Universidade Eduardo Mondlane

FACULDADE DE ENGENHARIA

LICENCIATURA EM ENGENHARIA INFORMÁTICA

Proposta de Reestruturação e Modernização da Rede de Dados

Caso de Estudo:

Universidade Eduardo Mondlane – Faculdade de Engenharia (DTIC)

AUTOR:

TAMELE, Edson Celso

SUPERVISORES:

Eng.º Délcio Chadreca (**UEM**), **MSc**

dr. Xavier Mahumane (**FEUEM - DTIC**)

Maputo, Junho de 2025

Universidade Eduardo Mondlane

FACULDADE DE ENGENHARIA

CURSO DE ENGENHARIA INFORMÁTICA

Tema: Proposta de Reestruturação e Modernização da Rede de Dados.

Caso de Estudo:

Universidade Eduardo Mondlane - Faculdadede Engenharia (DTIC)

Autor:

TAMELE, Edson Celso

Supervisores:

Eng.º Delcio Chadreca (**UEM**), **MSc**

dr. Xavier Mahumane (**FEUEM - DTIC**)

Maputo, Junho de 2025

Universidade Eduardo Mondlane

Faculdade de Engenharia

Departamento de Engenharia Electrotécnica

CURSO: ENGENHARIA INFORMÁTICA (LABORAL)

TERMO DE ENTREGA DE RELATÓRIO DO TRABALHO DE ESTÁGIO PROFISSIONAL

Declaro que o estudante Edson Celso Tamele entregou no dia ____/06/2025 as 2 cópias do relatório do seu Estágio Profissional com referência:

Intitulado: Proposta de Reestruturação e Modernização da Rede de Dados.

Maputo, _____ de _____ de 2025

A chefe da Secretaria

_____

(Arlete Cucu)

Universidade Eduardo Mondlane

Faculdade de Engenharia

Departamento de Engenharia Electrotécnica

DECLAREÇÃO DE HONRA

Declaro sob compromisso de honra que o presente trabalho é resultado da minha investigação e que foi concebido para ser submetido apenas para a obtenção do grau de Licenciatura em Engenharia Informática na Faculdade de Engenharia da Universidade Eduardo Mondlane.

Maputo, Junho de 2025

O Autor

(Edson Celso Tamele)

Dedicatória

Dedico este trabalho aos meus familiares e amigos, que sempre me apoiaram a dar continuidade aos meus estudos, em especial a minha falecida avó e a minha querida mãe.

Agradecimentos

Em primeiro lugar, agradeço a Deus, pela força, sabedoria e direção em todos os momentos da minha vida acadêmica e pessoal.

À minha família, em especial aos meus pais, pelo sacrifício, apoio incondicional e incentivo constante aos meus estudos, permitindo que eu alcançasse mais esta conquista.

À minha namorada, Daniela Matsinhe, à minha irmã, Florencia Tamele, e aos meus amigos Jacinto Xerinda e Delício Tamele, pelo apoio emocional, motivação e torcida em todos os momentos desta jornada.

Aos meus colegas e companheiros de curso, que estiveram ao meu lado nos desafios acadêmicos, compartilhando conhecimentos e auxílio sempre que necessário. Destaco, em particular: Luís Cossa, Fátima Massicame, Gilvaldo Massunguine, Pedro Madabula, Sara Tivane, Michel Bisqué, Luis Macuvele, Alen Loforte, Aleixandre Chavane, Heronilde Cossa e Carson Ribeirro.

Ao Corpo Docente do Curso de Engenharia Informática, pelo conhecimento transmitido e pela dedicação à nossa formação. Agradeço especialmente ao **Msc. Vali Issufo**, **dra. Bhavika Rugnath**, **Eng.ª Leila Omar**, **Eng.º Ruben Manhiça**, **Eng.ª Ivone Cipriano, Eng.º Felizardo Munguambe** e, de forma muito especial, ao **Eng.º Délcio Chadreca**, pela orientação na escolha do tema, pela supervisão deste trabalho e pelos valiosos ensinamentos ao longo do processo.

Por fim, a todos que, direta ou indiretamente, contribuíram para a realização deste trabalho, o meu sincero reconhecimento.

Epígrafe

“Se soubéssemos o que estamos fazendo, não seria chamado de pesquisa.”

Albert Einstein

Resumo

O presente trabalho propõe um projeto abrangente para modernizar e reforçar a infra-estrutura de tecnologia de informação da FEUEM, estruturado em duas fases estratégicas. Atualmente, a rede enfrenta desafios significativos, como equipamentos obsoletos que comprometem a velocidade, a falta de segmentação em VLANs, a ausência de padronização no cabeamento, a utilização de cabos de categoria 5 (Cat5) com limitações em velocidade, durabilidade e blindagem, e a inexistência de um firewall para garantir a segurança da rede. Para resolver estas questões, a primeira fase do projeto centrar-se-á na documentação detalhada dos ativos de TI, assegurando o alinhamento com os objetivos institucionais, enquanto a segunda fase consistirá na reestruturação prática da infra-estrutura e na modernização da rede. Com estas melhorias, a FEUEM disporá de uma rede mais segura, rápida e escalável, capaz de detectar e neutralizar ameaças em tempo real, oferecendo maior velocidade de internet e uma gestão de TI mais eficiente e organizada.

Palavras-chave: Modernização, Reestruturação, Infra-estrutura de TI, Documentação.

Abstract

This work presents a comprehensive project to modernize and strengthen FEUEM's IT infrastructure, structured into two strategic phases. Currently, the network faces significant challenges, including outdated equipment that slows performance, the lack of VLAN segmentation, unstandardized cabling, the use of Category 5 (Cat5) cables with limitations in speed, durability, and shielding, and the absence of a firewall to ensure network security. To address these issues, the first phase of the project will focus on the detailed documentation of IT assets, ensuring alignment with institutional objectives, while the second phase will involve the practical restructuring and modernization of the infrastructure. With these improvements, FEUEM will have a more secure, faster, and scalable network, capable of detecting and neutralizing threats in real time while providing higher internet speeds and more efficient, organized IT management.

Keywords: Modernization, Restructuring, IT Infrastructure, Documentation.

Índice

Lista de figura

Lista de tabelas

Lista de abreviaturas e acrónimos

ACL	Access Control List
Cat5	Categoria 5
Cat6	Categoria 6
FEUEM	Faculdade de Engenharia da UEM
IEEE	Institute of Electrical and Electronics Engineers
ISO	International Organization for Standardization
ITAM	Information Technology Asset Management
ITIL	Information Technology Infrastructure Library
IoT	Internet of Things
IP	Internet Protocol
LAN	Local Area Network
MAN	Metropolitan Area Network
MPSL	Multiprotocol Label Switching
OSI	Open Systems Interconnection
PAN	Personal Area Network
PoE	Power over Ethernet
QoS	Quality of Service
RSTP	Rapid Spanning Tree Protocol
SIP	Session Initiation Protocol
SDN	Software Defined Network
TCP	Trasport Control Protocol
TIC	Tecnologias de Informação e Comunicação
UDP	User Datagram Protocol
UPS	Uninterruptible Power Supply
VoIP	Voice over IP
VLAN	Virtual LAN
VPN	Virtual Privat Network
WAN	Wade Area Network

Glossário de termos

- **Documentação**

No contexto de redes de computadores, o termo documentação refere-se ao conjunto de registros, manuais, especificações e descrições técnicas que detalham a estrutura, configuração, operação e manutenção de uma rede.

- **Ethernet**

Ethernet é um padrão de rede de área local (LAN - *Local Area Network*) que define como os dispositivos (como computadores, routers, switches, entre outros) comunicam entre si através de cabos ou ligações sem fios. É uma tecnologia amplamente utilizada para conectar dispositivos em redes locais, permitindo a troca de dados a alta velocidade.

- **Infra-estrutura de rede Coporativa**

Compreende o conjunto de componentes (dispositivos de rede, sistemas, servidores, mecanismos de segurança, entre outros) necessários para a operação e gestão de serviços de TI em ambientes corporativos.

- **Modernização**

O termo Modernização, no contexto de uma rede de computadores, refere-se ao processo de atualização e aprimoramento da infra-estrutura, tecnologias e protocolos de rede para melhorar o desempenho, segurança, escalabilidade e eficiência.

- **Wi-Fi**

Wi-Fi (abreviação de *Wireless Fidelity*, em português "Fidelidade Sem Fios") é uma tecnologia de rede sem fio que permite a conexão de dispositivos electrónicos à internet ou a outras redes locais por meio de ondas de rádio, eliminando a necessidade de cabos físicos.

- **Reestruturação**

Em redes de computadores, reestruturação refere-se ao processo de reorganizar, modificar ou otimizar a arquitetura, a topologia ou os componentes de uma rede para melhorar seu desempenho, segurança, escalabilidade ou eficiência. Pode envolver mudanças físicas (*hardware*) ou lógicas (*software*/configurações).

1. Capítulo I - Introdução

1.1. Contextualização

A infra-estrutura de Tecnologia da Informação (TI) é um pilar essencial para o funcionamento eficiente de instituições acadêmicas e corporativas. No contexto da FEUEM, a modernização e organização dos sistemas de TI são fundamentais para suportar as demandas crescentes de conectividade, segurança e desempenho. Tendo em conta todas as limitações físicas e lógicas da rede actual da FEUEM este projeto propõe uma reestruturação completa da infra-estrutura, dividida em duas fases: documentação e planeamento, seguida pela implementação técnica.

A fase da documentação assegurará um mapeamento preciso dos ativos de TI em todos os departamentos da FEUEM, facilitando a gestão estratégica. Já a segunda fase focará na modernização da infra-estrutura. Essas melhorias visam não apenas melhorar e otimizar recursos, mas também aumentar a disponibilidade e a segurança dos sistemas.

Este trabalho é de estrema importância pois está na aplicação de boas práticas de governança de TI, garantindo que a FEUEM tenha uma infra-estrutura escalável, de fácil manutenção e alinhada às necessidades institucionais. Os resultados esperados incluem maior eficiência operacional, redução de custos e melhoria na experiência dos utilizadores.

Segundo (Firmino A. Nhanombe, 2022), “a rede da faculdade de engenhaia da UEM apresenta uma arquitetura tecnológica com largura de banda capaz de oferecer um sinal de rede sem fio estável e eficiente aos utilizadores, porém, nos últimos 3 anos, registou-se uma atenuação do sinal de cobertura desta rede”. Esse estudo foi feito em 2022, enfatizando mais uma vez a urgéncia da reestruturação completa da rede da FEUEM.

(Chiziane, 2022), reitera que “no departamento de Engenharia Eletrotécnica devido a vários fatores, os serviços da rede não estão disponíveis para vários utentes pois os dispositivos terminais não apresentam sinal de rede, o que reflete a falta de conexão entre os dispositivos da rede naquele departamento”. Essa obeservação denuncia mais uma vez o quão urgente é a reestruturação da rede na FEUEM.

1.2. Estruturação do trabalho

O trabalho encontra-se organizado da seguinte forma:

Capítulo I: Introdução - Apresenta-se a contextualização do estudo, o problema de pesquisa, a justificativa, a metodologia utilizada e os objetivos gerais e específicos a serem alcançados;

Capítulo II: Revisão da Literatura - Discutem-se os referenciais teóricos relacionados ao tema, com base em fontes científicas relevantes, estabelecendo o embasamento teórico e o estado da arte sobre redes de dados, virtualização e gestão de infraestrutura de TI;

Capítulo III: Caso de Estudo - Descreve-se o objeto de estudo, neste caso, a Faculdade de Engenharia da Universidade Eduardo Mondlane (FEUEM), abordando sua infraestrutura de rede atual, os serviços oferecidos, as funcionalidades existentes e as principais limitações identificadas;

Capítulo IV: Desenvolvimento do Trabalho - Apresenta-se a proposta de reestruturação da rede, incluindo:

- Documentação da rede (topologia, inventário de equipamentos);
- Configuração de serviços (VLANs, QoS).

Capítulo V: Considerações Finais - São apresentadas as conclusões do trabalho, a avaliação do cumprimento dos objetivos, as contribuições do projeto e recomendações para futuras melhorias ou expansões da rede.

- **Bibliografia -** Esta secção apresenta a lista completa das fontes consultadas ao longo da investigação, incluindo livros, artigos científicos, relatórios técnicos e recursos digitais. Estas referências foram fundamentais para a fundamentação teórica, metodológica e prática do trabalho, permitindo o alcance dos objectivos propostos e a consolidação dos resultados apresentados;
- **Anexos -** Incluem-se materiais complementares, como diagramas de rede, scripts de configuração, tabelas detalhadas e outros documentos relevantes para a compreensão do projeto.

1.3. Formulação do problema

A Faculdade de Engenharia da Universidade Eduardo Mondlane (FEUEM) enfrenta atualmente desafios críticos na sua infra-estrutura de rede de dados, os quais comprometem a eficiência operacional e a segurança dos sistemas. A falta de documentação adequada sobre a topologia da rede e o inventário de equipamentos dificulta significativamente a realização de manutenções preventivas e corretivas, bem como o planeamento de futuras expansões.

O bloco administrativo da FEUEM alberga os serviços mais críticos, nomeadamente académicos, financeiros e de gestão. Por essa razão, é imperativo que a rede seja reestruturada, com especial enfoque neste bloco.

Através de entrevistas realizadas aos técnicos da Direcção de Tecnologias de Informação e Comunicação (DTIC), responsável pela manutenção da rede e demais actividades TIC na FEUEM, constatou-se que os problemas na rede não foram sempre existentes, mas surgiram progressivamente. Com o crescimento da infra-estrutura e o aumento do número de utilizadores, foram aparecendo necessidades não previstas inicialmente. Equipamentos antigos degradaram-se, e novos dispositivos foram instalados como substituição, sem qualquer plano de padronização. Como resultado, a rede tornou-se cada vez mais desorganizada e caótica, sem documentação, mapas ou topologia definidos.

Um exemplo claro da ineficiência actual é o tempo médio de resolução de problemas relativamente simples, como a substituição de um switch num bastidor, que demora cerca de uma hora, quando, com cabos devidamente etiquetados e organizados por padrões de cor conforme o tipo de dispositivo, o mesmo processo poderia ser concluído em 5 a 10 minutos.

Torna-se, portanto, urgente a implementação de medidas que permitam a reorganização, padronização e documentação da rede, garantindo maior segurança, eficiência e escalabilidade para suportar as necessidades actuais e futuras da FEUEM.

1.4. Justificativa

A reestruturação da rede de dados da FEUEM se mostra necessária para superar diversos desafios operacionais e tecnológicos que impactam diretamente sua eficiência e segurança. Atualmente, a falta de documentação adequada da infra-estrutura de rede dificulta significativamente a identificação e resolução de falhas, além de comprometer o planejamento de expansões futuras. A implementação de um mapeamento detalhado permitirá uma gestão mais proativa, garantindo maior escalabilidade e manutenção eficiente do sistema.

No aspecto de segurança, a ausência de um sistema centralizado de autenticação e controle de acesso expõe a rede a vulnerabilidades e usos indevidos. A adoção de soluções como Windows Server para autenticação, combinada com políticas avançadas de firewall e segmentação via VLANs, proporcionará um ambiente mais seguro e controlado. Paralelamente, a virtualização de servidores emergirá como solução estratégica para otimização de recursos, reduzindo custos com hardware físico enquanto aumenta a disponibilidade dos serviços e facilita processos críticos como backups e recuperação de desastres.

Esta modernização da infra-estrutura é particularmente crucial para uma instituição acadêmica como a FEUEM, onde uma rede robusta e bem gerenciada é fundamental para suportar as demandas de ensino, pesquisa e extensão. A consolidação de servidores e automação de configurações trará ainda benefícios econômicos tangíveis, diminuindo gastos com energia, manutenção e licenças de software.

Além dos ganhos imediatos, a reestruturação preparará o terreno para a adopção de tecnologias emergentes como IoT e computação em nuvem, posicionando a faculdade na vanguarda tecnológica. O projeto transcende o âmbito institucional, servindo como estudo de caso replicável para outras instituições de ensino com desafios similares, contribuindo assim para o avanço do conhecimento em redes de dados e TI educacional. Desta forma, a iniciativa justifica-se tanto pelos benefícios operacionais imediatos quanto por seu potencial de impacto acadêmico e social mais amplo.

1.5. Objectivos

1.5.1. Geral:

Propor a reestruturação e modernização da infra-estrutura de rede da FEUEM, visando melhorar o desempenho, a segurança e a escalabilidade da rede.

1.5.2. Específicos:

- Analisar a infra-estrutura de rede da Faculdade de Engenharia da UEM, em particular no bloco administrativo;
- Apresentar os problemas e anomalias físicas e lógicas detectadas na rede;
- Realizar uma análise comparativa das soluções mais viáveis para resolver os problemas identificados;
- Descrever a implementação da solução selecionada como a mais adequada para a resolação dos problemas econtrados.

1.6. Metodologia

1.6.1. Pergunta de pesquisa

O presente trabalho de pesquisa propõe responder a seguinte pergunta:

De que forma pode uma modernização e reestruturação abrangente da infra-estrutura de rede da FEUEM - contemplando a documentação pormenorizada dos ativos, a superação das limitações de desempenho, o reforço da segurança e a optimização da gestão - melhorar a eficiência e escalabilidade da rede de dados?

1.6.2. Classificação da metodologia

Existem diversas formas de classificar as pesquisas de acordo com (Da Silva & Menezes, 2001) citado por (Mazivila, 2022). Para obtenção dos resultados e respostas do problema proposto, foram seguidas as seguintes classificações:

a) Quanto a natureza

O presente trabalho fundamenta-se em uma pesquisa de **natureza aplicada**, uma vez que se propõe a solucionar um problema concreto no âmbito da reorganização da infra-estrutura de tecnologias de informação da FEUEM, com objetivos eminentemente práticos, tais como a implementação de sistemas, a padronização de processos e a elaboração de documentação técnica. Essa abordagem permite não apenas a análise teórica dos desafios

identificados, mas também a proposição e execução de soluções técnicas alinhadas às necessidades institucionais, conferindo ao estudo um caráter essencialmente pragmático e orientado para a transformação do ambiente tecnológico em questão.

b) Quanto a abordagem

O presente trabalho adopta uma **abordagem qualitativa**, uma vez que se concentra na análise detalhada de processos, fluxos de trabalho e requisitos organizacionais da infra-estrutura de tecnologias de informação da FENG, bem como na descrição de tecnologias específicas, como virtualização de servidores e implementação do Active Directory para gestão centralizada de utilizadore. Caso sejam realizadas entrevistas ou questionários com stakeholders para coletar percepções sobre a transição ou eficácia das soluções propostas, esses dados também reforçarão a dimensão qualitativa da pesquisa, permitindo uma compreensão aprofundada dos desafios e benefícios associados à reestruturação tecnológica.

c) Quanto aos objectivos

O presente trabalho **caracteriza-se como descritivo**, pois detalha minuciosamente os processos envolvidos na documentação da infra-estrutura de tecnologias de informação e nas etapas da modernização da rede, além de classificar e organizar informações técnicas sobre o cenário atual e o planeado.

d) Quanto aos procedimentos

O presente trabalho baseou-se em:

- **pesquisa bibliográfica**

Consiste no levantamento sistemático de referências teóricas publicadas em meios escritos e eletrónicos, incluindo livros, artigos científicos e páginas web, servindo como etapa fundamental em qualquer trabalho científico. Esta abordagem tem como principais objetivos identificar se as questões de pesquisa já foram respondidas em estudos anteriores, avaliar a pertinência de replicar investigações cujos objetivos já foram alcançados e analisar métodos empregues em pesquisas similares, permitindo tanto contextualizar o estudo no conhecimento existente quanto embasar a busca por novas soluções metodológicas.

- **Pesquisa documental e**

Embora semelhante à pesquisa bibliográfica, distingue-se desta pelo tipo de fontes utilizadas. Enquanto a pesquisa bibliográfica se baseia em materiais já trabalhados e publicados, como livros e artigos científicos, a pesquisa documental recorre a fontes primárias e materiais diversos, muitas vezes não tratados analiticamente. Entre estes incluem-se: dados estatísticos, periódicos (jornais e revistas), documentos oficiais, correspondência (cartas), registos audiovisuais (filmes e fotografias), bem como relatórios técnicos e institucionais. Esta abordagem permite aceder a informação original e não filtrada, oferecendo uma base empírica mais direta para a investigação;

- **Caso de estudo e pesquisa acção**

Caracteriza-se como a análise aprofundada de uma entidade bem definida, podendo tratar-se de um programa, uma instituição, um sistema educativo, um indivíduo ou uma unidade social. Este método tem como objetivo compreender em profundidade o "como" e o "porquê" de uma determinada situação, presumindo-se que esta apresenta características únicas em diversos aspetos. O estudo procura identificar os elementos mais essenciais e distintivos do objeto em análise. No presente trabalho de investigação, adotou-se como estudo de caso a Faculdade de Engenharia da Universidade Eduardo Mondlane (FEUEM).

e) Quanto a coleta de dados.

O presente estudo adotou a entrevista semiestruturada como técnica primária de investigação, caracterizada pela interação oral direta entre pesquisador e sujeitos da pesquisa (estudantes, docentes e colaboradores da FEUEM), com roteiro pré-definido, porém flexível a aprofundamentos contextuais. Este instrumento visa:

- **Obtenção de dados qualitativos** sobre percepções, necessidades e desafios enfrentados pelos stakeholders no contexto da infraestrutura de TI;
- **Validação iterativa** das etapas de desenvolvimento da solução, assegurando alinhamento com as demandas reais identificadas em cada fase do projeto;
- **Triangulação de evidências**, complementando dados documentais e observacionais com perspectivas humanizadas.

f) Quanto a consulta aos supervisores

Para assegurar a robustez metodológica e o alinhamento estratégico do trabalho, foi implementado um processo sistemático de orientação, no qual os supervisores assumem um papel crítico em três dimensões principais:

- **Suporte Técnico - Conceitual –** Esclarecimento de dúvidas relacionadas a fundamentos teóricos, métodos de investigação e implementação prática, garantindo rigor científico;
- **Monitorização Contínua –** Acompanhamento estruturado do cronograma, com revisões periódicas para avaliar progresso, identificar riscos e propor ajustes;
- **Validação de Resultados –** Análise crítica das etapas concluídas (ex.: documentação de infra-estrutura, testes de soluções) para assegurar conformidade com os objetivos institucionais da FEUEM.

Conclusão:

Este trabalho caracteriza-se como uma pesquisa aplicada, de natureza qualitativa e descritiva, com abordagem bibliográfica (para fundamentar conceitos como tipos de redes e gestão de ativos) e documental (para análise do cenário atual da FEUEM). Caso haja implementação prática durante o estudo, adotar-se-á também a pesquisa-ação, registrando resultados da reestruturação.

2. Capítulo II – Revisão da Literatura

2.1. Redes de Computadores

Segundo (Kurose & Ross, 2020) Uma rede de computadores é um sistema que interconecta dispositivos computacionais (como hosts, roteadores, switches, entre outros) para permitir a comunicação e o compartilhamento de recursos.

Existem regras que devem ser pré-estabelecidas para que haja comunicação entre hosts (nós) de uma rede, essas regras são chamadas de protocolos, sem os quais não seria possível a comunicação ou a troca de dados em uma rede. Mais adiante no trabalho esse assuto é abordado com profundidade.

De acordo com (Tanenbaum & Wetherall, 2021), as redes de computadores são classificadas com base em diferentes critérios, como extensão geográfica, topologia, meio de transmissão e arquitetura.

No presente relatório, serão discutidas apenas as classificações de rede que serão usadas no processo da descrição dos problemas e proposta de solução.

2.1.1. Classificação da rede segundo a extensão geográfica

Um dos critérios de classificação de redes de computadores é a sua extensão geográfica, dependendo da distância que a rede ocupar, terá uma designação diferente, abaixo estão as designações das redes dependendo da área que ocupam:

2.1.1.1. Redes WAN

Segundo (Tanenbaum & Wetherall, 2021), Uma rede geograficamente distribuída, ou *WAN (wide area network)*, abrange uma grande área geográfica, com frequência um país ou continente. Ela contém um conjunto de máquinas cuja finalidade é executar os programas (ou seja, as aplicações) do usuário.

No entendimento do autor, Quando as distâncias envolvidas na interligação dos computadores são superiores a uma área metropolitana, podendo chegar a uma dispersão geográfica tão ampla quanto a distância entre continentes, a abordagem adequada é a rede de longa distância *(WAN).*

Segundo autores supracitados, as redes WAN conectam redes geograficamente separadas em longa distância, utilizando fibras ópticas e comunicação via satélite, cobrindo países, continentes ou o mundo todo, com projeto e manutenção difíceis, taxa de transferência de dados baixa, poucos utilizadores e custo de manutenção muito elevado.

Abaixo está uma figura que ilustra de forma clara como é uma rede *WAN:*

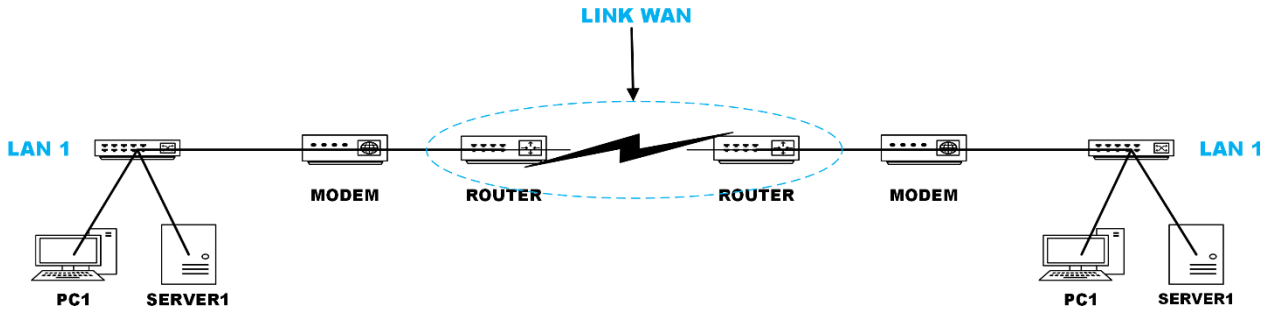


Figura 1: Rede WAN

Fonte: Elaborado pelo autor.

Conforme pode-se observar, a figura mostra duas redes LAN que são conectadas através de um link serial WAN, que representa uma fibra óptica que atravessa uma grande área geográfica. Essa fibra é conectada a um roteador (dispositivo com capacidade de conectar e fazer comunicar redes diferentes) de cada lado, e um Modem (Modulador – Demodulador). Através dessa rede é possivel fazer comunicar os PC's de cada lado, ou buscar serviços dos servidores de ambos os lados.

2.1.1.2. Redes MAN

(Kurose & Ross, 2020) afirmam que uma MAN é uma rede que abrange uma área metropolitana, como uma cidade ou uma grande zona urbana, interligando múltiplas redes locais (LANs) com infraestrutura de alta capacidade, como fibra óptica ou wireless dedicado. As MANs são projetadas para oferecer conectividade de alta velocidade a organizações distribuídas geograficamente dentro de uma mesma região, mas em escalas menores do que uma WAN.

No entendimento do autor, uma *Metropolitan Area Network*, ou Rede de Área Metropolitana, é um escopo de rede intermediário entre uma LAN e uma WAN. Trata-se de uma rede localizada em uma área geográfica confinada e bem definida, de tamanho médio, como por exemplo em um município ou região metropolitana.

De uma forma geral, as redes *MAN* interconectam redes numa cidade ou município, usando cabos coaxiais, wireless (WiMAX/celular) ou fibra óptica, cobrem até aproximadamente 100 km, têm projeto complexo de implementar, baixa taxa de dados, média/baixa taxa de utilização e um custo elevado de manutenção.

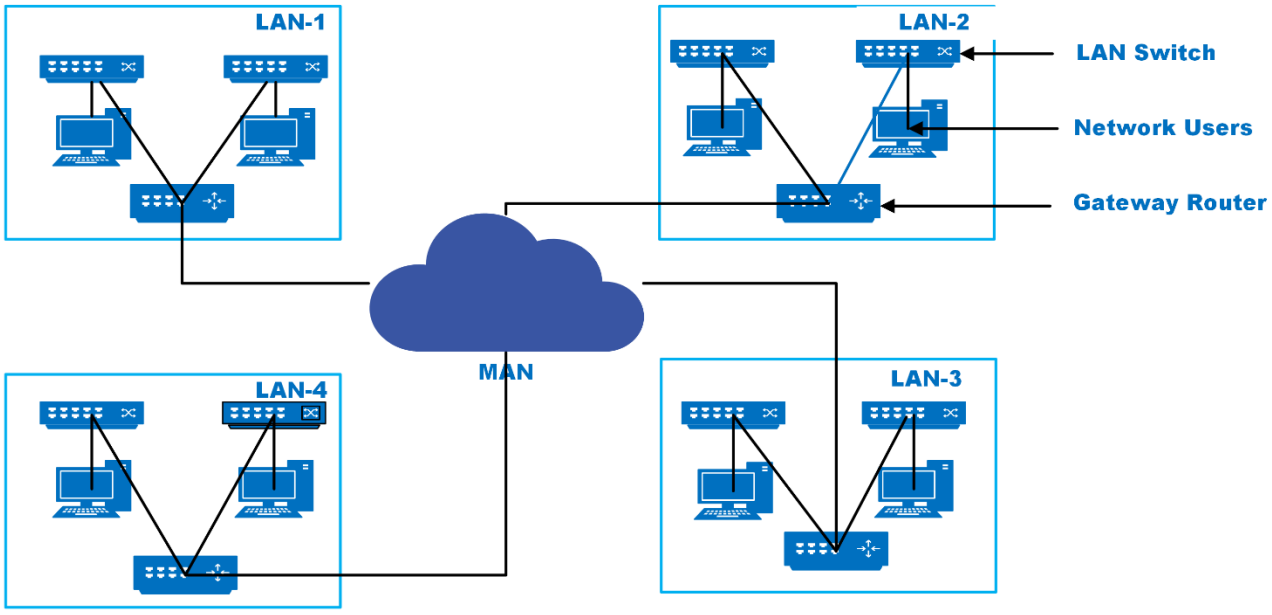


Figura 2: Rede MAN

Fonte: Elaborado pelo autor

Conforme pode-se observar na figara acima, uma rede MAN é constituida por várias LANs interligadas entre si, num espaço que compreende uma cidade por exemplo. Esse tipo de rede é muito usada por companhias que têm filiais aredorres com o intuito de manter a comunição entre elas.

Um exemplo claro de uma MAN é a rede da Universidade Eduardo Mondlane, a CIUEM actua como uma *ISP* propagando a internet para as demais faculdades, e as faculdades actuam como filiais, recebendo o sinal da CIUM formando neste caso uma MAN.

2.1.1.3. Redes LAN

Segundo (Peterson & Davie, 2021), uma rede *LAN* é uma rede de comunicação que abrange uma área geográfica limitada, como um único prédio ou campus, e oferece alta taxa de transferência de dados com baixa latência. LANs são tipicamente de propriedade privada e usam tecnologias como Ethernet ou Wi-Fi para conectar dispositivos locais, como computadores, impressoras e servidores.

No entendimento do autor, uma *Local Area Network*, ou Rede de Área Local, ou ainda simplesmente Rede Local, geralmente está localizada em um edifício, escritório, campus ou até mesmo m uma residência. Possui conectividade em alta velocidade e sua característica principal é ser uma rede privativa, ou seja, alguém (pessoa ou organização) controla essa rede e o acesso a ela, em uma área geográfica limitada.

As redes LAN conectam computadores, impressoras e outros dispositivos em ambientes locais, como empresas ou casas, utilizando cabos UTP ou Wi-Fi, com cobertura limitada, alta velocidade, poucos utilizadores e baixo custo de manutenção.

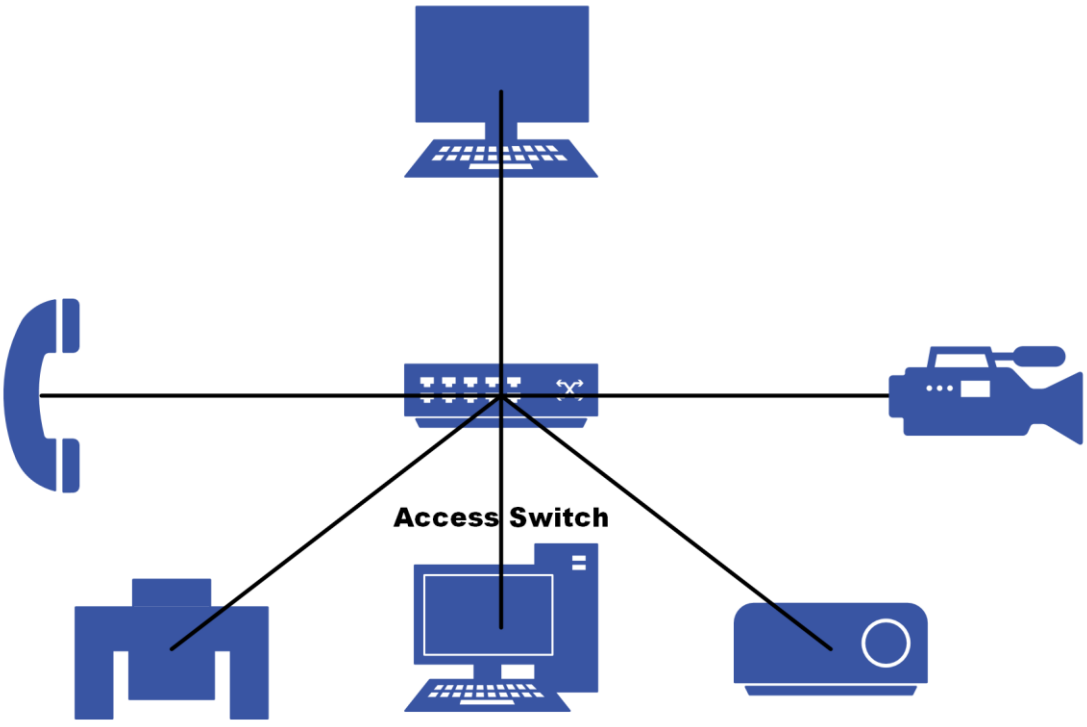


Figura 3: Rede LAN

Fonte:Elaborado pelo autor

Conforme ilustra a figura acima, é uma representação clássica de uma LAN, onde os hosts (nós) se conectam à um switch de destribuição através de um cabo ethernet, logo a seguir é atribuido um endereço IP, pelo qual será conhecido na rede, aliás, é ainda possível conhecer os hosts através do endereço de máquina *(MAC Adress*) que é um codigo de 48 bits gravado na placa de qualquer dispositivo de rede, que o identifica na rede.

As redes LAN têm as suas próprias arquitecturas, dependendo das necessidades da empresa que queira construir uma infra-estrutura de rede, pode usar a que mais se adeque às suas necessidades.

Neste trabalho irá se abordar somente sobre a arquitectura *Ideal Two Tier*, que vai de acordo com a proposta da solução dos problemas que aqui sarão abordados.

2.1.1.4. Arquitectura *LAN Ideal Two Tier (2-Layered collapsed core model)*:

(Tanenbaum & Wetherall, 2021), em sua obra *Computer Networks*, descreve o *2-Layered Collapsed Core Model* como uma arquitetura de rede simplificada que combina as funções do *core layer* (núcleo) e do *distribution layer* (distribuição) em uma única camada, resultando em uma topologia mais eficiente e econômica para redes de pequeno a médio porte.

Essa arquitectura se mostra bastante eficaz para redes médias, como por exemplo um edifício ou um bloco de uma instituição, pois garante alta disponibilidade, escalabilidde, evita o *single point of failury* (ponto único de falha) e é bastante simples de gerir.

- **Arquitectura *LAN Two Tier* apresenta as seguintes caracteristicas:**
    - Colapso do *core* e *distribution layers:*

No modelo tradicional de três camadas (*core, distribution* e *access*), o *core layer* é responsável pelo roteamento de alta velocidade, enquanto o *distribution layer* faz a agregação de tráfego e aplicação de políticas;

No modelo colapsado, essas duas camadas são fundidas em uma única, reduzindo complexidade e custos.

    - Topologia em dois níveis:

a) Camada Única (*Core* + *Distribution*): Capacidade de roteamento e switching de alto desempenho, agregação de múltiplos switches de acesso e aplicação de políticas (VLANs, QoS, ACLs).
b) Camada de acesso *(Access Layer):* Conecta dispositivos finais (PCs, telefones VoIP, entre outros) e opera em modo *edge* (sem roteamento complexo).

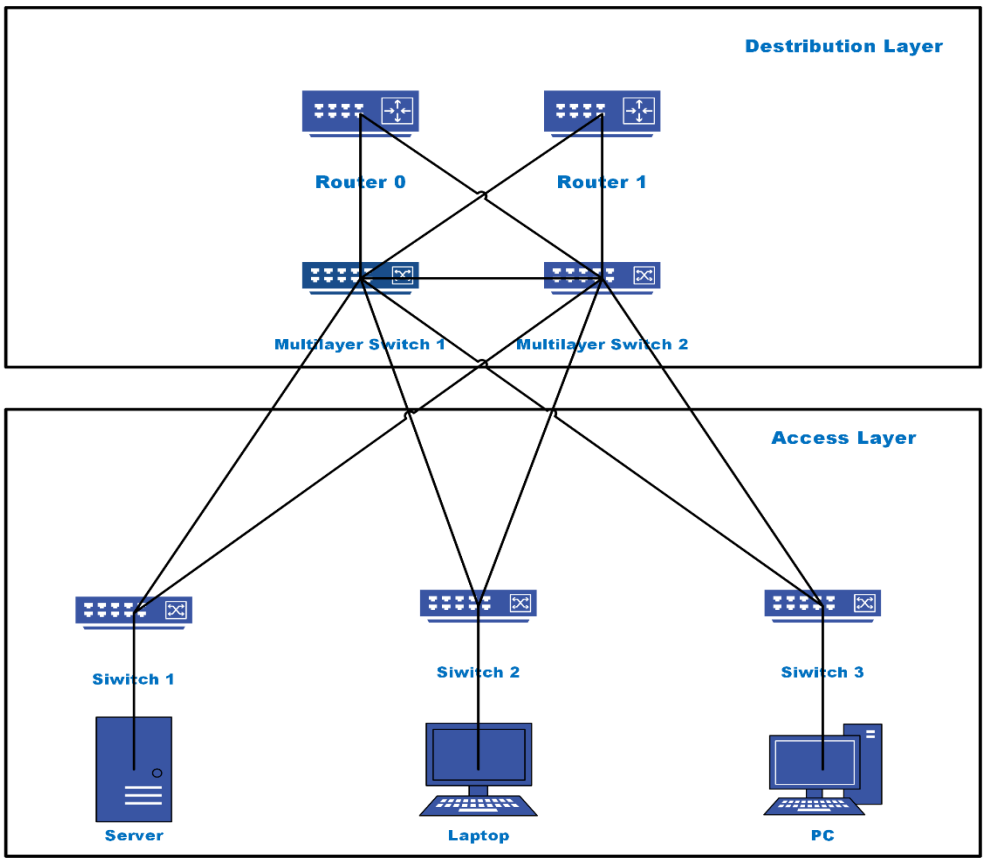


Figura 4: Ideal Two-Tier LAN Arquitecture

Fonte: Elaborado pelo autor

Em suma, a arquitetura *LAN Two Tier* colapsa as camadas *core* e *distribution* do modelo tradicional em uma única camada, combinando funções de roteamento de alta velocidade, agregação de tráfego e aplicação de políticas, enquanto a camada de acesso conecta dispositivos finais sem roteamento complexo.

Esta abordagem reduz custos e complexidade, oferece menor latência e é adequada para redes de tamanho moderado, mas tem limitações de escalabilidade em comparação com o modelo de três camadas em redes muito grandes.

2.1.2. Classificação da rede segundo a topologia

Redes de computaores também podem ser classificadas segundo a sua disposição física, (Tanenbaum & Wetherall, 2021) renomado especialista em redes de computadores, aborda a classificação de redes segundo as topologias em sua obra clássica *Computer Networks*. Ele destaca que a topologia de uma rede refere-se ao arranjo físico ou lógico dos nós (computadores, roteadores, switches, etc.) e às conexões entre eles.

abaixo está feita a descrição dos tipos de topologia que as redes podem apresentar:

2.1.2.1. Topologia Barramento *(Bus)*

Também chamada de topologia de *backbone*, *bus* ou linha, orienta os dispositivos ao longo de um único cabo que vai de uma extremidade da rede à outra. Os dados fluirão ao longo do cabo conforme ele se desloca até seu destino.

Na topologia Barramento todos os *hosts* (nós) compartilham um único meio de comunicação.

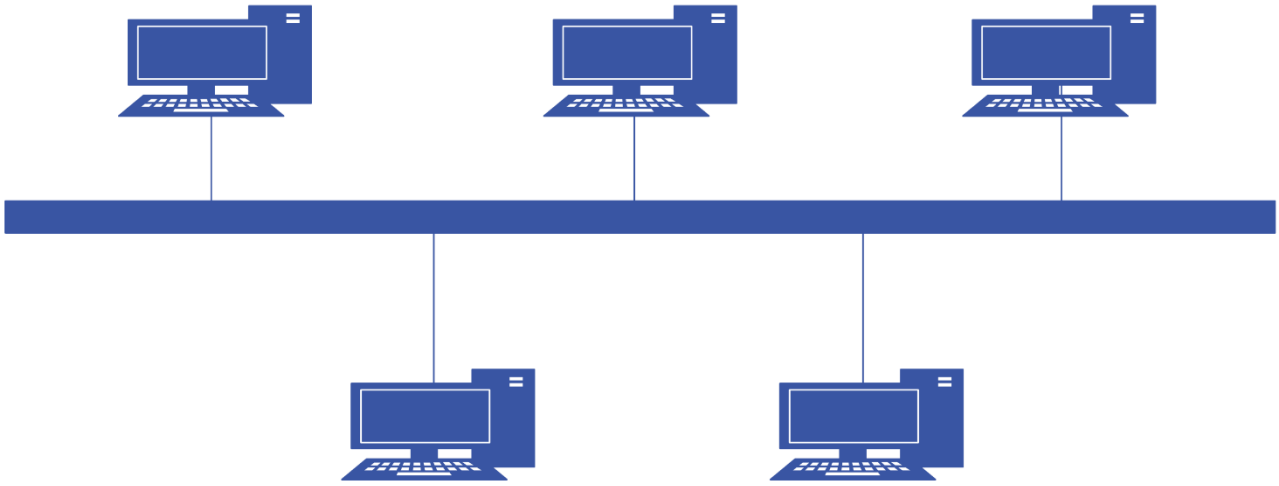


Figura 5: Topologia Barramento

Fonte: Elaborado pelo autor

A topologia Barramento apresenta as seguintes vantagens: Económico para redes pequenas, layout simples, conexão por um único cabo e expansão fácil.

A topologia Barramento apresenta as seguintes limitações: Vulnerável a falhas no cabo, velocidade reduzida com mais nós e comunicação *half-duplex*.

2.1.2.2. Topologia Estrela *(Star)*

Segundo os autores (Peterson & Davie, 2021) é o tipo de configuração mais comum. A rede é organizada de forma que os nós sejam conectados a um hub central, que atua como um servidor. O hub gerencia a transmissão de dados pela rede. Ou seja, qualquer dado enviado pela rede viaja pelo hub central antes de terminar em seu destino.

Na topologia em Estrela todos os nós estão conectados a um nó central (como um *switch* ou *hub*), conforme mostra a figura abaixo.

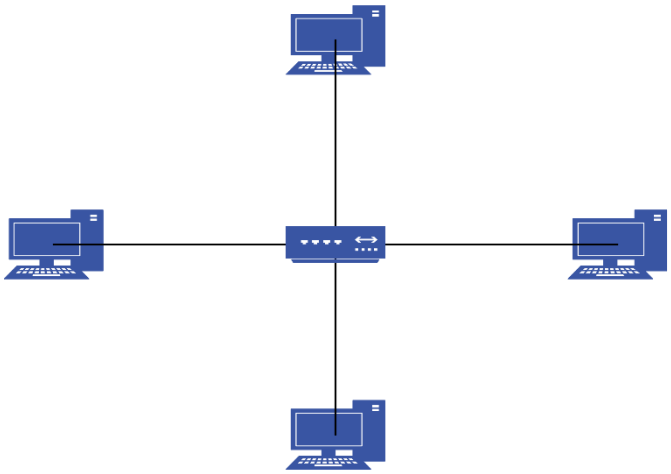


Figura 6: Topologia Estrela

Fonte: Elaborado pelo autor

De acordo com os autores (Kurose & Ross, 2020) a topologia Estrela apresenta as seguintes vantagens: gerenciamento centralizado, tolerância a falhas em nós individuais, escalabilidade sem interrupções e diagnóstico facilitado.

De acordo com os autores (Kurose & Ross, 2020) a topologia Estrela apresenta as seguintes desvantagens: Ponto único de falha no hub central, desempenho limitado pelo nó central e custos operacionais elevados.

2.1.2.3. Topologia Arvore *(Tree)*

Um nó central conecta hubs secundários. Esses *hubs* têm uma relação pai-filho com os dispositivos. O eixo central é como o tronco da árvore. Onde as ramificações se conectam

estão os hubs secundários ou nós de controle e, em seguida, os dispositivos conectados são anexados aos branches.

- **A topologia Arvore apresentam as seguintes caracteristicas:**
  - Combinação de topologias barramento e estrela, formando uma hierarquia;
  - Usada em redes grandes (como redes de provedores de *internet*).

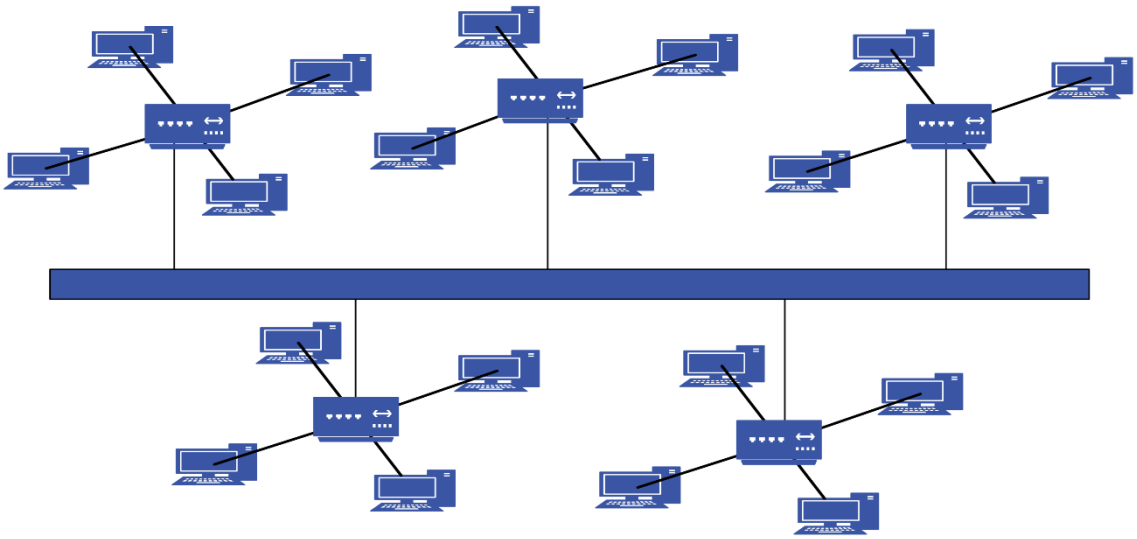


Figura 7: Topologia Arvore

Fonte: Elaborado pelo autor

Esta topologia oferece elevada flexibilidade e escalabilidade, permitindo a fácil identificação de falhas através da análise isolada de cada ramo da rede. No entanto, apresenta vulnerabilidade em caso de falha do hub central, que pode desconectar múltiplos nós, apesar de as ramificações poderem operar de forma independente. A gestão da rede pode tornar-se complexa, e o consumo de cabos é significativamente maior em comparação com outras topologias.

As redes de computadores também podem ser classificadas consoante o meio de transmissão de dados e a arquitetura que apresentam. Contudo, de modo a gerir a extensão do relatório, optou-se por não aprofundar estas duas formas de classificação, evitando assim ultrapassar o número máximo de páginas considerado aceitável.

2.1.3. Modelos de referência de redes de computadores

Como todas grandes invensões humanas, as redes de computadores apresentam modelos clássicos de referrência, neste caso se referre a dois grandes modelos, a saber: OSI *(Open Systems Interconnection)* e TCP/IP *(Transport Control Protocol / Internet Protocol)*. Diz (Tanenbaum & Wetherall, 2021) que embora os protocolos associados ao modelo OSI raramente sejam usados nos dias de hoje, o modelo em si é de facto bastante geral e ainda válido, e as características descritas em cada camada ainda são muito importantes. O modelo TCP/IP tem características opostas: o modelo propriamente dito não é muito utilizado, mas os protocolos têm uso geral. Por essa razão, examinaremos ambos em detalhes.

2.1.3.1. Aquitectura do modelo *OSI*

Segundo (Tanenbaum & Wetherall, 2021), o modelo OSI (*Open Systems Interconnection*) é um padrão conceitual desenvolvido pela ISO (*International Organization for Standardization*) para facilitar a comunicação entre sistemas distintos. Ele divide o processo de comunicação em 7 camadas, cada uma com funções específicas, garantindo que diferentes fabricantes possam criar tecnologias compatíveis.

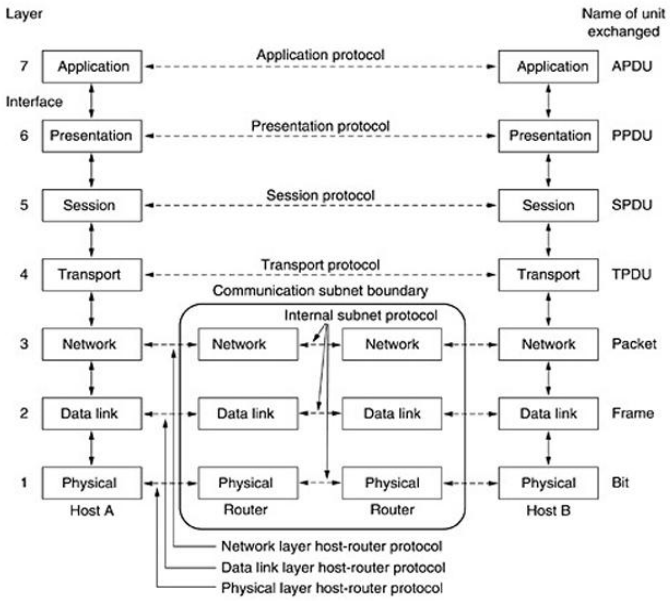


Figura 8: Modelo OSI

Fonte: (Tanenbaum & Wetherall, 2021)

A figura acima ilustra o esquema da arquitectura OSI que está dividida em sete camadas, cada camada apresenta o seu próprio PDU (*Protocol Data Unit*).

(Tanenbaum & Wetherall, 2021) Aborda sobre as camadas do modelo OSI da seguinte forma:

Camada	Nome	Função Principal	Exemlos de protocolos / Dispositivos
7	**Aplicação**	Interface entre o usuário e a rede (serviços como e-mail, navegação web).	HTTP, FTP, SMTP, DNS, SSH
6	**Apresentação**	Tradução/formatação de dados (criptografia, compressão, conversão de formatos).	SSL/TLS, JPEG, MPEG, ASCII
5	**Sessão**	Gerencia conexões (estabelece, mantém e encerra sessões).	NetBIOS, RPC, SIP
4	**Transporte**	Garante entrega confiável (ou não) dos dados (controle de fluxo e erro).	TCP (conexão confiável), UDP (rápido, sem confirmação)
3	**Rede**	Roteamento de pacotes entre redes (endereçamento lógico).	IP, ICMP, BGP, roteadores
2	**Enlace de dados**	Controle de acesso ao meio físico (MAC) e detecção/correção de erros em quadros.	Ethernet, PPP, switches, bridges
1	**Fíisica**	Transmissão de bits brutos (sinais elétricos, óticos ou sem fio).	Cabos (UTP, fibra ótica), hubs, repetidores

Tabela 1: Caracteristicas do modelo OSI

Fonte: Elaborado pelo autor

- **Modo de funçionamento do modelo OSI**
    - Encapsulamento: Os dados descem do nível de aplicação até o físico, ganhando cabeçalhos (ou *trailers)* em cada camada;
    - Desencapsulamento: No destino, o processo é invertido, removendo os cabeçalhos camada por camada.
- **Vantagens do modelo OSI**
    - Padronização: Permite interoperabilidade entre tecnologias de diferentes fabricantes.
    - Modularidade: Facilita desenvolvimento e troubleshooting (cada camada pode ser analisada separadamente).
    - Didático: Ajuda a entender redes de forma estruturada.
- **Limitações do modelo OSI:**
    - Complexidade: Nunca foi totalmente implementado na prática (o TCP/IP é mais usado);
    - Camadas redundantes: Apresentação e Sessão são menos relevantes em muitas aplicações modernas.

2.1.3.2. Aquitectura do modelo TCP/IP

Os autores (Kurose & Ross, 2020) descrevem a arquitetura TCP/IP como sendo um conjunto de protocolos organizados em camadas, seguindo uma abordagem hierárquica para a comunicação em redes.

A arquitetura TCP/IP é composta por quatro camadas principais, diferindo ligeiramente do modelo OSI (que possui sete camadas). Abaixo está a descrição conforme a visão dos escritores:

Camada	Funções Principal	Protocolos Principais	Unidades de Dados
Aplicação	Fornece serviços diretos às aplicações de rede e usuários.	HTTP, HTTPS, FTP, SMTP, DNS, DHCP, SSH, Telnet	Mensagem / Dado

Transporte	Garante comunicação fim-a-fim, controle de fluxo, erro e confiabilidade.	TCP (conexão confiável), UDP (rápido, sem conexão)	Segmento (TCP) / Datagrama (UDP)
Rede	Roteamento de pacotes entre redes diferentes (endereçamento lógico).	IP (IPv4/IPv6), ICMP, OSPF, BGP	Pacote
Interface de Dados	Transmissão física de dados em uma mesma rede local (endereçamento físico).	Ethernet, Wi-Fi (802.11), ARP, PPP	Quadro / Frame

Tabela 2: Caracteristicas do modelo TCP/IP

Fonte: Elaborado pelo autor

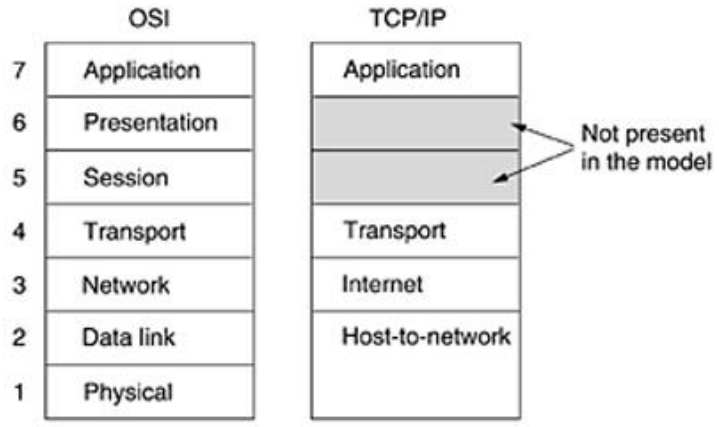


Figura 9: Arquitectura TCP/IP

Fonte: (Tanenbaum & Wetherall, 2021)

Com base na tabela acima conclui-se que o modelo TPC/IP é menos complexo e mais fácil de implementar relativamente ao modelo OSI, abaixo está uma tabela que faz a análise comparativa dos dois modelos segundos os autores (Kurose & Ross, 2020):

Modelo TCP / IP	Modelo OSI
Aplicação	Aplicação, Apresentação e Sessão
Transporte	Transporte
Rede (Internet)	Rede
Interface de Rede	Enlace, Física

Tabela 3: Comparação dos modelos OSI e TCP/IP

Fonte: Elaborado pelo autor

Com essa comparação de modelos, o autor entende que a fusão das camadas de aplicação, apresentação e sessão do modelo OSI numa única camada de aplicação no modelo TCP/IP, bem como a junção das camadas de enlace e física numa única camada de interface de rede, implica uma simplificação na implementação do modelo TCP/IP.

Esta abordagem reduz a complexidade, uma vez que os protocolos e os requisitos específicos de cada camada do modelo OSI passam a ser tratados de forma mais integrada dentro de uma única camada. Deste modo, o modelo TCP/IP torna-se mais direto na sua implementação, evitando a sobrecarga de múltiplas camadas com funções distintas, como ocorre no modelo OSI.

Consequentemente, esta simplificação contribui para uma maior eficiência na comunicação de dados, adaptando-se melhor às necessidades práticas das redes modernas.

2.1.4. Equipamentos de redes de computadores

Com o passar dos anos e o desenvolvimento da tecnologia, as redes de comptadores evoluiram exponencialmente, bem como os seus equipamentos. Esses equipamentos podem variar conforme o tamanho e a complexidade da rede (doméstica, empresarial ou data center).

Nesta secção, irá se abordar simplesmente dos equipamentos de rede que são indispensáveis para este trabalho.

2.1.4.1. Dispositivos de conectividade

Os dispositivos de conectividade de uma rede de computadores são descritos abaixo segundo os autores (Peterson & Davie, 2021):

- *Switch* – Dispositivo de rede que conecta hosts (nós) em uma rede local (LAN) e encaminha pacotes de dados apenas para o destinatário correto (usando endereços MAC);
    - *Switch L2* - Actua somente na camada de enlace, fazendo propogação de broadcast na rede;
    - *Switch L3* – Actua tanto na camada de enlace como na camada de rede, ou seja, pode actuar como um roteador.
- Roteador (*Router*) – Interconecta redes diferentes (como LAN e WAN) e encaminha tráfego com base em endereços IP;
- Modem **–** Converte sinais digitais em analógicos (e vice-versa) para acesso à *internet* (modem DSL ou a cabo).

2.1.4.2. Dispositivos de redes sem fio (*Wireless*)

- Ponto de Acesso Sem Fio (*Wireless Access Point - WAP*) – Permite que dispositivos se conectem à rede via Wi-Fi.

2.1.4.3. Dispositivos de Segurança

- Firewall – Filtra tráfego indesejado e protege a rede contra ameaças externas;
- IDS/IPS – Sistemas de detecção (*Intrusion Detection System)* e prevenção (*Intrusion Prevention System*) de intrusos.

2.1.4.4. Equipamentos de infra-estrutura

- Servidor – Fornece serviços como arquivos, e-mail, DNS, DHCP, entre outros.
- NAS *(Network Attached Storage)* **–** Armazenamento em rede para compartilhamento de arquivos.
- Repetidor (Extensor de Sinal *Wi-Fi*) – Amplifica o sinal de redes sem fio.

2.1.4.5. Cabos e meios de transmissão

- Cabos de Rede (Ethernet – Cat5e, Cat6, Cat7) **–** Usados para conexões físicas em LANs;
- Fibra Óptica **–** Transmite dados em alta velocidade por pulsos de luz (usado em redes de longa distância);
- Conectores (RJ45, LC/SC para fibra) **–** Interfaces para ligação de cabos.

2.1.5. Protocolos e padrões (Ethernet e SIP)

No entendimento do autor, em redes de computadores define-se protocolo como sendo um conjunto de regras que definem a comunicação entre dispositivos. Estas regras definem como os dados são formados, transmitidos e recebidos, garantindo interoperabilidade (que diferentes dispositivos possam interagir de forma eficaz), mesmo com hardware e software diferentes.

2.1.5.1. Ethernet (IEEE 802.3)

(Kurose & Ross, 2020) Ethernet (IEEE 802.3) é um padrão de rede para comunicação em LANs (*Local Area Networks)*, definindo cabeamento, formato de quadros (*frames*) e acesso ao meio físico.

O padrão Ethernet (IEEE 802.3) estabelece as normas para comunicação em redes locais (LANs), abrangendo especificações de cabeamento, estrutura de quadros (frames) e métodos de acesso ao meio físico. (Tanenbaum & Wetherall, 2021)

O padrão Ethernet (IEEE 802.3) suporta diversos meios de transmissão, incluindo cabos UTP (par trançado), fibra óptica e, em versões mais antigas, cabos coaxiais. Quanto à topologia, pode operar em estrela (utilizando switches) ou em barramento (com hubs, em implementações antigas). (Tanenbaum & Wetherall, 2021)

As taxas de transmissão variam desde 10 Mbps (Ethernet tradicional) até 400 Gbps (em versões de alta velocidade). O controle de acesso ao meio emprega o método CSMA/CD (*Carrier Sense Multiple Access with Collision Detection*) em redes *half-duplex* antigas, enquanto as redes modernas utilizam switches em modo *full duplex*. (Tanenbaum & Wetherall, 2021)

O quadro Ethernet (*frame*) é composto por campos como endereços MAC de origem e destino, identificação do tipo de protocolo (IPv4 ou IPv6) e um campo *CRC* para deteção de erros. Este padrão é amplamente utilizado como base para redes locais (LANs), conexões de internet banda larga e infra-estruturas de data centers. (Kurose & Ross, 2020)

Hoje o padrão Ethernet está presente em diferentes dispositivos e “as velocidades tiveram um aumento de três ordens de grandeza” (Kurose & Ross, 2020):

- **Redes Ethernet de 10Mbps**

A Ethernet de 10Mbps usa a técnica de controle de acesso ao meio CSMA/CD, essa rede foi muito usada em LANs e possui uma velocidade de sinalização de 20MHz. Nestas implementações, os dados são codificados usando o código de Manchester. (Tanenbaum & Wetherall, 2021).

- **Redes Ethernet de 100Mbps**

A Ethernet de 100Mbps permite a interconexão somente por hubs ou switches. É usado o algoritmo CSMA/CD para compartilhar o meio (Tanenbaum & Wetherall, 2021).. Por razões de velocidade e distância, surgiram apenas 3 especificações, que são:

a) **100Base-T4:** usa o esquema de par trançado sem blindagem (UTP), da categoria 3, que emprega uma velocidade de sinalização de 25MHz e utiliza a codificação Manchester. Esse esquema pode atingir uma distância de até 100 metros.
b) **100Base-TX:** usa o esquema de par trançado sem blindagem de categoria 5, além do projeto ser mais simples, possui uma velocidade de sinalização de 125 MHz. Esse sistema é full-duplex, ou seja, podem transmitir a 100Mbps em um par trançado e recebem em 100Mbps em outro par trançado ao mesmo tempo. Esse esquema pode atingir uma distância de até 100 metros.
c) **100Base-FX:** utiliza dois filamentos de fibra multimodo, um para cada sentido, sendo também full-duplex, com 100Mbps em cada sentido. Nesse sistema, a distância entre uma estação e o Switch pode ser de até 2Km.

- **Redes Ethernet de 1Gbps**

Após o sucesso da Fast Ethernet, o comitê 802.3 começou a desenvolver uma Ethernet ainda mais rápida, e em 1999 surgiu o padrão 802.3ab apelidada de Gigabit Ethernet, dez vezes mais rápida do que a Ethernet anterior e manteve a compatibilidade com os padrões Ethernet existentes (Tanenbaum & Wetherall, 2021). A Gigabit Ethernet suporta cabeamento de cobre e de fibra, com diferentes distâncias de segmentos, por isso, foi dividida em quatro especificações, que são:

a) **100Base-FX:** utiliza dois filamentos de fibra multimodo, um para cada sentido, sendo também full-duplex, com 100Mbps em cada sentido. Nesse sistema, a distância entre uma estação e o Switch pode ser de até 2Km.
b) **1000Base-SX**: usa o cabeamento de fibra óptica, possui uma distância máxima do segmento de 550 metros e tem como vantagem utilizar a fibra multimodo (50, 62 e 5 micra).
c) **1000Base-LX:** usa o cabeamento de fibra óptica, possui uma distância máxima do segmento de 5000 metros e tem como vantagem utilizar o modo único (10 micra) ou multimodo (50, 62 e 5 micra).
d) **1000Base-CX:** usa o cabeamento com 2 pares de STP, possui uma distância máxima do segmento de 25 metros e tem como vantagem utilizar o cabo de par trançado blindado.
e) **1000Base-T:** usa o cabeamento com 4 pares de UTP, possui uma distância máxima dos segmentos de 100 metros e tem como vantagem o cabo UTP padrão na categoria 5.

Abaixo está uma tabela elaborada pelo autor, que faz a análise comparativa da evolução da tecnologia Ethernet:

Característica	Ethernet 10Base-T	Ethernet 100Base-T	Ethernet 1000Base-T
Padrão IEEE	802.3 (10Base-T)	802.3u (100Base-TX)	802.3ab (1000Base-T)
Taxa de transmissão	10 Mbps	100Mbps	1000 Mbps (1Gbps)

Meio físico	Par trançado (Cat3) ou coaxial	Par trançado (Cat5)	Par trançado (Cat5e ou superior)
Modo de operação	Half-duplex (CSMA/CD) ou full-duplex	Full-duplex predominante	Full-duplex
Tamanho do Frame	64-1518 bytes	64-1518 bytes	64-1518 bytes
Aplicações típicas	Redes antigas (década de 1990)	Redes corporativas básicas	Redes modernas (LANs, data centers)
Latência	Alta	Moderada	Baixa
Escalabilidade	Limitada	Adequada para pequenas/médias redes	Alta (Suporta tráfego intenso)

Tabela 4: análise comparativa da evolução da tecnologia Ethernet

Fonte: Elaborado pelo autor

2.1.5.2. SIP (*Session Initiation Protocol* – RFC 3261)

Segundo o autor (Peterson & Davie, 2021) o protcolo *Session Initiation Protocol (SIP)*, definido na RFC 3261, é um protocolo de sinalização baseado em texto utilizado para estabelecer, modificar e terminar sessões multimédia, como voz, vídeo e mensagens, em redes IP.

De acordo com (Comer & Droms, 2022) o protocolo SIP segue um modelo cliente-servidor, semelhante ao HTTP, utilizando requisições e respostas, e destaca-se pela flexibilidade, suportando mobilidade, redirecionamento e integração com outros protocolos, como RTP/RTCP para transmissão de mídia. Opera normalmente nas portas 5060 (sem criptografia) ou 5061 (com TLS).

Entre as suas vantagens estão a leveza e a extensibilidade, sendo amplamente adotado em soluções de VoIP, como softphones e sistemas como o Asterisk. No entanto, depende de protocolos adicionais, como RTP e SDP, para o transporte efetivo de mídia.

As suas aplicações principais incluem VoIP, videoconferência e mensagens instantâneas.

2.1.6. Qualidade de Serviço *(Quality of Service)* em redes de dados, voz e vídeo

2.1.6.1. Qualidade de Serviço

Segundo (Kurose & Ross, 2020), QoS (*Quality of Service* – Qualidade de Serviço) refere-se a um conjunto de técnicas e mecanismos utilizados em redes de computadores para garantir um desempenho adequado a diferentes tipos de tráfego, como voz, vídeo ou dados críticos, mesmo em condições de congestionamento.

No entendimnto do autor, qualidade de serviço, então, pode ser definida por dois pontos de vista: o do lado do usuário e o da rede.

Sob ponto de vista do usuário, é a qualidade percebida do tipo de serviço/aplicação que é contratado da provedora de serviço.

Sob ponto de vista da rede, a qualidade de serviço depende da alocação dos seriços de comunicação disponíveis para manter certos parâmetros da rede em patamares necessários à oferta adequada de cada tipo de serviço requesitado.

Logo para prover qualidade de serviço, a rede precisa de:

- Diferenciar entre os tipos de fluxos de tráfego e de serviço para que sejam tratados diferentemente entre si;
- Tratar as diversas classes de serviço para que estas recebam tratamento diferenciado noque concerne a garantias na alocação dos recursos da rede.

A figura abaixo sumariza os requisitos necessários para prover qualidade de serviço, em blocos funcionais de um roteador IP, de acordo com o que foi discutido acima.

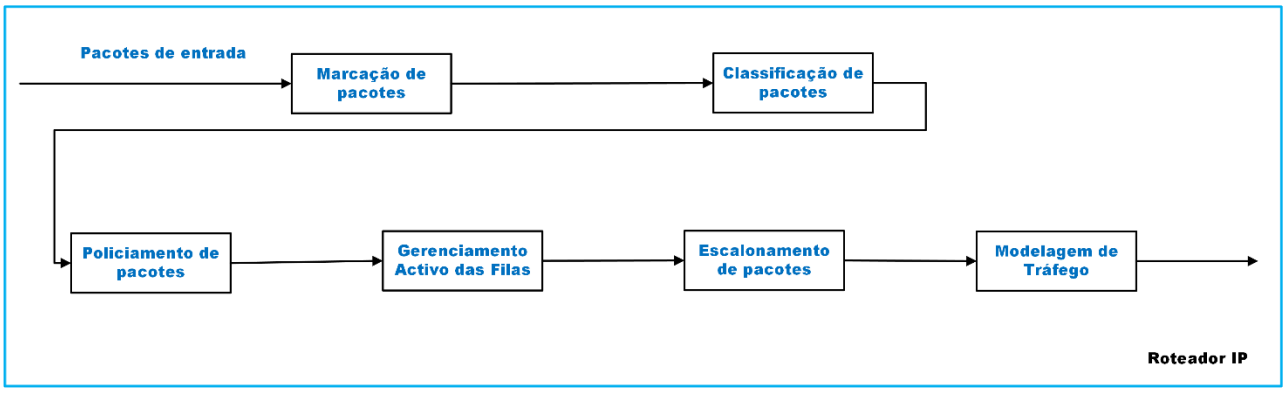


Figura 10: Requisitoos necessárioos para QoS

Fonte: Adaptado de (Kurose & Ross, 2020)

- **Atraso**

(Kurose & Ross, 2020) definem atraso como sendo o tempo medido entre o momento que um pacote de dados ingressa no sistema e o momento em que o destinatário recebe o pacote.

Em relação aos tipos de aplicações consideradas, o atraso deve obedecer às seguintes relações:

Aplicações de áudio: para a manutenção de um serviço satisfatório é necessário baixo atraso, máximo e médio. O limite máximi suportável de atraso em aplicações de áudio é de ordem de 400 ms.

- **Jitter**

Para (Kurose & Ross, 2020) o Jitter é defido como uma grandeza que expressa a flutuação temporal de atraso. Pode ser caracterizada por meio da variância estatísctica da variável aleatóriaque define o atraso dos pacotes, ou pode ser simplismente definida como o valor máximo desta mesma variável. Seu efeito é diferenciado em aplicações de vídeo e áudio, pois estas aplicações sãotípicas de tempo real.

- **Taxa de transmissão de dados**

Ainda para (Kurose & Ross, 2020) a taxa efectiva de transmissão de dados (para distinguir da taxa normal de transmissão de dados), é a velocidade com que os pacotes de cada tipo de aplicação percorrem o caminho entre origem e destino no que concerne à transmissão da informação. Sendo assim esta taxa é sensivel, a atrasos, retransmissões, e tudo aquilo mais que temporalmente afeta a transmissãodos pacotes.

- **Técnicas de QoS para priorização de tráfego**
  a) Classificação e marcação
     - Classificação: Identifica o tipo de tráfgo (Voz, Vídeo ou Dados);
     - Marcação: Usa campos como DSPC (DiffServ) ou COS (802.1p) para priorizar pacotes.
  b) Filas Prioritárias (Queuing)

- LLQ (Low Latency Queuing): Prioriz tráfego sensível a atrasos (voz).
- CBWFQ (Class-Based Weighted Fair Queuing): Aloca banda proporcionalmente para diferentes classes.

c) Policing e Shaping
- Policing: Descarta pacotes que excedem ataxa contratada;
- Shaping: Retarda pacotes para evitar congestionamento.

d) Fragmentação e interleaving
- Útil em redes com linkslentos (Voip sobre WAN), reduzindo o atraso na transmissão de pacotes (voz).

- **Protocolos e Padrões de QoS**
  - *Diffserv* (*Differentiated Services*): Prioriza tráfego com base no campo DSCP no cabeçalho;
  - *IntServ* (Integrated Services**):** Reserva recursos fim a fim (RSVP);
  - *MPLS QoS*: Usado em rede MPLS para garantir SLAs entre provedores;
  - 802.1/Q: Priorização em redes Ethernet (VLANs).
- **Boas Práticas para Implementação de *QoS***

1. Identificar tráfego crítico (*VoIP*, Videoconferênia);

2. Priorizar em roteadores / Switches usando LLQ ou CBWFQ

3. Monitorar continumente com ferramentas como wireshark, PETG, SolarWids.

4. Testar em ambiênte real antes de implementar em produção.

2.1.6.2. Relação entre redes de dado, vídeo, voz e QoS

As redes de dados, voz e vídeo exigem diferentes níveis de qualidade de serviço *(QoS - Quality of Service)* para garantir desempenho adequado, especialmente em ambientes onde os recursos de rede são compartilhados. A QoS é essencial para priorizar tráfego crítico, como chamadas de voz e streaming de vídeo, evitando atrasos, perdas de pacotes e degradação da experiência do usuário. (Pfleeger & Pfleeger, 2015).

Abaixo está uma tabela que ilustra as caracteristicas dos diferentes tipos de tráfego:

Tipo de tráfego	Requisitos de QoSExemplo	Exemplos
Voz (VoIP)	Baixa latência (<150 ms), baixo jitter, baixa perda de pacotes	Chamadas VoIP (Zoom, Skype)
Vídeo	Largura de banda consistente, baixo jitter, latência moderada	Streaming (YouTube, Netflix), Videoconfência
Dados	Tolerante a atrasos, mas exige integridade (sem perda de pacotes)	Download de arquivos, e-mail, navegação

Tabela 5: *QoS* para diferentes tipos de tráfego

Fonte: Adaptado de (Kurose & Ross, 2020)

A *QoS* é vital para garantir que redes que transportam voz, vídeo e dados ofereçam desempenho adequado. Sem *QoS*, aplicações sensíveis a latência podem sofrer degradação, impactando a experiência do usuário. A implementação requer planeamento, configuração adequada e monitoramenitorização contínua.

2.1.7. Problemas comuns em redes de computadores

Uma rede de computadores é composta por diversos tipos de equipamentos que se comunicam entre si trabalhando juntos, e cabos de transmissão para o tráfego de pacotes, nesse sentido é muito comum haver falhas de equipamentos ou de meio de transmissão, comprometendo o bom funcionamento da rede.

Abaixo está uma tabela que ilustra o tipo de falha, a causa e as soluções possíveis:

Problema	Causas Comuns	Soluções Possíveis
Sem Conexão (Indisponibilidade)	Cabo desconectado, falha no roteador / modem, configuração incorreta de IP	Verificar cabos, reiniciar roteador, verificar configurações e IP/DHCP

Lentidão na rede	Congestionamento de tráfego, limitação di *ISP*, hardware obsoleto	Priorizar tráfego (*QoS*), actualizar roteador, verificarplanode internet
Quedas intermitentes	Instabilidade do provedor, interferência *Wi-Fi*, superaquecimento do roteador	Testar conexão cabeada, reposicionar roteador, contactar *ISP*
Problemas de DNS	Servidor DNS inacessível, cache corrompido	Usar DNS alternativo (Google: 8.8.8.8), limpar cache (ipconfig / flushdns)
Wi-Fi fraco ou instável	Interferência de outros dispositivos, distância do roteador, paredes espessas	Mudar canal Wi-Fi, usar repetidor de sinal, optar por conexão 5GHz
Bloqueio de portas / Firewall	Configurações restritivas de firewall / antiviros	Verificar regrasde firewall, liberar portas necessárias
Ataques DdoS / Malware	Tráfegomalicioso, dispositivos infectados	Usar firewall, actualizar sistemas, moitorar rede
IP conflitante	Dois dispositivos com o msmo IP na rede	Reiniciar dispsitivos, configurar DHCP correctamente
Problemas físicos	Cabo danificado, falha na placa de rede, roteador com defeito	Substituir cabos,testar em outra porta / Switch

Tabela 6: Tipos de falhas e suas soluções

Fonte: Adaptado de (Stallings & Brown, 2018), citado por (Chiziane, 2022)

- **Outras possiveis soluções são:**

Usar comandos de diagnóstico como *ping, tracert (Windows)* / *traceroute* (Linux/macOS), *ipconfig* / *ifconfig* ou ainda actualizar *firmware* e *drivers* de rede.

2.1.8. Segurança em redes de computadores *(VLANs)*.

No entendimento do autor, a segurança cibernética é imprescindível em redes de computadores, pois a sua negligência pode causar danos catastróficos e irreversíveis. Se os computadores trocam dados entre si na rede, então torna-se necessário criar mecanismos que permitam que esses dados trafeguem em segurança, sem serem interceptados, e, caso haja uma interceptação, que não possam ser lidos.

Segundo (Pfleeger & Pfleeger, 2015) as VLANs são redes lógicas criadas dentro de uma infra-estrutura física única, permitindo a segmentação de dispositivos em grupos isolados, mesmo que compartilhem o mesmo hardware (como switches). Isso melhora a segurança, o desempenho e o gerenciamento da rede.

2.1.8.1. Benefícios das VLANs para a segurança

- Isolamento de Tráfego: VLANs impedem que dispositivos de grupos diferentes se comuniquem diretamente sem passar por um roteador ou firewall, reduzindo riscos como ataques sniffing ou propagação de malwares.
- Controle de Acesso: Políticas de segurança podem ser aplicadas por VLAN, restringindo acesso a recursos sensíveis.
- Segmentação de Domínios de Broadcast: Limita o escopo de broadcasts, dificultando ataques como broadcast storms.

2.1.8.2. Riscos e Vulnerabilidades

Os autores (Pfleeger & Pfleeger, 2015) alertam sobre possíveis falhas na implementação de VLANs:

- VLAN *Hopping*: Ataques onde um invasor envia tráfego malicioso para uma VLAN não autorizada, explorando configurações inadequadas de switches (como trunking aberto).
- Erros de Configuração: Má definição de VLANs pode levar a vazamentos de tráfego ou exposição de dados.
- Dependência de Dispositivos Físicos: A falha de um switch pode afetar múltiplas VLANs.

2.1.8.3. Melhores práticas

Os autores (Pfleeger & Pfleeger, 2015) recomendam:

- Desativar trunking automático em switches e configurar portas manualmente.
- Usar mecanismos como 802.1Q para *tagging* seguro de frames.
- Implementar *VLAN Access Control Lists* (VACLs) para filtrar tráfego entre VLANs.
- Auditar regularmente as configurações de VLAN para evitar brechas.

Segundo (Pfleeger & Pfleeger, 2015), VLANs são ferramentas poderosas para segurança em redes, mas sua eficácia depende de configuração rigorosa e monitoramento contínuo. A obra reforça que a segurança não é alcançada apenas com tecnologia, mas também com boas práticas de gestão e políticas claras.

2.2. Documentação e Planeamento de Sistemas de Informação

A área das Tecnologias de Informação e Comunicação (TIC) é bastante sensível, dado que proporciona serviços com um elevado nível de criticidade, especialmente em ambientes corporativos. Por este motivo, foram desenvolvidas normas e frameworks para melhorar a gestão desses serviços.

Neste trabalho, abordaremos de forma superficial as normas ISO19770, que são amplamente reconhecidas e valiosas, sobretudo no que diz respeito à gestão de equipamentos e à documentação da rede.

Estas ferramentas ajudam a garantir a eficiência, segurança e continuidade dos serviços de TIC, contribuindo para uma operação mais robusta e bem estruturada.

2.2.1. ISO 19770

Segundo (ISO/IEC 19770, 2024), a norma ISO 19770 é um conjunto de padrões internacionais para Gestão de ativos de Tecnologias de Informação (ITAM – *IT Asset Management*), incluindo hardware, software e licenças. No contexto da documentação de uma rede de computadores, esta norma fornece diretrizes para estruturar e manter registros precisos dos ativos de TI, garantindo conformidade, segurança e eficiência operacional.

2.2.1.1. Principais contribuições da ISO 19770 para a documentação de Infra-estruturas redes:

- **Inventário padronizado de activos**

Define métodos para catalogar *hardware* (servidores, switches, routers) e software (sistemas operacionais, aplicações) em um formato uniforme, facilitando a rastreabilidade.

Utiliza *tags* de identificação (como *SWID* para software e *HWID* para hardware) para automatizar a documentação e evitar inconsistências.

- **Gestão de licenças de software**

Estabelece esquemas para documentar direitos de uso (via *ENT tags*), prazos de validade e métricas de consumo, evitando multas por não conformidade .

Integra-se a sistemas financeiros para alinhar custos de licenças com a infra-estrutura registrada .

- **Ciclo de vida dos activos**

Registra desde a aquisição até a desativação de equipamentos, incluindo manutenções e atualizações, o que é crucial para planear actualizações ou substituições na rede.

- **Auditoria e conformidade**

Oferece modelos para criar trilhas de auditoria, documentando alterações na rede (configurações de firewall, políticas de acesso) e garantindo alinhamento com regulamentações.

- **Integração com outros padrões**

Pode ser combinada com normas como a ISO/IEC 27032 (segurança cibernética) para documentar ativos críticos e vulnerabilidades na rede .

- **Benefícios para redes de computadores:**
    - Redução de riscos: Minimiza falhas devido a equipamentos desatualizados ou licenças expiradas;
    - Optimização de custos**:** Evita compras desnecessárias ao identificar subutilização de recursos.
    - Transparência: Facilita a comunicação entre equipas de TI, gestão e stakeholders através de relatórios padronizados.

De um modo geral, a ISO 19770 ajuda a transformar a documentação de redes em um processo sistemático, contribuindo para governança de TI e continuidade operacional. Para implementação prática, ferramentas como módulos de *ITAM* (*NetEye*) podem automatizar partes do processo.

3. Capítulo III – Caso de Estudo

3.1. Faculdade De Engenharia Da Universidade Eduardo Mondlane (FEUEM)

A Faculdade de Engenharia constitui uma unidade orgânica da Universidade Eduardo Mondlane, dispondo de autonomia pedagógica e científica no âmbito dos cursos que leciona, bem como de autonomia administrativa, patrimonial e financeira relativamente aos seus próprios recursos, dentro dos limites legais estabelecidos. A Faculdade de Engenharia usufrui ainda de autonomia regulamentar e disciplinar, igualmente enquadrada nos parâmetros legais vigentes.

A Faculdade de Engenharia foi fundada em 1962 com uma estrutura de chefia centralizada, onde cada curso estava associado a um Departamento específico, oferecendo inicialmente quatro cursos: Engenharia Civil, Engenharia Electrotécnica, Engenharia Mecânica e Engenharia Química, com duração de seis anos (três anos dedicados a matérias gerais-básicas e três anos a disciplinas específicas de engenharia, incluindo gestão). Após a Independência, os departamentos assumiram o estatuto de Faculdade, adoptando uma gestão não centralizada mas com coordenação inter-faculdades, estrutura que se manteve até 1980, quando se regressou ao modelo inicial de 1962. Em 1970, a duração dos cursos foi reduzida para cinco anos (com dois anos de formação geral-básica), as disciplinas passaram a ser semestrais (em vez de anuais) e as horas de ensino foram aumentadas, tendo sido introduzidos nesse mesmo ano os cursos de Engenharia de Minas e Engenharia Metalúrgica, os quais, no entanto, não se mantiveram devido à sua longa duração (cinco e oito anos, respectivamente).

Actualmente, a Faculdade de Engenharia é composta por cinco departamentos académicos, nomeadamente Departamento de:

- Engenharia Civil (DECI);
- Engenharia Electrotécnica (DEEL);
- Engenharia Mecânica (DEMA);
- Engenharia Química (DEQUI);
- Cadeiras Gerais (DCG);

Cinco Departamentos não Académicos:

- Departamento de Património e Manutenção (DPM);
- Departamento do Registo Académico (DRA);
- Departamento de Tecnologias de Informação e Comunicação (DTIC);
- Departamento de Administração e Finanças (DAF);
- Departamento de Informação e Biblioteca (DIB); e um
- Centro de Estudos de Engenharia – Unidade de Produção (CEE-UP).

No conjunto dos seus Departamentos, a FEUEM oferece oito cursos de licenciatura, nas áreas de Engenharia Civil, Engenharia Eléctrica, Engenharia Electrónica, Engenharia Informática, Engenharia Mecânica, Engenharia de Gestão Industrial, Engenharia Química e Engenharia do Ambiente.

3.1.1. Visão, Missão e Valores

3.1.1.1. Visão

A Faculdade de Engenharia tem como Visão:

- Sermos uma referência nacional, regional e internacional na formação, treinamento e investigação em engenharia.

A Faculdade de Engenharia orienta a sua actividade para os seguintes objectivos gerais:

- Providenciar uma educação padrão à sociedade e conhecimento científico internacional;
- Providenciar compreensão da importância da tecnologia em áreas como economia, ecologia e sociedade no geral.

3.1.1.2. Missão

A Faculdade de Engenharia tem como Missão:

- Desenvolver competências e conhecimentos científicos na área de engenharia e contribuir na formação do homem.

3.1.1.3. Valores

A Faculdade de Engenharia tem como pilares da sua atuação os seguintes valores:

- Liberdade Académica;
- Ética e Imparcialidade;

- Responsabilidade;
- Confiança;
- Proatividade;
- Colegialidade;
- Engajamento Social e Comunitário;
- Autonomia Institucional.

3.1.2. Estrurura Orgânica

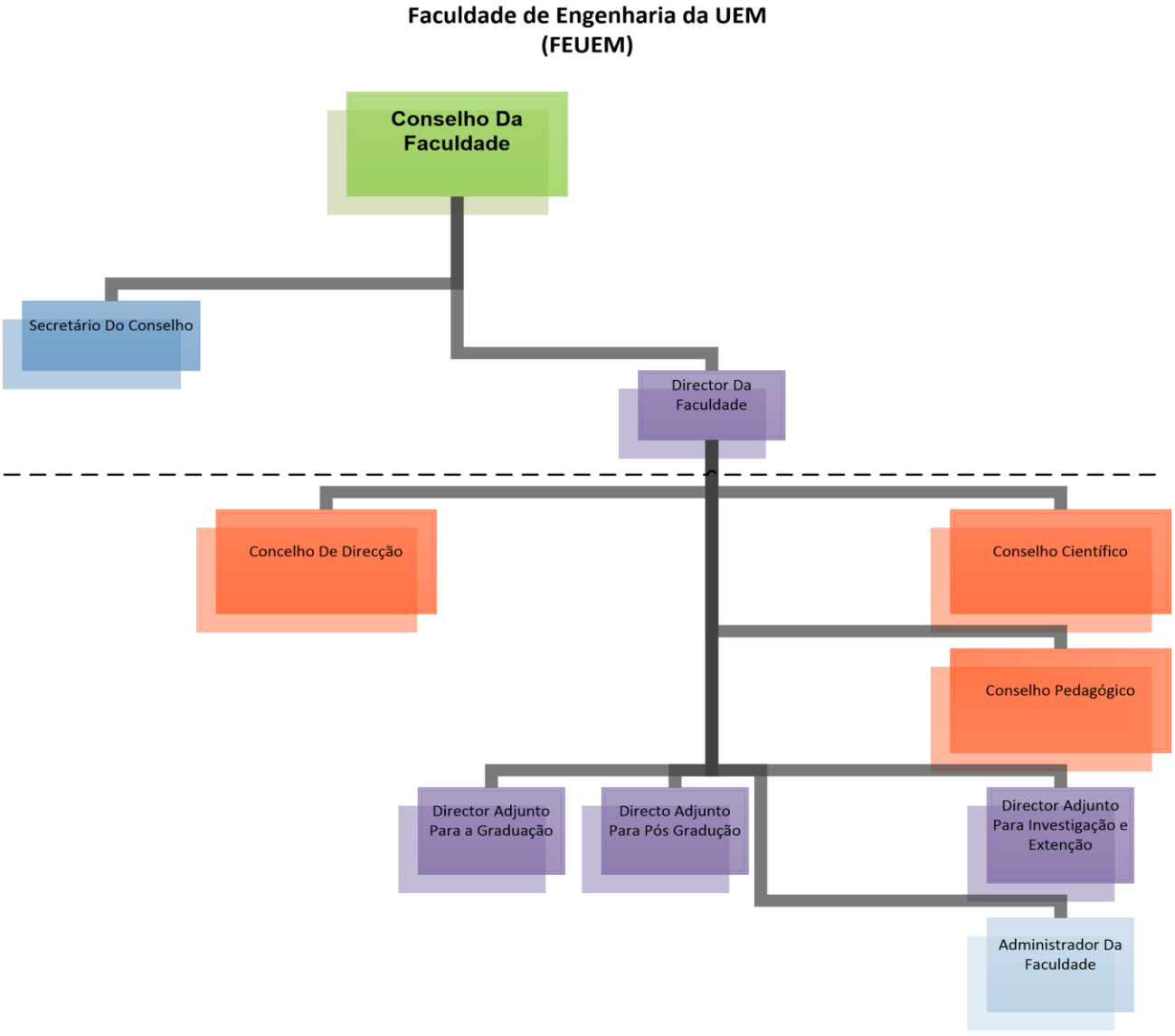


Figura 11: Estrutura orgânica da FEUEM

Fonte: Elaborado pelo autor

3.2. Descrição da situação actual

Esta secção do relatório descreve a situação atual da infra-estrutura de rede da Faculdade de Engenharia da Universidade Eduardo Mondlane (FEUEM), identificando problemas críticos por departamento. A análise é segmentada por departamentos para destacar divergências específicas, embora a maioria dos problemas sejam comuns.

3.2.1.1. Descrição da situação actual da sala de servidores da DEEL

Atualmente, a Faculdade de Engenharia da UEM (FEUEM) possui na sua infra-estrutura de rede uma sala de servidores onde se encontra um router (backbone) que recebe o sinal proveniente do Centro de Informática da UEM (CIUEM) através de fibra ótica. Esse sinal é distribuído por todos os departamentos da faculdade a partir de um switch gerível (Switch L3) da Cisco, como ilustra a figura abaixo:

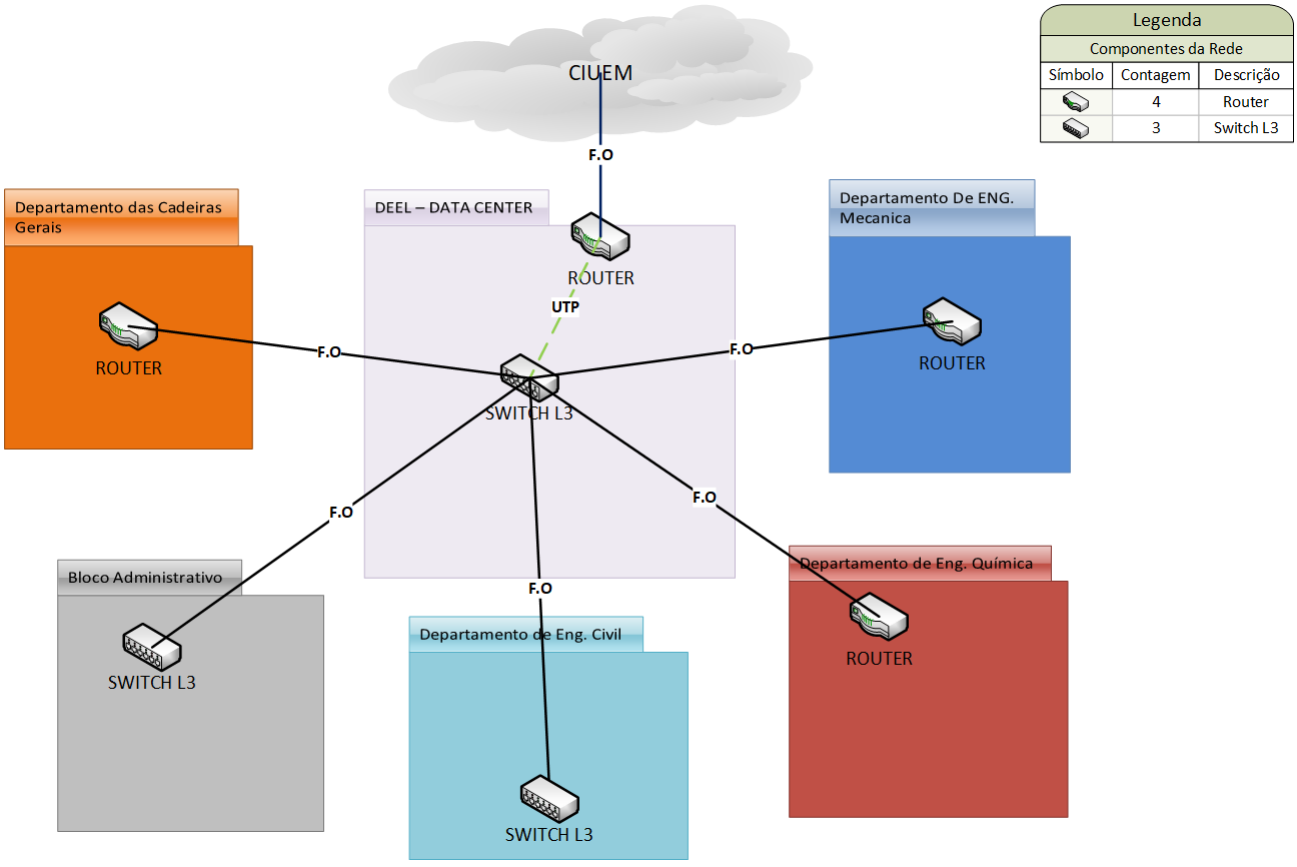


Figura 12: Topologia do Data Center da DEEL

Fonte: Elaborado pelo autor

3.2.1.2. Descrição da situação actual do departamento do bloco administrativo(DBA)

A infra-estrutura do Departamento do Bloco Administrativo é destribuida da seguinte forma:

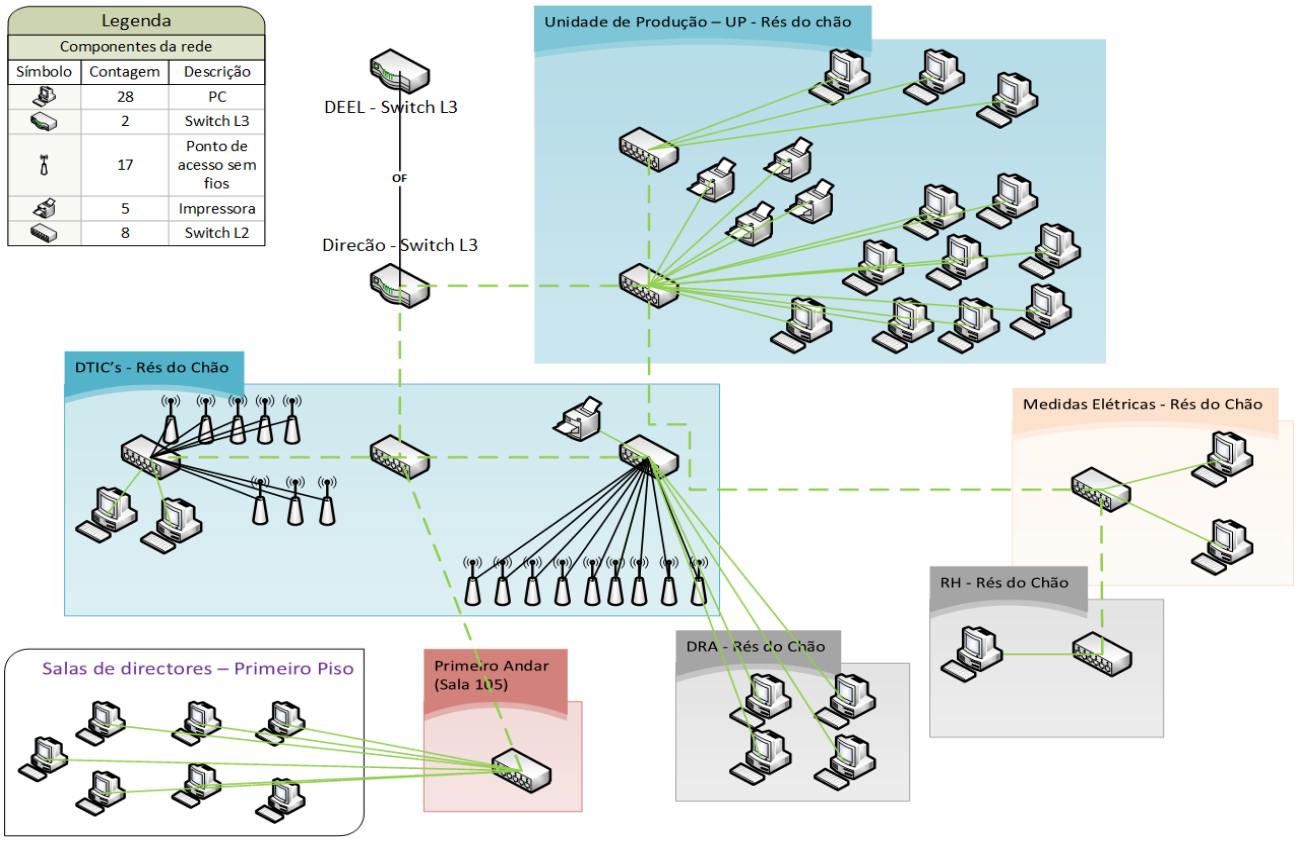


Figura 13: Topologia actual do Bloco Administrativo

Fonte: Elaborado pelo autor

a) Rés do Chão

- Um (1) Switch L3 da Cisco com capacidade de 1Gbps que recebe sinal da DEEL, dois Switch's L2 na unidade de produção, Três (3) Switch's L2 na sala do DTIC, um (1) Switch L2 na sala das medidas electricas, um Switch L2 na sala do RH;
- Desassete (17) AccessPoints ligados aos switches da DTIC, esses AccessPoinsts destribuem o sinal pelo bloco administrativo, excepto na unidade de produção.

b) Primeiro Piso

- Um (1) Switch L2 na sala 105, com capacidade de 1Gbps da Cisco que recebe o sinal do Switch da DTIC;
- Sete (7) Computadores de mesa conectados ao Switch L2 da sala 105.

Edifício do DBA												
Piso	Router				Switch				AccessPoint		PC	Impressora
	Qtde	Capac	Vendor	Mdl	Qtde	Capac	Vendor	Mdl	Qtde	Vendor	Qtde	Qtde
Rés do Chão	0	-	-	-	8	1Gig	Microtik, Cisco, TP Link	2960-24TT-L, CRS326-24G-2S+RM, TL-SG1024	15	Microtik, TP Link	-	5
Primeiro Piso	0	-	-	-	1	1Gig	Cisco Meraki	MS210-24P	8	Microtik, TP Link	16	-
Total	0	N/A	-	-	9	N/A	N/A	N/A	23	-	16	5

Tabela 7: Descrição do Bloco Administrativo

Fonte: Elaborado pelo autor

3.2.2. Descrição das vulnerabilidades encontradas na rede da FE-UEM

Esta secção será separada em duas, onde a primeira irá descrever as vulnerailidades físicas e lógicas gerais e a segunda secção irá fazer menção das vulnerabilidades individuais por departamento.

3.2.2.1. Descrição das vulnerabilidades físicas comuns nos departamentos

A infra-estrutura física da rede da FEUEM apresenta os seguintes problemas críticos:

- **Cabeamento inadequado:**
  - Cabos mal instalados e degradados nas salas de máquinas (salas de informática).
  - Falta de padronização nas cores dos cabos, dificultando a identificação das conexões.
- **Organização e identificação deficientes:**

- Equipamentos mal distribuídos nas racks.
- Tomadas de cabos Ethernet obsoletos (Cat5).
- Falta de etiquetagem (labels) nas portas dos switches e tomadas Ethernet, prejudicando a manutenção e o gerenciamento.

- **Segurança física comprometida:**
  - Ausência de firewalls em pontos críticos (sala de servidores, salas de informática e bloco administrativo).
  - Access Points removidos em alguns locais, causando falhas de cobertura Wi-Fi.
  - Ausência de câmeras de segurança em alguns pontos críticos como os corredores e salas de informática.

3.2.2.2. Descrição das vulnerabilidades Lógicas comuns em cada departamento

A configuração lógica da rede apresenta as seguintes fragilidades:

- **Falta de políticas de acesso:**
  - Não há controle adequado de usuários e dispositivos na rede;
  - Roteadores mal configurados:
    a) Ausência de protocolo de roteamento dinâmico (OSPF) entre os roteadores.
    b) Falta de restrições de acesso via ACL (Access Control Lists).
- **Switches sem gerenciamento eficiente:**
  - Switches gerenciáveis não possuem endereço IP para administração remota.
  - Em gabinete com múltiplos switches, não há protocolo de redundância (RSTP), aumentando o risco de falhas.
  - Falta de segmentação das LAN's por VLAN's, aumentando a vulnerabilidade da rede, principalmente em departamentos de gestão e finanças.
- **Qualidade de serviço (QoS) inexistente:**
  - Não há priorização de tráfego para dados, voz e vídeo, o que pode comprometer o desempenho de serviços críticos.

3.2.2.3. Descrição das vulnerabilidades individuais por departamento

a) DEEL Data Center

- **Topologia:** Arquitetura em estrela com single point of failure (switch central Cisco SX550X-16FT);
- **Segurança:** Ausência de firewall dedicado (dependência de NAT no roteador principal);
- **Monitoramento**
  - Não há sistema centralizado (Nagius, Zabbix, PRTG);
  - Congestionamento na VLAN principal (picos de 95% de uso da banda).

b) DEEL

- **QoS:** Switches (não gerenciáveis) impossibilitam QoS para equipamentos críticos.
- **Segurança:**
  - Gabinetes equipamento de rede acessíveis a não técnicos (Laboratório de informática);
  - Ausência de registros de acesso (logs).

c) DEQI

- **Topologia:** Existem dois servidores de última geração com cerca de 8T de armazenamento SSD cada, que não estão em uso ainda;

d) DECI

- **Topologia:** Ausência de conexão com o backbone da rede, actualmente o sinal provém do DEMA.

e) DCG

- **Topologia:** Ausência de tomadas Ethernet RJ45 e AccessPoits na biblioteca do primeiro piso, impossibilitando o acesso a rede aos estudantes.

f) DBA

- **Topologia:** Switch's obsoletos, com capacidade de propagação de broadcast muito baixa (100mbps);
- **Serviços:** Auséncia de Vlans para segmentar os serviços da rede, aumentando neste caso a vulnerabilidade da mesma.

4. Capítulo IV – Proposta de Solução

4.1. Escolha da solução ideal

A existência de um problema, pressupõe a existência de diversas formas de resolvê-lo. Para os problemas da rede da FEUEM foram analisadas três possíveis soluções. Abaixo são detalhadas as três propostas de soluções:

a) Reestruturação completa e documentação da infra-estrutura da rede

A presente proposta tem como objetivo principal resolver os constrangimentos identificadados na rede actual da FEUEM através de um processo de reestruturação, dividido em duas etapas fundamentais.

Na Primeira etapa, será realizado um inventário detalhado de todos osctivos de rede, registrando os equipamentos existentes e as suas respectivas localizações, de modo a garantir um mapeamento completo da infra-estrutura.

A segunda etapa consistirá na reestruturação física e lógica da rede, iniciando-se pela substituição de equipamentos obsoletos, como cabos UTP de categoria 5, Switches com capacidade limitada de 100Mbps e UPSs que não garantem a proteção adequada dos dispositivos. Estes serão substituidos por soluções modernas de alto desempenho, incluindo a implementação de firewalls da próxima geração para reforço da rede.

Paralelamente será proposta uma topologia de rede Two-Tier, assegurando maior desempenho, disponibilidade e escalabilidade, além de eliminar o risco de ponto único de falha (Single point of failure). A rede será segmentada em VLANs, as portas dos equipamentos serão devidamente etiquetadas e será estabelecida uma padronização cromática para os cabos, conforme o tipo de equipamento a que se destinam.

Posteriormente será feita a documentação completa da rede.

A implementação desta solução trará benefícios significativos, tais como uma maior disponibilidade da rede, aumentando a largura de banda com redução de perdas, reforço da segurança e uma infra-estrutura preparada para aintegração de novas tecnologias futuras. Desta forma, a rede ficará optimizada, robusta e capaz de suportar exigências actuais e evolutivas.

b) Substituição dos equipamentos obsoletos por equipamentos modernos

A presente proposta tem como objectivo principal resolver os constranimentos identificados na rde actual da FEUEM através da substição dos equipamentos obsoletos por soluções tecnológicas modernas.

O processo de modernização foca-se exclusivamente na renovação do parque tecnológico, nomeadamente na aquisição e instalação de novos switches, routers e UPSs de alto desempenho, sem alterar a topologia ou os serviços de rede existentes. Esta abordagem assegura uma optimização da infra-estrutura física garantindo maior eficiência e fiabilidade, mantendo a configuração lógica actual.

A solução proposta basea-se na implementação de equipamentos de rede de última geração, promoveno não apenas a melhoria do desempenho, mas também a uniformização dos dispositivos para uma gestão mais eficiênte e organizada. Contudo, importa referir que esta intervenção à componente física da rede, não contemplando alterações ao nível da topologia lógica ou dos serviços implementados.

Desta forma, a FEUEM beneficiará de uma infra-estrutura de rede actualizada, com equipamentos robustos e de elevada capacidade, preparadapara responder àsexigências actuais, sem comprometer a escalabilidade da configuração existente.

c) Instalação de firewalls e segmentação da rede por Vlans

A presente proposta tem como objetivo principal resolver os constrangimentos de segurança identificados na rede atual da FEUEM, através da implementação de duas medidas fundamentais: a instalação de firewalls e a segmentação da rede em VLANs.

Esta iniciativa concentra-se exclusivamente no reforço da segurança da infraestrutura de rede. A instalação de firewalls permitirá estabelecer uma eficaz segurança perimetral, protegendo a rede contra acessos não autorizados e potenciais ameaças externas.

A implementação de VLANs permitirá: Segmentar a rede por departamentos ou serviços, Melhorar a organização lógica da infraestrutura, Facilitar a gestão de acessos e políticas de segurança, Isolar tráfego entre diferentes áreas funcionais e Otimizar o desempenho geral da rede.

Esta solução proporcionará uma estrutura de rede mais segura e melhor organizada, mantendo intacta a sua componente física atual. Trata-se de uma medida essencial para proteger os ativos de informação da FEUEM, sem alterar a topologia de rede existente.

4.1.1. Análise comparativa das soluções propostas

Antes de realizar a análise comparativa das soluções propostas serão definidos os requisitos que constituem critérios de avaliação:

- **Conectividade**

Segundo (Tanenbaum & Wetherall , 2011), conectividade é a capacidade de interligar dispositivos (computadores, roteadores, servidores) para permitir comunicação bidirecional.

"A conectividade é a base de qualquer rede, permitindo que entidades heterogêneas se comuniquem."

- **Confiabilidade**

Segundo (Tanenbaum & Wetherall , 2011), confiabilidade é a garantia de que os dados são entregues sem erros, no tempo certo e na ordem correta.

"Redes confiáveis devem lidar com falhas de hardware, software e congestionamento sem prejudicar a comunicação."

- **Escalabilidade**

Segundo (Tanenbaum & Wetherall , 2011), escalabilidade é a capacidade da rede de crescer (em usuários, tráfego ou dispositivos) sem degradação do desempenho.

"A Internet é um exemplo de rede escalável, mas desafios persistem com o crescimento exponencial de dispositivos IoT."

- **Segurança**

Segundo (Tanenbaum & Wetherall , 2011), segurança é a proteção contra acessos não autorizados, ataques e vazamentos.

"Segurança é um requisito crítico, especialmente em redes abertas como a Internet, onde ataques são frequentes."

- **Desempenho**

Segundo (Tanenbaum & Wetherall , 2011), o desempenho de uma rede refere-se à sua capacidade de transmitir dados de forma eficiente, atendendo a requisitos como velocidade, tempo de resposta e confiabilidade, conforme as necessidades das aplicações e dos usuários.

"O desempenho de uma rede é determinado por um equilíbrio entre throughput, latência e confiabilidade. Projetistas devem otimizar esses fatores conforme a aplicação-alvo."

- **Qualidade de Serviço**

Segundo (Tanenbaum & Wetherall , 2011), qualidade de serviço é a capacidade de priorizar certos tipos de tráfego para garantir desempenho consistente.

"QoS é essencial para aplicações em tempo real, como vídeo chamadas, que exigem baixa latência."

- **Padronização**

Segundo (Tanenbaum & Wetherall , 2011), padronização é o uso de protocolos e normas universais para permitir a comunicação entre diferentes tecnologias.

"Padrões abertos são a chave para a interoperabilidade, evitando lock-in de fornecedores."

- **Interoperabilidade**

Interoperabilidade é a capacidade que dois sistemas distintos têm de trabalhar juntos para um determinado fim.

- **Eficiência**

Segundo (Tanenbaum & Wetherall , 2011), Eficiência é a optimalização no uso dos recursos da rede (largura de banda, energia, capacidade de processamento) para minimizar desperdícios.

"Protocolos eficientes reduzem o overhead e maximizam a capacidade útil da rede. Por exemplo, o IPv6 simplifica cabeçalhos em comparação ao IPv4."

- **Custo – Efectividade**

Segundo (Tanenbaum & Wetherall , 2011), Custo – Efectividade é o equilíbrio entre os benefícios da rede (desempenho, segurança, escalabilidade) e os custos de implantação e manutenção.

"Projetistas devem escolher tecnologias que atendam aos requisitos técnicos sem tornar a rede economicamente inviável. Soluções como VLANs reduzem custos ao segmentar redes logicamente, sem hardware adicional."

A tabela abaixo é composta por oito parâmetros que são os requisitos fundamentais de uma rede de computadores, esses critérios são valorados como Baixo, Médio e Alto, com exceção de padronização e interoperabilidade que são valorados por “sim” ou “não”.

Parâmetro	Proposta a)	Proposta b)	Proposta c)
Conectividade	Alta	Média	Média
Confiabilidade	Alta	Média	Média
Escalabilidade	Alta	Média	Baixa
Segurança	Alta	Baixa	Alta
Desempenho	Alto	Médio	Baixo
Qualidade de Serviço	Alta	Baixa	Média
Padronização	Sim	Não	Não
Interoperabilidade	Sim	Não	Não
Eficiência	Alta	Média	Baixa
Custo - Efectividade	Médio	Médio	Baixo

Tabela 8: Avaliação de requisitos para a escolha da melhor solução

Fonte: Elaborado pelo autor

A tabela abaixo ilustra o critério de selecção da escolha da solução mais viável, segundo os prós e contras ilustrados na tabela acima:

Critério	Proposta a)	Proposta b)	Proposta c)
Risco técnico	Baixo	Médio	Alto
Custo – Benefício	Alto	Médio	Baixo
Futuro - Proof	Sim	Parcialmente	Não

Tabela 9: Critério de selecção de escolha da melhor solução

Fonte: Elaborado pelo autor

A solução mais viável é a proposta a), porque oferece o melhor equilíbrio entre desempenho, segurança e crescimento futuro, mesmo com um custo moderado.

4.2. Desenvolvimento da proposta de solução para a reestruturação e a documentação da rede.

Conforme demonstrado no ponto 3.2, a maioria dos problemas enfrentados pela infra-estrutura de rede da FEUEM são semelhantes, pelo que foi acordado que a proposta de solução seria implementada primeiramente no bloco administrativo, por ser o departamento que engloba os serviços mais críticos; caso a solução se revele eficaz e escalável, será então estendida aos restantes departamentos, seguindo um cronograma de prioridades claramente definido.

4.2.1. Reestruturação da rede

4.2.1.1. Substituição do tipo de cabeamento Ethernet, de Cat5 para Cat6:

A substituição do cabeamento Cat5 para Cat6 é um upgrade estratégico para redes que exigem maior velocidade, menor latência e melhor preparação para futuras demandas.

- **Comparação entre os cabos Cat5 e Cat6:**

Parâmetro	Cat5	Cat6	Ganhos com Cat6
Velocidade maxima	100Mbps (Fast Ethernet)	1Gbps (10Gbps até 55m*)	Até 100x mais rápido
Banda (Frequência)	100Mbps	250Mbps	Maior capacidade de transmisssão
Crosstalk	Problemas em redes desnsas	Reduzido (melhor trançamento)	Menos perdas de pacotes
Blindagem	UTP (Não blindado)	UTP/TCP (Opções blindadas)	Resistência a interferências
Vida útil	Obsoleto	Recomendado até 2025+	Futuro – Proof

Tabela 10: Comparação de Cabos Cat5 e Cat6

Fonte: Elaborado pelo autor

NB: *10Gbps só é garantido até 55m* (Cat6 padrão) ou 100m (Cat6A).*

- **Vantagens técnicas:**
  - Suporte a 10G Ethernet (em curtas distâncias);

- Melhor desempenho em PoE (*Power over Ethernet*) para dispositivos como câmeras IP menos retransmissões TCP (redução de latência em *Voip*/videoconfência);

➢ **Vantagens operacionais:**

- Compatibilidade retroativa (Funciona com equipamentos Cat5 e Cat5-e);
- Custo-benefício (Preço só ~20% maior que Cat5e em média).

➢ **Padronização de corres**

Aplicação	Côr do cabo	Exemplo de uso
Dados (LAN)	Azul	PC's, Impressoras
Voip/Telefonia	Amarelo	Telefones IP
Câmeras IP	Preto	Sistemas de Segurança
Wi-Fi	Branco	Acces Points
Backbone	Verde	Switch to Switch
Servidores	Vermelho	Switch to Server

Tabela 11: Padronização de corres no cabeamento

Fonte: Elaborado pelo autor

➢ **Boas práticas:**

- Etiquetar (Lablar) ambas as extremidades do cabo;
- Documentar no mapa de rede.

➢ **Materiais necessários na implementação:**

- Cabos Cat6 UTP (Ou FTP se houver interferência);
- Conectores RJ45 Cat6 (Compatíveis com 568 – A/B);
- Pactch Panels Cat6 (24/48 portas);
- Ferramentas (Alicates de crimpagem, testador de rede e toner).

4.2.1.2. Implementação do padrão de cabeamento estrurutado ANSI/TIA-568:

O cabeamento estruturado é um sistema padronizado de infra-estrutura de cabos e conectores que permite a transmissão de dados, voz e vídeo em redes de comunicação de forma organizada, flexível e escalável. Ele segue normas internacionais (como ANSI/TIA-568, ISO/IEC 11801) para garantir interoperabilidade, desempenho e facilidade de manutenção.

Segundo (Oliviero & Woodward, 2023) (em "*Cabling: The Complete Guide to Copper and Fiber-Optic Networking*"), o cabeamento estruturado é projetado para suportar múltiplos ambientes de rede sem a necessidade de alterações significativas na infraestrutura física.

A implementação segue um modelo hierárquico dividido em subsistemas, conforme definido pela norma ANSI/TIA-568:

- **Subsistema de Entrada de Edifício (EE – Entrance Facilities)**
  - Ponto de interligação entre a rede externa (provedor) e a infraestrutura interna;
  - Inclui proteção contra surtos e pontos de demarcação.
- **Sala de Equipamentos (ER – Equipment Room)**
  - Abriga os principais equipamentos de rede (switches, servidores, PBX);
  - Deve ter controle de temperatura, umidade e segurança física.
- **Backbone (Cabeamento Vertical)**
  - Conecta a ER às salas de telecomunicações (TR) ou armários de distribuição;
  - Utiliza fibras ópticas (multimodo ou monomodo) ou cabos UTP Cat 6A/7 para alta velocidade.
- **Cabeamento Horizontal**
  - Liga as TR às tomadas de rede (RJ45) nas áreas de trabalho;
  - Cabos UTP (Cat 5e/6/6A) ou fibra, com limite de 90m + 10m para patch cords.
- **Área de Trabalho (Work Area)**
  - Local onde os dispositivos finais (computadores, IP phones) são conectados;
  - Utiliza patch cords e adaptadores padronizados.
- **Sistema de Telecomunicações (TR – Telecommunications Room)**
  - Armário onde termina o cabeamento horizontal e são instalados patch panels e switches;
  - Deve seguir normas de aterramento e organização (rotulagem, gestão de cabos).

4.2.1.3. Substituição e uniformização de Switchs obsoletos não geríveis por Switchs modernos e geríveis

A FEUEM já havia elaborado um plano de aquisição e substituição de Switchs obsoletos, com capacidade máxima de 100Mbps. Esses Switchs seriam substituidos por Switchs da Cisco (Catalyst 9200L) com capacidade de entregar até 1Gbps em portas Gigabit Ethernet e 10Gbits para portas Uplink's.

Os Switchs já foram adquiridos e estão em processo de substituição. Abaixo está uma tabela que faz a análise comparativa dos Switchs obsoteletos com os Switchs recentes:

Caracteristicas	Switchs Obsoletos (100mbps)	Switchs recentes (Cisco Catalyst 9200L)
Tipo de dispositovo	Switchs Básicos (100Mbps)	Switch enterprise gerível (L2/L3)
Velocidade das portas	100Mbps (Obsoleto)	1Gbps (Gigabit Ethernet/10Gigabit Uplinks')
Gerenciamento	Não gerível	Cisco DNA Center, CLT, Web, SNTP, Net Flow
VLAN,s e QoS	Não suportado	Suporte avançado (VLANs, QoS, Politicas de tráfego)
Segurança	Mínima (Sem controle)	802.1X, ACLs, Porta Secutity, DHCP Snooping
PoE (Power over Ethernet)	Não disponivel	PoE+
Número de portas	Váriável (Depende do modelo)	24 portas (flexivel)
Latência	Alta (devido a limitação 100Mbps)	Baixa (Hardware dedicado)
Custo	Baixo (mas obsoleto)	Médio-Alto (Custo Benefício a longo prazo)

Tabela 12: Comparação de Switches obsoletos com Switches novos

Fonte: Elaborado pelo autor

A substituição dos Switches não geríveis de 100Mbps pelos Cisco Catalyst 9200L trará:

Maior desempenho (Gigabit), Controle de rede (VLANs, QoS, segurança) e Futura expansão (PoE para IP Phones/APs Wi-Fi 6).

4.2.1.4. Instalação de um firewall no ponto mais crítico (Direcção do BAD).

Em geral o bloco administrativo é o ponto mais crítico da rede da FEUEM, é onde estão instalados os serviços de gestão e finanças, é no bloco administrativo onde são processadas e documentadas as pautas finais dos estudantes, então a auséncia de um firewall naquele ponto, torna a rede totalmente exposta à possiveis ataques.

A FEUEM dispõe de um número considerável de firewalls (Firewall XGS 126(W)) da nova geração (Cerca de 10), que serão montados e conectados à rede de forma faseada, dando prioridade à sala de servidores e ao bloco administrativo.

Abaixo está a descrição do Firewall XGS 126(W) proposto para a sala servidores:

O Sophos XGS é uma linha de firewalls de última geração (NGFW) projectada para PMEs (Prquenas e Médias Empresas) e empresas, com foco em segurança integrada, desempenho escalável e gestão simplificada via Sophos Central. Os modelos com "W" incluem *Wi-Fi* integrado para redes sem fio unificadas.

- **Tabela de especificações técnicas**

Modelo	XGS 119 (W)	XGS 126 (W)	XGS 136 (W)
WiFi	8x GbE + 2x SFP	12x GbE + 4x SFP+	16x GbE + 4x SFP+
Portas	Opcional (W)	Opcional (W)	Opcional (W)
Throughput	3Gbps Firewall	4Gbps Firewall	5Gbps Firewall
VPN	1Gbps (IPSec)	1.5Gbps (IPSec)	2Gbps (IPSec)
IPS	1Gbps	1.5Gbps	2Gbps
SSL Inspecção	500Mbps	700Mbps	1Gbps
RAM	4GB	8GB	8GB

Storage	32GB	64GB	64GB
Power	Redundante(Opcional)	Redundante(Opcional)	Redundante(Opcional)

Tabela 13: Especificações técnicas do Sophos XGS 126(W)

Fonte: Elaborado pelo autor

- **Tabela ilustrativa das vantagens do Sophos XGS 126 (W)**

Recurso	Benefício
Synchronized Security	Integração com endpoints sophos para bloqueio automático de ameaças
Gestão unificada	Controle centralizado via Sophos Central (Nuvem)
Wi-Fi integrado (W)	Simplifica redes sem fio com Vlans e políticas únicas.
Sandboxing avançado	Detecção de Ameaças zero-day via análise em sandbox.
Custo – Benefivio	Preço competitivo para PMEs comparado às concorrentes.

Tabela 14: Tabela ilustrativa das vantagens do Sophos XGS 126 (W)

Fonte: Elaborado pelo autor

- **Tabela ilustrativa das limitações do Sophos XGS (126)**

Limitação	Impacto
Licenças obrigatórias	Recursos como Sandboxing exigem assinaturas anuais.
Portas limitadas	Modelos básicos como GXS 119 têm menos portas que FortiGate equivalentes.
Dependência de cloud	Algumas funcionalidades requerem Sophos Central (Offline Limitado).

Curva de aprendizado	Interfaces menos intuitivas que soluções como Ubiquiti para iniciantes.

Tabela 15: Tabele Ilustrativa das limitações do Sophos XGS 126(W)

Fonte: Elaborado pelo autor

Recursos de Segurança do Sophos XGS 126 (W)

- Firewall de Aplicação: Controle granular por aplicativo;
- IPS/IDS: Detecção de intrusões em tempo real;
- Web Filtering: Bloqueio de categorias de sites (redes sociais, malware);
- VPN SSL/IPsec: Acesso remoto seguro com Sophos Connect;
- Relatórios Automatizados: Análise de ameaças via Sophos Central.

Em suma, o Sophos XGS 126 (W) é a solução adequada para FEUEM, que busca segurança integrada e facilidade de gestão, porém com limitações em escalabilidade física (portas) e dependência de licenças. Modelos com "W" são ideais para redes com Wi-Fi.

4.2.1.5. Instalação de UPSs para garantir a proteção de equipamentos em caso de oscilações de electricidade

Os equipamentos de rede, principalmente os dispositivos de transmissão, são altamente sensíveis a oscilações elétricas. A ausência de um sistema de proteção adequado pode comprometer a vida útil dos equipamentos ou, em casos extremos, provocar curtos-circuitos, levando à inoperacionalidade da rede.

Para mitigar estes riscos, propõe-se a instalação de uma fonte de alimentação ininterrupta (UPS) que garanta a estabilidade energética e proteja os equipamentos contra falhas de energia.

O modelo Proposto é o Tripp Lite SmartPro SMX1500SLT. Este modelo foi selecionado por apresentar um custo-benefício equilibrado em comparação com outras soluções da mesma categoria, além de oferecer funcionalidades avançadas, como gestão remota via rede.

Características Técnicas do UPS Tripp Lite SmartPro SMX1500SLT

Parâmetro	Especificações
Capacidade	1500VA / 1350W
Tensão de Entrada	230V (compatível com a rede elétrica padrão)
Autonomia	Tempo de backup variável consoante a carga (consultar tabela do fabricante)
Baterias	Baterias seladas de chumbo-ácido (VRLA), substituíveis
Gestão Remota	Interface de rede (SNMP, USB, serial) para monitorização e controlo
Proteções	Filtragem de surtos, correção ativa do fator de potência (PFC)
Formato	Rack-mount (2U) ou torre, conforme necessidade de instalação
Garantias	3 Anos (Icluindo cobertura para baterias)

Tabela 16: Caracteristicas da UPS Tripp Lite SmartPro SMX1500SLT

Fonte: Elaborado pelo autor

- **Vantagens da Implementação**
  - Proteção contra quedas e picos de tensão, aumentando a vida útil dos equipamentos;
  - Backup energético em caso de falha de energia, permitindo desligamentos seguros ou continuidade operacional;
  - Monitorização em tempo real via rede, facilitando a gestão proativa;
  - Design robusto, adequado para ambientes de rede e datacenters;

Esta solução assegura maior fiabilidade e resiliência da infra-estrutura de TI da FEUEM, reduzindo riscos de paragens não planeadas e custos com reparações.

4.2.2. Documentação da rede

A documentação da rede do bloco administrativo da FEUEM foi organizada seguindo um padrão de documentação estruturado, alinhado aos seguintes frameworks:

- ✓ ITIL (Information Technology Infrastructure Library);
- ✓ ISO/IEC 19770;
- ✓ Boas Práticas de Redes Cisco.

- **Rede**
  - 02 Link Internet de 1Gbps;
  - Backbone de Fibra óptica: 12 000 metros;
  - Cabeamento UTP Categoria 6: 2 000 metros;
  - Roteadores: 0;
  - Switches Cisco Catalyst 9200L: 7 e 9300: 2
- **Microinformática**
  - Estações de trabalho: 39 PC's;
  - Impressoras: 11 Impressoras;
  - Access Points:14 Access Points.
- **Topologia da rede**

A topologia da rede do bloco administrativo é descrita da seguinte forma:

Id	VLAN	Descrição
99	Vlan-Gestão	Vlan de gestão de equipamentos (Switches e Servidor)
10	Vlan-DTIC	Vlan para equipamentos do departamentos das TIC
20	Vlan-CEE	Vlan para o Centro de Estudos de Engenharia
30	Vlan-Estudantes	Vlan para Estudantes e Visitantes
40	Vlan-Docentes	Vlan para Docentes

50	Valn-DAF	Veln para o Departamento de Finanças
60	Vlan-DRA	Vlan para o Departamento do Registo Académico
70	Vlan-Wireless-BAD	Vlan de Access Points para utilizadores internos
80	Vlan-Wireless-BAD	Vlan de Access Points para utilizadores externos

Tabela 17: Segmentação dos sectores do DBA por VLANs

Fonte: Elaborado pelo autor

- **Diagrama físico da topologia**

A topologia abaixo representa a ilustração gráfica da proposta de resolução dos problemas que a rede do bloco administrativo da FEUME enfrenta. Como pode-se observar, foram adicionados:

- Um firewall para delimitar a fronteira entre a rede interna (*trusted*) e a rede externa (*untrusted*), garantindo controle de tráfego e proteção contra ameaças externas.
- Todos os switches (excepto os Switches da direcção) foram substituídos pelo modelo Catalyst 9200L, proporcionando maior capacidade de gerenciamento, eficiência energética e suporte a tecnologias modernas;
- Foram adicionados dois Switches da Cisco Catalyst 9300 na Direcção para actuarem na camada de destribuição da rede do bloco administrativo;
- Realizado *upgrad* do cabeamento de Cat5 para Cat6, assegurando maior largura de banda (até 1 Gbps) e redução de interferências.
- Implementação de cabeamento estruturado conforme os padrões:
  - TIA/EIA-568 (norma de infra-estrutura de telecomunicações);
  - ISO/IEC 11801 (padrão internacional para redes de cabos).
- Divisão da rede em VLANs por departamento, isolando logicamente os segmentos para:
  - Melhorar a segurança (contendo possíveis violações);
  - Optimizar o tráfego (reduzindo broadcasts);

- Facilitar a gestão de políticas de acesso.Foi evitado o problema de one point failure com recurso à redundáncias e ao protocolo RSPT (Rapid Spanning Tree Protocol).

- Redundância e Tolerância a Falhas
  - Eliminação de single point of failure mediante:
    - Implementação de redundância física (caminhos alternativos);
    - Configuração do protocolo RSTP (Rapid Spanning Tree Protocol), assegurando reconexão rápida (<2 segundos) em caso de falha em enlaces.
- Ganhos/Vantagens que a topologia traz:

As intervenções realizadas elevam a maturidade da infra-estrutura de rede, alinhando-a a boas práticas de TI. Os resultados esperados incluem:

- Maior segurança perimetral e interna;
- Escalabilidade para futuras expansões;
- Disponibilidade contínua (*uptime*).

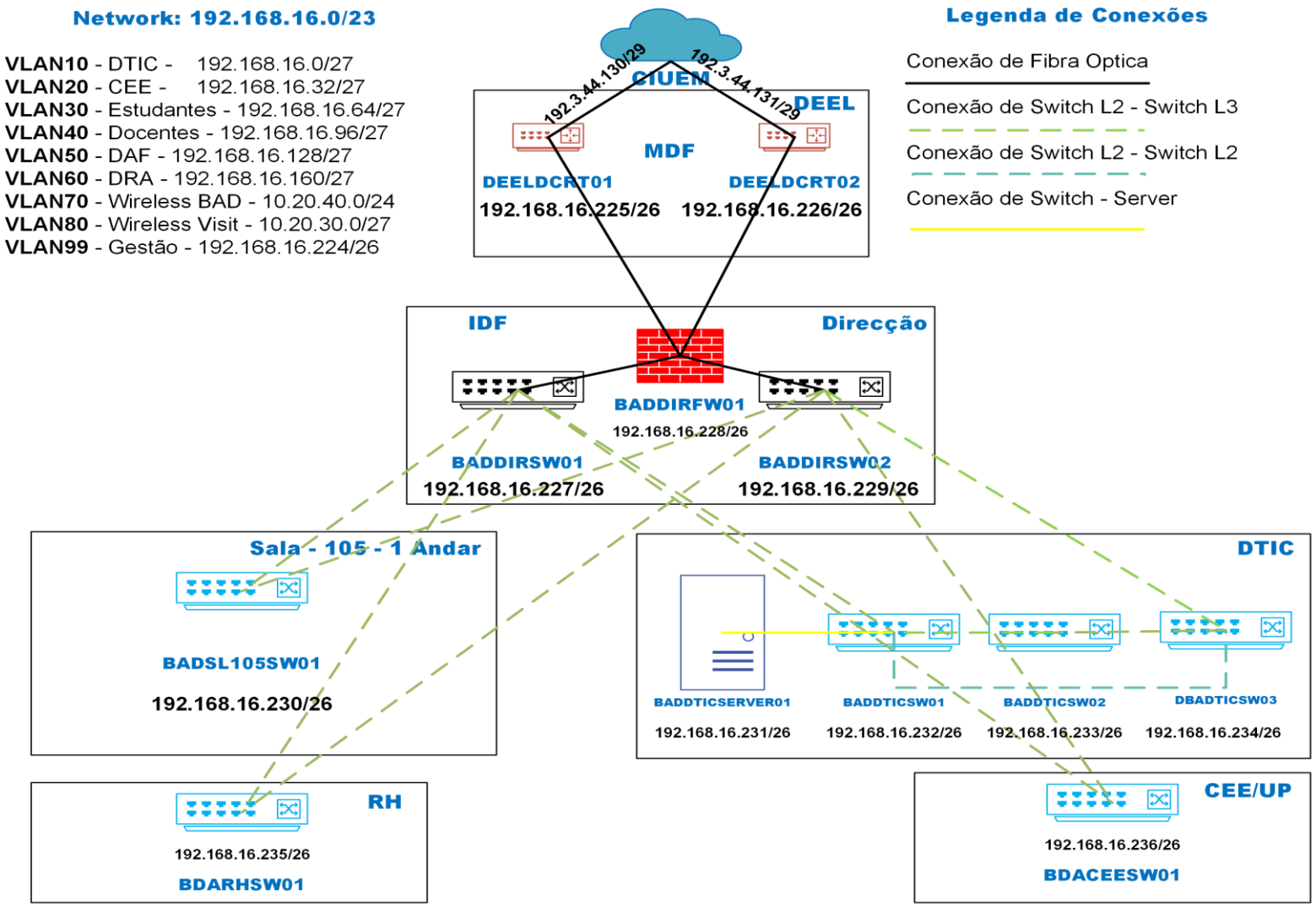


Figura 14: Topologia de rede proposta como solução

Fonte: Elaborado pelo autor

5. Capítulo V – Apresentação e Discussão de Resultados

5.1. Relação entre a revisão da literatura e o projecto

A revisão da literatura teve como objetivo principal fornecer uma visão abrangente sobre redes de computadores, analisando as suas arquiteturas fundamentais e modos de operação. O estudo focou-se particularmente nas redes locais (LAN), explorando as suas arquiteturas mais comuns, os dispositivos de rede essenciais e os protocolos que garantem o seu funcionamento adequado. Esta análise serviu de base para o desenvolvimento do trabalho.

Paralelamente, foram examinadas as normas ISO19770 relevantes para a documentação de infra-estruturas de rede, um aspecto crucial para manter um registo organizado e atualizado de todos os componentes e processos relacionados com a rede nas organizações. Esta abordagem normativa mostrou-se fundamental para a correta documentação da rede proposta no âmbito deste trabalho.

A segurança em redes corporativas mereceu especial atenção, destacando-se os riscos associados a redes não segmentadas em VLANs e a importância crítica da segurança perimetral, que exige a implementação de firewalls. O estudo reforçou a noção de que a segurança cibernética vai além de soluções técnicas como VLANs, firewalls ou sistemas de deteção e prevenção de intrusões (IDS/IPS), dependendo igualmente de fatores humanos e comportamentais.

No que diz respeito à qualidade de serviço (QoS), a revisão demonstrou a sua importância vital em redes que transportam voz, vídeo e dados, assegurando o desempenho adequado de aplicações sensíveis à latência. A ausência de mecanismos de QoS poderia comprometer significativamente a experiência do utilizador e a eficiência das operações.

Todos estes conceitos, abordados de forma sistemática na revisão bibliográfica, revelaram-se indispensáveis para a realização do trabalho de reestruturação e modernização da rede. Sem este conhecimento fundamental, a execução do trabalho técnico seria consideravelmente mais complexa e arriscada.

6. Capítulo VI – Considerações Finais

6.1. Conclusões do trabalho

O presente trabalho de pesquisa apresentou uma proposta abrangente para a reestruturação e modernização da infra-estrutura de rede da Faculdade de Engenharia da Universidade Eduardo Mondlane (FEUEM), com foco no bloco administrativo. A análise detalhada da rede atual revelou desafios críticos, como equipamentos obsoletos, falta de segmentação em VLANs, ausência de firewall e documentação inadequada. A solução proposta, dividida em fases de documentação e implementação técnica, demonstrou ser viável e alinhada às necessidades institucionais, garantindo maior segurança, eficiência e escalabilidade.

A implementação de VLANs, a substituição de cabos Cat5 por Cat6, a instalação de firewalls Sophos XGS126 (W), a adopção de switches de destribuição (Cisco Caltalyst 9300) e de acesso (Cisco Catalyst 9200L) trarão melhorias significativas na organização, desempenho e segurança da rede. Além disso, a padronização de cores e etiquetagem facilitará a manutenção e reduzirá o tempo de resolução de falhas.

O projeto evidenciou a importância de uma abordagem estruturada para a governança de tecnologias de informação, destacando a necessidade de alinhamento entre tecnologia e objectivos institucionais. Caso o projecto seja implementado futuramente, os resultados obtidos irão validar (ou não) a eficácia das soluções propostas, que podem ser replicadas em outros departamentos da FEUEM.

6.2. Contribuições do projecto e recomendações para futuras melhorias ou expansões da rede.

6.2.1. Contribuições:

De um modo geral, o presente trabalho teve as seguintes contribuições:

- ✓ **Segurança reforçada:** Implementação de firewalls e VLANs para isolamento lógico de tráfego, reduzindo riscos de ataques e acessos não autorizados.
- ✓ **Desempenho optimizado:** Upgrade para cabos Cat6 e switches geríveis, garantindo maior largura de banda e menor latência.

- ✓ **Documentação completa:** Criação de inventários detalhados, diagramas de rede e padrões de nomenclatura, facilitando a gestão e manutenção.
- ✓ **Escalabilidade:** Infra-estrutura preparada para futuras expansões, como adopção de IoT, Wi-Fi 6 e virtualização avançada.

6.2.2. Recomendações:

6.2.2.1. Faculdade de Engenharia da UEM

- ✓ Recomenda-se a FEUEM que elabore um cronograma de expansão gradual da rede, aplicando as soluções propostas nos demais departamentos da FEUEM, priorizando áreas críticas e;
- ✓ A capacitação da equipe de TIC, treinamento de técnicos em tecnologias modernas (SDN, QoS) e boas práticas de redes.

6.2.2.2. Em relação à futuros trabalhos de pesquisa, recomenda-se:

- ✓ **Monitorização contínua:** Implementar ferramentas como **Nagios**, **Zabbix** ou **Wireshark** para acompanhamento em tempo real do desempenho e segurança;
- ✓ **Atualização tecnológica:** Avaliar a migração para IPv6 e a adopção de soluções baseadas em nuvem para serviços não críticos;
- ✓ **Backup:** Implementar uma solução de backup (recomendado: Veeam Backup & Replication) para garantir e replição e recuperação de dados;
- ✓ **Redundância avançada:** Implementar links redundantes (Principalmente o link que trafega serviços da CIUEM para FEUEM) e servidores em cluster para evitar single points of failure.
- ✓ **Suporte Remote de Utilizadores:** Instalação de um software (recomendado: TeamViewer, AnyDesk, RDP) para suporte remoto de utilizadores da rede.

6.2.3. Constrangimentos

- ✓ **Recursos financeiros:** A aquisição de equipamentos de alta performance (Switch Catalyst 9300, Cabos Cat6, Acces Points e UPSs) exigiu investimento significativo, limitando a velocidade de implementação;
- ✓ **Tempo de implementação:** A complexidade da migração e a necessidade de minimizar impactos operacionais alteraram o cronograma de implmentação, sendo adiada para uma ocasião oportuna;

- ✓ **Resistência à mudança:** Adaptação de usuários e técnicos aos novos padrões e processos demandou esforço adicional em treinamento.
- ✓ **Dependência de licenças:** Soluções como o Sophos XGS exigem assinaturas anuais, aumentando custos operacionais.

Em resumo, apesar dos desafios e o adiamento da implemetação, o projeto alcançou seus objetivos principais, estabelecendo uma base sólida para a evolução da infra-estrutura de tecnologia de informação e comunicação da FEUEM. A sua implementação e a continuidade das melhorias dependerá do planeamento estratégico e alocação de recursos adequados.

Bibliografia

- **Referências Bibliográficas**

[1]. AXELOS. (2019). ITIL 4 Foundation. The Stationery Office.

[2]. Chiziane, E. G. (2022). Reestruturação da infraestrutura física da rede de computadores do departamento de engenharia eletrotécnica (DEEL) da faculdade de engenharia da UEM. Universidade Eduardo Mondlane.

[3]. Cheswick, W. R., Bellovin, S. M., & Rubin, A. D. (2003). Firewalls and Internet security: Repelling the wily hacker (2nd ed.). Addison-Wesley.

[4]. Comer, D. E., & Droms, R. E. (2022). Computer networks and internets. Pearson.

[5]. Da Silva, E. L., & Menezes, E. M. (2001). Metodologia da pesquisa e elaboração de dissertação. Universidade Federal de Santa Catarina.

[6]. International Organization for Standardization & International Electrotechnical Commission. (2022). *ISO/IEC 27001:2022 Information technology — Security techniques — Information security management systems — Requirements*. ISO.

[7]. International Organization for Standardization. (2024). *ISO/IEC 19770-1:2024 Information technology — IT asset management — Part 1: IT asset management systems — Requirements* (3rd ed.). ISO.

[8]. Kaufman, C., Perlman, R., & Speciner, M. (2002). Network security: Private communication in a public world (2nd ed.). Prentice Hall.

[9]. Kurose, J. F., & Ross, K. W. (2020). Computer networking: A top-down approach (8th ed.). Pearson.

[10]. Mazivila, E. I. (2022). Desenvolvimento de um sistema web de suporte técnico na área das TICs. Universidade Eduardo Mondlane.

[11]. Mbilane, E. A. (2022). Proposta de implementação de um sistema de comunicação telefónica VoIP. Universidade Eduardo Mondlane.

[12]. McClure, S., Scambray, J., & Kurtz, G. (2019). Hacking exposed: Network security secrets & solutions (7th ed.). McGraw-Hill.

[13]. Murdoch, D. (2014). Blue team handbook: Incident response edition (2nd ed.). CreateSpace Independent Publishing Platform.

[14]. Oliviero, A., & Woodward, B. (2023). Cabling: The complete guide to copper and fiber-optic networking (5th ed.). Sybex.

[15]. Peterson, L. L., & Davie, B. S. (2021). Computer networks: A systems approach (6th ed.). Morgan Kaufmann.

[16]. Pfleeger, C. P., & Pfleeger, S. L. (2015). Security in computing (5th ed.). Prentice Hall.

[17]. Sanders, C. (2017). Practical packet analysis: Using Wireshark to solve real-world network problems (3rd ed.). No Starch Press.

[18]. Sanders, C., & Smith, J. (2013). Applied network security monitoring: Collection, detection, and analysis. Syngress.

[19]. Stallings, W., & Brown, L. (2018). Computer security: Principles and practice (4th ed.). Pearson.

[20]. Stuttard, D., & Pinto, M. (2011). The web application hacker's handbook: Finding and exploiting security flaws. Wiley.

[21]. Cisco Systems. (2020). *CCNA 200-301 official cert guide library*. Cisco Press.

[22]. Tanenbaum, A. S., & Wetherall, D. J. (2021). Computer networks (6th ed.). Pearson.

[23]. Veras, C. M. (2013). Segurança de redes em ambientes corporativos. Brasport.

[24]. Zalewski, M. (2011). A guide to securing modern web applications. No Starch Press.

Anexos

Anexo 1: Descrição da situação actual da rede dos demais departamentos da FEUEM

1. Descrição da situação actual da DEEL

A infra-estrutura do DEEL é destribuida da seguinte forma:

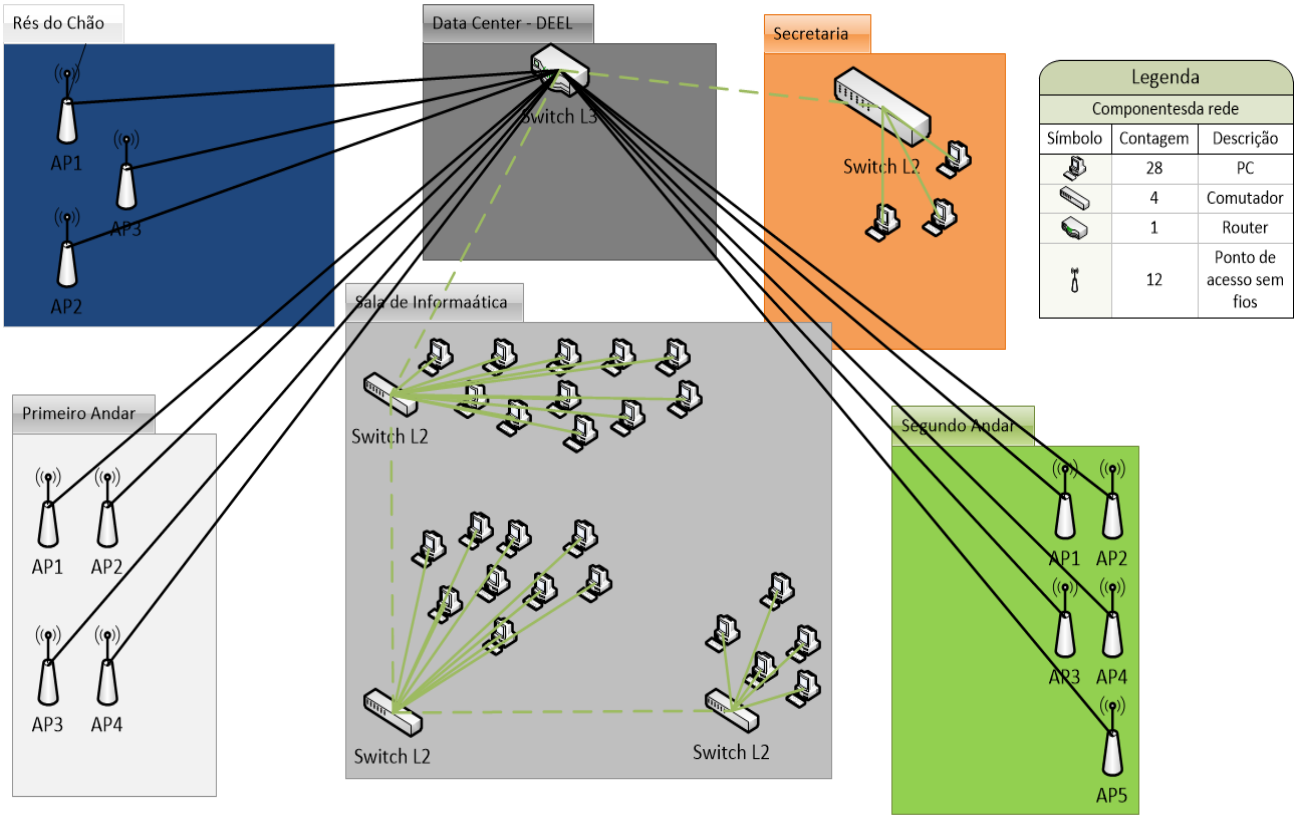


Figura 15: Topologia da DEEL

a) Rés do Chão

- Um Switch Gerível com capacidade de 1Gbps da Cisco;
- Três AccessPoints da Microtic.

b) Primeiro Piso

- Um Switch L2 com capacidade de 100Mbps da Cisco na secretaria;
- Quatro AccessPoints conectados ao Switch L3 do Data Center;
- Três Computadores de mesa conectados ao Switch L2 da Secretaria;
- Uma Impressora Conectado ao Switch da secretaria.

c) Segundo Piso

- Três Switch's L2 no bastidor da sala de informática;
- Vinte e cinco computadores de mesa conectados aos Switch's na sala de informática;
- Cinco AccessPoints conectados ao Switch L3 do Data Center, que fazem a destribuição do sinal pelas salas e pelo corredor.

Edifício do DEEL												
Piso	**Router**				**Switch**				**Access Point**		**PC**	**Impressora**
	Qtde	**Capac**	**Vendor**	**Mdl**	**Qtde**	**Capac**	**Vendor**	**Mdl**	**Qtde**	**Vendor**	**Qtde**	**Qtde**
Rés do Chão	0	-	-	-	1	1Gig	Cisco Meraki	MS225-24P	3	MikroTik, TP Link, D Link	-	-
Primeiro Piso	0	-	-	-	1	100Mbps	Cisco Catalyst	2960-24TT-L	4	MikroTik, TP Link, D Link	3	1
Segundo Piso	0	-	-	-	3	1Gig	Cisco, Mikrotik, TP Link	MS210-24P, TL-SG1024	5	MikroTik, TP Link, D Link	25	-
Total	0	N/A	-	N/A	5	N/A	N/A	N/A	12	N/A	28	1

Tabela 18: Descrição da DEEL

2. Descrição da Situação Actual do Departamento De Cadeiras Gerais (DCG)

A infra-estrutura do Departamento de Cadeiras Gerais é destribuida da seguinte forma:

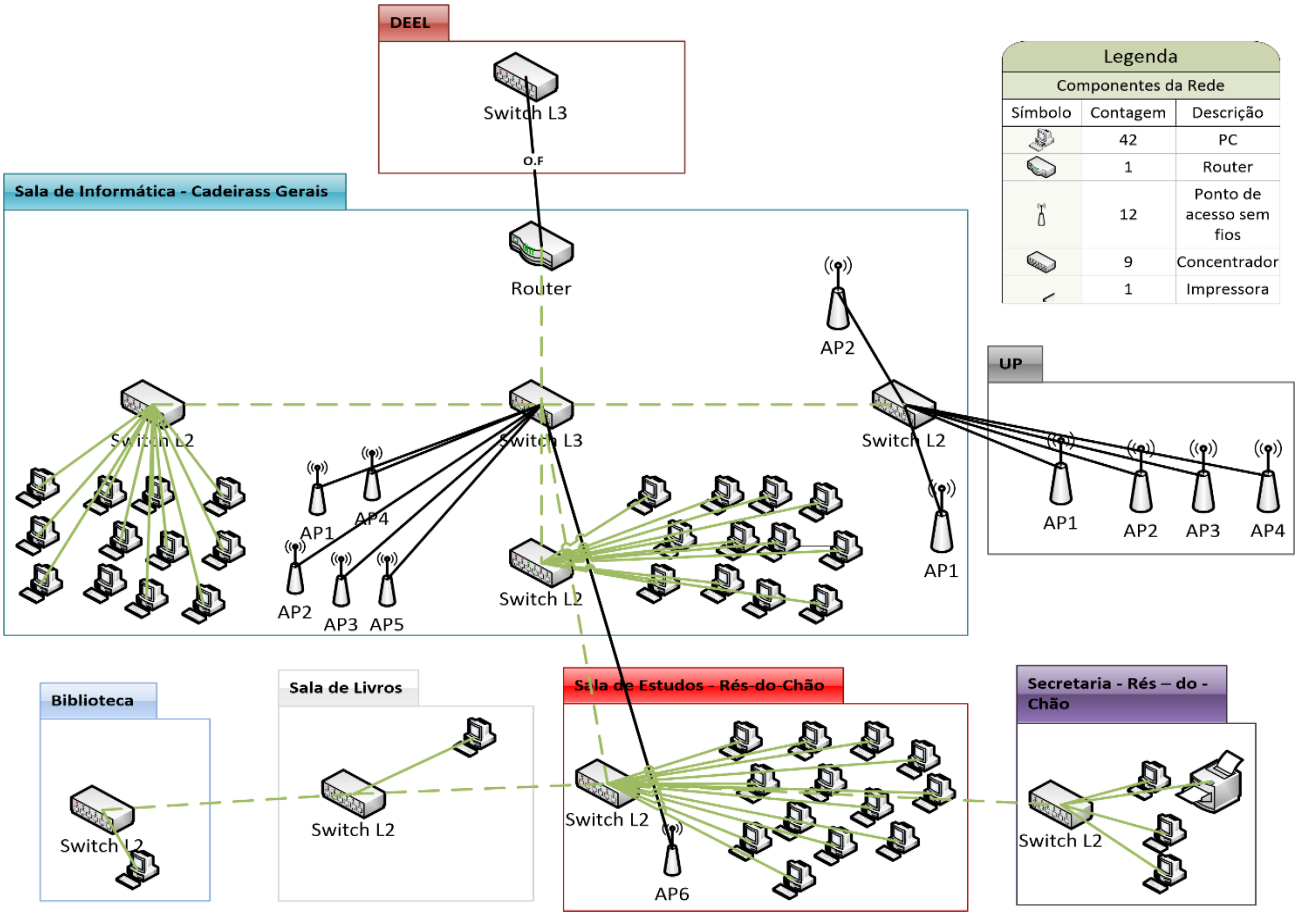


Figura 16: Topologia do Departamento das Cadeiras Gerais

a) Rés do Chão

- Três Switch's L2 da Cisco com capacidade de 1Gbps;
- Um AccessPoint da Microtic.

b) Primeiro Piso

- Um Router com capacidade de 1Gbps da Microtic na sala de máquinas que recebe o sinal que vem da DEEL;
- Um Switch L3 com capacidade de 1Gbps da Cisco que recebe o sinal do router e faz a destriuição para outros três Switch's L2;
- Sete AccessPoints conectados em dois Switch's, mais quatro AccessPoints que pertencem à unidade de produção;

- Quarenta e dois (42) Computadores de mesa conectados aos Switch's L2 da sala de informática;
- Uma Impressora Conectado ao Switch da secretaria.

Edifício do DCG												
Piso	**Router**				**Switch**				**Access Point**		**PC**	**Impressora**
	Qtde	**Capac**	**Vendor**	**Mdl**	**Qtde**	**Capac**	**Vendor**	**Mdl**	**Qtde**	**Vendor**	**Qtde**	**Qtde**
Rés do Chão	0	-	-	-	3	1Gig	Cisco, MicroTik, TP Link	MS210-24P, MS210-24P, TL-SG1024	1	MikroTik, TP Link, D Link	17	1
Primeiro Piso	1	1Gig	Cisco	ISR 4451-X	5	1Gig	Cisco, MicroTik, TP Link	MS210-24P, MS210-24P, TL-SG1024	7	MikroTik, TP Link, D Link	25	-
Total	1	N/A	N/A	N/A	8	N/A	N/A	N/A	8	N/A	42	1

Tabela 19: Descrição do Departamento das Cadeiras Gerais

3. Descrição da Situação Actual do Departamento De Engenharia Química(DEQI)

A infra-estrutura do Departamento de Engenharia Química é destribuida da seguinte forma:

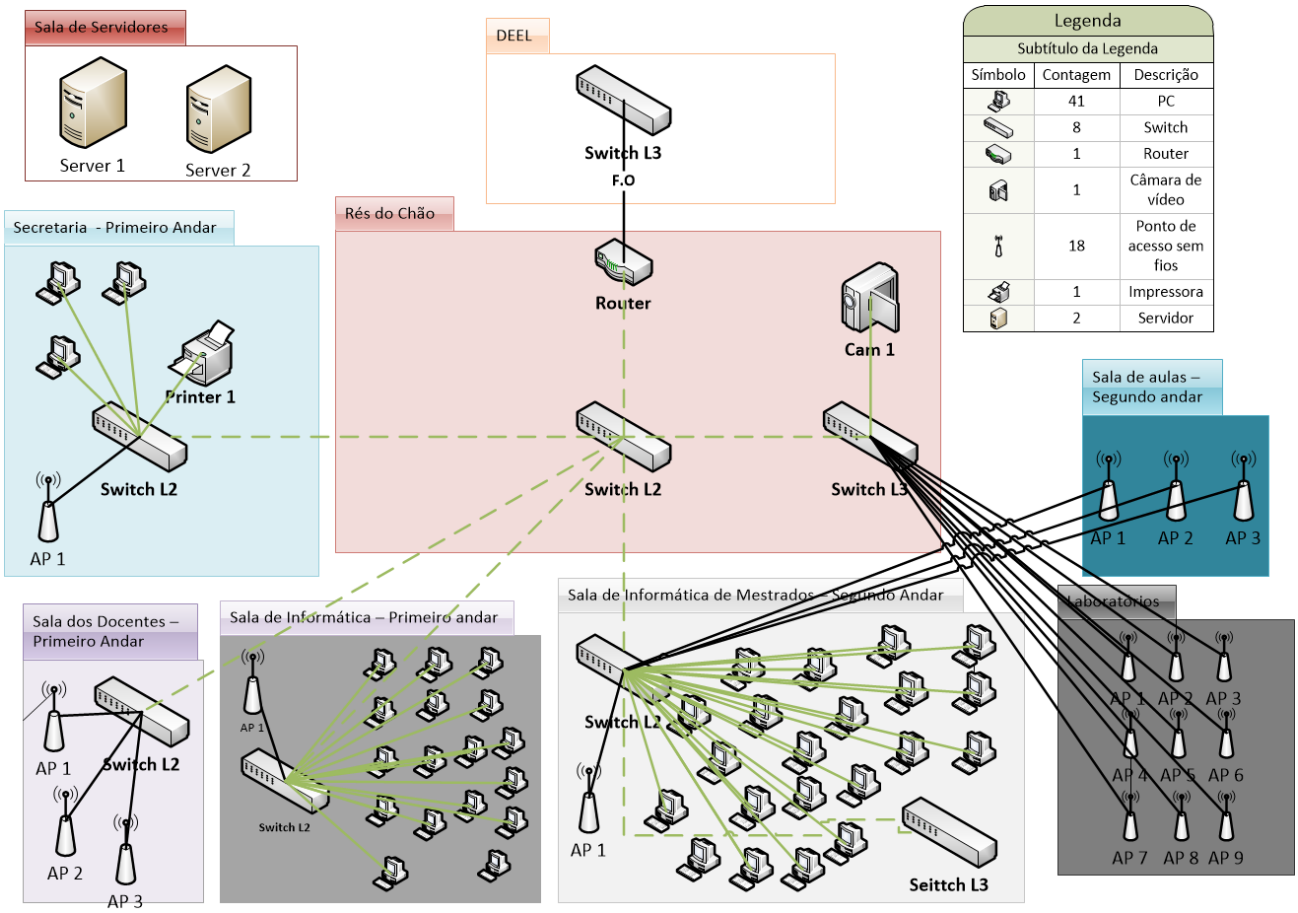


Figura 17: Topologia do Departamento de Engenharia Química

a) **Rés do Chão**

- Um Router que recebe o sinal da DEEL e faz a destribuição para os demais dispositivos;
- Um Switch L2 que recebe o sinal do Router, e um Switch L3 que está directamente conectado ao Switch L2 e a uma câmera de segurança;
- Nove AccessPoint da Microtic que estão destribuidas pelos laboratórios do departamento

b) **Primeiro Piso**

- Três Switch's L2 com capacidade de 1Gbps da Cisco, um instalado na sala de informática, outro instalado na sala dos Docentes, o último instalado na secretaria, os três recebem sinal do Switch L3 do rés do chão;
- Três AccessPoints na sala dos Docentes, um na sala de informática e o último na secretaria;
- Dezassete (17) Computadores de mesa conectados aos Switch's L2 da sala de informática;
- Uma Impressora Conectada ao Switch da secretaria.

c) **Segundo Piso**

- Um Switch L2 que recebe sinal do Switch L3 do Rés do Chão, mais um Switch L3 directamente conectado ao Switch L2;
- Um AccessPoint na sala de informática de Mestrado, mais três destribuidos pelos corredores e salas de aulas;
- Dois Servidores que não estão conectados à rede ainda.

Edifício do DEQI												
Piso	**Router**				**Switch**				**AccessPoint**		**PC**	**Impressora**
	Qtde	**Capac**	**Vendor**	**Mdl**	**Qtde**	**Capac**	**Vendor**	**Mdl**	**Qtde**	**Vendor**	**Qtde**	**Qtde**
Rés do Chão	1	1Gig	Cisco	ISR 4451-X	2	1Gig	Cisco	MS210-24P, MS210-24P	9	-	-	-
Primeiro Piso	0	-	-	-	3	1Gig	Cisco	MS210-24P, MS210-24P, TL-SG1024	3		17	1
Segundo Piso	0	-	-	-	2	1Gig	Cisco, MicoTik, TP Link	MS210-24P, TL-SG1024	6		29	-
Total	1	N/A	-	N/A	5	N/A	N/A	N/A	18	N/A	41	1

Tabela 20: Descrição do Departamento de Engenharia Química

4. Descrição da Situação Actual do Departamento De Engenharia Mecânica(DEMA)

A infra-estrutura do Departamento de Engenharia Química é destribuida da seguinte forma:

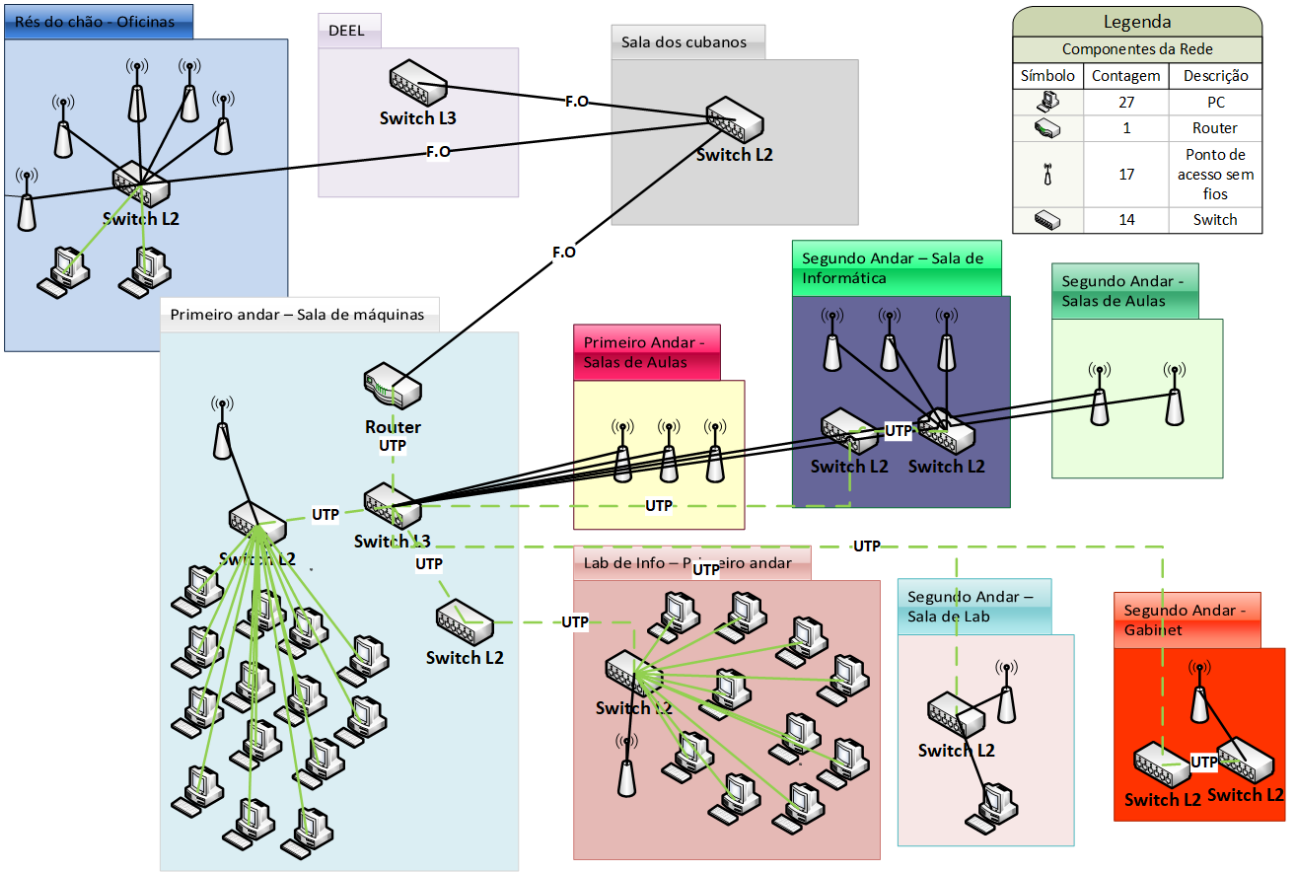


Figura 18: Topologia do Departamennto de Engenharia Mecânica

a) Rés do Chão

- Um Switch L2 na sala dos cubanos que recebe o sinal da DEEL e faz a destribuição para os demais dispositivos;
- Cinco AccessPoint da Microtik que estão destribuidas pelos laboratórios do departamento;
- Dois computadores de mesa contectados ao Switch L2 das oficinas.

b) Primeiro Piso

- Um Router na sala de máquinas que recebe o sinal da sala dos cubanos;
- Um Switch L3 que recebe o sinal do router na sala de máquinas e destribui o sinal para outros três Swtchs L2;

- Cinco AccessPoints destribuidos pelas salas de informática, salas de aulas e sala de máquinas;
- Quatorze (14) Computadores conectados ao Switch da sala de máquinas, Dez (10) Computadores de mesa conectados aos Switch's L2 da sala de informática.

c) Segundo Piso

- Dois Switchs L2 na sala e informática que recebem sinal do Switch L3 da sala de máquinas do primeiro andar, mais dois Switchs L2 (um no laborório e o outro no gabinete) directamente conectado ao Switch L3 da sala de máquinas do primeiro andar;
- Um AccessPoint na sala de informática de Mestrado, mais três destribuidos pelos corredores e salas de aulas;
- Sete AccessPoints destribuidos pelas salasde aulas, laboratórios e corredores.

Edifício do DEMA												
Piso	**Router**				**Switch**				**AccessPoint**		**PC**	**Impressora**
	Qtde	**Capac**	**Vendor**	**Mdl**	**Qtde**	**Capac**	**Vendor**	**Mdl**	**Qtde**	**Vendor**	**Qtde**	**Qtde**
Rés do Chão	0	-	-	-	2	1Gig	Cisco, Microtik	MS210-24P, CRS326-24G-2S+RM	5	Microtik	-	-
Primeiro Piso	1	1Gig	Microtik	CCR1036-12G-4S	4	1Gig, 100 Mbps	Cisco, Microtik, TP Link	2960-24TT-L, CRS326-24G-2S+RM, TL-SG1024	5	Microtik, Cisco, TP Link	24	-
Segundo Piso	0	-	-	-	5	1Gig	Cisco, MicoTik, TP Link	2960-24TT-L, CRS326-24G-2S+RM, TL-SG1024	7	Microtik, Cisco, TP Link	1	-
Total	1	N/A	N/A	N/A	11	N/A	` N/A	N/A	17	-	25	0

Tabela 21: Descrição do Departamento de Engenharia Mecânica

5. Descrição da Situação Actual do Departamento De Engenharia Civil(DECI)

A infra-estrutura do Departamento de Engenharia Civil é destribuida da seguinte forma:

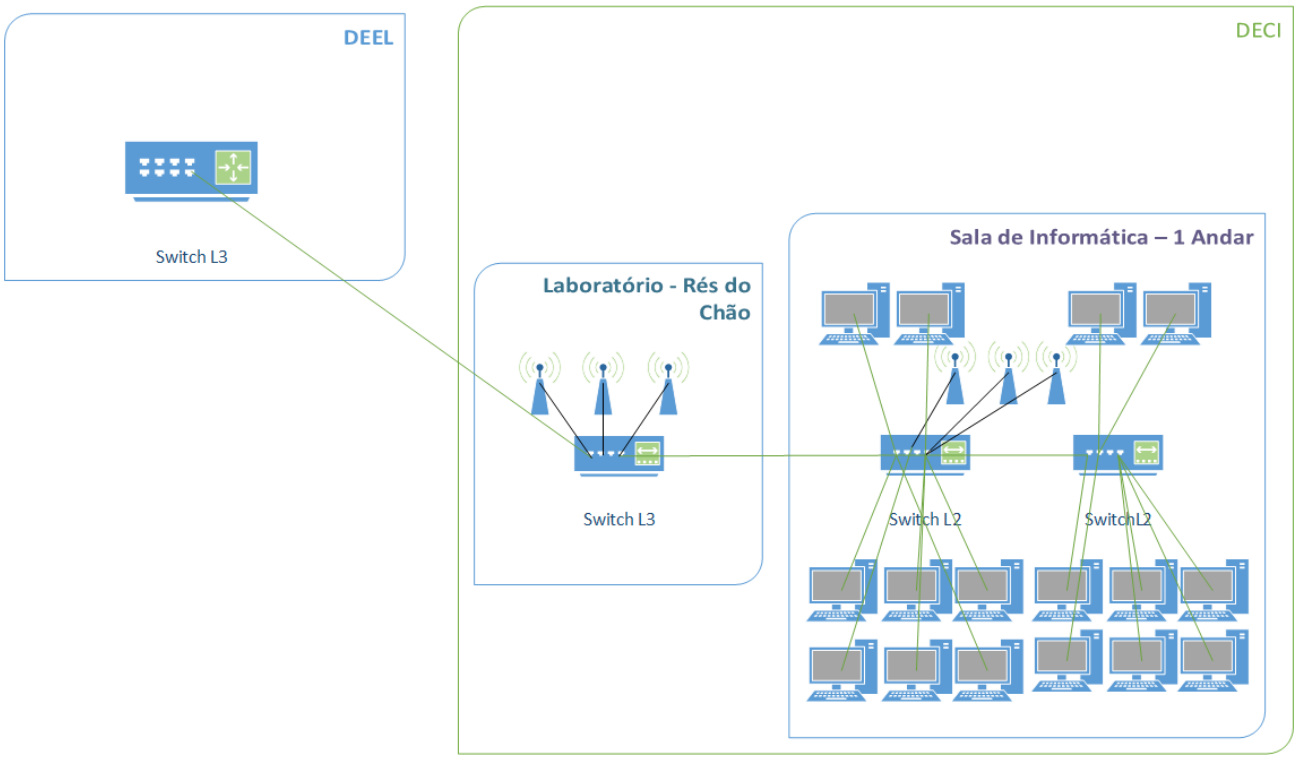


Figura 19: Topologia do Departamento de Engenharia Civil

a) Rés do Chão

- Um Switch L2 da Cisco com capacidade de 1Gbps que recebe sinal da DEEL;
- Três (3) AccessPoint da Microtik destribuidos pelos laboratórios e salas de aulas.

b) Primeiro Piso

- Dois Switch's L2 com capacidade de 1Gbps da Cisco que recebem o sinal do Switch do laoratório da rés do chão;
- Três AccessPoints conectados em um Switch da sala de informática;
- Dezasseis (16) Computadores de mesa conectados aos Switch's L2 da sala de informática.

Edifício do DECI												
Piso	**Router**				**Switch**				**AccessPoint**		**PC**	**Impressora**
	Qtde	**Capac**	**Vendor**	**Mdl**	**Qtde**	**Capac**	**Vendor**	**Mdl**	**Qtde**	**Vendor**	**Qtde**	**Qtde**
Rés do Chão	0	-	-	-	1	1Gig	Microtik	CRS326-24G-2S+RM	3	Microtik	-	-
Primeiro Piso	0	-	-		2	1Gig	Microtik, TP Link	CRS326-24G-2S+RM, TL-SG1024	3	Microtik, TP Link	16	-
Total	0	N/A	-		3	N/A	N/A	N/A	6	-	16	0

Tabela 22: Situação Actual do Departamento de Engenharia Civil

Anexo 2. Activos de rede da proposta de solução:

1. Activos de rede

Os activos da rede são destribuidos da seguinte forma:

- **Roteadores;**
- **Switches;**
- **Access Points;**
- **Impressoras;**
- **Computadores (PC);**
- **Fontes de alimentação Inunterruptas UPSs.**

A nomenclatura padrão adotada para os dispositivos da FEUEM obedece a seguinte ordem:
DepartamentoSalaTipoEquipamento

Onde TipoEquipamento pode ser:

- **RT:** Router;
- **SW:** Switch;
- **SERVER:** Servidores
- **PC:** Computador (Personal Computer);
- **AP:** Access Point;
- **UPS:** Fontes de alimentação Inunterruptas.

- **Switchs e Servidores:**

Nome	IP/Musk	Modelo	Localização
BADDIRSW01	192.168.16.227/25	Catalyst 9300	Bloco Administrativo, Direcção
BADDIRSW02	192.168.16.229/25	Catalyst 9300	Bloco Administrativo, Direcção
BADDIRFW01	192.168.16.228/25	Sophos 126 (W)	Bloco Administrativo, Direcção
BADDTICSW01	192.168.16.231/25	Catalyst 9200L	Bloco Administrativo, DTIC
BADDTICSW02	192.168.16.232/25	Catalyst 9200L	Bloco Administrativo, DTIC
BADDTICSW03	192.168.16.233/25	Catalyst 9200L	Bloco Administrativo, DTIC
BADDTICSERVER01	192.168.16.231/25	HP	Bloco Administrativo, DTIC
BADCEESW01	192.168.16.236/25	Catalyst 9200L	Bloco Administrativo, Centro de Estidos de Engenharia – Rés do Chão
BADCEESW02	192.168.16.237/25	Catalyst 9200L	Bloco Administrativo, Centro de Estidos de Engenharia – Primeiro Andar
BADSL105SW01	192.168.16.230/25	Catalyst 9200L	Bloco Administrativo, Sala 105 – Primeiro Andar
BADRHSW01	192.168.16.235/25	Catalyst 9200L	Bloco Administrativo, Recursos Humanos

Tabela 23: Nomenclatura dos Equipamentos da rede Proposta

1.1. Access Points e Impressoras

Nome	IP/Musk	Modelo	Localização
BADDTICAP01	192.168.16.235/25	TP-Link Omada EAP670	Bloco Administrativo, DTIC
BADDTICAP02	192.168.16.238/25	TP-Link Omada EAP670	Bloco Administrativo, DTIC (Corredor)
BADDRAAP01	192.168.16.239/25	TP-Link Omada EAP670	Bloco Administrativo, Direcção do Registo Acadêmico
BADDRAAP02	192.168.16.240/25	TP-Link Omada EAP670	Bloco Administrativo, Direcção do Registo Acadêmico (Corredor)
BADLABAP01	192.168.16.241/25	TP-Link Omada EAP670	Bloco Administrativo, Laboratório de Telecom
BADLABAP02	192.168.16.242/25	TP-Link Omada EAP670	Bloco Administrativo, Laboratório de Telecom (Corredor)
BADDIRAP01	192.168.16.243/25	TP-Link Omada EAP670	Bloco Administrativo, Direcção
BADDIRAP02	192.168.16.244/25	TP-Link Omada EAP670	Bloco Administrativo, Direcção
BADDIRAP03	192.168.16.245/25	TP-Link Omada EAP670	Bloco Administrativo, Direcção
BADDIRAP04	192.168.16.246/25	TP-Link Omada EAP670	Bloco Administrativo, Direcção (Corredor)
BAD105AP01	192.168.16.247/25	TP-Link Omada EAP670	Bloco Administrativo, Sala 105
BAD105AP02	192.168.255.248/25	TP-Link Omada EAP670	Bloco Administrativo, Sala 105 (Corredor)
BADUGEAAP01	192.168.16.249/25	TP-Link Omada EAP670	Bloco Administrativo, Ugea
BADUGEAAP02	192.168.16.249/25	TP-Link Omada EAP670	Bloco Administrativo, Ugea
BADDTICIMP01	192.168.16.250/25	Epson EcoTank L4260	Bloco Administrativo, DTIC

BADDRAIMP01	192.168.16.251/25	Epson EcoTank L4260	Bloco Administrativo, Direcção do Registo Acadêmico
BADDRAIMP02	192.168.16.252/25	Epson EcoTank L4260	Bloco Administrativo, Direcção do Registo Acadêmico
BADLABIMP01	192.168.16.253/25	Epson EcoTank L4260	Bloco Administrativo, Laboratório de Telecom
BADDIRIMP01	192.168.16.254/25	Epson EcoTank L4260	Bloco Administrativo, Direcção
BADDIRIMP02	192.168.16.255/25	Epson EcoTank L4260	Bloco Administrativo, Direcção
BADDIRIMP03	192.168.17.1/25	Epson EcoTank L4260	Bloco Administrativo, Direcção
BADDIRIMP04	192.168.17.2/25	Epson EcoTank L4260	Bloco Administrativo, Direcção
BADDIRIMP05	192.168.17.3/25	Epson EcoTank L4260	Bloco Administrativo, Direcção
BADUGEAIMP01	192.168.17.4/25	Epson EcoTank L4260	Bloco Administrativo, Ugea
BADUGEAIMP02	192.168.17.5/27	Epson EcoTank L4260	Bloco Administrativo, Ugea

Tabela 24: Nmenclatura dosEquipamentos da rede Proposta

1.2. Endereçamento IP e Roteamento

Endereços IP válidos alocados para a empresa:

- Endereços do Roteadores Principais: 192.3.44.130/29 – 192.3.44.131/29
- Rede: 192.3.44.128/29
- Gateway: 192.3.44.129/29
- Broadcast: 192.3.44.135/29
- Faixa de IP: 192.3.44.129 até 192.3.44.134/29

Subredes utilizadas

VLAN	Nome	Hosts Necessários	Sub-Redes	Faixa de IPs úteis	BroadCast	Máscara
99	**Gestão**	62	192.168.16.224/25	192.168.16.225 - 192.168.16.254	192.168.16.255	255.255.255.192
10	**DTIC**	30	192.168.16.0/27	192.168.16.1 - 192.168.16.30	192. 168.16.31	255.255.255.224
20	**CEE**	30	192.168.16.32/27	192.168.16.33 - 192.168.16.62	192.168.16.63	255.255.255.224
30	**Estudantes**	30	192.168.16.64/28	192.168.16.65 - 192.168.16.78	192.168.16.79	255.255.255.224
40	**Docentes**	30	192.168.16.96/27	192.168.16.97 - 192.168.16.126	192.168.16.127	255.255.255.224
50	**DAF**	30	192.168.16.128/27	192.168.16.129 - 192.168.16.158	192.168.16.130	255.255.255.224
60	**DRA**	30	192.168.16.160/27	192.168.16.161 - 192.168.17.190	192.168.17.191	255.255.255.224
70	**Wireless BDA**	30	192.168.16.192/27	192.168.16.193 - 192.168.16.222	192.168.16.223	255.255.255.224
80	**Wireless Visita**	30	10.20.30.0/27	10.20.30.1 – 1020.30.30	1020.30.31	255.255.255.224

Tabela 25: Tabela de Endereçamento

1.3. Internet

Informações sobre o link de internet

Provedor	Tecnologia	Num. Circuito	Suporte	Banda	Custo Mensal
CIUEM	IP MPLS	001.003.xxx	-	1Gbps	Sem Custo

Tabela 26: Informação sobre o Link de Internet

1.4. Domínios Registrados

Domínio	Entidade	Validade	DNS Master	DNS Slave
@feng				

Tabela 27: Domíneos Registrados

1.5. Hardware

Servidor do Bloco Administrativo

Nome	IP	Função	Tipo	SO
BDADIRSERVER	192.168.255.20/27	Centralização de acesso à rede	Domínio único	Windows Server 2025

Tabela 28: Especificações do servidor do Bloco Administrativo

Processador: Intel Xeon(R) Gold 644Y (96 CPUs)

Memória RAM: 32GB

Disco: 4.5TB (/dev/sda)

Software

Serviço	Software	Porta	Protocolo
ftp	vsftpd	21	TCP
ssh	sshd	22	TCP
http	apache	80	TCP

Tabela 29: Serviços no Servidor

1.6. Serviços críticos

Os serviços listados a seguir devem receber atenção especial da equipe de suporte pois são críticos para o funcionamento da infra-estrutura.

- **Serviços de alta criticidade:**
    - Acesso à Internet (incluindo o roteador);
    - Firewalls;
    - Windows Server (DNS);
    - E-mail: Postfix (MX) + Cyrus (Ger. de caixas postais);
    - Expresso Livre (Groupware);
    - PosgreSQL (Banco de Dados);
    - Wndows Server (DHCPD - Distribuidor de Ips);
    - Storage RAID 5;
    - Veeam Backup & Replication (Backup).

1.7. Licenças de softwares

Fornecedor	Software	Usuários	Modalidade de Cobrança
Microsoft	Windows Server 2022	Ilimitados	-

Tabela 30: Licenças de Software

1.8. Hardware adiquirido recentimente

Fornecedor	Modelo	Aquisição	Garantia	quantidade	Custo/Unidade
Sophos	XGS 126(W)	2024	-	10	-
Cisco	Cisco Catalyst 9200L	2024	-	80	-
Cisco	Cisco Catalyst 9300	2025	-	12	-
Procomputers	UTP CAT6	2025	-	2000M	-

Tabela 31: Hardware Adquirido Recentimente

Anexo 3: Invetário do equipamento actual da FEUEM

Localização Física			Dispositivo											
Edifício / Departamento	Piso	Compartimento	Roteador		Switch		Access Point		Computador	Impressora	Servidor	Conversor	Firewall	Observação
			Quantidade	Marca e modelo	Quantidade	Marca e modelo	Quantidade	Marca e Nome	Quantidade	Quantidade	Quantidade	Quantidade	Quantidade	
Bloco Administrativo	RC	Administração	0		1		0		1	1	0	0	0	O Switch da administração é da camada 3
		DTIC	0		3		1		4	1	0	0	0	
		DPM	0		0		1		9	2	0	0	0	
		UP	0		1		3		7	1	0	0	0	
		UGEA	0		0		1		5	1	0	0	0	
		Lab. Estruturas	0		0		1		2	1	0	0	0	
		R. Académico	0		0		1		7	1	0	0	0	
	1º	Gab. Do Director	0		0		1		2	1	0	0	0	
		Corredor da Dir	0		0		1		0	0	0	0	0	
		Sala de reunião	0		0		1		1	0	0	0	0	
	Subtotal		0		5		11		39	9	0	0	0	
Cadeiras Gerais	RC	Secretaria	0		1		1		3	1	0	0	0	A Sala 2 (De mestrados) pertence ao edifício/departamento de Pós-Graduação.
		Sala de estudos	0		1		1		0	0	0	0	0	
		Sala de formações	0		0		0		10	0	0	0	0	
		Salas administrativas	0		0		0		4	0	0	0	0	
	1º	Sala de informática	1		4		1		25	0	0	0	0	
		Sala 2 (De mestrados)	0		1		0		20	0	0	0	0	
		Salas de Aulas e corredor	0		0		6		0	0	0	0	0	
		Anfiteatro	0		0		1		0	0	0	0	0	
		Biblioteca	0		0		1		1	0	0	0	0	
	Subtotal		1		7		11		63	1	0	0	0	
Pós-Graduados	RC	Pós-Graduados	0		1		1		0	0	0	0	0	O sinal da sala Pós-Graduados provém directamente do backbone e o da RH provém do LAB de Alta Tensão, pois esta sala (RH) pertence ao Bloco Administrativo.
		Sala de Mestrados	1		1		3		25	0	0	0	0	
		RH	0		2		0		3	2	0	0	0	
	Subtotal		1		4		4		28	2	0	0	0	
Lab. De Alta Tensão			0		1		3		0	0	0	0	0	O sinal provém do Bloco Administrativo mas o edifício pertence ao DEEL.
CEEI			0		2		2		0	0	0	0	0	Pertence ao DEEL
EQ	RC	Sala 0	0		4		0		0	0	0	0	0	Existe um switch da camada 3, o que recebe o Sinal
	RC, 1º e 2º	Laboratórios	0		0		9		0	0	0	0	0	
	1º	Secretaria	0		1		1		4	2	0	0	0	
		Salas dos docentes	0		1		3		0	0	0	0	0	
	2º	Sala de Informtica	0		1		1		17	0	0	0	0	
		Sala de Informática de Mestrados	0		1		1		20	0	0	0	0	
		Salas de Aulas	0		0		3		0	0	0	0	0	
	Subtotal		0		8		18		41	2	0	0	0	
EC	RC	Laboratório	0		1		3		0	0	0	0	0	
	1º	Sala de Informática	0		2		3		16	0	0	0	0	
	Subtotal		0		3		6		16	0	0	0	0	
EM	RC	Oficinas	0		0		5		0	0	0	0	0	
	1º	Lab. Info de Mestrados	0		2		1		12	1	0	0	0	Pertence à Pós-Graduação.
		Laboratorio	1		3		1		0	0	0	0	0	
		Salas de Aulas	0		0		3		0	0	0	0	0	
	2º	Sala de Informática	0		2		1		0	0	1	0	0	
		Sala de Lab.	0		1		1		1	0	0		0	
		Salas de aulas	0		0		2		0	0	0	0	0	
		Gabinete	0		2		0		1	1	0	1	0	
	Subtotal		1		10		14		14	2	1	1	0	
DEEL	RC	Sala Máquinas Electricas	0		0		2		0	0	0	0	0	
		Sala de formações	0		0		3		10	0	0	0	0	
	RC | Data Center	Huawei	1		2		0		0	0	1	0	2	Serve apenas no DEEL. O servidor possui 8 discos de 4 TB cada. Dois (2) Storages de 5 discos (4 TB cada).
		Backbone	3		3		0		0	0	1	2	0	Apenas um roteador funciona. Tem também a Starlink mas não sendo usando. Um Storage de 6 TB. Controlador de WI-FI.
		Mestrados dos Petrolio	0		2		0		0	0	0	0	1	Tem um RTN 905 (Radio Transponder Network).
	1º	Secretaria	0		1				4	1	0	0	0	
		Salas de Aulas	0		0		4		0	0	0	0	0	
	2º	Sala Lab. Informática	0		3		1		25	0	0	0	0	
		Salas/Lab. de Aulas	0		0		4		1	1	0	0	0	
	Subtotal		4		11		14		40	2	2	2	3	
Total			7		51		83		241	18	3	3	3	

Legenda

1. **CEI:** Centro de Eletrónica e instrumentacão
2. **DEEL:** Departamento de Engenharia Electrotécnica
3. **DTIC:** Departamento de Tecnologia de Informacão e Comunicacão
4. **DPM:** Departamento de Património e Manutencão
5. **UP:** Centro de Estudos de Informática
6. **UGEA:**
7. **RC:** Rés do Chão
8. **EM:** Engenharia Mecanica
9. **EQ:** Engenharia Química
10. **EC:** Engenharia Civil

Anexo 4. Inquéritos : Guião de Entrevista

Universidade Eduardo Mondlane

Faculdade de Engenharia

Departamento de Engenharia Electrotécnica

Curso: Licenciatura em Engenharia Informática

Guião – Entrevista

1. Existe alguma regra/padrão no processo de cabeamento da rede da FEUEM?
2. Que tipo de cabeamento é usado / que categoria é usada?
3. Existe algum padrão de corres ou uma forma de distinção dos cabos que conectam os diversos equipamentos na rede?
4. Em relação aos Switches do Bloco Administrativo, quais são as capacidades máxima e minima?
5. Ainda sobre os Switches do Bloco Administrativo (DTIC), Existem Switches dedicados somente para a conexão de estações de trabalho (PCs) ou qualquer dispositivo pode ser conectado a qualquer Switch?
6. Os Switches do Bloco Administrativo são padronizados? Ou são do mesmo vendor? Caso não, existe um plano para a padronização?
7. Em relação aos AccessPoints, eles são suficiêntes para fazer a cobertura de todo o bloco administrativo?
8. Os AccessPoints são padronizados em termos de vendor e capacidade?
9. Em relação ao sinal que vem da *ISP* (CIUEM), existe uma redundância?
10. Ainda em relação ao sinal que vem da *ISP* (CIUEM), alguma vez tiveram um *Blackout* na rede por falta de redundância.

Anexo 5. Inquéritos : Guião de Questionário

Universidade Eduardo Mondlane

Faculdade de Engenharia

Departamento de Engenharia Electrotécnica

Curso: Licenciatura em Engenharia Informática

Guião – Questionário

Inquérito

Este questionário tem como objectivo avaliar a infra-estrutura de rede da **FE-UEM** para identificar melhorias necessárias. Suas respostas são essenciais para garantir um serviço de internet mais eficiente. Desde já gradeço pela sua participação!

1. Alguma vez enfrentou problemas para acessar a internet na rede da FE-UEM?

- [ ] Sim (especifique a frequência: _____)
- [ ] Não

2. Alguma vez teve problemas ao conectar o computador a uma tomada/porta RJ45 na sala de aula?

- [ ] Sim
- [ ] Não

3. Avalie a qualidade da internet na FE-UEM, considerando suas necessidades:

- [ ] 1 (Muito má)
- [ ] 2 (Má)
- [ ] 3 (Razoável)

- [ ] 4 (Boa)

- [ ] 5 (Excelente)

4. Na sala de informática, alguma vez já enfrentou dificuldades para acessar a internet?

- [ ] Falta de conexão

- [ ] Lentidão

- [ ] Interrupções frequentes

- [ ] Outros (especifique): _____

5. Sobre a liberdade de instalar programas nos computadores da faculdade:

- [ ] Totalmente livre

- [ ] Parcialmente livre

- [ ] Nenhuma liberdade

- [ ] Outros (comente): _____

6. Sugestões para melhorar o controle de acesso aos computadores:

- [ ] Senhas individuais

- [ ] Monitoramento por software

- [ ] Restrição de instalação de programas.

Informações demográficas:

- Cargo/Função: _____.

- Tempo de trabalho na FE-UEM: _____.

Grelha de respostas:

P	1	2
Sim	X	X
Não		

P	3
Muito Má	
Má	
Razoável	X

P	4
Falta de conexão	
Lentidão	X
Interrupções frequentes	
Outros	

P	5
Totalmente Livre	
Parcialmente Livre	X
Nenhuma Librdade	
Outros	

P	6
Senahas Individuais	
Monitorização por Software	
Restrição de instalação de programas	X

Anexo 6. Análise orçamental do projecto

Para realizar a análise orçamental do projeto de reestruturação e modernização da rede de dados da Faculdade de Engenharia da Universidade Eduardo Mondlane (FEUEM) no bloco administrativo, foram consideradas as principais categorias de custos envolvidas. As tabelas abaixo ilustram de forma clara a informação detalhada:

1. Detalhamento por categoria

a) Equipamentos de rede

Inclui os disposiivos necessários para a modernização da rede, como switches, firewalls, access points, roteadores e servidores.

Equipamento	Quantidade	Preço unitário (MZN)	Total (MZN)
Switches Cisco Catalyst 9200L	7	-	-
Switches Cisco Catalyst 9300	2	50.000	100.000
Firewall Sophos XGS 126 (W)	1	-	-
Access Points TP-Link EAP670	14	5.000	70.000
Roteador	1	20.000	20.000
Servidor	1	-	-
Subtotal	-	-	170.000

b) Cabeamento de infra-estrutura física

Refere-se aos materiais e ferramentas necessários para a infra-estrutura física da rede.

Equipamentos	Quantidade	Preço unitário (MZN)	Total (MZN)
Cabos UTP Cat6	2.000m	50	100.000
Patch Panels	10	2.000	20.000
Racks e Bastidores	5	10.000	50.000
Ferramentas e Materiais	-	-	30.000
Subtotal	-	-	200.000

c) Sistemas de energia e proteção

Refere-se aos equipamentos de proteção energética, essenciais para a estabilidade dos dispositivos.

Equipamentos	Quantidade	Preço unitário (MZN)	Total
UPS Tripp Lite SmartPro	10	15.000	150.000
Estabilizadores de tensão	10	5.000	50.000
Subtotal	-	-	200.000

d) Software e Licenças

Inclui os custos de software e licenças necessárias para a gestão e segurança de rede.

Item	Quantidade	Preço unitário (MZN)	Total (MZN)
Windows Server 2022	1	50.000	50.000
Software de Gestão de rede	-	-	-
Licenças de Firewall (anual)	1	10.000	10.000
Subtotal	-	-	60.000

e) Outros custos

Inclui despesas adicionais como planeamento e cotigência

Item	Custo Estimado (MZN)
Documentação Planeada	50.000
Contingência (10% do total)	68.000
Subtotal	118.000

2. Resumo do orçamento

A tabela abaixo resume os custos estimados por categoria, proporcionando uma visão geral do investimento total necessário para o projecto.

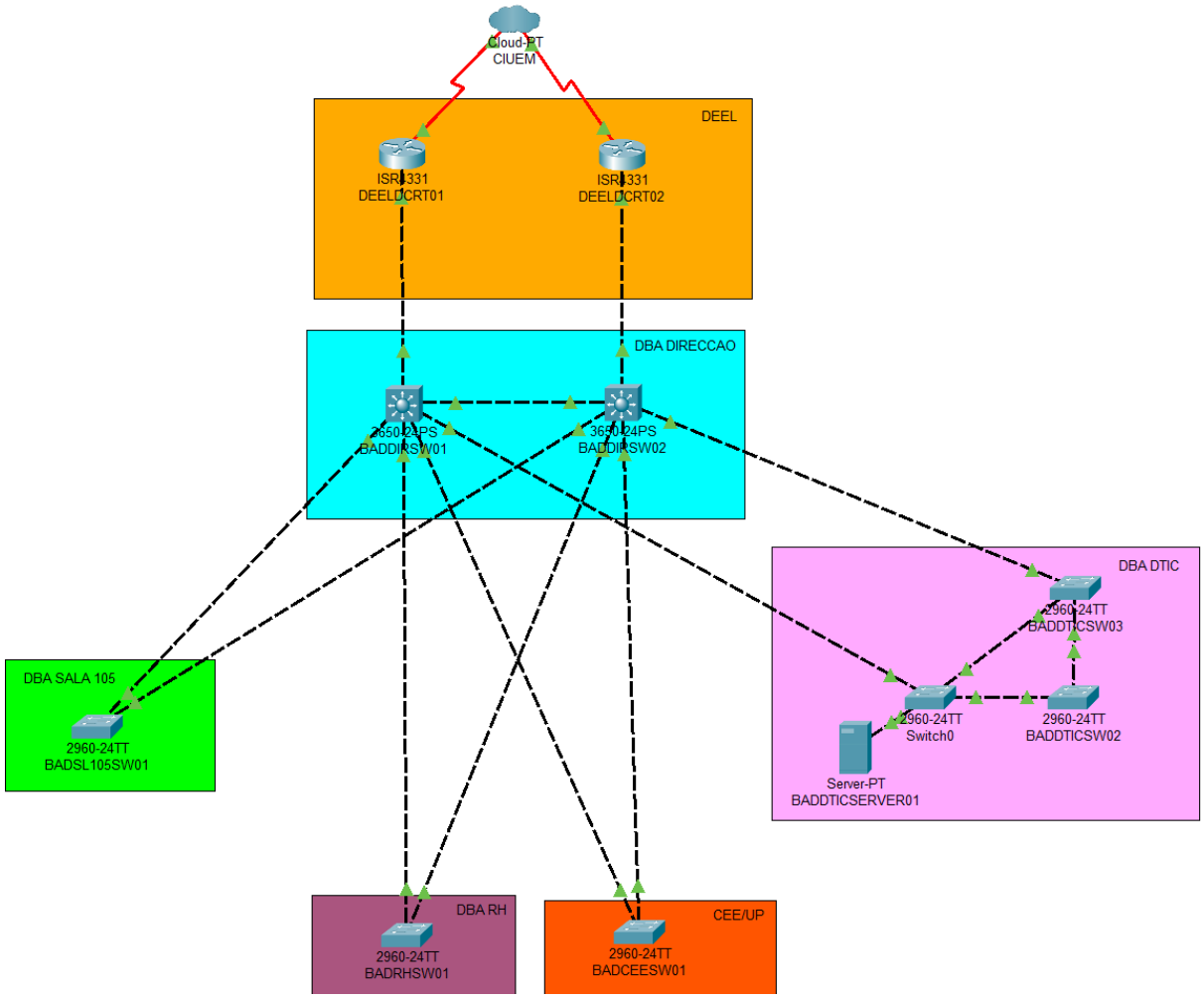
Categoria	Custo Estimado (MZN)
Equipamentos de rede	170.000
Cabeamento e infra-estrutura física	200.000
Sistemas de energia e proteção	200.000
Software e licenças	60.000
Outros custos	118.000
Total geral	748.000

3. Notas Adicionais

- Variação de Preços: Os valores são estimativas baseadas em preços de mercado e podem variar conforme o fornecedor;
- Custos Recorrentes: Licenças de software e suporte técnico são anuais e devem ser considerados para os anos seguintes;
- Contingências: Uma reserva de 10% foi incluída para cobrir imprevistos, uma prática comum em projetos desta natureza;
- Implementação Faseada: A execução em fases pode ajudar a distribuir os custos ao longo do tempo, facilitando o planeamento financeiro.

Anexo 7. Simulação da rede proposta no emulador Cisco Packet Tracer

A rede proposta foi simulada no emulador de redes Packet Tracer com o propósito de testar a sua implementação num ambiente controlado, permitindo antecipar e resolver eventuais dificuldades antes da sua instalação física.



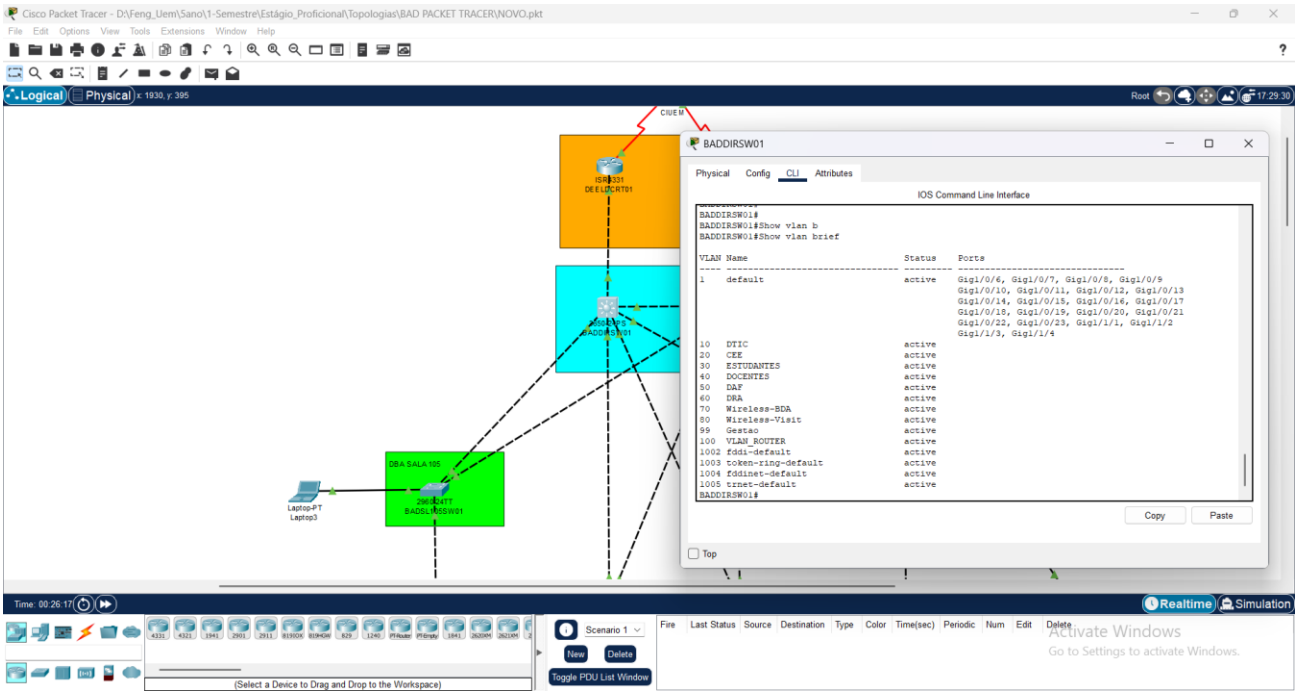
Conforme é visível na imagem apresentada, esta ilustra a proposta de solução para a reestruturação da rede do bloco académico da Faculdade de Engenharia da Universidade Eduardo Mondlane (FEUEM).A rede foi concebida com base em princípios modernos, garantindo elevada disponibilidade e robustez. Para assegurar um funcionamento estável e eficiente, foram implementados protocolos avançados de gestão de tráfego, nomeadamente o Rapid Spanning Tree. Adicionalmente, foram configurados protocolos de redundância dinâmica nos roteadores, permitindo que operem em conjunto de forma harmoniosa, sem conflitos, assegurando continuidade do serviço mesmo em caso de falha parcial.

Anexos – Anexo 7

Para reforçar a segurança e optimizar o desempenho, a rede foi segmentada em VLANs, distribuídas de acordo com critérios funcionais e departamentais. Esta segmentação não apenas melhora a gestão do tráfego, como também limita o acesso entre diferentes áreas da rede, reduzindo riscos de intrusão ou propagação de ameaças.

Desta forma, a arquitectura proposta garante uma infra-estrutura resiliente, segura e adaptada às exigências de um ambiente académico moderna.

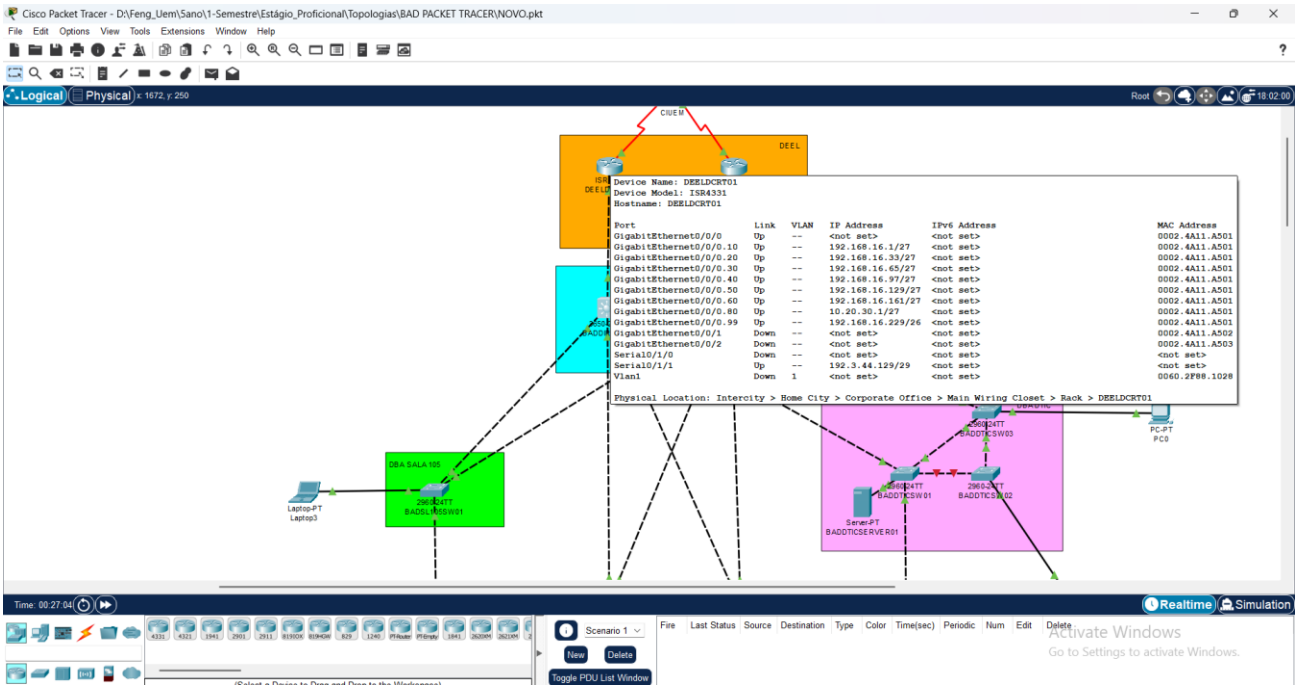
Vlans configuradas nos Switches



A figura acima ilustra as Vlans configuradas nos Switches, tendo em conta que a rede do bloca administrativo foi projectada para conceber sete (7) Vlans, todas elas foram configuradas e atribuidas a um *range* de endereços IP de modo a permitir a segmentação na rede.

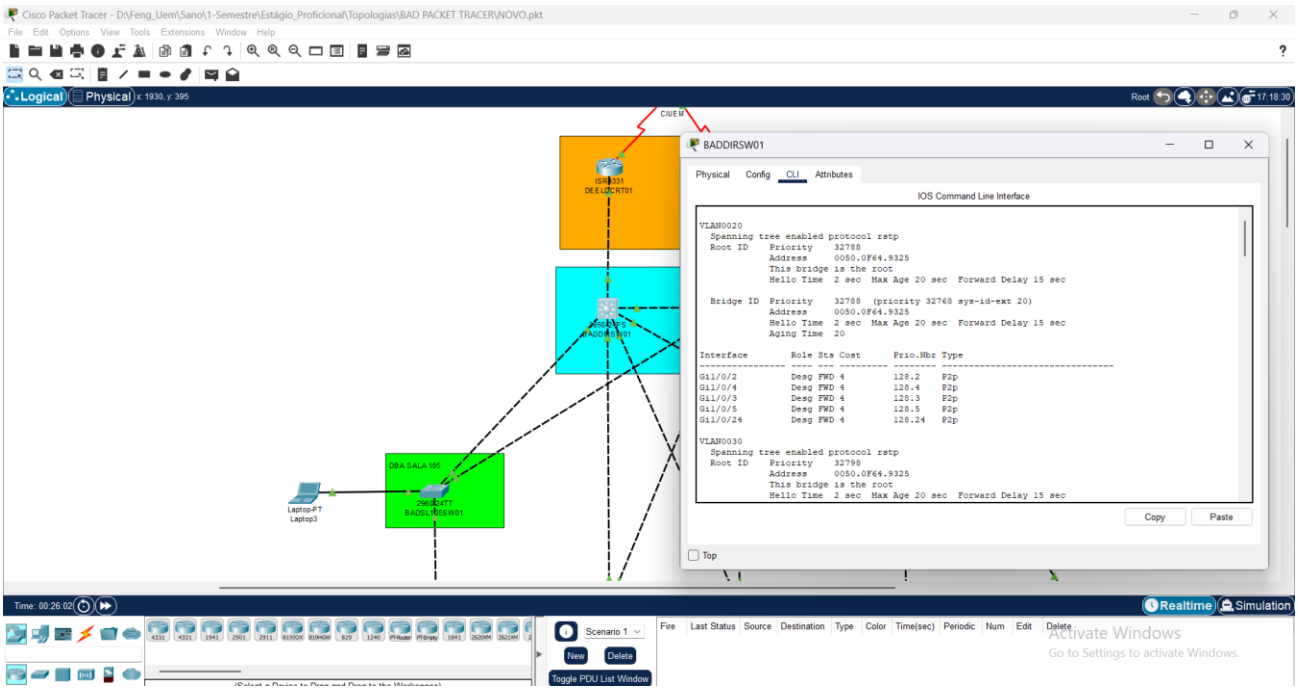
Anexos – Anexo 7

Vlans configuradas nos Routers



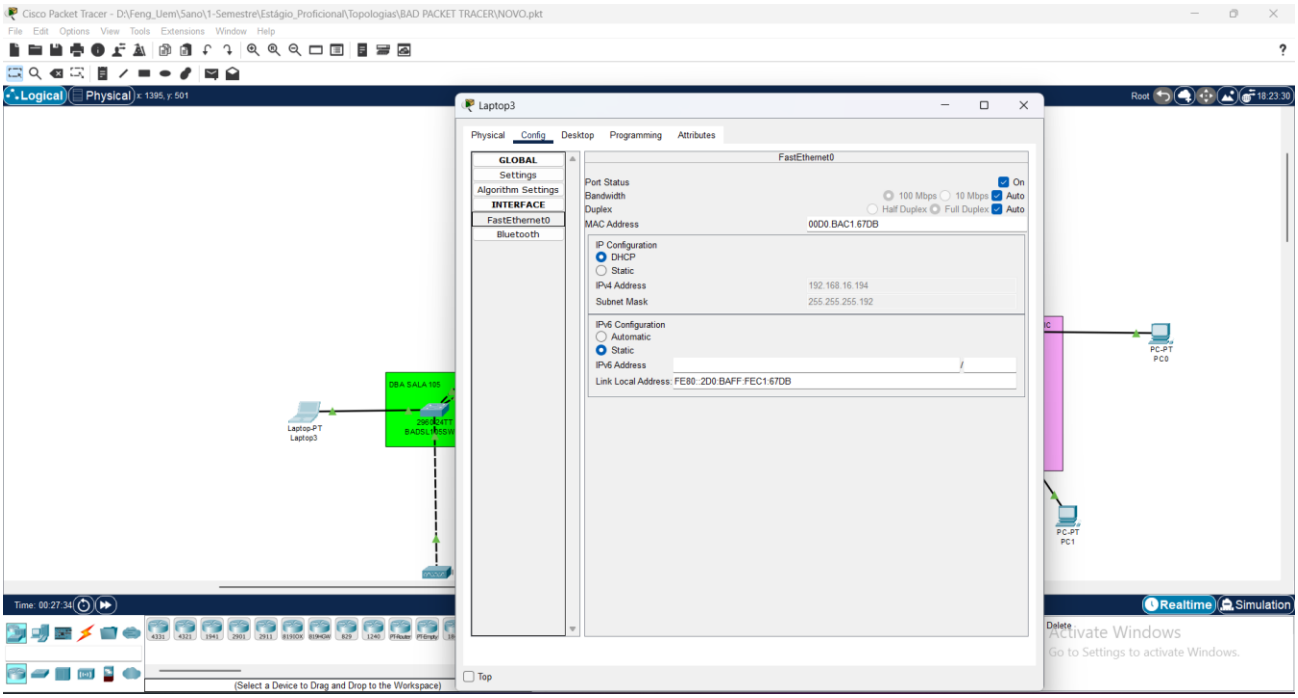
A figura acima ilustra as VLANs configuradas nos routers, essas configurações visam permitir que os usuários da rede possam aceder a redes externas, como por exemplo a internet.

Configuração do protocol RSTP

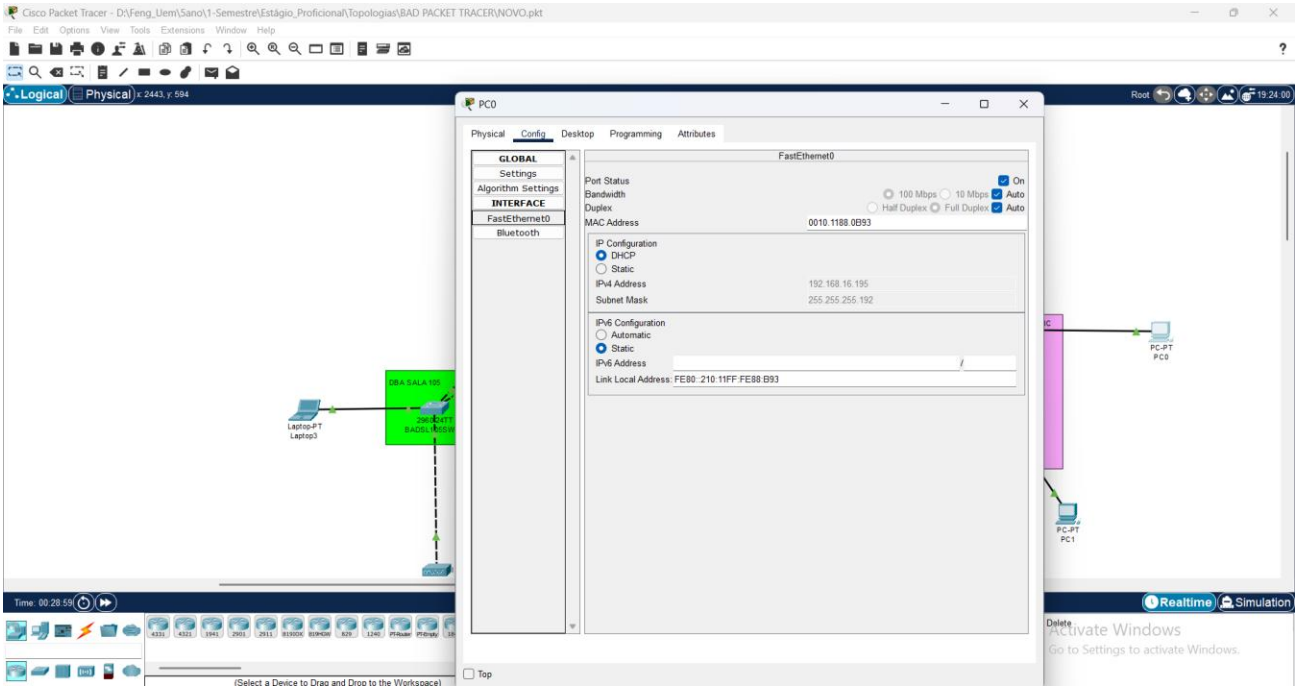


Anexos – Anexo 7

Destribuição de endereços IP via DHCP no PC1 para o texte de conectividade entre PCs conectados na mesma VLAN mas em Switches diferentes.

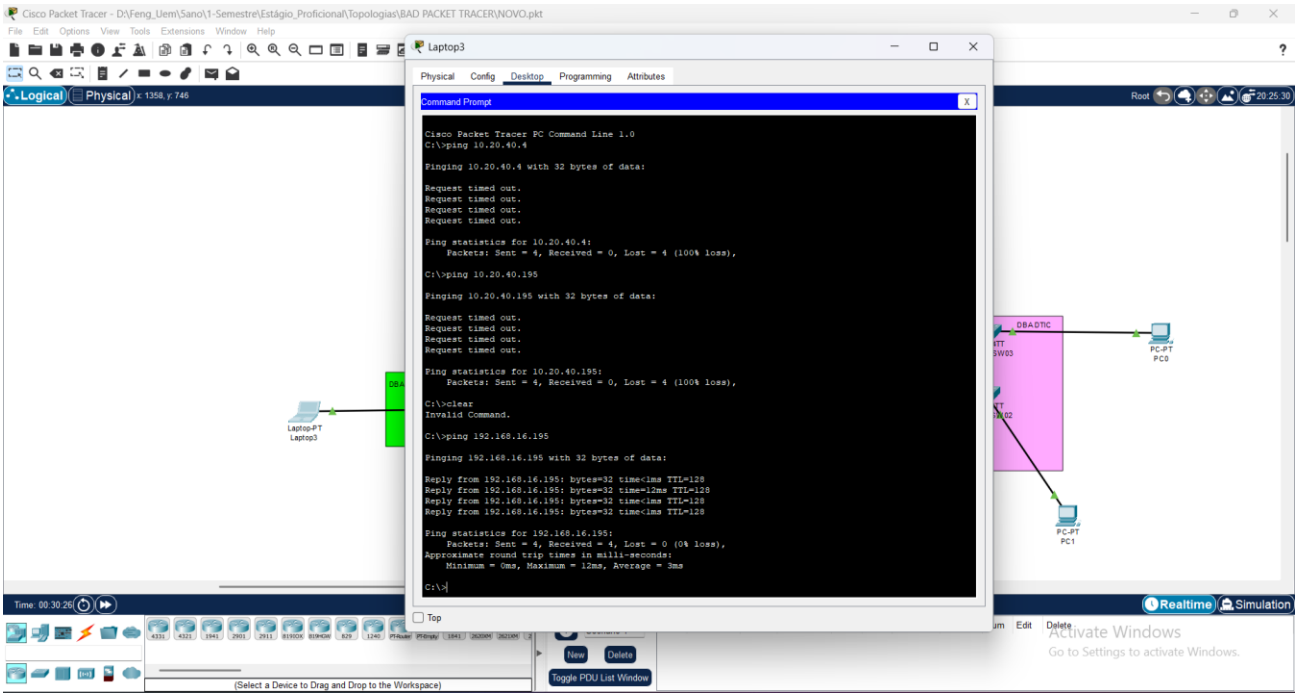


Destribuição de endereços IP via DHCP no PC2 para o texte de conectividade entre PCs conectados na mesma VLAN mas em Switches diferentes.



Anexos – Anexo 7

Texte de conectividade (Ping) entre o PC1 e o PC2



Anexos – Anexo 7

Anexos – Anexo 7