Universidade Eduardo Mondlane

Faculdade de Engenharia

Curso de Engenharia Informática

PROPOSTA DE MELHORAMENTO DE INFRAESTRUTURA E IMPLANTAÇÃO DE UM SISTEMA DE GESTÃO DE REDE COM *ACTIVE DIRECTORY*

Caso de Estudo: FACULDADE DE ENGENHARIA

Autor
Vilanculos, Sérgio Raúl

Supervisora
Eng. Tatiana Kovalenko

Maputo, Agosto de 2013

Universidade Eduardo Mondlane

Faculdade de Engenharia

Curso de Engenharia Informática

PROPOSTA DE MELHORAMENTO DE INFRAESTRUTURA E IMPLANTAÇÃO DE UM SISTEMA DE GESTÃO DE REDE COM *ACTIVE DIRECTORY*

Caso de Estudo: **FACULDADE DE ENGENHARIA**

Autor
Vilanculos, Sérgio Raúl

Supervisora
Eng. Tatiana Kovalenko

Maputo, Agosto de 2013

Agradecimentos

Por este trabalho ter chegado ao fim, quero agradecer aos meus pais Raúl Faife Vilanculos e Glória João Chirrinze que incondicionalmente têm me dado o seu apoio e que mesmo estando longe de mim sempre demonstraram o quão amorosos são comigo.

.A Deus pela sua graça e saúde que me proporciona a cada dia da minha existência;

Aos meus irmãos os quais tenho maior apreço por eles junto com os seus companheiros das suas vidas conjugais;

Aos meus pais Raúl Faife Vilanculos e Glória João Chirrinze pelo seu sacrifício ao qual se deve a minha formação;

Ao meu chará Arnaldo Mazive e sua esposa (às suas memórias) que tanto fizeram por mim;

Ao meu irmão Raúl Julião Vilanculos junto com a sua esposa Luísa Justino Chichava;

Às minhas irmãs Anita Raúl Vilanculos, Aida Julião Vilanculos, Adélia Raúl;

Vilanculos, Esperança Julião Vilanculos, Noémia Raúl Vilanculos e Nólia Julião Vilanculos;

Ao meu tio Lourenço Alfredo Chirrinze e sua esposa Quitina;

À minha supervisora Eng.ª Tatiana Kovalenko pelo seu acompanhamento durante a execução deste projecto;

Aos meus colegas e amigos Felício Jaime Balane, Helber Chin Choo e Rúben Moisés Manhiça pelas suas críticas e pontos de vista.

Resumo

Em sistemas de redes de computadores, a necessidade de uma gestão integral dos seus recursos é imprescindível de modo a garantir uma maior disponibilidade dos mesmos, oferecendo de forma centralizada e eficaz informações referentes ao estado de cada serviço ou dispositivo gerenciável ligado à rede, garantindo dessa forma a interoperabilidade do sistema visto que situações anómalas passam a ser reportadas em tempo real e integral.

E porque só se pode gerir algo que realmente exista, é importante que a infraestrutura de rede esteja devidamente operacional de modo a fazer valer o esforço, nesse âmbito, numa primeira instância coube avaliar a infraestrutura da rede local e com base nessa informação desenvolver uma nova topologia de rede. Em seguida, foram objecto de análise aspectos relacionado com a implantação de uma ferramenta de monitoramento e controlo de activos de rede.

O estudo avalia a integração de uma ferramenta de gestão de rede aliada a uma aplicação de gestão de informação e de alguma tecnologia física necessária de modo a suprimir as necessidades correntes, nomeadamente:

- ✓ requalificação da infraestrutura de rede;
- ✓ monitoramento de toda a infraestrutura da rede informática da Faculdade de Engenharia, especificamente todos os dispositivos de interconexão gerenciáveis, estações de trabalho, aplicações clientes e servidoras, e;
- ✓ gestão de utilizadores da rede dando possibilidade de restrição de actividades por grupos de utilizadores e audição dos acessos efectuados por estes com maior ênfase à auditoria referente ao uso de serviços web.

Neste trabalho são apresentados requisitos funcionais e não funcionais para a estruturação e desenvolvimento de um ambiente de gestão da rede informática da Faculdade de Engenharia, baseado em pesquisas e avaliação de projectos semelhantes e de forma particular a interpretação das necessidades do ambiente de estudo. Com base no estudo realizado e na base de experiências efectuadas, pode se verificar que o ambiente proposto responde as necessidades actuais.

Palavras-chave: gestão, gestão, controlo, sistema, topologia, *Active Directory*.

Índice

Lista de abreviaturas e acrónimos

AD- *Actve Directory*

AD DS- *Active Directory Domain Services*

CIUEM- Centro de Informática da Universidade Eduardo Mondlane

CMIP- *Common Management Information Protocol*.

CMIS- *Common Management Information Service*

CPU- Unidade Central de Processamento

DECI- Departamento de Engenharia Civil

DEEL- Departamento de Engenharia Electrotécnica

DEMA- Departamento de Engenharia Mecânica

DEQUI- Departamento de Engenharia Química

DHCP- *Dynamic Host Configuration Protocol*

DNS- *Domain Name System*

FTP- *File Transfer Protocol*

Gab- Gabinete

HTML – *Hypertext Markup Language* (Linguagem de Marcação de Hipertexto)

HTTP- Protocolo de comunicação utilizado na internet que permite a transferência de dados entre um dado servidor e os computadores a este conectados.

HTTPs- *http* seguro

IP- *Internet protocol*

LAN- *Local Area Network*

LDAP- *LightWeight Directory Access Protocol*

MAC - *Media Access Control*

MIB- Base de informação de gestão

OSI- *Open Systems Interconnection*

SGBD- Sistema de Gestão de Banco de Dados

SMS- *Short Message Service* (Serviço de Mensagens Curtas)

SNMP- *Simple Network Management protocol*

TIC- Departamento de Tecnologias de Informação e Comunicação

UDP- *User Datagram Protocol*

UML- *Unified Modeling Language*

UPS- *Universal Power Supply*

UTP- Cabo de dados de par trançado

VLAN- *Virtual LAN*

WAN- *Wide Area Network*

Wireless- Sem fio

Glossário de termos

Access Point- dispositivo de rede que disponibiliza conectividade duma rede aos utilizadores sem fio.

Buffer- meio de armazenamento temporário de dados para compensar as diferenças na velocidade de tráfego de informações durante a transmissão.

DMZ- zona desmilitarizada, área de uma rede na qual sistemas residentes possuem acesso irrestrito ao mundo exterior (*Internet*).

DNS- *Domain Name Server,* trata se de um sistema de tradução de nomes em endereços *IP's* válidos, e vice-versa.

Gateway- dispositivo de rede com capacidade de conectar duas redes distintas.

Iptables- uma aplicação encontrada em sistemas Unix que oferece funcionalidades de *firewall*

Link- linha física ou lógica que estabelece a conectividade entre dois pontos de uma rede.

Login- nome de usuário utilizado durante o processo de identificação para o acesso a um sistema restrito.

Plug-in- acessório de *software* que estende a capacidade de uma aplicação.

Rack- um contentor físico de dispositivos de implementação de rede.

Switch- dispositivo de interconexão que permite a segmentação da rede em domínios de colisão menores.

Vírus- programas ou arquivos desenhados para causar danos a um sistema de computadores, podendo estar anexado ou embutido a uma página Web, *e-mail*, ficheiros distintos ou macro.

Lista de Figuras

Lista de Diagramas

Lista de Tabelas

1 Introdução

1.1 Contextualização

O avanço tecnológico da humanidade nos diversos campos de conhecimentos tem exigido de forma cada vez mais acentuada, excelência técnica e precisão na execução das suas actividades, aliada a este avanço encontra se a comunicação entre entidades individuais ou empresarias. De acordo com o crescimento das civilizações que geograficamente foram ocupando áreas cada vez mais dispersas, a comunicação a longa distância se tornava uma necessidade cada vez maior e desafiante.

Nos meados de século XIX, Samuel F. B. Morse viria inaugurar uma nova época nas comunicações ao inventar o telégrafo especificamente no ano de 1838. Nesse sistema as mensagens eram codificadas em cadeias de símbolos binários (código Morse) e eram transmitidas manualmente por um operador através de um dispositivo gerador de pulsos eléctricos. A comunicação através de pulsos elétricos atravessou uma grande evolução, dando origem a maior parte dos grandes sistemas de comunicação encontrados actualmente como o telefone, o rádio e a televisão.

Com introdução de computadores pessoais na década 70 deu se origem a um novo modelo computacional para o atendimento às necessidades das organizações no qual um grande número de computadores separados, porém interconectados executam suas tarefas compartilhando dispositivos, periféricos e equipamentos como impressoras, *modems*, e outros. Através dessa distribuição chegou se as arquitecturas de redes de computadores que se encontram actualmente.

Entretanto, o crescimento acentuado do número de utilizadores da rede de computadores da Faculdade de Engenharia e o constante surgimento de aplicações cada vez mais complexas e dependentes da troca mútua de informações torna indispensável a existência de ferramentas que melhorem o processo de gestão da rede, permitindo aos administradores desta, uma fácil e rápida reacção às ocorrências que possam de alguma forma afectar o seu funcionamento.

Por via disso, o presente trabalho centrou-se na análise do estado actual da rede de modo a produzir uma topologia de rede melhorada no concernente a abrangência e disponibilidade desta. Em adição propôs-se um conjunto de ferramentas de controlo e monitoramento da rede, paralelamente a isto foram analisados mecanismos de melhoramento de desempenho da rede.

1.2 Objectivos

1.2.1 Objectivos gerais

O presente projecto, consiste no estudo de uma proposta de melhoramento da rede informática da Faculdade de Engenharia, sob ponto de vista físico e lógico. Tendo como objectivos gerais:

- desenvolver uma topologia de rede que atenda às necessidades da instituição.
- propor ferramentas para gerir com maior desempenho a rede informática da Faculdade de Engenharia.

1.2.2 Objectivos específicos

O presente projecto, tem como objectivos específicos:

- efectuar o levantamento do estado actual da rede;
- determinar locais de implantação de pontos de acesso para utilizadores móveis;
- propor uma topologia de rede que se adequa a solução obtida;
- incorporar um mecanismo de gestão de recursos de rede entre dispositivos terminais, dispositivos de implementação da rede, segmentos de rede, sistemas operativos e aplicações clientes.
- encontrar uma solução que permita controlar o acesso à rede informática, e permitir a determinação de quotas de consumo de largura de banda por utilizador.

1.3 Metodologia

Para alcançar os objectivos acima citados, primeiramente fez-se diversas entrevistas aos funcionários do departamento de TIC da Faculdade de Engenharia com vista a adquirir mais informações sobre o estado da rede actual, bem como o processo de gestão desta.

Em seguida foram realizadas revisões bibliográficas em diversos manuais e *sites* com a finalidade de adquirir conhecimentos básicos e específicos sobre a metodologia de desenvolvimento de projectos de redes.

Para a produção da topologia lógica da rede, foi feita uma análise comparativa de situações conhecidas, procedendo se a posterior com elaboração de um mapa específico para a situação da Faculdade de Engenharia. No que tange ao projecto físico, procurou se adaptar a estrutura física actual as exigências por hora estabelecidas de modo a minimizar os custos de mudança de tecnologia.

Neste processo de revisões bibliográficas, foi feita uma procura de diferentes ferramentas de gestão de redes tendo-se procedido à comparação entre elas e na base de resultados obtidos em testes estabelecer a solução final.

1.4 Organização do projecto

O presente relatório encontra se divido pelas seguintes partes:

- **Capitulo I - Introdução**

Neste capítulo são abordados aspectos introdutórios.

- **Capítulo II – Revisão Bibliográfica**

Neste capítulo fazem-se descrições teóricas sobre alguns aspectos que serão levados em conta durante processo de elaboração do relatório.

- **Capítulo III-Visão geral do sistema actual e processo de tomada de decisão**

Neste capítulo descreve-se o estado actual da rede

- **Capitulo IV – Desenvolvimento do projecto**

É neste capítulo onde é feita a análise de requisitos do sistema, análise das ferramentas de gestão, e desenvolvimento de topologias da rede.

- **Capitulo V – Conclusões e Recomendações**

Neste capítulo discutem-se as conclusões obtidas e propõe-se algumas recomendações

- **Capítulo VI-Referencias Bibliográficas**

Neste capítulo são apresentadas todas as fontes que permitiram a elaboração do projecto assim como do relatório.

- **Capítulo VII-Anexos**

Neste capítulo são apresentados os anexos do trabalho.

2 Revisão Bibliográfica

Neste capítulo, são apresentados aspectos teóricos que serviram de base de conhecimento para a produção do presente relatório.

2.1 Gestão de Redes e modelos de gestão

A maior parte das empresas e instituições de ensino informatizadas (1) encaram a tecnologia de redes como um instrumento imprescindível para o seu sucesso na implementação das suas tarefas comerciais e educacionais respectivamente.

Essencialmente um administrador de redes de computadores tem como actividades: desenvolvimento, implantação, monitoramento, análise e controlo da rede bem como dos seus recursos computacionais.

Um sistema de gestão de rede é definido como sendo um conjunto de ferramentas utilizadas para monitoramento e controlo da rede. Para a gestão de uma rede TCP/IP se faz necessária à consideração de alguns elementos.

2.1.1 Estação de gestão

A estação de gestão é vista como interface para o administrador de rede, definido como sistema de gestão de rede, este contém um conjunto de *softwares* executando diferentes serviços de gestão. Todas as atividades de gestão são colectadas nessa máquina de forma a prover relatórios do estado dos diferentes serviços monitorados, sendo que sua visualização pode ser feita localmente ou remotamente através de interfaces de acesso como navegador *web*.

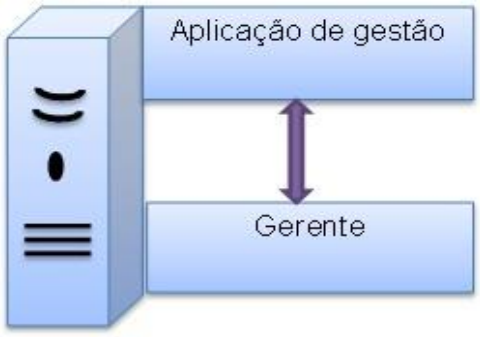


Figura 2-1: Estação de gestão

2.1.2 Agente de gestão

O agente de gestão responde às solicitações de informações e de acções da estação de gestão. Este deve por sua vez assincronamente prover informações

importantes que podem não ter sido solicitadas, enviando uma mensagem de notificação à estação, anunciando o sucedido. A mensagem pode ser enviada em forma de *e-mail*, de um alarme ou de um *sms*.

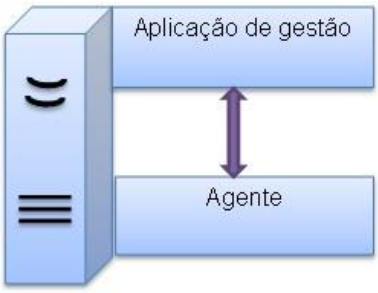


Figura 2-2: Agente de gestão

2.1.3 Base de informação de gestão (*MIB)*

Os recursos a serem geridos são representados como objectos, sendo a colecção de objectos referenciada como a base de informações geridas. Para o presente projecto compreendem a base de informação os recursos de *hardware* e *software* presentes nas diferentes estações de trabalho e dispositivos de interconexão.

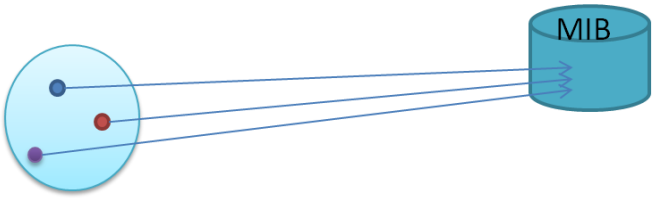


Figura 2-3: Base de Informação

2.1.4 Protocolo de gestão de redes

O protocolo de gestão de redes corresponde à forma de comunicação entre as estações de gestão e o agente de gestão. Para este projecto, foi objecto de estudo o protocolo *SNMP* como protocolo de gestão da rede por ser o mais difundido e de alguma forma ser o protocolo usado nas diferentes estações de gestão que compõem o escopo desse trabalho, isto é, os sistemas operativos em uso na instituição possuem um agente *SNMP* nativo.

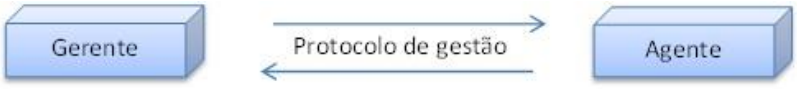


Figura 2-4: Protocolo de gestão de redes

2.1.5 Protocolo *SNMP*

O protocolo *SNMP* (2) foi projectado em meados dos anos 80 como uma resposta aos problemas de comunicação entre diversos tipos de redes. A ideia básica por trás do *SNMP* era oferecer uma maneira facilmente implementável para a gestão de roteadores, servidores, estações de trabalho e outros recursos de rede.

O *SNMP* é um protocolo do nível de aplicação da Arquitectura *TCP/IP*, operando tipicamente sobre o *UDP* (*User Datagram Protocol*). O *SNMP* é considerado simples dado que seus agentes requerem um *software* mínimo pois a maior parte do poder de processamento e de armazenamento de dados reside no sistema de gestão, enquanto um subconjunto complementar dessas funções reside no sistema gerido. Suas principais características são:

- ✓ suporte para a transferência eficiente de grandes blocos de dados;
- ✓ estratégias de gestão de rede centralizada;
- ✓ controlo de acesso;
- ✓ criptografia de dados.

2.2 Modelo de gestão *OSI*

O modelo *OSI* (*Open Systems Interconnection*) pertencente a *ISO* (3) baseia-se na teoria de orientação a objectos, sendo que o sistema representa os recursos geridos através de entidades lógicas, as quais recebem a denominação de objectos. Provendo deste modo, uma arquitectura de gestão capaz de atender à diversidade de equipamentos da rede. Num sistema de gestão de redes de computadores baseado neste modelo, o gerente transmite operações de gestão aos agentes a fim de obter informações actualizadas sobre os agentes. Recebidas as operações pelo agente, este executa as acções necessárias sobre os objectos e transmite as notificações geradas por estes ou notificações sobre a ocorrência de eventos. Neste modelo para a troca de informações entre os gerentes e seus agentes de gestão é utilizado o serviço *CMIS* (*Common Management Information Service*) e o protocolo *CMIP* (*Common Management Information Protocol*).

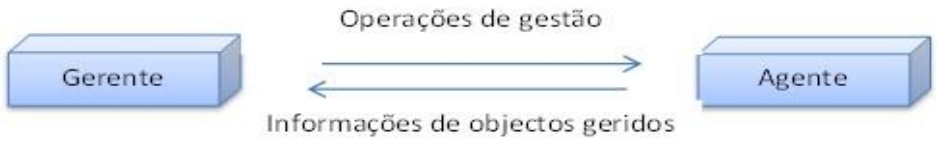


Figura 2-5: Troca de Informações

Portanto a *ISO* define cinco itens de gestão de redes de computadores, descrevendo as diferentes áreas funcionais de gestão de redes.

2.2.1 Gestão de falhas

Para que se prossiga com o gestão de falhas é preciso que o sistema seja controlado como um todo, destacando cada componente essencial de modo que seja monitorado individualmente, permitindo o seu devido funcionamento. Desta maneira, quando ocorre uma falha será fácil e rapidamente determinado o componente exacto onde a falha ocorreu. Em seguida, é preciso isolar o resto da rede da falha de tal forma que continue a funcionar sem interferências, em seguida pode se proceder a reconfiguração da rede, reparando ou retirando o componente em falha para que se possa restaurar o funcionamento normal da rede.

2.2.2 Gestão de contabilização

Em várias situações é preciso cobrar pela utilização dos recursos da rede, não sendo o caso da Faculdade de Engenharia, contudo é preciso contabilizar a utilização dos mesmos por diversas razões:

- ✓ uso ineficiente dos recursos;
- ✓ sobrecarga da utilização por diversos utilizadores;
- ✓ administradores da rede poderão futuramente se referenciar para tomadas de decisão (por exemplo, como faria para expansão da rede caso se justifique), sendo isso possível se este estiver ciente das actividades de seus utilizadores.

2.2.3 Gestão de configuração

Em sistemas modernos de comunicação encontram-se diversos equipamentos, podendo um mesmo dispositivo ser configurado como um roteador ou um *switch* ou mesmo um analisador de tráfico, esta componente inclui tarefas de manutenção, adição e actualização dos dispositivos e serviços da rede, assim como o mapeamento da rede. Na perspectiva de serviços, permite a disponibilização de parâmetros de desempenho tais como tempo de resposta, taxa de erros e a disponibilidade dos dispositivos e/ou serviços da rede. Portanto é necessário que seja feita uma melhor escolha de *software* e parâmetros adequados que permitam a inicialização e actualização dos mesmos.

2.2.4 Gestão de desempenho

A necessidade de acompanhamento de limites de desempenho, monitoramento, rastreamento de actividades na rede, fazem com que seja imprescindível a necessidade de obter respostas as seguintes questões, sempre que for preciso:

- ✓ qual é a capacidade actual de utilização?
- ✓ existe algum tráfego excedente?
- ✓ existe uma diminuição acentuada na largura de banda efectiva?
- ✓ existe congestionamento em algum ponto da rede?

Com base nas informações colectadas, obtêm-se as respostas às questões outrora levantadas.

2.2.5 Gestão de segurança

A informação, como sendo o elo mais importante de uma instituição, necessita de uma total segurança para que pessoas não autorizadas tenham acesso restrito à mesma. Para isso a geração e distribuição de chaves de criptografia são imprescindíveis para garantir que as informações que trafegam pela rede sejam integras e seguras. A instituição precisa de estar informada sobre quem são os utilizadores autorizados a utilizarem tais recursos disponibilizados e concedidos pela administração da rede. Para isso é necessário que haja um monitoramento e controlo de acessos à rede e que se faça uma manutenção de *logs* e arquivos de auditoria.

2.3 Segurança de redes

Para uma solução de segurança de uma rede de computadores existem outros aspectos a considerar como é o caso de implantação de uma barreira entre uma rede insegura como é o caso de *Internet* e a rede local da instituição, e a gestão de utilizadores.

2.3.1 *Firewall*

Firewall é o nome dado ao dispositivo de rede que tem como objectivo regular o tráfego entre redes distintas e impedir a transmissão de dados nocivos ou não autorizados entre elas. Desta forma não deixando passar o tráfego indesejado de informações e garantindo que certos serviços ou dados sejam acedidos somente a partir da rede privada e/ou por pessoas autorizadas. Isto é feito com estabelecimento

de regras colocadas estrategicamente na máquina que será usada como porta de saída e entrada para as redes inseguras.

2.3.2 Servidor *Proxy*

Um servidor *Proxy* possibilita aos computadores contidos em uma determinada rede o acesso a uma rede pública. É um serviço normalmente instalado num dispositivo com acesso directo à *Internet*, podendo ser no *firewall* acima descrito, ou outro dispositivo dedicado, sendo assim toda a solicitação externa a rede deve ser efectuada a esta máquina que por sua vez realiza as requisições em nome das outras máquinas da rede. Podem ser acopladas outras funcionalidades a este servidor tais como:

Web-proxy que é responsável pelo armazenamento de páginas já visitadas por computadores de uma rede (*cach*) tornando o acesso a estas mais rápido e consequente liberação do segmento de rede para outras funções. É também, uma das principais funcionalidades impedir o acesso indevido às páginas da *Internet* pelos utilizadores, isto é, restrição de páginas por conteúdo.

NAT (*Network Address Translation*-Tradução de endereços de rede) (4), uma funcionalidade que permite que o endereço interno de um computador da rede seja ocultado na *Internet* apresentando um *IP* que não tem relação com os *IP's* internos da instituição, procedendo da seguinte forma: como já foi referenciado, todo o tráfego da instituição destinado à *Internet* é enviado para o servidor *Proxy*. Quando o pacote chega ao dispositivo com *NAT* configurado, este atribui ao pacote, um outro endereço *IP* no caso público antes de transmiti-lo para *Internet*, quando o pacote de resposta chega, o mesmo dispositivo envia ao computador local que havia feito o pedido, com base nas informações de tradução de nomes mantidas no mesmo dispositivo. Este procedimento protege os endereços *IP's* verdadeiros da rede interna da *Internet*, dificultando os ataques externos ao sistema.

O *firewall* efectua uma filtragem de pacotes que consiste em analisar o cabeçalho dos pacotes, enquanto passam por este, decide o que fazer com os mesmos.

2.3.3 Controlador de domínio

Sendo o *DNS* (*Domain Name Service*) (1) serviço essencial para o funcionamento da *Internet*, essa importância encontra-se associada à natureza das informações que este armazena, tais como resolução de nomes para os utilizadores da

rede e provimento de informações a respeito de zonas sobre as quais possuem autoridade. Aliado a esse conceito, encontra se o controlador de domínio que se descreve a seguir.

Controlador de domínio (5) é um serviço que se destina a centralizar todos os direitos aos diversos recursos de uma rede tais como nomes de utilizadores, senhas de acesso, recursos acessíveis por utilizador. Em análise encontra-se o controlador de domínio *AD DS (Active Directory Domain Services*) baseado no sistema operativo Windows, que é uma implementação de serviço de directório do protocolo *LDAP*[1] que armazena informações sobre os objectos de uma rede, tais como estações de trabalho e utilizadores e disponibiliza essas informações a utilizadores e administradores da rede. É também responsável por gerir interacções entre utilizadores e domínios inclusive processo de autenticação e de pesquisa de directórios.

[1]*LDAP* (*Lightweight Directory Access Protocol*) é um protocolo utilizado pelos servidores para concentrar informações em um repositório logicamente organizado. Graças a este protocolo é possível inserir, alterar excluir informações comuns em uma espécie de banco de dados de informações

3 Visão Geral do sistema Actual

Segundo um dos Administradores da rede da Faculdade de Engenharia (6), actualmente a Faculdade de Engenharia possui uma rede de computadores oferecendo diversos serviços como acesso a *Internet*, bases de dados, contendo diversas informações de funcionários e estudantes, e várias estações de trabalho disponibilizando um conjunto de aplicações dos utentes. Porém a rede encontra se desprovida de políticas de segurança e de um sistema de gestão da mesma. Tomando como base o Diagrama 3-1, desenvolvido após um trabalho de levantamento de informações sobre a estrutura física e lógica actual da rede, é possível verificar a ausência de vários componentes e serviços importantes que garantem a disponibilidade, segurança, e gerenciabilidade de uma rede de computadores.

Observando o diagrama nota-se que qualquer estação de trabalho tem uma total liberdade para se comunicar com qualquer outra, seja qual for o serviço requisitado a máquina receptora. A conexão entre os dispositivos de distribuição é efectuada sem a presença de um *link* redundante devido à obsolescência das conexões de fibra óptica, traduzindo se num ponto único de falha para as conexões. Portanto, é importante estabelecer uma redundância de conexão que permita a recuperação da conexão em casos de uma falha no *link* primário. No aspecto de segurança, verifica-se que a rede é desprovida de políticas de acesso sendo esta acessível por qualquer utilizador que tenha essa pretensão. O acesso à *Internet* é efectuado sem restrições localmente definidas, estando apenas a mercê do provedor de serviços. No entanto, a solução actual não é das mais seguras, apesar do *gateway* da rede estar baseado num sistema desenhado especificamente para oferecer uma maior segurança à rede.

Ao longo dos diferentes pontos da rede são notáveis vários pontos de acesso, disponibilizando acesso à rede para utilizadores sem fio, porém o uso desta rede não apresenta nenhuma restrição de acesso, isto é, qualquer utilizador pode se conectar a qualquer uma das redes, tanto a rede sem fio quanto a rede cabeada sem necessidade de se autenticar, entretanto, apenas um dos dois pontos de acesso operacionais neste momento no caso o ponto de acesso da Administração é que requer a utilização de uma senha para autenticação dos utentes. De referir que apenas os pontos de acesso da Administração e das *TIC's* encontram-se operacionais.

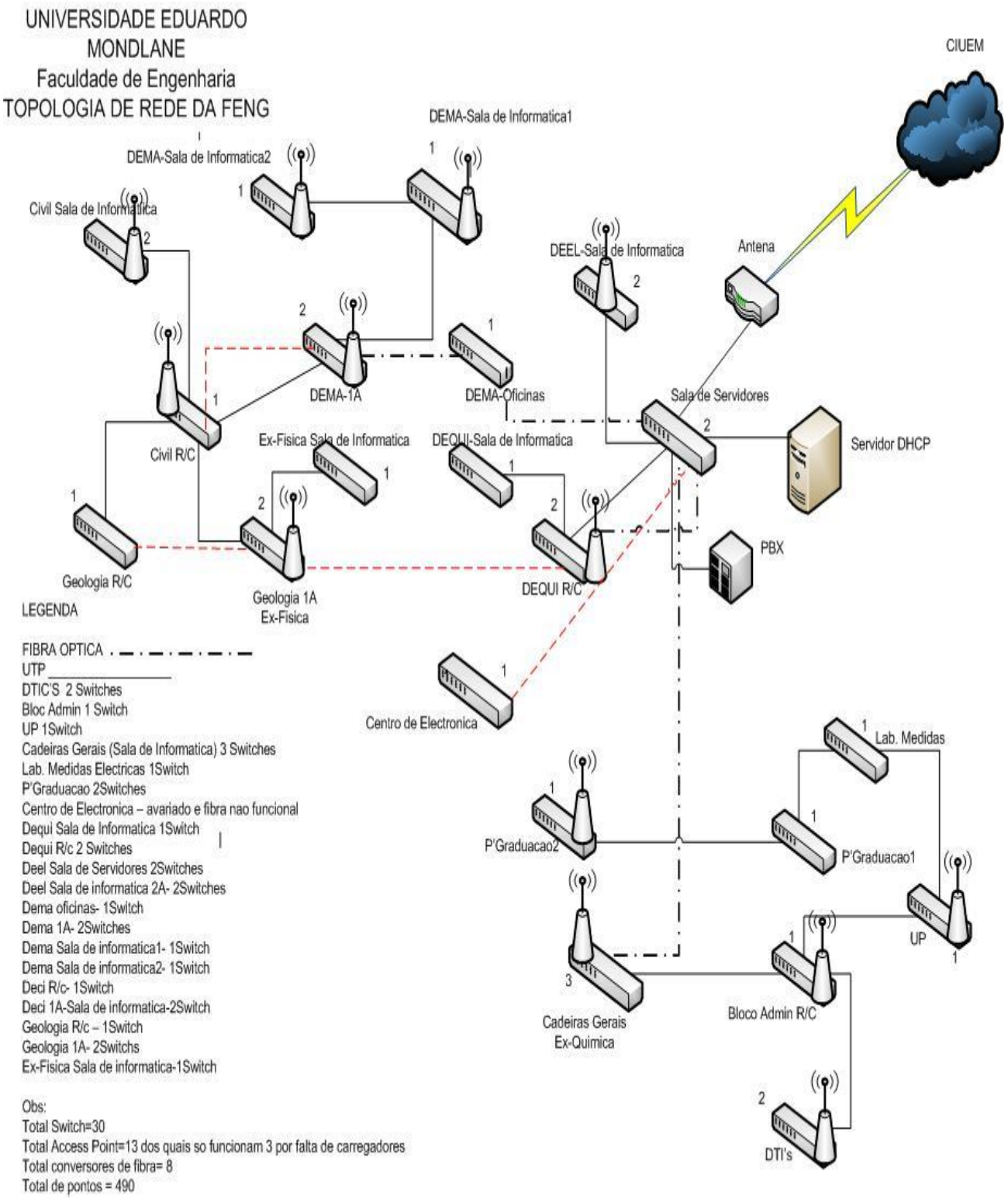


Diagrama 3-1 Diagrama actual da rede

A análise do estado actual da rede incluiu também a contabilização de pontos de rede disponíveis e obsoletos ao longo de toda a infraestrutura perspectivando a renovação ou inclusão de novos pontos conforme necessário, vide anexo 1.

3.1 Tomada de Decisão

Segundo (7) o processo de tomada de decisão é a selecção consciente de um curso de acção dentre as alternativas disponíveis para obter um resultado desejado, isto é, para se proceder a um processo de tomada decisão faz se necessária à existência de pelo menos duas soluções possíveis.

O processo de tomada de decisão desenvolve se em sete etapas, a saber:

1. Percepção da situação que abrange algum problema.
2. Diagnóstico e definição do problema.
3. Definição dos objectivos.
4. Busca de alternativas de solução ou de cursos de acção.
5. Escolha da alternativa mais apropriada ao alcance dos objectivos.
6. Avaliação e comparação dessas alternativas.
7. Implementação da alternativa escolhida.

É importante realçar que cada etapa influência no desenvolvimento das outras.

3.1.1 Definição do Problema

A Faculdade de Engenharia, sendo uma instituição de ensino superior, tem se empenhado na massificação do uso dos sistemas de informação como um recurso indispensável para alcançar seus objectivos que passam por oferecer serviços íntegros e confiáveis aos seus utentes, esta possui uma rede de computadores distribuída em todos os departamentos que a constituem, porém, o acesso à mesma encontra se por hora limitada devido à degradação da infraestrutura de rede local. Sendo comum encontrar pontos de rede inutilizados, locais de trabalho sem acesso a rede, com a estrutura de cabos desfeita em vários departamentos inclusive salas de informática, tornando a disponibilidade da rede um requisito por hora insatisfeito.

Nesse contexto, existe a necessidade de uma revisão abrangente da infraestrutura de rede local da Faculdade de Engenharia de modo que a disponibilidade desta se torne um desejo alcançável. É de maior importância que todos os gabinetes de trabalho, salas de aulas, laboratórios, bibliotecas e outros locais de estudo individual ou em grupo beneficiem se de acesso à rede de dados, seja pela rede cabeada ou pela rede sem fio de modo a garantir um acesso mais abrangente e eficiente aos recursos disponibilizados por esta.

Por conseguinte, para garantir a operacionalização da rede, far-se-á necessário incorporar mecanismos de segurança e de gestão integrais para que esta não seja alvo de um dispêndio sem benefícios a longo prazo. Para tal, é necessário que se faça uma gestão e acompanhamento contínuos, permitindo assim que situações indesejáveis sejam fácil e rapidamente diagnosticadas de tal forma que entidades responsáveis pela administração da rede possam determinar quando e que procedimentos de contingência devem ser tomados, bem como obtenção de estatísticas para melhorar o processo de gestão da rede e contribuir para optimização de desempenho.

Até então, o processo de gestão dos recursos da rede é feito mecanicamente, tornando assim o trabalho mais árduo para os administradores da rede. Não provê mecanismos de geração de relatórios de desempenho da rede, recolha de informações sobre os diferentes equipamentos responsáveis pelo encaminhamento dos serviços aos utentes da rede. Por via disso é preciso proceder à implantação de um sistema de gestão da rede que possa monitorar e controlar os diversos equipamentos e serviços desta e permitir que facilmente sejam adoptadas políticas de utilização.

3.1.2 Avaliação de Alternativas

O processo de avaliação de alternativas levou em conta a análise diferentes ferramentas de gestão de redes onde com base na avaliação das funcionalidades de cada um deles aliado aos resultados dos testes, foi possível determinar a solução final.

Durante este processo, foi possível verificar que cada uma dessas ferramentas responde a certas áreas funcionais e não a totalidade das áreas funcionais de gestão outrora definidas, havendo dessa forma uma necessidade de fazer um estudo comparativo das diferentes ferramentas baseando se nas funcionalidades para as quais cada uma responde conforme as áreas gestão definidas no capítulo 2, para tal é apresentada abaixo uma tabela que destaca as áreas de actuação de cada ferramenta, e posteriormente são apresentadas as respectivas tabelas comparativas.

Tabela 3-1 Identificação de áreas funcionais

Identificação de áreas funcionais de gestão por ferramenta					
	Configuração	Segurança	Desempenho	Contabilização	Falhas
Nagios	✓		✓	✓	✓

Zabbix	✓		✓	✓	✓
Spiceworks	✓		✓	✓	✓
Squid		✓	✓	✓	
Mikrotik	✓	✓		✓	

Como se pode notar o conjunto formado por *Nagios, Zabbix* e *Spiceworks*, são ferramentas desprovidas da funcionalidade de gestão de segurança, sendo que as restantes têm essa funcionalidade e a de gestão de contabilização porém desprovidas das outras funcionalidades. Sendo assim fez se a escolha das ferramentas para atender às necessidades aqui descritas, efectuando uma comparação entre estas, baseada nas suas áreas funcionais e as características consideradas principais para o escopo desse projecto. Para facilitar a compreensão do que sucede nas tabelas abaixo adopta se um critério de designação de cada um dos grupos de *software* que estabelece que as primeiras três ferramentas são ferramentas de gestão de configuração, e as últimas duas são ferramentas de gestão de segurança, contudo isto não significa que respondem simplesmente às áreas definidas pelo nome a elas atribuído.

Tabela 3-2 Ferramentas de gestão de configuração

Estudo comparativo das ferramentas de gestão de configuração			
	Nagios	***Zabbix***	***Spiceworks***
Protocolo de comunicação *SNMP*	✓	✓	✓
Alertas via *e-mail*	✓	✓	✓
Alertas via sms	✓	✓	✓
Suporte a *plugins* de terceiros	✓		✓
Multiusário *Web* com níveis de acesso	✓	✓	✓
Autobusca de dispositivos		✓	✓
Alertas costumizáveis	✓		✓
Desenvolvimento de sistemas costumizáveis	✓		
Execução de comandos remotos		✓	✓
Suporte a plataformas *Windows*	✓		✓
Suporte a plataformas *Unix*	✓	✓	✓
Licença livre	✓	✓	✓
Licença commercial		✓	
Suporte		✓	

Tabela 3-3 Ferramentas de Segurança

Estudo comparativo das ferramentas de gestão de segurança		
	Squid	*Mikrotic*
Suporte a plataformas *Windows*	✓	✓
Suporte a plataformas *Linux*	✓	✓
Suporte a plataforma *Router OS*		✓
Web-proxy	✓	✓
Filtro de conteúdo	✓	✓
Controlo de largura banda por usário	✓	✓
Relatórios	✓	✓
Filtro por nível de acesso	✓	✓
Filtro por *Mac address*	✓	✓
Filtro por IP	✓	✓

Serviço *hotspot*[2]	✓	✓
Comunicação com o AD do *Windows*	✓	✓
Licença livre	✓	
Licença commercial		✓
Suporte técnico		✓
Licença permanente	✓	✓

3.2 Proposta de solução

Dada a necessidade descrita acima, a solução, como dissera anteriormente passa por uma revisão integral da infraestrutura da rede local de modo a produzir uma topologia de rede que possa fornecer acesso aos diferentes departamentos da Faculdade. Para tal, é preciso estabelecer locais sem ou com pontos obsoletos, definir locais de implantação de pontos de acesso para utilizadores móveis. No que tange a gestão da rede, são aspectos importantes para o caso de estudo (8):

- ✓ compatibilidade com as plataformas de *software* correntes;
- ✓ utilização de padrões abertos;
- ✓ custo de implementação acessível;
- ✓ qualidade e desempenho de *software* aceitáveis;

Serviços de rede

A solução que se propõe, necessita de alguns serviços importantes como alicerces para um melhor desempenho e uma maior disponibilidade da rede, eis:

1. incorporação de um controlador de domínio baseado no *Active Directory*, que irá permitir a criação de grupos de trabalho, criação de políticas de grupos, acesso à informações personalizado, isto é, de acordo com o nível e grupo nele afecto.
2. implantação duma aplicação *Web* integrada ao AD, que irá permitir um acesso personalizado e intuitivo a diversas informações como material de apoio, informações dirigidas aos estudantes, professores e funcionários. Para garantir a integridade desta e de outras informações são definidos níveis de acesso que permitem a criação, alteração, distribuição e visualização de conteúdos.

[2] *Hotspot*- serviço que permite contabilização de consumo de largura de banda, bem como a criação de quotas de consumo; onde seus utilizadores devem possuir credenciais válidas para autenticação no momento de acesso à página requesitada.

3. implantação de um serviço de protecção de acesso à rede. Trata se de um serviço que vela pela saúde da rede em situações de risco eminente, isto é, antes que um computador tenha conexão com os demais são verificados alguns parâmetros de segurança pré-estabelecidos só depois de aprovado o seu estado é direccionado à rede corporativa, enquanto isso é direccionado para uma rede de remediação contendo os serviços requeridos e mecanismos de configuração de segurança.
4. configuração de um servidor de impressoras com diferentes níveis de acesso.
5. Implantação de um servidor *Proxy* que irá permitir um controlo efectivo de acesso ao exterior (*Internet*), e permitir um armazenamento de páginas mais acedidas para garantir a optimização do consumo de largura de banda.
6. implantação de um sistema de monitoramento de activos da rede, como impressoras, roteadores, pontos de acesso, computadores pessoais, *switches* e segmentos de rede.
7. garantir o uso de mesmas contas de acesso entre as redes cabeada e sem fio para os mesmos utilizadores.

Tabela 3-4 Requisitos de produtos de gestão

Requisitos de produtos de gestão	
Característica	**Apresentação**
Interface com utilizador	*Web*
Comunicação com os recursos geridos	*SNMP* versões 1, 2 e 3; *ICMP*, *Telnet*.
Notificação	*E-mail*, SMS, instantâneas.
Núcleo	Elaboração de mapa da rede; Relatórios; Levantamento de topologia da rede;
Processo de identificação de falhas	Manuseio de eventos; Isolamento de falhas
Monitoração remota	Uso de agentes ou *plug-ins*; Análise de protocolos em segmentos *WAN* e *LAN*;

4 Desenvolvimento do projecto

4.1 Resumo executivo

A Faculdade de Engenharia como instituição de ensino debate se com uma necessidade de requalificação da sua rede informática, necessidade esta que passa pelo melhoramento da sua infraestrutura física nos diferentes níveis de acesso e distribuição de forma a garantir um acesso mais abrangente à sua comunidade de utilizadores que por sinal encontra se em franco crescimento devido ao aumento de utilizadores móveis. Sob essa perspectiva, coube desenvolver uma proposta de renovação da rede, enfatizando a incorporação de novos serviços que a torne eficientemente gerenciável, bem como a expansão da rede sem fio de modo a garantir maior acesso à mesma.

4.2 Escopo do projecto

O escopo do projecto é de actualizar a rede local da Faculdade de engenhariam abrangendo um total de cinco departamentos nomeadamente Departamento de Engenharia Mecânica, Civil, Química, Electrotécnica, Cadeiras Gerais e Administração. A rede em questão será acedida por funcionários da Faculdade distribuídos pelos diferentes Departamentos, professores, estudantes internos e externos (visitantes). Não faz parte do escopo do projecto a actualização de qualquer *WAN* usada por esta instituição, bem como a rede de transmissão de voz.

4.3 Análise e descrição de negócio da Faculdade de engenharia

A análise dos objectivos de negócio é absolutamente crucial ao sucesso de um projecto de rede na medida em que a análise final deste não se baseia na sua beleza ou elegância técnica, contudo, em termos dos benefícios envolvidos para o negócio da instituição. Para o efeito, e com base em entrevistas efectuadas junto á instituição procede-se a identificação dos aspectos seguintes.

A Faculdade de Engenharia é uma instituição pública[3] de ensino superior, sendo o seu maior negócio ministrar cursos de engenharia a cidadãos moçambicanos e

[3]Instituição que oferece serviços ao público em geral sem fins lucrativos

estrangeiros, sendo o seu maior fornecedor o Governo de Moçambique dada a sua natureza pública. O seu Universo de parceiros estende-se a outras faculdades de âmbito nacional e internacional, bem como empresas de diferentes origens que contribuem de diferentes formas no processo de ensino desta instituição, de um lado na atribuição de bolsas de estudo aos estudantes e de outro provêm recrutamento para estudantes finalistas e recém-graduados para seus quadros.

4.4 Diagrama de casos de uso

O diagrama de casos de uso representado abaixo espelha as diferentes intervenções que se efectuam ao sistema no seu todo, intervenções protagonizadas pelos administradores da rede, utilizador final e os sistemas individuais que compõem a solução de gestão de uma rede de computadores. Ao longo do projecto, especificamente na revisão literária foram identificadas cinco áreas funcionais de gestão de uma rede de computadores, é na base destas que os casos de uso em descrição se baseiam. O diagrama 4-2 ilustra de forma mais detalhada as diferentes intervenções efectuadas pelos administradores da rede e pelos utilizadores finais.

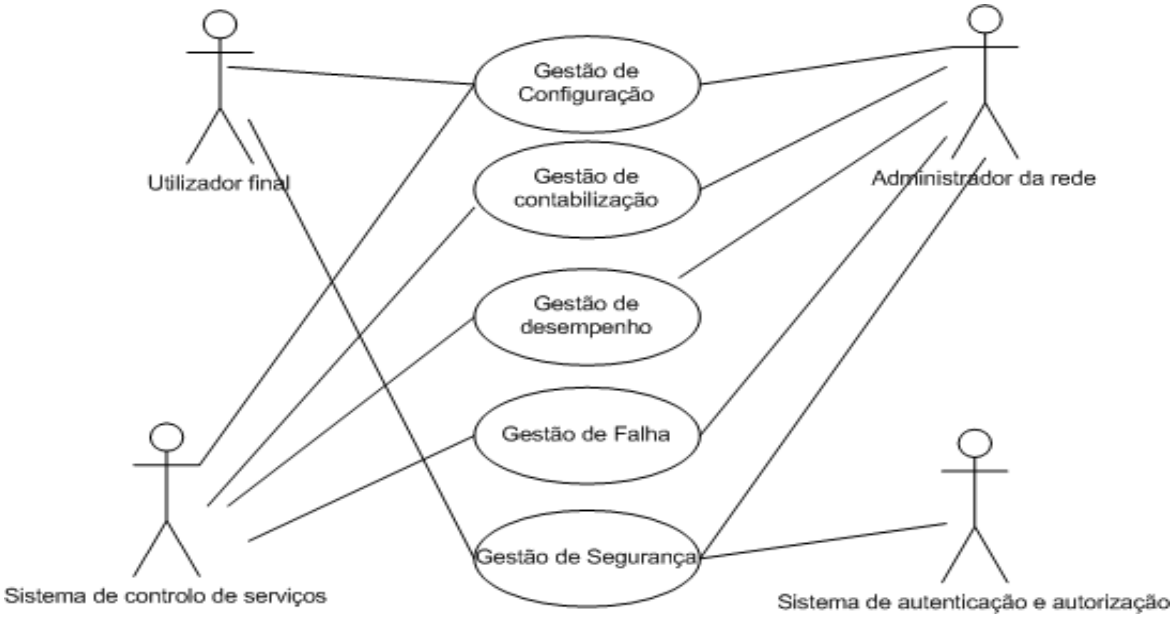


Diagrama 4-1 Casos de uso de alto nível

Nome: Gestão de configuração

Actores: Administrador da rede, utilizador final, sistema de controlo de serviços

Tipo: primário

Resumo: o administrador da rede, parametriza o sistema de gestão indicando as estações críticas tais que requerem o monitoramento contínuo, e o sistema de controlo

de serviços efectua a colecta de informações disponibilizadas pelas estações monitoradas, sendo que o utilizador final participa reportando questões anómalas referentes ao desempenho da rede.

Nome: Gestão de contabilização
Actores: Administrador da rede, sistema de controlo de serviços
Tipo: primário
Resumo: o administrador da rede, parametriza o sistema de gestão indicando o consumo de largura de banda necessário, e o sistema disponibiliza relatórios de consumo da mesma, bem como os acessos efectuados.

Nome: Gestão de Desempenho
Actores: Administrador da rede, sistema de controlo de serviços
Tipo: primário
Resumo: o administrador da rede, parametriza o sistema de gestão indicando os limiares de utilização de forma a serem gerados alertas por parte do sistema na medida em que estes atingirem o nível crítico.

Nome: Gestão de falha
Actores: Administrador da rede, sistema de controlo de serviços
Tipo: primário
Resumo: o administrador da rede, parametriza o sistema de gestão indicando as respostas a serem efectuadas pelo sistema na ocorrência de falhas previamente conhecidas, e o sistema responde os devidos parâmetros de modo a restabelecer o serviço em questão.

Nome: Gestão de segurança
Actores: Administrador da rede, sistema de autenticação e autorização, utilizador final
Tipo: primário
Resumo: o administrador da rede, define mecanismos e políticas de segurança a serem tomados em conta sendo responsabilidade do sistema prover mecanismos de acesso com base nas mesmas políticas aos utilizadores finais.

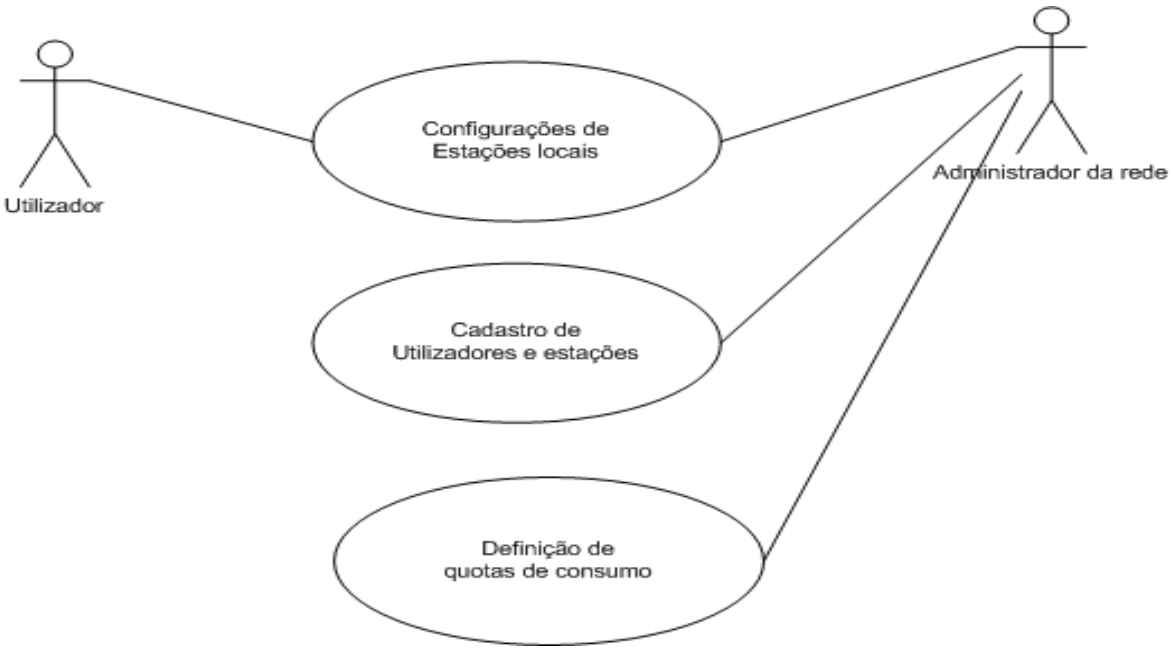


Diagrama 4-2 Casos de uso expandidos

Descrição de casos de uso expandidos

Nome: cadastro de usuários e estações

Actores: Administrador da rede

Propósito: cadastrar os utilizadores e os computadores locais no domínio

Resumo: o administrador da rede, faz o cadastro dos utilizadores com direitos de acesso a rede juntamente com os computadores locais

Tipo: primário

Nome: Configuração de estações locais

Actores: Administrador da rede, usuário final

Propósito: definir parâmetros de segurança para permitir o acesso a rede

Resumo: o administrador da rede, após cadastrados os usuários e os computadores locais no domínio, faz o *login* no computador em questão altera as configurações do sistema de modo a indicar o domínio, sendo que a posterior o utilizador deverá modificar a senha criada pelo administrador da rede antes de ter o acesso à rede.

Tipo: primário

Referências cruzadas: cadastro de usuários e estações

Nome: Definição de quotas de consumo

Actores: Administrador da rede

Propósito: definir o conjunto de recursos acessíveis por utilizador

Resumo: o administrador da rede, após cadastrados os usuários e os computadores locais no domínio, faz o *login* no computador em questão altera as configurações do sistema de modo a indicar os recursos que um utilizador ou grupo têm acesso, especificando também as restrições de acesso Web para o mesmo conjunto.

Tipo: primário, essencial

Referências cruzadas: cadastro de usuários e estações

4.5 Critérios de sucesso *versus* fracasso

O sucesso do presente projecto teve como base os aspectos a saber:

- comunicação efectiva junto a equipa proponente do projecto;
- troca de informações sobre o andamento do projecto;
- dedicação integral no desenvolvimento do projecto e na produção do relatório;
- realização de laboratórios de testes;

A falha de efectivação dos pontos acima descritos pode de alguma forma comprometer o sucesso do projecto e desta forma compromete também os objectivos da direcção da organização que passam pelo melhoramento da infraestrutura da rede local, bem como o controlo de consumo dos recursos oferecidos pela rede.

4.6 Restrições orçamentais

A implantação deste projecto requer a disponibilidade de um orçamento tal que possa cobrir todas as despesas envolvidas no processo desde a fase de implementação a fase de avaliação e monitoramento, entretanto, conhecidas as dificuldades apresentadas pela instituição no concernente à aquisição de equipamentos, optou-se por uma solução baseada numa maior restruturação lógica e menor restruturação física, bem como a utilização se *softwares* livres para o processo de monitoria. Desse modo, garante-se uma solução que atenda as necessidades funcionais e ao mesmo tempo as restrições de carácter orçamental.

4.7 Análise de objectivos e restrições técnicas

A análise de objectivos técnicos de um projecto de rede é uma parte fundamental e crucial para que se possam recomendar tecnologias apropriadas a realidade em estudo de forma a satisfazer o cliente (entidade proponente).

4.7.1 Escalabilidade

A rede, resultante deste projecto, deve permitir um crescimento gradual conforme as exigências funcionais da organização, visto que, com o tempo vão sendo integrados novos utilizadores, novas aplicações, novos *sites* e conexões de rede conforme a procura.

Devido à acessibilidade de aquisição de computadores portáteis, é notável o crescimento do número de utentes móveis, abrindo espaço para uma procura mais acentuada da rede sem fio, havendo dessa forma a necessidade de expandir o acesso a esta conforme as exigências dos utentes.

Sob essa perspectiva, diga-se que a rede deve:

- ✓ prover uma melhor conexão entre os departamentos da instituição;
- ✓ resolução de gargalos de desempenho que possam surgir como resultado de maior tráfego entre os departamentos;
- ✓ prover uma centralização de servidores num *Server farm*.
- ✓ permitir a inclusão de novos *sites* de modo a suportar novos agrupamentos que possam eventualmente surgir como consequência de crescimento da instituição.

4.7.2 Disponibilidade e desempenho da rede

Durante a análise de requisitos é comum encontrar clientes sem conhecimento suficiente para especificar seus requisitos de desempenho, limitando se apenas a necessidade de que a rede deve ser rápida, contudo sem especificações numéricas para o efeito, neste caso o projectista de rede é obrigado a fazer certas suposições de acordo com os critérios que são levados em conta para determinação de requisitos de desempenho da rede.

A medição de desempenho de uma rede de computadores pode ser feita com base num conjunto de critérios definidos como métricas de desempenho para uma dada situação, para o efeito considere-se o seguinte:

Aplicações interactivas precisam de atraso mínimo, para tal é conveniente à revitalização das linhas de fibra de forma que possam prover conexão aos diferentes departamentos junto da central de distribuição, desfazendo se da actual situação em que a interconexão dos diferentes departamentos é baseada em cabos *UTP*, que chegam a ultrapassar 100 metros de comprimento. No aspecto de acesso a Internet, dada a dependência de um único provedor de serviços, é conveniente optimizar a largura de banda disponível fazendo se a priorização de tráfego com *proxy.*

4.7.3 Segurança

Trata-se de um aspecto muito importante do projecto de uma rede de computadores, especialmente com conexões à *Internet* e *Extranet* dada a vulnerabilidade a qual se expõe. O objectivo básico desta precaução passa por garantir que problemas de segurança não afectem a os negócios da instituição. Para tal, é preciso proceder com as questões seguintes:

- Planificação
- análise de riscos
- levantamento de requisitos

4.7.3.1 Planificação

A planificação de aspecto de segurança é crucial para garantir a operacionalidade de uma rede a longo prazo, levando em conta que este processo inclui duas vertentes, a física e a lógica.

a) Vertente física

- A segurança física de uma rede inclui a protecção de todo um conjunto de componentes constituintes desta. É de extrema importância o estabelecimento de um perímetro devidamente protegido para todos os equipamentos de rede. A segurança física num ambiente de rede deve incluir: estabelecimento de uma sala especializada (*Server farm)* para incorporação dos diferentes servidores de rede, *switches* de camada de distribuição, e dispositivos de acesso *WAN*. Sendo que este é um aspecto patente na instituição e com condições apropriadas para o efeito desde o ponto de vista de acesso a climatização da mesma. É importante realçar

que a segurança física dum ambiente de rede estende se ainda a necessidade de incorporação de uma sala de *UPS's* capazes de garantir à alimentação dos componentes de rede prevenindo perdas de dados e danificação dos sistemas informáticos que possa ser causado por quedas de energia. Sob esse aspecto a rede não dispõe dessa capacidade na sua totalidade dado que apenas a sala de servidores e sala de *TIC's* possuem um conjunto de *UPS's* capazes de responder as necessidades dessas divisões.

b) Vertente lógica

- A segurança lógica de uma rede de computadores constitui um aspecto crucial na administração da mesma, a falta de políticas claras de segurança pode comprometer a disponibilidade da rede e, até no nível mais crítico do negócio da instituição. Havendo necessidade de garantir o sigilo de informações sensíveis e garantir a privacidade dos utentes da rede, prover parâmetros de conduta para utilizadores da rede. Contudo, a Faculdade de Engenharia até o exacto momento encontra se desprovida de mecanismos de segurança próprios, dependendo apenas do seu provedor de serviço, no caso o Centro de Informática da Universidade Eduardo Mondlane (CIUEM). Aspectos como protecção de perímetro, protecção de acesso interno e externo, são de grande relevância neste projecto.

4.7.3.2 Análise de riscos

Para implementar a segurança de um *site* ou grupo de utilizadores, deve-se investigar os riscos de não implementar a segurança fazendo a seguinte análise: qual é a sensibilidade dos dados disponibilizados pela instituição e quais são os efeitos de roubo ou mudança dos mesmos na medida em que as empresas se preocupam principalmente com os seguintes três aspectos da segurança:

- vírus[4]
- problemas causados por erros de utilizadores
- problemas causados por utilizadores internos maliciosos

4.7.3.3 Requisitos de segurança

Os recursos que devem ser protegidos são:

- hospedeiros, incluindo servidores.
- dispositivos de interconexão (*switches*, roteadores, pontos de acesso).
- dados de sistemas ou de aplicações
- a imagem da empresa

Os requisitos devem atingir os seguintes objectivos:

- permitir que pessoas externas tenham acesso a dados públicos (via *http*, *https* e *ftp*), mas não dados internos;
- identificar, autenticar e autorizar utilizadores da organização, utilizadores móveis e funcionários que eventualmente trabalhem remotamente;
- detectar intrusos e identificar os danos causados por estes;
- proteger *hosts* e dispositivos fisicamente;
- proteger *hosts* e dispositivos logicamente através de senhas e direitos de uso;
- proteger aplicações e dados contra vírus;
- prover cópias de segurança
- treinar utilizadores sobre a política de segurança da empresa e sobre formas de evitar problemas de segurança.

4.7.3.4 Usabilidade

Usabilidade diz respeito à facilidade com a qual utilizadores acedem os serviços da rede. Enquanto a gerenciabilidade melhora a vida do gerente de rede, a usabilidade foca o utilizador final.

Para melhorar a usabilidade adoptou se pelo seguinte:

[4] Vírus- Programas ou arquivos preparados para causar danos em computadores. Podem estar anexados ou embutidos em páginas de internet, documentos, anexos de *e-mail* e outros recursos lectrónicos.

- ✓ racionalização de políticas de segurança;
- ✓ facilidade de configuração da rede (usando *DHCP*);
- ✓ a facilidade com a qual um utilizador móvel pode se integrar à rede em vários pontos da rede no caso sob os diferentes departamentos;

4.7.3.5 Adaptabilidade

A adaptabilidade descreve como o projecto de rede pode se adaptar a mudanças de:

- tecnologia
- protocolos
- formas de negócio
- legislação

O desenvolvimento deste projecto não inclui requisitos de mudanças estruturais na organização da instituição, contudo, algumas políticas importantes, que até então não se fazem sentir, são definidas de forma a garantir o sucesso deste projecto. No aspecto das tecnologias envolvidas, focou-se numa solução em torno da realidade actual sob o risco de exceder as capacidades orçamentais da instituição.

- A definição de grupos de trabalho, de *sites* ou unidades organizacionais trazem consigo uma componente nova no trabalho colaborativo da empresa, na medida em que a partilha de dados melhora a produtividade da instituição.
- A inclusão de novas aplicações de gestão da rede trazem consigo alguma necessidade de incorporação de novos protocolos, no caso o *SNMP*.
- Um dos aspectos mais importantes da adaptabilidade é a facilidade com a qual as mudanças podem ser feitas na rede (usando *VLAN's*, por exemplo), porém a não existência de dispositivos de interconexão que suportem tal componente, dá espaço para a segmentação da rede recorrendo a unidades organizativas.

4.8 Projecto lógico

O projecto lógico de uma rede de computadores termina com a criação de um mapa de rede indicando segmentos de rede, pontos de interconexão e comunidades de

utilizadores. Actualmente, com o crescimento das redes corporativas emprega se uma arquitectura hierárquica, que permite desenvolver uma rede em fracções sendo que cada fracção foca um objectivo diferente. A criação de uma topologia lógica da rede deve levar em conta questões de redundância de enlaces e de dispositivos de interconexão de forma a garantir uma maior disponibilidade, eliminando pontos únicos de falha.

Existem alguns pontos essenciais que devem ser observados num projecto de topologia de uma rede, nomeadamente:

- ✓ minimização de domínios de *broadcast*, esta característica pode ser alcançada com a inclusão de dispositivos de camada três na camada de distribuição ou pela criação de *VLAN's*;
- ✓ inclusão de segmentos redundantes implica a incorporação de *links* redundantes entre os *switches* de forma a aumentar a disponibilidade;
- ✓ uso de redundância para servidores importantes, é de extrema relevância que servidores como de controlo de domínio, de *DNS* e de controlo de acesso à rede sejam duplicados de forma a garantir a disponibilidade dos serviços por estes oferecidos, mesmo com a queda do servidor primário;
- ✓ incluir caminhos de roteamento alternativos, é conveniente definir rotas alternativas para um dado domínio de *broadcast* para casos de falha da rota principal.

4.8.1 Projecto de segurança da rede

A segurança num ambiente compartilhado, no caso a rede da Faculdade de Engenharia é cada vez mais importante devido a:

- ✓ Conexão para *Internet;*
- ✓ A formação de uma intranet
- ✓ Uso da rede corporativa por utilizadores móveis e funcionários que trabalham remotamente

As etapas que compõem o projecto da segurança são:

a. identificação dos recursos de rede;

b. análise de riscos (implicações) de segurança;
c. elaboração de um plano de segurança;
d. elaboração de políticas de segurança;
e. elaboração de procedimentos para aplicação e implementação das políticas de segurança;
f. manutenção da segurança através de auditorias periódicas.

4.8.1.1 Identificação de recursos de rede e análise de riscos

Em capítulos anteriores, foi dito que para implementar a segurança de um *site* ou grupo de utilizadores, deve-se investigar os riscos de não implementar a segurança. Feita essa análise, verificou-se que:

- A Faculdade de Engenharia possui um servidor de base de dados contendo um conjunto de informações referentes aos funcionários da instituição e dos estudantes da mesma, sendo que estas requerem um nível de protecção maior dado que sua alteração, ou roubo das mesmas pode resultar na anulação de nível de certo estudante.
- Entretanto, são recursos a proteger: as bases de dados da instituição, os dispositivos de interconexão, sistemas operativos e máquinas hospedeiras.

4.8.1.2 Análise de implicações de segurança

O custo da protecção contra uma ameaça deve ser menor do que recuperar-se da concretização desta, portanto, a segurança como qualquer outro requisito possui implicações que devem ser tomadas em conta, eis:

- custo- maior complexidade pode exigir custos de manutenção maiores;
- usabilidade- mecanismos complexos dificultam o utilizador final;
- disponibilidade- pode originar um ponto único de falha no *firewall*;
- gerenciabilidade- existe a necessidade de manter o histórico de *logins*, senhas, e nomes de utilizadores e posteriormente fazer uma auditoria de segurança; portanto a perda ou aquisição ilegal destas pode abrir brechas de segurança maiores.

4.8.1.3 Desenvolvimento de um plano de segurança

Um plano de segurança é um conjunto de especificações a serem feitas de modo a cumprir requisitos de segurança, especificando o tempo, as pessoas e outros recursos necessários para desenvolver e implementar as políticas de segurança.

O plano faz referência à topologia da rede e determina quais serviços serão providos, especificando os provedores de serviços, pessoas com direitos de acesso, forma de acesso e os administradores de acesso.

Como resposta a estas especificações, importa referir que a Faculdade de Engenharia oferece serviços de acesso *web* providos pela CIUEM, a princípio para todos os estudantes e funcionários da instituição, sendo que com a implantação deste projecto, o acesso a este recurso será mediante uma conta de acesso assim como para outros serviços disponibilizados pela rede.

É importante que todos os envolvidos se sintam comprometidos com o plano de segurança.

4.8.1.4 Desenvolvimento de políticas de segurança

Uma política de segurança especifica formalmente as regras que devem ser seguidas pelas pessoas que irão aceder os recursos da instituição, as obrigações das pessoas (utilizadores, e equipe técnica) para manter a segurança passam pelo cumprimento das componentes que abaixo se descrevem.

1. Uma política de acesso
    a. Todos os estudantes, funcionários, técnicos de redes e dirigentes têm direito de acesso a rede mediante uma senha provida pelo Administrador de rede.
    b. Todos esses com excepção dos administradores de redes têm acesso a estes recursos de segunda a sexta no horário compreendido entre as 700h e 2200h, e aos sábados das 7:00h as 18:00h;
    c. O acesso à sala de servidores é concedido apenas aos técnicos de redes, da manutenção e de outros trabalhos de rotina mediante a presença de um agente do departamento de TIC;
    d. Só os técnicos de redes é que podem efectuar uma sessão de acesso remoto;

e. Todos utentes a excepção dos agentes do departamento de TIC possuem uma conta de *login* de domínio e não local, tal conta é válida para utilização conjunta das redes *Ethernet* e *wireless;*
f. A conexão a dispositivos de rede é concedida apenas a equipe das TIC;
g. A incorporação de um novo *software* nas estações de trabalho é concedida apenas ao pessoal de TIC sendo que para as salas públicas como as de informática, o processo será encarregue ao responsável pela sala em questão;
h. Restringir o acesso à páginas por conteúdo;

2. Uma política de responsabilidade
   a. Os utilizadores são responsáveis pela gestão dos seus próprios conteúdos, sendo estes de acesso exclusivo;
   b. Todos os utilizadores de rede são responsáveis pela alteração das suas chaves de acesso e nunca de conta de acesso;
   c. A equipa de operações de rede é responsável pela atribuição de direitos de uso a todos utentes de acordo com o seu nível de acesso;
   d. Apenas a equipe de redes é que possui direitos de criação, alteração e remoção de contas de domínio mediante uma justificação para o efeito;
   e. O sistema deve gerar *logs* de auditoria para avaliar situações de risco.
3. Uma política de autenticação
   a. A política de autenticação estabelece a existência de uma única sessão para cada conta criada.
   b. Os utilizadores da rede sem fio poderão aceder qualquer ponto de acesso ligado à rede bastando prover as mesmas credenciais designadas a este para a rede fixa.

4.8.1.5 Desenvolvimento de procedimentos de segurança

Os procedimentos de segurança implementam as políticas de segurança, os mesmos, definem os processos de configuração, *login*, auditoria e manutenção sendo específicos para cada utente.

Utilizadores - estes possuem capacidade para manuseio de conteúdos designados para si, devem alterar a sua senha de três em três meses preferencialmente. Em casos de acesso negado para certa conta, deve se anunciar o ocorrido à equipe de administração de redes para as estações clientes referentes aos

funcionários da instituição e ao responsável da sala, no caso de ocorrências idênticas nas salas de informática.

Administradores de rede - são responsáveis pela colecta de inquisições e posterior resposta a incidentes de segurança e de outros âmbitos relacionados com a rede.

4.8.2 Mecanismos de segurança

Os mecanismos de segurança levados em conta neste projecto dependem do nível de segurança exigido pela Faculdade de Engenharia de acordo com o nível de sensibilidade de informações disponibilizadas por esta, caso de informações mantidas no registo académico, é de grande importância que estas sejam íntegras e seguras.

I. Autenticação

Mecanismo normal: nome de *login* e senha, usadas durante a sessão de *login*, sendo que todas as estações de trabalho poderão pedir a emissão da senha em casos de mais de 10 minutos de inactividade.

II. Autorização
   - Baseada em permissões de acesso usando *Access Control Lists* para conexões a *Internet*.
   - Baseada em políticas de grupos para acesso local, usando grupos de utilizadores do AD.

III. Auditoria

Colecta de dados sobre o uso de recursos para relacionar as ocorrências no tempo e espaço.

Informações a serem colectadas:

- Todas as tentativas de autenticação e autorização
- Nome de *login*
- *Logouts*
- Mudanças de permissões

Os *logs* devem ser periodicamente analisados de modo a garantir o ajuste das políticas de segurança.

4.8.2.1 Escolha de soluções de segurança

A escolha de solução de segurança passa por identificar meios que permitam usar os mecanismos acima numa solução de segurança, havendo necessidade de definir mecanismos de segurança para diferentes tipos de acções:

- conexão com a *Internet*
- acesso sem fio
- serviços de rede
- serviços do utilizador

4.8.2.2 Segurança de conexão a Internet

Para alcançar uma maior segurança no acesso à *Internet* deve se proceder com a combinação dos seguintes mecanismos, descritos em capítulos anteriores:

- *Firewalls*
- *Proxy*
- Segurança física
- *Logs* de auditoria
- Autenticação
- Autorização

Refira-se que todos os serviços desnecessários serão desligados nas políticas de *firewall*.

A inclusão de um servidor *Proxy* permite controlar o acesso dos utentes ao exterior, criando um conjunto de *ACL's* que estabelecem a conduta de navegação pela *web*. Trata se de um sistema (*Squid*) que roda em plataformas *Unix*, apesar disso, este pode interagir com o AD permitindo autenticações baseadas nas contas de utilizador do AD.

4.8.2.3 Segurança de acesso sem fio

O processo de autenticação é provido pelo serviço *Remote Authentication Dial-In User Server* (*RADIUS Server*) integrado ao AD de modo a permitir a utilização de mesmas senhas em acessos as redes *Ethernet* e *Wireless.* Com a utilização do *RADIUS Server*, mantém se um banco de dados centralizado de utilizadores/senhas especificando o tipo de serviço permitido (*telnet, rlogin, http*).

4.8.2.4 Segurança de serviços de rede

- Para uma melhor segurança, é importante sempre desligar os serviços desnecessários, isto é, sem contributo no funcionamento da rede.
- Proteger o acesso físico e lógico a roteadores, *switches* e servidores com senhas disponibilizadas apenas ao pessoal de administração de rede.
- São definidos dois níveis de autorização, a saber:
    a. Visualização do estado dos dispositivos (primeiro nível), em que pode se visualizar o estado dos dispositivos e reportar ao pessoal com privilégios de alteração.
    b. Visualização e alteração de configuração (segundo nível), para além de visualizar o estado dos dispositivos e serviços pode efectuar algumas alterações conforme se justifique.

4.8.2.5 Segurança de serviços do utilizador

A segurança de serviços de utilizador irá depender da conduta deste e da cooperação da equipe de suporte que deve passar informações sobre critérios de escolha de chaves, e a necessidade de alteração das mesmas.

O utilizador deverá escolher uma senha que não tenha nenhuma combinação dos seus dados pessoais.

E por conveniência o administrador de rede deve habilitar o *logout* automático

4.8.2.6 Topologia de *firewall*

Conforme já foi referenciado no capítulo 2, um *firewall* é um sistema que estabelece um limite entre duas ou mais redes. Como forma de garantir a privacidade da rede corporativa, o uso de *Network Address Translation (NAT)* é necessário, sendo implementado no roteador com acesso a *Internet*; e o uso de um *proxy* para serviços (*web e ftp*).

Pensando no futuro, e na expansibilidade da rede é conveniente estabelecer uma zona desmilitarizada onde possam ser hospedados os servidores públicos. Com base nessas especificações apresenta se a seguinte arquitectura.

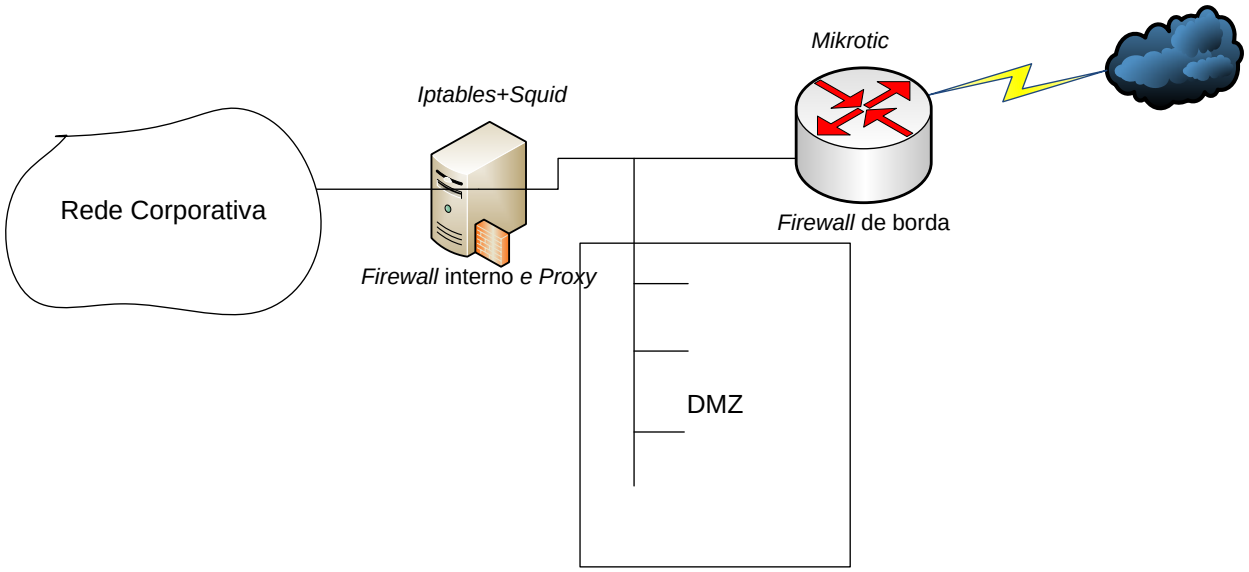


Diagrama 4-3 Topologia de Segurança

A figura acima apresenta a solução de segurança requerida para este projecto, donde pode se destacar a inclusão de uma máquina rodando um servidor *proxy* e ao mesmo tempo com *access control lists* baseados em pacotes definidos. Refira-se que esta máquina, define políticas de acesso ao exterior, enquanto o roteador, além de ser *gateway* padrão define políticas de acesso interno.

4.9 Projecto de gestão da rede

A gestão da rede constitui um aspecto operacional que deve ser levado em conta, pois a disponibilidade desta depende desse aspecto, sendo assim, são desenvolvidos mecanismos de gestão da rede da Faculdade atendendo às seguintes especificações.

4.9.1 Determinação dos requisitos de gestão

Nesta fase tem se como foco gerar uma lista priorizada dos serviços que deverão ser gerenciados, daí a necessidade de adoptar uma metodologia que congrega questões de projecto de rede no seu todo, pra tal fez-se um levantamento das

informações da rede corporativa basicamente a topologia da rede e os tipos de recursos utilizados, descrevem se a seguir algumas etapas desse item.

I. Obtenção das restrições

Foramreferenciadas junto à entidade proponente as seguintes restrições técnicas

1. Só o Administrador da tem direito de ver o que sucede na rede a dado momento;
2. O Administrador tem de ter a possibilidade de retirar um utilizador da rede;
3. O Administrador da rede tem de ter a possibilidade de visualizar o conteúdo acessado pelo o utilizador da rede a qualquer instante, porém destaca se algum grupo de utentes que suas acções na rede não devem ser monitoradas, a destacar, as entidades administrativas da Faculdade;
4. Deve se proceder à obtenção de relatórios de uso e desempenho da rede que deverão ser disponibilizados ao Administrador da rede e as entidades Administrativas da Faculdade;
5. Obtenção de relatórios referentes a tentativas de conexão a rede sejam sucedidas ou não;
6. Obter informações sobre o desempenho de cada segmento da rede;

II. Lista de serviços que devem ser geridos na rede

1. Utilização de segmento de rede;
2. E-mail;
3. Bases de dados;
4. Compartilhamento de arquivos;
5. Acesso e utilização das estações locais;
6. Utilização de serviços *Web*;

III. Determinação dos tipos de recursos da rede corporativa por gerir

Tabela 4-1 Estações de Trabalho

Estações de trabalho	
Designação	Descreve se também uma quantidade não contabilizada actualmente de estações de trabalho, uma tarefa que poderá ser efectuada com ajuda duma das funcionalidades da solução que se espera apresentar no decorrer desse trabalho, que é o inventário tanto de *hardware* quanto de *software*;

Tabela 4-2 Requisitos de gestão para componentes de rede

Requisitos de gestão para componentes de rede		
Servidores e estações de trabalho	Requisito de gestão	Área funcional
	Detecção de falta de conexão do servidor na rede	Falha
	Visualização e alteração da configuração de parâmetros de rede	Configuração
	Contabilização de tráfego de dados por recurso	Contabilização
	Bloqueio ou permissão de acesso proveniente de recursos externos	Segurança
	Detecção de falhas de *hardware* (disco, unidades de memória) e de *software* (término anormal de processo do sistema).	Falha
	Contabilização por utilizador ou grupo de utilizadores do número de transações referentes ao volume de dados transmitidos/recebidos	Contabilização
	Detecção de falhas de segurança, tentativas excessivas de *login* fora do conjunto de máquinas a si permitidas.	Segurança

	Configuração de temporização para secção inactiva	Segurança
	Inventário de *hardware* e *software*	Configuração
	Armazenamento de histórico de tempo resposta de aplicações *on-line*	Desempenho
	Bloquear um utilizador após um conjunto de tentativas de acesso fracassadas	Segurança
	Bloqueio de utilizador na tentativa de abrir secções simultâneas	Segurança
	Armazenamento de histórico de tentativas de acesso (sucedidas e fracassadas)	Segurança
Equipamentos de rede	Detecção de falhas do dispositivo baseando se em limiares como pacotes transmitidos/recebidos, colisões e erros.	Falha
	Controlo de acesso para alteração de parâmetros de configuração do dispositivo	Segurança
	Colecta de tráfego de dados para contabilização por recurso	Contabilização
	Armazenamento de histórico de indicadores de desempenho tais como pacotes transmitidos/recebidos, colisões e erros.	Desempenho
Segmento de rede	Detecção de falha no segmento baseando se em limiares como pacotes transmitidos/ recebidos	Falha
	Monitoração em tempo real e armazenamento de histórico de indicadores de desempenho tais como pacotes transmitidos/recebidos, colisões e erros.	Desempenho
	Colecta de tráfego de dados para contabilização por segmento e recurso nele existente	Contabilização

Tabela 4-3 Políticas de gestão

Políticas de Gestão		
Área de Gestão	Política	
Falhas	Tempo para a solução das ocorrências	Dependente da gravidade da ocorrência
	Ocorrências resolvidas no primeiro nível	Falhas de dispositivos de interconexão e serviços correndo nestes e nas máquinas servidoras
	Ocorrências resolvidas no segundo nível	Falhas de estações de trabalho locais
	Disponibilidade	Notificação em tempo real sobre disponibilidade de serviços e equipamentos
Desempenho	Utilização de CPU	Notificar sobre equipamentos com utilização de *CPU* durante mais de 5 minutos
	Utilização de memória	Notificar sobre equipamentos com utilização de memória durante mais de 5 minutos
	Utilização de segmento de rede	Notificar sobre utilização acima de 80% durante mais de 5 minutos
	Taxa de erros de segmento de rede	Notificar caso ocorram cinco erros de mesma espécie ou cinco erros consecutivos
	Taxa de entrada e saída para disco	Notificar caso a taxa de transferência de dados seja superior a
	Utilização de espaço em disco	Notificar se alguma unidade de armazenamento estiver abaixo de 5% de espaço livre

Configuração	Número de inconsistências	Notificar se o número de inconsistências atingir cinco ocorrências
	Número de consultas realizadas ao inventário	Notificar sobre todas as ocorrências de consulta ao sistema de gestão
	Avaliação dos utilizadores	Participação de utilizadores sob forma de repórter de ocorrências
Contabilização	Avaliação dos utilizadores	Estabelecimento de quotas de acesso à *Internet* por quantidade de download upload bem como por tempo de conexão
	Avalição do segmento de rede	Determinação de quantidade de download e upload por utilizador
Segurança	Critério de contingência	Bloquear e reportar situações de tentativas de acesso não autorizados aos diversos serviços
	Critério de acesso	Criação de utilizadores e grupos de utilizadores

4.9.2 Topologia lógica de acesso aos recursos de rede

Esta topologia tem como suporte o *AD DC* no qual especifica se a distribuição de recursos de rede e estruturação dos utentes em unidades organizacionais. Como se pode observar, existem quatro grupos de utilizadores distintos com níveis de acesso diferentes. Para cada utilizador é reservado um espaço fixo onde este possa executar as suas actividades, seja de qual for à estação de trabalho estiver conectado. Ainda é possível ver que para cada utilizador é atribuído um *print queue* que lhe permite enviar seus documentos à impressora de preferência, sendo este armazenado no servidor de impressoras até a autorização do operador de impressora, situação aplicável às impressoras designadas como públicas. Espaços comuns são criados para permitir a interacção entre estudantes e professores em matérias de material didáctico, sendo

delegada a cada professor a gestão desses espaços comuns podendo este visualizar, adicionar, alterar ou excluir informações.

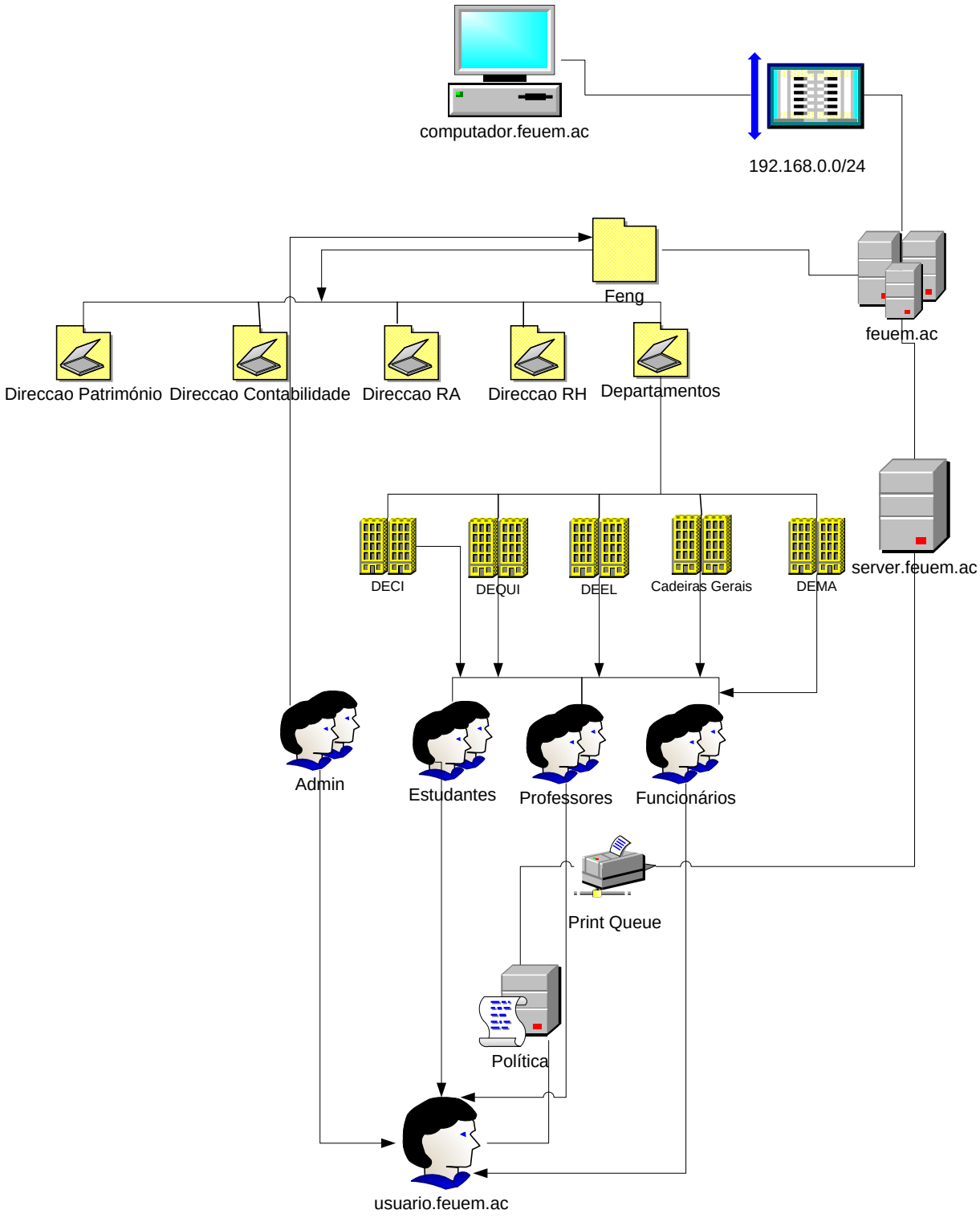
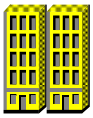
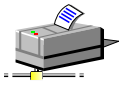


Diagrama 4-4 Recursos de *AD DS*

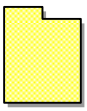
Legenda:


Site

Area de conectividade usada para localização de recursos de rede mais próximos


Print Queue

Buffer de documentos por imprimir


contentor

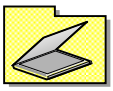
Contentor lógico de objectos


Estação de trabalho

Estação local de trabalho


Dominio local

Especificação do dominio local


Unidades organizacionais

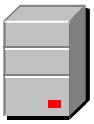
Agrupamento de sectores em unidades organizacionais/ Departamentos


Política

Política de acesso para utilizadores e estações de rede


utilizadores

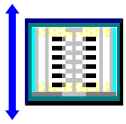
Utilizador


servidor

Servidor de dominio


Grupos de utilizadores

Grupos de utilizadores


IP subnet

Subdivisão da rede/ *IP subnet*

4.9.3 Topologia lógica da rede

O diagrama abaixo ilustra a topologia lógica da rede resultante de todo um estudo que vem sendo efectuado, onde são especificadas todas as interconexões necessárias para que a rede seja disponível e gerenciava, bem como locais de implantação de pontos de acesso para utilizadores sem fio.

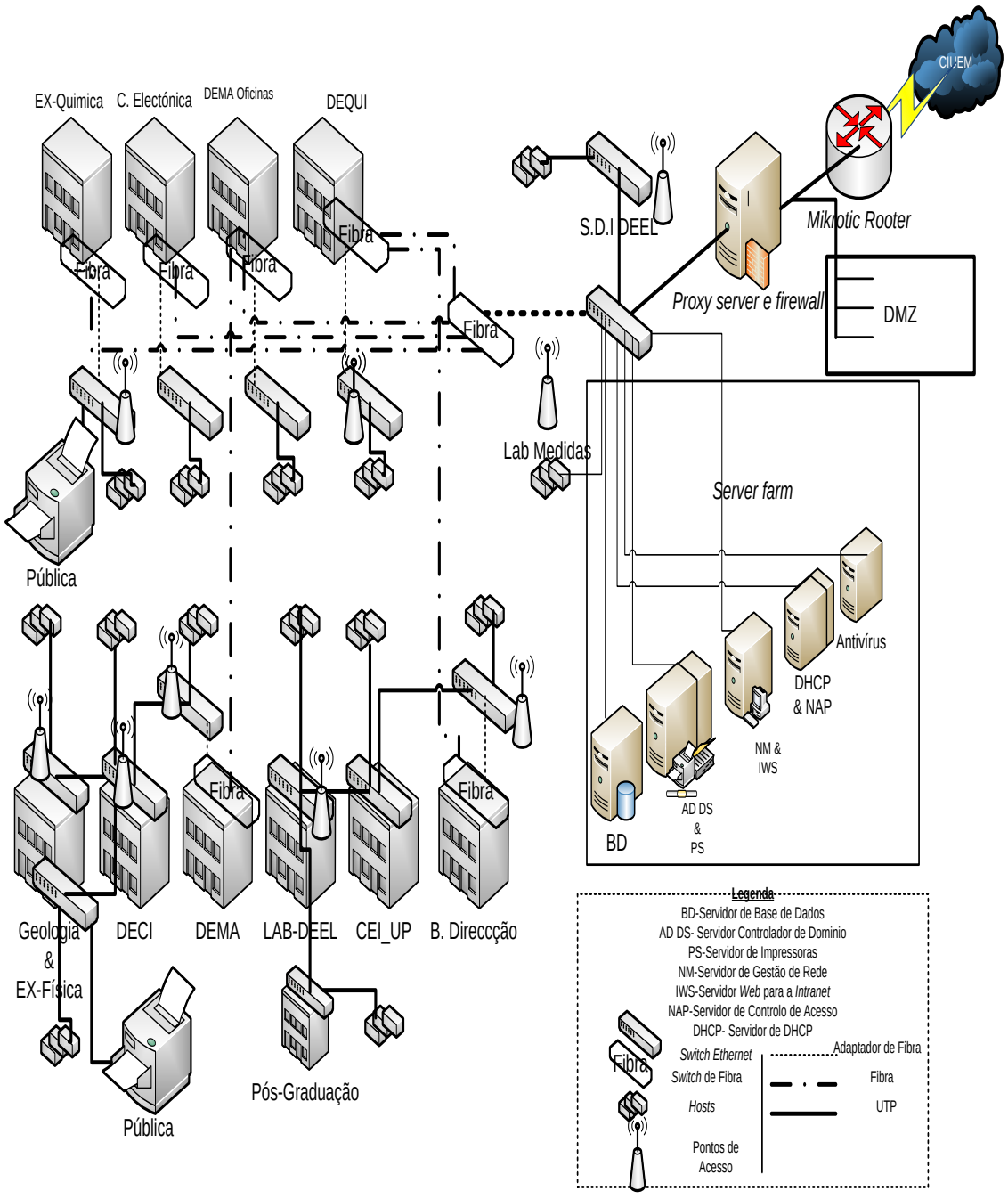


Diagrama 4-5 Topologia da rede

4.10 Projecto Físico

O projecto físico de uma rede de computadores envolve a selecção de cabeamento, a escolha de protocolos das camadas Física e de elance, bem como de dispositivos de interconexão.

4.10.1 Projecto de cabeamento para LAN

O planeamento de cabeamento tem que levar em consideração a necessidade deste ser usado durante mais tempo do que as tecnologias de rede propriamente ditas, sendo que para este caso, trata se de um projecto que deve se adaptar a uma tecnologia outrora existente. Dada a infraestrutura constituinte da rede de computadores da Faculdade de Engenharia, é conveniente estabelecer dois tipos de cabeamento nomeadamente:

4.10.2 Topologias de cabeamento

Para estabelecer uma arquitectura de cabeamento para um projecto de rede é conveniente saber que existem dois tipos de cabeamento:

Cabeamento centralizado- trata se de uma arquitectura onde todos os cabos são dirigidos a mesma área física;

Cabeamento distribuído- situação em que os cabos podem terminar em diferentes áreas físicas.

i. Cabeamento para prédios

O processo de cabeamento para prédios, levando em consideração a arquitectura por hora existente, trata se de uma arquitectura distribuída situação conveniente para aquilo que é a infraestrutura predial da Faculdade de Engenharia, pela existência de infra-estruturas longas, havendo pelo menos dois *racks* de distribuição em prédios com essas características. Esta particularidade permite encurtar as distâncias de conexão garantindo um maior desempenho da rede.

ii. Cabeamento entre prédios

Trata se de um aspecto sensível devido a existência de vários perigos físicos aliados a existência de outras redes tais como fluvial e eléctrica, para uma topologia altamente disponível e segura irá se proceder com uma arquitectura distribuída de modo a evitar a existência de um ponto único de falha. Como se pode observar pela

topologia da rede, encontram se diferentes locais desempenhando o papel de distribuição do sinal de um prédio para o outro usando uma linha de fibra óptica sendo que as linhas de cabo par trançado utilizadas actualmente servem de link redundante.

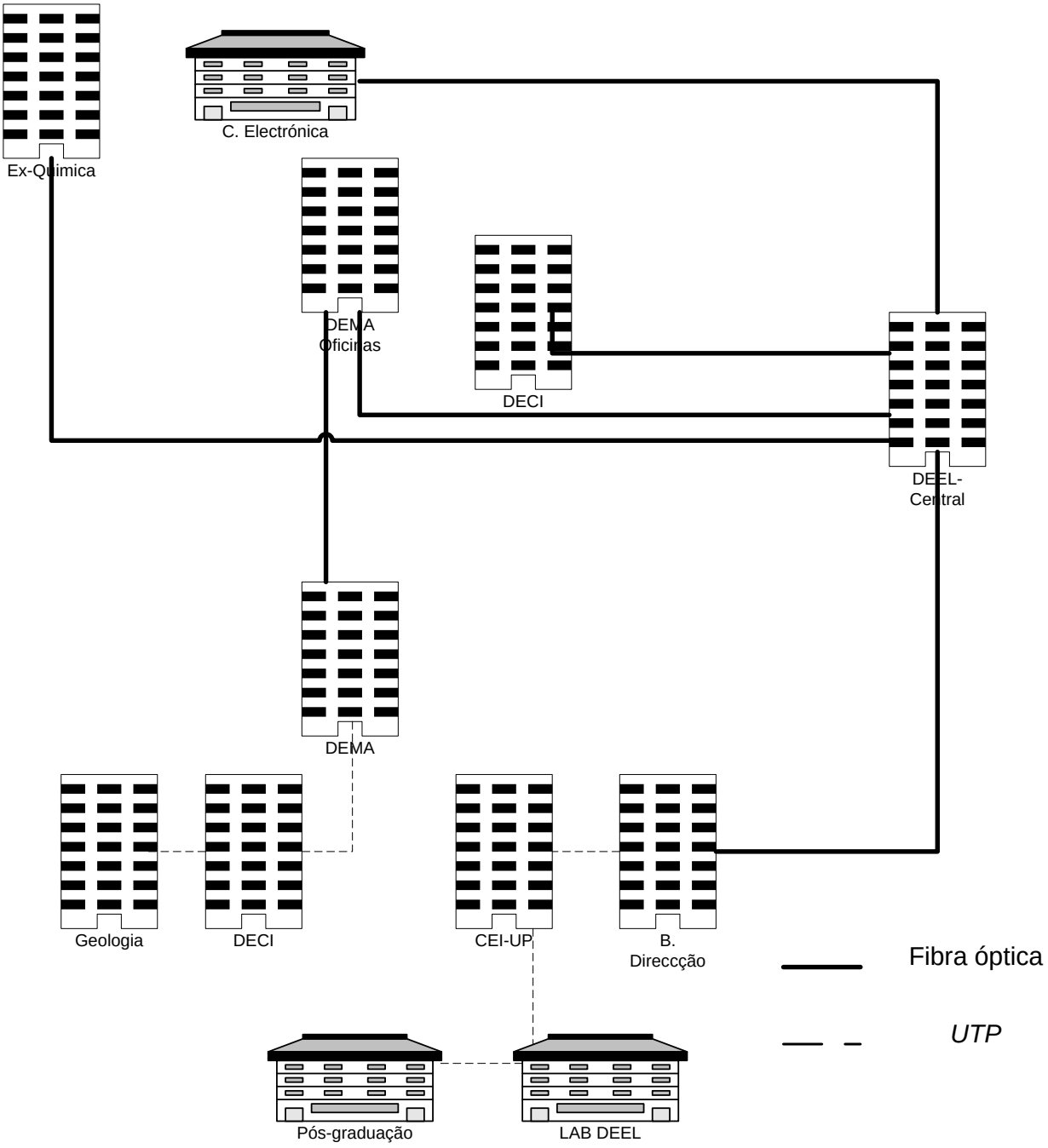


Diagrama 4-6 Topologia física

4.11 Análise económica

A disponibilidade orçamental, poderá influenciar de forma acentuada na efectivação do presente projecto, daí a razão da escolha de uma solução que não esteja aquém das restrições orçamentais outrora definidas. Para este facto, o orçamento necessário inclui despesas de:

Tabela 4-4 Recursos necessários

Aquisição de *hardware*- compra de 3 servidores	300.000 Meticais
Aquisição de *software*- aquisição de duas licenças *Windows Server* 2008 R2	40.000 Meticais
Recursos humanos- equipa de implementação do projecto	70.000 Meticais
Suporte e manutenção- período refente a 45 dias de assistência técnica à equipa local de gestão da rede	30.000 Meticais
Despesas suplementares- incluem a aquisição de 4 conectores de fibra óptica, 5 baterias de *access points,* marcadores de cabos e contingências.	20.000 Meticais
Total	**460.000 Meticais**

Retorno no investimento

Considerando as despesas apresentadas na Tabela 4-4, se em vez da aquisição dos itens especificados, o mesmo valor for submetido a um investimento financeiro durante 5 anos a uma taxa de 12%, o retorno será de 12% e considera-se portanto que o investimento seja de 515200 Meticais, sendo no entanto um retorno de 276000 Meticais passados 5 anos.

A depreciação do equipamento ao longo dos 5 anos deverá ser suprimida por uma amortização de 6000/mês, o equivalente a 4 anos e 5 meses. Nessas condições, considera se o projecto viável para a realidade da Faculdade de Engenharia.

5 Conclusões e recomendações

5.1 Conclusões

Durante a execução do presente projecto foi possível concluir que a gestão duma rede é uma tarefa indispensável para qualquer instituição que possui uma rede de computadores, nesse contexto, baseando se nos testes efectuados verificou-se que a implantação de um sistema de gestão baseado nas ferramentas *Nagios* (para monitoração de activos de rede) e *Squid* (para o controlo de acesso a Internet) resolve de forma satisfatória o problema actual, a partir do momento em que essas duas ferramentas juntas oferecem o suporte para gerir os diferentes serviços estabelecidos como requisitos de gestão.

Com a integração do *Nagios*, foi possível identificar e isolar falhas nas estações de trabalho configuradas na rede virtual de testes, permitiu o monitoramento do segmento de rede, e ainda a disponibilização de um serviço de alertas sobre o estado da rede.

Com a integração do *Squid*, tornou se possível o controlo de acesso à Internet, criação de quotas de consumo de largura de banda por grupos de utilizadores, e singulares criados no domínio da rede teste; possibilidade de geração de relatórios periódicos sobre o consumo de largura de banda. Tendo da mesma forma melhorado consideravelmente a velocidade de acesso a Internet para utilizadores da rede criada devido ao armazenamento interno de páginas *Web*.

A incorporação de um servidor *AD DS*, que oferece os serviços de controlador de domínio permitiu de maneira mais simples e eficaz a autenticidade dos utilizadores no acesso a rede de teste garantido da mesma forma que utilizadores tenham um ambiente individual de trabalho, com possibilidade de armazenar e trocar com outros utilizadores arquivos de seu interesse. Juntamente com este serviço foi possível a integração de um serviço de controlo de acesso à rede destinado às máquinas locais, serviço este que permite isolar máquinas com brechas de segurança das demais protegendo a rede de situações de infecção por vírus ou *spywares*.

A introdução de uma *DMZ* permite isolar os servidores internos dos servidores de disponibilidade pública, protegendo-os de acessos indevidos.

A partir da topologia da rede especificada, nota-se que a incorporação de pontos de acesso ao longo da rede aumenta a disponibilidade desta para os utilizadores móveis. De realçar que os objectivos do trabalho foram alcançados.

5.2 Recomendações

Recomenda se a Faculdade de Engenharia para implementação desta solução, pois traz consigo um conjunto de vantagens no que se refere aquilo que virá ser o processo de gestão desta rede;

É também recomendável que no futuro se faça uma segmentação da rede em domínios de *broadcast* menores;

Recomenda se também, a identificação de cabos de forma abrangente para facilitar a tarefa dos operadores de rede;

Da mesma forma, recomenda se a criação de VLAN's facto que requer a aquisição de *switches* com tal capacidade;

Por último recomenda se a Faculdade de Engenharia a incorporação de mais um provedor de serviços de Internet de modo a atenuar as constantes perdas de conexão que chegam a durar uma semana, dificultado as actividades da instituição nos diferentes aspectos.

6 Referências Bibliográficas

6.1 Bibliografia

1. **Kurose, James F. and Ross, Keith W.** *Redes de Computadores e a Inertnet.* São Paulo : Pearson Education, 2006.

2. **D. Harrington, R. Presuhn, B. Wijnen.** *An Architecture for Describing Simple Network Management Protocol.* s.l. : RFC 3411, 2002.

3. **J. Case, R Mundy.** *Internet standard Management Framework.* 2002. RFC 3410.

4. **M.Holdrege, P.Srisuresh.** *IP Network Address Translation (NAT) Terminology and Considerations.* 2008.

5. **Joseph Davies, Tony Northrup, Microsoft Network Team.** Windows Server 2008 Networking and Network Access Protetion. U.S.A : Interative Composition Corporation, 2008.

6. **Mahumane, Xavier.** *estrutura da rede.* Junho 14, 2013.

7. **Chiavenato, Idalberto.** *Introdução à Teoria da Administração.* São Paulo : Makron Books, 1997.

8. Projecto de Rede. *www.projectoderede.kit.net.* [Online] 2008. [Cited: 06 10, 2013.]

9. **GNU.** Licenses - GNU Project - Free Software Foundation (FSF). *GNU Project.* [Online] Setembro 20, 2011. [Cited: Setembro 29, 2011.] http://www.gnu.org/licenses/licenses.html.

10. **DEEL.** *REGULAMENTO DO PROJECTO DO CURSO.* Maputo, Maputo, Moçambique : s.n., Março 17, 2008.

11. **Pereira, Maria José Lara de Bretãs and Fonseca, Joao Gabriel Marques.** *Faces da Decisão: as mudanças de paradigmas e o poder da decisão.* São Paulo : Makron Books, 1997. p. 241.

12. **Magedanz, T.Saydam & T.** *Networks and Network.*

13. **Nemeth, Evi, et al., et al.** *Unix and Linux Systems Administration Handbook.* Boston : Pearson Education, 2010. 978-0-13-148005-6.

14. **Davies, Joseph and Northrup, Tony.** *Windows Server 2008 Networking and Network Access Protetion (NAP).* United States : Microsoft Press, 2008.

15. **Johnson, Staven.** *MCLTP Windows Server 2008 Enterprise Administrator.* Indiana City : Wiley Publishing, 2009. 978-0-470-029316-4.

16. **Corporation, Cisco.** *CCNA.* s.l. : Cisco, 2008.

17. **Haster, Matthew and Henley, Chris.** *Windows Server 2008 R2 Administration.* Indiana City : Whiley Pblushing, 2010. 978-0-470-52539-5.

6.2 Outra bibliografia consultada

18. http://www.nagios.org/documentation. [25-07-2013]

19. http://www.nagios.org/documentation. [15-07-2013]

20. http://www.zabbix.com/. [10-07-2013]

21. http://www.spiceworks.com/. [15-07-2013]

22. http://www.mikrotik.com/. [20-06-2013]

23. http://www.antamedia.com/bandwidth-manager/. [20-06-2013]

24. http://www.vivalinux.com.br/. [20-07.2013]

7 Anexos

Anexo 1 Distribuição de pontos

Tabela A1-7-1 Distribuição de pontos

Localização	**Identificação de Pontos**	**Total de Pontos**
BLOCO ADMINISTRATIVO		
DPM		
Secretaria	14	
Património	12	
Chefe de Manutenção	8	**6**
Chefe de Transportes	7	
Chefe do apoio geral	5	
Chefe do DPM	2	
DTI's	15, 17,18	**3**
UGEA	19, 20,21, 22, 23, 24, 25 e 26	
Laboratório de Estruturas	28, 29, 30	4
Registo Académico	31, 32, 33,34	**4**
Secretaria	40	**1**
Contabilidade	41,42, 43, 44, 46, 47	6
ADMINISTRAÇÃO		
Secretária do Director	62, 64	2
Director da Faculdade	48,50	**2**
Sala de Reuniões	51, 52, 53, 54, 55	5
Secretaria dos Directores Adjuntos	66, 68, 65	3
Administrador	56	**1**
Director Adjunto Pós-graduação	58	**1**
UP		

dra. Leandra	18, 19	**2**
Chefe da Contabilidade	01, 02, 05	**3**
Sala de Reuniões	15, 16	**2**
Sala de Desenho	12, 13, 14	**3**
Secretaria	10, 11	**2**
Gab. Director	05, 06, 08	**3**
Frio	20, 21	**2**
DEEL		
Secretaria	64	**1**
Lab. Control	01, 02, 03, 04, 05, 06	**6**
Gab.01	51	**1**
Gab.02	10	**1**
Gab.03	11	**1**
Gab.04	Sem identificação	**1**
Gab.05	12	**1**
Gab.06	13	**1**
Gab.07	14	**1**
Gab.08	16,17	**2**
Lab. Digital	18,20,21,22,23	**5**
Lab. Telecomunicações	24, 25, 26, 27, 29	**5**
Gab.18	56	**1**
Gab.16	54	**1**
Gab.15	Sem pontos	
Chefe do Departamento	62	**1**
Gab.29	3	**1**
Gab.28	Sem pontos	
Lab. Máquinas Eléctricas	13	**1**
Lab. Medidas Eléctricas	12,13,20	**3**
Gab.02	14,15	**2**
Gab.03	16,17	**2**

Gab.04	18,19	**2**
Gab.06	11	**1**
Gab.07	3	**1**
Lab. Alta tensão	06,08	**2**
Oficinas de Electricidade	05,01	**2**
Sala de Informática	30,31,32,34,35,36,37,38,39, 40,41,42,43,44,45,46,47,48,49,50	**20**
DEQUI		
Secretaria	56	**1**
Eng. Isabel	39	**1**
dr. Cumbane	38	**1**
Eng. Bequisa	37	**1**
Dr. Luís Pelembe	36	**1**
Dr. Cruz	34	**1**
Eng. Hélder	35	**1**
Lab. Dona Victória	2	**1**
Eng. Boris	04,06	**2**
Dr. Vasco da gama	8	**1**
Salão de Assistente	6	**1**
Gab.111	01,03	**2**
Dr. Carlos Lucas	09,18	**2**
Eng. Condo	62	**1**
HPLC	Sem identificação	**2**
Chefe DEQUI	58,59	**2**
Lab. Gina	48	**1**
Dra. Adélia	25,26,27	**3**
Estufas	Sem identificação	**2**
Ambiente Livre	20,22,08,07	**4**
Dra. Serafina	10	**1**
Lab. Operações Unitárias	29,30	**2**

Eng. Maida Khan	32,33,34	**3**
Sala de informática	11,12,14,15,16,17,18,19,20,21,22,23	**17**
	26,27,28,29,30	
Sala dos professores	01,04 (+6 pontos ligados ao *swicth* do Gab. do Dr. Carlos Lucas)	**8**
	02,03	**2**
DEMA		
Secretaria	57	**4**
Lab. Mecânica Aplicada	60	**2**
Eng. Lacita	08,09	**2**
Chefe DEMA	22	**2**
Lab. Lola	2	**2**
Eng. Viandro	Sem numeração	**3**
Dr. Nhambiu	14,15	**3**
Dr. Nhumaio	20	**3**
Eng. Job Tai	17,18	**2**
Eng. Mocomoque	66,67	**3**
Eng. Rachide	64	**3**
Gab.106	22	**1**
Gab.107	62	**2**
Ferramentaria	68	**3**
Sala de Informática (HCB)	01,02,03,04,05,06,24,25,26,27,28,29	**20**
	30,31,32,33,34,35,36	
Sala de Informática (UBUNTO)	01,02,03,04,05,06,07,08,09,10,11,	**20**
	12,13,14,15,16,17,18,19,20	
Eng. Amílcar	Sem pontos	
Eng. Mulima		
Dr. Sitoe		
DECI		
Secretaria	03,04,06,07	**4**

102	33,34,35	**3**
105	11,12	**2**
106	08,09,10	**3**
109	2	**2**
112	36	**2**
113	38,39,40	**3**
114	42	**2**
115	44,45,46,48	**5**
116	49	**3**
Sr. Niquisse	12	**2**
Lab. Hidráulica Sanitária	Sem identificação	**1**
Lab. Aguas Residuais	Sem pontos	
Sala de Informática	13,14,15,16,17,18,19,20,21,22, 23,24,25,26,27,28,29,30,31,32	**20**
GEOLOGIA		
Secretaria	01,02,04	**5**
Biblioteca	8	**1**
Dr. Amadeu	09,10	**2**
Sr. Felisberto	16,17	**2**
Geofísica	11,12,13	**3**
Dr. Salvador Mondlane	18,19	**2**
Dr. Helone	14,15	**2**
Dr. Amoran		
Dr. Nguenha		
Lab.Sedimentalogia	28,29	**2**
Cozinha	Sem identificação	**1**
LPA	01,02	**2**
Dr. Elidio	Sem identificação	**1**
Chefe Geologia	Sem identificação	**1**
Dra. Sandra	7	**1**

Sala de Maquinas	4	**1**
Lab. Hidro Carbonetos	Sem pontos	
Sala de Reuniões	Sem identificação	**1**
Dr. Farisse	17	**2**
Dra. Micaela	Sem pontos	
Dr. Belarmino		
Sala de Informática	01,02,03,04,05,06,07,08,09,10,11,	**14**
	12,13,14	
Registo Académico	15	**2**
Sr.Onófre	17,18	**2**
Dr.Lopo	20,21	**2**
Dr. Siquila	22	**1**
Dr . Ibraimo	30	**1**
Dr. Jamal	29	**1**
Dra. Zita	28	**1**
Dr. Estevão Sumburane	27	**1**
Dra . Laura	26	**1**
NEEA	Sem pontos	
Dr. Mugabe	4	**1**
CADEIRAS GERAIS		
Secretaria	06,46,47	**4**
Chefe DAF	48	**2**
UGEA	14,16	**4**
Biblioteca (1^0 Piso)	24,25	**3**
Biblioteca (R/C)	20	**3**
Sala de Estudante em Grupo	Sem identificação	**3**
Dona Natalia	23	**1**
Eng. Paulo Conselho	2	**1**
Pós-graduação	03,04,05,06,07,08,09,10,11,12,13,14,15,	**16**
	16,17,18	

Sr. Arcanjo	Sem pontos	
SALA DE AULA		
DEMA		
101	58	**1**
103	52	**1**
104	51	**1**
105	50	**1**
203	44	**1**
Sala de Reuniões	Sem pontos	
DEQUI		
114	11,12	**2**
Ex. Física	Sem identificação	**1**
201	9	**1**
202	10	**1**
GEOLOGIA		
Sala-2	Sem identificação	**1**
Sala-3	12	**1**
Anfiteatro	21	**1**
G1	31	**1**
G2	32	**1**
CADEIRAS GERAIS		
109	Sem pontos	
118	Sem pontos	
119		
123	Sem identificação	**1**
124	3	**1**
Anfiteatro (202)	Sem pontos	
104		
TOTAL	**43**	**480**

Observações:

- Durante a ronda de levantamento de pontos de **dados** na Faculdade de Engenharia, constatou-se que na maior parte dos sectores, há problemas de identificação de pontos *(*não tem identificadores, que diferenciam os pontos de dados e de voz*),* de referir que existem no momento 377 pontos de dados operacionais, nove salas sem pontos de acesso à rede e doze salas com pontos não identificados;
- Em alguns pontos com identificadores, constatou-se ainda que estes (pontos) são usados incorrectamente, isto é, no lugar de **dados** usa-se para **voz** e *vice-versa*.

1. Departamento de Engenharia Electrotécnica (DEEL)
    a. Os gabinetes n^{o} 06 e 07, possuem mesma numeração de pontos (13), sendo que no Gab. n^{o} 06, o ponto 13 indica **dados** e no Gab. n^{o} 07, indica **voz**;
2. Departamento de Engenharia Mecânica (DEMA)
    a. Os gabinetes do Eng. Mocomoque e do Eng. Rachide, possuem mesma numeração de pontos (65), sendo que nos dois gabinetes indica **voz**;
    b. Os gabinetes do Eng. Amílcar, Eng. Mulima e dr. Sitoe, possuem pontos *"improvisados"*, isto é, não tem calha;
3. Departamento de Geologia
    a. Todos sectores do R/C ligados ao armário localizado no gabinete do chefe do departamento, não tem acesso à Internet;

Sugestões:

- Identificação correcta de pontos com auxílio de etiquetas;
- Definição correcta de usabilidade dos pontos (pontos de **dado** devem funcionar simplesmente para dados e os de **voz** também para voz e eliminar-se o uso opcional);

Correcção na duplicação de números de pontos nos gabinetes mencionados;

Anexo 2 Resultados de testes

Neste capítulo são ilustradas imagens de relatórios de ferramentas que fazem parte da solução.

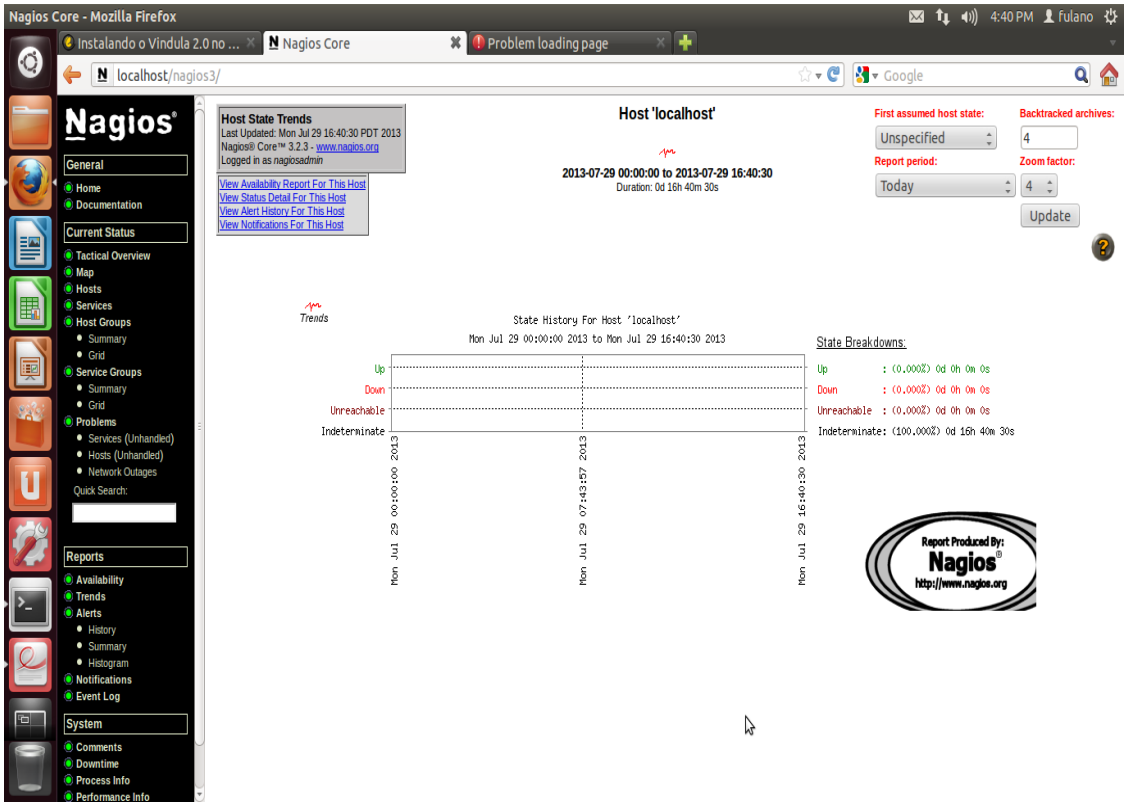


Figura A2-1 Resultado de monitoramento

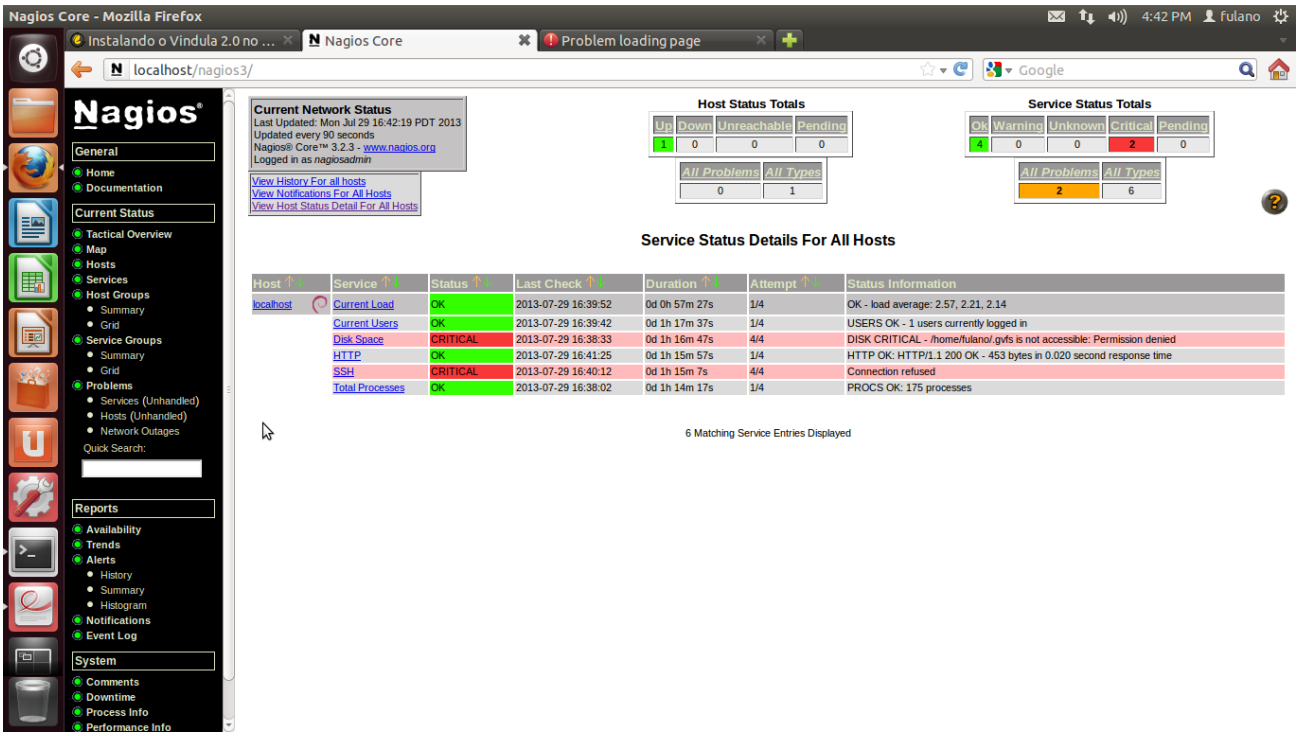


Figura A2-2 Estado de serviços

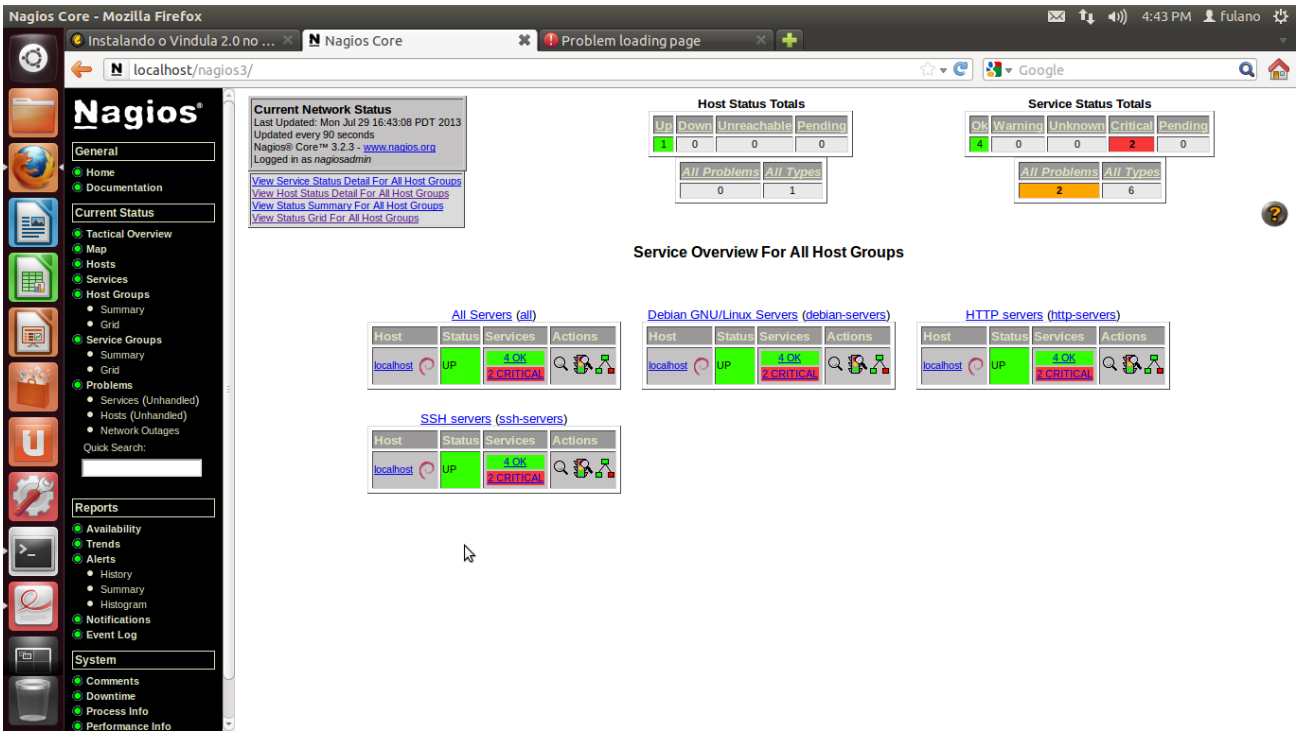


Figura A2-3 Estado de serviços em categoria

Configuração de *iptables*

```
#!/bin/sh -e/
    #

        ####definição de variáveis
    iptables -t filter -P INPUT DROP
    iptables -t filter -A INPUT -j ACCEPT -i lo
        iptables -t filter -A OUTPUT -j ACCEPT -o lo
        iptables -t filter -P OUTPUT ACCEPT
    iptables -t filter -P FORWARD DROP
    # Tabela nat
    iptables -t nat -P PREROUTING ACCEPT
    iptables -t nat -P OUTPUT ACCEPT
    iptables -t nat -P POSTROUTING DROP
    # Tabela mangle
    iptables -t mangle -P PREROUTING ACCEPT
    iptables -t mangle -P OUTPUT ACCEPT




    ##### Ativ se o redirecionamento de pacotes (requerido para NAT) #####
    echo "1" >/proc/sys/net/ipv4/ip_forward

    echo "2048" > /proc/sys/net/ipv4/ip_conntrack_max


    ###################################################################
    #                  Tabela filter                  #
    ###################################################################
```

```
iptables -N ppp-input

iptables -A INPUT -i lo -j ACCEPT
iptables -A INPUT -s 192.168.6.0/24 -i eth0 -j ACCEPT


# Qualquer outra conexão desconhecida é imediatamente registrada e derrubada
iptables -A INPUT -j LOG --log-prefix "FIREWALL: INPUT "
iptables -A INPUT -j DROP


iptables -A FORWARD -d 192.168.6.0/24 -i ppp  -o eth0 -j ACCEPT
iptables -A FORWARD -s 192.168.6.0/24 -i eth0 -o ppp  -j ACCEPT
iptables -A FORWARD -j LOG --log-prefix "FIREWALL: FORWARD "
iptables -A FORWARD -j DROP

iptables -A ppp-input -p icmp -m limit --limit 2/s -j ACCEPT

iptables -A ppp-input -p tcp --dport 80 -j ACCEPT

iptables -A ppp-input -p tcp --dport 21 -j LOG --log-prefix "FIREWALL: ftp "
iptables -A ppp-input -p tcp --dport 25 -j LOG --log-prefix "FIREWALL: smtp "
iptables -A ppp-input -p udp --dport 53 -j LOG --log-prefix "FIREWALL: dns "
iptables -A ppp-input -p tcp --dport 110 -j LOG --log-prefix "FIREWALL: pop3 "
iptables -A ppp-input -p tcp --dport 113 -j LOG --log-prefix "FIREWALL: identd "
iptables -A ppp-input -p udp --dport 111 -j LOG --log-prefix "FIREWALL: rpc"
iptables -A ppp-input -p tcp --dport 111 -j LOG --log-prefix "FIREWALL: rpc"
iptables -A ppp-input -p tcp --dport 137:139 -j LOG --log-prefix "FIREWALL: samba "
iptables -A ppp-input -p udp --dport 137:139 -j LOG --log-prefix "FIREWALL: samba "
```

```
iptables -A ppp-input -m state --state ! ESTABLISHED,RELATED -j LOG --log-prefix "FIREWALL: ppp-in "
iptables -A ppp-input -m state --state ! ESTABLISHED,RELATED -j DROP
# Qualquer outro tipo de tráfego é aceito
iptables -A ppp-input -j ACCEPT


############################################################
#                Tabela nat                #
############################################################

##### Chain POSTROUTING #####
# Permite qualquer conexão vinda com destino a lo e rede local para eth0
iptables -t nat -A POSTROUTING -o lo -j ACCEPT
iptables -t nat -A POSTROUTING -s 192.168.6.0/24 -o eth0 -j ACCEPT

iptables -t nat -A POSTROUTING -s 192.168.6.0/24 -o ppp  -j MASQUERADE
```