



**UNIVERSIDADE EDUARDO MONDLANE
FACULDADE DE ENGENHARIA**

**DEPARTAMENTO DE ENGENHARIA ELECTROTÉCNICA
CURSO DE ENGENHARIA ELECTRÓNICA**

**Projecto de Rede de Dados Para o
Melhoramento da Rede do Conselho
Municipal da Cidade da Matola (CMCM)**

Relatório do Estágio Profissional

César Tomás Ferroi

**Supervisor: Eng^a Irzelina Gune
(UEM, Faculdade de Engenharia, Departamento de Engenharia Electrotécnica)**

Maputo, Julho 2025



**UNIVERSIDADE EDUARDO MONDLANE
FACULDADE DE ENGENHARIA**

**DEPARTAMENTO DE ENGENHARIA ELECTROTÉCNICA
CURSO DE ENGENHARIA ELECTRÓNICA**

**Projecto de Rede de Dados Para o Melhoramento da
Rede do Conselho Municipal da Cidade da Matola
(CMCM)**

Relatório do Estágio Profissional

César Tomás Ferroi

**Supervisor: Eng^a Irzelina Gune
(UEM, Faculdade de Engenharia, Departamento de Engenharia Electrotécnica)**

Maputo, Julho 2025

CÉSAR TOMÁS FERROI

Projecto de Rede de Dados Para o Melhoramento da Rede do Conselho Municipal da Cidade da Matola (CMCM)

Trabalho apresentado ao Departamento de Engenharia Eletrotécnica da Faculdade de Engenharia da Universidade Eduardo Mondlane, na cadeira do IX semestre Estágio Profissional, como requisito parcial a aprovação.

Supervisor: Eng^a Irzelina Gune
(UEM, Faculdade de Engenharia, Departamento de Engenharia Electrotécnica)

Maputo, Julho 2025

TERMO DE ENTREGA DO RELATÓRIO DO EP



UNIVERSIDADE EDUARDO MONDLANE

FACULDADE DE ENGENHARIA

DEPARTAMENTO DE ENGENHARIA ELECTROTÉCNICA

TERMO DE ENTREGA DE RELATÓRIO DO RELATÓRIO DO ESTÁGIO PROFISSIONAL

Declaro que o estudante César Tomás Ferroi

entregou no dia ____/____/20 ____ as ____ cópias do relatório do seu Relatório do Estágio Profissional com a referência: _____

intitulado: Projecto de Rede de Dados Para o Melhoramento da Rede do Conselho Municipal da Cidade da Matola (CMCM)

Maputo, _____ de _____ de 20_____

O Chefe de Secretaria

DECLARAÇÃO DE HONRA

Declaro sobre palavra de honra que o trabalho apresentado neste relatório é original e foi por mim desenvolvido com base nos meus conhecimentos e com a ajuda dos recursos que ao longo do mesmo faço criteriosa referência.

EPÍGRAFE

*“O principal objectivo da educação é criar pessoas capazes de
fazer coisas novas e não simplesmente repetir o que outras
gerações fizeram.”*

Jean Piaget

DEDICATÓRIA

Este trabalho é dedicado à minha família. Meus pais Helena Nhabinde e Francisco Tchauque. Luísa Mulima, minha esposa, você é minha luz, minha parceira e minha melhor amiga, aquela que me dá forças para enxergar mais longe e sempre me incentiva a alcançar meus objetivos. Tyler Ferroi, meu filho, vejo em você uma grande promessa e quero sempre lhe dar o melhor.

AGRADECIMENTOS

Agradeço primeiramente a Deus, pelo dom da vida.

Agradeço à minha mãe por toda a paciência e carinho com que me demonstrou, por me ensinar os valores éticos e morais com os quais fui criado e por ser meu apoio emocional e espiritual em todas as etapas da minha vida até hoje.

Ao meu pai por todos os ensinamentos e conselhos que me deu, por toda essa motivação para ser melhor a cada dia e nunca deixar de me preparar tanto academicamente assim como profissionalmente para ter um futuro melhor.

À minha esposa Luísa, por me apoiar incondicionalmente nestes anos, e crescermos dia após dia juntos em todos os sentidos com muitos objetivos em comum, como por exemplo continuar a formar-me académicamente de forma a contribuir positivamente para a sociedade.

A supervisora deste relatório de estágio, a engenheira Irzelina Gune, que mesmo no meio de tantas actividades e compromissos, mostrou-se apta a ajudar incansavelmente, por me orientar detalhadamente para a compilação do presente trabalho. Pela confiança, paciência e dedicação acima de tudo.

Ao meu Co-supervisor dr. Bruno Cuco, agradeço imensamente pela paciência e profissionalismo.

A todos os meus colegas da classe, que contribuíram directa ou indirectamente na minha formação, meu muito obrigado.

E por fim, agradeço à comunidade académica da Faculdade de Engenharia da Universidade Eduardo Mondlane.

RESUMO

Projecto de Rede de Dados Para o Melhoramento da Rede do Conselho Municipal da Cidade da Matola (CMCM)

Este relatório é resultado do Estágio Profissional que foi realizado no Conselho Municipal da Cidade da Matola (CMCM) e tem como tema, Projecto de Melhoramento da Rede de dados do Conselho Municipal da Cidade da Matola. Tem como objectivos específicos apresentar o cenário actual da infraestrutura de rede de dados do Conselho Municipal da Cidade da Matola, identificar problemas e propor possíveis soluções de melhoria do desempenho da rede de dados. Para que se alcançasse os objectivos, a metodologia usada para a elaboração deste trabalho baseou-se numa pesquisa quantitativa e qualitativa, onde consistiu no levantamento de conhecimento através do material bibliográfico e de estudo do caso, na qual foi possível perceber que a segmentação e uso de dispositivos de segurança da rede são indispensáveis para um bom desempenho de rede. Segmentar a rede usando VLAN's permite o administrador separar a rede em redes menores, melhorando a segurança, desempenho e principalmente diminuindo o domínio de *broadcast*. Foi feita a segmentação da rede simulada na ferramenta **Cisco Packet Tracer**, a rede foi dividida em 20 sectores, distribuídos da seguinte maneira: 10 (dez) Vereações, 1 (um) para Administração e Recursos Humanos, 1 (um) para o Gabinete do Presidente, 1 (um) Biblioteca, 1 (um) Balcão Único, 1 (um) para uso no Museu e Auditório Municipal, 1 (um) para Sala Magna, 1 (um) para Linha Verde, 1 (um) para Pontos Públicos, 1 (um) Secretaria Geral e Arquivo e o último reserva para possível expansão que totalizou 20 VLANs. As VLANs são configuradas em 21 *switches*, sendo um *switch* de núcleo e os outros *switches* de distribuição.

Palavras Chaves: Redes de Computadores, Conselho Municipal da Cidade da Matola, *Broadcast*, VLAN, *Firewall*

ABSTRACT

Projecto de Rede de Dados Para o Melhoramento da Rede do Conselho Municipal da Cidade da Matola (CMCM)

This report is the result of the Professional Internship that was carried out at the Municipal Council of the City of Matola (CMCM) and has as its theme, Data Network Project for the Improvement of the Network of the Municipal Council of the City of Matola (CMCM). Its specific objectives are to present the current scenario of the data network infrastructure of the Municipal Council of the City of Matola (CMCM), identify mechanisms for improving the performance of the data network and propose mechanisms for improving the network. In order to achieve the objectives, the methodology used to prepare this work was based on quantitative and qualitative research, which consisted of a survey of knowledge through bibliographic material and case studies, in which it was possible to perceive that segmentation and use of network security devices are essential for good network performance. Segmenting the network using VLANs allows the administrator to separate the network into smaller networks, improving security, performance and mainly reducing the broadcast domain. The simulated network was segmented using the **Cisco Packet Tracer** tool, and divided into 20 sectors, distributed as follows: 10 (ten) City Councils, 1 (one) for Administration and Human Resources, 1 (one) for the President's Office, 1 (one) Library, 1 (one) One-Stop Shop, 1 (one) for use in the Museum and Municipal Auditorium, 1 (one) for Sala Magna, 1 (one) for Linha Verde, 1 (one) for Public Points, 1 (one) General Secretariat and Archives, and the last one is a reserve for possible expansion, totaling 20 VLANs. The VLANs are configured in 21 switches, one being a core switch and the others distribution switches.

Keywords: Computer Networks, Cousel Of Matola City, VLAN, Firewall

Índice de Conteúdo

Índice	xx
Lista de Figuras	xxiii
Lista de Acrónimos	xxviii
1 Introdução	1
1.1 Contextualização	1
1.2 Definição do problema	2
1.3 Motivação e Justificativa	3
1.4 Objectivos	3
1.4.1 Objectivo Geral	3
1.4.2 Objectivos Específicos	3
1.5 Metodologia de investigação	4
1.5.1 Classificação da metodologia de investigação	4
1.5.2 Procedimentos e aplicativos usados do trabalho	5
1.6 Estrutura do trabalho	5
2 Pesquisa Bibliográfica e Tecnológica	6
2.1 Conceito de rede de computadores	6
2.2 Comunicação de dados	7
2.3 Arquiteturas do Modelo OSI	8
2.4 TCP/IP	9
2.5 Modelo hierárquico de três camadas da Cisco	10
2.6 Elementos Activos de Uma Rede de Dados	12
2.6.1 Hub	12
2.6.2 Switches	13
2.6.3 <i>Access Point</i> (Ponto de Acesso - PA)	14
	xx

2.6.4	Roteadores (Router)	14
2.6.5	Firewall	15
2.7	Classificação de redes de computadores	19
2.7.1	PAN - Personal Area Network	19
2.7.2	LAN - Local Area Network	20
2.7.3	MAN - Metropolitan Area Network	20
2.7.4	WAN - Wide Area Network	21
2.7.5	Rede Privada Virtual	22
2.8	Factores que proporcionam bom desempenho em uma rede	22
2.8.1	Conceito de Segmentação	23
2.8.2	Redes Virtuais	23
2.8.3	Função Trunk Protocolo VLAN Trunking (VLANs/VTP)	27
2.8.4	Domínio Vlan Trunking Protocol	27
2.8.5	Roteamento entre VLANs	28
2.9	Elementos Passivos de Uma Rede de Dados	28
2.9.1	Calha	28
2.9.2	Tipos de calhas	29
2.9.3	Tubulação	30
2.9.4	Acessórios	31
2.9.5	Cabeamento Estruturado	33
2.9.6	Principais Elementos de um Cabeamento Estruturado	34
2.9.7	Área de trabalho	34
2.9.8	Cabeamento Horizontal	35
2.9.9	Cabeamento Vertical	36
2.9.10	Sala de Telecomunicações (Bastidores)	37
2.10	Regulamentos	38
3	Localização Geográfica, Actividades e Infraestrutura de Rede Actual do CMCM	41
3.1	Conselho Municipal da Cidade da Matola	41
3.2	Actividades	42
3.3	Localização e Contacto	43
3.4	Edifício-sede do Conselho Municipal da Cidade da Matola	43
3.5	Organograma	44
3.6	Missão, Visão e Valores do Conselho Municipal da Cidade da Matola	44

3.6.1	Missão	44
3.6.2	Visão	45
3.6.3	Valores	45
3.7	Sector a Realizar o Estágio	45
3.8	Actividade Realizadas Durante o Estágio	45
3.9	Infraestrutura Actual de Rede	46
4	Implementação e Discussão de Resultados	48
4.1	Avaliação das Propostas de Solução	48
4.2	Segmentação da Rede	48
4.2.1	Endereçamento das VLANs	51
4.2.2	Configurações no Switch	52
4.2.2.1	Comunicação Trunk para o Router	52
4.2.2.2	Atribuição de portas de switch a VLANs	53
4.2.2.3	Configuração de Default-Gateway	54
4.2.3	Configuração do Router	55
4.2.3.1	Criar Sub-interfaces para cada VLAN	56
4.2.4	Orçamento da Proposta	57
4.2.5	Resultados e discussão	57
4.2.5.1	Simulação da Rede	57
4.2.5.2	Verificação das configurações do Router	58
4.2.5.3	Verificação das VLANs	59
4.2.5.4	Verificação do DHCP nos Hosts	60
4.2.5.5	Teste de Conectividade da Rede	61
5	Conclusão e Recomendações	64
5.1	Conclusão	64
5.1.1	Limitação	65
5.2	Recomendações	66
	Referências Bibliográficas	69
	Anexos	69
1	Pedido, Resposta e Ficha de Avaliação do Estágio Profissional.	1

Lista de Figuras

2.1	Comunicação de dados, Fonte: http://www.brasilecola.com/upload/e/img1.jpg	7
2.2	Modelo OSI. Fonte: AUTOR adaptado de Comer, 2007, p. 245	8
2.3	TCP/IP. Fonte: http://gridra.files.wordpress.com/2025/04/tcp-ip3.jpg	10
2.4	Camadas do Modelo Hierárquico para Desenho de Redes. Fonte: http://cisco.netwok.com (2025)	11
2.5	Hub Fonte: http://www.gdhpress.com.br/hmc/leia/cap12.12.html.m4a8777ed.jpg	13
2.6	Switch gerenciável da marca tp-link Fonte: https://www.tp-link.com/en/business-networking/omada-sdn-switch/sg3218xm2/ (2025)	13
2.7	Ponto de Acesso Fonte: https://telemundi.com.br/blog/diferenca-de-roteador-accesspoint-e-repetidor/ (2025)	14
2.8	Exemplo de um Router. Fonte: https://www.belden.com/products/Industrial-Networking-Cybersecurity/Routers (2025)	15
2.9	Representação básica de um firewall. Fonte: https://www.infowester.com/firewall.php	16
2.10	Filtragem de pacotes num firewall. Fonte: https://www.infowester.com/firewall.php (2025)	17
2.11	Proxy. Fonte: https://www.infowester.com/firewall.php	18
2.12	Um <i>firewall</i> Netgear modelo FVS318. Fonte: https://www.infowester.com/firewall.php	19
2.13	Rede de Área Pessoal. Fonte: Imagem da internet (Media, 2025).	20
2.14	Rede Local. Fonte: http://danielcosta.info/pics/lan.gif .	20
2.15	MAN – Metropolitan Area Network. Fonte: Imagem da internet (JSTECH Training, 2023)	21
2.16	WAN - Word Area Networkig. Fonte: (Nertworks Training, 2023)	21
2.17	Exemplo de VLANs como Redes definidas logicamente. Fonte: (CISCO, 2025)	24
2.18	Benefícios de VLANs Fonte: (CISCO PRESS, 2014)	25
2.19	Exemplo de função trunk Fonte: (CISCO PRESS, 2014)	27

2.20 Exemplo de uma Calhas das escadas. Fonte: (INEN, 2009)	29
2.21 Calha Tipo U Metálica Fechada Fonte: (INEN, 2009)	29
2.22 Calha Plástica Fonte: (Elétrico, 2011)	30
2.23 Calha ou Meio-fio do Piso FOnTe: (Elétrico, 2011)	30
2.24 Tubo EMT, IMC. Fonte: (Metalco, 2014)	31
2.25 Tubo Metálico Flexível BX. Fonte: (PANDUIT, 2011)	31
2.26 Acessórios Plásticos. Fonte: (PANDUIT, 2011)	32
2.27 Acessórios Metálicos. Fonte: (PANDUIT, 2011)	33
2.28 Sistema de Cabeamento Estruturado. Fonte: (PANDUIT, 2011)	33
2.29 Área de Trabalho. Fonte: (ARQHYS, 2010)	35
2.30 Fiação Horizontal.Fonte: (PANDUIT, 2011)	35
2.31 Fiação Vertical. Fonte: (PANDUIT, 2011)	37
2.32 Sala de Equipamentos. Fonte: (PANDUIT, SALA DE MÁQUINAS, 2010) . .	38
3.1 Edifício-sede do Conselho Municipal da Cidade da Matola, Fonte: O Autor, Abril de 2025	43
3.2 Logotipo oficial do Conselho Municipal da Cidade da Matola, Fonte: CMCM	43
3.3 Organograma do CMCM. Fonte: CMCM	44
3.4 Um dos Racks da Sala de Telecomunicações. Fonte: O Autor	47
4.1 Rede de Dados Proposta Fonte: Autor	50
4.2 Comunicação Trunk e Encapsulamento dot1q, Fonte: Autor	52
4.3 Atribuição de portas do Switch a VLANs, Fonte: Autor	53
4.4 Configuração de Default-Gateway. Fonte: Autor	55
4.5 Criação das Subinterfaces para cada VLAN	56
4.6 Interface configurada do Router. Fonte: Autor	58
4.7 Interface configurada do Router "IPs". Fonte: Autor	59
4.8 VLANs criadas no Switch. Fonte: Autor	60
4.9 Computador da VF recebendo IP via DHCP. Fonte: Autor	61
4.10 Teste de Conectividade. Fonte: Autor	62
1.1 Pedido do Estágio Profissional, Fonte: Autor	2
1.2 Guia de Apresentação, Fonte: Autor	3
1.3 Ficha de Avaliação do Estágio Profissional, Fonte: Autor	4
2.1 Configuração Básica do Firewall. Fonte: Autor	5

2.2	Atribuição de IPs e definição das Rotas. Fonte: Autor	6
2.3	Configuração de acessos. Fonte: Autor	7
2.4	Roteamento no Firewall Fonte: Autor	8
2.5	Configuração da DMZ Fonte: Autor	9
2.6	Interface configurada do Router. Fonte: Autor	10
2.7	Configuração do modo de acesso e indicação da direção do DHCP para os hosts Fonte: Autor	11
2.8	Configuração do Switch da Vereação de Finanças. Fonte: Autor	12
2.9	Configuração basica do Switch da DMZ. Fonte: Autor	13
2.10	Configuração de de portas Trunk no Switch Fonte: Autor	14
2.11	Configuração de nivel de segurança da Firewal Fonte: Autor	15

Lista de Tabelas

4.1 Tabela de Endereços 51
4.2 Tabela de Orçamento 57

glossariespresortacronym14glo@CMCM@sortCMCMglo@OSI@sortOSIglo@ISO@sortISOglo@

Capítulo 1

Introdução

1.1 Contextualização

Desde os primórdios da humanidade até à sociedade actual sempre existiu a necessidade de comunicação entre seres vivos. A comunicação ao longo dos séculos foi evoluindo e não se processou sempre da mesma forma, nem com os mesmos meios. Com o desenvolvimento da tecnologia e dos conhecimentos em diferentes áreas de investigação foi possível melhorar os sistemas de comunicação em prol do ser humano. O interesse da comunicação não se restringe apenas aos seres humanos, também se estende às máquinas construídas por ele, que embora não possuam a inteligência do ser humano, auxiliam-no em diferentes tarefas. Na pré-história a comunicação entre os seres vivos iniciou-se através de sinais de fumos e gritos, visualizáveis e audíveis a distâncias relativamente curtas. A par do progressivo avanço tecnológico, assinala-se com maior destaque a importância das soluções de engenharia, em Hardware, Software e Redes de Comunicações, etc. Daí resultaram os critérios de missão crítica, desenvolvidos e aplicados principalmente a equipamentos informáticos e de comunicações, tais como: requinte, eficiência, rentabilidade, operacionalidade, capacidade de planeamento, planos de contingência, etc., para garantir a continuidade dos serviços prestados. As redes de computadores constituem-se de um conjunto de dois ou mais computadores interligados com o objetivo de partilhar recursos e trocar informações. Cada vez mais presentes no dia-a-dia das pessoas, as redes de computadores estão espalhadas em diversos locais: grandes e médias empresas, pequenos escritórios ou até mesmo em casa. Um exemplo de uma rede de computadores é a internet. A internet é caracterizada por uma rede de computadores descentralizada que envolve diferentes meios de comunicação, que per-

mite aos seus usuários a troca de informações constante. As redes de computadores, geralmente, são classificadas de acordo com sua disposição geográfica e hierarquia.

1.2 Definição do problema

O Conselho Municipal da Cidade da Matola (CMCM) é uma instituição pública de gestão descentralizada e legalmente constituído, com actividades diversas entre elas o atendimento a pessoas e não só, dentre as actividades prestadas no CMCM, a cobrança de impostos autárquicos é uma das fundamentais. Para alcançar os objetivos traçados pela urbe no que diz respeito a aquisição de receitas para executar as actividades planificadas anualmente, as condições para que sejam atingidas as metas estabelecidas pelo CMCM é crucial que os sistemas, computadores, programas e a rede de dados usados sejam de forma conjunta convenientes. Todas as empresas ou instituições que se dedicam à prestação de serviços devem possuir uma infraestrutura e TIC's que beneficiem ou garantam que as actividades de seus clientes internos (os funcionários) e externos (os munícipes ou todos interessados), funcionem adequadamente, não podendo este tipo de produto ou serviço ser oferecido se não for alavancado por um suporte tecnológico eficiente e de qualidade. A infraestrutura de rede actualmente existente no Conselho Municipal da Cidade da Matola, apresenta diversas deficiências de operação, apresentando uma latência muito alta, falta de catálogos a nível dos bastidores centrais e locais, a desproporcionalidade dos pontos de *switches* e tomadas e ao número de usuários, configurações estáticas e dinâmicas de endereços IP nos computadores, problemas relacionados com a segurança da rede por dispositivos como um *Firewall* entre outros que de alguma forma dificulta a execução de algumas actividades do dia-dia. Problemas derivados da desestruturação da rede:

- a) O não dimensionamento da rede em função de número de usuários;
- b) A não identificação dos ramais que constituem a rede;
- c) A não separação das redes em vereações ou departamentos através de VLAN's, isto é, todos os usuários estão no mesmo domínio de *broadcast*, colocando a rede demasiadamente congestionada e com atrasos significativos.

1.3 Motivação e Justificativa

O desenvolvimento das tecnologias de informação nas atividades sociais e económicas das instituições ou empresas tem levado a um substancial aumento e desenvolvimento das organizações e do número de postos de trabalho. A motivação para a realização deste projecto é de fazer parte do desenvolvimento tecnológico, e de segurança das empresas locais para o caso da CMCM. Para que haja desenvolvimento tecnológico independentemente da área a comunicação deve ser das melhores, portanto há necessidade de reajustar as condições de rede da rede do CMCM aos padrões internacionais de forma a garantir a fluidez da comunicação interna assim como externa, tendo em conta a infraestrutura já existente.

1.4 Objectivos

Esta secção visa apresentar e descrever os objetivos gerais e específicos deste trabalho.

1.4.1 Objectivo Geral

- Melhorar a rede de dados do Conselho Municipal da Cidade da Matola (CMCM)

1.4.2 Objectivos Específicos

- a) Estudar, compreender a arquitectura, funcionamento e segurança de redes locais IP na periferia de internet;
- b) Traçar uma estrutura de rede com dimensão da CMCM incluindo aspectos de segurança;
- c) Especificar os equipamentos necessários a expansão da rede actual p/a nova estrutura proposta;
- d) Realizar uma montagem experimental e/ou simular a nova estrutura, apresentar e discutir as qualidades (e defeitos) observados;
- e) Fazer a proposta final e orçamental do projecto;

1.5 Metodologia de investigação

Em todo tipo de trabalho de pesquisa, a metodologia de trabalho é uma ferramenta que indica o caminho a trilhar para a concepção da pesquisa.

1.5.1 Classificação da metodologia de investigação

a) Quanto à natureza

Cotta, et al (2014) ensinam que quanto à natureza existem dois tipos de pesquisas, nomeadamente a pesquisa científica básica e a pesquisa científica aplicada. O segundo tipo de pesquisa, pesquisa aplicada, que é o caso do presente relatório segundo os mesmos autores tem o intuito de resolver problemas ou necessidades concretas e imediatas. Este trabalho consiste numa pesquisa aplicada, porque tem por intuito resolver um problema específico enfrentado pelos usuários de uma rede de comunicação de dados.

b) Quanto à técnica aplicada

Segundo Alves (2012) esta categoria diz respeito à forma pela qual se obtêm os dados necessários para a realização da pesquisa, onde podemos ter: a pesquisa documental e bibliográfica. De acordo com o mesmo autor citado, as duas formas de pesquisa têm o mesmo objecto de investigação; a diferença entre ambos reside no facto de que a pesquisa documental utiliza fontes primárias: os dados estatísticos e documentos históricos ao passo que a pesquisa bibliográfica usa fontes secundárias os manuais, livros e artigos. Este trabalho enquadra-se nas duas formas de pesquisa citadas pois, para sua elaboração serão consultados manuais, livros, websites, artigos, legislação aplicável ao tema, documentos escritos bem como trabalho no sitio da infraestrutura da rede do CMCM.

c) Quanto à abordagem do tema

Segundo Marconi e Lakatos (2003), nesta categoria encontramos a pesquisa Qualitativa e Quantitativa. A qualitativa consiste em analisar e interpretar aspectos profundos, descrevendo a complexidade do comportamento humano, etc., ao passo que a quantitativa se caracteriza pelo emprego da quantificação tanto nas modalidades de recolha de informações, quanto no tratamento delas por meio de técnicas estatísticas, desde as mais simples como percentual, média, desvio padrão, às mais complexas como coeficiente de correlação, análise de regressão e outros.

1.5.2 Procedimentos e aplicativos usados do trabalho

A concepção do projecto deste trabalho inicia propriamente com o desenho geral da rede, levantamento dos requisitos técnicos e funcionais, levantamento de materiais e componentes para a concepção do projecto, simulação e/ou implementação. Ademais, neste passo, serão seguidos os seguintes procedimentos:

1. Levantamento das necessidades e requisitos para a rede;
2. Especificação e selecção dos componentes necessários para a configuração da rede;
3. Configuração da rede (fase de testes iniciais);
4. Simulação da rede usando Cisco Packet Tracer;

1.6 Estrutura do trabalho

Este trabalho é apresentado em 5 capítulos cuja descrição é apresentada a seguir:

CAPÍTULO 1 - Introdução

O Capítulo 1, orienta-nos a entender o problema, os antecedentes e a justificativa para o desenvolvimento do projeto alavancado nos objetivos a serem alcançados.

CAPÍTULO 2 - Pesquisa Bibliográfica e Tecnológica

O Capítulo 2 nos fornece toda a parte conceitual necessária para a implementação da solução, onde pode-se reforçar os conhecimentos tanto da parte passiva assim como da parte activa do projecto.

CAPÍTULO 3 – Análise da Infraestrutura Existente

O Capítulo 3, consiste na análise da infraestrutura existente e da solução a implementar após análise das vantagens técnicas de cada parte que compõe a solução de infraestrutura tecnológica para o CMCM.

CAPÍTULO 4 – Implementação e Discussão de Resultados

No Capítulo 4 é realizada uma análise econômica como os testes de desempenho da parte activa do projecto, fazer a proposta final e orçamental do projecto, antes da implementação da solução.

CAPÍTULO 5 - Considerações Finais e Recomendações

Por fim, o Capítulo 5 onde respondemos aos objetivos descrevendo as conclusões e recomendações a seguir na implementação da solução.

Capítulo 2

Pesquisa Bibliográfica e Tecnológica

Este capítulo apresenta o referencial teórico indispensável para a elaboração deste trabalho, reunindo conceitos e definições fundamentais para a compreensão do projeto. Além disso, inclui pesquisas bibliográficas relevantes que embasam e contextualizam o tema abordado neste trabalho de conclusão de curso.

2.1 Conceito de rede de computadores

A infraestrutura de redes de computadores sempre foi e ainda é a base para que toda a tecnologia da informação de uma empresa tenha um desempenho adequado. (Cisco Networking, 2025) define rede de computadores como um conjunto de equipamentos de processamento de dados situados em centros distantes uns dos outros, interconectados por telecomunicação e compartilhando seus recursos.

Por sua vez, (Monteiro e Boavida, 2011) definem rede de computadores como dois ou mais computadores interligados, trocando informações e compartilhando recursos físicos e lógicos entre si.

Rede de computadores é um conjunto de computadores interligados entre si de maneira a possibilitar a comunicação local ou remota de dados, incluindo todos os equipamentos electrónicos necessários a interconexão. Esses dispositivos são chamados de nós, estação de trabalho ou também de dispositivos de rede. Bastariam apenas dois computadores ou nós para formarmos uma rede. (Miranda, 2008, p. 77)

Nos três conceitos é notório o entendimento comum de que rede de computadores consiste em 2 (dois) ou mais computadores interligados por uma mídia de transmissão, seja ela através de (cabo: par trançado, coaxial, fibra óptica, etc.) ou (sem cabo: wireless,

rádio frequência) com o objectivo de compartilhar; arquivos, periféricos, aplicações, etc.

Segundo Tanenbaum, uma organização cria redes de computadores para deixar todos os programas, equipamentos e, especialmente dados ao alcance de todas as pessoas na rede, independentemente da localização física do recurso ou do usuário. O principal objectivo das redes de computadores é tornar disponível aos usuários os programas, dados e outros recursos, proporcionando maior confiabilidade e disponibilidade dos recursos.

2.2 Comunicação de dados

Conforme Forouzan (2006), comunicação de dados é a troca de informação entre dois dispositivos através de algum meio de comunicação como, por exemplo, um par de fios.

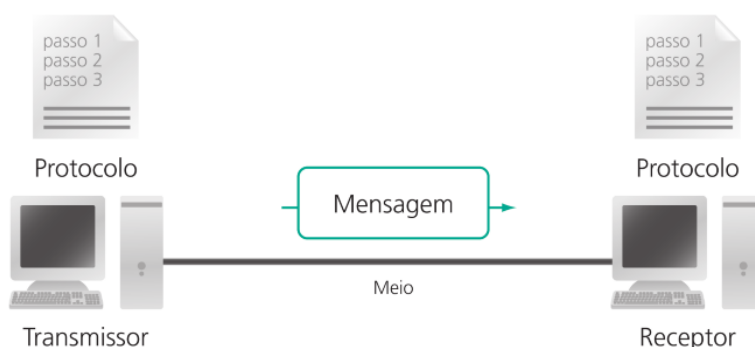


Figura 2.1: Comunicação de dados, Fonte:<http://www.brasilecola.com/upload/e/img1.jpg>

Um sistema básico de comunicação de dados é composto por cinco elementos:

- a) **Mensagem:** é a informação a ser transmitida. Pode ser constituída de texto, números, figuras, áudio e vídeo – ou qualquer combinação desses elementos;
- b) **Transmissor:** é o dispositivo que envia a mensagem de dados. Pode ser um computador, uma estação de trabalho, um telefone, uma câmera de vídeo, entre outros;
- c) **Receptor:** é o dispositivo que recebe a mensagem. Pode ser um computador, uma estação de trabalho, um telefone, uma câmera de vídeo, etc.;
- d) **Meio:** é o caminho físico por onde viaja uma mensagem dirigida ao receptor
- e) **Protocolo:** é um conjunto de regras que governa a comunicação de dados. Ele representa um acordo entre os dispositivos que se comunicam.

2.3 Arquiteturas do Modelo OSI

O modelo de referência Sistema Aberto de Interconexão (OSI), surgiu como resultado de um projecto desenvolvida pela Organização Internacional de Padronização (ISO) durante os anos 70 e 80. Este modelo surge com o objectivo de definir um conjunto de conceitos para o desenvolvimento de protocolos e serviços de comunicação concretos.



Figura 2.2: Modelo OSI. Fonte: AUTOR adaptado de Comer, 2007, p. 245

A camada mais próxima ao usuário final é a sete (7), chamada de camada de aplicação. Já a camada um (1) ou física é a mais próxima do cabeamento ou da infraestrutura de redes. Cada camada possui uma estrutura própria, chamada Protocolo de Datagrama do Utilizador (UDP). Essa divisão em camadas traz diversas vantagens, dentre elas:

- Decompõe as comunicações de rede em partes menores e mais simples.
- Padroniza os componentes de rede.
- Possibilita a comunicação entre diferentes tipos de hardware e de software de rede.
- Evita que as modificações em uma camada afetem as outras. Cada uma das camadas deve fornecer seus serviços exclusivamente à camada imediatamente superior, e conseqüentemente a função de cada camada depende dos serviços da camada imediatamente inferior.

A Camada-1 ou Camada Física do Modelo OSI trata da transmissão transparente de seqüências de bits pelo meio físico, sendo a parte final da comunicação, ou seja, onde a transmissão pelo meio de comunicação realmente acontece.

A Camada-2 (de Enlace) (Camada 2 do modelo OSI) tem a função de preparar os pacotes que vem da camada de rede para que eles possam ser enviados corretamente pelos diferentes tipos de meios físicos. Esse processo é chamado enquadramento (fra-

ming), ou seja, ao pacote que está vindo da camada de rede serão inseridas informações de controle e será gerado um quadro (frame) de camada 2 apropriado para cada meio de transmissão que estiver sendo utilizado.

A camada-3 ou camada de Rede fornece o esquema de endereçamento lógico utilizado para identificar os dispositivos de maneira única dentro das diversas redes existentes e o roteamento.

A camada-4 a camada de transporte desempenha outras importantes funções, tais como a segmentação dos dados (quebra os dados das camadas superiores em segmentos menores), controle de fluxo, transporte confiável de dados não importando o meio físico, etc.

A camada-5 a camada de sessão do Modelo OSI tem a função de disponibilizar acessos remotos, estabelecendo serviços de segurança, verificando a identificação do usuário, sua senha de acesso e suas características, por exemplo, seus perfis de usuário.

A camada-6 a camada de apresentação é responsável pelas transformações ou traduções adequadas nos dados antes do seu envio a camada de sessão, sendo que essas transformações podem ser referentes à compressão de textos, criptografia, conversão de padrões de terminais e arquivos para padrões de rede e vice-versa.

A camada-7 a camada de aplicação é a mais superior e é responsável pela interface com as aplicações dos computadores (hosts), ou seja, a camada de aplicação tem a função de dar acesso à rede aos aplicativos dos usuários que estão instalados nos computadores.

2.4 TCP/IP

Apesar do modelo OSI ser a referência para as redes e toda sua nomenclatura, a arquitetura TCP/IP (*Transmission Control Protocol / Internet Protocol*) é a que foi realmente implementada e está em uso até os dias de hoje tanto nas redes internas (Intranets) como na Internet.

A arquitetura TCP/IP é composta por apenas 4 camadas (formando a pilha da estrutura do protocolo), sendo que na prática, as camadas 5, 6, e 7 do modelo OSI foram mescladas para formar a camada de Aplicação do TCP/IP.

Já as camadas 3 e 4 do modelo OSI são similares às camadas 2 e 3 do TCP/IP, inclusive a camada de transporte do TCP/IP tem o mesmo nome, porém a camada 3 do

modelo OSI (rede) no TCP/IP é chamada de Internet.

Por fim, as camadas 1 e 2 do modelo OSI foram mescladas no TCP/IP para formar a camada de acesso aos meios ou acesso à rede.

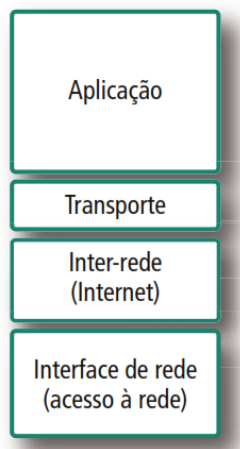


Figura 2.3: TCP/IP. Fonte: <http://gridra.files.wordpress.com/2025/04/tcp-ip3.jpg>

No TCP/IP não costumamos nos referir pelos números das camadas e sim pelos nomes delas, pois quando nos referimos pelo número da camada estamos falando do OSI.

2.5 Modelo hierárquico de três camadas da Cisco

Dividir as redes em camadas permite que cada camada implemente funções específicas, o que simplifica o desenho da rede e, portanto, a implantação e o gerenciamento da rede. A modularidade no desenho de rede permite criar elementos de design que podem ser replicados em toda a rede. A replicação oferece uma maneira fácil de estender a rede, bem como um método de implantação consistente. (Cisco, Lan Network Design, 2025)

O desenho hierárquico permite que alterações operacionais sejam restritas a um sub-grupo da rede, o que facilita a administração e melhora a capacidade de recuperação do sistema. O desenho hierárquico inclui três camadas de acesso, distribuição e núcleo. Na figura 2.3 podemos ver em detalhes:

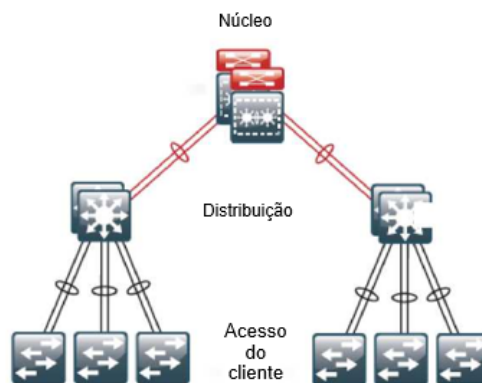


Figura 2.4: Camadas do Modelo Hierárquico para Desenho de Redes.
 Fonte: <http://cisco.netwok.com> (2025)

As camadas e suas funções típicas são:

- **Camada de acesso do cliente**

Controla usuários e acesso a grupos de trabalho ou recursos de rede. Os recursos mais utilizados pelos usuários devem estar localizados localmente, mas o tráfego de serviços remotos é tratado aqui, e entre suas funções estão a continuação do controle de acesso e políticas, criação de domínios de colisão separados (segmentação), conectividade de grupos de trabalho em a camada de distribuição. Nessa camada, ocorre a comutação Ethernet, DDR e roteamento estático (o dinâmico faz parte da camada de distribuição).

- **A camada de distribuição**

É o meio de comunicação entre a camada de acesso e o núcleo. As funções desta camada são fornecer roteamento, filtragem, acesso à rede Rede de Longa Distância (WAN) e determinar quais pacotes devem chegar ao núcleo. Além disso, determina a maneira mais rápida de responder às solicitações da rede. Além disso, são implementadas políticas de rede, roteamento, lista de acesso, filtragem de pacotes, fila, políticas de rede e segurança (traduções Conversão de Endereço de Rede (NAT) e firewalls), redistribuição entre protocolos de roteamento (incluindo rotas estáticas), roteamento entre VLANs e outras funções de grupo de trabalho, transmissão e domínios multicast são definidos.

- **O núcleo**

É literalmente o núcleo da rede, sua única função é comutar o tráfego o mais rápido possível e é responsável por transportar grandes quantidades de tráfego de forma confiável e rápida. Latência e velocidade são factores importantes nesta camada, a sua operação é similar a uma central telefónica tandem. O tráfego que ele carrega é comum para

a maioria dos usuários, mas o tráfego é processado na camada de distribuição que, por sua vez, envia solicitações ao núcleo, se necessário. Em caso de falha, todos os usuários são afetados, portanto, a tolerância a falhas é importante. Além disso, dada a importância da velocidade, ele não executa funções que podem aumentar a latência, como lista de acesso, roteamento entre VLANs, filtragem de pacotes ou acesso a grupos de trabalho. Aumentar o número de dispositivos no núcleo deve ser evitado a todo custo (não adicionar roteadores), se a capacidade do núcleo for insuficiente, devemos considerar aumentos na plataforma actual (upgrades) antes de expansões com novos equipamentos. Devemos projetar o núcleo para alta confiabilidade, redundância e velocidade, com baixa latência. Cada camada oferece uma funcionalidade diferente. Dependendo das características do local de implantação, uma, duas ou todas as três camadas podem ser necessárias.

2.6 Elementos Activos de Uma Rede de Dados

Uma rede permite que todos os membros se conectem entre si. O melhor de uma rede é que tanto os aplicativos quanto as informações podem ser compartilhados e facilmente acessados por qualquer membro. A operação de uma rede consiste em conectar estações de trabalho e periféricos através de dois equipamentos: Switches e Roteadores. Esses dois elementos permitem que os dispositivos conectados se comuniquem entre si e com outras redes. (Cisco, 2012)

2.6.1 Hub

Segundo Torres (2004), os hubs são dispositivos concentradores, responsáveis por centralizar a distribuição dos quadros de dados em redes fisicamente ligadas em estrela. Todo *hub* é um repetidor responsável por replicar, em todas as suas portas, as informações recebidas pelas máquinas da rede.



Figura 2.5: *Hub* Fonte:<http://www.gdhpress.com.br/hmc/leia/cap12.12.html.m4a8777ed.jpg>

2.6.2 Switches

Os switches são usados para conectar vários dispositivos na mesma rede local ou varias redes virtuais (*switch* gerenciável). Um *switch* pode conectar estações de trabalho, impressoras, servidores, etc., criando uma rede de recursos compartilhados, o *switch* actua como um controlador, permitindo que diferentes dispositivos compartilhem informações e se comuniquem entre si.

Existem switches que, dependendo de sua aplicação, podem ter diversos modelos, entre os principais estão: gerenciáveis e não gerenciáveis.

Os administráveis/gerenciáveis podem ser programados pelo administrador, o que proporciona grande flexibilidade, pois o switch pode ser monitorado localmente ou remotamente para dar o controle do tráfego na rede e quem tem acesso a ela.

Os switches não gerenciados funcionam automaticamente e não permitem alterações. É mais usado em redes domésticas.



Figura 2.6: Switch gerenciável da marca tp-link Fonte:[https://www.tp-link.com/en/business-networking/omada-sdn-switch/sg3218xp m2/](https://www.tp-link.com/en/business-networking/omada-sdn-switch/sg3218xp%20m2/) (2025)

2.6.3 Access Point (Ponto de Acesso - PA)

Ponto de Acesso (AP) é um dispositivo de rede usado para estender a cobertura de redes de Internet. O aparelho funciona conectado via cabo a um roteador – ou um *switch* – e distribui sinal Wi-Fi na outra ponta. Basicamente, o **access point** pode ser compreendido como um tipo de repetidor Wi-fi que usa cabos e não pode ser usado como um substituto a um roteador. Comparado a outros dispositivos que aumentam a cobertura da Internet, os pontos de acesso têm algumas vantagens associadas, principalmente, à velocidade e ao gerenciamento da rede.



Figura 2.7: Ponto de Acesso Fonte: <https://telemundi.com.br/blog/diferenca-de-roteador-accesspoint-e-repetidor/> (2025)

2.6.4 Roteadores (Router)

Roteadores são usados para conectar várias redes, pode-se usar um roteador para conectar computadores à internet. O roteador atuará como um “despachante”, selecionando a melhor rota para a informação trafegar para que seja recebida rapidamente. (Cisco, 2012)

Os roteadores analisam os dados a serem enviados pela rede, empacotam-nos de maneira diferente e os enviam para outra rede. Eles conectam a rede local de uma empresa, escritório, instituição ao mundo exterior, protegem as informações contra ameaças de segurança e podem até decidir quais estações de trabalho têm prioridade sobre outras.

Switches e roteadores são os blocos de construção de todas as comunicações, de dados a voz e vídeo a acesso sem fio. Roteadores e *switches* podem fornecer acesso a aplicativos avançados e ativar serviços como IP de voz, videoconferência, etc.



Figura 2.8: Exemplo de um Router. Fonte: <https://www.belden.com/products/Industrial-Networking-Cybersecurity/Routers> (2025)

2.6.5 Firewall

Firewall é uma solução de segurança baseada em hardware ou software (mais comum) que, a partir de um conjunto de regras ou instruções, analisa o tráfego de rede para determinar quais operações de transmissão ou recepção de dados podem ser executadas. "Parede de fogo", a tradução literal do nome, já deixa claro que o firewall se enquadra em uma espécie de barreira de defesa. A sua missão, por assim dizer, consiste basicamente em bloquear tráfego de dados indesejado e liberar acessos bem-vindos. (Bellovin, 2015)

A segurança de rede é uma área focada na proteção de redes de computadores contra ameaças virtuais. Seus principais propósitos incluem a prevenção do acesso não autorizado aos recursos de rede, a detecção e interrupção de ataques cibernéticos, bem como as violações de segurança, e assegurar que os usuários autorizados desfrutem de acesso seguro aos recursos de rede necessários. Para a segurança, um dos principais métodos é a implementação de um *firewall* na rede, possibilitando proteger e filtrar recursos da organização.

Firewall é uma tecnologia de segurança de rede, responsável por supervisionar e regular o tráfego de dados que atravessa uma rede. Ao filtrar os pacotes de dados que entram e saem da rede, o *firewall* é capaz de identificar e neutralizar ameaças, como *malware* e ataques de negação de serviço. Além disso, ele facilita a criação de políticas de acesso para limitar o tráfego não autorizado ou indesejado. Os *firewalls* se apresentam em diversos tipos, desde os implementados em software, como aqueles integrados a sistemas operacionais, até os baseados em hardware, que consistem em dispositivos

especializados para essa finalidade. (Tanenbaum, 2011). A figura 2.9 ilustra posicionamento do *firewall* entre rede externa e rede interna, sendo o mais comum e tradicional.

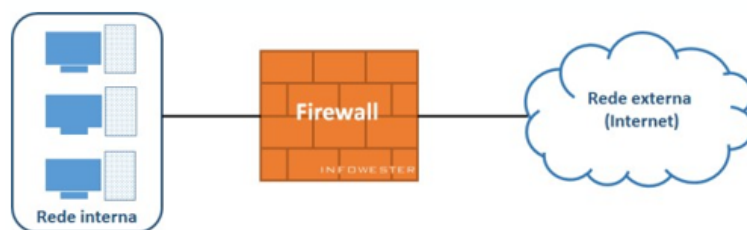


Figura 2.9: Representação básica de um firewall. Fonte: <https://www.infowester.com/firewall.php>

Uma firewall pode ser configurada para bloquear todo e qualquer tráfego no computador ou na rede. O problema é que esta condição isola este computador ou esta rede, então pode-se criar uma regra para que, por exemplo, todo aplicativo aguarde autorização do usuário ou administrador para ter seu acesso liberado.

Esta autorização poderá inclusive ser permanente: uma vez dada, os acessos seguintes serão automaticamente permitidos.

Em um modo mais versátil, uma firewall pode ser configurada para permitir automaticamente o tráfego de determinados tipos de dados, como requisições Protocolo de Transferência de Hipertexto (HTTP) - protocolo usado para acesso a páginas Web), e bloquear outras, como conexões a serviços de e-mail.

O trabalho de uma firewall pode ser realizado de várias formas. O que define uma metodologia ou outra são factores como critérios do desenvolvedor, necessidades específicas do que será protegido, características do sistema operacional que o mantém, estrutura da rede e assim por diante. É por isso que podemos encontrar mais de um tipo de firewall.

As primeiras soluções de firewall surgiram na década de 1980 baseando-se em filtragem de pacotes de dados (**packet filtering**), uma metodologia mais simples e, por isso, mais limitada, embora ofereça um nível de segurança significativo. Para compreender, é importante saber que cada pacote possui um cabeçalho com diversas informações a seu respeito, como endereço IP de origem, endereço IP do destino, tipo de serviço, tamanho, entre outros.

O Firewall então analisa estas informações de acordo com as regras estabelecidas para liberar ou não o pacote (seja para sair ou para entrar na máquina/rede), podendo

também executar alguma tarefa relacionada, como registrar o acesso (ou tentativa de) em um arquivo de log.



Figura 2.10: Filtragem de pacotes num firewall. Fonte: <https://www.infowester.com/firewall.php> (2025)

A transmissão dos dados é feita com base no padrão TCP/IP (*Transmission Control Protocol/Internet Protocol*), que é organizado em camadas, a filtragem normalmente se limita às camadas de rede e de transporte: a primeira é onde ocorre o endereçamento dos equipamentos que fazem parte da rede e processos de roteamento, por exemplo; a segunda é onde estão os protocolos que permitem o tráfego de dados, como o Protocolo de Controle da Transmissão (TCP) e o UDP (User Datagram Protocol).

É possível encontrar dois tipos de firewall de filtragem de pacotes. O primeiro utiliza o que é conhecido como filtros estáticos, enquanto que o segundo é um pouco mais evoluído, utilizando filtros dinâmicos.

Na filtragem estática, os dados são bloqueados ou liberados meramente com base nas regras, não importando a ligação que cada pacote tem com outro. A princípio, esta abordagem não é um problema, mas determinados serviços ou aplicativos podem depender de respostas ou requisições específicas para iniciar e manter a transmissão. É possível então que os filtros contenham regras que permitem o tráfego destes serviços, mas ao mesmo tempo bloqueiem as respostas/requisições necessárias, impedindo a execução da tarefa.

Esta situação é capaz de ocasionar um sério enfraquecimento da segurança, uma vez que um administrador poderia se ver obrigado a criar regras menos rígidas para evitar que os serviços sejam impedidos de trabalhar, aumentando os riscos de o *firewall* não filtrar pacotes que deveriam ser, de fato, bloqueados.

A filtragem dinâmica surgiu para superar as limitações dos filtros estáticos. Nesta categoria, os filtros consideram o contexto em que os pacotes estão inseridos para "criar" regras que se adaptam ao cenário, permitindo que determinados pacotes trafeguem, mas so-

mente quando necessário e durante o período correspondente. Desta forma, as chances de respostas de serviços serem barradas, por exemplo, cai consideravelmente.

A *firewall* de aplicação, também conhecido como proxy de serviços (*proxy services*) ou apenas *proxy* é uma solução de segurança que atua como intermediário entre um computador ou uma rede interna e outra rede, externa - normalmente, a internet. Geralmente instalados em servidores potentes por precisarem lidar com um grande número de solicitações, *firewalls* deste tipo são opções interessantes de segurança porque não permitem a comunicação direta entre origem e destino.

A imagem a seguir ajuda na compreensão do conceito. Percebe-se que em vez de a rede interna se comunicar diretamente com a internet, há um equipamento entre ambos que cria duas conexões: entre a rede e o *proxy*; e entre o *proxy* e a internet.

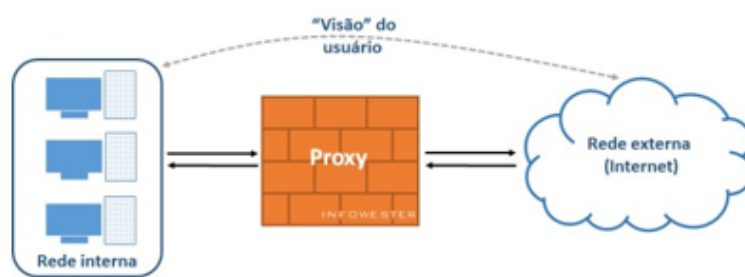


Figura 2.11: Proxy. Fonte: <https://www.infowester.com/firewall.php>

Todo o fluxo de dados necessita passar pelo *proxy*. Desta forma, é possível, por exemplo, estabelecer regras que impeçam o acesso de determinados endereços externos, assim como que proíbam a comunicação entre computadores internos e determinados serviços remotos. Este controle amplo também possibilita o uso do *proxy* para tarefas complementares: o equipamento pode registrar o tráfego de dados em um arquivo de log; conteúdo muito utilizado pode ser guardado em uma espécie de cache (uma página Web muito acessada fica guardada temporariamente no *proxy*, fazendo com que não seja necessário requisitá-la no endereço original a todo instante, por exemplo); determinados recursos podem ser liberados apenas mediante autenticação do usuário; entre outros.

A implementação de um *proxy* não é tarefa fácil, haja visto a enorme quantidade de serviços e protocolos existentes na internet, fazendo com que, dependendo das circunstâncias, este tipo de *firewall* não consiga ou exija muito trabalho de configuração para bloquear ou autorizar determinados acessos.

A vantagem de uma *firewall* de hardware é que o equipamento, por ser desenvolvido especificamente para este fim, é preparado para lidar com grandes volumes de dados e

não está sujeito a vulnerabilidades que eventualmente podem ser encontrados em um servidor convencional (por conta de uma falha em outro software, por exemplo).



Figura 2.12: Um *firewall* Netgear modelo FVS318. Fonte: <https://www.infowester.com/firewall.php>

2.7 Classificação de redes de computadores

As Redes de computadores podem ser classificadas seguindo diversos critérios, entre eles dimensão da Rede (redes pessoais, redes locais, redes metropolitanas), Topologia (estrela, anel, barramento). De acordo com Dantas (2002), uma das características mais utilizadas para a classificação das redes é a sua abrangência geográfica. Assim, é convencional a classificação das redes em locais – PAN (Personal Area Networks), LANs (Local Area Networks), metropolitanas – MANs (Metropolitan Area Networks), VPN (Virtual Private Network) e geograficamente distribuídas – WANs (Wide Area Networks).

A seguir será analisada as redes conforme a sua dimensão. Pode-se classificá-las em cinco classes de rede.

2.7.1 PAN - Personal Area Network

O conceito de Rede de Área Pessoal (PAN), são redes de curta distância, constituída de uma rede de computadores com nós muito próximos uns dos outros. Um exemplo de uma PAN são dois computadores dentro de um ambiente compartilhando a mesma impressora, utilizando as frequências de rádio ou raios infravermelhos para efectuar a troca de informações entre eles.

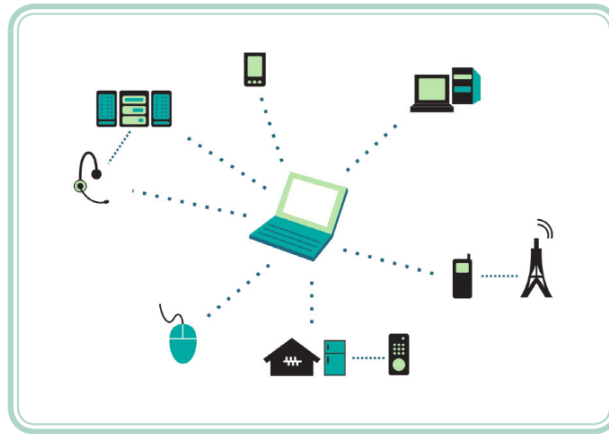


Figura 2.13: Rede de Área Pessoal. Fonte: Imagem da internet (Media, 2025).

2.7.2 LAN - Local Area Network

Área de Rede Local - *Local Area Network* (LAN), geralmente é composta por vários computadores conectados entre si, por meio de dispositivos como placas de redes, switches, entre outros, possibilitando o compartilhamento de recursos e a troca de informações. A limitação geográfica de uma LAN faz com que elas sejam utilizadas em escritórios, empresas, escolas, entre outros locais.

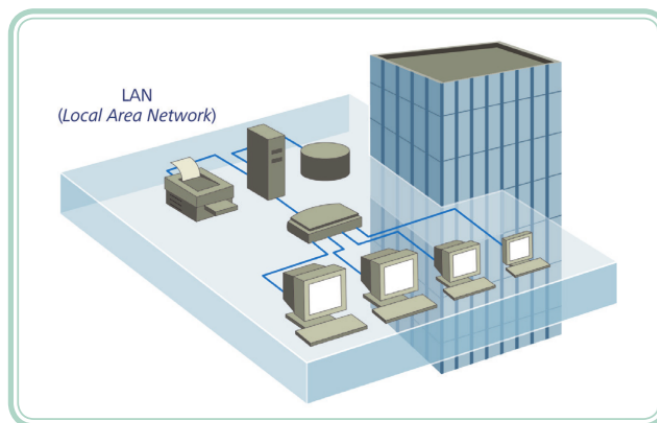


Figura 2.14: Rede Local. Fonte: <http://danielcosta.info/pics/lan.gif>.

2.7.3 MAN - Metropolitan Area Network

A Rede de Área Metropolitana (MAN) é a rede de computadores que corresponde um espaço de grande dimensão como uma cidade, uma região ou um campus. Normalmente uma MAN, conecta várias LANs. As redes ISP (Internet Service Protocol) ou provedor de

serviço de internet, ou seja, um provedor que fornece acesso à internet é um exemplo de uma MAN.

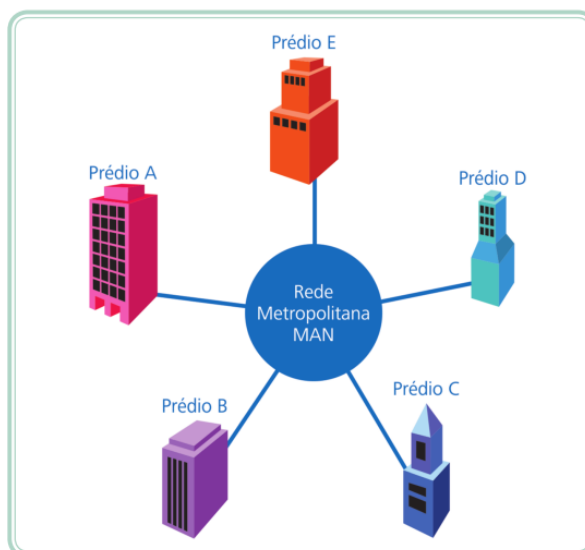


Figura 2.15: MAN – Metropolitan Area Network. Fonte: Imagem da internet (JSTECH Training, 2023)

2.7.4 WAN - Wide Area Network

WAN, são as redes de computadores que abrangem uma grande área geográfica, como um país, um continente. Uma WAN é essencialmente uma rede das redes, sendo que a Internet é a maior WAN do mundo.

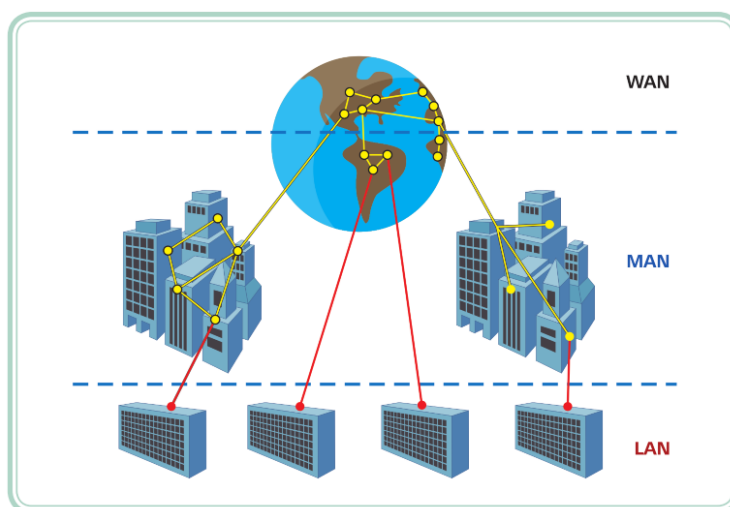


Figura 2.16: WAN - Wide Area Network. Fonte: (Networks Training, 2023)

2.7.5 Rede Privada Virtual

É um método que permite que usuários remotos acessem sua rede de forma segura, com todos os seus serviços dependendo das políticas da empresa sobre seus usuários, aumentando assim a produtividade.

Rede Privada Virtual. (VPN) é uma rede privada construída dentro de uma infraestrutura de rede pública, como a rede mundial de computadores da Internet. As empresas podem usar redes privadas virtuais para conectar com segurança escritórios remotos e usuários por meio de acesso barato à Internet de terceiros, em vez de links WAN dedicados caros ou links dial-up de longa distância.

2.8 Factores que proporcionam bom desempenho em uma rede

Para o bom desempenho de rede existem muitas abordagens, é importante dizer quais aspectos que se relacionam com o desempenho de rede. Para se mensurar o desempenho de uma rede (OPPENHEIMER, 1999) descreve diversos parâmetros de Desempenho de uma Rede, neste trabalho vai se destacar os seguintes:

a) **Disponibilidade:** definido como percentual de tempo durante o qual uma rede está disponível para os usuários.

b) **Capacidade (largura de banda):** capacidade de transporte de dados de um circuito ou uma rede, medida em bits por segundo [bps].

c) **Tempo de resposta:** o intervalo de tempo entre a solicitação de algum serviço de rede e uma resposta ao pedido.

d) **Vazão (Throughput):** quantidade de dados isentos de erros transferidos com sucesso entre dois nós por unidade de tempo, e;

e) **Segura, confiabilidade dos dados e mobilidade:** É importante salientar que para uma rede proporcione um bom desempenho há várias alternativas nas quais, podem se ter em conta esses parâmetros, passa-se a citar:

- Implementação de VLAN (segmentação da rede);
- Sistemas de monitoramento de rede;
- Sistema de monitoramento de Largura de banda;
- Redundância no cabeamento.

2.8.1 Conceito de Segmentação

Quando a rede de uma instituição é grande, contendo muitos computadores (algumas dezenas ou mais), e cobrindo uma área física ampla, costuma-se dividi-la em redes menores. Esse procedimento chama-se segmentação da rede, e o objectivo é reduzir a complexidade de administração de uma rede grande. (Kurose e Ross, 2014)

Essas redes menores, cada uma com sua própria sub-rede, são úteis para separar conjuntos de equipamentos, de acordo com seus usos ou finalidades. Por exemplo, em uma empresa pode haver uma rede para directoria, outra para o grupo do atendimento ao público, e uma terceira para a equipe técnica. Essa divisão torna mais fácil definir diferentes políticas de segurança e usos de recursos da rede.

Assim, dados esses benefícios, segmentar redes é uma prática comum, e pode ser feita de diferentes formas, e nesse trabalho vai-se abordar as redes LANs baseado em virtualização.

2.8.2 Redes Virtuais

Devido ao crescimento em redes de computadores, nem sempre uma determinada infraestrutura de uma rede local consegue suprir a demanda computacional de seus usuários. Se isso acontece, uma reestruturação lógica de redes de computadores faz-se necessária, visando aproveitar os recursos pré-existentes e melhorar as actividades de gestão da rede.

Isso é possível por meio da criação de *Virtual Local Area Network* (VLAN), em outras palavras, a segmentação virtual de redes de computadores, ou seja, a rede física é "dividida" em vários segmentos lógicos.

Uma VLAN é uma rede local que agrupa conjuntos de nodos (máquinas) de maneira lógica. Este agrupamento de vários nodos pode ser de acordo com vários critérios (ex. grupos de utilizadores, por departamentos, tipo de tráfego, etc). (Forouzan, 2006)

Segundo a (Science Direct, 2014), o termo VLAN refere-se à criação de redes locais virtuais em um mesmo dispositivo de rede ou conjunto deles. E também afirmam que as VLANs contribuem para reduzir os domínios de colisão em segmentos de redes Ethernet muito extensos, melhorando assim o seu desempenho.

As VLANs permitem a segmentação das redes físicas, sendo que a comunicação entre nós de diferentes VLANs terá de passar obrigatoriamente por um router ou outro equipamento capaz de realizar encaminhamento (*switch* de camada 3), que será responsável

por encaminhar o tráfego entre redes (VLANs) distintas. Nota-se que é possível criar redes totalmente separadas para diferentes departamentos dentro do mesmo ambiente físico, e aplicando políticas de segurança diferentes para os grupos, utilizando o conceito de VLANs.

A principal característica atribuída ao uso de VLANs é a possibilidade de agrupar estações pertencentes a uma ou mais LANs físicas, de forma a criar um único domínio de *broadcast*, garantindo a comunicação entre estas LANs, mesmo que façam parte de segmentos físicos diferentes. (Forouzan, 2006)

Em uma rede não segmentada, computadores, impressoras e outros dispositivos conectados disseminam uma grande quantidade de pacotes de *broadcast* por diversos motivos, seja por falhas na conexão dos cabos, mau funcionamento de interfaces de rede, ou até mesmo por protocolos e aplicações que geram este tipo de tráfego, podendo causar atraso no tempo de resposta e lentidão na rede local. (de Magalhães Dias Frinhani, 2005). No modelo de VLANs, existe um domínio lógico de difusão por onde os pacotes de *broadcast* ou *multicast* são contidos e não se propagam a outras redes virtuais (de Magalhães Dias Frinhani, 2005). Assim sendo, os pacotes de difusão ficam contidos apenas em sua rede local, reduzindo drasticamente o volume de tráfego na rede.

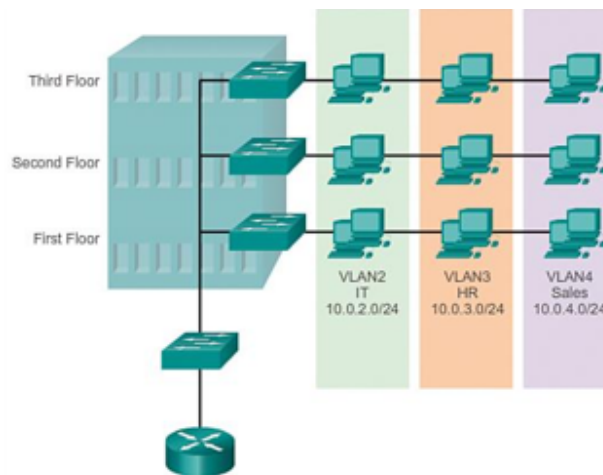


Figura 2.17: Exemplo de VLANs como Redes definidas logicamente. Fonte: (CISCO, 2025)

Como podemos ver na figura 2.15, os nodos que pertencem a mesma VLAN não precisam necessariamente estar no mesmo ambiente físico. Vantagens de uso de VLANs A implementação de redes virtuais proporciona inúmeros benefícios, dentre os quais pode-se citar (CISCO PRESS, 2014):

a) Segurança de dados

As redes locais virtuais limitam o tráfego a domínios específicos proporcionando mais segurança a estes. O tráfego em uma VLAN não interfere a outros membros de outra rede virtual, já que estas não se comunicam sem que haja um dispositivo de rede desempenhando a função de roteador entre elas. Dessa forma, o acesso a servidores que não estejam na mesma VLAN é restrito, criando assim domínios de segurança no acesso a recursos. Os grupos que têm dados sensíveis são separados do resto da rede, diminuindo as hipóteses de violação de informação confidencial. Como mostrado na Figura 2.18, os computadores do corpo docente (Faculty) estão na VLAN 10 e completamente separados do tráfego de dados de estudantes (student) e convidados (Guest).

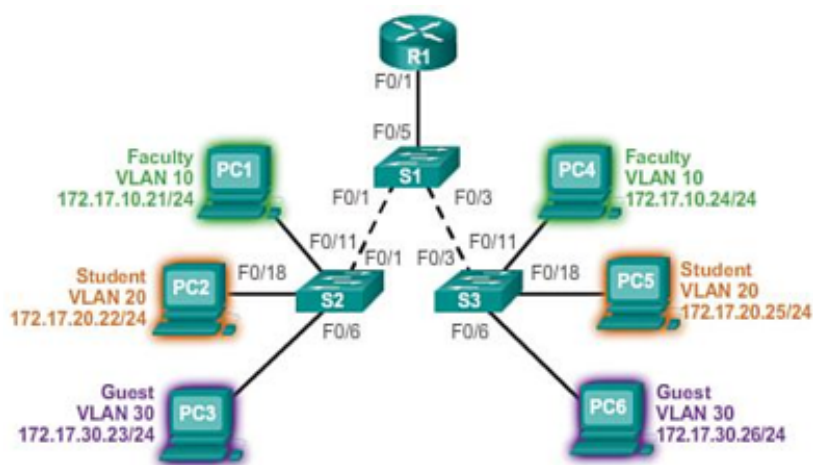


Figura 2.18: Benefícios de VLANs Fonte: (CISCO PRESS, 2014)

b) Redução de custos

Grande parte do custo de uma rede se deve ao facto da inclusão e da movimentação de usuários nela. Cada vez que um usuário se movimenta é necessários um novo cabeamento, um novo endereçamento para estação de trabalho e uma nova configuração de repetidores e roteadores. Já em uma VLAN, a adição e movimentação de usuários podem ser feitas remotamente pelo administrador da rede (da sua própria estação), sem a necessidade de modificações físicas, proporcionando uma alta flexibilidade.

c) Melhor desempenho controle do tráfego broadcast

As VLANs apresentam um desempenho superior às tradicionais redes locais, principalmente devido ao controle do tráfego broadcast.

Tempestades de quadros de broadcast (*broadcast storms*) podem ser causadas por mau funcionamento de placas de interface de rede, conexões de cabos malfeitas e apli-

cações ou protocolos que geram esse tipo de tráfego, entre outros.

d) Segmentação lógica da rede

Dividir uma rede em VLANs reduz o número de dispositivos no domínio de difusão. Como mostrado na Figura 2.18, existem seis computadores nesta rede, mas existem três domínios de difusão: Faculdade, Estudante e Convidado. Cada VLAN pode ser associada a um departamento ou grupo de trabalho, mesmo que seus membros estejam fisicamente distantes. Isso proporciona uma segmentação lógica da rede.

e) Facilidade de gerenciamento

As VLANs facilitam a administração da rede porque os utilizadores com requisitos de rede semelhantes partilham a mesma VLAN. Quando um novo switch é provisionado, todas as políticas e procedimentos já configurados para a VLAN específica são implementados quando as portas são atribuídas. É também fácil para o grupo de IT identificar a função de uma VLAN, dando-lhe um nome apropriado. Na Figura 2.18, para facilitar a identificação, a VLAN 10 foi nomeada "Faculdade", a VLAN 20 foi nomeada "Estudante", e a VLAN 30 "Convidado". (de Magalhães Dias Frinhani, 2005) também aponta algumas vantagens, afirmando que a implementação de VLANs para segmentar uma rede melhora a performance. Como visto anteriormente, os pacotes de broadcast e multicast ficam presos somente na VLAN onde trafegam, evitando congestionamentos. Outra característica é o facto de diminuir o número de estações que compartilham o mesmo canal lógico, reduzindo assim o tempo de acesso. Pode se concluir que o uso de VLANs é benéfico para restringir a comunicação de computadores instalados em sectores críticos como por exemplo financeiro, protegendo assim informações sigilosas da instituição.

A segurança é uma das características mais importantes quando é decidido segmentar a rede em VLANs, já que ela permite que dispositivos localizados em diferentes segmentos físicos, mas em uma mesma VLAN comuniquem-se sem que dispositivos fisicamente próximos tenham acesso (de Magalhães Dias Frinhani, 2005).

Cada VLAN numa rede comutada corresponde a uma rede IP, portanto, a concepção da VLAN deve ter em consideração a implementação de um esquema hierárquico de endereçamento de rede. Um esquema hierárquico de endereçamento de rede significa que os números de rede IP são aplicados a segmentos de rede ou VLANs de uma forma ordenada que leva a rede como um todo em consideração. Os blocos de endereços de rede contíguos são reservados e configurados em dispositivos numa área específica da rede, como se mostra na Figura 2.18.

2.8.3 Função Trunk Protocolo VLAN Trunking (VLANs/VTP)

VLAN Trunking é um padrão definido pelo IEEE 802.1ad e tem como característica a transmissão de pacotes para diferentes VLANs em um mesmo link. A figura 2.19 demonstra um exemplo de trunk, onde as vlans 10,20,30 do switch 2 enviam informações por uma mesma porta ao switch 2 e ao switch 3. As VLANs podem se comunicar entre si por meio da conexão trunking entre os switches através dos links F0/1 e F0/3.

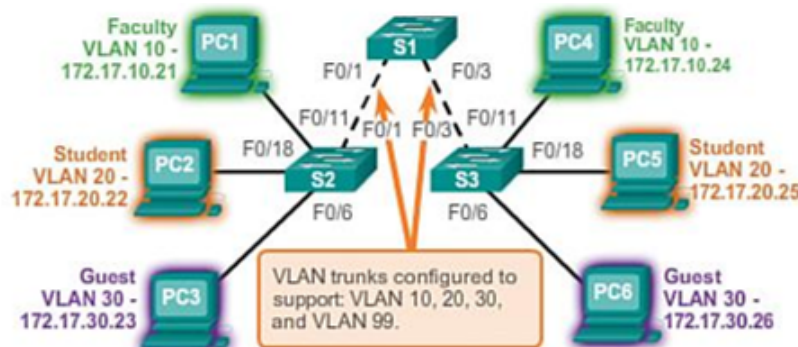


Figura 2.19: Exemplo de função trunk Fonte: (CISCO PRESS, 2014)

Segundo o (Barros, 2009), define VLAN Trunking como um link ponto-a-ponto em uma rede comutada que suporta várias VLANs (link entre os switch S1 – S2 e S1 – S3, como podemos ver na figura 2.18).

A função trunk é utilizada para configurar portas e adicionar VLANs à lista permitida. A capacidade do trunking depende do hardware. Alguns switches ajustam automaticamente as ligações das portas ao trunk. Para que uma porta se ajuste para se tornar uma porta trunk, dependerá da modalidade e do tipo do trunk especificado para essa porta, e para que o trunk seja ajustado a portas rápidas é necessário que as portas estejam no mesmo domínio de VTP (VLAN Trunking Protocol).

2.8.4 Domínio Vlan Trunking Protocol

O protocolo Protocolo de Tronco VLAN (VTP), simplifica a configuração de uma VLAN em uma rede com vários switches garantindo um método mais fácil para a manutenção de uma configuração em toda a rede.

Segundo (CISCO, 2022), este protocolo faz a gestão de VLANs automaticamente, permitindo assim, que o administrador de rede consiga adicionar, remover e alterar a configuração de VLAN em qualquer switch desde que pertençam ao mesmo domínio e

tenham ligação partilhada.

Tal protocolo é utilizado para distribuir e sincronizar informações de identificação das VLANs configuradas em toda a rede. As configurações estabelecidas em um único servidor VTP são propagadas através do enlace trunk para todos os switches conectados na rede.

2.8.5 Roteamento entre VLANs

O roteamento entre VLANs é necessário quando um dispositivo de uma VLAN precisa se comunicar com um dispositivo de outra VLAN. Esse roteamento pode ser feito por meio de um switch de camada 3 ou utilizando um roteador. No exemplo da figura 2.16, o switch tem suas interfaces e cada uma tem um endereço de rede correspondente a cada VLAN. Assim, caso um dispositivo deseje se comunicar com outra VLAN, o pedido de conexão será feito ao gateway que vai rotear o pacote, caso autorizado pelas directivas de acesso. É necessário que seja informado o IP de destino para que o pacote seja correctamente encaminhado.

2.9 Elementos Passivos de Uma Rede de Dados

2.9.1 Calha

As calhas são tubos metálicos ou plásticos que, quando conectados corretamente, conferem ao cabo maior proteção contra interferências eletromagnéticas. Para que os electroductos protejam os cabos de tais perturbações, é essencial uma instalação ideal e uma conexão perfeita em suas extremidades. Existem dois modelos; com divisão quando a fiação é elétrica e de dados e sem divisão quando é um único tipo de cabo. A utilização dos acessórios na instalação é para que os cabos não sofram deformações físicas que acabem causando perdas nas transmissões. Existem em vários tamanhos: 20 x 12 (mm), 32 x 12 (mm), 40 x 25 (mm), 60 x 40 (mm), 100 x 45 (mm), nas cores branco e marfim, de diversos fabricantes. (Elétrico, 2011) A quantidade de cabos a serem utilizados depende do tipo de cabo a ser instalado, ou seja, deve haver uma reserva de 40 porcentos para futuras instalações e pedidos de cabos. (INEN, 2009)

2.9.2 Tipos de calhas

Calhas da escada: Estas bandejas são muito flexíveis, fáceis de instalar e fabricadas em diferentes tamanhos, sendo utilizadas exclusivamente para áreas com tetos falsos, em chapa de aço galvanizado ou revestidas com isolamento plástico. Na figura podemos ver como instalar os cabos na escada.



Figura 2.20: Exemplo de uma Calhas das escadas. Fonte: (INEN, 2009)

Tipo fechado: Bandeja em U com divisória e sem divisória, utilizada com ou sem tampa superior, disponível em diversos tamanhos 200 x 70 (mm), 300 x 70 (mm), etc., para instalações à vista do usuário ou em tecto falso. É usado para instalações eléctricas, de comunicação ou de dados. A utilização de acessórios é muito importante para cumprir as normas de colocação de cabos.



Figura 2.21: Calha Tipo U Metálica Fechada Fonte: (INEN, 2009)

Calhas de plástico: Facilita e resolve todos os problemas de condução e distribuição de cabos, utilizados em paredes, tubos de descarga e painéis, são do tipo vertical e horizontal. Os canais, em toda a sua extensão, são providos de linhas de pré-quebra

dispostas na base para facilitar o corte de um segmento. A figura mostra como uma calha de plástico é estruturada.



Figura 2.22: Calha Plástica Fonte: (Elétrico, 2011)

Canal de salvamento a cabo: Especialmente concebido para proteger e decorar a passagem de telefone, electricidade, sonorização, cabos de computador, etc. para pisos de escritório. Possuem compartimentos que permitem diferenciar os diferentes meios guiados. Na figura a seguir, o meio-fio com três compartimentos:



Figura 2.23: Calha ou Meio-fio do Piso Fonte: (Elétrico, 2011)

2.9.3 Tubulação

O tubo é muito utilizado em instalações do sector industrial, onde deve haver proteção diferenciada nos cabos de comunicação e dados devido ao ruído que o ambiente pode gerar. Existem vários modelos e características dependendo do material, regulamentações, etc., como tubo IMC, EMTs, etc. Existem em vários tamanhos: 2", 1", 3/4", 1/2". Na figura tubo de diferentes dimensões:



Figura 2.24: Tubo EMT, IMC. Fonte: (Metalco, 2014)

Tubo de metal flexível (Bx): Este tipo é fabricado com fita metálica afixada, sem nenhum revestimento, para sua aplicação é recomendado em locais secos onde não fique exposto a corrosão ou danos mecânicos, facilitam a instalação quando há colunas ou curvaturas muito pronunciadas que causem descumprimento de regulamentos de instalação. Existem em vários tamanhos 2", 1", 3/4", 1/2". Os acessórios são chamados de conectores Bx e possuem a mesma medida de diâmetro. Na figura a seguir tubo BX 3/4".



Figura 2.25: Tubo Metálico Flexível BX. Fonte: (PANDUIT, 2011)

2.9.4 Acessórios

São todos aqueles que servem para formar um canal bem estruturado, suas medidas dependem do tipo de calha ou tubulação a ser instalada.

Plásticos

- Ângulo externo
- Ângulo interno
- Ângulo plano

- Derivação -T
- Uniões
- Tampa final
- Caixa de passagem



Figura 2.26: Acessórios Plásticos. Fonte: (PANDUIT, 2011)

Metálico

- Acoplamentos
- Ramo T
- Cotovelo
- Conectores EMT
- Conectores Bx
- Sindicatos
- Ângulos planos



Figura 2.27: Acessórios Metálicos. Fonte: (PANDUIT, 2011)

2.9.5 Cabeamento Estruturado

Um Sistema de Cabeamento Estruturado consiste em uma infraestrutura de meios físicos que permitem a comunicação em uma determinada área. Um Sistema de Cabeamento Estruturado permite a interligação de equipamentos activos, a integração de diversos serviços como Dados, Telefonia, Vídeo, Segurança, etc. (PANDUIT, 2011).

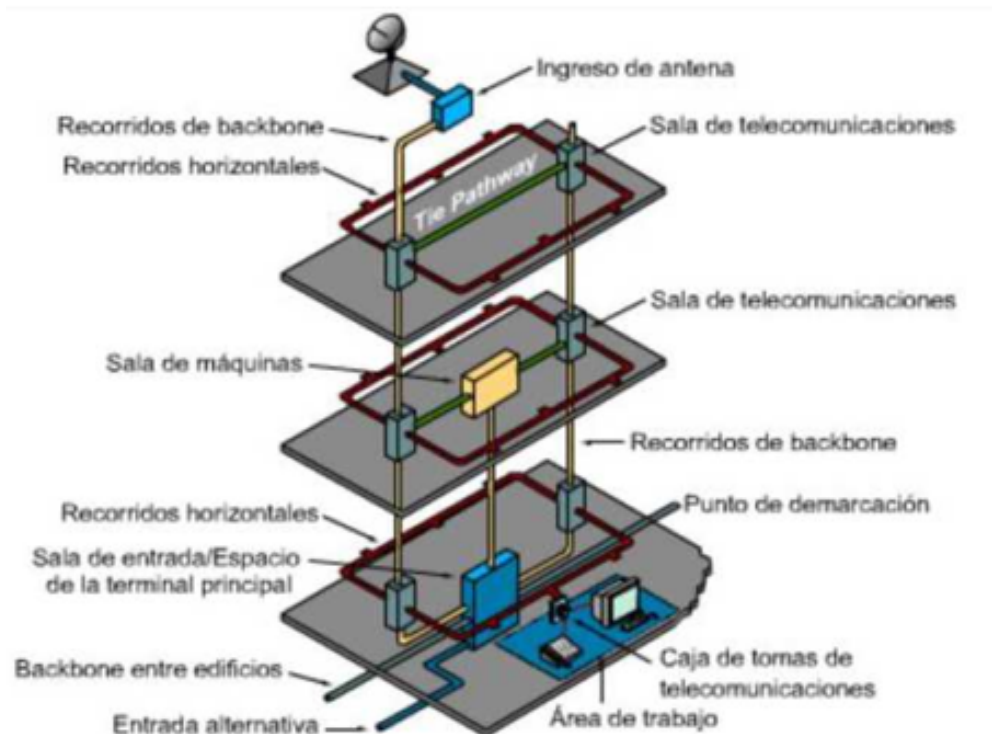


Figura 2.28: Sistema de Cabeamento Estruturado. Fonte: (PANDUIT, 2011)

Em um sistema de cabeamento estruturado, cada área de trabalho é conectada a um

ponto central (Sala de Telecomunicações), através de uma infraestrutura física (Cablagem Horizontal) utilizando uma rede completa, infraestrutura de equipamentos, elementos de conexão, acessórios e cabos. A comunicação por meio guiado ou não guiado entre a sala de telecomunicações e cada nó secundário é chamada de Cabeamento Vertical.

2.9.6 Principais Elementos de um Cabeamento Estruturado

Os Elementos ou subsistemas que compõem um sistema de Cabeamento Estruturado são: (PANDUIT, 2011)

- Área de Trabalho (WA - Work Area)
- Fiação Horizontal (HC - Horizontal Cable)
- Sala de Telecomunicações (TR - Telecommunications Room)
- Cabeamento de Backbone (BC - Backbone Cabling)
- Sala de Equipamentos/Bastidores Centrais (ER - Backbone Cabling)
- Instalação de entrada (EF - Entrance Facility)

2.9.7 Área de trabalho

A área de trabalho estende-se desde a tomada/conector de telecomunicações ou a extremidade do sistema de cabeamento horizontal até o equipamento da estação. O equipamento da estação pode incluir, mas não está limitado a, telefones, terminais de dados e computadores. (ARQHYS, 2010) Os padrões estabelecidos pela TIA/EIA 568-B.1 (SIEMON, 2011) estipulam que cada área de trabalho deve ser cabeada com pelo menos duas tomadas de telecomunicações. Se você for instalar telefonia IP, essas saídas podem ser apenas uma, embora algumas empresas instalem duas saídas com telefonia IP para lidar com um nível de redundância em estações de trabalho críticas. Na figura podemos ver como está estruturada a área de trabalho de um usuário:

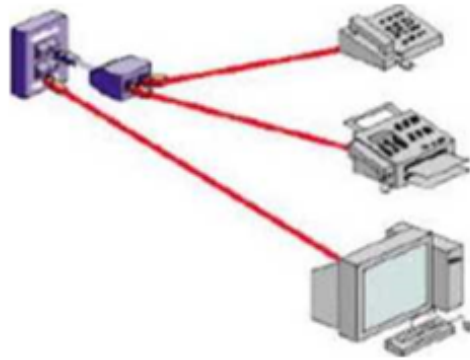


Figura 2.29: Área de Trabalho. Fonte: (ARQHYS, 2010)

2.9.8 Cabeamento Horizontal

O termo horizontal é utilizado porque esta parte do sistema de cabeamento percorre horizontalmente entre os pisos e tetos de um edifício, ou seja, o cabeamento que vai do armário de Telecomunicações até a tomada do usuário. A figura mostra como é constituído um cabeamento horizontal.

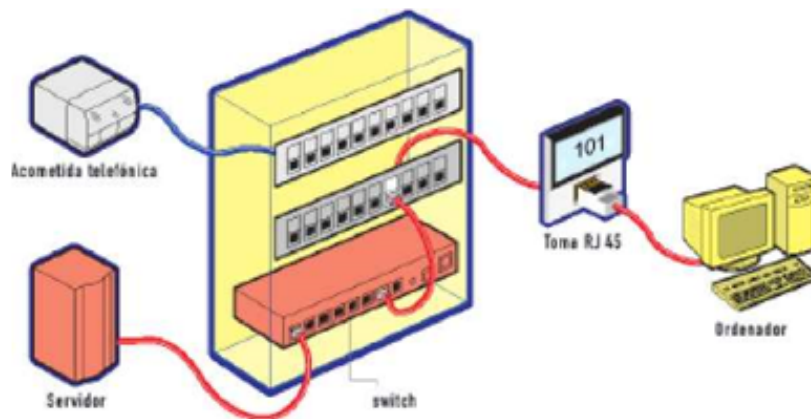


Figura 2.30: Fiação Horizontal. Fonte: (PANDUIT, 2011)

Deve-se considerar sua proximidade com fiações elétricas que geram altos níveis de interferência eletromagnética (motores, elevadores, transformadores, etc.) e cujas limitações se encontram na norma ANSI/EIA/TIA 569. (SIEMON, 2011)

A norma faz as seguintes recomendações em relação à topologia do cabeamento horizontal:

- O cabeamento horizontal deve seguir uma topologia em estrela.
- Cada tomada/conector de telecomunicações na área de trabalho deve se conectar

a uma interconexão na sala de telecomunicações.

- Componentes eléctricos não serão instalados como parte do cabeamento horizontal; quando necessário, esses componentes devem ser colocados fora do conector/tomada de telecomunicações.

- O cabeamento horizontal não deve conter mais de um ponto de transição entre o cabo horizontal e o cabo plano.

- Emendas de qualquer tipo não são permitidas na fiação horizontal. Distâncias: Independentemente do ambiente físico, a distância horizontal máxima não deve ultrapassar 90 m. A distância é medida da terminação mecânica do meio na interconexão horizontal na sala de telecomunicações até a tomada/conector de telecomunicações na área de trabalho. (PANDUIT, 2011).

Além disso, as seguintes distâncias são recomendadas:

- 10m são separados para cabos na área de trabalho e cabos na sala de telecomunicações (patch cords, cabos de equipamentos).

- Patch cords e patch cords que conectam cabeamento horizontal a equipamentos ou cabos de backbone em instalações de patch não devem exceder 6 m de comprimento.

- Na área de trabalho, recomenda-se uma distância máxima de 3 m do equipamento à tomada/conector de telecomunicações.

2.9.9 Cabeamento Vertical

A palavra vertical em cabeamento estruturado é a ligação que existe entre nós principais, nós secundários ou entre nós principais e secundários, normalmente o cabeamento vertical é instalado com meio guiado e em alguns casos com não guiado. Na figura observa-se como fica a estrutura do cabeamento vertical.



Figura 2.31: Fiação Vertical. Fonte: (PANDUIT, 2011)

O cabeamento vertical é instalado com o mesmo cabo do cabeamento horizontal ou acima, o principal é que os dados gerados em cada nó sejam transmitidos através deste link, é recomendado que se usarmos par trançado na horizontal, a vertical pode ser fibra óptica. Os equipamentos ativos também têm papel fundamental, devem possuir portas para par trançado e módulos de fibra óptica.

Distâncias de fiação: As distâncias estão diretamente relacionadas às características do meio instalado, se estamos falando de par trançado não deve ultrapassar 90m e se for fibra óptica as distâncias podem ser maiores tanto com fibra Mono-modo quanto Multimodo.

2.9.10 Sala de Telecomunicações (Bastidores)

Uma sala de telecomunicações é a área de um edifício destinada ao uso exclusivo de equipamentos associados ao sistema de cabeamento de telecomunicações. O espaço da sala de comunicações não deve ser compartilhado com instalações elétricas que não sejam de telecomunicações. A sala de telecomunicações deve ser capaz de abrigar equipamentos de telecomunicações, terminações de cabos e cabeamento de interconexão. O projeto das salas de telecomunicações deve considerar, além de voz e dados, a incorporação de outros sistemas de informação da empresa, como televisão a cabo (CATV),

alarmes, segurança, áudio e outros sistemas de telecomunicações. Toda empresa deve ter pelo menos uma sala de telecomunicações ou sala de equipamentos. Não há limite máximo para o número de salas de telecomunicações que podem existir na empresa. A figura mostra uma sala de servidores com um rack de comunicação. (ELETRÔNICA, 2010)



Figura 2.32: Sala de Equipamentos. Fonte: (PANDUIT, SALA DE MÁQUINAS, 2010)

Na sala de telecomunicações existe um tecto e chão falsos que facilitam a circulação do ar para manter uma temperatura média entre os 17 e os 20 graus Celsius. A instalação de pisos e tecto não deve ser inferior a 30 cm a uma altura não inferior a 2,60 m. No espaço que me dá o tecto ao tecto falso e o chão ao chão falso, são instalados os meios de condução onde vão chegar todos os meios guiados que correspondem à cablagem estruturada e ligações dos prestadores de serviços de telecomunicações.

2.10 Regulamentos

Para o dimensionamento da infraestrutura física para implantação do cabeamento estruturado, será baseado nas normas: (UNITEL, 2014)

- **ANSI/TIA/EIA-568-B:** Fiação de Telecomunicações em Edifícios Anúncios de como instalar a fiação: Requisitos Gerais TIA/EIA 568-B1; TIA/EIA 568-B2: Componentes de fiação de par trançado balanceado; TIA/EIA 568-B3 Componentes de fiação, fibra óptica.

- **EIA/TIA-568-C:** Conjunto de normas para instalações de cabeamento para instalações do cliente.

- **EIA/TIA-569-B:** Padrão de Edifícios Comerciais para Vias e Espaços de Telecomunicações, que padroniza as práticas de projeto e construção dentro e entre os edifícios, que são feitos para suportar mídia e/ou equipamentos de telecomunicações, como pistas e guias, instalações de entrada de edifícios, gabinetes e/ou rack de equipamentos e sala de equipamentos.

Esta norma indica os seguintes elementos para espaços e vias de telecomunicações em edifícios:

Percursos horizontais

- Envolvem infra-estruturas para instalação de cabos de telecomunicações provenientes dos seus armários e destinados a uma tomada/conector de telecomunicações.

- Os lances horizontais podem ser de dois tipos: calha sob o piso, piso de acesso, conduíte elétrico, bandejas de cabos e tubos, teto e perímetro.

- As diretrizes e procedimentos do projeto são especificados diretamente para esses tipos de rotas.

- Eles consistem em rotas internas (dentro de um edifício) e entre edifícios (externo).

- São compostos por conduíte elétrico, luva de conexão, aberturas e bandejas. Passagens entre os Edifícios.

- Eles são compostos por lances de cabos subterrâneos, enterrados, aéreos ou de túneis.

Estação de trabalho

- Espaço interno de um edifício onde um ocupante interage entre si com dispositivos de telecomunicações

Tomadas de telecomunicações

- Localização do ponto de conexão entre o cabo horizontal e os dispositivos de conexão do cabo na área de trabalho. Refere-se à caixa (carcaça) ou placa de fase em geral, em oposição aos soquetes incluindo os conectores de telecomunicações individuais.

- É necessário um mínimo de uma tomada por estação de trabalho (duas por área de trabalho). O destino do espaço de trabalho é um para cada 10 m²

- Pelo menos uma tomada elétrica deve ser instalada perto de cada tomada de telecomunicações.

Bastidores/Gabinete de Telecomunicações

- Dedicado exclusivamente à infra-estrutura de telecomunicações.

- Equipamentos e instalações que não sejam de telecomunicações não devem ser instalados, passados ou inseridos nesses gabinetes.

- Mínimo de um armário por andar.
- Armários adicionais devem ser obtidos para cada área acima de 1.000 m², desde que:

- A área útil do piso é superior a 1.000 m²
- A distância horizontal excede 90 m.
- **EIA/TIA-606 A:** Norma de Administração para Edifícios Comerciais de Telecomunicações de Edifícios Comerciais, que fornece diretrizes para marcação e gerenciamento dos componentes de um sistema de Cabeamento Estruturado.

Esta norma estabelece diretrizes para proprietários, usuários finais, consultores, empreiteiros, projectistas, instaladores e administradores de infraestrutura de telecomunicações e sistemas relacionados.

Capítulo 3

Localização Geográfica, Actividades e Infraestrutura de Rede Actual do CMCM

Neste capítulo descreve-se o estado actual da infraestrutura de rede do CMCM, sua localização, caracterização, actividades desenvolvidas, estatuto orgânico, regulamentação entre outros.

3.1 Conselho Municipal da Cidade da Matola

A Cidade da Matola é a capital da Província de Maputo, confinando com a Cidade de Maputo, o Município da Matola tem como limites: a Norte e Nordeste o distrito da Moamba, a Nordeste o distrito de Marracuene, a Este e Sudoeste a Cidade de Maputo, a Sudoeste o estuário de Maputo, a Sul o distrito de Boane e o distrito Municipal da Catembe e a Sudoeste o distrito de Boane. Com uma área de 375 km² e uma população estimada em aproximadamente 1.032.197 (um milhão, trinta e dois mil, cento e noventa e sete habitantes), a Cidade da Matola é de características urbana, semi-urbana e rural e tem um padrão e tecido social rico e diversificado, sendo detentora de um vasto e diversificado parque industrial. A Cidade da Matola organiza-se territorialmente em 3 Postos Administrativos Municipais, subdivididos em 42 Bairros municipais.

No ano 2018, entrou em vigor o novo quadro jurídico-legal que regula a actividade das Autarquias locais, designadamente a lei nº6/2018 de 3 de Agosto, republicada pela lei nº13/2018 de 17 de Dezembro, abrindo-se uma nova etapa no processo de descentralização do poder administrativo central.

Actualmente o CMCM conta com mais de 1500 funcionários, dentre eles o Presidente

(PCM), Vereadores, Chefes dos Postos Administrativos, Directores dos departamentos, Chefes de serviços municipais, Chefes dos bairros municipais, Técnicos Administrativos e Agentes de limpeza.

3.2 Actividades

O Conselho Municipal da Cidade da Matola é uma instituição pública de gestão indireta do Estado, i.e o município faz gestão independente da área que lhe diz respeito, sob consideração da lei mãe e local. O conselho Municipal sobrevive de receitas próprias e transferência da feita pelo Estado, porém tem responsabilidade, deveres, direitos e obrigações. Para execução das suas actividades tais como, construção de estradas, recolha de resíduos sólidos, garantia de acesso a serviços básicos dentre outras responsabilidades do CMCM, O conselho para a execução das actividades da sua responsabilidade tem como necessidade de meios financeiros e para o efeito, varias são as actividades pelo município executadas para o alcance dos objetivos traçados por cada governo, que por sua vez são programados anualmente. O CMCM, tem com algumas das suas actividades as seguintes:

a) Cobrança de impostos:

- Imposto Pessoal Autárquico (IPA);
- Imposto de Veiculos;
- Imposto Predial, etc.

b) Cobrança de Taxas:

- Taxa de Actividade Econômica;
- Taxa de Publicidade;
- Taxa de Circulação e Transportes Públicos e de Viaturas Pesadas;

c) Cobrança de Licenças:

- Licença de Circulação;
- Licença para exercício da Actividade de Limpezas;
- Licença para pequenos Ginásios;
- Licença de Construção, etc.

Essas são algumas das actividades desenvolvidas no CMCM

3.3 Localização e Contacto

O Conselho Municipal da Cidade da Matola, localiza-se na Província de Maputo, Cidade da Matola, Av. União Africana, nº 2083. Contactável pelo endereço: www.cmcm.gov.mz e pela Linha Verde: 800615615

3.4 Edifício-sede do Conselho Municipal da Cidade da Matola



Figura 3.1: Edifício-sede do Conselho Municipal da Cidade da Matola, Fonte: O Autor, Abril de 2025



Figura 3.2: Logotipo oficial do Conselho Municipal da Cidade da Matola, Fonte: CMCM

3.5 Organograma

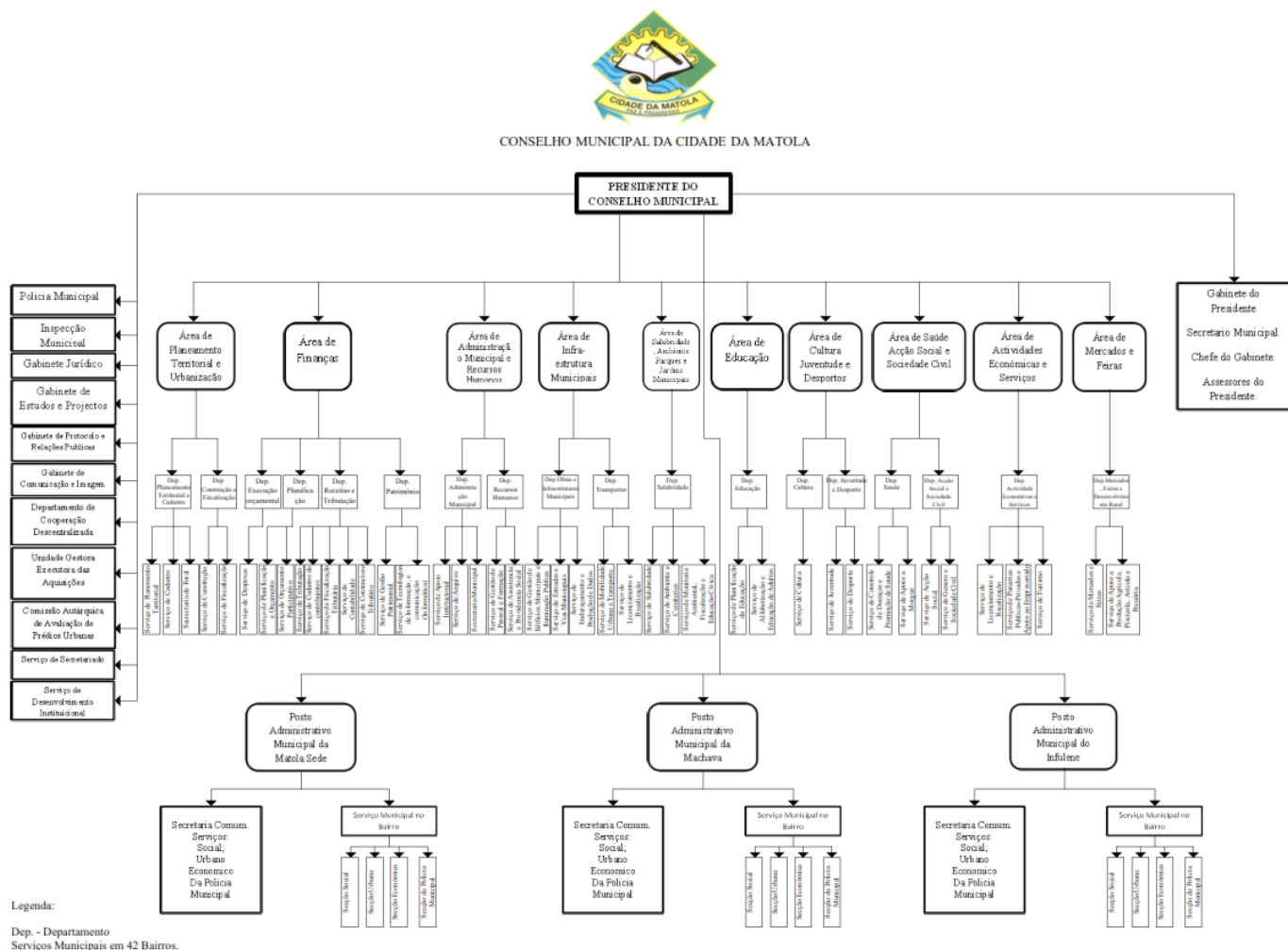


Figura 3.3: Organograma do CMCM. Fonte: CMCM

3.6 Missão, Visão e Valores do Conselho Municipal da Cidade da Matola

3.6.1 Missão

Servir os Munícipes e visitantes, com comprometimento, proporcionando oportunidades de habitação, negocio e bem estar social.

3.6.2 Visão

Matola, Cidade com características cada vez mais urbana, sustentável, consolidando-se como capital Industrial e Cultural de destaque em Moçambique.

3.6.3 Valores

União, Colaboração, Responsabilidade, Solidariedade, Inovação, Transparência e Apropriação.

3.7 Sector a Realizar o Estágio

O estágio profissional realizou-se no Departamento do Patrimônio, Sector de Tecnologias de Informação e Comunicação, este sector é responsável por garantir a funcionalidade contínua de toda infraestrutura tecnológica do CMCM, como exemplos computadores, impressoras, softwares (em dispositivos), redes, entre outros.

3.8 Actividade Realizadas Durante o Estágio

O estágio concedido por um período de 3 meses que compreenderam o tempo para a realização do estágio profissional, foram dadas tarefas e responsabilidades e estabelecidos os objectivos a serem alcançados entre elas a proposta de melhoramento da infraestrutura de rede local. Inicialmente, foi apresentado a infraestrutura de rede local, e também, e foram disponibilizadas as informações e documentos necessários para melhor integração. Embora as actividades que foram desenvolvidas já tivessem uma planificação prévia, foi-me incumbida a tarefa de fazer o estudo da infraestrutura da rede lógica, levantamento dos problemas e propor soluções a fim de mitigar os problemas actuais

As principais actividades desenvolvidas pelo estagiário foram:

- a) Configurar a rede tendo em conta os aspectos de segurança;
- b) Solucionar problemas de roteamento na rede;
- c) Configurar VLANs e roteamento entre VLANs;
- d) Projectar redes de computadores;
- e) Suporte e assistência técnica aos colaboradores;
- f) Instalação de softwares em computadores e equipamentos electrónicos;

- g) Manutenção preventiva e correctiva de dispositivos electrónicos (Impressoras e Computadores);
- h) Configuração e reparação de impressoras, e substituição de toner;
- i) Configuração de computadores (*start up*).

3.9 Infraestrutura Actual de Rede

O CMCM actualmente apresenta uma rede estruturada, com modem, *patch painel*, *router*, *switches*, *access points* (pontos de acesso), cabeamento estruturado (vertical e horizontal), entre outras componentes que constituem uma rede estruturada. Porém a rede não está catalogada, i.e, os ramais que constituem a rede não estão identificados, a nível dos bastidores centrais e locais. O *patch painel* dos bastidores centrais não indica qual é o destino do cabo nele fixado, dificultando assim actividades como, a manutenção, verificação de dados, diagnóstico, entre outras dificuldades quem podem ser encontradas numa rede onde não se sabe por onde começar a trabalhar. A não separação da rede em vereações ou departamentos através de VLAN's, isto é, todos os usuários estão no mesmo domínio de *broadcast*, colocando a rede demasiadamente congestionada e com atrasos significativos. A rede não está dimensionada em função de número de usuários.

Actualmente a instituição dispõe de dois fornecedores de sinal de internet, com a largura de banda 40 Mbps (internet dedicada), fornecido pela Empresa Telecomunicações de Moçambique Celular (T-mcel), e outra fornecida pela TV-Cabo de 24 Mbps (internet partilhada) ambas em fibra óptica que são recebidos por dois modems das operadoras e que depois passados para um router que recebe os dois sinais e depois para um *switch* nuclear, em seguida distribuído pelo edifício através de *switches* de distribuição em outros pisos e sectores.

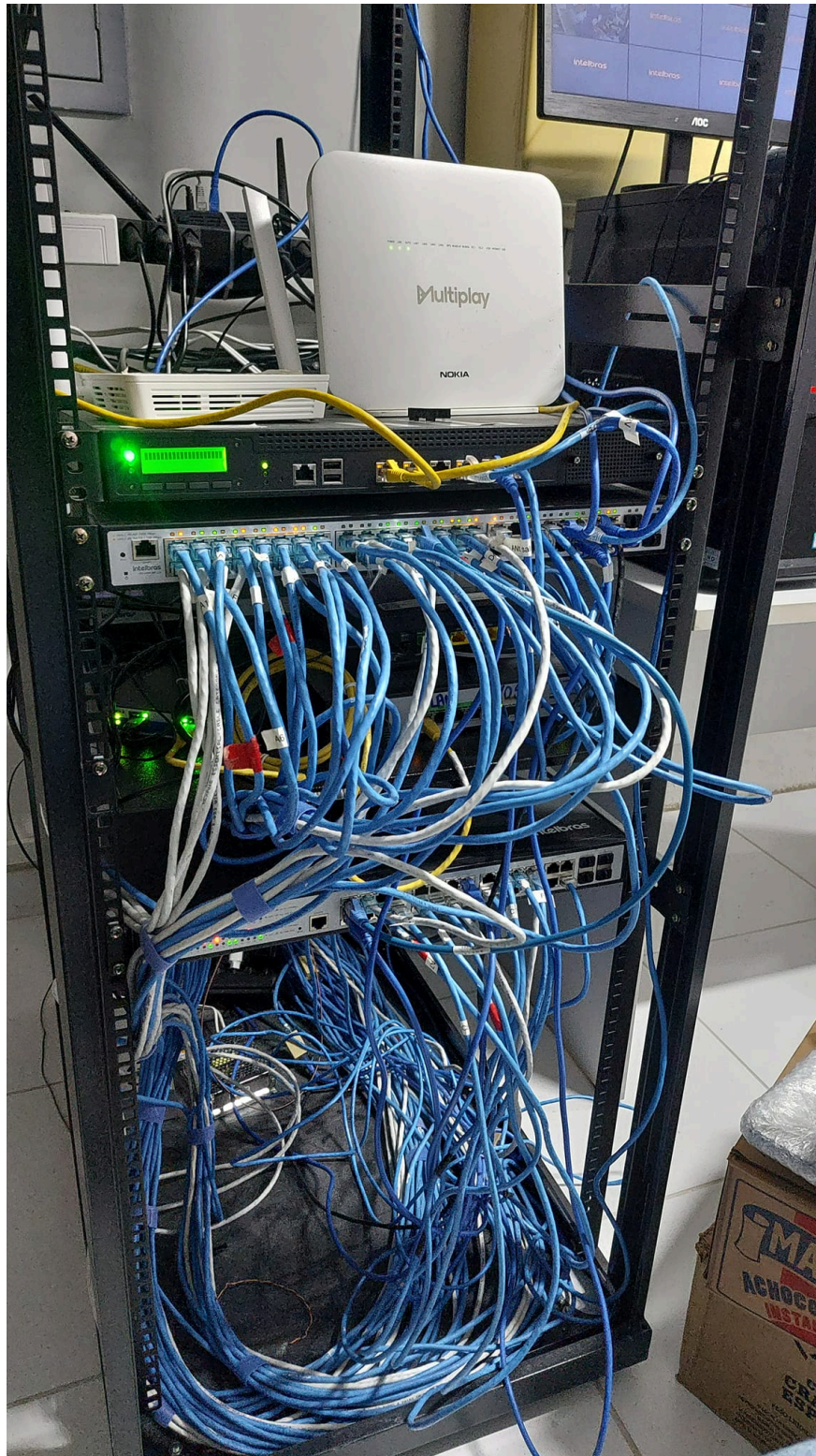


Figura 3.4: Um dos Racks da Sala de Telecomunicações. Fonte: O Autor

Capítulo 4

Implementação e Discussão de Resultados

4.1 Avaliação das Propostas de Solução

Do cenário apresentado para o alcance do melhor desempenho de rede será implementada tendo em consideração os pontos a baixo:

- Implementação de VLANs (segmentação da rede VLAN); e
- Redundância com uso de Switches interligados.

Face aos problemas identificados na rede, e das 2 propostas de solução, serão usadas as propostas de segmentação de rede usando VLANs e a utilização de switches de distribuição interligados para garantir que os dados fluem caso um dos links do switches esteja baixo (por razões diversas), se possa usar o link alternativo garantindo maior disponibilidade na rede.

4.2 Segmentação da Rede

Segmentar a rede vai minimizar domínios de broadcast, esta característica pode ser alcançada com a inclusão de dispositivos de camada três na camada de distribuição portanto para a configuração de VLAN, vai se usar um *Switch* gerenciável (L3).

Neste tema, é apresentado como foi realizada a implementação da segmentação da rede lógica, utilizando *switches* Cisco da ferramenta **Cisco Packet Tracer** para que fosse possível visualizar um ambiente com uma ideia mais prática. Cisco Packet Tracer, é um software gratuito para simulação de redes de computadores desenvolvido pela empresa

Cisco também fabricante de dispositivos de rede.

Este software oferece visualização, simulação, criação, avaliação e recursos de colaboração que facilitam o ensino e aprendizagem de diversos conceitos complexos de tecnologias de redes e telecomunicações. (Cisco Networking, 2025).

O CMCM dispõe de uma rede estruturada, porém, a falta de separação da rede em VLANs e a não catalogação, ausência de dispositivos de segurança, apresenta uma dificuldade na operação, dificuldade de identificar e corrigir problemas que a rede frequentemente apresenta, entretanto, o trabalho consistirá em refazer e corrigir todos esses defeitos, padronizando a mesma tendo em conta os padrões internacionais. Serão reutilizados os dispositivos de rede já existente, acrescentando os dispositivos de segurança, servidores e aumentando a quantidade de switch necessários, tendo em conta os usuários actuais e possível crescimento da rede no futuro.

conforme a figura abaixo, na camada de acesso estão instalados os *switch's* utilizados pelos usuários e o switch de distribuição, com maior capacidade de transmissão, é responsável por interconectar a rede de acesso.

Na figura a seguir, é apresentado o esquema completo da rede. É de ser observar uma rede hierárquica dependente da redundância (dispositivos *firewall* e *routers*) entre os pontos da rede, essa redundância permite que caso houver uma falha, a rota seja alterada para o ponto de ligação seguinte, assim não comprometendo o acesso aos recursos da rede.

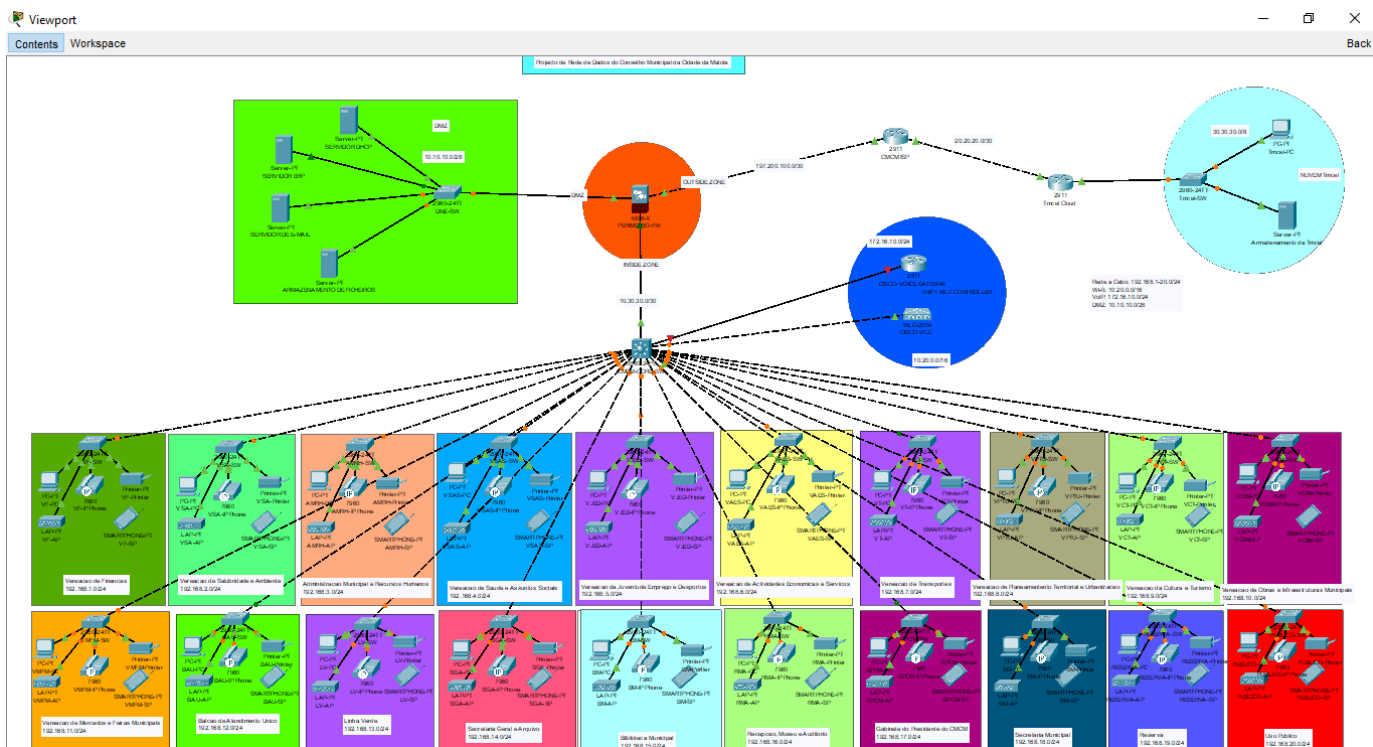


Figura 4.1: Rede de Dados Proposta Fonte: Autor

Para obter os benefícios de uma rede local segmentada, foi atribuída a cada departamento/sector uma VLAN diferente.

O roteamento entre elas é feito por um par de dispositivos redundantes. O esquema completo pode ser visualizado na figura a seguir:

Na rede proposta, composta por um universo de 18 VLANs, uma dessas VLANs, a VLAN 70 por exemplo não ira precisar de sair para fora da rede interna sendo que os serviços por si requisitados são fornecidos pelo servidor de aplicativos localizado no Rack da empresa.

As VLANs não comunicaram entre si, para evitar que informação de sectores críticos como as finanças e recursos humanos possa ficar comprometida.

A VLAN 80, a rede dos visitantes, também estará separada de toda a rede, ela contempla a rede Wi-fi fornecida pelo ponto de acesso e outros usuários.

O DMZ (Zona Desmilitarizada), mecanismo de segurança composto por um servidor multifuncional (NAT, POP3, HTTP, entre outros serviços), que serve para interligar a rede interna da externa através do Firewalls da cisco do modelo ASA 5506-X para evitar que hacker ou malweres da internet não possam invadir a rede interna com facilidade, entretanto, garantindo a segurança dos usuários da rede.

Na proposta colocada haverá também redundância quanto ao sinal de internet a em-

presa terá duas fornecedoras do sinal de internet, a actual TV Cabo e uma outra a escolha da Empresa, mas que forneça o sinal na mesma largura de banda 24Mbps, igual ao sinal actualmente usado, entretanto esta deve ser internet dedicada.

4.2.1 Endereçamento das VLANs

A partir da definição das VLANs o gerenciamento pode ser feito de forma a caracterizar as mesmas isoladamente, possibilitando, assim, um monitoramento e gerenciamento direccionado ao tráfego real de cada VLAN. A tabela a seguir, apresenta os endereços e os dados usados nas VLANs, a gama de endereços de host na rede que seriam utilizados para atribuir endereços IP em cada VLAN de cada departamento.

Tabela 4.1: Tabela de Endereços

Departamento	Rede/Musk	VLAN	Broadcast
VF	192.168.1.0/24	VLAN 10	192.168.1.255
VSA	192.168.2.0/24	VLAN 20	192.168.2.255
AMRH	192.168.3.0/24	VLAN 30	192.168.3.255
VSAS	192.168.4.0/24	VLAN 40	192.168.4.255
VJED	192.168.5.0/24	VLAN 50	192.168.5.255
VAES	192.168.6.0/24	VLAN 60	192.168.6.255
VT	192.168.7.0/24	VLAN 70	192.168.7.255
VPTU	192.168.8.0/24	VLAN 80	192.168.8.255
VCT	192.168.9.0/24	VLAN 90	192.168.9.255
VOIM	192.168.10.0/24	VLAN 100	192.168.10.255
VMFM	192.168.11.0/24	VLAN 110	192.168.11.255
BAU	192.168.12.0/24	VLAN 120	192.168.12.255
LV	192.168.13.0/24	VLAN 130	192.168.13.255
SGA	192.168.14.0/24	VLAN 140	192.168.14.255
BM	192.168.15.0/24	VLAN 150	192.168.15.255
RMA	192.168.16.0/24	VLAN 160	192.168.16.255
GPCM	192.168.17.0/24	VLAN 170	192.168.17.255
SM	192.168.18.0/24	VLAN 180	192.168.18.255
RESERVA	192.168.19.0/24	VLAN 190	192.168.19.255
PUBLICO	192.168.20.0/24	VLAN 200	192.168.20.255

As VLANs foram divididas por sectores, e é possível visualizar na tabela os endereços

lógicos das VLANs que foram utilizados tanto na identificação dos hosts nos departamentos e dados para a configuração das mesmas no switch de acesso. A tabela possui, na sua primeira coluna, o nome de cada departamento, pois auxilia na organização da rede, na segunda coluna corresponde à endereço de rede de cada VLAN, na terceira coluna corresponde a identificação da VLAN, número correspondente de cada VLAN. Por cada VLAN pode se ter até 254 endereços de host, por exemplo, a VLAN 10, poderia variar seus hosts de 192.168.1.1 a 192.168.1.254, sendo 192.168.1.0 o endereço da rede e 192.168.1.255 o endereço de broadcast, o sufixo /24 (255.255.255.0) corresponde a definição de sua máscara de sub-rede.

4.2.2 Configurações no Switch

Os códigos configurados nos Switchs são:

- Criação de porta trunk para o Router;
- Criação de portas de acesso;
- Configuração de porta de default-gateway;
- Criação de VLANs e atribuição de portas de comutação às VLANs.

4.2.2.1 Comunicação Trunk para o Router

Os seguintes comandos foram utilizados para configurar três portas Trunk no Switch de distribuição, uma que liga ao Firewall e as outras ligadas aos Switches, a interface de linha de comando (CLI) do Cisco Packet Tracer foi utilizada para executar os comandos.

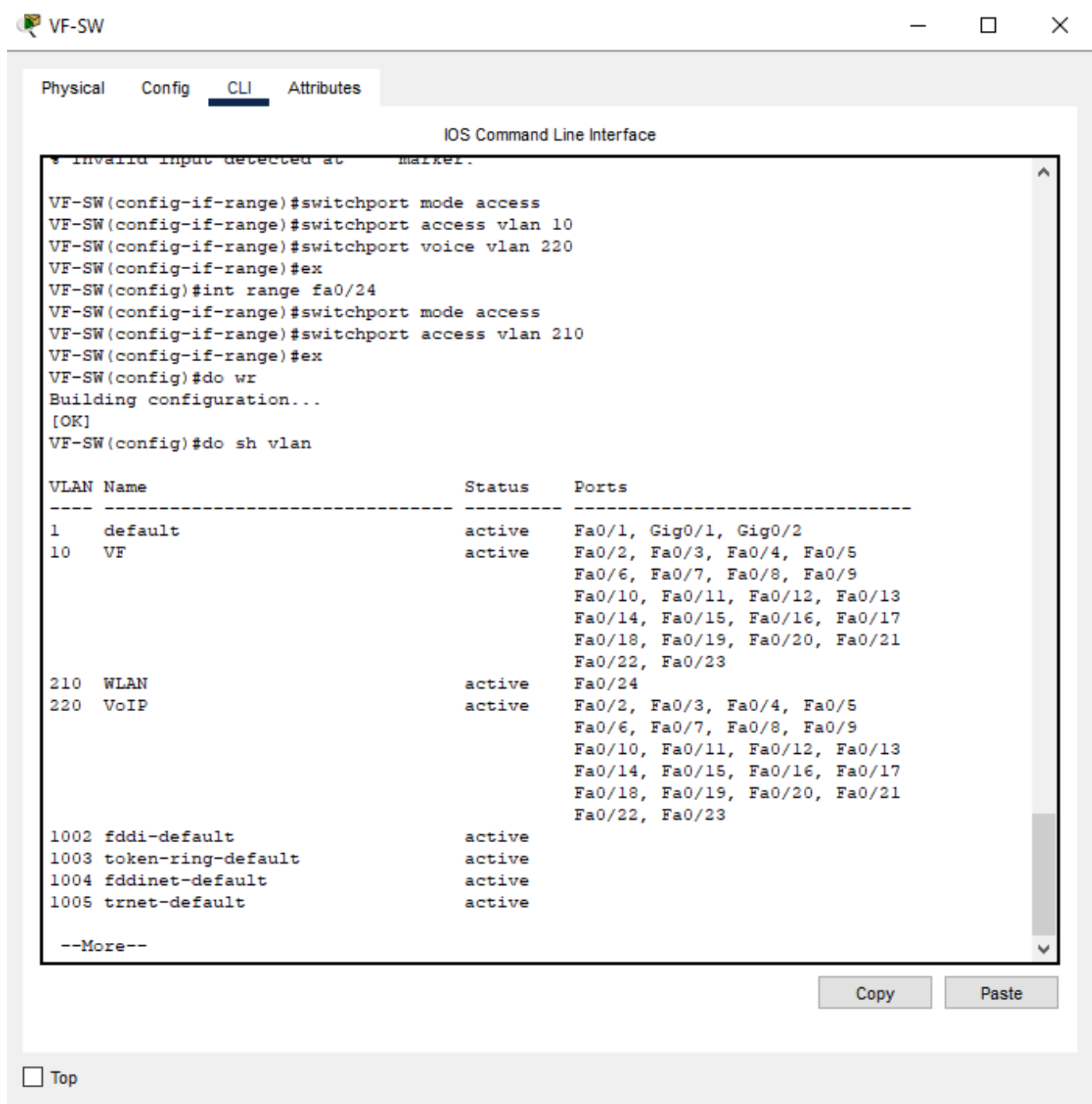
```
Switch(config-if)#switchport trunk encapsulation dot1q
Switch(config-if)#switch mode trunk
Switch(config-if)#int fa0/24
Switch(config-if)#int fa0/23
Switch(config-if)#switchport trunk encapsulation dot1q
Switch(config-if)#int fa0/24
Switch(config-if)#int fa0/23
Switch(config-if)#switch mode trunk
Switch(config-if)#int fa0/24
Switch(config-if)#switchport trunk encapsulation dot1q
Switch(config-if)#switch mode trunk
Switch(config-if)#int g0/1
Switch(config-if)#switchport trunk encapsulation dot1q
Switch(config-if)#switch mode trunk

Switch(config-if)#
```

Figura 4.2: Comunicação Trunk e Encapsulamento dot1q, Fonte: Autor

4.2.2.2 Atribuição de portas de switch a VLANs

Para que o switch tenha um domínio de difusão diferente, atribuiu-se cada VLAN criada a uma porta do Switch de distribuição. Os códigos utilizados para atribuir uma porta de switch a uma VLAN são os seguintes:



```
VF-SW
Physical Config CLI Attributes
IOS Command Line Interface
* Invalid input detected at ... marker.
VF-SW(config-if-range)#switchport mode access
VF-SW(config-if-range)#switchport access vlan 10
VF-SW(config-if-range)#switchport voice vlan 220
VF-SW(config-if-range)#ex
VF-SW(config)#int range fa0/24
VF-SW(config-if-range)#switchport mode access
VF-SW(config-if-range)#switchport access vlan 210
VF-SW(config-if-range)#ex
VF-SW(config)#do wr
Building configuration...
[OK]
VF-SW(config)#do sh vlan

VLAN Name                Status    Ports
-----
1    default                 active    Fa0/1, Gig0/1, Gig0/2
10   VF                      active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
                                           Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                           Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                           Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                           Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                           Fa0/22, Fa0/23
210  WLAN                   active    Fa0/24
220  VoIP                   active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
                                           Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                           Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                           Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                           Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                           Fa0/22, Fa0/23
1002 fddi-default           active
1003 token-ring-default   active
1004 fddinet-default       active
1005 trnet-default         active

--More--
```

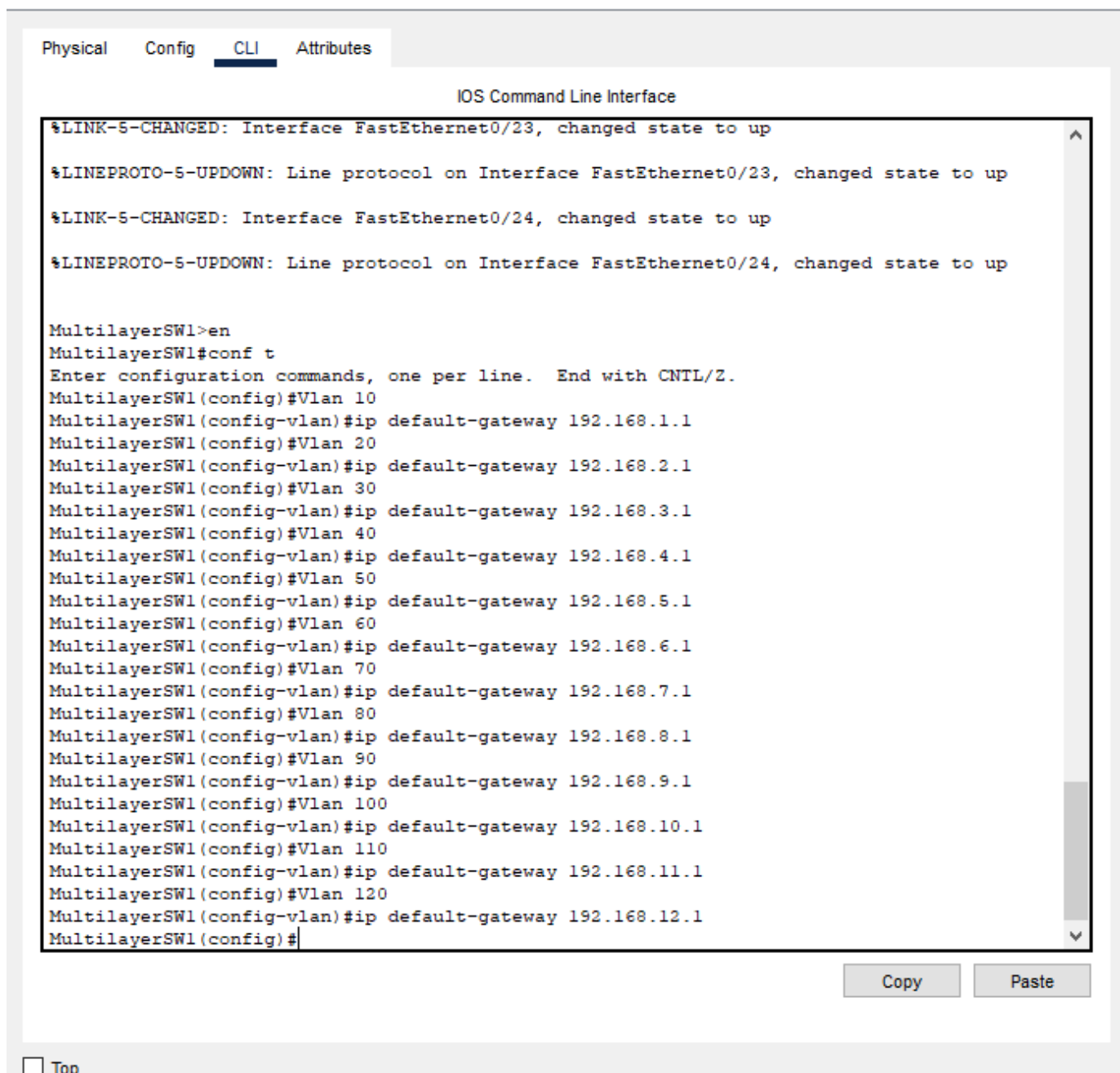
Figura 4.3: Atribuição de portas do Switch a VLANs, Fonte: Autor

A função da primeira linha de código é selecionar a porta do switch à qual se pretende atribuir a VLAN. O tipo de interface do switch na porta usado é fastethernet e o identifica-

dor de interface 0/3, corresponde a terceira porta do switch. Também se atribui um ID a VLAN na respectiva a porta.

4.2.2.3 Configuração de Default-Gateway

As linhas de comando utilizado para configurar o default-gateway (gateway padrão) para cada VLAN é mostrado abaixo. O default-gateway está configurado para permitir pacotes destinados à rede externa da actual. É sempre atribuído para a interface que liga a VLAN ao Switch de Distribuição.



The screenshot shows a network switch CLI interface with the following content:

```
Physical  Config  CLI  Attributes
IOS Command Line Interface

%LINK-5-CHANGED: Interface FastEthernet0/23, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/23, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/24, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/24, changed state to up

MultilayerSW1>en
MultilayerSW1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
MultilayerSW1(config)#Vlan 10
MultilayerSW1(config-vlan)#ip default-gateway 192.168.1.1
MultilayerSW1(config)#Vlan 20
MultilayerSW1(config-vlan)#ip default-gateway 192.168.2.1
MultilayerSW1(config)#Vlan 30
MultilayerSW1(config-vlan)#ip default-gateway 192.168.3.1
MultilayerSW1(config)#Vlan 40
MultilayerSW1(config-vlan)#ip default-gateway 192.168.4.1
MultilayerSW1(config)#Vlan 50
MultilayerSW1(config-vlan)#ip default-gateway 192.168.5.1
MultilayerSW1(config)#Vlan 60
MultilayerSW1(config-vlan)#ip default-gateway 192.168.6.1
MultilayerSW1(config)#Vlan 70
MultilayerSW1(config-vlan)#ip default-gateway 192.168.7.1
MultilayerSW1(config)#Vlan 80
MultilayerSW1(config-vlan)#ip default-gateway 192.168.8.1
MultilayerSW1(config)#Vlan 90
MultilayerSW1(config-vlan)#ip default-gateway 192.168.9.1
MultilayerSW1(config)#Vlan 100
MultilayerSW1(config-vlan)#ip default-gateway 192.168.10.1
MultilayerSW1(config)#Vlan 110
MultilayerSW1(config-vlan)#ip default-gateway 192.168.11.1
MultilayerSW1(config)#Vlan 120
MultilayerSW1(config-vlan)#ip default-gateway 192.168.12.1
MultilayerSW1(config)#
```

Buttons: Copy, Paste

Top

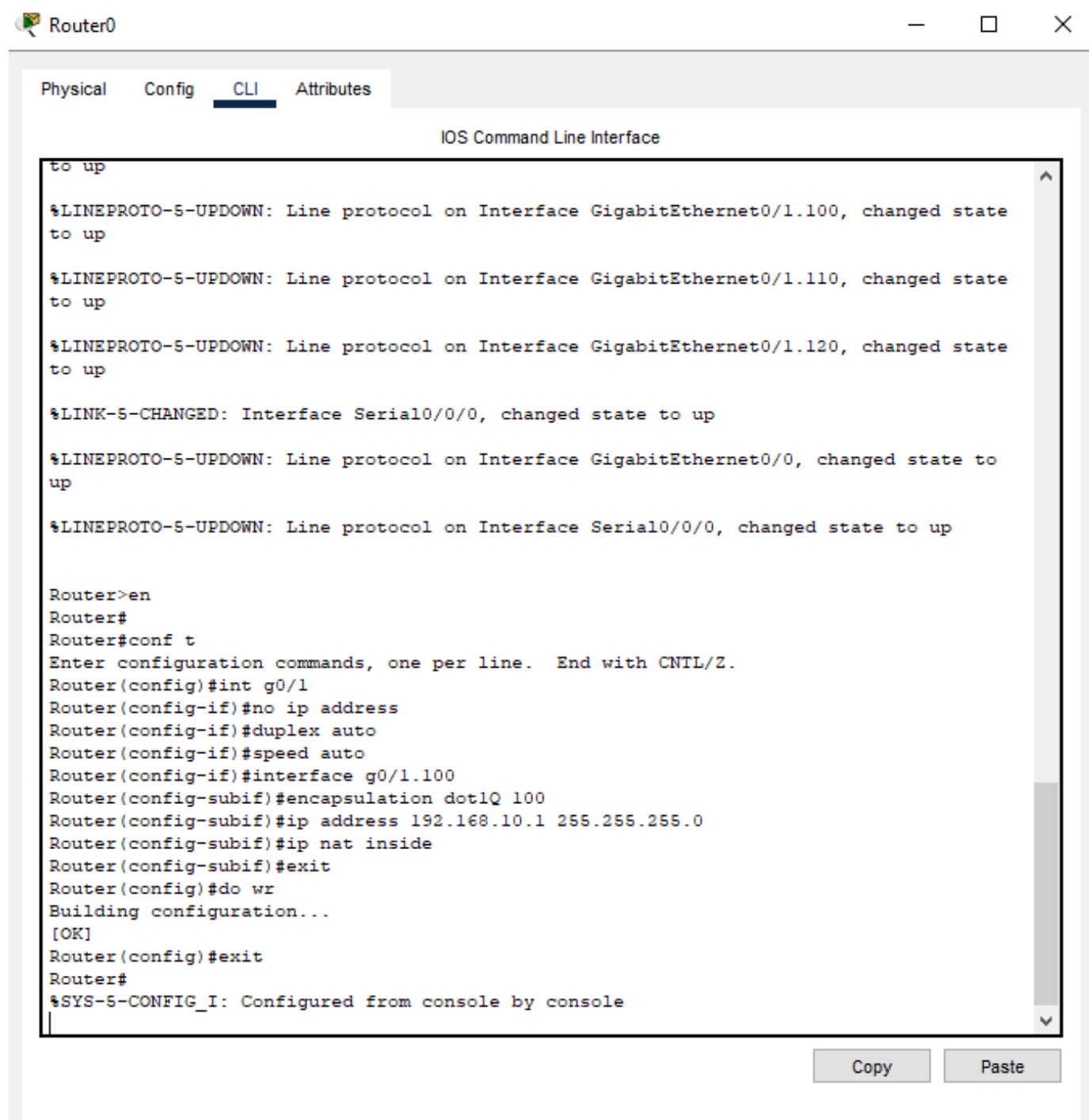
Figura 4.4: Configuração de Default-Gateway. Fonte: Autor

4.2.3 Configuração do Router

Foram feitas, a configuração de DHCP, encaminhamento para as interfaces VLAN, tradução de endereços de rede (NAT), codificação de interfaces para todas as VLANs nos dois Switchs principais (Switch de Distribuição).

4.2.3.1 Criar Sub-interfaces para cada VLAN

As subinterfaces foram configuradas na interface do router que liga porta do firewall e a posterior a porta do switch. As subinterfaces permitirão que os dados de todas as VLANs cheguem ao router, para que esta permita à comunicação com sub-redes externas. As sub-interfaces do router, NAT e encaminhamento de interfaces VLAN são configuradas usando os comandos abaixo.



```
Router0
Physical Config CLI Attributes
IOS Command Line Interface

to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1.100, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1.110, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1.120, changed state to up

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

Router>en
Router#
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int g0/1
Router(config-if)#no ip address
Router(config-if)#duplex auto
Router(config-if)#speed auto
Router(config-if)#interface g0/1.100
Router(config-subif)#encapsulation dot1Q 100
Router(config-subif)#ip address 192.168.10.1 255.255.255.0
Router(config-subif)#ip nat inside
Router(config-subif)#exit
Router(config)#do wr
Building configuration...
[OK]
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
```

Copy Paste

Figura 4.5: Criação das Subinterfaces para cada VLAN

O ID e os endereços IP das outras VLANs foram configurados usando o mesmo comando acima. A Todas Linhas de comando de projecto constam do ANEXO.

4.2.4 Orçamento da Proposta

Tabela 4.2: Orçamento

Descrição	Preço Unitário (MZN)	Quantidade	Total (MZN)
Switches (WS- C2960-X-24PSQ-L)	200.000	12	2.400.000
Controlador de Wi-fi WLC	10.000	1	10.000
Telefones IP	30.000	20	600.000
Switch (WS- C3560-Multyaler-24PSQ-L)	200.000	1	200.000
Firewall (Cisco ASA 5500-X)	60.000	1	60.000
Servidor (HPE Proliant DL388)	180.000	3	540.000
Rack Server (Vertiv 42U)	18.000	2	36.000
Extensão Eléctrica (14 Portas)	9.600	2	19.200
Cabos <i>Patch Cord</i> (0.6m)	100	75	7.500
Patch Panel 48 Portas	5.000	4	20.000
		Total sem IVA	3.873.500

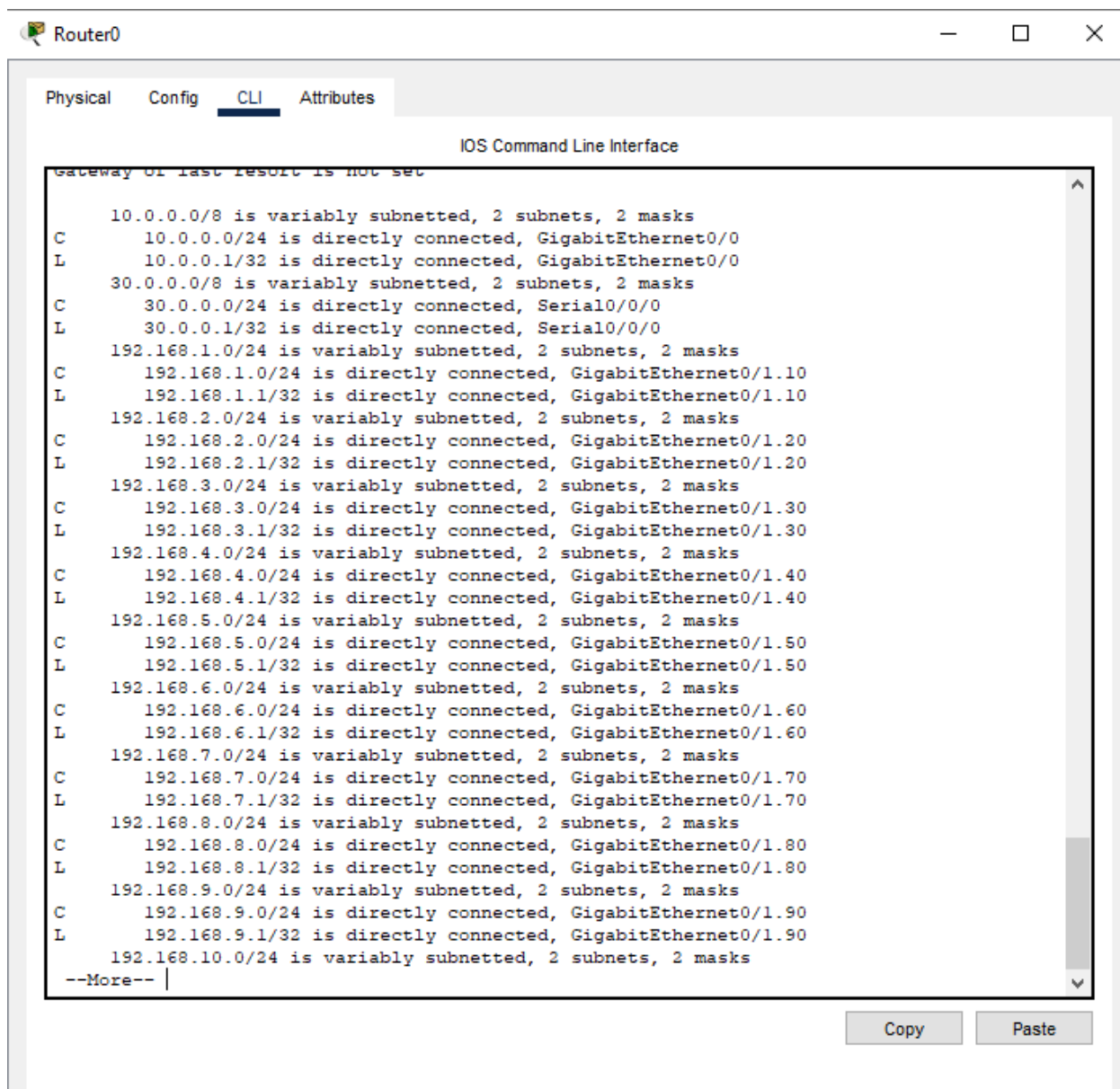
4.2.5 Resultados e discussão

4.2.5.1 Simulação da Rede

Como podemos observar a simulação mostrada na figura 4.1, é um desenho de protótipo virtual da rede que nesse trabalho é proposto. Aliando-se a boas práticas de projecto de rede de computadores, apresenta-se a hierarquia de redes nomeadamente, a camada de núcleo de rede (Core Router), camada de distribuição (Switch Multilayer) e camada de acesso Switchs de acesso configuradas para todas as VLAN. Todas essas camadas foram devidamente configuradas para fornecer cobertura de rede a toda a infraestrutura do CMCM. As sinalizações triangulares verdes indicam conectividade de rede entre os servidores, router, switches, e outros dispositivos. Devido a falta de recursos para sua implantação, como já referido recorre-se unicamente a simulação da mesma usando o Cisco Packet Tracer.

4.2.5.2 Verificação das configurações do Router

O resultado dos comandos "show ip route" e "show ip int brief" é o mostrado nas figuras a seguir, o resultado indica que o protocolo de roteamento e a configuração da interface do router estava a funcionar como esperado.



```
IOS Command Line Interface
Gateway of last resort is not set

 10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C    10.0.0.0/24 is directly connected, GigabitEthernet0/0
L    10.0.0.1/32 is directly connected, GigabitEthernet0/0
 30.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C    30.0.0.0/24 is directly connected, Serial0/0/0
L    30.0.0.1/32 is directly connected, Serial0/0/0
192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.1.0/24 is directly connected, GigabitEthernet0/1.10
L    192.168.1.1/32 is directly connected, GigabitEthernet0/1.10
192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.2.0/24 is directly connected, GigabitEthernet0/1.20
L    192.168.2.1/32 is directly connected, GigabitEthernet0/1.20
192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.3.0/24 is directly connected, GigabitEthernet0/1.30
L    192.168.3.1/32 is directly connected, GigabitEthernet0/1.30
192.168.4.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.4.0/24 is directly connected, GigabitEthernet0/1.40
L    192.168.4.1/32 is directly connected, GigabitEthernet0/1.40
192.168.5.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.5.0/24 is directly connected, GigabitEthernet0/1.50
L    192.168.5.1/32 is directly connected, GigabitEthernet0/1.50
192.168.6.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.6.0/24 is directly connected, GigabitEthernet0/1.60
L    192.168.6.1/32 is directly connected, GigabitEthernet0/1.60
192.168.7.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.7.0/24 is directly connected, GigabitEthernet0/1.70
L    192.168.7.1/32 is directly connected, GigabitEthernet0/1.70
192.168.8.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.8.0/24 is directly connected, GigabitEthernet0/1.80
L    192.168.8.1/32 is directly connected, GigabitEthernet0/1.80
192.168.9.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.9.0/24 is directly connected, GigabitEthernet0/1.90
L    192.168.9.1/32 is directly connected, GigabitEthernet0/1.90
192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
--More-- |
```

Figura 4.6: Interface configurada do Router. Fonte: Autor

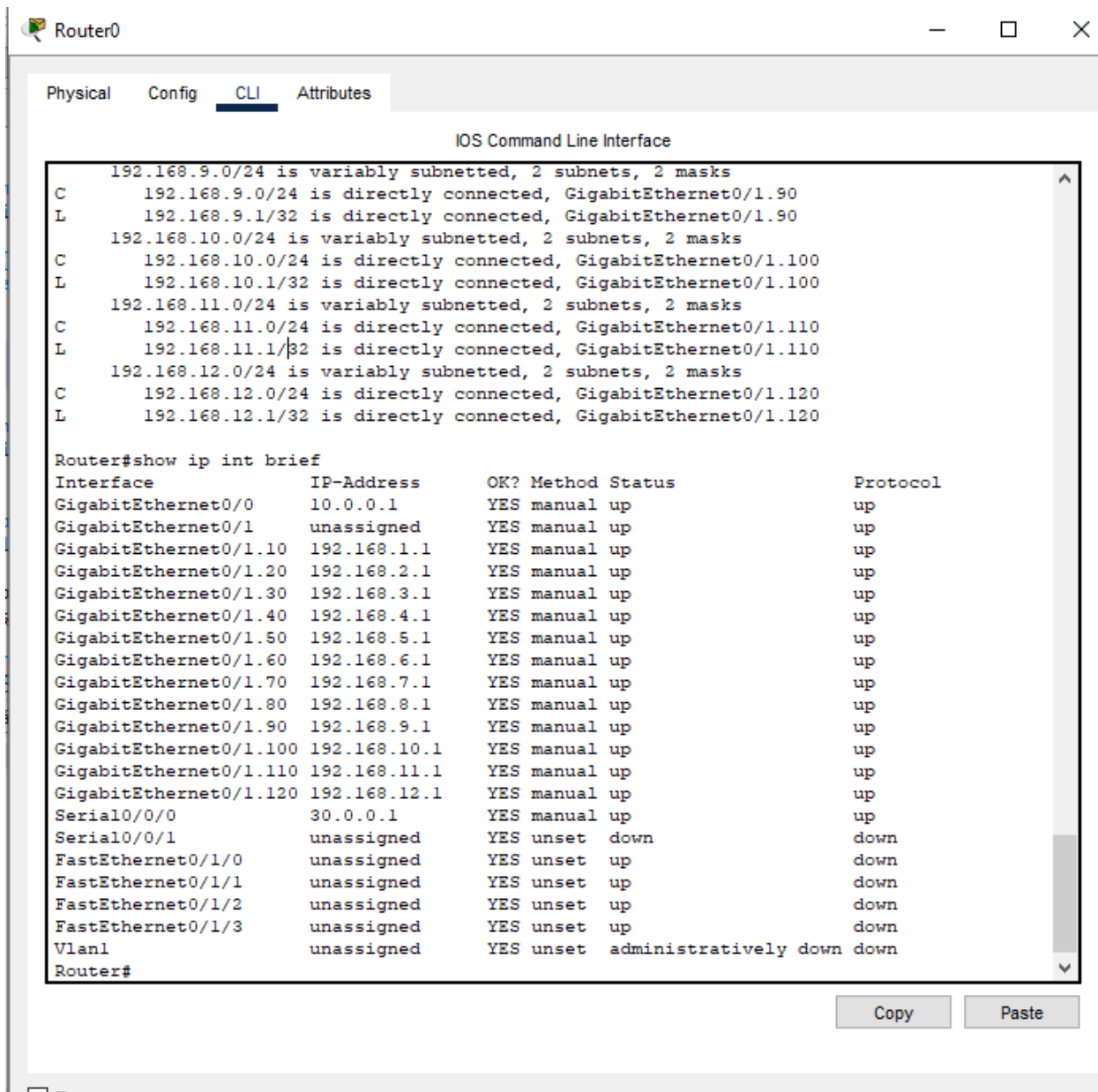


Figura 4.7: Interface configurada do Router "IPs". Fonte: Autor

4.2.5.3 Verificação das VLANs

O resultado do comando "show vlan brief" é mostrado na figura a seguir que indica que as VLANs estão activo, o ID e as portas correspondentes a todas as VLANs atribuída a cada departamento estão activos e trabalhar como esperado.

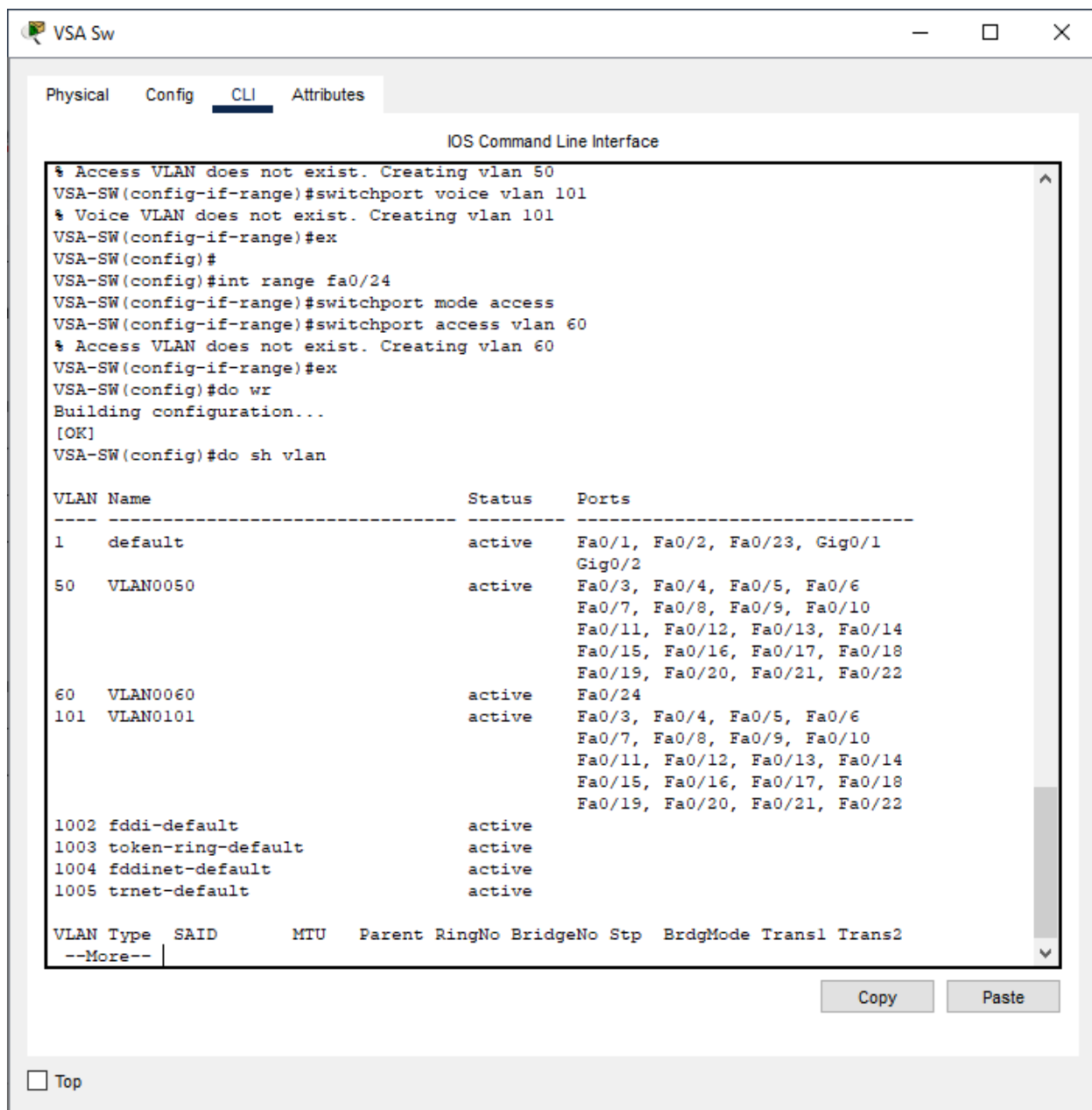


Figura 4.8: VLANs criadas no Switch. Fonte: Autor

4.2.5.4 Verificação do DHCP nos Hosts

A seguir é ilustrado que dispositivo PC1 que recebeu um endereço IP após a ligação à rede, com a VLAN em que estão ligados (configuração feitas nos Switches de acesso).

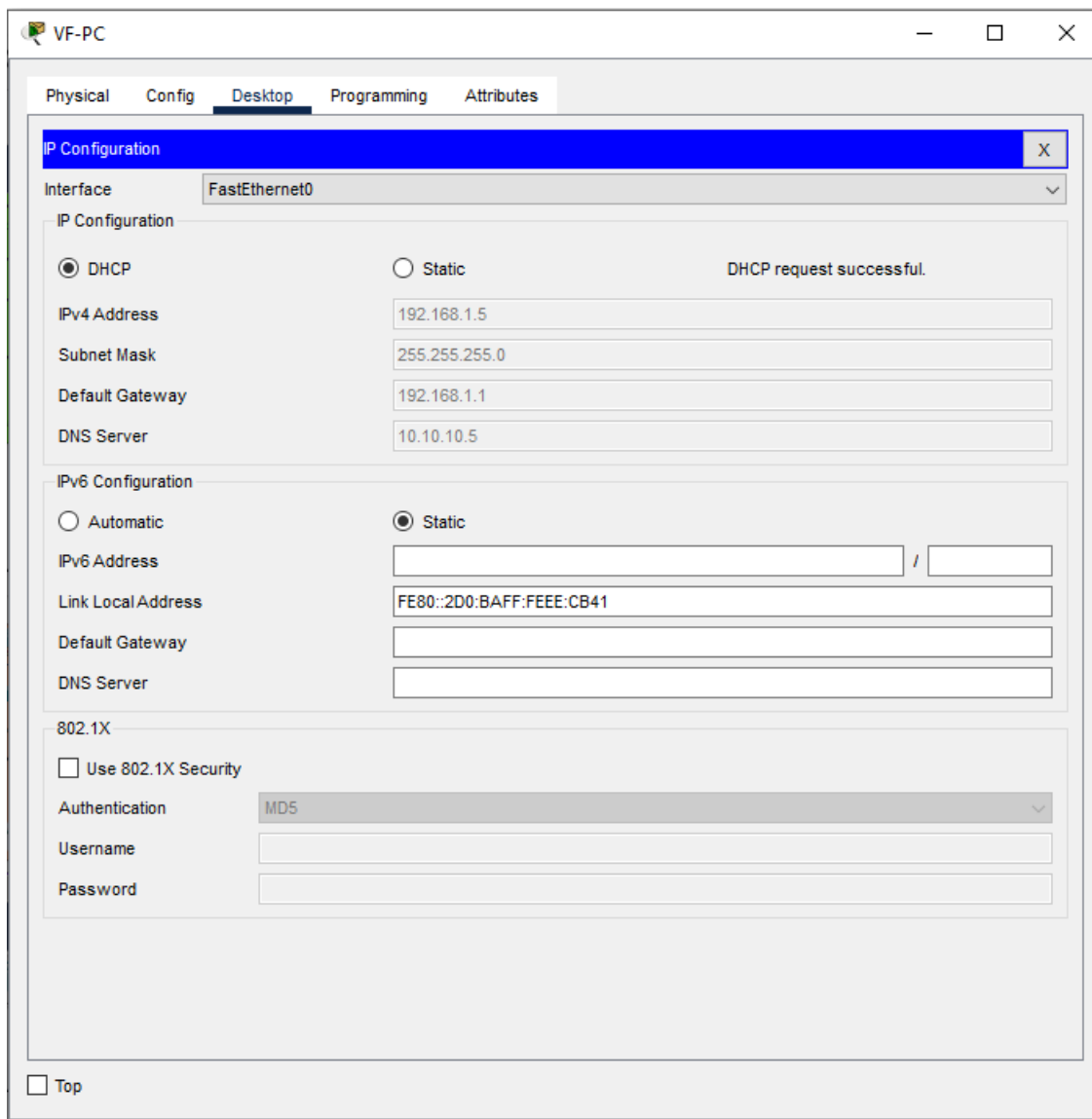
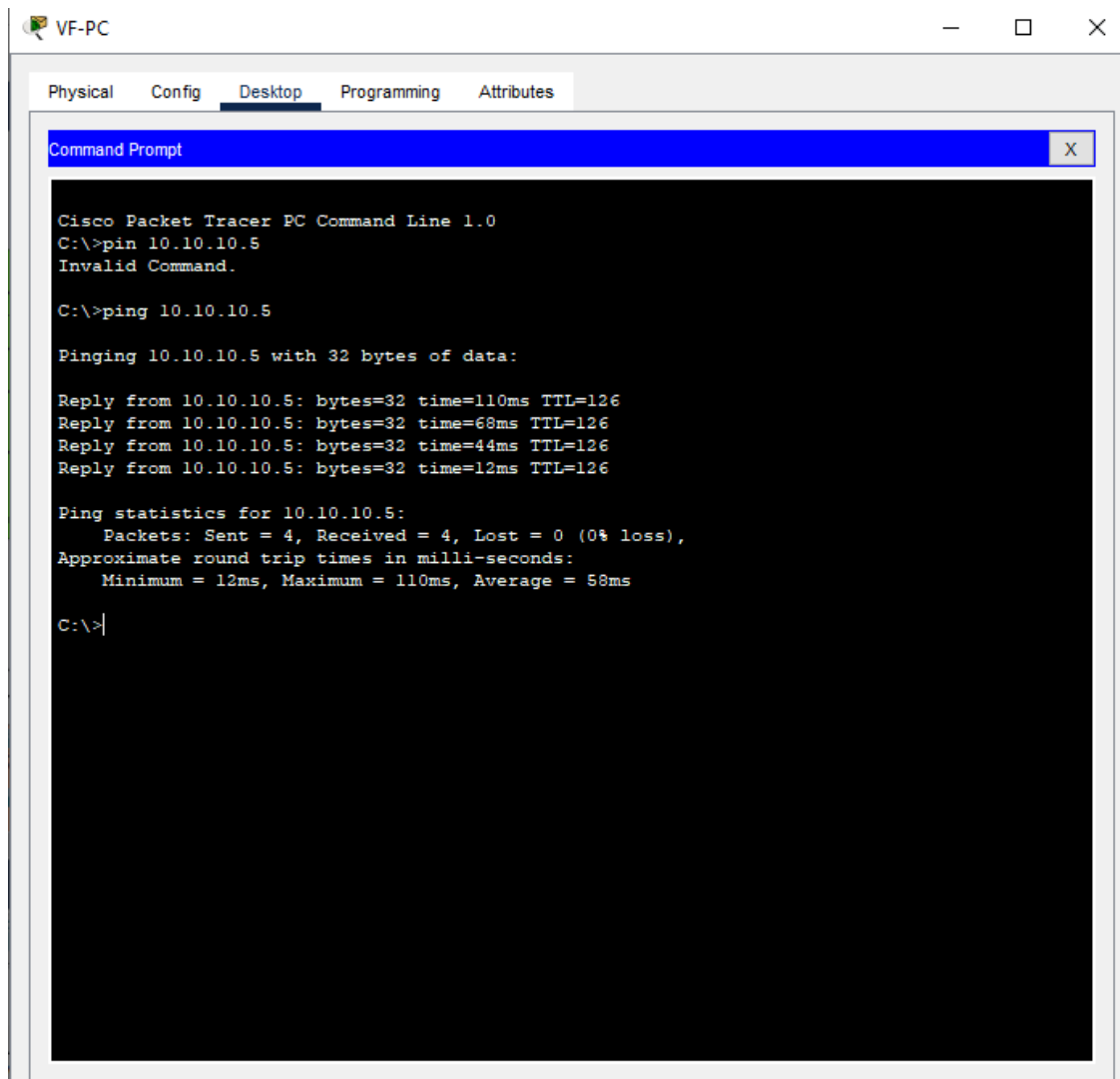


Figura 4.9: Computador da VF recebendo IP via DHCP. Fonte: Autor

A partir acima, é possível notar que o utilizador ligado à rede conseguiu obter dinamicamente o endereço IP de acordo com a VLAN a que o dispositivo do utilizador estava ligado pelo DHCP Server.

4.2.5.5 Teste de Conectividade da Rede

O comando ping foi utilizado para testar a comunicação e a conectividade da rede, com o endereço IP do utilizador, nas 12 VLANs criadas. Figura a seguir mostra os resultados obtidos no teste.



```
Cisco Packet Tracer PC Command Line 1.0
C:\>pin 10.10.10.5
Invalid Command.

C:\>ping 10.10.10.5

Pinging 10.10.10.5 with 32 bytes of data:

Reply from 10.10.10.5: bytes=32 time=110ms TTL=126
Reply from 10.10.10.5: bytes=32 time=68ms TTL=126
Reply from 10.10.10.5: bytes=32 time=44ms TTL=126
Reply from 10.10.10.5: bytes=32 time=12ms TTL=126

Ping statistics for 10.10.10.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 12ms, Maximum = 110ms, Average = 58ms

C:\>|
```

Figura 4.10: Teste de Conectividade. Fonte: Autor

A partir da figura acima é possível verificar que a rede esta bem configurada e que está a funcionar como esperado. Assim, os utilizadores visitantes em qualquer local dentro da área de cobertura poderiam aceder aos recursos na Rede, mas com restrições acesso.

O comando ping foi também utilizado para testar e confirmar se a configuração do servidor estava a funcionar como esperado, a interface de linha de comando foi utilizada para testar a conexão com endereço de servidor, e resultou em conectividade, como o resultado do teste é mostrado.

Com essas implementações de LANs, a rede do CMCM está dividida em 20 redes, sendo que cada uma possui o seu devido serviço. Podendo assim diminuir os atrasos no tráfego na rede, sendo que anteriormente, a rede era somente uma. Quanto a questão de segurança, as redes estão mais seguras, com a proteção de um *firewall*, e no caso de a rede ser atingida por um vírus/*malwere*, so irá atingir uma rede, pois elas estão divididas

por VLAN.

Capítulo 5

Conclusão e Recomendações

5.1 Conclusão

A pesquisa teve como principal objectivo apresentar um projecto de rede para o melhoramento da infraestrutura de rede local do CMCM. A pesquisa conduziu a concepção de uma rede estruturada que, para além da sua catalogação, a sua concepção poderá melhorar o tráfego de dados, assim como a segurança da mesma, internamente através da utilização de VLANs e externamente (na periferia da internet) através da utilização de *firewall* e o DMZ (Zona Desmilitarizada), permitindo deste modo o acesso a rede a todos utentes com eficácia e segurança.

Foi possível alcançar o primeiro objectivo específico desse trabalho, porque foram identificados os principais componentes de rede baseado no levantamento teórico e na investigação das características da rede que foi feita a nível local do CMCM.

Para o alcance do segundo objectivo específico, dimensionamento da rede tendo em conta os aspectos de segurança baseou-se nas características de rede identificados, para ter uma maior clareza a respeito de como identificar os mecanismos para alcance do objectivo geral tendo em conta os aspectos de segurança, em especial nesse trabalho propôs-se a implementação de segmentação da rede e uso de *firewal* e servidores.

Nesse contexto, o uso de VLANs possibilitou uma melhor organização da rede, criando VLANs para cada vereação ou partição da instituição, proporciona maior desempenho, visto que cada VLAN trafega no seu próprio domínio de *broadcast* desfazendo assim, um e único domínio de *broadcast* para toda rede, o que aumenta a segurança, pois evita que usuários de um sector possa acessar a rede de outros sectores. A segmentação da infraestrutura de rede proposta foi simulada na ferramenta **Cisco Packet Tracer** e durante

a realização dos testes foi possível verificar que cada utilizador ligado à rede conseguiu obter conectividade aos dispositivos contidos no mesmo domínio de *broadcast* (mesma VLAN).

Foi alcançado o terceiro objectivo específico, através da informação colhida na instituição através de levantamento dos equipamentos de rede em utilização na actual infraestrutura existente e fazendo uma avaliação do material necessário para a proposta.

E os resultados foram satisfatórios. Feita a segmentação da rede conclui-se que rede melhor segmentada vai trazer melhor desempenho porque uma vez que ela está dividida vai reduzir o excessivo tráfego de *broadcast*.

Foram realizados testes (montagem experimental), a proposta do orçamento foi produzido por via do *procurment* realizado online no mercado nacional e internacional em mercados virtuais.

Em suma, foi possível concluir que a administração duma rede é uma tarefa indispensável para qualquer instituição que possui uma rede de computadores e não só, assim como é possível afirmar que os objectivos deste projecto foram alcançados, na medida em que, foi possível desenvolver uma proposta de melhoria da estrutura lógica e física da rede do CMCM, e mostrar que com a segmentação de rede, é essencial para o bom funcionamento, administração, melhor desempenho e maior segurança, fazendo com que os administradores de rede controle da melhor forma possível.

5.1.1 Limitação

A proposta deverá ser apresentada a instituição para uma possível aplicação, entretanto a maior limitação nesta fase da proposta é falta de planeamento pela instituição para a implementação projecto proposto para o ano de 2025, segundo o seu Plano Anual e Orçamento de 2025 (PAO 2025), tendo em conta que para a aplicação ou contratação desse tipo de projecto para empresas ou instituições públicas, seguem vários protocolos administrativos para concepção de serviços ou produtos, entre eles o lançamento de concurso públicos entre tratamentos jurídicos, etc.

Tendo como exemplo a publicação da intenção de concepção de uma rede, no jornal de maior circulação no país, para que empresas da área (de redes) apresentem suas propostas (projectos de redes) para a concepção, portanto este projecto, limita-se em ambiente de simulação.

5.2 Recomendações

Acredita-se, que este trabalho vai proporcionar algumas contribuições aos meios académicos, a instituição e oferece diversas oportunidades para continuação de seu desenvolvimento.

As recomendações para um aperfeiçoamento deste projecto são:

-Extender a rede para o uso das plataformas da internet das coisas (IoT), possibilitando o monitoramento de dispositivos tais como ar-condicionado, impressoras, CCTV etc.;

-Configuração adicional pode ser implementada na rede para permitir a videoconferência além das funcionalidades VoIP presentes no projecto apresentado, para substituição dos sistema actualmente usados para comunicação de voz (PBX) disponíveis;

-Utilização de um sistema de monitoramento da rede para que seja possível verificar prováveis baixas em links e resolver a tempo, aviso em caso de intrusão indevida entre outros serviços que os a monitoração da rede pode oferecer.

Referências Bibliográficas

- [1] Alves, M. d. P., 2012. Metodologia Científica. Escolar editora, Lisboa.
- [2] DEL-MASSO, M.; COTTA, M.; SANTOS, M. 2014 -Ética em Pesquisa Científica: conceitos e finalidades. UNESP. São Paulo.
- [3] Faculdade de Engenharia. 2009 -Regulamento de culminação de estudos nos cursos de engenharia. UEM. Maputo.
- [4] Lakatos, E. Marconi, M. 2003 -Fundamentos de metodologia científica. Editora Atlas. 5ª edição. São Paulo.
- [5] CISCO. (7 de 09 de 2023). Configuring VLANs. Obtido em 7 de 09 de 2023, do site da CISCO: <https://www.cisco.com/c/en/us/td/docs/switches/datacenter2>
- [6] Miranda, A. (2008). Introdução a Rede de Computadores. Vila Velha: ESAB – Escola Superior Aberta do Brasil.
- [7] Monteiro, E., e Boavida, F. (2011). Engenharia de Redes Informáticas. Lisboa: Lisboa FCA 2011.
- [8] Tanenbaum, A. S., e Wetherall, D. (2011). Redes de computadores Quarta edição. São Paulo: Pearson Prentice Hall.
- [9] Bellovin, S., e Cheswick, W. (2009). Network Firewalls- Firewalls (barriers between two. Em S. Bellovin, e W. Cheswick, Network Firewalls- Firewalls (barriers between two (pag. 50-58). Califórnia: IEEE Communications Magazine.
- [10] Cisco Systems, U. (s.d.). Cisco Certified Network Associate (CCNA-RS) Routing and Switching Training Manual on Network Protocols and Communications. Cisco Systems, 1-48.
- [11] Comer, D. E. (2000). Internetworking with TCP/IP Principles, Protocols, And Architecture. New Jersey: Prentice Hall.
- [12] Dantas, M. A. (2005). Computação distribuída de alto desempenho. São Paulo: Axcel Books. de Magalhães Dias Frinhani, R. (2005). Projeto de Reestruturação do Gerenciamento e Otimização da Rede Computacional da Universidade Federal de Lavras. Lavras: Universidade Federal de Lavras.
- [13] Forouzan, B. A. (2006). Comunicação de dados e Redes de computadores. Rio: Bookman.
- [14] JSTECH Training, C. (19 de 09 de 2023). JSTECH. Obtido de JSTECH Training Center: <https://jstech.com.ng/metropolitan-area-network-man/>
- [15] Kurose, J. F., e Ross, K. W. (2014). Redes de Computadores e a Internet (6ª ed.). Chicago: Pearson.

- [16] Miranda, A. (2008). Introdução a Rede de Computadores. Vila Velha: ESAB Escola Superior Aberta do Brasil.
- [17] Cruz, M. Cableado Estructurado. Obtenido de <http://4.bp.blogspot.com>
- [18] ELECTRÓNICA. (2010). Cableado estructurado de Redes. Obtido de <http://www.electronica.com>.
- [19] ITU:<https://www.itu.int/rec/dologin-pub.asp> Acesso a 17 de Setembro de 2023
- [20] Metalco. (2014). Obtido de <http://www.metalco.net/largos-tuberia-emt.php>
- [21] PANDUIT. (2011). CCNA SUPLEMENTO CABLEADO ESTRUCTURADO. Obtido de <http://www.panduit.com/es/products-and-services/products/routing-and-pathways>
- [23] SIEMON. Normativas. Obtido em <http://www.siemon.com/us/standards/1327-TIA-569-B.asp>
- [24] UNITEL. (2014). NORMATIVAS. Obtido em <http://unitel-tc.com/normas-sobre-cabeado-estructurado/>
- [25] Prentice-Hall (2002), Computer Networks, 4ta Edición, Tanenbaum, Andrew S, Madrid-Espana.
- [26] COMER, Douglas E. Redes de computadores e internet. Porto Alegre: Bookman, 2007. 85-60031367.

Anexos

Anexo 1

Pedido, Resposta e Ficha de Avaliação do Estágio Profissional.

Exm^{as}. Senhores

CONSELHO MUNICIPAL DA CIDADE DA MATOLA (CMCM)

M A P U T O

Sua Referência: Sua Comunicação de: Nossa Referência: Maputo
FE-001/2025 05/03/2025

Assunto: Solicitação de vaga de estágio Profissional — César Tomás Ferrei

O Estágio Profissional dos Cursos de Engenharia é uma das formas alternativas de culminação de estudos, assim como o Trabalho de Licenciatura. A culminação do curso deve ser de forma a garantir a aplicação globalizante dos conhecimentos adquiridos ao longo do mesmo e permite ao estudante demonstrar a capacidade de investigação e inovação adquirida durante a formação.

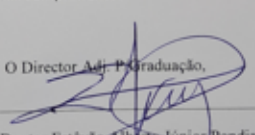
O Estágio Profissional é uma disciplina curricular sendo parte integrante do processo de formação do estudante. Realiza-se nas empresas/instituições ou organizações sociais desenvolvendo actividades na área de Engenharia, em qualquer dos dois semestres lectivos definidos no Calendário Académico da Universidade Eduardo Mondlane. Seu objectivo é dotar o estudante finalista de alguma experiência profissional, promover o seu primeiro contacto com a prática profissional e de desenvolver nele habilidades e atitude positiva no exercício de actividades práticas de engenharia. Assim, é vedada a frequência simultânea do Estágio Profissional com qualquer outra disciplina do curso, para permitir a integração plena do estudante na vida laboral. Neste contexto, é imprescindível para a Faculdade, o parecer da Empresa após o estágio, sobre o desenvolvimento do estudante.

O Estágio Profissional está previsto para o período de entre 3 à 4 meses a contar da data de início do Estágio. É de salientar que a atribuição de subsídio ao estudante estagiário é facultativa e da responsabilidade exclusiva da empresa, devendo obedecer às regras vigentes em cada empresa.

Neste contexto, vimos por este meio solicitar vaga para o estudante-finalista do curso de Engenharia Electrónica-Laboral. Informação adicional poderá ser adquirida através do número: 21 478100 Ext. 2072 (secretária: Sr^a Amélia Timbe) ou por e-mail, amelia.timbe@gmail.com.

Cientes da atenção que será dispensada ao assunto, antecipadamente agradecemos e aproveitamos a oportunidade para endereçar os nossos cumprimentos.

Atenciosamente.

O Director Adj. P. Graduação,

Prof. Doutor Estêvão Alberto Júnior Pondja, Eng^o
(Professor Auxiliar)

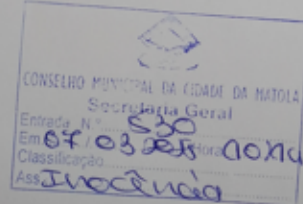


Figura 1.1: Pedido do Estágio Profissional, Fonte: Autor



CONSELHO MUNICIPAL DA CIDADE DA MATOLA
ADMINISTRAÇÃO MUNICIPAL E RECURSOS HUMANOS

GUIA DE MARCHA Nº 19 /025.5/ CMCM/AMRH/25.

- - - Segue a apresentar-se no Departamento de Património da Vereação de Administração e Finanças, o senhor **César Tomás Ferroi**, estudante do curso do curso do curso de Licenciatura em *Engenharia Eletrónica*, onde irá prestar o estágio pré profissional no período de (03) três meses, com início a partir do dia 17 de Março de 2025. -----

Matola, aos 12 de Março de 2025

A Secretária Municipal

Deolinda Moiane
Sec. Supl.



Figura 1.2: Guia de Apresentação, Fonte: Autor



CONSELHO MUNICIPAL DA CIDADE DA MATOLA
ADMINISTRAÇÃO MUNICIPAL E RECURSOS HUMANOS

CERTIFICADO DE ESTÁGIO PROFISSIONAL.

Certifica-se que **César Tomás Ferroi**, natural da Matola, nascido aos 14 de Junho de 1997, portador do BI nº 110101619852P, emitido pelo Arquivo de Identificação Civil da Cidade da Matola, aos 07 de Julho de 2023, estudante do curso de **Engenharia Electrónica**, concluiu no Serviço de Tecnologias de Informação e Comunicação do Departamento do Património, na Vereação de Administração e Finanças, o estágio pré-profissional, aprovado pelo Decreto nº 95/2021 de 23 de Dezembro, em contexto real de trabalho, que decorreu de 17 de Março de 2025 a 17 de Junho de 2025, tendo obtido aproveitamento: **Muito Bom.**

Matola, aos 27 de Junho de 2025

A Secretária Municipal

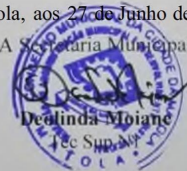


Figura 1.3: Ficha de Avaliação do Estágio Profissional, Fonte: Autor

Anexo 2

Configurações e Comandos

```
ciscoasa#CONF T
ciscoasa(config)#hostname PERIMETRO-FW
PERIMETRO-FW(config)#enable password cmcm
PERIMETRO-FW(config)#username cmcm password cmcm
PERIMETRO-FW(config)#domain-name cmcm.net
PERIMETRO-FW(config)#wr mem
Building configuration...
Cryptochecksum: 528955c7 644elf22 6dda2cca 349f3d60

1221 bytes copied in 2.457 secs (496 bytes/sec)
[OK]
PERIMETRO-FW(config)#
```

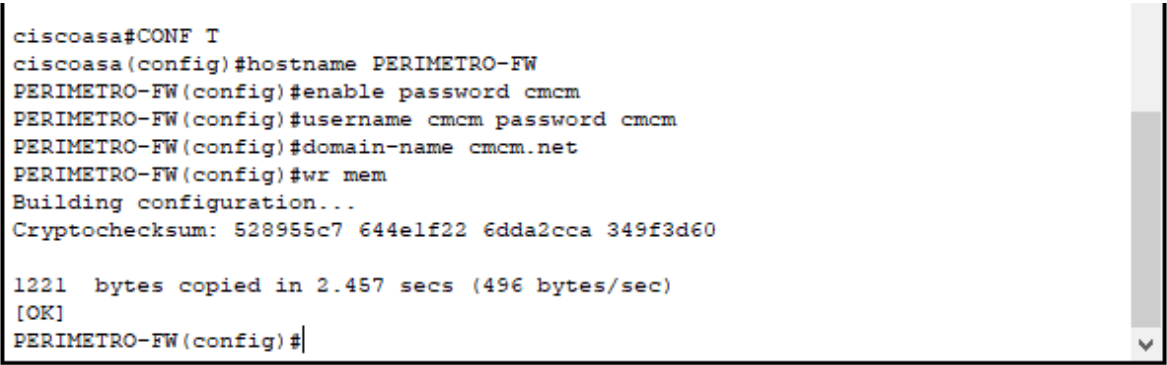


Figura 2.1: Configuração Básica do Firewall. Fonte: Autor

Configuração do Router

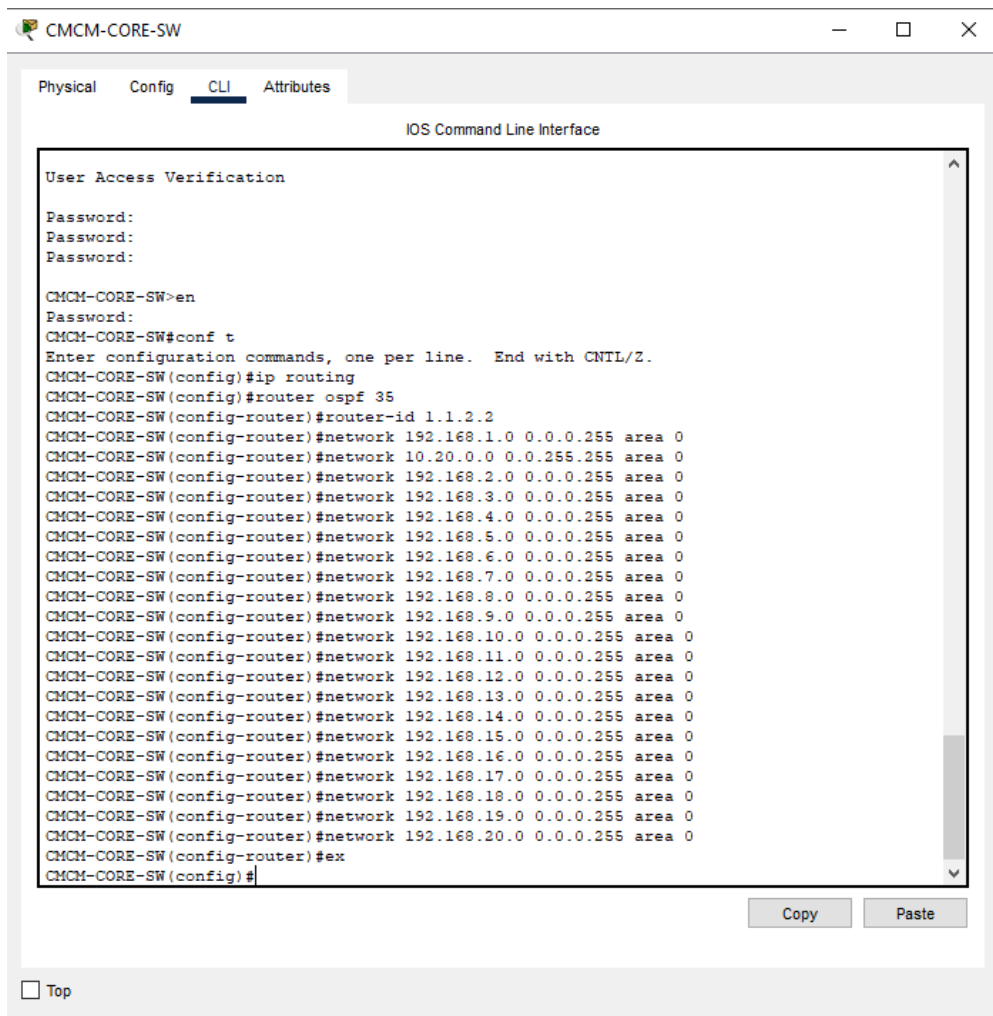


Figura 2.2: Atribuição de IPs e definição das Rotas. Fonte: Autor

```
PERIMETRO-FW(config-network-object)#subnet 192.168.17.0 255.255.255.0
PERIMETRO-FW(config-network-object)#nat (INSIDE,OUTSIDE) dynamic interface
PERIMETRO-FW(config-network-object)#ex
PERIMETRO-FW#conf t
PERIMETRO-FW(config)#object network INSIDE-OUT11
PERIMETRO-FW(config-network-object)#subnet 192.168.19.0 255.255.255.0
PERIMETRO-FW(config-network-object)#nat (INSIDE,OUTSIDE) dynamic interface
PERIMETRO-FW(config-network-object)#ex
PERIMETRO-FW#conf t
PERIMETRO-FW(config)#object network INSIDE-OUT22
PERIMETRO-FW(config-network-object)#subnet 192.168.19.0 255.255.255.0
PERIMETRO-FW(config-network-object)#nat (INSIDE,OUTSIDE) dynamic interface
PERIMETRO-FW(config-network-object)#ex
PERIMETRO-FW#conf t
PERIMETRO-FW(config)#object network INSIDE-OUT23
PERIMETRO-FW(config-network-object)#subnet 192.168.20.0 255.255.255.0
PERIMETRO-FW(config-network-object)#nat (INSIDE,OUTSIDE) dynamic interface
PERIMETRO-FW(config-network-object)#ex
PERIMETRO-FW#wr mem
Building configuration...
Cryptochecksum: 617443f8 67311329 2c8b2df5 10b60466

3631 bytes copied in 1.69 secs (2148 bytes/sec)
[OK]
PERIMETRO-FW#
PERIMETRO-FW#conf t
PERIMETRO-FW(config)#route OUTSIDE 0.0.0.0 0.0.0.0 197.200.100.1
PERIMETRO-FW(config)#access-list INSIDE-DMZ extended permit icmp any any
PERIMETRO-FW(config)#access-list INSIDE-DMZ extended permit udp any any eq 67
PERIMETRO-FW(config)#access-list INSIDE-DMZ extended permit udp any any eq 68
PERIMETRO-FW(config)#access-list INSIDE-DMZ extended permit udp any any eq 53
PERIMETRO-FW(config)#access-list INSIDE-DMZ extended permit tcp any any eq 53
PERIMETRO-FW(config)#access-list INSIDE-DMZ extended permit tcp any any eq 80
PERIMETRO-FW(config)#access-list INSIDE-DMZ extended permit tcp any any eq 8080
PERIMETRO-FW(config)#access-list INSIDE-DMZ extended permit tcp any any eq 443
PERIMETRO-FW(config)#access-list INSIDE-DMZ extended permit tcp any any eq 9443
PERIMETRO-FW(config)#
```

Figura 2.3: Configuração de acessos. Fonte: Autor

The screenshot shows a window titled "PERIMETRO-FW" with tabs for "Physical", "Config", "CLI", and "Attributes". The "CLI" tab is active, displaying the "IOS Command Line Interface". The terminal output shows the following commands and responses:

```
PERIMETRO-FW(config)#int gig1/2
PERIMETRO-FW(config-if)#no shut

PERIMETRO-FW(config-if)#nameif DMZ
INFO: Security level for "DMZ" set to 0 by default.
PERIMETRO-FW(config-if)#security-level 70
PERIMETRO-FW(config-if)#ip add 10.10.10.1 255.255.255.240
PERIMETRO-FW(config-if)#ex
PERIMETRO-FW(config)#int gig1/3
PERIMETRO-FW(config-if)#no shut

%LINK-5-CHANGED: Interface GigabitEthernet1/3, changed state to down
PERIMETRO-FW(config-if)#nameif OUTSIDE
INFO: Security level for "OUTSIDE" set to 0 by default.
PERIMETRO-FW(config-if)#security-level 0
PERIMETRO-FW(config-if)#ip add 197.200.100.2 255.255.255.252
PERIMETRO-FW(config-if)#ex
PERIMETRO-FW(config)#wr mem
Building configuration...
Cryptochecksum: 617443f8 67311329 2c8b2df5 10b60466

1279 bytes copied in 1.492 secs (857 bytes/sec)
[OK]
PERIMETRO-FW(config)#router ospf 35
PERIMETRO-FW(config-router)#router-id 1.1.3.3
PERIMETRO-FW(config-router)#network 10.30.30.0 255.255.255.252 area 0
PERIMETRO-FW(config-router)#network 10.10.10.0 255.255.255.240 area 0
PERIMETRO-FW(config-router)#network 197.200.100.0 255.255.255.252 area 0
PERIMETRO-FW(config-router)#ex
PERIMETRO-FW(config)#do wr
PERIMETRO-FW(config)#wr mem
Building configuration...
Cryptochecksum: 617443f8 67311329 2c8b2df5 10b60466

1457 bytes copied in 2.504 secs (581 bytes/sec)
[OK]
PERIMETRO-FW(config)#
```

At the bottom of the window, there are "Copy" and "Paste" buttons, and a "Top" button with a checkbox.

Figura 2.4: Roteamento no Firewall Fonte: Autor

```
PERIMETRO-FW(config)#object network INSIDE-OUT2
PERIMETRO-FW(config-network-object)#subnet 10.20.0.0 255.255.0.0
PERIMETRO-FW(config-network-object)#nat (INSIDE,OUTSIDE) dynamic interface
PERIMETRO-FW(config-network-object)#EX
PERIMETRO-FW#conf t
PERIMETRO-FW(config)#object network INSIDE-OUT3
PERIMETRO-FW(config-network-object)#subnet 10.10.10.0 255.255.255.240
PERIMETRO-FW(config-network-object)#nat (DMZ, OUTSIDE) dynamic interface
PERIMETRO-FW(config-network-object)#ex
PERIMETRO-FW#wr mem
Building configuration...
Cryptochecksum: 528955c7 644e1f22 6dda2cca 349f3d60

1745 bytes copied in 2.531 secs (689 bytes/sec)
[OK]
PERIMETRO-FW# conf t
PERIMETRO-FW(config)#route OUTSIDE 0.0.0.0 0.0.0.0 197.200.100.1
PERIMETRO-FW(config)#access-list INSIDE-DMZ extended permit icmp any any
PERIMETRO-FW(config)#access-list INSIDE-DMZ extended permit udp any any 67
^
% Invalid input detected at '^' marker.

PERIMETRO-FW(config)#access-list INSIDE-DMZ extended permit udp any any eq 67
PERIMETRO-FW(config)#access-list INSIDE-DMZ extended permit udp any any eq 68
PERIMETRO-FW(config)#access-list INSIDE-DMZ extended permit udp any any eq 57
PERIMETRO-FW(config)#access-list INSIDE-DMZ extended permit tcp any any eq 53
PERIMETRO-FW(config)#access-list INSIDE-DMZ extended permit udp any any eq 53
PERIMETRO-FW(config)#access-list INSIDE-DMZ extended permit tcp any any eq 80
PERIMETRO-FW(config)#access-list INSIDE-DMZ extended permit tcp any any eq 8080
PERIMETRO-FW(config)#access-list INSIDE-DMZ extended permit tcp any any eq 443
PERIMETRO-FW(config)#access-list INSIDE-DMZ extended permit tcp any any eq 8443
PERIMETRO-FW(config)#access-group INSIDE-DMZ in interface DMZ
PERIMETRO-FW(config)#ex
PERIMETRO-FW#wr mem
Building configuration...
Cryptochecksum: 528955c7 644e1f22 6dda2cca 349f3d60
```

Figura 2.5: Configuração da DMZ Fonte: Autor

The screenshot shows a terminal window titled "PERIMETRO" with tabs for "Physical", "Config", "CLI", and "Attributes". The "CLI" tab is active, displaying the "IOS Command Line Interface". The terminal output shows the following commands and responses:

```
PERIMETRO-FW(config-if)#no shut
%LINK-5-CHANGED: Interface GigabitEthernet1/3, changed state to down
PERIMETRO-FW(config-if)#nameif OUTSIDE
INFO: Security level for "OUTSIDE" set to 0 by default.
PERIMETRO-FW(config-if)#security-level 0
PERIMETRO-FW(config-if)#ip add 197.200.100.2 255.255.255.252
PERIMETRO-FW(config-if)#EX
PERIMETRO-FW(config)#do wr
PERIMETRO-FW(config)#WR MEM
Building configuration...
Cryptochecksum: 528955c7 644e1f22 6dda2cca 349f3d60

1273 bytes copied in 1.522 secs (836 bytes/sec)
[OK]
PERIMETRO-FW(config)#router ospf 35
PERIMETRO-FW(config-router)#router-id 1.1.3.3
PERIMETRO-FW(config-router)#network 10.30.30.0 0.0.0.3 area
% Incomplete command.
PERIMETRO-FW(config-router)#network 10.30.30.0 0.0.0.3 area 0
% OSPF: Invalid address/mask combination
PERIMETRO-FW(config-router)#ex
PERIMETRO-FW(config)#do wr
PERIMETRO-FW(config)#router ospf 35
PERIMETRO-FW(config-router)#router-id 1.1.3.3
PERIMETRO-FW(config-router)#network 10.30.30.0 255.255.255.252 area 0
PERIMETRO-FW(config-router)#network 10.10.10.0 255.255.255.240 area 0
PERIMETRO-FW(config-router)#network 197.200.100.0 255.255.255.252 area
% Incomplete command.
PERIMETRO-FW(config-router)#network 197.200.100.0 255.255.255.252 area 0
PERIMETRO-FW(config-router)#ex
PERIMETRO-FW(config)#do wr
PERIMETRO-FW(config)#wr
PERIMETRO-FW(config)#
% Invalid input detected at '^' marker.

PERIMETRO-FW(config)#
```

At the bottom of the terminal window, there are "Copy" and "Paste" buttons, and a "Top" button.

Figura 2.6: Interface configurada do Router. Fonte: Autor

Configuração do Switch de Distribuição (Multilayer)

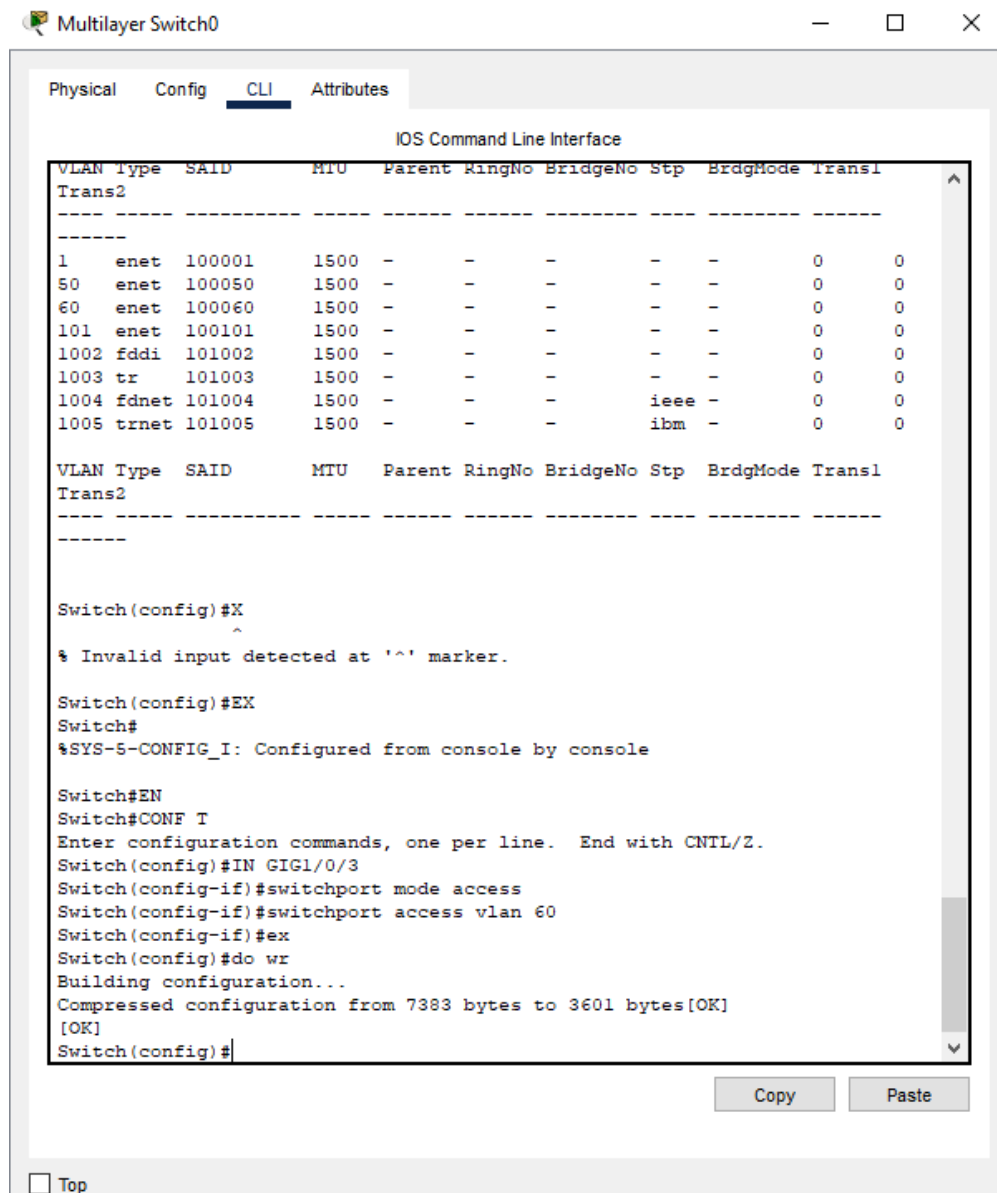


Figura 2.7: Configuração do modo de acesso e indicação da direção do DHCP para os hosts Fonte: Autor

Configuração do Switch de Acesso

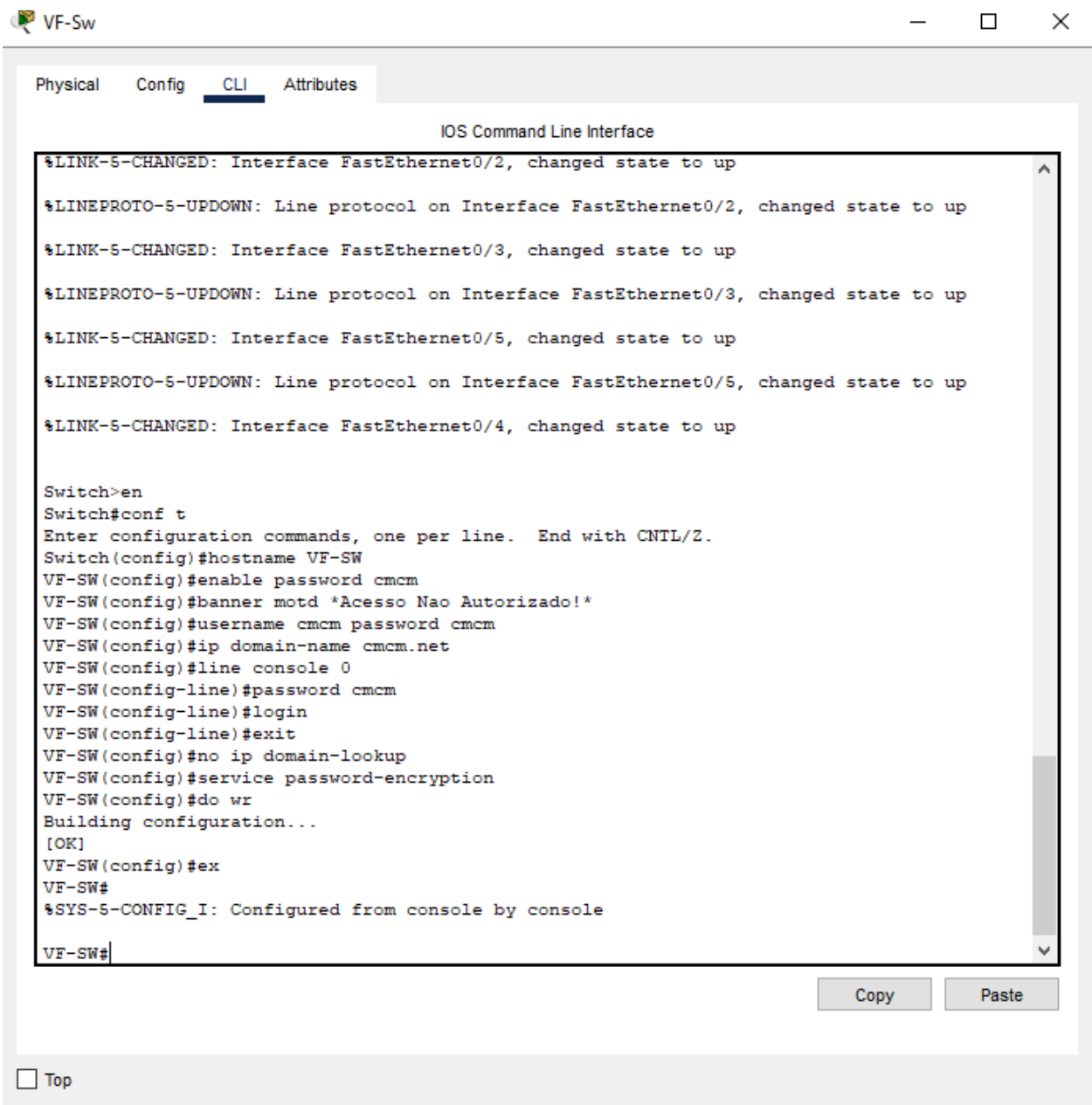
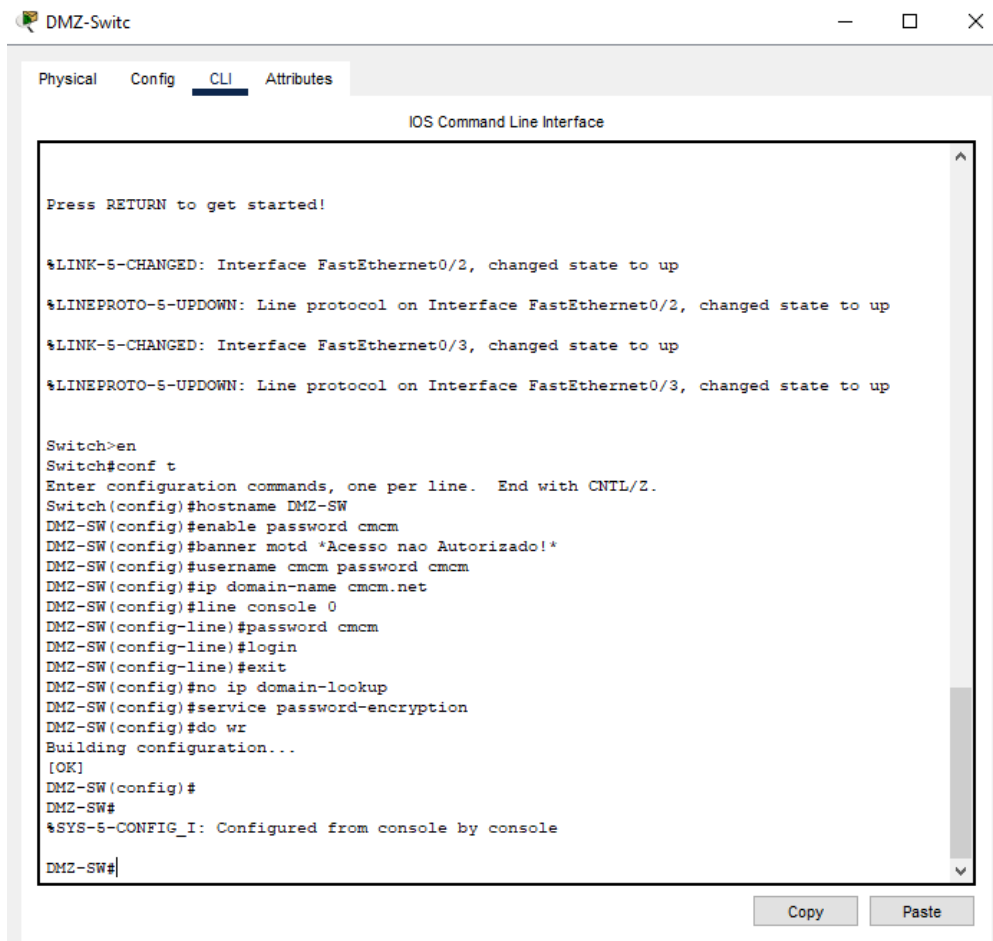


Figura 2.8: Configuração do Switch da Vereação de Finanças. Fonte: Autor



The screenshot shows a window titled "DMZ-Switic" with a tabbed interface. The "CLI" tab is active, displaying the "IOS Command Line Interface". The terminal output shows the following sequence of commands and responses:

```
Press RETURN to get started!

%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up

Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTRL/Z.
Switch(config)#hostname DMZ-SW
DMZ-SW(config)#enable password cmcm
DMZ-SW(config)#banner motd ^Acesso nao Autorizado!*
DMZ-SW(config)#username cmcm password cmcm
DMZ-SW(config)#ip domain-name cmcm.net
DMZ-SW(config)#line console 0
DMZ-SW(config-line)#password cmcm
DMZ-SW(config-line)#login
DMZ-SW(config-line)#exit
DMZ-SW(config)#no ip domain-lookup
DMZ-SW(config)#service password-encryption
DMZ-SW(config)#do wr
Building configuration...
[OK]
DMZ-SW(config)#
DMZ-SW#
%SYS-5-CONFIG_I: Configured from console by console

DMZ-SW#
```

At the bottom right of the terminal window, there are "Copy" and "Paste" buttons.

Figura 2.9: Configuração básica do Switch da DMZ. Fonte: Autor

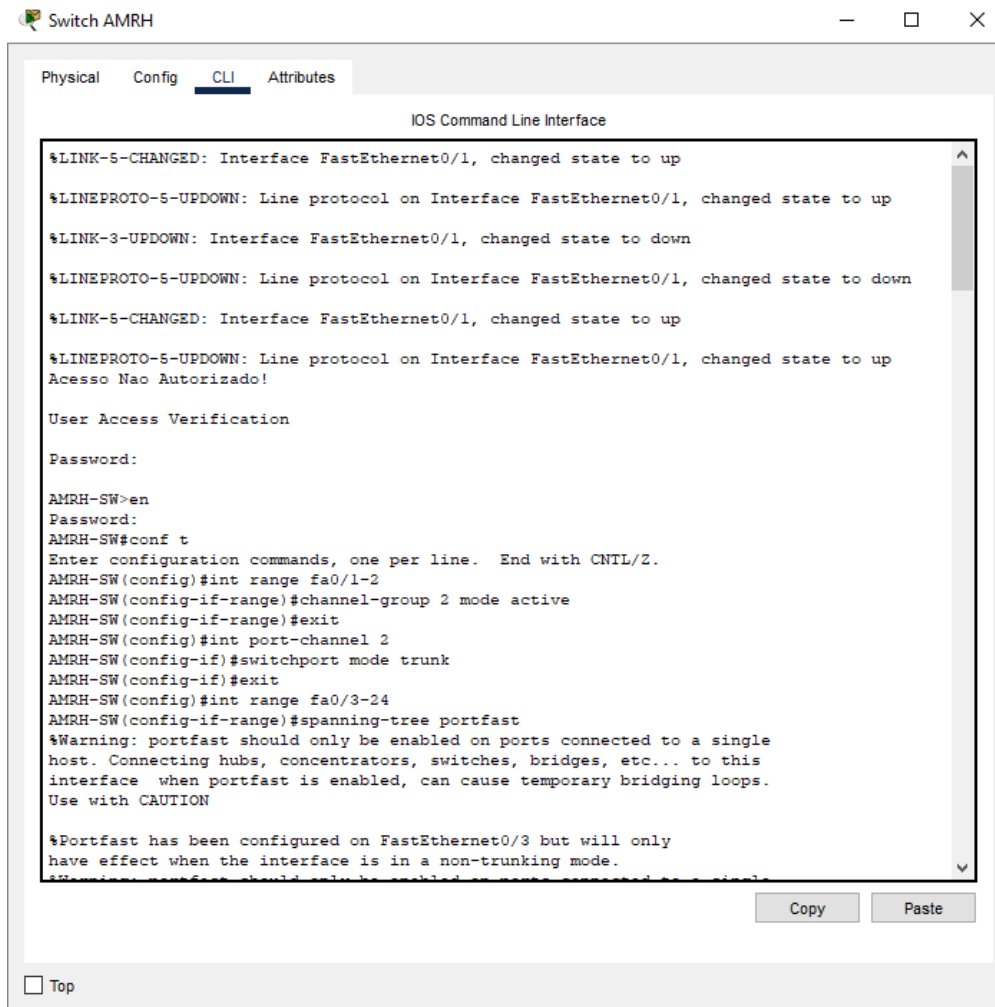


Figura 2.10: Configuração de de portas Trunk no Switch Fonte: Autor

```
PERIMETRO-FW>en
Password:
PERIMETRO-FW#conf t
PERIMETRO-FW(config)#int gig1/1
PERIMETRO-FW(config-if)#no shut

PERIMETRO-FW(config-if)#nameif INSIDE
INFO: Security level for "INSIDE" set to 0 by default.
PERIMETRO-FW(config-if)#security-level 100
PERIMETRO-FW(config-if)#ip add 10.30.30.1 255.255.255.252
PERIMETRO-FW(config-if)#ex
PERIMETRO-FW(config)#int gig1/2
PERIMETRO-FW(config-if)#no shut

PERIMETRO-FW(config-if)#nameif DMZ
INFO: Security level for "DMZ" set to 0 by default.
PERIMETRO-FW(config-if)#security-level 70
PERIMETRO-FW(config-if)#ip add 10.10.10.1 255.255.255.240
PERIMETRO-FW(config-if)#EX
PERIMETRO-FW(config)#INT GIG1/3
PERIMETRO-FW(config-if)#NO SHUT

%LINK-5-CHANGED: Interface GigabitEthernet1/3, changed state to down
PERIMETRO-FW(config-if)#nameif OUTSIDE
INFO: Security level for "OUTSIDE" set to 0 by default.
PERIMETRO-FW(config-if)#security-level 0
PERIMETRO-FW(config-if)#ip add 197.200.100.2 255.255.255.252
PERIMETRO-FW(config-if)#EX
PERIMETRO-FW(config)#DO WR
PERIMETRO-FW(config)#WR MEM
Building configuration...
Cryptochecksum: 528955c7 644e1f22 6dda2cca 349f3d60

1273 bytes copied in 1.522 secs (836 bytes/sec)
[OK]
PERIMETRO-FW(config)#
```

Figura 2.11: Configuração de nível de segurança da Firewall Fonte: Autor

Configuracao do Firewall