trigonométrica seno, a essa variação associamos uma grandeza chamada frequência, que é medida em hertz". A corrente então oscila ao longo de um condutor e essa oscilação vai produzir um campo eletromagnético, ou seja, vai produzir ondas eletromagnéticas. As ondas eletromagnéticas produzidas são emitidas e viajam através do espaço em todas as direções, como o espaço está repleto de ondas eletromagnéticas vindas de diversas fontes, e como são ondas, elas possuem frequência e comprimento de onda. É exatamente essas duas grandezas que vão diferenciar uma da outra.

Cada onda tem sua própria frequência, quanto maior o valor da frequência, menor será o comprimento de onda. Logo, quanto maior o comprimento de onda, menor será a frequência da onda. Essas ondas chegam a uma infinidade de antenas receptadoras espalhadas pelas cidades, mas cada antena irá captar apenas as ondas que estão na faixa de frequência programada. Ao chegar na antena receptora, a onda irá induzir uma corrente alternada que oscilará com uma frequência igual a sua. Apesar dessa corrente ser bem mais fraca do que a corrente que gerou a onda na antena transmissora, ela pode ser amplificada no aparelho receptor.

1.3.2. Meios de rede

Existem vários meios físicos que podem ser usados para realizar a transmissão de dados. Cada um tem o seu próprio nicho em termos de largura de banda, retardo, custo e facilidade de instalação e manutenção. Os meios físicos são agrupados em meios guiados, como fios de cobre e fibras ópticas, e em meios não guiados, como as ondas de rádios e os raios laser transmitidos pelo ar.

❖ **Cabo de par trançado**

Segundo Booch (1999), O cabo par trançado é um conjunto de pares de fios de cobre que são revestidos de isolamento plástico codificado por cores e trançados juntos. As vezes uma blindagem metálica é colocada sobre eles, daí o nome par trançado blindado" (p. 23). O cabo sem blindagem é chamado par trançado não blindado e é usado em ligações até 1Gigabit por segundos"

- **UTP**

UTP ("Unshielded Twisted Pair", ou seja, par trançado não blindado) conta exclusivamente com o efeito de cancelamento produzido pelos pares de fios trançados o qual limita a degradação do sinal causada pela interferência eletromagnética EMI (Electromagnetic Interference) e pela interferência de radiofrequência RFI (Radio Frequency Interference). O UTP é tipo de cabeamento mais comumente usados em redes. Os cabos UTP têm um alcance de 100 metros.

- **STP**

No STP ("Shielded Twisted Pair", ou seja, par trançado blindado), cada par de fios é revertido por uma folha metálica para melhor proteger os fios de ruído. Quatro pares de fios são então completamente revestidos em uma fita ou folha metálica. O STP reduz o ruído eléctrico de dentro do cabo. Também reduz a EMI e a RFI de fora do cabo. Embora o STP evite a interferência com mais eficiência do que o UDP, o STP é mais caro devido a blindagem extra e é mais difícil de instalar devido a sua espessura. Além disso, a blindagem metálica deve ser aterrada em ambas as extremidades. Se for indevidamente aterrada, a blindagem age como uma antena captando sinais indesejados.

❖ **Cabo coaxial**

Outro meio de transmissão é o cabo coaxial. Ele tem maior blindagem que os pares trançados e, assim, pode se estender por distâncias mais longas em velocidades mais altas. Um cabo coaxial consiste em um fio de cobre esticado na parte central, protegido por material isolante.

❖ **Fibra óptica**

Uma fibra óptica é um condutor de vidro ou plástico que transmite informações usando luz. A fibra óptica é totalmente imune a ruídos, com isso a comunicação é mais rápida. As fibras

ópticas utilizadas nas redes são classificadas de acordo com a forma que a luz trafega no cabo, sendo elas monomodo e multímodo (Duarte, 2016, p. 43).

- **Multimodo**

Para Balder (2012) Cabo com núcleo mais grosso que o cabo monomodo. “É mais fácil de ser produzido, permite o uso de fontes luminosas mais simples como LED´s (Light Emitting Diodes) díodos emissores de luz, e funciona bem em distâncias de alguns poucos quilômetros ou menos” (p. 31).

- **Monomodo**

Cabo com um núcleo muito fino. É mais difícil de ser produzido, usa lasers como fonte luminosa e pode transmitir sinais a dezenas de quilômetros com facilidade. Uma fibra óptica é uma ou mais fibras ópticas revestidas por uma camisa ou jaqueta de proteção.

❖ **Redes sem fios**

Para Rudio (2007) “As redes sem fios surgiram como redes complementares ás redes cabeadas, com o intuito de promover a mobilidade e a visualização rápida dos dados independentemente da localização do usuário tendo os dados transmitidos pelo ar ou espaços, que se constituem como meio físico para propagação de sinais eletromagnéticos” (p.37).

CAPITULO II - FUNDAMENTAÇÃO METODOLÓGICA

No presente capítulo, apresentamos a caracterização do campo de estudo, o modelo da pesquisa, participantes do estudo, técnicas e instrumentos bem como os procedimentos e as dificuldades.

2.1. Caracterização do campo de estudo

Os subtítulos a seguir irão descrever os elementos necessários para caracterização do campo de estudo.

2.1.1. Localização geográfica

Relactivamente a situação geográfica, A MEDNET LDA localiza-se no Bairro da Carreira de tiro, Zona nº 6, nos arredores da Escola Primária António Agostinho Neto. E encontra-se limitada a Norte com o Hospital Municipal de Malanje, a Sul com a Shoprite, A Leste com a Escola Primária Samora Machel e a Oeste com a Igreja São Paulo.

2.1.2. Historial

A MEDNET LDA – é uma organização de direito angolano de comércio e prestação de serviços, foi criada em Angola no ano de 2019. Tendo começado com as suas actividades comerciais em março de 2020.

Está conta actualmente com mais de 20 funcionários, repartidos em três (3) ramos de actividades (Farmácia, restaurante, bar, salão de beleza e spar).

Posição competitiva: solidez patrimonial e técnica, eficiência operacional, gestão e desenvolvimento dos recursos humanos, oferta adaptada de produtos ao mercado angolano. Bem como a inovação nos seus serviços.

2.1.3. Missão

A mesma tem como missão: participar activamente no desenvolvimento da economia angolana com uma oferta global nos ramos de farmácia, restaurante, bar, salão de beleza e spar, garantir o melhor serviço aos seus clientes e ser a referência no mercado Angolano.

Oferecer produtos e serviço na área gastronómica, o saber e a correta técnica de elaboração de cada alimento, para contribuir na saúde dos nossos clientes, ofertando um sistema de atendimento diferenciado.

Encantar e surpreender nossos clientes através do nosso ambiente, atendimento e gastronomia de alta qualidade, proporcionando uma experiência completa e inesquecível.

2.1.4. Visão

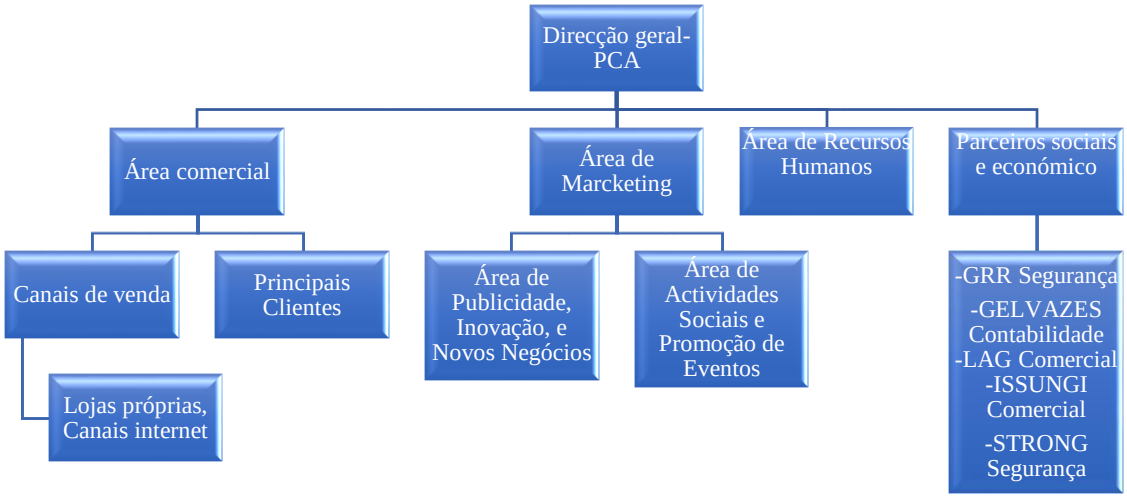
Ser a preferência dos angolanos. Ser uma empresa reconhecida como referência dentro da gastronomia angolana buscando qualidade, agilidade no atendimento em manter um bom relacionamento com clientes, colaboradores e fornecedores. Sempre valorizando a troca de experiência na convivência entre restaurante e nossos clientes em um espaço aconchegante num ambiente familiar.

Tornar-se num restaurante reconhecido, sendo referência de alto padrão e de alta qualidade, se destacando como um restaurante diferenciado no mercado, onde a busca de crescimento e desenvolvimento seja constante em todos os níveis e sectores da empresa

2.1.5. Valores

- ❖ Cliente em primeiro lugar, Qualidade, Eficiência e Inovação.
- ❖ Nutrição, para promover a saúde e a boa qualidade de vida.
- ❖ Sabor para proporcionar o prazer de comer bem.
- ❖ Variedade, para oferecer opções com qualidade com todos os gostos
- ❖ Atendimento com excelência, para apresentar soluções gastronômicas.
- ❖ Serviço rápido e práticos, para adequar o estilo de vida de quem não tem tempo a perder.

Figura 13: Organograma da empresa MEDNET.



Fonte: Dados da pesquisa

2.2. Modelo de pesquisa

Para a concretização do presente estudo, usou-se a pesquisa qualitativa. Por permitir a utilização do método indutivo, que por meio da análise de conteúdo, levou a diferentes fases de

desenvolvimento do presente trabalho de investigação, se constituísse como elemento contínuo que liga o problema aos dados.

A escolha da abordagem qualitativa deveu-se pelo facto de ser uma abordagem que visa envolver as pessoas que agem em função das suas experiências sociais, econômica e cultural, além disso, descrevem as ideias, crenças e opiniões tal como elas acontecem.

Para analisar os dados recolhidos através dos instrumentos de recolha de dados, privilegiou-se a análise de conteúdo categorial, por se adequar ao tratamento de informações qualitativas, e por ser uma técnica de tratamento de dados coletados, que visa a interpretação do material de caráter qualitativo.

2.3. Participantes do estudo

Para o presente estudo, tivemos um total de desaseis (16) participantes.

Participantes selecionados

Do número total de participantes, foram eleitos como amostra para a pesquisa cinco (5) participantes, concretamente, um (1) Gerente, três (3) balconistas (1) farmacêutico.

Tabela 1: Características dos participantes da pesquisa.

Nº de Participantes	Idade	Sexo		Nível académico		
		M	F	Médio	Licenciado	Total
Gerente	35/40	01	00	00	01	01
Balconista (02)	20/26	02	02	04	00	04
Cabelereiro(07)	23/26	01	06	07	00	07
Farmacêuticos	20/28	02	02	04	00	04
TOTAL		06	10	15	01	16

Fonte: Dados da pesquisa

2.4. Técnicas e instrumentos

Segundo Pardal & Correia (1995) consideram técnicas como “um instrumento de trabalho que viabiliza a realização de uma pesquisa” (p. 14). Segundo Rudio (1986)” chama-se

de instrumento de pesquisa o que é utilizado para a coleta de dados". Para a Concepção do mesmo sistema, foram utilizadas várias técnicas, nomeadamente:

Técnica documentaria: que consistiu em consulta, livros e outros documentos relacionados a nossa pesquisa, assim como livros, sebentas, artigos, etc.

Técnica de entrevista: esta nos facilitou um contacto directo com os responsaveis da empresa que nos forneceram informações precisas. Este contacto foi feito com 5 funcionários da referida empresa.

A técnica documentária foi utilizada porque a mesma utiliza fontes primárias, ou seja, recorre as fontes mais diversificadas e dispersas. Já a técnica da entrevista foi utilizada porque a mesma se distingue da simples conversação que tem como objectivo básico a coleta de dados.

2.5. Procedimentos

Para a realização do presente trabalho foram feitos vários procedimentos, desde a aprovação do tema até a conclusão. No entanto, quanto a escolha e aprovação do tema, surgiu em nós um interesse em implementar uma rede local (LAN) para melhorar o reabastecimento e monitoramento da área de produção para loja de um amigo que usava métodos manuais para o controlo da produção e das vendas. Também o escolhemos para atingir o grau de licenciatura em Engenharia Informática que foi remetido ao departamento de Engenharias e logo foi aprovado.

Para o trabalho, foi usado 1 guião de entrevista aplicado a 10 participantes, sendo que as entrevistas foram feitas a alguns funcionários da empresa. Usamos os métodos de desenvolvimentos ágeis de software que nos permitiram obter resultados e chegar a uma conclusão de desenvolver uma rede local (LAN) que ajudasse e atendesse as necessidades do Cliente.

Trabalhava em 3 períodos, nomeadamente: Manhã, Tarde e Noite. No período da Manhã fazia o levantamento de requisitos e entrevistas sempre que fosse necessário. No período da Tarde fazia o mapeamento da rede e escrevia a Monografia. Já no período da Noite fazia a configuração da rede.

2.6. Dificuldades

Durante o trabalho, se deparamos com vários problemas ou dificuldades como a pouca colaboração dos clientes em falar sobre as dificuldades que tinham quando compravam artigos no Bar Mednet. Também encontramos dificuldades por parte do desenvolvimento da rede, pois

algumas funcionalidades das aplicações usadas como recurso carecem de pagamento de licença para estarem habilitadas.

Do número total de participantes, foram eleitos como amostra para a pesquisa cinco (5) participantes, concretamente, um (1) gerente, três (3) balconistas e um (1) farmacêuticos.

2.7. Análise de requisitos

O objectivo da implementação dessa rede é criar uma ligação entre a área de produção e a área de monitoramento e reabastecimento, para garantir uma distribuição rápida, e diminuir o tempo de espera por parte de clientes que solicitam um produto ou um serviço, bem como o controlo do stock e das vendas realizadas.

Apartir da rede, a área de produção poderá fazer pedidos de reabastecimento de matéria primas para o confeccionamento dos produtos e apartir da mesma informar o produto confeccionado para então planejar o reabastecimento.

Escalabilidade

A escalabilidade refere-se ao quanto de crescimento da rede que um projeto deve suportar. Grandes empresas adicionam usuários, aplicativos, sites adicionais e conexões de redes externas rapidamente. O projeto de rede que se propõe a um cliente deve ser capaz de se adaptar aos aumentos no uso e no seu escopo.

Cada departamento deverá ter uma sub-rede própria, com uma demanda específica de crescimento. Todos os dispositivos que forem acessados por mais de um departamento deverão se localizar em uma única sub-rede privada compartilhada. Os dispositivos que precisarem ser acessados por meio de uma rede externa deverão estar em uma sub-rede. Essa sub-rede terá que ser alocada com base nos endereços públicos designados à empresa.

Disponibilidade

A disponibilidade está relacionada ao tempo em que a rede está disponível para os usuários. Deve assegurar-se que os sistemas operem prontamente e seus serviços não fiquem indisponíveis para os usuários autorizados.

Desempenho

As redes de computadores são projetadas para exibir alto desempenho. Programas distribuídos em diversas máquinas utilizam a rede para trocar dados. A eficácia desse modelo de processamento muitas vezes depende fundamentalmente da eficácia da rede por intermédio

da qual os dados são trocados entre tais programas. O desempenho visa assegurar que a rede está com alta eficiência, boa vazão de dados, baixo atraso.

Políticas de Segurança

Uma política de segurança da informação bem elaborada, facilita o gerenciamento da segurança de uma empresa, por meio de padrões para a proteção dos dados. A segurança de rede e de internet consiste em um conjunto de medidas para desviar, prevenir, detectar e corrigir violações de segurança que envolvam a transmissão de informações. Os principais objetivos que as políticas visam garantir são:

a) Disponibilidade

Serão adotados mecanismos de backup no acesso às informações do modelo hierárquico da rede, de links de internet alternativos e servidores alternativos, visando aumentar ao máximo a disponibilidade dos dados.

b) Confidencialidade

Utilizando mecanismos de segurança, na firewall com suas políticas de restrição de acesso da internet para a rede interna, reduz-se a chance de acesso não autorizado de pessoas do meio externo para o interno.

c) Integridade

Para garantir que a informação armazenada ou transferida mantenha características originais estabelecidas pelo proprietário da informação, incluindo controle de mudanças. Garantir e apresentar corretamente para os usuários que consultarem. Dentro da rede cada usuário utilizará um usuário e sua senha para que seja feito o acesso somente aos conteúdos pertinentes às suas necessidades.

d) Não Repúdio

Será também utilizado logs de acesso 12 e logs dos servidores de arquivo e do sistema, para que cada usuário tenha a responsabilidade de todas as alterações e acesso ao conteúdo da corporação. Cada usuário é responsável por suas credenciais, sendo inaceitável a alegação de que a alteração não foi feita por ele, caso conste nos logs.

Os requisitos de Autenticidade e Integridade são feitos da mesma forma, utilizando as credenciais e as políticas de segurança, dispensando suas descrições nesses documentos.

Um projeto de segurança, em síntese, procura garantir proteção aos dados e aos espaços da organização.

e) Gerenciabilidade

Segundo Reis (2013) “O gerenciamento da rede envolve um conjunto de políticas e algumas ferramentas de gerência que colherão informações importantes para a tomada de decisão” (p. 23).

Essas informações serão fornecidas pelos equipamentos por meio de gerentes e agentes de monitoramento, que serão armazenadas e organizadas para permitir a geração de gráficos que facilitarão a administração da rede. O gerenciamento da rede envolve um conjunto de gerências que resultam na facilidade de administrá-la.

CAPÍTULO III - APRESENTAÇÃO, ANÁLISE E INTERPRETAÇÃO DOS RESULTADOS

Neste capítulo abordaremos sobre implementação da tecnologia DMVPM para interligar duas entidades privadas relativamente a MEDNET e a MEDNET-Filial, bem como de alguns dos seus principais protocolos e serviços e o uso da infraestrutura de rede usada para prover a comunicação de um ponto ao outro usando sinais de rádio frequência.

Há uma variedade de serviços e de informações que podem ser partilhadas entre as duas empresas, no entanto, a tecnologia que soluciona esta interligação são os túneis mGre, entanto a mesma permite que possam trafegar serviços como VoIP, HTTP, DHCP entre outros.

3.1. ISP

ISP (Internet Service Provider ou Provedor de serviços de Internet), são empresas que fornecem serviços de acesso à internet, geralmente por uma conexão discada, DSL ou de banda larga. Os ISPs também podem oferecer serviços relacionados, como contas de e-mail, hospedagem, registro de nome de domínio e até serviços de comunicação de dados, blogs, televisão, telefonia e outros.

Para tanto, o provedor pode escolher diferentes meios de fornecer o serviço de internet, sendo que os mais utilizados atualmente é por fibra óptica e radio frequência, tendo em vista que a tecnologia fibra óptica está cada vez mais avançada e possibilita que os provedores ofereçam serviços de altíssima qualidade.

3.2. Topologias

Toda infraestrutura de rede de qualquer provedora ou entidade empresarial tem uma rede, ou seja, a estrutura topológica da rede e pode ser descrito física ou logicamente. Há várias formas nas quais se podem organizar a interligação em cada um dos nós da rede. Existem duas categorias básicas de topologia de redes:

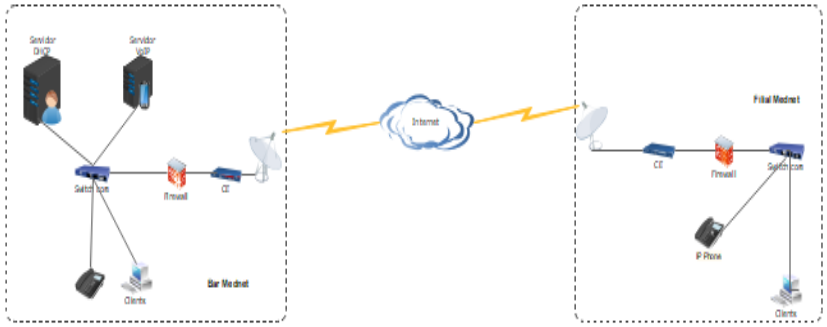
- **Topologia Física.**
- **Topologia Lógica.**

A **topologia física** é a verdadeira aparência da rede ou o layout da rede, isto é, representando como as redes estão conectadas e os meios de conexão dos dispositivos de redes.

A **topologia lógica** refere-se a maneira como os sinais agem sobre os meios de rede ou a maneira como os dados são transmitidos através da rede a partir de um dispositivo para outro sem ter em conta a interligação dos dispositivos de redes.

Para a topologia que se segue, ficou reduzida a 4 administrações em termos de resolução da topologia pois mais do que isso, não haveria uma topologia visível.

Figura 14: Topologia Física proposta de ligações entre o bar Mednet e a filial



Fonte: Dados da pesquisa

3.2.1. Configuração da topologia lógica (simulada).

A realização deste projecto foi feito através de simulações de ambientes, usando a ferramenta de emulação e outros softwares que serão descritos abaixo:

O emulador **GNS3** permite a reprodução fiel das características de diversos modelos de roteadores, sobretudo do fabricante Cisco Systems, possibilitando a criação de diversos cenários, com plataformas de roteadores 1700, 2600, 3600, 3700 e 7200. O GNS3 também permite a adição virtual de alguns módulos disponíveis para cada plataforma de roteador.

Figura 15: GNS3 versão 2.1.21

Fonte: Dados da pesquisa

Usou-se também um software de virtualização de dispositivos, que permite executar várias instâncias de sistemas operacionais em uma única máquina física, o **VMWARE.**

Figura 16: WMWARE.

Fonte: Dados da pesquisa

Wireshark é um software analisador de pacotes e protocolos de rede, permite capturar e navegar sobre o tráfego da rede e visualizar o plano de controle dos serviços implementados em execução.

Figura 17: Wireshark.

Fonte: Dados da pesquisa

Windows 7 é uma versão do Microsoft Windows, uma série de sistemas operativos produzidos pela Microsoft para uso em computadores pessoais, incluindo computadores domésticos e empresariais, laptops, tablets e PCs de centros de mídia, entre outros.

Figura 18: Windows 7

Fonte: Dados da pesquisa

O aplicativo **Zoiper** é um IAX e SIP aplicação softphone gratuito para chamadas VoIP via 4G ou Wi-Fi e oferece uma interface de usuário simples e excelente qualidade de áudio para a voz suave sobre a experiência IP.

Figura 19: Zoiper.

Fonte: Dados da pesquisa

Elastix é uma distribuição livre de Servidor de Comunicações Unificadas que integra em um só pacote: VoIP, PBX, Fax, Mensagem Instantânea, Correio electrónico.

Figura 20: Elastix.

Fonte: Dados da pesquisa

O FortiGate utiliza processadores de segurança especialmente desenvolvidos e serviços de segurança de inteligência de ameaças dos laboratórios FortiGuard com tecnologia de IA para oferecer proteção de alto nível e inspeção de alto desempenho de tráfego criptografado e de texto claro.

Os firewalls de última geração reduzem o custo e a complexidade com visibilidade total dos aplicativos, usuários e redes e fornecem a melhor segurança do mercado.

Como parte integrante do Fortinet Security Fabric, os firewalls de próxima geração podem se comunicar dentro do abrangente portfólio de segurança da Fortinet, bem como soluções de segurança de terceiros em um ambiente de vários fornecedores.

Figura 21: Fortigate.

Fonte: Dados da pesquisa

Para o presente projecto fez-se a simulação da rede em um ambiente simulado, com auxílio da ferramenta GNS3, com o mesmo foi possível configurar os equipamentos de rede que seguem na tabela abaixo.

Tabela 2: Dispositivos usados na Simulação

Dispositivos	Quantidade	Versão e Software	Capacidade
Roteadores	2	c3725-adventerprisek9-mz124-15	250 Mb
Switches	2	N/A	N/A
Computadores	2	Windows 7 x64	25 Gb
Servidor	1	Elastix-2.5.0-STABLE-I386-bin-08may2015	20 Gb
Firewall	1	Fortigate6.2.2-2	150 Mb
Softphone	2	Zoiper5_Installerv5.4.12	193 Mb

Fonte: Dados da pesquisa

A topologia completa que servirá como base para todas as implementações e testes realizados é apresentada na figura abaixo. Embora essa topologia não reflita, em termos de dimensão, a realidade de um backbone de um provedor de serviços, normalmente composto de centenas de roteadores, procurou-se utilizar uma topologia suficiente para exibição dos serviços aqui propostos, podendo servir em sua integridade a um backbone real.

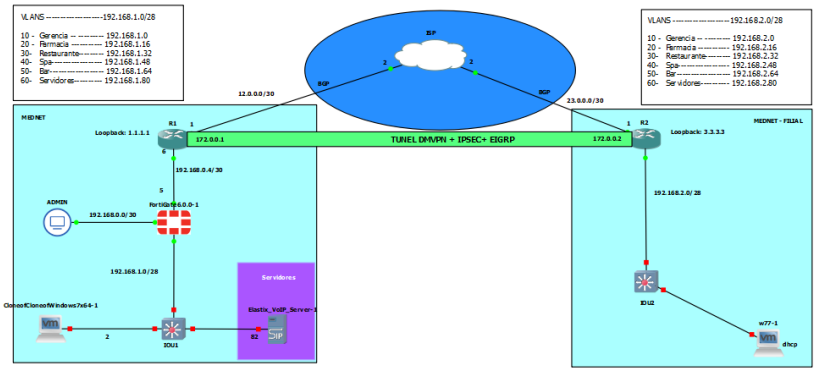
Representou-se assim os resultados da implementação da DMVPN derivada da materialização dos objectivos proposto neste trabalho. A rede tem 2 pontos uma sede e uma filial que será representada na figura abaixo.

Tabela 3: Tabela de roteamento da rede

Dispositivo	**Interface**	**Endereço IP**	**Máscara de Subrede**	**Observação**
R1	Fastethernet 1/0	12.0.0.1	255.255.255.252	Site 1- HUB-MEDNET
	Fastethernet 2/0	192.168.0.6	255.255.255.252	
	Loopback 0	1.1.1.1	255.255.255.255	
PC-Clone of clone Windows7	N/A	DCHP	DHCP	
PC- W77	Fastethernet 0/0.10	192.168.2.1	255.255.255.240	Site 2- Spoke-MEDNET - FILIAL
	Fastethernet 2/0	23.0.0.1	255.255.255.252	
	Loopback 0	3.3.3.3	255.255.255.255	
R2	N/A	DCHP	DHCP	

Fonte: Dados da pesquisa

Figura 22: Topologia Simulada



Fonte: Dados da pesquisa

O plano de endereçamento obedeceu o padrão de escalabilidade assim como facilidade de identificação do site a nível de resolução de problema. Os endereços públicos foram fornecidos pelo ISP sendo estático para cada site.

Planeou-se os endereços privados da seguinte forma, os primeiros e os segundos octetos não são alterados 192.168.X.X, sendo que o terceiro octeto como identifica a rede então combinou-se com a identificação do site e a identificação do endereço de túnel padronizando assim o endereçamento de cada site:

MEDNET (Site-ID #1): LAN IP – 192.168.1.0/28 – Túnel IP 172.0.0.1/24

MEDNET FILIAL (Site-ID #2): LAN IP – 192.168.2.0/28 – Túnel IP 172.0.0.2/24

a) Site

Site é uma instalação isolada, restrita, monitorada, com temperatura e umidade controladas para evitar o superaquecimento dos equipamentos, especialmente projetado para concentrar dispositivos de informática e telecomunicações, com o objetivo de manter em segurança hardwares críticos e informações geradas por uma empresa ou instituição pública.

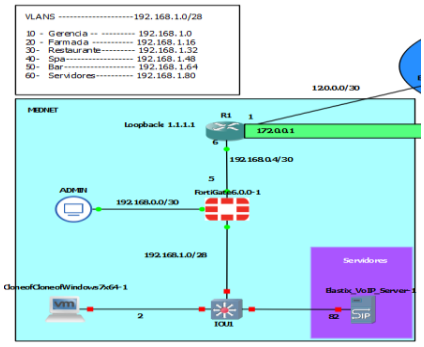
Figura 23: Site de Telecomunicações

Fonte: Dados do autor

3.2.2. Configurações no Hub (Site 1) – MEDNET

Para configuração do Hub ou simplesmente a MEDNET, foram escalados um roteador de borda responsável pelo encaminhamento de pacotes, o servidor Elastix responsável por prover serviço de voz sobre IP, um firewall Fortigate responsável por garantir as políticas de acesso, configuração de serviços como DHCP, VLAN´s e demais serviços e também verifica-se um swicth, e um computador com o sistema operativo Windows 7 instalado com o softphone Zoiper para acesso aos serviços disponibilizados pela infraestrutura como o VoIP, foram criadas VLAN´s, visto que é um ambiente corporativo privado é de extrema importância, reduzindo assim o congestionamento na rede principal e separando o trafego por departamentos . A figura abaixo ilustra a disposição dos elementos da MEDNET.

Figura 24: Configuração dos endereços IP´s das interfaces do Router da MEDNET.



Fonte: Dados da pesquisa

Figura 25: Configuração dos endereços IP´s das interfaces do Router

```
MEDNET-RT#show ip interface brief | include up
FastEthernet1/0            12.0.0.1        YES NVRAM  up                    up
FastEthernet2/0            192.168.0.6     YES NVRAM  up                    up
Loopback0                  1.1.1.1         YES NVRAM  up                    up
Tunnel100                  172.0.0.1       YES NVRAM  up                    up
```

Fonte: Dados da pesquis

Figura 26: Configuração do Túnel da Sede

```
MEDNET-RT#Show running-config interface tunnel 100
Building configuration...

Current configuration : 362 bytes
!
interface Tunnel100
 ip address 172.0.0.1 255.255.255.0
 no ip redirects
 ip mtu 1400
 no ip next-hop-self eigrp 1
 ip nhrp authentication 123
 ip nhrp map multicast dynamic
 ip nhrp network-id 10
 ip nhrp holdtime 10
 ip tcp adjust-mss 1360
 tunnel source FastEthernet1/0
 tunnel mode gre multipoint
 tunnel key 10
 tunnel protection ipsec profile DMVPN
end
```

Fonte: Dados da pesquisa

Figura 27: Configuração do protocolo EIGRP

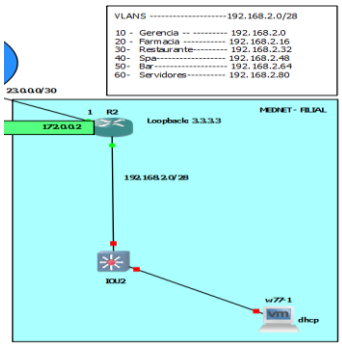
```
MEDNET-RT#show running-config | section eigrp
 no ip next-hop-self eigrp 1
router eigrp 1
 redistribute static
 network 172.0.0.0
 network 192.168.0.0
 no auto-summary
```

Fonte: Dados da pesquisa

3.2.3. Configurações no Spoke (Site 2) MEDNET-FILIAL

Os equipamentos configurados no spoke teremos um roteador da mesma família com o roteador do Hub e um switch. Configurou-se também o softphone Zoiper para fazer chamadas via VoIP e acesso a pasta de partilha de informação, tudo em computador virtualizado com o sistema operativo Windows 7.

Figura 28: Descrição das interfaces no spoke MEDNET-filial



Fonte: Dados da pesquisa

Figura 29: Configuração dos endereços IP´s das interfaces do Router da filial.

```
MEDNET-FILIAL-RT#show ip interface brief | include up
FastEthernet0/0            unassigned      YES NVRAM  up                    up
FastEthernet0/0.10         192.168.2.1     YES NVRAM  up                    up
FastEthernet2/0            23.0.0.1        YES NVRAM  up                    up
Loopback0                  3.3.3.3         YES NVRAM  up                    up
Tunnel100                  172.0.0.2       YES NVRAM  up                    up
```

Fonte: Dados da pesquisa

Figura 30: Configuração do Túnel da MEDNET-Filial.

```
MEDNET-FILIAL-RT#show running-config interface tunnel 100
Building configuration...

Current configuration : 368 bytes
!
interface Tunnel100
 ip address 172.0.0.2 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip nhrp authentication 123
 ip nhrp map multicast 12.0.0.1
 ip nhrp map 172.0.0.1 12.0.0.1
 ip nhrp network-id 10
 ip nhrp nhs 172.0.0.1
 ip tcp adjust-mss 1360
 tunnel source FastEthernet2/0
 tunnel mode gre multipoint
 tunnel key 10
 tunnel protection ipsec profile DMVPN
end
```

Fonte: Dados da pesquisa

Figura 31: Configuração do protocolo EIGRP da da MEDNET-Filial

```
MEDNET-FILIAL-RT#show running-config | section eigrp
router eigrp 1
 network 172.0.0.0
 network 192.168.2.0
 no auto-summary
```

Fonte: Dados da pesquisa

3.2.4. Configuração de Serviços

Nesta secção configurou-se os serviços para a rede que interliga o Hub e o spoke. Os serviços configurados são:

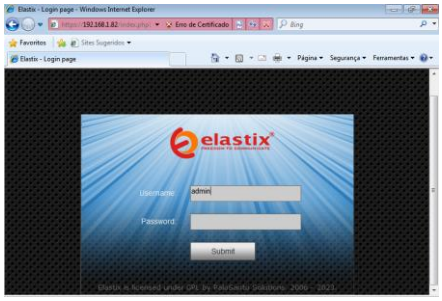
- VOIP
- Firewall fortigate
- DHCP
- Pasta da rede

a) Configuração do serviço VoIP

De modo que seja possível a conversação entre os clientes, configurou-se a central de voz, com isso pode-se cadastrar os ramais para poder assim habilitar as chamadas.

A configuração foi feita em um ambiente gráfico interativo, com recurso de uso de um navegador web para poder aceder o servidor Elastix com o endereço 192.168.1.82, que é a PBX virtual.

Figura 32: Autenticação para aceder o Servidor Elastix

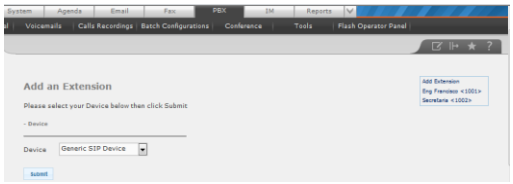


Fonte: Dados da pesquisa

Para poder aceder o servidor, no momento de instalação é definida uma palavra passe, para proteger o servidor contra o uso indevido, cabendo assim apenas o acesso ao administrador de rede como ilustrado na figura 32.

A seguir ao processo de autenticação, configurou-se os ramais, para este caso sempre que um novo cliente for adicionado na rede o processo será repetido.

Figura 33: Adição de uma extensão pelo Servidor



Fonte: Dados da pesquisa

Com o servidor devidamente configurado, usou-se o softphone Zoiper como já frisado nas secções anteriores que será o software que permitirá fazer chamadas. Para configurar o softphone, digita-se a extensão e senha, que anteriormente adicionados no servidor, para que o mesmo cliente depois de terminada a inserção dos dados no Zoiper, o mesmo consiga efectuar chamadas.

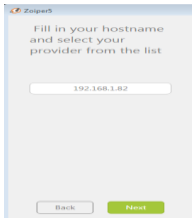
Figura 34: Adição dos dados do Cliente no softphone

Fonte: Dados da pesquisa

O passo a seguir será apontar para o nosso servidor PBX virtual, onde estão configurados os ramais, pois sem este passo o usuário não será capaz de efectuar chamadas.

Processo simples com a introdução do endereço do servidor Elastix, com esta etapa concluída, a figura 4.36 exibe o resultado final mostrando que a solicitação do softphone encontrou a extensão presente no servidor.

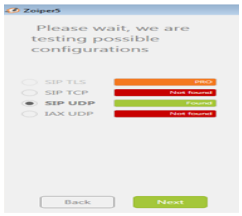
Figura 35: Adição do endereço IP do Servidor Elastix



Fonte: Dados da pesquisa

Como mencionado anteriormente, com as credenciais adicionadas, o campo SIP UDP estará verde com a mensagem found.

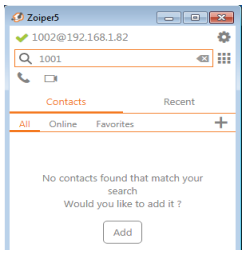
Figura 36: Sucesso na adição das credenciais do Cliente



Fonte: Dados da pesquisa

Com todos os passos concluídos com sucesso pode-se efectuar a chamada.

Figura 37: Softphone preparado para efectuar chamadas



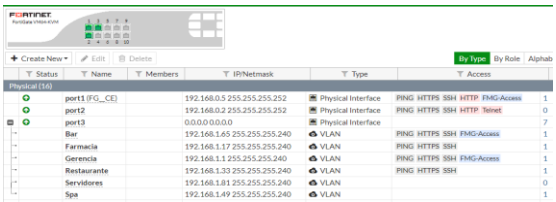
Fonte: Dados da pesquisa

b) Configuração do Firewall Fortigate

Para segurança da rede devido ao acesso à internet, optou-se por um firewall Fortigate 3000d.

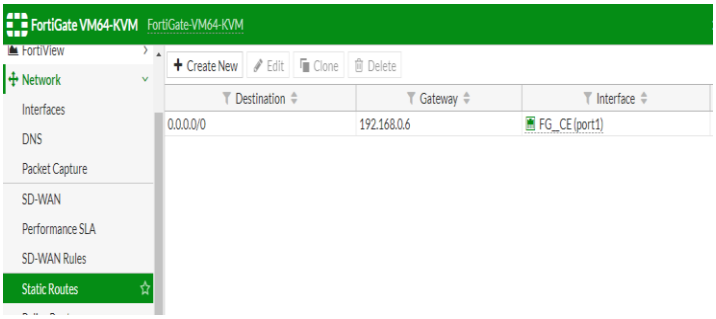
Configurou-se interface WAN onde foi habilitado o acesso via WEB e para a LAN uma sub-interface que proverá IPs dinâmicos à rede da sede MEDNET . Foi habilitado firewall police, modo a filtrar o tráfego vindo da rede externa (Internet).

Figura 38: Configurando as VLANs



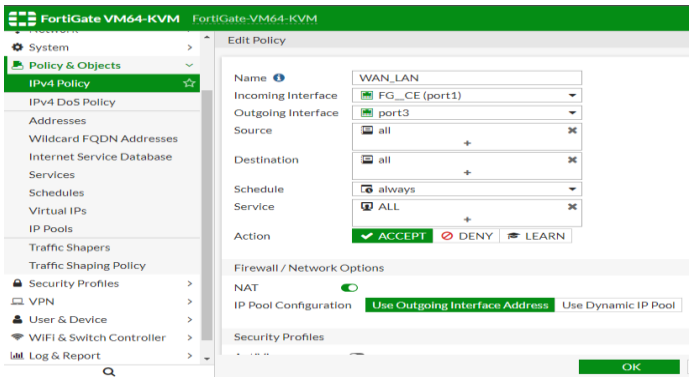
Fonte: Dados da pesquisa

Figura 39: Configurando a rota estática.



Fonte: Dados da pesquisa

Figura 40: Configurando as políticas de acesso.



Fonte: Dados da pesquisa

c) Configuração do DHCP

Como característica de uma rede convergente, foi configurado na filial o serviço DHCP para permitir que os hosts obtenham IP de forma dinâmica dispensando a necessidade de adicionar de forma manual.

Figura 41: Configurando as políticas de acesso.

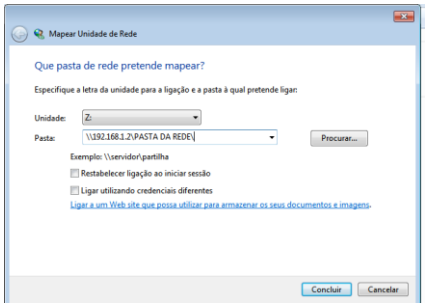
```
MEDNET-FILIAL-RT#show running-config | section dhcp
no ip dhcp use vrf connected
ip dhcp excluded-address 192.168.2.1
ip dhcp pool LAN10
   network 192.168.2.0 255.255.255.240
   default-router 192.168.2.1
   dns-server 8.8.8.8
```

Fonte: Dados da pesquisa

d) Configuração da pasta da rede

Como um dos objectivos deste projecto é o compartilhamento da informação de forma rápida e segura , foi configurado uma pasta de rede onde a filial e a sede poderão partilhar as informações.

Figura 42: Mapeamento da pasta de rede.



Fonte: Dados da pesquisa

3.2.5. Análise de resultados

a) Tecnologia de interligação e segurança

O ***show dmvpn*** é o camando que nos permite visualizar o estado da DMVPN

Figura 43: Visualização do estado da DMVPN.

```
MEDNET-RT#show dmvpn
Legend: Attrb --> S - Static, D - Dynamic, I - Incompletea
       N - NATed, L - Local, X - No Socket
       # Ent --> Number of NHRP entries with same NBMA peer

Tunnel100, Type:Hub, NHRP Peers:1,
 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1        23.0.0.1       172.0.0.2    UP    never D
```

Fonte: Dados da pesquisa

O ***show ip nhrp detail*** é o comando que nos permite verificar o estado do nosso NHRP, tempo de criação assim como de expiração e os IP´s associados.

Figura 44: Visualização do estado da NHRP.

```
MEDNET-RT#show ip nhrp detail
172.0.0.2/32 via 172.0.0.2, Tunnel100 created 01:44:07, expire 01:34:09
  Type: dynamic, Flags: unique registered
  NBMA address: 23.0.0.1
```

Fonte: Dados da pesquisa

O camando ***show tunnel endpoint***, mostra a visibilidade do tipo de túnel assim como os IP´s dos destinos quer públicos assim como o privado nas interfaces.

Figura 45: Visualização do e os IP´s dos destinos.

```
MEDNET-RT#show tunnel endpoint
 Tunnel100 running in multi-GRE/IP mode

 Endpoint transport 23.0.0.1 Refcount 2 Base 0x660302C0
   overlay 172.0.0.2 Refcount 2 Parent 0x660302C0
```

Fonte: Dados da pesquisa

O comando ***show crypto isakmp sa*** visualiza-nos o estado do isakmp.

Figura 46: Visualização do estado da isakmp.

```
MEDNET-RT#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status
12.0.0.1        23.0.0.1        QM_IDLE           1001    0 ACTIVE

IPv6 Crypto ISAKMP SA
```

Fonte: Dados da pesquisa

O ***show crypto ipsec sa*** visualiza interface na qual está configurado o crypto map a identificação local assim como a identificação remota e os IP´s correspondentes da fonte e destino.

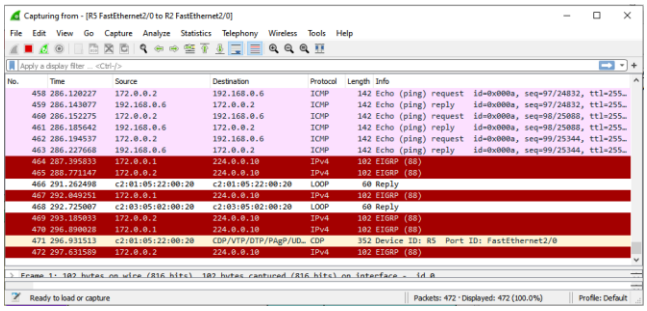
Figura 47: Visualização do estado da IPSEC.

```
MEDNET-RT#show crypto ipsec sa

interface: Tunnel100
    Crypto map tag: Tunnel100-head-0, local addr 12.0.0.1

  protected vrf: (none)
  local  ident (addr/mask/prot/port): (12.0.0.1/255.255.255.255/47/0)
  remote ident (addr/mask/prot/port): (23.0.0.1/255.255.255.255/47/0)
  current_peer 23.0.0.1 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 1413, #pkts encrypt: 1413, #pkts digest: 1413
   #pkts decaps: 1412, #pkts decrypt: 1412, #pkts verify: 1412
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 0, #recv errors 0

    local crypto endpt.: 12.0.0.1, remote crypto endpt.: 23.0.0.1
    path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet1/0
    current outbound spi: 0x8F698486(2406057142)

    inbound esp sas:
     spi: 0xC0476313(3225903891)
       transform: esp-3des esp-md5-hmac ,
       in use settings ={Tunnel, }
       conn id: 153, flow_id: SW:153, crypto map: Tunnel100-head-0
       sa timing: remaining key lifetime (k/sec): (4535022/65)
       IV size: 8 bytes
       replay detection support: Y
       Status: ACTIVE

    inbound ah sas:

    inbound pcp sas:

    outbound esp sas:
     spi: 0x8F698486(2406057142)
       transform: esp-3des esp-md5-hmac ,
       in use settings ={Tunnel, }
       conn id: 154, flow_id: SW:154, crypto map: Tunnel100-head-0
       sa timing: remaining key lifetime (k/sec): (4535022/65)
       IV size: 8 bytes
```

Fonte: Dados da pesquisa

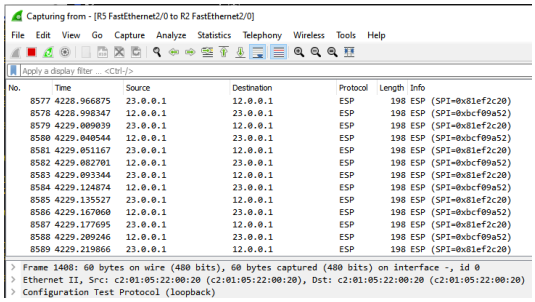
As figuras abaixo mostram o mesmo teste de ping feito, sem e com o IPSec habilitado na interface túnel e com a informação devidamente encriptada e sem acesso aos protocolos usados na nossa rede.

Figura 48: Visualização dos pacotes sem o IPSec habilitado.



Fonte: Dados da pesquisa

Figura 49: Visualização dos pacotes encriptados

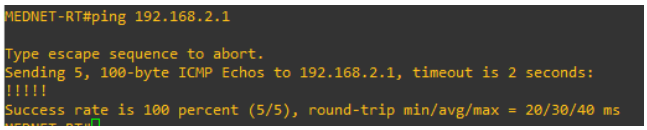


Fonte: Dados da pesquisa

b) Teste de conectividade

Como apresentado nas figuras acima, pode-se verificar e confirmar o sucesso na operação das configurações, e a seguir os resultados da conectividade e dos serviços configurados.

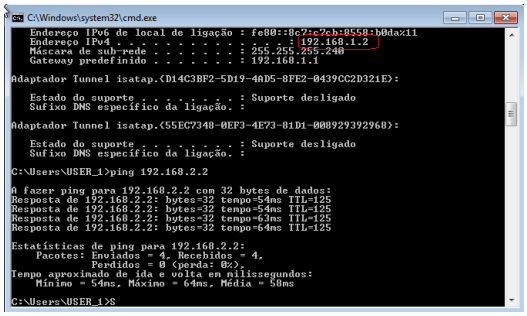
Figura 50: Teste de conectividade.



Fonte: Dados da pesquisa

O teste realizou-se no roteador MEDNET fez-se ping para o roteadores da filial, como é possível observar na figura acima com o endereço 192.168.2.1 um endereço da MEDNET-Filial na VLAN da gerencia.

Figura 51: Teste de conectividade entre dispositivos finais.



Fonte: Dados da pesquisa

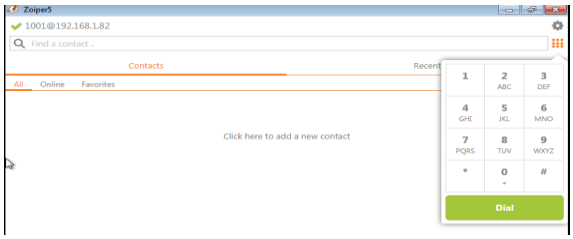
O teste de conectividade entre dispositivos finais, fez-se no PC no hub, ou seja, MEDMET com o endereço 192.168.1.2 e realizou-se um ping para um PC na rede da MEDNET-Filial com o endereço 192.168.2.2.

c) Teste dos serviços

Serviço VoIP

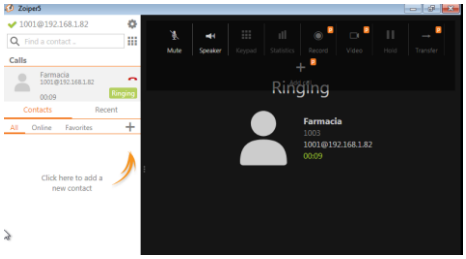
Com as configurações bem definidas, fez-se uma chamada para confirmar a operabilidade do serviço configurado, fez-se uma ligação a partir da MEDNET para MEDNET-Filial, como pode-se observar nas figuras abaixo.

Figura 52: Discagem da extensão desejada.



Fonte: Dados da pesquisa

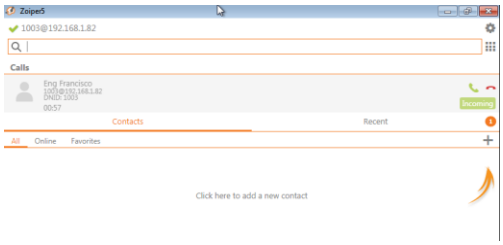
Figura 53: Efectuando a chamada da extensão desejada



Fonte: Dados da pesquisa

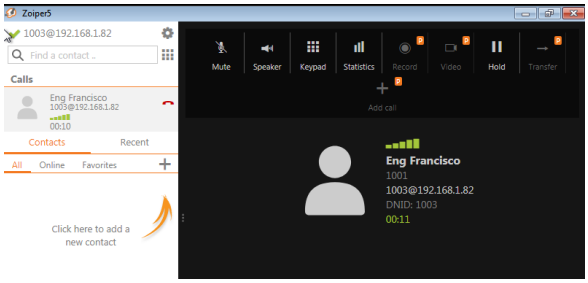
Com a extensão devidamente inserida, faz-se a chamada pressionando em *Dial,* e em seguida a chamada é realizada.

Figura 54: Recepção da chamada



Fonte: Dados da pesquisa

Figura 55: Conversação em curso



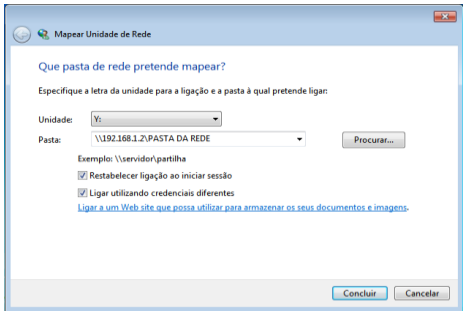
Fonte: Dados da pesquisa

d) Teste de Transferência de Ficheiro via pasta da rede

Propósito: Compartilhar ficheiros entre a sede e a filial.

Procedimento: Efetuou-se a transferência de ficheiros de a partir da pasta de rede criada na sede MEDNET e a MEDNET-Filial acedeu via mapeamento e pode ter acesso e o mesmo partilhar as informações.

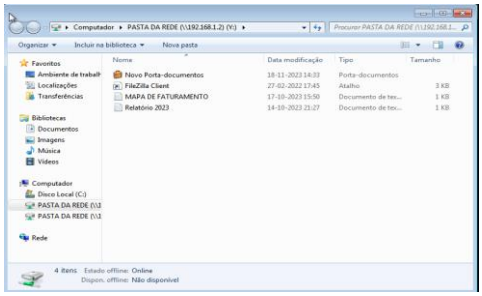
Figura 56: Mapeamento da pasta da rede.



Fonte: Dados da pesquisa

Resultados obtidos: Foi possivel efectuar a transferência de ficheiros entre na sede MEDNET e a MEDNET-Filial.

Figura 57: Acesso a pasta da rede.



Fonte: Dados da pesquisa

CONSIDERAÇÕES FINAIS

As VPN´s têm dado um grande contributo para as organizações, que tenham filiais em pontos geograficamente diferentes.

A tecnologia DMVPN que permitiu o estabelecimento da comunicação entre central e filial e vice-versa, usando o mesmo provedor ou provedores distintos sem o seu aprovisionamento e como mecanismo de proteção nos túneis foi usado o IPsec.

Podemos também concluir que houve uma redução significativa a nível de custo, pelo uso de transmissão por micro-ondas, pois esse tipo de sistema é bastante utilizado para conectar redes de uma mesma organização, pois é mais barato que fazer a mesma ligação usando cabos ou alugando linhas de transmissão privadas. Fez-se o uso da rede pública, mas com recurso da tecnologia DMVPN, Dynamic Multipoint Virtual Private Network, permitindo assim o uso de tuneis dinâmicos multiponto para a transação e criptografia de dados, o que é mais simples e mais barato de ser implementado.

Todos os objetivos listados neste trabalho foram obedecidos e alcançados, conforme aborda o terceiro capítulo. Nisso conclui-se que a tecnologia escolhida para a resolução do problema apresentado foi eficaz para os objetivos que pretendiam alcançar.

Na verdade, conforme se demonstrou através da simulação, é possível estabelecer comunicação entre a MEDNET e as MEDNET-FILIAL e as transações são feitas de forma segura através do uso do IPSec nas interfaces túneis. Os serviços e recursos presentes em cada local são partilhados e acessados a partir de qualquer ponto na rede.

Referências bibliográficas

Azure M. (2019). Abordagem moderna e completa de redes. (4ªed.) Dijon.

Balde (2007). Sistema de Gerenciamento de redes. (2ªed.) Town Hood.

Bhsharma (2007). Sistemas de Controle e Gerenciamento de redes (5ªed). São Paulo: Atlas.

Brandino (2015). Fundamentos de rede. (3edª). São paulo.

Catramby (2006). Instalação de rede (5ªed). Bookman, Porto Alegre.

Duarte (2006). Instrumentos de redes e seu uso (4ªedª). Londres.

I.Backup (19997). *Estudo de redes e sua aplicação* (Vol. 6 edition). IGI Global.

Bertaglia (2016). Logística e Gerenciamento da cadeia de abastecimento. (3ed) São Paulo.

Benjamim (2015). *Engenharia de Software e seus recusos (Vol. 3 Edition). Brasport.*

Fernando Boaventura (1997). Business management and sales. (4edª). River.

Guller (2012). Desenvolvimento de redes (4ªedª). Londres.

Kossui (2008). Forecasting for the ordering and stock-holding of consumable spare parts. (2edª). Londres

Leskiw (2016). Fundamentos do estudo de redes e suas tipologias. (6.ed). Jacarte.

M.Leonardi (2012). Gestão de redes (2ªed). São Paulo.

M.D. Nascimente (2009). Estudo de redes e serviço em Computação em Nuvens. (4ªedª). Cuiabá.

N. Kocharians (2005). Gestão de Estoques: Ação e monitoramento na cadeia de logística integrada. (4ªedª). Rio de Janeiro.

T. Boyles (2004). Sistemas de informação de apoio à gestão. (4ªedª). Green Hood.

Pardal (2017). Métodos e Técnicas de Investigação Social. (1ªedª). Porto:Areal.

GIL (2009). Elaborar Projectos de Pesquisa (3ªed). São Paulo: Atlas.

Xoxo (2006). Modelagem de Sistemas de Informação. (6ªedª). Crespo.

Korth (2001) Sistemas de comunicação (2ª Edição) Daily

Rudio (2013) Introdução ao projecto de pesquisa científica. (9ªedª). Atlas

Reis, Rudio (2013) Introdução ao projecto de pesquisa científica. (6ªedª). Rio Grande

Cortês (2008). *Gestao Compartilhada (3ªEdition)*. Rio grande.

Dantas, M. A. (2005). Políticas de gestão de estoques. (3edª). Rio de Janeiro.

Davenport (2008). Forecasting for the ordering and stock-holding of consumable spare parts. (4edª). Londres.

Ercolin (2012). Gestão de estoques na cadeia de logística integrada (2ªed). São Paulo.

Houaiss (2009). Stock management and marketin (2ªedª). Boston.

Marimoto (2007). *Engenharia de Software - Uma Abordagem Profissional*. (4ªed). Bookman, Porto.

Magela (2006)

Mattos (2005). *Desenvolvimento de Programas Concorrentes Orientados a Objetos: Uma Abordagem Progressiva.* (2ªed). São Paulo.

Mueller (2004) Gestão de vendas (6edª). Políticas de gestão de estoques. (6 edª).

Caxias do sul.

Pardal & Correia (1995). Um estudo sobre o banco de dados como serviço em Computação em Nuvens. . (4ªedª). Cuiabá.

Ranito, & Gouveia. (2004). Sistemas de informação de apoio à gestão. (4ªedª). Porto.

Reis (2010). *Guia Prático de Engenharia de Software.* (3ªed). Aveiro.

Sommerville, I. (2003). *Engenharia de Software* (Vol. 6a Edição). Adisson Wesley.

Sommerville, I. (2005). *Engenharia de Software e Sistemas de Informação (Vol. 3 Edition). Brasport.*

Schwartz, J. (2003). *Engenharia de Software*(4ªedª). Brasport.

Silva (2005). Gestão de Estoques: Ação e monitoramento na cadeia de logística integrada. (4ªedª). Rio de Janeiro.

Sharp & Mcdermott (2008). Engenharia de Requisitos (4ªedª). Londres.

ANEXOS

INSTITUTO SUPERIOR POLITÉCNICO PRIVADO DA CATEPA

(Aprovado por decreto nº 132/17 de 19 de Junho)

DEPARTAMENTO DE INVESTIGAÇÃO CIENTÍFICA

A

DIRECÇÃO DO RESTAURANTE E BAR MEDNET

N/Refª 110/GDGAAC/202

Assunto: **Solicitação de autorização para pesquisa**

O Instituto Superior Politécnico Privado da Catepa (ISCAT) é uma instituição de Ensino Superior Privado, criada através do Decreto Presidencial nº 132/17 de 19 de Junho.

Estando em curso o processo de elaboração dos trabalhos do fim de curso, com objectivo de possibilitar o estudante finalista à realização deste, a direcção do ISCAT, vem por este meio solicitar a vossa colaboração no sentido de autorizar que o nosso estudante **Mendes Domingos Francisco,** matriculado no curso de Engenharia Informática, desenvolva a sua pesquisa na vossa instituição, sob orientação do Professor Buco António A. Golombe.

O estudante pretende realizar um trabalho de campo, com o tema: **"IMPLEMENTAÇÃO DE UMA REDE LANPARA LIGAÇÃO REMTA DOS SERVIÇOS DE PRODUÇÃO COM OS SERVIÇOS DE MONITORAMENTO E REABASTECIMENTO, NO BAR MEDNET-MALANJE" .** A pesquisa exigirá aplicação do questionário e entrevistas aos Funcionários, bem como informações ligadas à pesquisa, que serão fornecidas pelos responsáveis da instituição, ou da área dos Recursos Humanos.

Solicitamos a permissão para que sejam aplicados os questionários e as entrevistas, para posterior análise e interpretação dos resultados. Garantimos que a participação de todos os sujeitos terá carácter voluntária e os dados servirão exclusivamente para a pesquisa mencionada. As informações serão tratadas de forma sigilosa e a identidade dos participantes será preservada.

Informamos que depois da conclusão da pesquisa, a instituição receberá uma cópia física, dos resultados desta investigação.

Agradecemos pela vossa colaboração e reiteramos as cordiais saudações.

Malanje, aos 19 de Outubro de 2023.

Vice - Presidente para Área de Investigação Científica e Pós Graduação

José Domingos Fazenda, PhD

APÊNDICES

Apêndice 1: Imagem frontal da Empresa Mednet-Malanje

Fonte: Dados da pesquisa

Apêndice 2: Roteiro de entrevista dirigido aos funcionários

GUIÃO DE ENTREVISTA DIRIGIDO AOS FUNCIONÁRIOS

Estimado

A presente entrevista tem como objectivo, recolher informações sobre a implementação de uma rede lan na empresa Mednet-Malanje.

A sua resposta ajudará a desenvolver o trabalho de fim de curso na especialidade de Engenharia Informática.

A entrevista é confidencial pelo que, desde já, agradecemos a sua disponibilidade em responder as questões aqui expostas:

A – Identificação pessoal

Sexo: F ☐ M Cargo ☐_____ Estado civil_____ **Idade:** 20 – 25 anos (____); 26 – 30 anos (____); 31 – 35 (____); 36 – 40 (____); 41 – 45 (___); Maior de 45 (____).

B – Formação Acadêmica

Técnico médio	
Bacharel	
Licenciado	
Mestre	

C – Questões

1- Como tem sido a comunicação comercial nesta empresa?
2- Qual é a tua opinião sobre a relação, funcionários e clientes?
3- A tua atuação como funcionário da empresa, tem influenciado para o crescimento da mesma?
4- Quais têm sido as principais dificuldades no processo de atendimento?
5- Quantos funcionário tem a empresa?
6- Quantos anos a empresa tem?
7- O gerente trabalha aqui desde a abertura da empresa?
8- Como é feito o reabastecimento dos produtos?
9- Como é feito a gestão dos produtos?
10- De que forma é feito os relatórios das vendas?
11- Como é feita a localização dos produtos?
12- Com que frequência é feita a atualização do estoque na empresa?