Universidade Federal de Itajubá
UNIFEI

Proposta de reestruturação da rede UNIFEI utilizando os atuais paradigmas da comunicação de dados

CAIO MARCUS DIAS FLAUSINO

Itajubá 2004

Universidade Federal de Itajubá
UNIFEI

CAIO MARCUS DIAS FLAUSINO

Proposta de reestruturação da rede UNIFEI utilizando os atuais paradigmas da comunicação de dados

Dissertação apresentada à Universidade Federal de Itajubá para obtenção do título de Mestre em Engenharia Elétrica.

Área de Concentração:
Automação e Sistemas Elétricos Industriais
Orientador: Prof. Dr. Germano Lambert Torres
Co-orientador: Prof. Dr. Luiz Eduardo Borges da Silva

Itajubá 2004

Dedico este trabalho a Deus e aos meus pais pelo amor, carinho e dedicação presentes em cada um dos seus atos e conselhos.

Agradecimentos

Agradeço a todos que de alguma forma contribuíram para o desenvolvimento deste trabalho, em especial:

Ao meu querido mestre Maurílio Coutinho que me ajudou em um dos momentos mais difíceis da minha vida.

Aos meus amigos Roberto S. Netto e Cezar José Sant'Anna Jr.

Ainda aos meus orientadores Germano Lambert Torres e Luis Eduardo Borges da Silva.

Também aos administradores da rede da universidade, que colaboraram na elaboração deste trabalho.

Agradecimentos especiais à minha esposa, meus queridos filhos, meus irmãos e principalmente aos meus pais pelo amor e carinho.

Por fim, quero agradecer a todos os professores e funcionários da Universidade Federal de Itajubá e espero que todos nós possamos continuar a engrandecer ainda mais nossa universidade.

Resumo

Nesta proposta, as primeiras tarefas realizadas foram o levantamento e análise das necessidades dos usuários e da universidade e, em seguida, a caracterização do tráfego da rede atual. Após a realização destas tarefas foi possível propor algumas mudanças na rede, a fim de melhorar seu desempenho, gerenciamento e a segurança dos dados que nela trafegam.

Portanto, foi realizada uma análise detalhada dos aplicativos e do tráfego gerado pelos usuários antes de começar a projetar as mudanças na rede, definir as tecnologias e os equipamentos a serem utilizados. Através da realização destas tarefas pode-se constatar que o planejamento de um projeto vem antes da sua implementação.

Um dos objetivos desta dissertação é mostrar que a centralização dos recursos técnicos e humanos é uma boa opção para a universidade, podendo assim, melhorar os serviços disponibilizados aos seus usuários como, por exemplo, suporte técnico e acesso à Internet.

Esta proposta sugere a centralização dos servidores corporativos em uma única sala, chamada *Server Farm*. Neste local também serão colocados todos os equipamentos que irão auxiliar os administradores da rede a gerenciar e monitorar a rede com melhor eficiência.

Este trabalho fornece um plano de ação para melhorar o desempenho do acesso à Internet e também incentivar a troca de informações na rede interna da universidade. Este plano propõe o uso de equipamentos que irão fornecer condições de não só gerenciar ativamente a rede, como também evitar problemas com a segurança dos dados como, por exemplo, vírus ou a utilização dos recursos da rede por usuários não autorizados ou mal intencionados.

Na conclusão são citados os testes de desempenho, que devem ser realizados na rede após a implementação das soluções apresentadas neste trabalho. São citados também, diversos assuntos para futuros estudos na área de gerenciamento e segurança da informação da rede UNIFEI.

Abstract

In this proposal the firsts tasks made were the survey and the analysis of the users and university's requirements, and following the traffic and existing network characteristics. After that it was possible to propose some changes in the network in order to improve its performance, management and the security for the data flowing along the network.

Therefore, it was made a detailed analysis of the programs and traffic generated by users, before planning the changes in the network, defining the technologies and the equipments to be used. Through making these tasks we realize that the project planning comes before its implementation.

One of the objectives of this dissertation is to show that the centralization of the technical and human resources is a good option for the university, providing an improvement on the services made available for the users, for example, the technical support and the access to the Internet.

This proposal suggests the centralization of the corporative servers in a sole room, called *Server Farm*. In this place also will be located all the equipments that will help the network administrators in managing and monitoring the network with better efficiency.

This work supplies an action plan to improve the performance in accessing the Internet and also to incentive the information exchange in the university private network. The plan suggest the use of equipments that will provide the conditions for the active management of the network as well as to prevent problems regarding the security of the data, for instance, viruses or the use of the network resources by non-authorized users or with bad intensions.

In the conclusion are mentioned the performance tests that should be made in the network after, the completion of the suggested solutions in this paper. Many subjects for future studies also are listed, with respect to management and information security in the university's network.

Lista de Abreviaturas e Siglas

ACLs - Access Control Lists
ASP - Assessoria de Planejamento
BIM - Biblioteca Mauá
COR - Centro de Operações de Redes
CPD - Centro de Processamento de Dados
CSMA/CD - Carrier Sense Multiple Access / Collision Detection
DET - Departamento de Eletrotécnica
DHCP - Dynamic Host Configuration Protocol
DNS - Domain Name System
DON - Departamento de Eletrônica
DRA - Departamento de Registro Acadêmico
FAPESP –Fundação de Amparo à Pesquisa do Estado de São Paulo
FDDI - Fiber Distributed Data Interface
FTP - File Transfer Protocol
HIDS - Host-based Intrusion Detection System
HTML - Hypertext markup language
ICI - Instituto de Ciências
IDS - Intrusion Detection System
IEE - Instituto de Engenharia Elétrica
IEM - Instituto de Engenharia Mecânica
IP - Internet Protocol
ISO - International Organization for Standardization
LAN - Local Area Network
LASER - Light Amplification by Stimulated Emission of Radiation
LHPCH - Laboratório Hidromecânico para Pequenas Centrais Hidrelétricas PDG -
LED - Light Emission Diode
MAC - Media Access Control
MAN - Metropolitan Area Network
NAT - Network Address Translator
MRTG - Multi Router Traffic Grapher

NIDS - Network-based Intrusion Detection System

OSI - Open system Interconnection

PPG - Pró-Diretoria de Pós-Graduação

Pró-Diretoria de Graduação

QoS - Quality of Service

RFC – Request for Comments

RNP - Rede Nacional de Pesquisa 2

ScTP - Screened Twisted Pair

STP - Shielded Twisted Pair

TCP/IP - Transmission Control Protocol / Internet Protocol

UNIFEI - Universidade Federal de Itajubá

UTP - Unshielded Twisted Pair

VOIP - Voice Over IP

WAN - Wide Area Network

Web Browser - Programa de navegação na Internet

WLAN - Wireless Local Area Network

Sumário

Lista de Figuras

Lista de Tabelas

1 INTRODUÇÃO

1.1 Considerações Iniciais [1]

Este trabalho foi motivado pela situação alarmante em que se encontra a rede da universidade. Um dos sérios problemas que acontece frequentemente por toda rede da universidade é a infecção por vírus e *worms*. Outro problema sério é a lentidão e o mal uso do acesso à Internet, que é agravado pela alta incidência de vírus na rede e também pela utilização de programas *peer to peer* (P2P). Para desenvolver uma possível solução para estes problemas utilizou-se a metodologia de projeto de redes em camadas.

O desenvolvimento de projetos de redes é um processo de elaboração focado nos aplicativos que rodam em uma rede, nas metas da organização, nas restrições técnicas e nas especificações requisitadas. Esta proposta dá uma visão lógica da rede, mostrando detalhadamente o fluxo de dados, antes de desenvolver uma visão física da rede.

A idéia principal deste trabalho não é somente elaborar uma proposta de reestruturação da rede da universidade, mas também mostrar que o planejamento de um projeto vem antes da sua implantação, enfatizando que deve haver uma preocupação em se realizar uma análise dos aplicativos e do tráfego gerado, antes de começar a projetar a rede.

Esta proposta utiliza o método de desenvolvimento em camadas, que se baseia no modelo de referência OSI. Este método é iniciado pelas camadas superiores, destacando os aplicativos e o transporte dos dados antes de especificar os dispositivos de rede a serem usados, que operam nas camadas inferiores do modelo OSI.

De acordo com Oppenheimer [1], a primeira etapa de um projeto de redes em camadas é a identificação dos requisitos dos usuários. Esta etapa é complementada com o levantamento e análise dos requisitos técnicos da rede e da universidade.

A próxima etapa é a caracterização da rede atual, sua estrutura física e o seu desempenho. Em seguida, deve-se realizar uma análise do tráfego da rede para levantar as necessidades de largura de banda da rede interna e verificar a ocupação do *link* de acesso à Internet.

A terceira etapa do desenvolvimento de um projeto envolve a elaboração de uma topologia lógica da rede, um modelo de endereçamento lógico e também uma proposta de um projeto de segurança e de gerenciamento.

A próxima etapa compreende a elaboração de uma topologia física da rede, a escolha do tipo de cabeamento a ser implantado, a seleção do tipo de tecnologia de rede local e os equipamentos de rede a serem utilizados.

A quinta etapa inclui um plano básico de testes para a criação de uma linha de base para comparar freqüentemente o desempenho da rede, um estudo para otimização dos requisitos técnicos da rede como, por exemplo, disponibilidade, escalonabilidade e também a definição de alguns assuntos, que auxiliam a elaboração de uma documentação completa da rede de uma determinada instituição ou empresa.

1.2 Objetivos

Esta proposta foi desenvolvida com o auxílio de alguns conceitos importantes de gerenciamento de rede e segurança da informação. Com estes recursos, os administradores poderão melhorar o desempenho da rede e também o suporte aos usuários.

O objetivo principal deste trabalho é sugerir uma proposta de reestruturação da rede UNIFEI, que vise atender às expectativas dos usuários e da universidade. A idéia é apresentar uma solução que aproveite, ao máximo, os recursos de rede já existentes na universidade e promover a centralização dos recursos técnicos e humanos da área de administração e suporte da rede.

Atualmente a universidade possui uma rede descentralizada, com diversos servidores espalhados pelo campus e com alguns serviços sendo fornecidos por mais de um servidor, deixando claro o desperdício dos recursos de informática e de técnicos responsáveis pelo suporte e administração destes equipamentos.

1.3 Estrutura da dissertação

Esta dissertação está organizada em oito capítulos. O primeiro, capítulo atual, apresenta algumas considerações iniciais, os objetivos da dissertação e sua estrutura.

O segundo capítulo descreve toda a fundamentação teórica necessária para esta dissertação como, por exemplo, o modelo de referência OSI e a funcionalidade de suas camadas, os meios de rede existentes, as tecnologias de cada camada, os dispositivos de redes mais conhecidos, noções de política de segurança da informação, ferramentas para caracterização do tráfego de informações na rede, entre outros conceitos.

O terceiro capítulo mostra os métodos existentes para o levantamento dos requisitos e das necessidades dos usuários da rede e da universidade, bem como o método utilizado para a realização desta tarefa. O método utilizado para levantar as informações é baseado em entrevistas e questionários com grupos-chave de usuários da rede. Um dos pontos levantados na pesquisa envolve algumas considerações sobre a qualidade e o desempenho dos recursos de rede existentes na universidade.

No quarto capítulo, é apresentada uma análise geral das metas e restrições dos usuários e da universidade. Nesta análise é possível observar os requisitos principais dos usuários e suas necessidades em relação à utilização dos recursos de rede. Outros pontos observados neste capítulo se referem às metas e restrições

técnicas da rede UNIFEI como disponibilidade, gerenciabilidade, desempenho e a mudança física da administração da rede.

O quinto capítulo mostra o levantamento e a análise das características da rede atual da universidade. Estas informações levantadas e analisadas se referem a diversos assuntos, tais como, topologia da rede, dispositivos de rede, servidores de rede entre outros. Por fim, é realizada a caracterização do tráfego da rede para levantar as necessidades de largura de banda da rede interna e verificar a taxa de ocupação dos *links* de acesso à Internet.

O sexto capítulo apresenta a topologia lógica da rede, um modelo de endereçamento lógico e uma proposta para um projeto de gerenciamento da rede e segurança da informação.

O sétimo capítulo define a elaboração de um projeto de rede física. Este projeto envolve a elaboração de uma topologia física da rede, escolha do tipo de cabeamento, a seleção da tecnologia de rede local e os equipamentos de rede a serem utilizados.

No capítulo oito, são apresentadas as conclusões e as proposições dos trabalhos futuros, que permitirão complementar esta proposta com novas pesquisas. Um dos pontos citados neste capítulo propõe a elaboração de um plano de testes para monitorar o desempenho da rede. Outro ponto levantado se refere à elaboração da documentação da rede UNIFEI.

2 FUNDAMENTAÇÃO TEÓRICA

2.1 Redes de comunicação de dados

As redes de comunicação de dados surgiram com a evolução dos computadores, a necessidade de se evitar a duplicação de equipamentos, aumentar a eficiência dos aplicativos desenvolvidos e a economia de recursos financeiros.

Segundo Tanenbaum [2], o termo rede de computadores pode ser especificado como um conjunto de computadores autônomos, interconectados, capazes de trocar informações. Esta interconexão pode ser feita através de fios de cobre, *laser*s, microondas, satélites e também por fibras ópticas.

Uma rede de computadores é formada por um conjunto de *hosts*, sejam eles computadores, impressoras ou quaisquer outros dispositivos, capazes de trocarem dados e compartilhar recursos, interligados por um sistema de comunicação, conforme mostra a figura 1.

Segundo Soares [3], um sistema de comunicação de dados é formado por um arranjo topológico interligando os vários *hosts* através dos enlaces físicos e de um conjunto de regras e normas, chamado protocolo, com o intuito de estabelecer a comunicação.

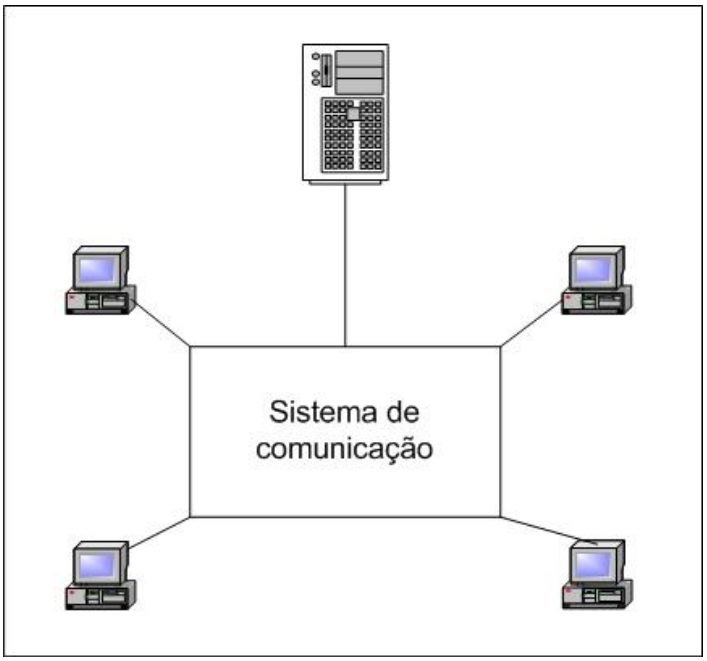

Figura 1 – Topologia de uma rede de computadores.

Segundo Chiozzotto [4], as redes de computadores ou *hosts* podem ser classificadas baseadas em seus alcances e se dividem em:

- **Redes locais ou *LANs***

  As redes enquadradas nesta classificação são formadas por *hosts* conectados entre si em um escritório, em um edifício ou ainda em um campus de uma universidade, de forma a respeitar o limite de alguns kilômetros.

- **Redes metropolitanas ou *MANs***

  São aquelas que possuem um alcance médio, por exemplo, espalhadas por uma cidade de médio ou grande porte.

- **Redes geograficamente distribuídas ou *WANs***

  São aquelas que abrangem cidades, estados e até países, por exemplo, a maior delas é a Internet.

De acordo com Tanenbaum [2], algumas das vantagens e características da interconexão de computadores por um sistema de comunicação são:

- **Compartilhamento de recursos**

  Faz com que todos os programas, dados e equipamentos da rede estejam disponíveis a todos os usuários independentemente de sua localização física.

- **Economia**

  A substituição gradativa dos antigos *mainframes* para as redes de computadores de pequeno porte significou uma redução muito grande nos custos de manutenção dos sistemas de informação, possibilitando uma verdadeira revolução nos CPDs.

- **Prover um elo de comunicação**

  As redes de computadores são um poderoso meio de comunicação entre indivíduos, possibilitando inclusive o trabalho em conjunto, mesmo estando separados geograficamente ou em locais distintos.

2.2 Modelo de referência OSI

Com o aumento na quantidade e no tamanho, as redes foram criadas com diferentes implementações de *hardware* e *software*. Conseqüentemente, muitas redes tornaram-se incompatíveis, e a comunicação entre elas ficou difícil e complicada.

Na tentativa de solucionar este problema, a ISO realizou uma pesquisa sobre os vários esquemas de rede existentes e percebeu a necessidade da criação de um modelo com o objetivo de ajudar os desenvolvedores a implementar redes que pudessem ser compatíveis entre si. Assim, a ISO lançou em 1984 o modelo de referência OSI [5].

Este modelo ofereceu aos fabricantes um conjunto de padrões que garantiram maior compatibilidade e interoperabilidade entre os diversos tipos de tecnologias de rede, criados por várias empresas de todo o mundo.

O modelo de referência OSI é dividido em sete camadas e cada uma delas possui uma função particular na rede, contendo suas especificações e os seus

protocolos de comunicação. Um protocolo é um conjunto de regras ou um acordo, que determina o formato e a transmissão de dados em uma comunicação. As sete camadas do modelo OSI são [5-7]:

- **Camada 7 - camada de aplicação**

  É a camada mais próxima do usuário. Ela difere das outras camadas, pois não fornece serviço para outra camada do modelo OSI e sim para aplicativos. Alguns exemplos destes aplicativos são: *web browsers*, processadores de texto, planilhas eletrônicas e programas de correio eletrônico.

- **Camada 6 - camada de apresentação**

  Esta camada assegura que a informação enviada pela camada de aplicação de um sistema de origem seja legível no sistema de destino. Se for necessário, a camada de apresentação faz a conversão entre diversos formatos de dados para um formato comum, ou seja, ela é responsável por apresentar os dados de uma forma que o dispositivo de destino possa entender as informações enviadas.

  Outra função desta camada é a estruturação dos dados que são usados pelos aplicativos, onde se pode incluir a compactação e a criptografia destes dados.

- **Camada 5 - camada de sessão**

  Ela estabelece, gerencia e termina sessões entre aplicativos de dois *hosts*. A camada de sessão é responsável por prover serviços à camada de apresentação. Ela sincroniza e controla o diálogo entre as camadas de apresentação dos dois *hosts*, e também gerencia a troca de dados entre eles.

- **Camada 4 - camada de transporte**

  Esta camada é responsável pelo transporte de informações, da origem para o destino, de forma confiável e precisa.

Para fornecer o serviço de transporte de dados de forma confiável, a camada de transporte estabelece, mantém e termina circuitos virtuais. Ela também utiliza os recursos de controle do fluxo de informações e a detecção e recuperação de erros no transporte dos dados.

Enquanto as camadas de aplicação, de apresentação e de sessão estão relacionadas a problemas de aplicativos, as quatro camadas inferiores estão relacionadas a problemas no transporte de dados, ou seja, como os dados são transmitidos entre a origem e o destino.

- **Camada 3 - camada de rede**

Esta camada fornece conectividade e seleção de caminhos entre dois sistemas que podem estar localizados em redes geograficamente separadas.

O esquema de endereçamento lógico é usado pelos dispositivos que trabalham nesta camada para determinar o destino dos dados à medida que eles se movem pelas redes. Nesta camada não existe nenhum mecanismo para verificar se os dados chegaram bem ao destino. Ela apenas procura entregar os dados da maneira mais eficiente possível.

Os protocolos que suportam a camada de rede utilizam um esquema de endereçamento hierárquico, permitindo que endereços exclusivos atravessem os limites das redes, tendo juntamente com isso, um método para encontrar um caminho para o dado trafegar entre as redes. Um exemplo de endereço de camada 3 é o *IP - Internet Protocol.*

- **Camada 2 - camada de enlace de dados**

Esta camada fornece acesso aos meios de rede e à transmissão física através dos meios, o que permite que os dados localizem seus destinos pretendidos em uma rede. Além disso, essa camada cuida da notificação de erros, da topologia da rede, da entrega ordenada de quadros e do controle de acesso ao meio.

O controle de acesso ao meio, fornecido por esta camada, utiliza o endereço de hardware ou também chamado de endereço MAC. Este

endereço, que está localizado na placa de rede, é usado para definir como os *hosts* compartilham o mesmo meio e se identificam de forma exclusiva.

O endereçamento MAC é composto por uma numeração única de 48 *bits*, onde os primeiros 24 *bits* são usados para identificar o fabricante e os outros 24 *bits* identificam o número seqüencial da placa de rede de um equipamento. Um exemplo de tecnologia de rede que utiliza estes conceitos é a *Ethernet*, que será explicada mais adiante.

- **Camada 1 - camada física**

Esta camada define as características elétricas, mecânicas, funcionais e os procedimentos para iniciar, manter e terminar as conexões físicas destinadas à transmissão de bits entre os sistemas de origem e destino.

As características elétricas especificam os valores dos sinais elétricos como, por exemplo, níveis de tensão e corrente, que representam os dígitos binários. Ela define também, as taxas de transmissão e as distâncias máximas que os sinais podem alcançar.

As especificações mecânicas definem o tamanho e a forma dos conectores, pinos, tomadas, painel de conexões, cabos, etc.

As características funcionais determinam o significado dos sinais transmitidos nas interfaces do meio físico.

Os procedimentos para iniciar, manter e terminar as conexões físicas definem sequências e combinações de sinais, que devem ocorrer para que um dispositivo desta camada desempenhe a sua função de transmitir e receber bits.

Soares em [3], ressalta que o modelo OSI, por si só, não define a arquitetura de uma rede. Isso acontece porque ele não especifica com exatidão os serviços e protocolos de cada camada. O modelo OSI simplesmente “diz o que cada camada deve fazer ou implementar”.

A divisão da comunicação de dados em camadas oferece diversas vantagens, entre elas podem-se citar [8, 9]:

- Divide a comunicação de dados em partes menores para tornar mais simples o entendimento.
- Padroniza os componentes de rede, para permitir o desenvolvimento e o suporte, por parte dos vários fabricantes existentes.
- Viabiliza a comunicação entre tipos diferentes de *hardware* e de *software* de rede, independente do fabricante.
- Evita que as modificações em uma camada afetem as outras camadas, permitindo assim uma maior rapidez no seu desenvolvimento.
- Decompõe, em partes menores, a comunicação de dados em uma rede, facilitando sua aprendizagem e compreensão.

2.3 Modelo TCP/IP

Apesar do modelo de referência OSI ser reconhecido universalmente, o padrão técnico aberto e histórico da Internet é o TCP/IP [6].

A pilha de protocolos TCP/IP possibilita a comunicação de dados entre dois computadores localizados em qualquer parte do mundo.

O modelo TCP/IP possui quatro camadas: camada de aplicação, de transporte, de Internet e a camada de interface de rede. É muito importante perceber que algumas camadas do modelo TCP/IP possuem o mesmo nome das camadas no modelo OSI, portanto deve-se ficar atento para não confundir as camadas dos dois modelos. A figura 2 mostra uma comparação entre as camadas destes dois modelos.

A camada de aplicação do modelo TCP/IP é comparável às camadas de aplicação, de apresentação e de sessão do modelo OSI. As camadas de transporte de ambos são comparáveis. Já a camada de rede do OSI é comparável à camada de Internet do TCP/IP.

O modelo TCP/IP combina os aspectos da camada física e de enlace do modelo OSI em uma camada, chamada de camada de acesso à rede ou camada de interface de rede [6, 7].

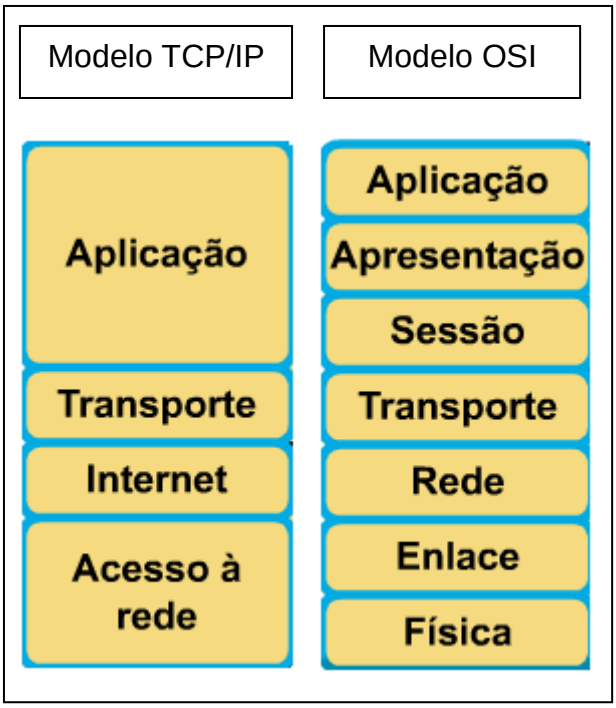

Figura 2 – Comparação entre o modelo OSI e o TCP/IP.

2.4 Topologia de rede

Topologia de uma rede de computadores define a estrutura de uma rede, ou seja, ela descreve a maneira como os seus componentes se conectam entre si.

O conceito da topologia de rede pode ser dividido em dois aspectos [5]:

- **Topologia física**: representa como os computadores ou *hosts* estão conectados fisicamente, mostrando o *layout* real do fio ou do meio de rede.
- **Topologia lógica**: define como os meios são acessados pelos computadores, mostrando como o fluxo de informação ocorre entre os *hosts*.

2.4.1 Topologia física

A figura 3 mostra os esquemas de topologias físicas mais comuns. As topologias físicas mais comumente usadas são [4, 9]:

- **Topologia de barramento**: utiliza um segmento comum de rede onde os *hosts* se conectam.
- **Topologia em anel**: conecta todos os dispositivos diretamente uns aos outros, ou seja, conecta um *host* ao próximo e o último *host* ao primeiro.
- **Topologia em estrela**: conecta todos os cabos ao ponto central de concentração.
- **Topologia em estrela estendida:** possui uma topologia em estrela central, em que cada um dos nós finais da topologia central atua como centro de sua própria topologia em estrela.
- **Topologia hierárquica:** criada de forma similar a uma estrela estendida, mas com algumas diferenças, pois os *hosts* possuem níveis hierárquicos de conexões entre si.
- **Topologia em malha:** também chamada de topologia ponto a ponto. Cada *host* tem suas próprias conexões com todos os outros *hosts*.

  Esta topologia é usada em redes onde não pode haver nenhuma interrupção nas comunicações, por exemplo, os sistemas de controle de uma usina nuclear.

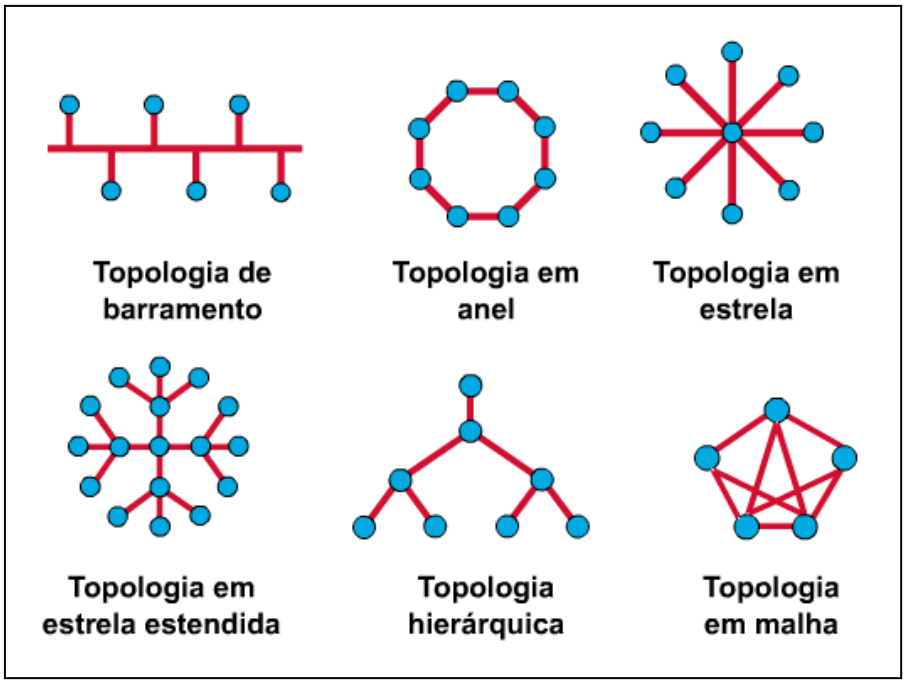

Figura 3 – Topologias de rede.

2.4.2 Topologia lógica

As topologias lógicas mais comuns são de broadcast e passagem de *token* [8, 9].

- ***Broadcast***

  Neste tipo de topologia cada *host* envia seus dados a todos os outros *hosts* no meio da rede. As estações não seguem nenhuma ordem para usar a rede, a primeira a solicitar é a atendida.

  As tecnologias que utilizam este tipo de topologia são chamadas de não determinísticas, ou seja, não tem como descobrir quem acessará o meio em um determinado tempo.

- **Passagem de *token* ou *token passing***

  Ela controla o acesso à rede, passando um *token* eletrônico seqüencialmente para cada host conectado a rede. Ao receber o *token*, um *host* pode enviar dados para um *host* destino. As tecnologias que utilizam este tipo de topologia são chamadas de determinísticas, ou seja, existe um modo de descobrir quem acessará o meio em um determinado tempo.

2.5 Cabeamento de rede

O cabeamento de rede é o meio pelo qual a informação dos usuários flui entre origem e destino. A função básica dos meios é carregar o fluxo de informações. Há basicamente dois tipos de cabeamento, o de *backbone* também chamado de vertical ou primário e o cabeamento horizontal ou secundário.

O cabeamento vertical ou de *backbone* é utilizado para conectar dois ou mais dispositivos de rede, instalados em armários de telecomunicações distintos.

Os meios de rede mais comuns existentes são: cabo par trançado, fibra óptica e o ar [10, 11].

2.5.1 Cabo par trançado

O cabo UTP é utilizado para interligar dois dispositivos a uma distância máxima de 100 metros. Ele é usado como cabeamento horizontal na rede, possibilitando a interligação de um ou mais *hosts* a um equipamento ou dispositivo de rede. Entre as categorias existentes de cabeamento par trançado, três se destacam pelas suas características [1]:

- Categoria 5 testada a 100MHz e dá suporte à tecnologia *Fast Ethernet.*
- Categoria 5e testada a 100MHz e dá suporte à tecnologia *Fast Ethernet*, mas com uma maior exigência nos padrões de testes em relação à categoria 5.
- Categoria 6 testada a 250MHz, que fornece melhores condições de uso para a tecnologia *Gigabit Ethernet* em relação à categoria 5e.

O cabo par trançado se divide basicamente em dois modelos, o par trançado não blindado e o blindado.

O cabo par trançado não blindado, também chamado de UTP, possui 4 pares de fios. Cada um dos oito fios de cobre do cabo UTP é coberto por um material isolante. Além disso, cada fio é torcido, ou melhor, trançado em volta de outro fio, dando um par de fios trançados, conforme mostra a figura 4.

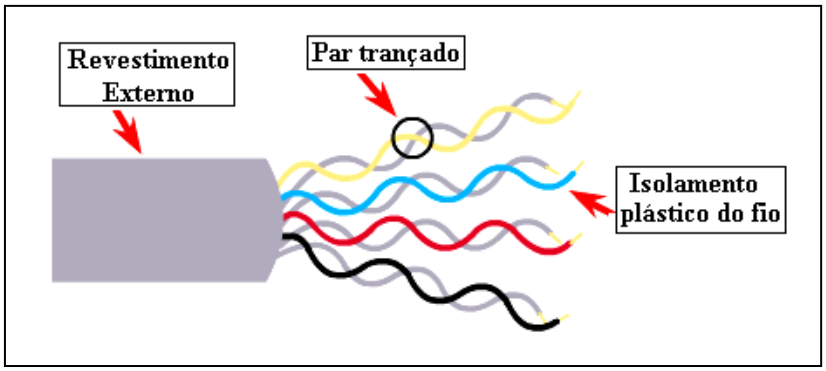

Figura 4 – Exemplo de um cabo par trançado não blindado.

Uma das vantagens do cabo UTP é a facilidade de instalação. Outra importante vantagem deste cabo é o custo, pois ele é mais barato do que qualquer outro tipo de meio de rede.

Em relação às suas desvantagens, pode-se citar que ele é mais propenso a ruído e a interferência eletromagnética do que outros tipos de meios de rede. Outra desvantagem do cabo UTP está na distância entre a origem e o destino dos sinais, que é menor no cabo UTP do que na fibra óptica, por exemplo.

O segundo modelo de cabo par trançado é o blindado. O cabo par traçado blindado, também chamado de STP, possui dois tipos de cabos blindados. O primeiro tipo é o STP, onde cada par de fios é envolvido por uma lâmina metálica. Em seguida, os pares de fios são totalmente envolvidos por outra lâmina metálica, conforme ilustrado na figura 5.

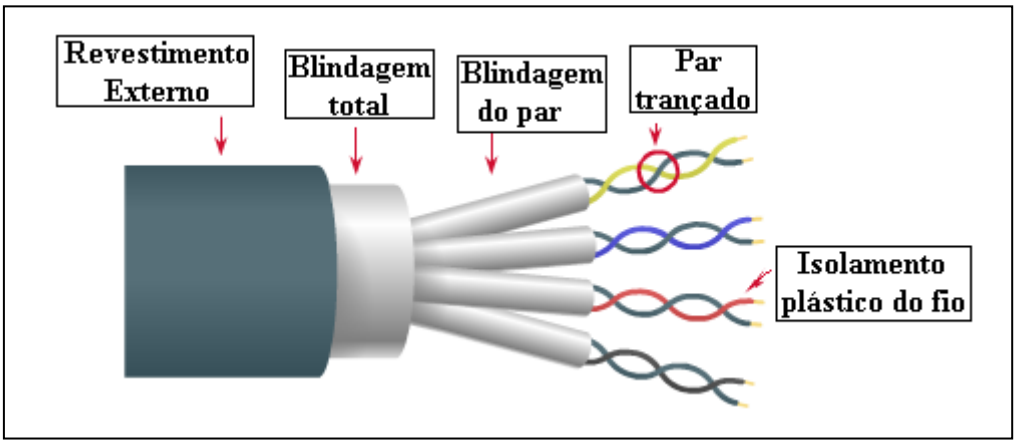

Figura 5 – Exemplo de um cabo blindado STP.

Uma das vantagens do cabo STP em relação ao UTP é diminuição do ruído elétrico, tanto dentro do cabo como fora dele (interferência eletromagnética e

interferência de freqüência de rádio). Entretanto o cabo STP é mais caro e mais difícil de conectorizar e instalar do que o UTP.

O segundo tipo de cabo blindado é o ScTP, que é basicamente o UTP envolvido por uma malha de metal, conforme a figura 6.

Outro ponto importante sobre o cabo blindado é a necessidade de a blindagem metálica estar aterrada nas duas extremidades. Se não estiver aterrada apropriadamente ou se existir uma descontinuidade na extensão do material da blindagem, o cabo torna-se suscetível a problemas de ruído, pois a blindagem atuará como uma antena, captando sinais indesejados.

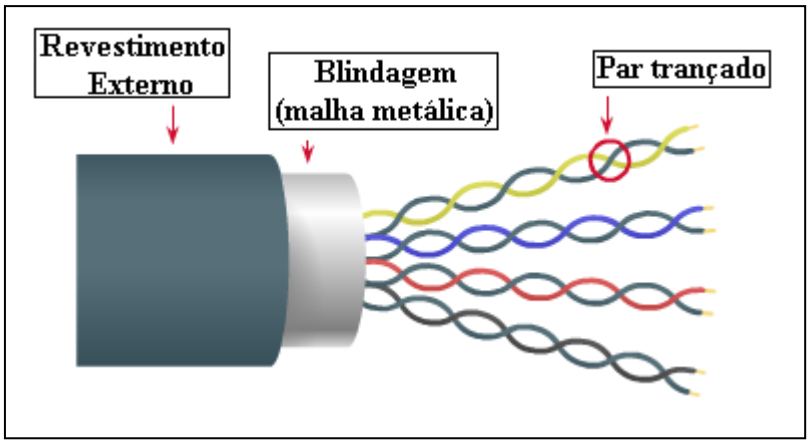

Figura 6 – Exemplo de um cabo ScTP.

2.5.2 Fibra óptica

O cabo de fibra óptica utilizado em redes de comunicação possui duas fibras, uma para transmissão e a outra para recepção dos dados, conforme mostra a figura 7. A fibra óptica é um meio de transmissão que transporta a luz, convertendo os bits em feixes de luz. Há basicamente dois tipos de fibras, a monomodo e a multimodo.

A fibra óptica é comumente utilizada como cabeamento vertical, possibilitando a interligação dos armários de telecomunicações dentro de um edifício e também é muito utilizada para a interligação de edifícios.

A fibra monomodo possui seu feixe de luz gerado por um *LASER* e na fibra multimodo o feixe é gerado por um *LED*.

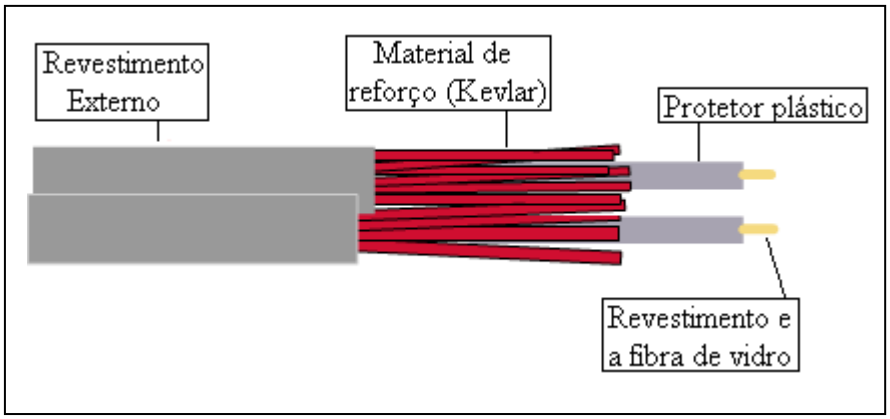

Figura 7 – Fibra óptica

Segundo Ribeiro [11], as maiores vantagens de se utilizar a fibra óptica na comunicação de dados em relação ao cabo par trançado são:

- Pequena atenuação.
- Maior capacidade de transmissão de dados, ou seja, maior largura de banda em relação aos outros meios de transmissão.
- Grande redução nas dimensões e no peso dos cabos.
- Imunidade às interferências eletromagnéticas.

Apesar de as vantagens da fibra óptica superarem suas desvantagens, alguns pontos negativos devem ser considerados a fim de possibilitar uma melhor orientação sobre sua aplicação, por exemplo:

- Dificuldade na emenda e conectorização.
- Custo ainda elevado para sistemas de pequenas larguras de faixa.

2.5.3 Ar

A comunicação sem-fio utiliza o ar como meio de transmissão de dados. Os sinais são ondas eletromagnéticas, que fazem deste tipo de meio uma forma muito flexível de se criar uma rede de comunicação. Uma aplicação muito utilizada na comunicação de dados sem-fio é a WLAN ou rede local sem fio, desenvolvida de acordo com os padrões IEEE 802.11. As vantagens que a WLAN oferece são [5, 9]:

- **Mobilidade dos usuários**

  Os usuários podem acessar arquivos, recursos de rede, e a Internet sem ter que conectar fisicamente à rede cabeada. Eles podem ter mobilidade e ainda possuir um *link* de acesso com alta velocidade.

- **Rapidez na instalação**

  O tempo requerido para instalação de um ponto é muito menor, pois não há a necessidade de passar cabos por paredes ou tetos nem de instalar tomadas de rede.

- **Flexibilidade**

  A flexibilidade é outra vantagem muito atraente para as empresas, pois elas podem montar um escritório provisório com maior rapidez, não se preocupando com os cabos e conectorizações de rede e depois desmontá-lo sem maiores problemas com a rede local.

Porém, as redes locais *wireless* possuem suas desvantagens, que limitam sua utilização. Uma delas é o fato de que os dados estão no ar, logo outras pessoas podem ter acesso facilmente a estas informações. Outra desvantagem da comunicação sem fio é a perda de sinal ou atenuação quando o mesmo atravessa paredes, montanhas ou outros obstáculos.

2.6 Tecnologia de enlace de dados

As tecnologias de redes locais mais conhecidas atualmente são: *Ethernet* / IEEE 802.3, *Token Ring* e FDDI. A *Ethernet* (IEEE 802.3) é a tecnologia de rede local mais utilizada atualmente. Esta tecnologia é responsável por aproximadamente 85% dos *hosts* conectados em rede. As vantagens que possibilitam a tecnologia *Ethernet* / IEEE 802.3 ser a mais utilizada são [12-14]:

- Simples de entender, implementar, administrar e manter.
- Permite implementações de rede baratas.

- Fornece flexibilidade na instalação de redes.
- Assegura uma boa interconexão e operação sem se preocupar com o fabricante dos equipamentos.

Existe uma pequena diferença entre a tecnologia *Ethernet* e a IEEE 802.3, que se concentra no formato dos quadros ou estruturas de camada 2. Esta diferença deve ser levada em consideração quando for realizada a configuração dos equipamentos de rede *Ethernet* ou IEEE 802.3.

A arquitetura da rede *Ethernet* tem suas origens nos anos 60, na Universidade do Havaí, onde o método de acesso ao meio foi desenvolvido. Este método é chamado de CSMA/CD.

A rede *Ethernet* foi originada nos anos 70, no *Palo Alto Research Center – PARC* da Xerox Corporation, que desenvolveu o primeiro sistema *Ethernet* experimental.

Este sistema foi usado como base para a especificação IEEE 802.3, criada em 1980. Logo após a concepção desta especificação a Digital, Intel e Xerox formaram um consórcio responsável pelo desenvolvimento e lançamento da *Ethernet* versão 2, criada em 1983. Este padrão é substancialmente compatível com a IEEE 802.3 [13, 15].

Atualmente, o termo *Ethernet* é muito utilizado para se referir a toda rede local baseada em detecção de portadora para múltiplo acesso com detecção de Colisão ou CSMA/CD, que normalmente está em conformidade com as especificações IEEE 802.3.

Um *host* conectado em uma rede local, que utiliza o método de acesso CSMA/CD, pode acessar a rede a qualquer momento. Mas, antes de enviar os dados, o *host* deve verificar ou “escutar” se a rede está em uso, se estiver, ele terá que aguardar para transmitir os dados.

Um problema preocupante deste método é a colisão. Ela ocorre quando duas ou mais estações “escutam” o tráfego da rede, não “ouvem” nada e transmitem simultaneamente. Neste caso, ambas transmissões são danificadas, e os *hosts* devem retransmitir novamente os dados. Quando isto ocorrer, serão utilizados os algoritmos de *backoff*, que irão ajudar na retransmissão dos dados.

Segundo Odom em [8], a tecnologia *Ethernet* é uma rede de *broadcast*. Portanto, todos os *hosts* podem ver e verificar todos os quadros ou pacotes de dados, independentemente de serem ou não o destinatário desses dados. Cada *host* analisa os quadros recebidos para determinar se ele é o destino. Se for, o quadro é enviado para a camada acima, que neste caso é a camada 3 do modelo OSI.

O modo de transmissão é uma característica importante da tecnologia *Ethernet* e pode ser [5]:

- *Half-duplex*: cada estação transmite ou recebe informações, não acontecendo transmissões simultâneas.
- *Full-duplex*: cada estação transmite e/ou recebe, podendo ocorrer transmissões simultâneas.

O Controle de Acesso ao Meio (*MAC*) refere-se ao protocolo que determina qual computador em um ambiente de meio compartilhado tem permissão para transmitir dados. Portanto, o padrão *Ethernet* foi inicialmente concebido como uma tecnologia *half-duplex* e largura de banda de 10Mbps.

Atualmente o processamento em uma rede *Ethernet* tradicional está muito comprometido, pois os usuários estão utilizando cada vez mais aplicativos cliente-servidor, que fazem os *hosts* transmitirem mais freqüentemente e por períodos mais longos. Uma solução para este tipo de problema é a *Ethernet* comutada. Esta tecnologia melhora a largura de banda, isola o tráfego por usuário e segmenta a rede.

Com a segmentação de uma rede há uma diminuição do domínio de colisão, que é o conjunto de *hosts* ligados a um mesmo segmento de rede. Os dispositivos que podem fazer esta segmentação na rede são os *switches* e os roteadores.

A *Ethernet full-duplex* exige o uso de conexões com comutação entre cada nó, ou seja, ponto a ponto. Esta tecnologia pode usar o meio compartilhado existente, desde que o meio atenda aos padrões *Ethernet* mínimos.

Atualmente existem mais de 18 variedades distintas da família *Ethernet*. Os padrões mais conhecidos utilizam três taxas de transmissão de dados e são definidos para operarem em cima de fibra óptica ou cabo par trançado [12]:

- 10 Mbps - *Ethernet* (10BASE –T e 10BASE-FL).
- 100 Mbps - *Fast Ethernet* (100BASE-TX e 100BASE-FX).
- 1000 Mbps - *Gigabit Ethernet* (1000BASE-T, 1000BASE-TX, 1000BASE-LX e 1000BASE-SX).

Os padrões 10BASE-T, 100BASE-TX, 1000BASE-T e 1000BASE-TX operam em cima de cabo par trançado. Já os padrões 10BASE-FL, 100BASE-FX, 1000BASE-LX e 1000BASE-SX operam em cima de fibra óptica.

2.6.1 Redes locais virtuais

Uma LAN virtual (VLAN) é um agrupamento lógico de *hosts* ou usuários que podem ser agrupados por função, departamento ou aplicativo, independentemente da localização física desses grupos, ou seja, a transferência de dados ocorre sem as restrições físicas impostas sobre uma rede local. Uma VLAN cria um único domínio de broadcast que não está limitado ao segmento físico e, por conseguinte essa VLAN é tratada como uma sub-rede.

Os administradores de rede podem agrupar os *hosts* a uma determinada *VLAN*, de maneira que eles possam se comunicar como se estivessem conectados ao mesmo segmento ou fio, quando na realidade eles podem estar situados em segmentos físicos distintos. As VLANs se baseiam em conexões lógicas ao invés de físicas logo, são muito maleáveis. As VLANs possuem algumas características muito interessantes [5, 9]:

- Elas operam na camada 2 e 3 do modelo OSI.
- A comunicação entre as VLANs é fornecida pelo roteamento da camada 3. Esta particularidade tem um uso muito importante, pois estes agrupamentos lógicos de usuários não se comunicam entre si.

  Para que isto ocorra é necessário utilizar um dispositivo de camada 3, por exemplo, um roteador. Este equipamento faz o roteamento do tráfego entre as VLANs.
- VLANs proporcionam o controle de *broadcast* na rede. Esta característica é muito útil, pois nesta proposta os usuários estão separados por classe.

- O administrador da rede é que atribui os usuários a uma VLAN.
- Podem aumentar a segurança da rede definindo quais nós da rede podem se comunicar com os outros. Esta característica é muito importante para esta proposta de reestruturação da rede, pois ela permite, por exemplo, que sejam separados os *hosts* dos alunos, professores e dos funcionários administrativos da universidade.

A figura 8 mostra um exemplo de VLAN, onde existem duas comunicações entre usuários fisicamente separados, mas pertencentes à mesma VLAN. Este exemplo é composto de três blocos, sendo que cada *host* está conectado a uma VLAN existente. A comunicação entre as VLANs é realizada por intermédio do roteador.

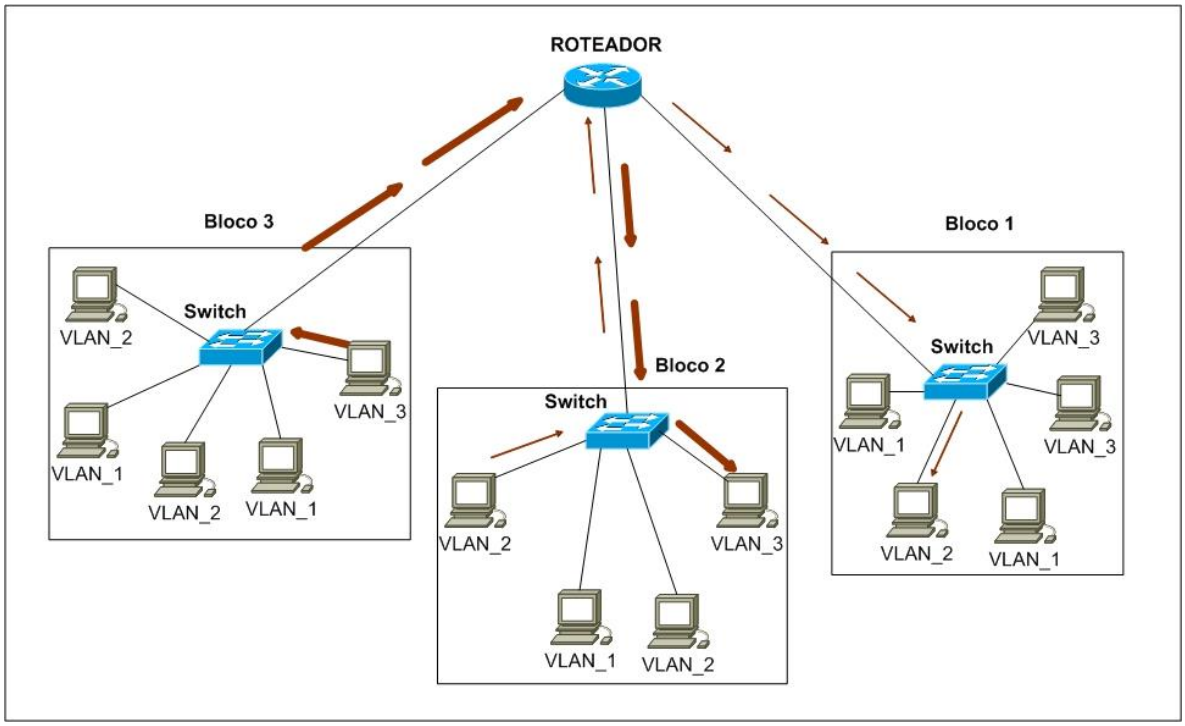

Figura 8 – Exemplo de uma rede usando o recurso de LAN virtual.

2.7 Dispositivos de rede

Estes equipamentos conectam os usuários aos diversos recursos que uma rede possui. Eles podem prover acesso à Internet, imprimir documentos, planilhas, compartilhar arquivos entre outras funcionalidades. Sem os dispositivos de rede não haveria a possibilidade de se criar a Internet, que hoje une quase todo o mundo, formando uma das maiores redes de comunicação de dados. Os equipamentos mais conhecidos são: *hosts*, *hubs*, *switches* e roteadores, e seus respectivos símbolos são mostrados na figura 9 [4, 5].

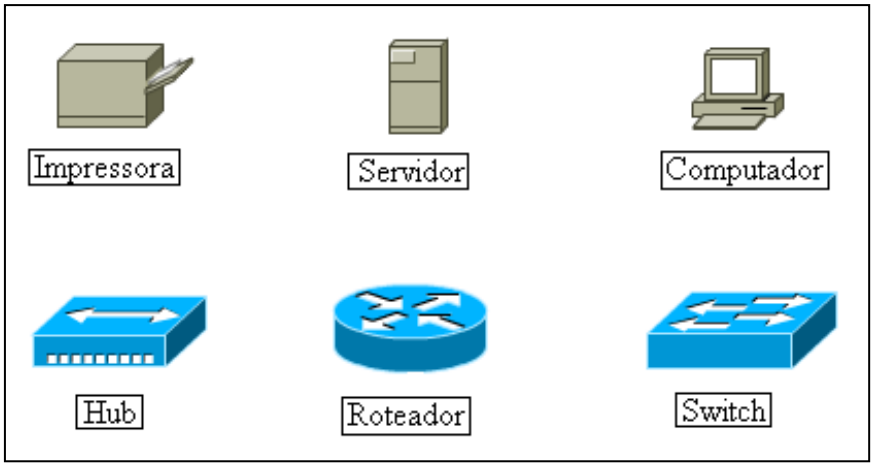

Figura 9 – Dispositivos de rede.

2.7.1 Host

Os dispositivos conectados a um segmento de rede são chamados de *host*. Este nome é dado para diversos equipamentos tais como: computadores (estações de trabalho ou servidores), *scanners*, impressoras, entre outros.

2.7.2 Hub

A função de um *hub* é regenerar e retemporizar um determinado sinal na rede a nível binário ou sinal elétrico, pois ele trabalha na camada 1 do OSI. Ele possui diversas portas onde os *hosts* são conectados, por isso muitas vezes ele é chamado de concentrador. Quando um sinal chega a uma de suas portas ele trata este sinal,

retemporizando-o e regenerando-o, e depois o transmite para todas as suas outras portas.

O *hub* pode ser classificado como “inteligente” ou “burro”. O *hub* “burro” simplesmente pega o sinal que entra por uma de suas portas e o retransmite para todas as outras. Já o *hub* “inteligente” faz isso e também possui uma porta console, por onde ele pode ser programado para gerenciar basicamente o tráfego em uma rede.

2.7.3 Switch

O *switch* ou comutador é um dispositivo que trabalha na camada 2 do modelo de referência OSI, portanto ele possui características mais avançadas em relação a um *hub*. Ele possui habilidade de encaminhar os dados para o destino levando em consideração o endereço de camada 2 ou endereço MAC.

Baseado neste endereço, o *switch* decide para qual de suas portas ele enviará os bits ou quadro de dados para chegar até o destino apropriado. Esta operação é chamada de filtragem de quadros.

Os *switches* reduzem as colisões e aumentam a largura de banda real nos segmentos da rede porque fornecem largura de banda dedicada a cada segmento. A finalidade de um *switch* é concentrar a conectividade e tornar mais eficiente a transmissão de dados.

2.7.4 Roteador

Este dispositivo fornece conectividade e seleção de caminhos entre dois sistemas, que podem estar localizados em redes separadas. Os roteadores são dispositivos que trabalham na camada de rede e um dos equipamentos de controle de tráfego mais importantes para as grandes redes, como a Internet.

Sua função principal é verificar os pacotes de dados que chegam a uma de suas interfaces e escolher o melhor caminho ou rota para eles através da rede. Em seguida, estes dados são enviados para a interface ou porta de saída apropriada.

Segundo Odom [8], o roteador toma decisão lógica relativa ao melhor caminho para a entrega dos dados em uma rede baseados nas informações da camada 3. Este processo que o roteador executa é chamado de determinação de caminho.

A determinação de caminho possibilita que um roteador avalie os caminhos disponíveis a um destino e estabeleça um tratamento eficiente de entrega do pacote de dados ao destino. Outros serviços que um roteador pode realizar são os filtros de pacotes com a utilização de *ACLs* e o *NAT*.

2.8 Endereçamento lógico

O Internet Protocol (*IP*) é o esquema de endereçamento de rede hierárquico ou lógico mais conhecido. O endereço *IP* é o protocolo de rede utilizado pela Internet. Na camada de rede, os dados são encapsulados dentro de pacotes, também conhecidos como datagramas.

O pacote IP possui as informações necessárias para encaminhar um pacote através da rede. Este pacote contém diversas informações das quais, as mais importantes são os endereços de origem e destino de cada *host* envolvido na comunicação.

O endereço IP é composto por 32 bits dispostos em quatro octetos. A forma usada para representar um endereço é a decimal, mostrada na figura 10 [6]. Pode-se observar que o endereço IP possui duas partes distintas, uma identifica a rede a que o dispositivo está conectado, e a outra parte identifica o dispositivo específico nessa rede, ou seja, o *host*.

Os três primeiros octetos juntos ou não, podem ser usados para identificar o endereço de rede. De forma análoga, os últimos três octetos podem ser usados para identificar a parte do *host* de um endereço IP.

Basicamente, existem três classes de endereços IP e são controladas e distribuídas pela *American Registry for* Internet *Numbers*. No Brasil quem disponibiliza estes endereços é a FAPESP.

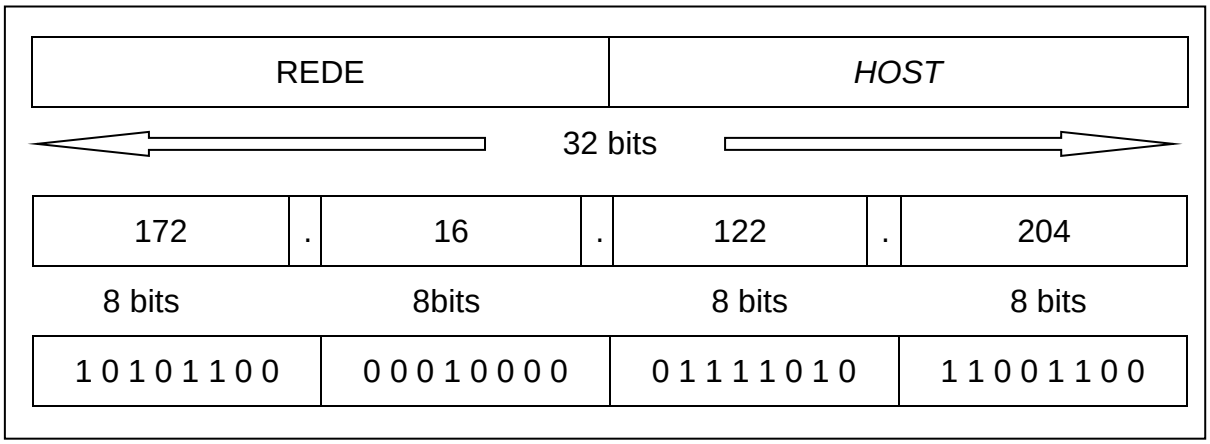

Figura 10 – Formato do endereço IP.

A figura 11 apresenta as três classes de endereços IP. Dentro de cada uma dessas classes existem faixas de endereços destinados a endereços IP particulares ou privados. Estes endereços são atribuídos aos *hosts* e às redes internas pelo seu administrador de rede.

Segundo a RFC 1918 [16], as faixas de endereços privados são:

- 10.0.0.0 a 10.255.255.255
- 172.16.0.0 a 172.31.0.0
- 192.168.0.0 a 192.168.255.255

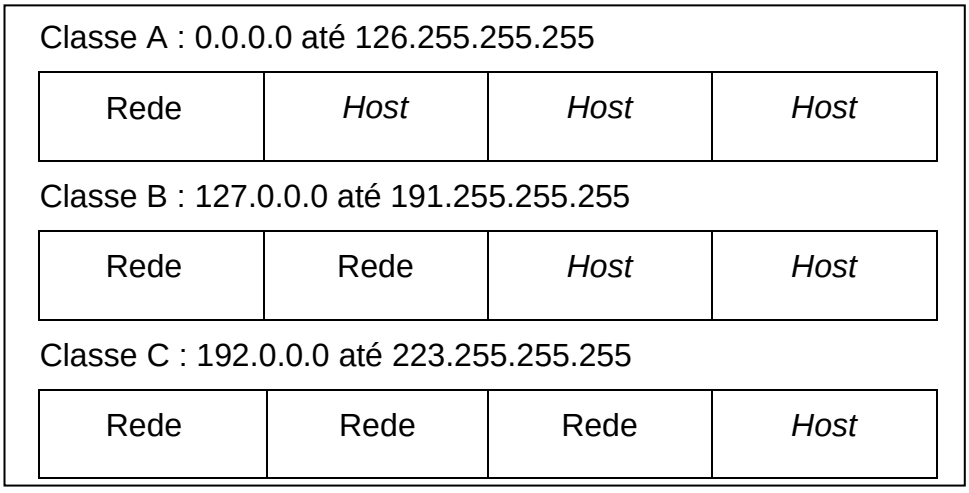

Figura 11 – Classes de endereços IP.

Uma das vantagens dos endereços particulares reside na segurança, pois estes endereços não são roteáveis na rede pública, logo, não podem ser anunciados na Internet.

Outra vantagem deste tipo de endereço é a economia de IP, pois com alguns IP públicos é possível fornecer acesso a muitos *hosts* com endereços particulares.

Porém, existem algumas desvantagens no uso do endereçamento privado, entre elas está o problema da administração remota da rede, que se torna mais difícil e complexa.

Em seguida, serão mostrados alguns conceitos importantes, tais como, métodos de endereçamento lógico, endereços de rede, *broadcast*, sub-redes e máscara de rede [4-6].

2.8.1 Métodos de atribuição de endereços lógicos

Basicamente, existem dois métodos para atribuir endereços IP: endereçamento estático e o dinâmico. Independentemente do esquema de endereçamento usado, dois *hosts* ou interfaces de rede não podem ter o mesmo IP.

Quando se utiliza o endereçamento estático, cada *host* é configurado manualmente. Este método exige a elaboração de um registro muito minucioso para evitar a ocorrência de problemas na rede como, por exemplo, o uso endereços IP duplicados.

O endereçamento dinâmico reduz as tarefas de configuração dos *hosts* utilizando, por exemplo, o DHCP. Este serviço é utilizado para automatizar as configurações do protocolo TCP/IP.

Sem a utilização deste recurso, os administradores teriam que configurar manualmente as propriedades do protocolo TCP/IP em cada *host* na rede. A utilização do DHCP traz diversos benefícios, dentro os quais se destacam [1, 9]:

- Automação do processo de configuração do protocolo TCP/IP nos *hosts*. Esta automação torna o suporte de rede mais eficiente e menos penoso para os administradores, pois atualmente a equipe de suporte da universidade é muito pequena.

- Facilidade de alteração dos parâmetros de rede, tais como, *default gateway*, servidor de DNS, endereço IP, máscara de rede entre outros parâmetros. Isto é possível porque toda a configuração é realizada no servidor DHCP.
- Eliminação dos erros de configuração das interfaces de rede, tais como, digitação incorreta de uma máscara de sub-rede ou utilização de um mesmo número IP em dois *hosts*.

O DHCP é um serviço baseado em aplicativos cliente-servidor. Os servidores alocam os endereços IP e armazenam as informações sobre esses endereços atribuídos aos *hosts*. Entre os métodos de alocação dinâmica de endereços IP, dois se destacam pelas suas funcionalidades. Estes métodos são [1]:

- **Atribuição automática**

  Neste método, o servidor DHCP atribui um IP definitivo a um *host*. Cada vez que este *host* sair e depois entrar na rede ele irá receber o mesmo endereço IP.

- **Atribuição dinâmica**

  O servidor DHCP atribui um IP a um *host* por um período de tempo limitado, e este período é chamado de arrendamento. Este método de atribuição é o mais utilizado.

2.8.2 Endereço de rede

É um IP que termina com “zeros” binários em todos os *bits* da porção de *host* deste endereço. Por exemplo, um endereço IP classe C 199.10.20.0 é o endereço de rede que contém o *host* 199.10.20.3. Os *hosts* em uma rede podem se comunicar diretamente com outros que possuem o mesmo endereço de rede.

2.8.3 Endereço de broadcast

É o endereço usado para enviar pacotes de dados para todos os *hosts* em uma mesma rede. Para garantir que todos os *hosts* na rede vão perceber esse

broadcast, a origem deve usar um endereço IP de destino que todos eles possam reconhecer e analisar.

O endereço de *broadcast* termina com dígitos “uns” na parte do *host* deste endereço. Como exemplo, tem-se o endereço de rede 199.10.20.0. O último octeto identifica a porção de *host*, portanto, o endereço de *broadcast* será 199.10.20.255. Se for enviado um pacote com este IP de destino, estes dados serão recebidos e processados por todos os *hosts* pertencentes a esta rede 199.10.20.0.

Portanto, pode-se concluir que domínio de *broadcast* é o conjunto de *hosts* pertencentes à mesma rede ou que possuem o mesmo endereço de rede.

2.8.4 Sub-redes

As sub-redes são criadas a partir dos endereços A, B ou C. A parte do endereço que especifica a porção de *host* é dividida em duas partes. Uma delas é a parte de sub-rede e a outra é a nova porção de *host*. O motivo principal de se utilizar este recurso é diminuir o tamanho de um domínio de *broadcast*.

2.8.5 Máscara de rede ou sub-rede

A máscara de rede ou sub-rede não é um endereço, mas determina qual parte de um endereço IP é a porção de rede e qual parte é a porção de *host*. Uma máscara também possui 32 bits separados em quatro octetos [5, 6]. A figura 12 mostra um exemplo de como se determinar a máscara de uma sub-rede.

O método utilizado para descobrir a máscara de uma sub-rede qualquer é muito simples. Por exemplo: onde for porção de rede no endereço IP, na máscara será indicado por “uns” binários e onde for porção de *host* será indicado por “zeros” binários. Em seguida, é só converter este número binário em decimal.

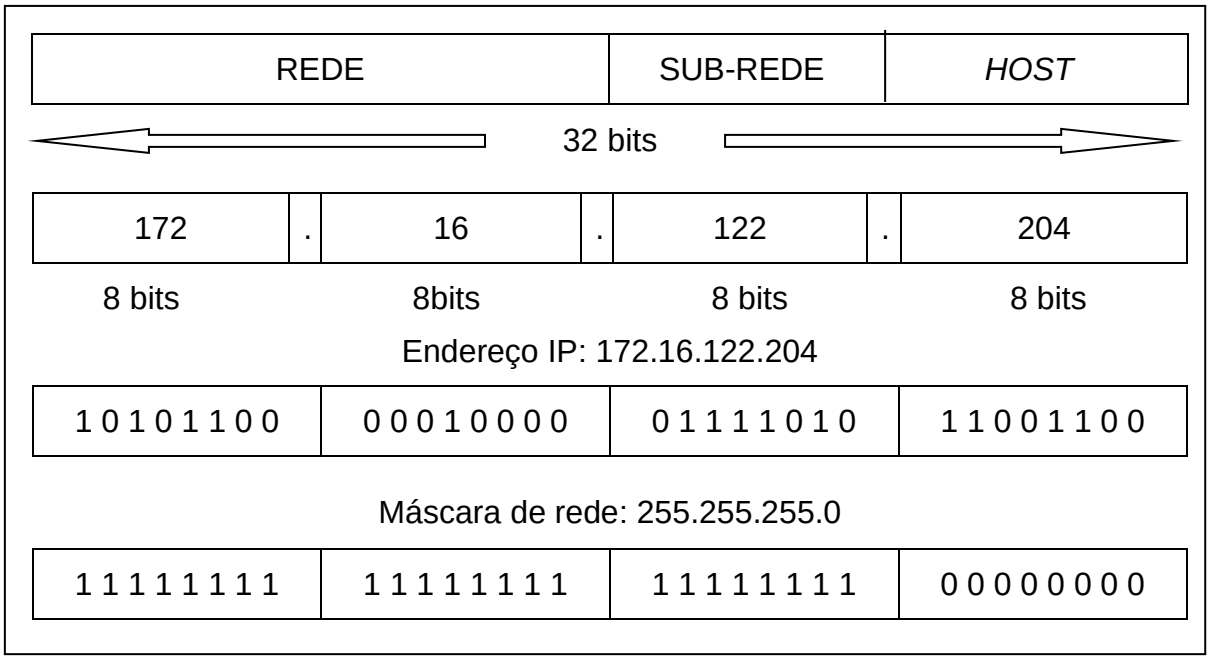

Figura 12 – Determinação de uma máscara de sub-rede.

2.9 Servidores de rede

O servidor de rede é um *host* executando determinada função e/ou serviço, tais como compartilhamento de arquivos, resolução de nomes de domínio, aplicativos, impressão e comunicação. Normalmente os servidores de rede não funcionam como estações de trabalho, mas executam sistemas operacionais especializados, como o *Netware*, *Windows Server*, *UNIX* ou *Linux*.

Um servidor pode ser classificado em duas categorias distintas: corporativo e de grupo de trabalho [8, 9].

2.9.1 Servidor corporativo

O servidor corporativo fornece serviço para todos os usuários de uma rede, por exemplo, serviço de hospedagem de página, resolução de nomes de domínio, correio eletrônico, entre outros aplicativos. As funções mais comuns dos servidores corporativos são mostradas a seguir.

2.9.1.1 Resolução de nomes de domínio

Um domínio é um grupo de *hosts* associados por sua localização geográfica ou pelo seu tipo de negócio. O nome de um domínio é uma seqüência de caracteres e/ou números, geralmente um nome ou abreviatura, que representa o endereço numérico de um *site* na Internet.

O servidor que executa este serviço é chamado de servidor de DNS. Ele responde às solicitações dos usuários para traduzir um nome de domínio para um endereço *IP* associado. O sistema DNS é configurado em uma hierarquia que cria diferentes níveis de servidores.

2.9.1.2 Correio eletrônico

Este serviço possui a função de enviar e receber mensagens de correio eletrônico entre *hosts* conectados à mesma rede ou não. O procedimento para se enviar um *e-mail* se divide em duas partes.

A primeira parte é responsável por enviar as mensagens eletrônicas à agência de correio do usuário ou seu servidor de correio eletrônico. A segunda parte desse procedimento é responsável por entregar ao usuário de destino o seu e-*mail*.

Para o usuário de rede enviar ou receber e-*mails* é necessário usar *softwares* destinados ao envio ou recepção de mensagens como, por exemplo, o *Microsoft Outlook* ou *Mozilla Thunderbird*.

2.9.1.3 Transferência de arquivos

Este serviço utiliza um protocolo de transferência de arquivos ou FTP. Este protocolo foi projetado para fazer *download* ou *upload* de arquivos.

O *FTP* é uma aplicação cliente-servidor assim como o *e-mail* ou DNS. Ele exige um *software* servidor sendo executado em um *host* que possa ser acessado pelo usuário através de um *software* cliente.

Portanto, a finalidade principal do FTP é transferir arquivos de um computador para outro, copiando e movendo arquivos do servidor para o cliente e vice-versa.

2.9.1.4 Web Server

Este tipo de servidor fornece hospedagem de páginas, sejam estas pessoais, de determinados institutos ou da própria universidade. Para acessar uma página de w*eb* é preciso utilizar um navegador *web*.

Este tipo de navegador apresenta os dados em formato multimídia nas páginas da w*eb* que usam texto, figuras, som e vídeo.

2.9.1.5 Intranet

É uma rede muito semelhante à Internet, só que voltada para dentro de uma instituição. Ela otimiza os processos de administração e troca de informações, permitindo o compartilhamento interno das mesmas utilizando um *web browser*. Outro ponto a ser observado é que a *Intranet* não disponibiliza as informações que circulam por ela a qualquer um com acesso à Internet.

2.9.2 Servidor de grupo de trabalho

Os servidores de grupo de trabalho fornecem serviços a um grupo específico de usuários de uma rede, que possuem necessidades semelhantes, por exemplo, impressão de arquivos, compartilhamento de arquivos, processamento de textos utilizados por usuários de determinados departamentos, tais como, departamento de contabilidade, de recursos humanos ou de engenharia.

Esta classe de servidor não é abordada neste trabalho, pois o foco principal desta proposta são os servidores corporativos.

2.10 Política de segurança da informação

Segundo Soares em [3], a política de segurança é um conjunto de leis, regras e práticas que regulam como uma instituição gerencia, protege e distribui suas informações e recursos.

A política de segurança é um mecanismo preventivo de proteção dos dados e processos importantes de uma instituição, que define um padrão de segurança a ser

seguido pelo corpo técnico e gerencial e, também, pelos usuários internos e externos.

A política de segurança pode ser usada para definir as interfaces entre usuários, fornecedores e parceiros e, para medir a qualidade e a segurança dos sistemas usados.

A informação é um ativo da instituição, que possui sua importância e por isso deve ser preservada e protegida. A informação possui muitas formas, dentre elas, pode-se citar a mídia impressa ou de papel, mídia eletrônica, mídia falada ou filmada.

Para que a informação seja considerada segura, ela deve possuir as seguintes características [17]:

- **Confidencialidade**: garantir que a informação seja acessível somente aos usuários autorizados.
- **Integridade dos dados**: evitar que dados sejam apagados ou alterados sem prévia permissão.
- **Disponibilidade:** garantir o funcionamento do serviço de informática, sob demanda, sempre que necessário aos usuários autorizados.

De acordo com Carvalho [18], a política de segurança trabalha com os aspectos humanos, culturais e tecnológicos de uma instituição. Levando-se em conta estes aspectos, devem-se criar os diversos procedimentos e normas de segurança dentro de uma instituição.

A política de segurança gera impacto em todos os projetos de informática, tais como, plano de desenvolvimento de novos sistemas, plano de contingências, planejamento de capacidade, entre outros. É importante lembrar que a política não envolve apenas a área de informática, mas todas as áreas da instituição.

Segundo Kisser [19], deve-se ter em mente que segurança sólida é um processo e não um produto. Conseqüentemente, não haverá uma melhora muito significativa se a instituição adquirir um *firewall* e um antivírus. É necessário criar toda uma política norteando a segurança da informação da instituição, de acordo com seus objetivos e necessidades.

2.11 Plano gestor de informática

O plano estratégico ou gestor de informática é um conjunto de normas e regras que regulamentam o uso dos recursos de informática em uma organização. Sua principal finalidade é propiciar o conhecimento de seu próprio ambiente computacional, com uma visão global [17, 20]. Esta visão possibilita um melhor planejamento de como se investir os recursos disponíveis na área de informática.

O Plano estratégico de Informática é um documento que deve acompanhar a evolução das necessidades da instituição, devendo refletir os processos envolvidos dentro de cada setor da organização.

2.12 Caracterização do tráfego da rede

Este processo é responsável por identificar a origem e o destino dos pacotes de dados que trafegam pela rede. Outro ponto a ser observado é o mapeamento do fluxo da informação, que precisa ter o conhecimento de todos os locais responsáveis pelo armazenamento das informações mais pertinentes.

Segundo Oppenheimer [1], um dos métodos mais simples para auxiliar a caracterização do fluxo de dados é medir o número de *bytes* por segundo entre a origem e o destino.

Para realizar esta tarefa, pode-se utilizar um analisador de protocolos ou um *software* de gerenciamento e monitoramento de redes para registrar o fluxo entre sistemas finais como, por exemplo, entre clientes e servidores.

O analisador de protocolos é uma ferramenta de gerenciamento de desempenho e falhas, que captura o tráfego da rede, decodifica os protocolos usados nos pacotes, e depois fornece diversas informações e estatísticas, que permitem a caracterização do tráfego que passa pela rede.

O intervalo de levantamento dos dados é muito importante, pois a escolha errada pode prejudicar a análise dos dados e a elaboração do projeto. Entre os diversos recursos usados para levantar as informações sobre a utilização da largura

de banda, taxa de utilização dos servidores e os requisitos de qualidade de serviço, podem-se citar três: *NetFlow*, MRTG e o *Nagios* [20-22].

- *NetFlow* é uma tecnologia da Cisco que disponibiliza uma base de valores e métricas para aplicações de monitoramento, incluindo relatórios de tráfego da rede, criação de faturas baseadas no uso da rede.

  O *NetFlow* fornece informações de quem está utilizando a rede, quais aplicações estão sendo usadas, quando a rede esta sendo utilizada, entre outras informações. Esta tecnologia é um recurso muito importante utilizado pelos administradores de rede, que o utiliza para detectar ataques de *denial of service*, ataques de *worms*, entre outras funcionalidades. Para conseguir capturar as informações fornecidas pelo *NetFlow* deve-se utilizar alguns pacotes de aplicativos como o *FlowScan e o FlowTools*.

  O aplicativo *FlowTools* é um conjunto de programas que tem a finalidade de fazer a coleta e processamento de dados *NetFlow* provenientes dos roteadores Cisco. Este pacote foi desenvolvido em C e possui suporte para exportar dados para outros *softwares* de visualização e de coleta. Em função do uso específico para o *Netflow*, o mesmo é marcado pela sua simplicidade na coleta, visualização e totalização das informações.

  O pacote *FlowScan* possibilita a criação de gráficos baseados nos dados fornecidos pelos programas de coleta. Uma vez que os dados são fornecidos, uma ferramenta deste pacote lê estes dados e gera arquivos no formato RRD (Round Robin Database). Depois que estes arquivos são criados e atualizados com uma freqüência pré-configurada, os gráficos podem ser gerados.

- MRTG é uma ferramenta *open source* para monitoramento de carga do tráfego da rede e outras características de gerenciamento de desempenho e de falhas.

- *Nagios* é um programa *open source* de monitoramento de *hosts*, serviços e redes, que verifica constantemente a disponibilidade do serviço local ou remoto. Ele é capaz de monitorar *switches*, impressoras, computadores, enfim, quase tudo que estiver conectado à rede.

3 LEVANTAMENTO DOS REQUISITOS DOS USUÁRIOS E DA UNIFEI

O primeiro passo para o levantamento das metas e dos requisitos desejados é a realização de uma pesquisa sobre a universidade e seus colaboradores, sejam eles alunos, professores ou funcionários técnico-administrativos.

Basicamente, este trabalho cita três métodos possíveis para a realização deste levantamento dos requisitos. Os métodos citados são [5]:

- **Perfis da comunidade de usuários**

  Este método analisa os diferentes grupos de usuários e suas necessidades. Com isto, é possível levantar as necessidades e as metas mais importantes.

  Embora a maioria dos usuários comuns possua os mesmos requisitos de correio eletrônico ou acesso à Internet, eles também podem ter necessidades diferentes como, por exemplo, o compartilhamento de servidores de impressão, compartilhamento de arquivos locais.

  Deve-se compreender que alguns grupos podem requerer acesso aos mesmos servidores, já outros podem desejar permitir o acesso externo a recursos internos de computação específicos.

- **Entrevistas com grupos-chave**

  Este método utiliza-se de entrevistas com os usuários para reunir as informações pertinentes. Os grupos dos usuários pesquisados também podem ser usados para reunir informações e gerar discussões entre diferentes usuários com interesses semelhantes ou distintos.

- **Testes de fatores humanos**

  Este método é o mais caro, demorado e possivelmente o mais esclarecedor para se levantar os requisitos do usuário.

  É baseado na realização de testes envolvendo representantes de usuários em um ambiente de laboratório. Isso é mais apropriado quando se pretende avaliar os requisitos de tempo de resposta. Por exemplo, podem-se configurar sistemas de trabalho e fazer com que os usuários executem atividades normais de *host* remoto a partir da rede do laboratório.

  Analisando as reações dos usuários às variações na resposta do *host*, podem-se criar limites de avaliação de desempenho para níveis aceitáveis.

3.1 Método utilizado para o levantamento dos requisitos

Utilizou-se o método das entrevistas e questionários com grupos-chave junto à universidade para realizar o levantamento das metas e dos requisitos dos usuários e da UNIFEI.

Estes questionários foram elaborados levando-se em conta três classes distintas de usuários entrevistados e, estes questionários podem ser encontrados no apêndice A desta dissertação.

Estes questionários foram elaborados com o intuito de levantar informações sobre os aplicativos utilizados, o desempenho da rede, aplicativos futuros, entre outras.

Devido ao número de usuários, esta pesquisa se limitou a elaborar entrevistas por amostragem, ou seja, foram escolhidos em torno de quarenta usuários da rede.

Estas classes de usuários foram qualificadas da seguinte maneira:

- **Usuários da rede**

  São os usuários que utilizam a rede como ferramenta de trabalho, tais como pesquisa, e-mail e não como parte integrante de suas atividades.

- **Administradores da rede**

  São os usuários responsáveis pela gerência e administração da rede UNIFEI.

- **Administração da UNIFEI**:

  São os usuários da rede que possuem as funções de administração e planejamento das metas da instituição, no que se refere à gestão de tecnologia da informação na universidade.

3.2 Abrangência do questionário

Cada uma das classes de usuários analisada pela pesquisa possui uma visão única da rede e sua situação atual. Observando-se este cenário, ficou evidente a necessidade da criação de questionários personalizados para cada classe de usuário. Essa personalização gerou alguns tópicos dentro de cada um dos perfis dos usuários.

3.2.1 Usuários da rede

Para esta classe de usuários foi desenvolvido um questionário com questões relacionadas aos seguintes tópicos:

- Atividades desenvolvidas pelos usuários, ligadas à rede interna.
- Atividades desenvolvidas pelo usuário, ligadas à Internet.
- Avaliação e observação sobre o desempenho da rede interna e do acesso à Internet.
- Atividades futuras dos usuários.

- Possíveis recursos tecnológicos necessários para implementar estas atividades futuras.

3.2.2 Administradores da rede

As perguntas realizadas para esta classe foram direcionadas para se obter informações referentes aos recursos humanos e ao nível de capacitação dos administradores da rede. Os principais pontos levantados foram:

- Avaliação dos recursos humanos quanto à:
    - Quantidade de pessoas ligadas à administração e a gerência da rede.
    - Capacitação técnica das pessoas ligadas à administração e a gerência da rede.

- Avaliação dos recursos técnicos atualmente em uso na rede, quanto:
    - Ao número e capacidade dos servidores corporativos.
    - À qualidade e desempenho da infra-estrutura implantada.
    - À qualidade e desempenho dos dispositivos de rede atuais.
    - Ao número e capacidade dos computadores usados pelos clientes.

3.2.3 Administração da UNIFEI

Nesta classe de usuários as perguntas foram direcionadas com o intuito de se obter informações referentes aos recursos técnicos e financeiros da universidade. Os pontos levantados com o auxílio do questionário foram:

- Desempenho da rede interna quanto às expectativas da UNIFEI.
- Desempenho do acesso à Internet quanto às expectativas da UNIFEI.
- Planejamento da instituição para as novas tecnologias.
- Metas da instituição para a gestão dos recursos de tecnologia da informação.
- Investimento em tecnologia da informação para os próximos anos.

3.3 Levantamento dos requisitos dos usuários

Após a elaboração dos questionários, foram escolhidos alguns usuários de cada uma das classes definidas para a realização das entrevistas.

As respostas foram obtidas através de visitas realizadas a cada um dos usuários escolhidos. As informações a seguir refletem as metas e os requisitos dos usuários.

3.3.1 Usuários da rede UNIFEI

Estes usuários usam a rede interna para diversas atividades como, por exemplo, compartilhamento de arquivos e equipamentos de informática, utilização do sistema acadêmico de notas, ensino a distância, consultas à *Intranet* e também para pesquisa e desenvolvimento acadêmico.

Com relação às atividades que utilizam a Internet, os pontos citados estão relacionados ao uso do correio eletrônico, pesquisa a *sites* acadêmicos, *download* de arquivos, pesquisa e desenvolvimento de trabalhos, publicação de artigos e divulgação de informações.

A maioria dos usuários afirmou que o desempenho do acesso à Internet está muito ruim. Já a rede interna possui uma deficiência na qualidade e quantidade de serviços oferecidos aos usuários.

Foram apontadas diversas causas para justificar o baixo desempenho da rede. Entre elas, pode-se citar a falta de recursos humanos, excesso de vírus na rede, falta de um plano de capacitação técnica dos administradores da rede, equipamentos de rede obsoletos, falta de políticas de informática e computadores desatualizados e insuficientes para atender a todos os usuários.

As respostas adquiridas sobre as atividades que serão desenvolvidas pelos usuários nos próximos anos, se concentram no ensino a distância, uso do sistema acadêmico via *web* e o aumento dos serviços disponibilizados pela *Intranet*.

Segundo esta classe de usuários, os recursos tecnológicos necessários para o desenvolvimento das futuras atividades estão relacionados à modernização e à

ampliação da base de computadores disponíveis e à atualização dos dispositivos de rede instalados atualmente.

3.3.2 Administradores da rede UNIFEI

A administração da rede é em parte descentralizada logo, para levantar estas informações foi necessário procurar a maioria dos administradores locais, de cada um dos institutos. As primeiras informações levantadas foram em relação aos recursos humanos e suas características atuais.

Um dado muito importante levantado nesta pesquisa, diz respeito ao número de funcionários da administração. Atualmente, a universidade possui cerca de três a quatro funcionários para gerenciar a rede principal. Portanto, fica evidente a necessidade de mais funcionários para desempenhar esta função.

Outro ponto abordado pela pesquisa é a capacitação técnica dos administradores. Há um *déficit* considerável nesta área, pois os investimentos em treinamento e aperfeiçoamento técnico não são suficientes para atender toda a demanda.

Na área de informática, os avanços tecnológicos são muito intensos. Logo, deve-se elaborar um plano de investimentos que proporcione uma melhor capacitação dos administradores da rede.

Para a maioria dos usuários entrevistados, os recursos técnicos da rede como, por exemplo, os computadores para os usuários, se apresentam em número insuficiente e muitas vezes com capacidade inadequada para o uso.

Completando este assunto, foi observado que os computadores utilizados pelos administradores não são adequados para fornecer condições satisfatórias para a gerência da rede.

Outro recurso técnico citado na pesquisa diz respeito aos servidores da rede, que foram considerados inadequados para atender às necessidades da UNIFEI. Um bom exemplo é o servidor de correio eletrônico, que possui uma taxa de ocupação em torno de 90%.

Por outro lado, existem alguns servidores locais, dentro dos institutos, que estão com uma taxa de ocupação relativamente pequena.

Em relação aos dispositivos de rede, foi verificado que a maioria é inadequada para atender corretamente a demanda de conectividade da UNIFEI.

Os administradores da rede UNIFEI recomendaram a elaboração de um plano gestor de informática e a centralização dos recursos de rede para facilitar o gerenciamento e o monitoramento da rede.

Por fim, estes usuários citam a fragilidade do atual sistema, sem uma política de segurança da informação e um plano eficiente de gerenciamento dos recursos de rede.

3.3.3 Administradores da UNIFEI

Para a maioria dos entrevistados o desempenho da rede foi classificado como insuficiente para atender os requisitos dos usuários. A causa deste problema está ligada a diversos fatores, entre eles o alto índice de vírus na rede, suporte inadequado aos usuários, instabilidade do acesso à Internet e a lentidão observada em horários distintos.

A maioria dos administradores acredita que as novas tecnologias e recursos de rede pretendidos para a universidade estão ligados ao ensino à distância, projeto do novo sistema acadêmico, melhora do acesso à Internet, centralização da gerência da rede e o aumento na confiabilidade da rede.

Os entrevistados disseram que a instituição precisa de um plano de metas para a gestão e segurança dos recursos de tecnologia da informação, bem como um planejamento de investimentos em tecnologia da informação para os próximos anos.

3.4 Levantamento das informações suplementares sobre a UNIFEI

A Universidade Federal de Itajubá é uma universidade tecnológica com cerca de 2200 alunos entre os cursos de graduação e pós-graduação. Ela dispõe de 96% de seus docentes em regime de trabalho em tempo integral com dedicação exclusiva, sendo 56% com o título de doutor, 37% com o título de mestre, 3% com especialização e 4% graduados. Portanto, cerca de 93% dos docentes possuem pós-graduação em nível de mestrado e doutorado [23].

A UNIFEI dispõe de diversos cursos como, por exemplo, ciência da computação, engenharia de computação, engenharia elétrica, engenharia mecânica, entre outros.

O campus da universidade é constituído de oito blocos, onde estão distribuídos os diversos institutos, laboratórios, grupos de estudos, a biblioteca, a administração da universidade e a reitoria.

4 ANÁLISE DAS METAS E RESTRIÇÕES DOS USUÁRIOS E DA UNIFEI

Após a realização das entrevistas com os grupos de usuários, foram obtidas diversas respostas de cada grupo pesquisado, que possibilitaram uma análise mais detalhada das necessidades e requisitos dos usuários e da UNIFEI.

4.1 Análise das metas dos usuários

As metas mais relevantes da universidade dizem respeito à utilização dos recursos de tecnologia da informação e às necessidades dos usuários.

4.1.1 Acesso à Internet e à rede interna

A UNIFEI possui dois *links* de acesso à Internet, mas a falta de um controle de banda eficaz impede um melhor aproveitamento destes recursos, por parte dos pesquisadores, professores e alunos desta instituição, que procuram novos conhecimentos, materiais didáticos para o desenvolvimento de trabalhos e pesquisas e também, a publicação e divulgação de informações e trabalhos acadêmicos.

Os usuários citaram a necessidade da elaboração de novas atividades e recursos para serem disponibilizados na rede interna como o compartilhamento de arquivos e equipamentos, artigos e materiais para pesquisa e desenvolvimento acadêmico.

4.1.2 Novo sistema acadêmico

Com a crescente evolução tecnológica, a universidade carece de um novo sistema acadêmico, que venha oferecer um conjunto de recursos adicionais, visando melhorar a integração e a atuação dos professores, funcionários e alunos nos procedimentos de matrícula, lançamento de notas, entre outros.

4.1.3 Ensino a distância

De todos os requisitos levantados, este é o que possui uma maior necessidade de gerenciamento e disponibilidade de banda.

O ambiente de ensino a distância promove um novo conceito de educação continuada, onde mesmo fora da sala de aula, os alunos e ex-alunos podem continuar a desenvolver suas capacidades e aprender novos conceitos.

4.2 Análise das restrições da UNIFEI

Os dados obtidos neste tópico se referem às restrições orçamentárias e de pessoal. Analisando os dados adquiridos percebe-se que existe a necessidade de investimento em treinamento e capacitação técnica dos gerentes e funcionários responsáveis pela administração da rede local.

Outro ponto importante a ser considerado é a falta de um orçamento próprio para o setor de informática. Isso causa uma insegurança nos administradores da rede, pois não sabem quando receberão os recursos e nem onde irão empregá-los.

Outro aspecto relevante do projeto é a questão funcional. Esta proposta de reestruturação da rede será coordenada pelos administradores de rede, podendo sofrer alterações de acordo com suas necessidades e opiniões.

4.3 Análise das metas e restrições técnicas da rede UNIFEI

As metas de cada instituição são muito específicas, mas existem alguns requisitos que aparecem na maioria dos projetos de rede como a disponibilidade, escalonabilidade e a gerenciabilidade da rede [5, 9].

Foram levantadas outras metas da rede como, por exemplo, confiabilidade, desempenho e a mudança do centro de operações de rede.

4.3.1 Disponibilidade

Este requisito se refere ao tempo em que a rede está disponível ao usuário com velocidade e confiabilidade aceitável.

Segundo o levantamento realizado, esta meta tem sido parcialmente atendida, pois diversos usuários reclamaram da necessidade de utilizar a rede em certos momentos, e ela não estar disponível.

A falta de sistemas redundantes de energia e as precárias instalações físicas das salas de equipamentos não garantem o funcionamento constante dos serviços de rede.

4.3.2 Escalonabilidade

Refere-se ao nível de crescimento que um projeto inicial pode ter sem causar nenhuma mudança fundamental no projeto geral.

Esta meta possui uma importância fundamental para a proposta em questão, pois atualmente não há nenhum estudo na universidade que revele alguma preocupação com este requisito.

A atual infra-estrutura da rede não permite que se alcancem as metas propostas pelos usuários. Os novos serviços requisitados como, por exemplo, a centralização dos recursos da rede e um novo sistema acadêmico, não podem ser implementados sem uma mudança significativa na rede.

4.3.3 Gerenciabilidade

Esta meta visa atender às necessidades de se projetar uma rede com o intuito de facilitar sua monitoração e gerenciamento, assegurando com isto, sua estabilidade permanente de operação.

Segundo as respostas obtidas, a universidade possui um número insuficiente de funcionários para administrar a rede. Outro ponto citado pelos usuários foi a ausência de um plano de investimento na área de informática.

Este plano deve prever investimentos em capacitação técnica dos administradores e também na atualização dos equipamentos de informática.

O gerenciamento da rede é um assunto muito extenso e complexo, que requer um estudo mais aprofundado do que o sugerido nesta proposta.

Uma das finalidades desta proposta é colocar em discussão as possíveis melhorias que podem ser realizadas na rede e também, propor algumas soluções iniciais para a rede da universidade.

4.3.4 Confiabilidade da rede

Com as informações tendo cada vez mais importância nas tomadas de decisões da administração da UNIFEI, é inconcebível que os usuários da UNIFEI fiquem dependentes de um conjunto de fatores relacionados com a operação da rede para executarem suas funções.

Nos dados levantados junto aos usuários da rede, não existe atualmente uma política de segurança da informação para tentar garantir uma maior confiabilidade da rede.

Não há um conjunto de equipamentos na universidade que possa dar um nível mínimo de segurança para as informações dos usuários. Atualmente as únicas ferramentas disponíveis são um antivírus e um filtro de pacotes implementado no roteador.

4.3.5 Desempenho da rede e do acesso à Internet

Como resultado da análise das informações levantadas, pode-se perceber que em todas as classes pesquisadas, a Internet é essencial para a realização das tarefas dos usuários da rede. Muitas vezes estas tarefas são dificultadas ou impedidas por falta de um melhor gerenciamento e monitoramento dos recursos de rede.

Constatou-se que a universidade não possui equipamentos para prover um melhor gerenciamento dos *links* de Internet como, por exemplo, um controlador de banda ou um equipamento para executar o balanceamento de carga nos *links*.

Atualmente toda a atividade de ensino a distância da UNIFEI está sendo disponibilizada em um servidor, que também executa os serviços de *e-mail*, DNS, FTP e servidor *web* de todo o Instituto de Engenharia Elétrica. Pode-se observar que esta situação pode produzir uma sobrecarga neste servidor, tornando precária a execução destes serviços.

4.3.6 Mudança do centro de operações

Segundo os usuários entrevistados, para otimizar e simplificar a resolução dos problemas de gerência e operação da rede, eles optaram pelo processo de centralização dos recursos de rede existentes.

Todos os servidores corporativos serão colocados em uma sala apropriada. Todos os serviços estarão sendo gerenciados e monitorados pelos administradores da rede com uma maior eficiência.

Com a topologia lógica descentralizada é comum usuários da rede não conseguirem acessar recursos disponibilizados em outros departamentos da UNIFEI.

Tanto a infra-estrutura da rede quanto as instalações elétricas não fornecem as características necessárias de confiabilidade, disponibilidade e gerenciabilidade essenciais para garantir o funcionamento adequado dos equipamentos de rede.

5 LEVANTAMENTO E ANÁLISE DAS CARACTERÍSTICAS DA REDE

O levantamento da situação atual da rede foi elaborado através de visitas realizadas aos blocos que compõem o Campus UNIFEI.

Os dados obtidos nesta pesquisa foram adquiridos com a ajuda dos administradores da rede. Os tópicos levantados sobre as características da rede são listados a seguir.

- Topologia da rede.
- Cabeamento de rede.
- Tecnologia de rede local.
- Dispositivos de rede.
- Endereçamento lógico ou de camada 3.
- Servidores corporativos e de grupo de trabalho.
- Política de segurança e plano gestor de informática.
- Caracterização do tráfego da rede UNIFEI.

5.1 Topologia da rede UNIFEI

A topologia utilizada pela universidade é a estrela estendida. Este tipo de topologia possui um nó central, onde se encontra atualmente um roteador Cisco 7200, localizado no prédio do CPD, conforme a figura 13.

Esta figura foi desenvolvida através das informações adquiridas junto aos funcionários responsáveis pela administração da rede e com a ajuda do *software Microsoft Visio*. Nesta figura são mostrados os equipamentos de rede, os servidores principais e o *backbone* principal.

O *link* de saída da instituição é composto por dois acessos distintos de 2Mbps, um pela RNP2 via Embratel e o outro acesso é fornecido por uma empresa local chamada Jetweb. Estes *links* estão conectados ao roteador Cisco 7200.

O *link* de saída via Embratel fornece conexão à Internet para três localidades, CPD, IEE e ICI. Todos os outros institutos e laboratórios são conectados à Internet pelo *link* da Jetweb.

O campus da universidade é constituído de oito blocos, que são interligados por fibra óptica multimodo, formando o *backbone* ou cabeamento principal da rede. Este cabeamento é o mais importante da rede, pois é o responsável por interligar todos os edifícios ao nó central da rede, no CPD.

Atualmente, o campus da universidade possui cerca de 1200 computadores ou estações de trabalho, que são utilizados pelos alunos, professores e os funcionários técnico-administrativos. A maioria desses computadores possui acesso à Internet.

5.2 Tecnologia de enlace de dados

A tecnologia de rede utilizada na universidade é a *Ethernet* e a *Fast Ethernet*. Alguns institutos estão conectados às interfaces *Fast Ethernet* do roteador e outros estão conectados às interfaces *Ethernet*, conforme apresentado na figura 13.

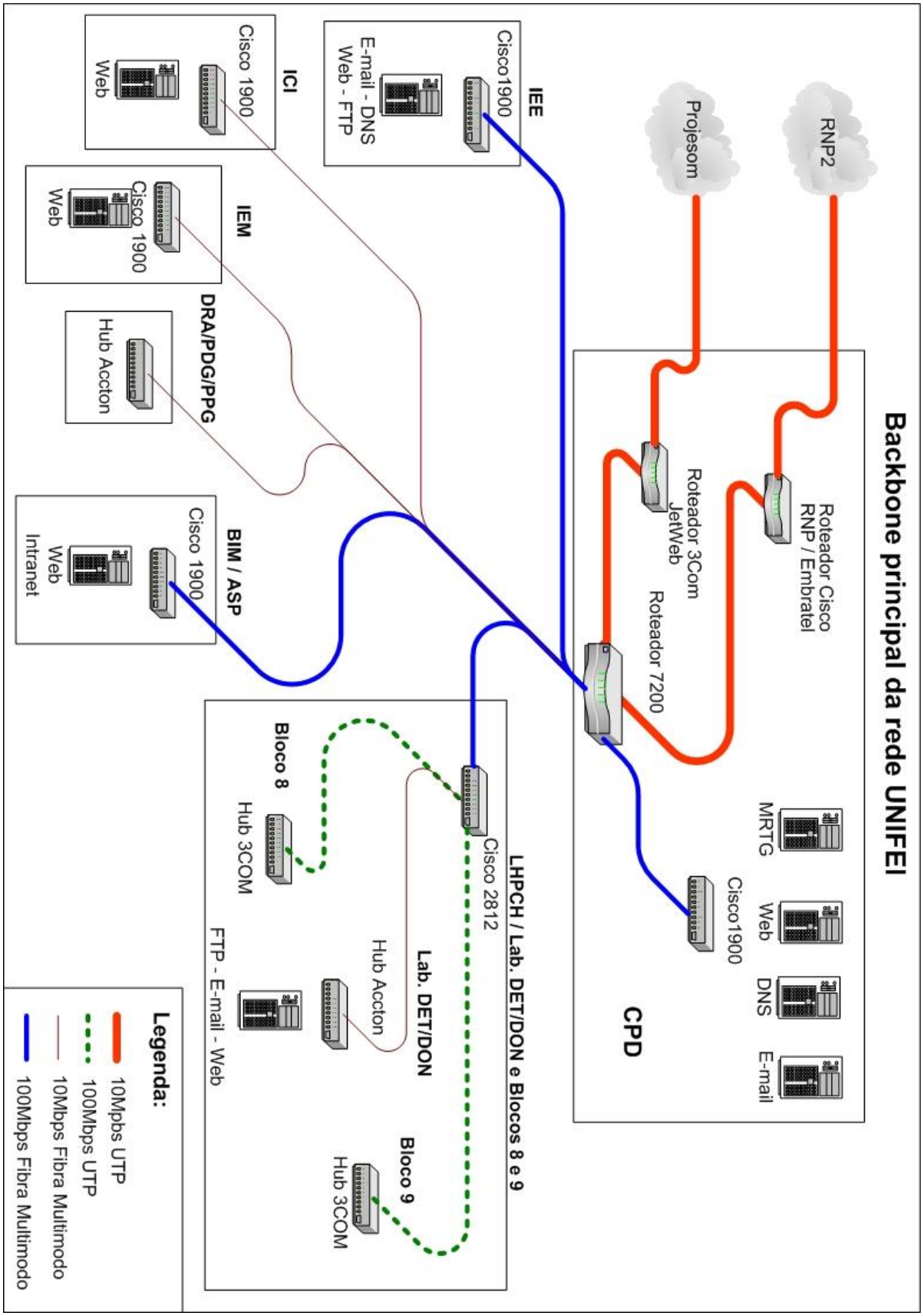

Figura 13 – Topologia atual do *backbone* da UNIFEI.

Os blocos conectados ao *backbone* com largura de banda de 100Mbps são:

- Instituto de Engenharia Elétrica.
- BIM/ASP - Este bloco contempla a reitoria, a biblioteca da UNIFEI, a assessoria de planejamento, o departamento de pessoal e o auditório da BIM.
- CPD - É o ponto central da rede, onde estão localizados os equipamentos mais importantes.
- LHPCH/Lab. DET/DON - O bloco LHPCH é conectado diretamente ao CPD, e os outros blocos se conectam na rede através dele.

  Os outros blocos que fazem parte deste segmento de rede são: bloco 8, bloco 9 e o Lab. DET/DON. O Laboratório DET/DON é conectado através de um *link* de fibra óptica de 10Mbps. Já os blocos 8 e 9 são conectados por cabo UTP com largura de banda de 100Mbps.

Os edifícios conectados ao *backbone* com largura de banda de 10Mbps são: Instituto de Ciências, Instituto de Engenharia Mecânica e o bloco DRA/PDG/PPG.

5.3 Cabeamento da rede UNIFEI

Conforme o levantamento realizado, a infra-estrutura e o cabeamento da rede não estão de acordo com as normas brasileiras e internacionais de cabeamento estruturado, principalmente o cabeamento horizontal. Foram constatadas diversas violações da norma como, por exemplo:

- Cabeamento fora da eletrocalha e da especificação mínima.
- Cabo de rede UTP enrolado junto ao cabo de energia elétrica, causando interferência no *link* UTP.
- Cabo UTP para uso interno sendo usado externamente (fora do edifício) sem qualquer tipo de proteção.
- Cabo de rede ocupando a mesma eletrocalha do cabo de energia elétrica, sem uma separação física adequada entre eles.

- Equipamentos de rede fora do *rack* de distribuição, não havendo uma infra-estrutura adequada.
- Falta de fontes redundantes de energia como, por exemplo, *no-breaks* para evitar que os dispositivos e os servidores de rede fiquem susceptíveis a quedas e picos de energia. Isto pode ocasionar danos ou interrupções nos serviços de rede.

5.4 Dispositivos de rede

Dentro de cada instituto, departamento ou laboratório existem diversos dispositivos de rede, em sua maioria *hubs*, que são responsáveis por conectar os *hosts* na rede.

A universidade possui outros equipamentos, mas para este trabalho foram considerados apenas aqueles que fazem parte do *backbone* principal. Os equipamentos que compõem o *backbone* são listados na tabela 1.

O equipamento mais importante da rede é o roteador Cisco 7200, pois ele é o responsável por interligar todos os edifícios do campus. Ele possui quatro interfaces *Fast Ethernet* e dez interfaces *Ethernet* de 10Mbps.

Outra funcionalidade deste equipamento são os filtros de pacotes, que são implementados através das listas de controle de acesso.

Outro serviço executado pelo roteador é o NAT. Este recurso permite que os *hosts* na rede interna da instituição utilizem IP privados na Internet, evitando a necessidade de adquirir grandes blocos destes endereços, além de aumentar a segurança das estações de trabalho e alguns servidores internos.

Segundo as informações adquiridas, a taxa atual de utilização do roteador encontra-se em torno de 15 a 20% de sua capacidade. Logo, conclui-se que este equipamento possui uma taxa de utilização menor do que ele pode suportar. Portanto, outras funcionalidades podem ser estabelecidas para ele executar como, por exemplo, as redes locais virtuais, o servidor de DHCP e o *traffic show*.

Em cada um dos nós finais da topologia central existe um equipamento de rede, chamado de *switch* de borda, que fornece conectividade ao instituto ou laboratório. Estes *switches* são conectados ao roteador através de uma fibra óptica.

Além dos *switches*, existem também alguns *hubs* responsáveis por interligar alguns blocos ao *backbone* da rede, conforme mostrado na figura 13.

Tabela 1 – Dispositivos de rede conectados ao *backbone* da UNIFEI.

Localização-Prédio	Equipamento	Modelo / Marca
DRA	*Hub*	Accton
CPD	*Switch*	Cisco 1900
CPD	Roteador	Cisco 7204
IEM	*Switch*	Cisco 1900
IEE	*Switch*	Cisco 1900
LHPCH	*Switch*	Cisco 2812XL
Blocos 8	*Hub*	3COM
Blocos 9	*Hub*	3COM
Lab. DET / DON	*Hub*	Accton
BIM / ASP	*Switch*	Cisco 1900
ICI	*Switch*	Cisco 1900

5.5 Endereçamento lógico

Como citado anteriormente, a universidade usa o esquema de endereçamento privado, ou seja, endereçamento não roteável na Internet. Este recurso é implementado no roteador através do *network address translation*.

Segundo a RFC 1631 [24], *Network Address Translation* ou tradução de endereço de rede é um mecanismo que permite, por exemplo, que máquinas com

endereços IP de redes privadas se comuniquem com máquinas na Internet, que possuem IP públicos.

Este recurso evita que a instituição tenha que adquirir grandes blocos de endereços IP públicos, além de aumentar a segurança das estações de trabalho e servidores internos.

Para cada bloco, conjunto ou instituto foi reservado uma faixa de endereços IP. O problema maior desta solução é a ausência de um planejamento visando o crescimento da rede. A tabela 2 mostra as faixas de endereço IP utilizadas.

Pela falta de planejamento na implementação da atual rede da universidade, pode-se observar que existem problemas de endereçamento lógico. Isto pode ser comprovado no instituto de engenharia elétrica, onde são usadas duas faixas distintas de endereçamento IP.

A mais antiga é a 10.10.3.0 /24, que com o tempo tornou-se pequena devido ao aumento no número de *hosts*. A outra faixa de endereços IP disponibilizada pela administração da rede é a 10.10.8.0 /24, para prover serviço aos novos usuários do instituto.

Tabela 2 – Esquema de endereçamento lógico.

Localização-Prédio	Endereçamento	Máscara
CPD	10.10.1.0	255.255.255.0
BIM / ASP	10.10.2.0	255.255.255.0
IEE	10.10.3.0	255.255.255.0
LHPCH / Blocos 8 e 9 / Lab. DET / DON	10.10.4.0	255.255.255.0
DRA / PDG / PPG	10.10.5.0	255.255.255.0
ICI	10.10.6.0	255.255.255.0
IEM	10.10.7.0	255.255.255.0
IEE	10.10.8.0	255.255.255.0

Portanto, é possível verificar que *hosts* próximos, pertencentes fisicamente à mesma rede, possuem endereços IP de redes diferentes. Este problema ocorre devido à falta de um plano de expansão da rede.

Outro problema encontrado na rede é a duplicação de endereços IP. Alguns usuários reclamaram que ao ligar seus micros, uma mensagem de erro aparecia na tela, dizendo que seu IP estava sendo utilizado por outro usuário. Este tipo de problema acontece quando se utiliza endereçamento estático ou fixo, que é o utilizado pela rede atual.

5.6 Servidores de rede

Conforme citado anteriormente, os servidores podem ser classificados como corporativos ou de grupo de trabalho. Na pesquisa realizada foram levantados todos os servidores existentes na rede, mas apenas os servidores corporativos de cada bloco, instituto ou laboratório possuem uma maior importância para este trabalho. Portanto, a meta principal desta proposta é centralizar os serviços e recursos de rede oferecidos a todos os usuários.

A tabela 3 mostra a relação dos servidores corporativos existentes na rede atual. Analisando estas informações pode-se constatar que existem alguns servidores corporativos prestando o mesmo serviço em institutos diferentes, logo, é possível concluir que há uma redundância nos serviços executados e conseqüentemente, um desperdício de recursos técnicos e humanos.

Um bom exemplo desta situação é o *Web Server*, que é fornecido por quase todos os institutos da universidade, conforme relata a tabela 3.

Geralmente, o serviço de hospedagem de páginas, função de um servidor corporativo, está sendo configurado em cada instituto como servidor de grupo de trabalho. Esta situação ocasiona um gasto desnecessário de recursos de informática, que poderiam estar sendo aproveitados para desempenhar outras funções e serviços na rede.

A proposta apresentada neste trabalho visa mostrar que na situação particular em que se encontra a universidade, a melhor opção é a centralização da rede. Esta idéia será abordada com mais detalhes posteriormente.

Outro ponto importante a ser comentado se refere ao ensino a distância. Este tipo de serviço deve ser fornecido por um servidor corporativo, e não por um servidor de grupo de trabalho.

O recurso de ensino a distância deve ser disponibilizado em um servidor corporativo no atual CPD, pois se trata de um serviço que todos utilizam, sejam eles usuários internos ou externos.

Tabela 3 – Relação de servidores corporativos.

Localização	Função	Modelo / Marca
CPD	*Web*	*SPARC 20* – SUN
	DNS e *e-mail*	*ULTRA 1* – SUN
	e-mail	*SPARC 20* – SUN
IEM	*Web*	*PC Pentium III* 800MHz
IEE	*Web,* DNS, FTP *e e-mail*	*ENTERPRISE 450* - SUN
Lab. DET / DON	FTP*, Web* e *e-mail*	*Pentium III* 900MHz
BIM / ASP	FTP*, Web e Intranet*	*PC COMPAQ PRO 1600*
ICI	*Web*	*PC Pentium III* 700MHz

Segundo o levantamento realizado pelos administradores da rede, com o auxílio do *software Nagios*, os atuais servidores estão com suas capacidades esgotadas.

Um exemplo claro desta situação é o servidor de correio eletrônico principal da rede, localizado no atual CPD, que está com uma taxa de utilização em torno de 90% de sua capacidade.

Isto vem reforçar os dados levantados no início deste trabalho, onde se constatou a situação crítica em que se encontram os servidores corporativos da rede UNIFEI, devido à falta de investimentos na atualização destes servidores.

5.7 Política de segurança e plano gestor de informática

Não há nenhuma política de segurança, muito menos algum estudo para o desenvolvimento de um futuro projeto de segurança da informação.

Quanto ao plano gestor de informática foi possível constatar que dentro da universidade não existe um plano de gestão para os recursos de informática, nem um planejamento de investimentos em recursos técnicos e humanos. O que existe na universidade são apenas ações pontuais e esporádicas buscando garantir a simples continuidade dos serviços de rede.

5.8 Caracterização do tráfego na rede

A análise do tráfego da rede foi executada através de pesquisas realizadas com os usuários e também com o auxílio dos *softwares* analisadores de protocolos, que captaram algumas sessões típicas para analisar as características atuais do tráfego da rede UNIFEI.

Foram utilizados alguns recursos técnicos, dentre os quais estão o *NetFlow*, MRTG e *Nagios* para levantar as informações sobre a utilização da largura de banda e os requisitos de qualidade de serviço da rede UNIFEI.

Os gráficos apresentados a seguir exibem o comportamento dos dois *links* de acesso à Internet. O período de monitoramento escolhido foi durante a segunda semana do mês de agosto desse ano. O recurso técnico utilizado para efetuar o levantamento destas informações foi o MRTG.

A figura 14 mostra a taxa de *download* e *upload* da interface do roteador Cisco 7200, que está conectada ao *link* de 2Mbps fornecido pela RNP/Embratel. Este *link* de saída para a Internet fornece acesso aos institutos IEE, ICI e, também, ao CPD.

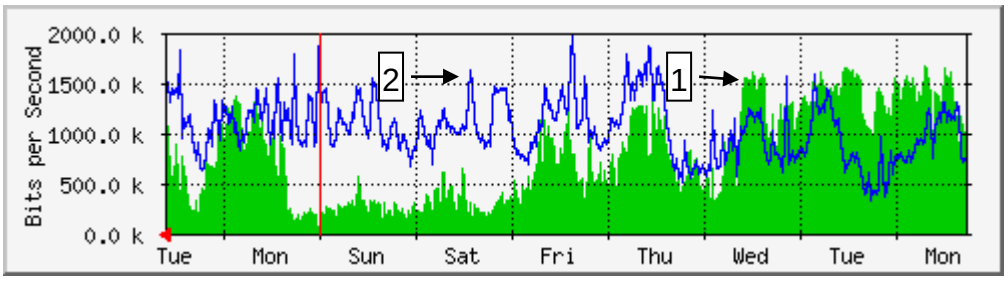

Figura 14 – Gráfico de utilização do link de saída RNP fornecido pelo MRTG.

A figura 15 mostra a taxa de *download* e *upload* da interface do roteador Cisco 7200. Esta interface está conectada ao *link* de 2Mbps fornecido pela empresa Jetweb, que fornece acesso à Internet aos outros institutos da universidade.

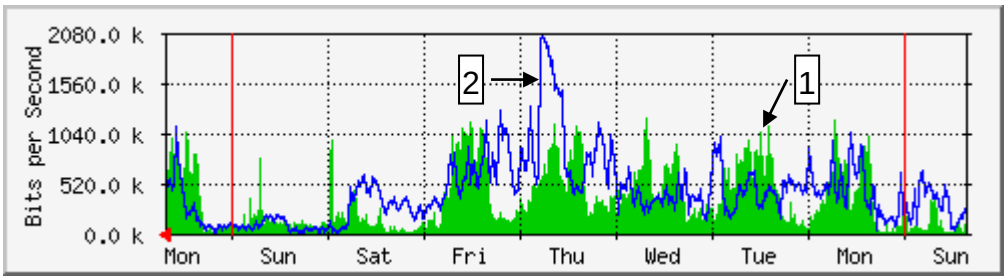

Figura 15 – Gráfico de utilização do link de saída Jetweb fornecido pelo MRTG.

Nas figuras 14 a 17, o gráfico 2 mostra a taxa de *upload* do referido *link*, que está saindo da rede interna. Já o gráfico 1 mostra a taxa de *download*, que está vindo da Internet e entrando na rede interna da universidade.

As figuras 16 e 17 apresentam os gráficos de utilização dos links de acesso à Internet fornecidos pela RNP e pela Jetweb. O período de monitoramento desses *links* compreende os últimos doze meses.

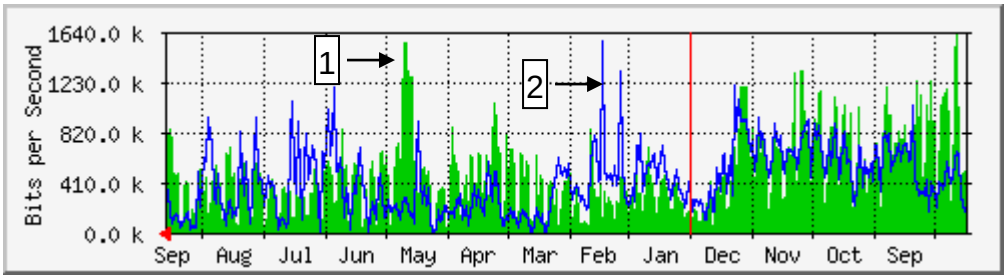

Figura 16 – Gráfico de utilização do link de saída Jetweb fornecido pelo MRTG.

Os gráficos apresentados nas figuras 16 e 17 representam a média diária, das taxas de *download* e *upload*, dos respectivos meses mostrados na escala do tempo.

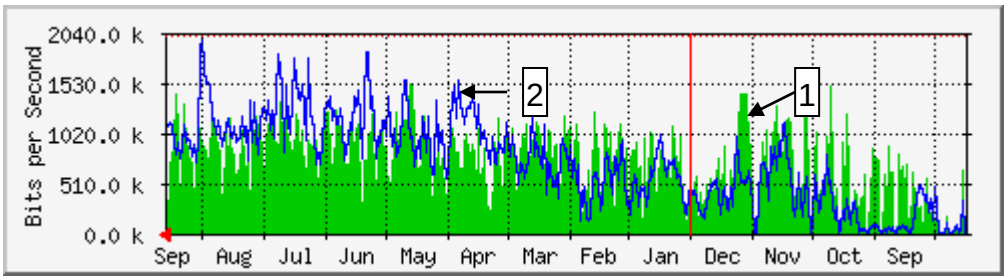

Figura 17 – Gráfico de utilização do link de saída RNP fornecido pelo MRTG.

Analisando os gráficos das figuras 14 a 17 pode-se observar que casualmente a comunicação na rede ultrapassa 2Mbps. Portanto, é possível concluir que:

- Os dois *links* de acesso à Internet são suficientes para atender a demanda de largura de banda dos usuários.
- A tecnologia de rede local *Ethernet* de 10Mbps, utilizada na universidade, atende aos requisitos de largura de banda da universidade e de seus usuários.
- A taxa de *upload* da rede é geralmente menor que a taxa de *download* e os gráficos mostram que estas taxas estão muito próximas.

  Esta observação é muito importante, pois está relacionada ao uso indevido de alguns aplicativos, por parte de alguns usuários mal intencionados, causando o baixo desempenho da rede. Existem outros problemas relacionados ao baixo desempenho da rede como, por exemplo, a alta incidência de vírus.

Com a utilização da tecnologia *NetFlow* foi possível obter diversas informações sobre o tráfego na rede. Através destas informações pode-se analisar o tráfego de entrada e saída da interface do roteador que conecta a rede do IEE ao *backbone* da universidade. Durante a segunda semana do mês de agosto, desse ano, a largura de banda ocupada pelos usuários do instituto foi em torno de 1Mbps.

Para analisar as informações fornecidas pelo *NetFlow* foram utilizadas algumas ferramentas *open source* como, por exemplo, o *FlowScan* responsável por gerar os gráficos pré-definidos e o *FlowTools,* que permitiu o levantamento, a detecção, o armazenamento e a verificação do tráfego dos usuários.

As informações mais relevantes sobre os aplicativos e protocolos mais utilizados pelos usuários foram:

- Os dois aplicativos que mais utilizaram a banda disponível foram o *BitTorrent* e o *e-mule*, que são aplicativos *peer-to-peer*. Cada aplicativo ocupou cerca de 30% da banda de *download* e *upload* do *link*, ou seja, 60% do tráfego gerado nesta rede corresponde ao uso de aplicativos que não são prioridade para os usuários. Estes aplicativos são utilizados para fazer *downloads*, por exemplo, de jogos e filmes.
- O tráfego de correio eletrônico ocupou cerca de 25% do *link* de *download* para o protocolo POP3 e, o aplicativo SMTP ocupou cerca 4% do link de *upload*.
- O aplicativo *Webmail* ocupou cerca de 3% do link de *download*. Este aplicativo é utilizado para acessar o correio eletrônico via *web browser*.
- Cerca de 90% do tráfego de correio eletrônico ocorre entre os usuários internos e usuários de outras instituições ou localidades.
- Apenas uma pequena parte dos usuários utilizou o navegador *web* para acessar os servidores *web* internos. A maioria dos usuários utilizou o navegador para acessar *sites* externos, na Internet.
- O protocolo http utilizou 11% do *link* de *download* e cerca de 1% do *link* de *upload*. Este protocolo é muito utilizado pelo *web browser*. Este protocolo também pode ser usado para o *download* de arquivos.
- O tráfego de FTP detectado nesta semana foi muito esporádico, ocupando cerca de 0,1% do *link*.

Analisando os dados fornecidos pode-se constatar que os atuais *links* de acesso à Internet atendem aos requisitos de largura de banda dos usuários.

Um dos maiores problemas de desempenho da rede e do acesso à Internet são os aplicativos *peer-to-peer*, que ocupam boa parte da largura de banda dos *links*.

Outro problema encontrado diz respeito aos equipamentos de rede, mais precisamente, aos *hubs*. Estes equipamentos aumentam o domínio de colisão e conseqüentemente, diminuem a largura de banda disponível por usuário e prejudicam o desempenho da rede.

Para solucionar estes problemas é imprescindível a universidade investir em um plano de investimento em tecnologia da informação. Esta proposta sugere a utilização de alguns equipamentos, que irão ajudar no gerenciamento da rede e na segurança da informação.

6 PROJETO DE REDE LÓGICA

Nesta etapa será desenvolvida uma proposta de uma topologia de rede lógica, um modelo de endereçamento de camada 3 e uma proposta inicial para um projeto de segurança e de gerenciamento da rede da universidade.

Depois de analisar as metas da UNIFEI e a caracterização do tráfego da rede atual é muito importante desenvolver a arquitetura da topologia lógica, antes de escolher os equipamentos e tecnologias físicas de rede. Esta topologia fornece uma visão geral de como será a interligação dos equipamentos, sem se preocupar com o tipo de meio físico e quais serão os equipamentos a serem utilizados.

As redes que crescem sem um planejamento tendem a se desenvolver de maneira desestruturada. Este trabalho usa o modelo hierárquico para desenvolver a topologia lógica da rede da universidade.

O modelo hierárquico utiliza o desenvolvimento em camadas para simplificar as tarefas necessárias para a interligação de uma rede. Cada camada pode se concentrar em funções específicas, permitindo que sejam escolhidos os recursos corretos para cada camada [1].

A modularidade no projeto de uma rede permite manter cada parte do projeto simples e fácil de entender. A simplicidade diminui a necessidade de capacitação extensiva para os operadores da rede e acelera a execução de um projeto.

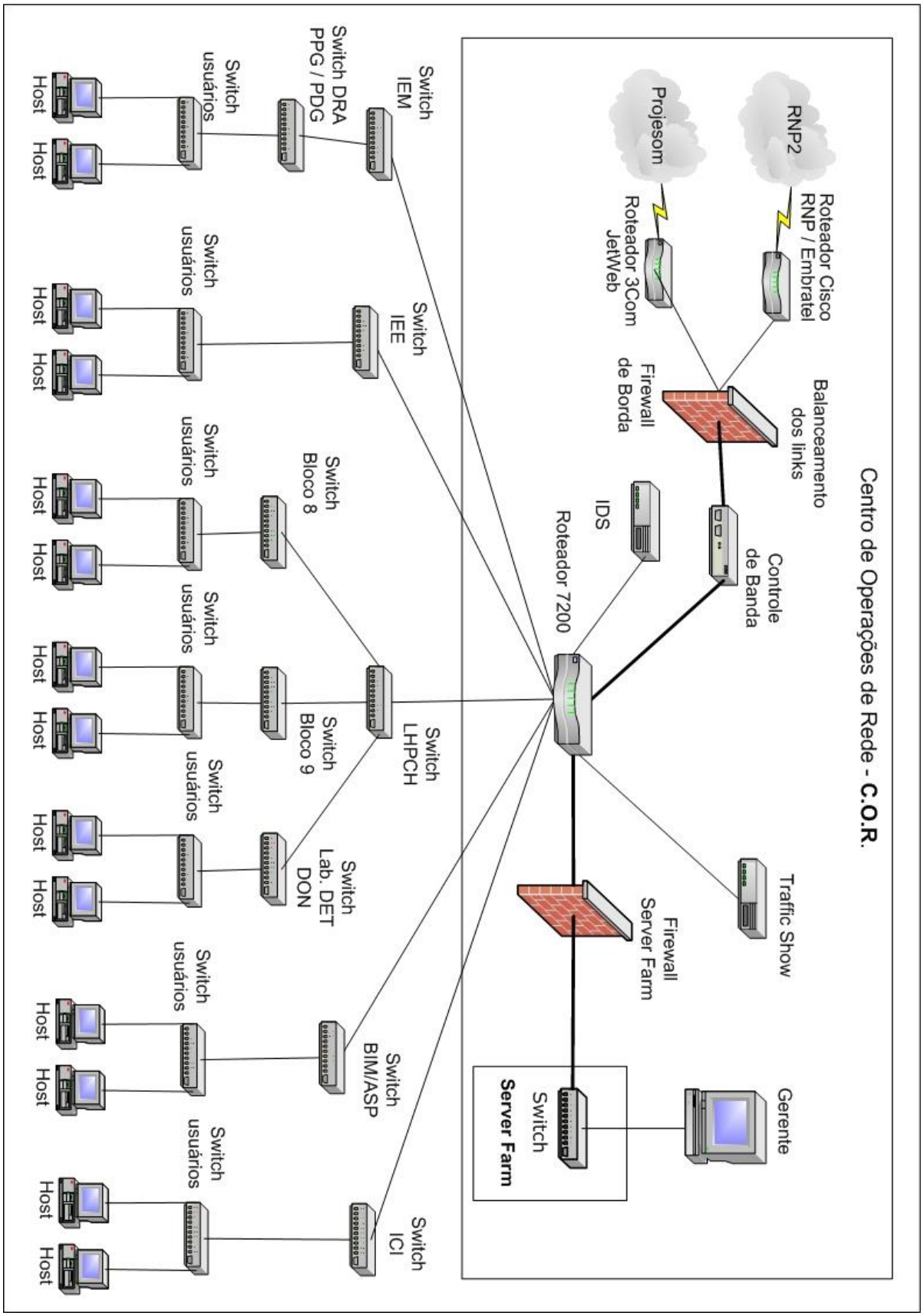

Figura 18 – Proposta da topologia lógica para a rede UNIFEI.

6.1 Projeto da topologia lógica

Após analisar as metas e restrições dos usuários e também o comportamento dos aplicativos atuais e futuros, foi proposta uma nova topologia lógica para a rede da universidade, conforme a figura 18.

Pode-se observar que a topologia proposta não difere muito da topologia atual, pois uma das metas desta proposta é aproveitar ao máximo os recursos disponíveis. As principais mudanças na topologia são:

- Mudança física da administração da rede para o prédio da biblioteca, próximo à reitoria. Esta nova localidade receberá o nome de Centro de Operações de Redes (COR).
- O acesso à rede do bloco DRA/PPG/PDG será fornecido pelo IEM, que será conectado diretamente ao cabeamento de *backbone*. O acesso dos laboratórios no CPD à rede será fornecido pelo IEM - Instituto de Engenharia Mecânica, conforme mostra a figura 18.
- Outra mudança proposta é a utilização de VLANs. Para isto será necessária a substituição gradual dos *hubs* por *switches*.
- Implementação dos equipamentos que irão ajudar no gerenciamento e monitoramento da rede e também na segurança da informação.
- Os equipamentos dos provedores de acesso à Internet, mostrados na figura 18, serão deslocados para o mesmo local onde será criado o *Server Farm* e a sala dos equipamentos de rede.

6.1.1 Redes locais virtuais

Para garantir as metas de disponibilidade e segurança da rede foi proposto o uso de VLANs ou redes virtuais. Utilizando este recurso será possível implementar algumas metas dos usuários como, por exemplo, a segmentação da rede por classe de usuário e maior segurança para os professores, que necessitam de uma rede separada da rede utilizada pelos alunos.

Nesta proposta são criados três grupos distintos de usuários: professores, alunos e funcionários.

- VLAN_1: rede virtual dos professores.
- VLAN_2: rede virtual dos funcionários técnico-administrativos.
- VLAN_3: rede virtual dos alunos da universidade.

Para complementar o uso das VLANs, pode-se considerar o seguinte esquema de comunicação entre elas:

- VLAN_1 terá acesso a VLAN_2 e VLAN_3.
- VLAN_2 não se comunicará com a VLAN_3 nem com a VLAN_1.
- VLAN_3 não se comunicará com a VLAN_1 nem com a VLAN_2.

A comunicação entre as redes locais virtuais é realizada através do roteador. Portanto, este recurso será implementado no roteador com o auxílio das listas de controle de acesso.

6.1.2 Cabeamento de backbone redundante

Como citado anteriormente, a universidade pretende mudar a administração da rede de lugar. Esta administração irá mudar do atual prédio do CPD para o 2º andar do prédio da Biblioteca Mauá, onde está sendo construído o centro de operações de redes da universidade.

Todo o *backbone* principal, que interliga os institutos e laboratórios, terá que ser reestruturado. Aproveitando a mudança, esta proposta vem sugerir a implantação de um outro *backbone* para servir com um *link* redundante prevenindo assim, problemas de interrupção nos serviços de rede.

6.1.3 Redundância dos servidores

Como este trabalho propõe uma solução centralizada para a rede da universidade, deve-se pensar em utilizar redundância de servidores a fim de manter uma disponibilidade dos serviços aos usuários.

A redundância possui vantagens de disponibilidade e desempenho, pois com os servidores de arquivos espelhados, por exemplo, pode-se compartilhar a carga de trabalho entre os servidores, se for necessário.

Os serviços oferecidos pelos servidores corporativos são os mais aptos a tornarem-se redundantes ou espelhados, pois são oferecidos para todos os usuários da rede.

Se por algum motivo a redundância de servidores não for possível, pode-se utilizar outro recurso como a duplexação ou espelhamento do disco rígido. A duplexação tem uma vantagem a mais sobre o espelhamento, pois os discos rígidos são conectados em controladoras distintas ao contrário do espelhamento [1].

Os servidores corporativos implementados nesta proposta serão apresentados posteriormente. A alocação de um serviço corporativo por servidor visa atender as metas de disponibilidade e segurança da informação.

6.2 Projeto de endereçamento de camada 3

Este tópico aborda a importância de um modelo de endereçamento da camada de rede. Sem este planejamento, torna-se fácil esgotar os endereços, inserir endereços duplicados, além de dificultar o gerenciamento da rede. Estes tipos de problemas já foram citados anteriormente pelos usuários.

No planejamento proposto serão utilizados alguns serviços que já estão em uso na universidade como, por exemplo, o uso de endereços privados e o NAT.

Atualmente, alguns institutos e grupos de estudo utilizam servidores DHCP para atribuir IP aos seus *hosts*. Uma das metas deste trabalho é disponibilizar este recurso para todos os usuários da rede.

6.2.1 Endereçamento dinâmico

Esta proposta utiliza um servidor corporativo DHCP e também um servidor redundante para este serviço. Este serviço utilizará o método de alocação dinâmica de endereços IP.

Atualmente, a universidade adota a faixa de endereço privado 10.10.0.0. Esta proposta utiliza a mesma faixa, mas com uma máscara de sub-rede diferente.

O endereçamento dinâmico irá reduzir as tarefas de configuração dos *hosts* automatizando assim, o processo de configuração do protocolo TCP/IP.

Esta automação tornará o suporte de rede mais eficiente e menos penoso para os administradores, pois atualmente a equipe de suporte da universidade é muito pequena.

6.2.2 Planejamento de Endereços IP

Com o intuito de cumprir as metas de facilidade de escalonamento e de gerenciamento, foram utilizadas algumas diretrizes para permitir a elaboração deste planejamento de forma adequada. Estas diretrizes são:

- Projeto de um modelo de endereçamento estruturado, mostrado na tabela 4. Este modelo visa atender uma futura expansão da rede da universidade.

  Cada instituto terá uma faixa de endereços muito maior que suas necessidades atuais. Cada faixa de endereços terá a capacidade de endereçar até 1022 *hosts*.

- Utilização do esquema de endereçamento dinâmico, a fim de otimizar a flexibilidade e diminuir a necessidade de configuração dos *hosts*.

- Com o intuito de melhorar a segurança e a adaptabilidade, será utilizado o endereçamento privado em conjunto com a tradução de endereços de rede.

- Além destas diretrizes será necessário também, elaborar uma documentação clara e objetiva com o intuito de facilitar a administração e solução de problemas na rede.

Tabela 4 – Modelo de endereçamento lógico.

Localização-Prédio	Endereçamento	Máscara
BIM / ASP	10.10.4.0	255.255.252.0
IEE	10.10.8.0	255.255.252.0
LHPCH / Blocos 8 e 9 / Lab. DET / DON	10.10.12.0	255.255.252.0
ICI	10.10.16.0	255.255.252.0
IEM / DRA / PDG / PPG	10.10.20.0	255.255.252.0

6.3 Proposta de um projeto de segurança da rede

Entre os aspectos de um projeto de rede lógica, os mais importantes são a segurança e o gerenciamento de redes. Estes aspectos costumam ser negligenciados na elaboração de um projeto, por se tratarem de assuntos operacionais ao invés de temas de projeto.

A segurança da rede, tanto física como lógica, é um tema muito importante atualmente, pois com o aumento das atividades que dependem das redes internas e da Internet surgiram também, os diversos tipos de ataques praticados por usuários maliciosos como, por exemplo, os *crackers, hackers* e até mesmo usuários internos mal intencionados ou mal orientados. Entre as etapas de um projeto de segurança, as mais relevantes são [1]:

- **Identificação dos ativos de rede**. Esta identificação inclui os *hosts*, equipamentos de rede e as informações que trafegam por essa rede.
- **Análise das metas de segurança**. Estas metas são assumidas em conjunto com as metas de disponibilidade, adaptabilidade, desempenho e gerenciabilidade.
- **Desenvolvimento de um plano de segurança**. Este plano estabelece as diretrizes que a universidade deve seguir para atingir as metas de segurança.

Este plano deve ter o comprometimento dos funcionários, professores e alunos da universidade.

- **Definição da política de segurança**. Esta norma é um conjunto de leis e regras, que os usuários com acesso à rede e aos ativos da universidade devem obedecer.
- **Conseguir o comprometimento dos alunos, funcionários e professores em torno do projeto de segurança**. Não adianta impor a política de segurança se não houver o comprometimento de todos os usuários. Só assim este projeto terá sucesso.

O objetivo principal deste tópico é mostrar a importância do desenvolvimento de um projeto de segurança para a universidade. Nesta proposta foram desenvolvidas algumas soluções de segurança, mas enfatizando apenas o lado físico ou do desenvolvimento de soluções técnicas de segurança. Os equipamentos utilizados são:

- ***Firewall***

  Nesta proposta são utilizados dois *firewalls* baseados em *stateful packet filter*, conforme mostra a figura 19. Um deles é o *firewall* de borda e o outro, o *firewall* do *Server Farm*.

- **Sistemas de detecção de intrusos**

  Nesta proposta será implementado o IDS baseado em rede, para conseguir uma maior abrangência e proteção da rede.

- ***Software* antivírus com distribuição livre**

Os administradores da rede já utilizam um *software* antivírus de distribuição livre para verificar o tráfego de correio eletrônico dos usuários.

6.3.1 Firewall

Segundo Nakamura [20], um *firewall* pode ser definido como sendo um ponto de ligação entre duas ou mais redes, podendo ser um componente ou um conjunto de componentes, por onde passa todo o tráfego, permitindo a realização do controle, autenticação e os registros de todo o tráfego.

Sendo assim, o melhor lugar para se colocar um *firewall* é a divisa entre uma ou mais redes, obtendo um melhor aproveitamento de suas funções e, conseqüentemente, evitando as tentativas de invasão entre os pontos conectados pelo *firewall.*

Este dispositivo de rede pode ser baseado em *static filter* (filtro de pacotes), *proxy filter* ou em *stateful packet filter* (filtros de pacotes baseados em estados) [25, 26].

6.3.1.1 Firewall baseado em static filter

O *firewall* baseado em *static filter* trabalha nas camadas 3 e 4 do modelo OSI. Portanto, as decisões de filtragem se baseiam nas informações contidas nos cabeçalhos da camada de rede e de transporte, onde estão os endereços IP e as portas de serviço.

Filtro de pacotes são listas de controle de acesso que observam cada pacote que entra e sai de uma rede. Este recurso já é utilizado na instituição pela administração da rede. Estas listas são aplicadas nas interfaces do roteador Cisco 7200. Elas informam ao roteador que tipos de pacotes devem ser aceitos ou recusados.

A aceitação e a recusa podem ser baseadas em certas especificações, por exemplo, endereço IP de origem ou de destino, porta de serviço de origem ou de destino e também, podem ser baseadas em protocolos.

6.3.1.2 Firewall baseado em proxy filter

No *firewall* baseado em um *proxy filter*, o usuário deve primeiramente se conectar ao *firewall.* Após o *proxy server* autenticar o usuário é que sua conexão

com a Internet estará liberada, porém com o endereço IP do *firewall*, mascarando assim, o endereço IP do usuário interno.

O servidor *proxy* é colocado entre uma rede interna e a externa. Se por exemplo, um usuário interno desejar navegar em um *web site*, será criada uma sessão com este servidor, que irá requerer uma autenticação. Esta implementação de *firewall* se comporta como uma barreira entre os usuários internos de uma rede e o mundo externo, protegendo assim, esses usuários de ataques externos.

6.3.1.3 Firewall baseado em stateful packet filter

Segundo Nakamura [20], os *firewalls* baseados em *stateful packet filter* tomam as decisões de filtragem tendo como referência dois parâmetros:

- As informações dos cabeçalhos de camada 3 e 4.
- Uma tabela de estados, que guarda os estados de todas as conexões.

Os *firewalls* baseados em estado são capazes de manter o rastreamento de sessões de rede. Quando um pacote ACK for recebido, este dispositivo determinará sua legitimidade comparando o pacote com a correspondente entrada na sua tabela de estados.

Uma entrada é criada quando um *firewall* detecta o primeiro pacote SYN, que inicializa uma sessão TCP. Esta entrada é referenciada para os pacotes sucessivos e podem ser automaticamente expiradas depois de um tempo de *timeout* configurável.

Esta implementação de *firewall* fornece a melhor solução entre os métodos apresentados. Esta solução oferece maior desempenho e reduz a exposição ao ataque externo.

Por manter informações sobre os estados das sessões da camada de rede, de transporte e da camada de aplicação, esta implementação pode prover uma filtragem mais eficiente que os filtros de pacotes e melhor desempenho que os *proxy filters*.

6.3.2 Sistemas de detecção de intrusão – IDS

Segundo a RFC 2828 [27], um sistema de detecção de intrusão é definido como sendo um serviço que monitora e analisa eventos de uma rede, com o intuito de encontrar e fornecer alertas em tempo real de acessos não autorizados aos recursos da rede.

O IDS pode ser definido como um programa ou sistema, que está permanentemente em segundo plano e, de maneira imperceptível para o usuário comum, monitorando o tráfego de uma rede a procura de indícios de invasões. No caso de encontrar algo suspeito, este dispositivo acionará as rotinas pré-definidas pelos administradores da rede, a fim de inibir este acesso não autorizado.

A primeira linha de defesa desta proposta é fornecida pelo *firewall* de borda. Uma segunda linha de defesa, baseada em um sistema de detecção de intrusão, é apresentada com o objetivo de fornecer uma maior proteção e o monitoramento do tráfego interno e externo.

Um IDS pode ser essencialmente classificado como *host-based* (baseado em *host*) ou *network-based* (baseado em rede).

6.3.2.1 Sistema de detecção de intrusão baseado em host [28-31]

O IDS baseado em *host* possui a finalidade de monitorar um sistema e caracterizar uma possível intrusão, com base em informações dos registros do sistema ou de arquivos de *logs*. Se uma ocorrência de intrusão for detectada, o IDS irá informar ao administrador de segurança da rede que foi encontrado um comportamento fora do padrão, e em que ele se baseou para detectar esse comportamento.

Esta implementação de IDS pode monitorar os acessos e alterações ocorridas nos arquivos de sistema, a taxa de utilização da CPU, as modificações nos privilégios de usuários, a execução dos programas, a integridade dos arquivos e a detecção de *port scanning*. Algumas das vantagens de um IDS baseado em *host* são:

- Detecção de ataques que utilizam criptografia.

- Pequena emissão de alertas “falsos positivos” para os administradores, ou seja, alarmes falsos de invasões ou ataques.
- Pode ser utilizado em redes separadas por *switches*.
- Não precisa de hardware adicional.

Mas este tipo de IDS possui também algumas desvantagens que devem ser consideradas, tais como:

- Não consegue detectar ataques de rede como, por exemplo, o *scanning* de rede.
- Proporciona uma diminuição do desempenho no *host* monitorado.
- Esta implementação está sujeita ao tipo de sistema operacional. Por exemplo: um *host-based* IDS utilizado no *Unix* é bem diferente de outro que funciona no *Windows*.

6.3.2.2 Sistema de detecção de intrusão baseado em rede – NIDS [28-32]

O sistema de detecção de intrusos baseado em rede monitora o tráfego de um segmento de rede, geralmente com o auxílio do recurso de espelhamento de portas. Este recurso permite ao NIDS capturar todo o tráfego da rede e, em seguida, analisá-lo para poder descobrir possíveis ataques.

Portanto, a detecção de intrusos é obtida com essa captura em conjunto com a análise em tempo real do conteúdo dos pacotes de dados, que são checados com os padrões conhecidos. Algumas das vantagens de um IDS baseado em rede são:

- A invasão pode ser detectada e identificada em tempo real e o administrador pode decidir o tipo de resposta adequada a ser dada.
- Não prejudica o desempenho da rede.
- O monitoramento pode ser fornecido a várias plataformas.
- Não permite ao invasor descobrir facilmente se existe algum sistema de detecção de intrusos implementado na rede.

Porém, este tipo de IDS possui algumas desvantagens que devem ser consideradas, tais como:

- Não consegue monitorar um tráfego de dados criptografados.
- Possui certa dificuldade em monitorar redes muito segmentadas.

Há basicamente dois métodos que podem ser utilizados por um IDS para a detecção de intrusão: um denominado A*nomaly Detection System* e o outro M*isuse Detection System*.

O método *Anomaly Detection System* é baseado em um padrão normal de comportamento do tráfego dos usuários ou do sistema. Quando o IDS captura um pacote de dados que não é compatível com o padrão estabelecido, este pacote será considerado uma anomalia ou intrusão.

Portanto, este método se baseia nos desvios de comportamento dos usuários ou do sistema para definir uma possível intrusão.

O método *Misuse Detection System* baseia-se na comparação do tráfego de dados na rede com as assinaturas de ataques conhecidos, armazenados em um banco de dados.

O funcionamento de um IDS baseado neste método é muito parecido com o funcionamento de um *software* antivírus. Assim, para fornecer uma proteção adequada é necessário ter uma base de dados sempre atualizada.

6.3.3 Antivírus

De forma geral, um vírus é um tipo de *software* cuja finalidade é prejudicar a operação de uma rede ou de um usuário. Os vírus, *worms* e *trojans* são ameaças constantes às empresas e instituições [5].

Os *worms* diferem dos vírus por se espalharem mais rapidamente e de maneira automática, não precisando de uma interação com o usuário, como acontece com o vírus.

O *trojan* ou cavalo de Tróia é um *software* destrutivo disfarçado de jogo, utilitário ou de algum aplicativo. Quando executado, o *trojan* faz algo danoso ao sistema de um *host* enquanto parece estar fazendo algo útil.

O *software* antivírus é uma ferramenta muito importante para a administração da rede. O funcionamento de um *software* antivírus é baseado na comparação da assinatura do *software* suspeito com as contidas na base de dados do antivírus. Portanto, esta base de dados deve ser atualizada constantemente, se possível diariamente.

6.4 Proposta de um projeto de gerenciamento da rede

Segundo a ISO [33], o gerenciamento de redes fornece mecanismos para o monitoramento, controle e coordenação dos recursos em um ambiente OSI e também, define padrões de protocolo OSI para a troca de informações entre estes recursos.

O gerenciamento da rede é uma das ferramentas mais importantes para monitorar e solucionar diversos problemas da rede. O monitoramento da rede durante a sua operação normal pode descobrir problemas em potencial, melhorar o desempenho e planejar atualizações.

6.4.1 Processos de gerenciamento de redes

Segundo a ISO [34], o gerenciamento é dividido em cinco processos de administração de rede:

- **Gerenciamento de falhas**

  Responsável por detectar, isolar, diagnosticar e corrigir os problemas, que afetam a comunicação de dados através da rede, podendo encontrá-los tanto em *hardware* quanto em *software*.

- **Gerenciamento da configuração**

  Ajuda o administrador de rede a controlar e a manter informações sobre como os equipamentos estão configurados. Este gerenciamento permite ao gerente criar e manter uma documentação dos ativos de rede, e, obter um registro das versões dos sistemas operacionais ou aplicativos em execução nos equipamentos de rede.

- **Gerenciamento de contabilidade**

  Administra a taxa de utilização de cada recurso de rede, que está sendo usado por um determinado instituto ou usuário. Este recurso é muito útil para descobrir os usuários que “abusam” da rede.

  Este tipo de processo de administração da rede é implementado nesta proposta através dos dispositivos: *traffic show* e controle de banda.

- **Gerenciamento de desempenho**

  Permite monitorar o comportamento e a eficiência da rede. Este tipo de processo de gerenciamento abrange a análise dos aplicativos, acessibilidade e o comportamento dos protocolos. A administração de rede visa garantir a qualidade de serviço, mas antes, tenta obter os menores custos possíveis para realizar esta tarefa.

- **Gerenciamento de segurança**

  Permite ao administrador manter e distribuir senhas e outras informações de autorização e autenticação. Este gerenciamento abrange os processos para criar, distribuir e armazenar chaves de criptografia. Portanto, este processo controla toda forma de monitoração e controle de informações sigilosas, que trafegam pela rede. Neste tipo de gerenciamento que se encaixam os equipamentos propostos como, por exemplo, o firewall e o IDS.

6.4.2 Dispositivos de gerenciamento da rede

Os recursos de rede são finitos, valiosos e precisam ser utilizados da melhor maneira possível. Neste trabalho foram apresentadas algumas soluções para atingir

as metas de gerenciamento da rede. Os dispositivos que irão auxiliar o gerenciamento da rede da universidade são: *traffic show*, o controle de banda e o balanceamento de carga dos *links*.

Estes dispositivos irão trabalhar em conjunto, visando garantir uma melhor utilização do b*ackbone,* um controle de banda eficiente e um melhor gerenciamento e monitoramento da rede.

6.4.2.1 Traffic show [35, 36]

Devido ao crescimento da rede, a interpretação das estatísticas referentes à utilização da rede tornou-se mais complexa. Com a utilização desta ferramenta é possível obter uma melhor interpretação das informações e conseqüentemente, criar uma definição de quais configurações e parâmetros serão adotados no controle de banda.

Esta ferramenta fornece um recurso de engenharia de tráfego baseado em *accounting,* mostrando como e onde o tráfego de IP flui na rede, no intuito de aperfeiçoar os recursos e oferecer suporte para soluções de gerenciamento como o *billing*. Para gerar os dados a serem analisados, pode-se utilizar basicamente dois tipos de ferramentas: *NetFlow Exports* ou *FlowScan*.

A primeira é o *NetFlow Exports*, que é uma poderosa ferramenta para o monitoramento de redes, criado pela Cisco *Systems*, mas uma solução proprietária. A outra ferramenta é o *FlowScan*, que é uma solução *open source.*

Baseado nas informações geradas no formato *NetFlow*, o *traffic show* retorna diversas informações, tais como, o endereço IP de origem e destino, porta de origem e destino, quantidade de tráfego gerado por determinado endereço IP, entre outras.

Estes dados são de fundamental importância para determinar como estão sendo utilizados os recursos de rede e também, verificar se o *link* está sendo usado para fornecer aos seus usuários disponibilidade e um bom desempenho no acesso à Internet.

Esta solução é muito útil para se detectar problemas com *worms* como, por exemplo, *Blaster*, *Mydoom* ou *Sasser*.

6.4.2.2 Controle de banda [35-37]

Em um ambiente com acesso a diversos recursos, existe um problema muito sério na rede: o uso abusivo e desleal dos recursos de rede. Isto ocasiona um baixo desempenho no acesso dos usuários, que utilizam a rede para acessar páginas *web*, ler e enviar seus *e-mails*.

A utilização abusiva e desleal de alguns recursos baseia-se principalmente em aplicativos *peer-to-peer*. Nestes aplicativos a taxa de recepção está vinculada à taxa de transmissão.

Portanto, para se efetuar um *download* de um arquivo qualquer, por exemplo, um filme ou um jogo, tem-se que habilitar o *upload* deste arquivo ou de outros que se encontram em uma pasta de compartilhamento, utilizada por esses tipos de aplicativos.

Conforme citado na caracterização do tráfego atual da rede, estes aplicativos ocupam uma parcela muito grande dos *links* de Internet. Logo, o tráfego destes aplicativos *peer-to-peer* acarreta uma alta taxa de perda de pacotes e um *delay* alto na rede.

Uma das idéias principais desta proposta não é bloquear o acesso a estes aplicativos, mas adotar uma política de priorização do tráfego, dando maior prioridade aos aplicativos que atendam aos requisitos da universidade e dos usuários.

Com o intuito de oferecer uma solução diplomática para este problema, esta proposta sugere a utilização de um dispositivo, que irá priorizar e limitar o uso dos *links* de saída para a Internet, baseado em dados obtidos pelo *traffic show*.

Deste modo, com o auxílio do *traffic show* será possível descobrir quais usuários estão utilizando aplicativos *peer-to-peer*. Pode-se com isso criar regras e políticas, que serão implementadas no equipamento de controle de banda.

6.4.2.3 Balanceamento de Carga nos links [35]

Através de análises da utilização dos *links* de acesso à Internet, verificou-se que a divisão do tráfego não tem ocorrido de forma simétrica ou de maneira dinâmica. Por essa razão, pode-se verificar muitas vezes que enquanto um *link*

estava com sua taxa de ocupação máxima, o outro funcionava com uma taxa de utilização bem inferior ao máximo aceitável.

Conseqüentemente, isso origina não só uma perda de desempenho, mas também, a má utilização dos recursos de rede empregados para garantir um bom desempenho do acesso à Internet.

Visando diminuir ou até mesmo erradicar esse problema, esta proposta sugere a instalação de um sistema para o balanceamento de carga entre os dois *links*. Este recurso será implementado no *firewall* de borda, e irá permitir uma melhor distribuição do tráfego da rede entre os dois *links* disponíveis na universidade.

7 PROJETO DA REDE FÍSICA

Esta etapa inclui a elaboração de uma topologia da rede física, a escolha do tipo de cabeamento a ser implantado, a seleção da tecnologia de rede local e também, dos equipamentos de rede a serem utilizados nesta proposta de reestruturação.

7.1 Cabeamento da rede UNIFEI

O projeto de cabeamento da rede, e também da infra-estrutura para suportar este cabeamento deve ser cuidadosamente elaborado, pois sua importância é essencial no cumprimento das metas de disponibilidade e facilidade de escalonamento desta proposta [1].

A maioria do cabeamento horizontal, que a universidade utiliza, é categoria 5 ou 5e, mas uma pequena parcela, em alguns institutos, ainda é de categoria 3. Portanto, este cabeamento categoria 3 é inferior aos padrões adotados pelas normas de cabeamento.

Nesta proposta, o cabeamento de rede segue basicamente as mesmas diretrizes atuais de utilização na universidade, com algumas ressalvas, por exemplo, a recomendação de troca dos cabos categoria 3 para categoria 5e.

Portanto, a fibra óptica será utilizada para interligar os prédios no campus da universidade ao ponto central da topologia, conforme a figura 19. Já para interligar os *hosts* aos equipamentos de rede, nos armários de telecomunicações, será utilizado o cabeamento UTP categoria 5e.

7.2 Tecnologia de rede local

A tecnologia de rede local, que a universidade utiliza é o *Ethernet*. Como esta proposta busca satisfazer os requisitos e restrições da universidade, optou-se por manter a tecnologia de rede já implementada. Além desta característica, foram levadas em conta as vantagens da tecnologia *Ethernet* em relação às outras tecnologias LANs existentes.

Atualmente a tecnologia *Ethernet* de 10Mbps compartilhada, implantada na universidade, é suficiente para suprir as necessidades dos usuários, conforme constatado no levantamento e análise dos requisitos e na análise do tráfego da rede. Portanto, não há motivos convincentes para despender recursos financeiros na troca de alguns equipamentos por outros mais novos.

Para garantir as metas de disponibilidade e segurança dos usuários foi escolhida a tecnologia *Ethernet* comutada ou ponto a ponto. Pode-se perceber que alguns institutos estão conectados ao backbone por *links* de 100Mbps e outros por *links* de 10Mbps, conforme mostra a figura 19.

Portanto, antes de escolher qual tecnologia e quais equipamentos seriam utilizados, foi possível descobrir as reais necessidades da universidade. Com isto, constatou-se que dos atuais equipamentos, alguns deles atendem às necessidades desta proposta de reestruturação da rede. Esta descoberta é sem dúvida uma das principais vantagens da elaboração de um projeto em camadas.

7.3 Projeto da topologia física

O roteador Cisco 7200 é o responsável por interligar todos os prédios ao *backbone* da rede e assim, tornando-se o elemento central da topologia em estrela estendida.

Este equipamento também será responsável por interligar os servidores corporativos, os equipamentos de segurança e de gerenciamento de rede e também, os dois *links* de acesso à Internet ao *backbone* principal da rede, conforme mostra a figura 19.

Como citado anteriormente, com a idéia de se utilizar o recurso de VLAN, todos os *hubs* da rede da universidade terão que ser gradativamente trocados por *switches*. Com isto, outra funcionalidade do roteador será dar suporte à comunicação entre as VLANs.

Os institutos de engenharia elétrica e mecânica e também, o laboratório LHPCH são conectados às interfaces de 100Mbps do roteador, pois a maior concentração de *hosts* está nestes locais.

Outro dispositivo conectado na última interface de 100Mbps do roteador é o firewall *Server Farm*. Este equipamento irá conectar todos os servidores corporativos à rede da universidade. Todos os outros prédios do campus serão conectados em cada uma das interfaces de 10Mbps do roteador, de acordo com a figura 19.

7.4 Especificação dos equipamentos de rede

O sistema de detecção de intrusão colocado na topologia física é um IDS baseado em rede. Este dispositivo está conectado ao roteador, que interliga todos os prédios do campus à rede externa.

Nesta posição, o IDS é capaz de observar o tráfego originado ou destinado aos servidores na *Server Farm,* que pode ser de usuários internos ou externos. A figura 19 mostra o posicionamento do IDS na topologia física proposta.

Outro recurso utilizado para proteger a rede da universidade é o *firewall*. Nesta proposta foram utilizados dois *firewalls*.

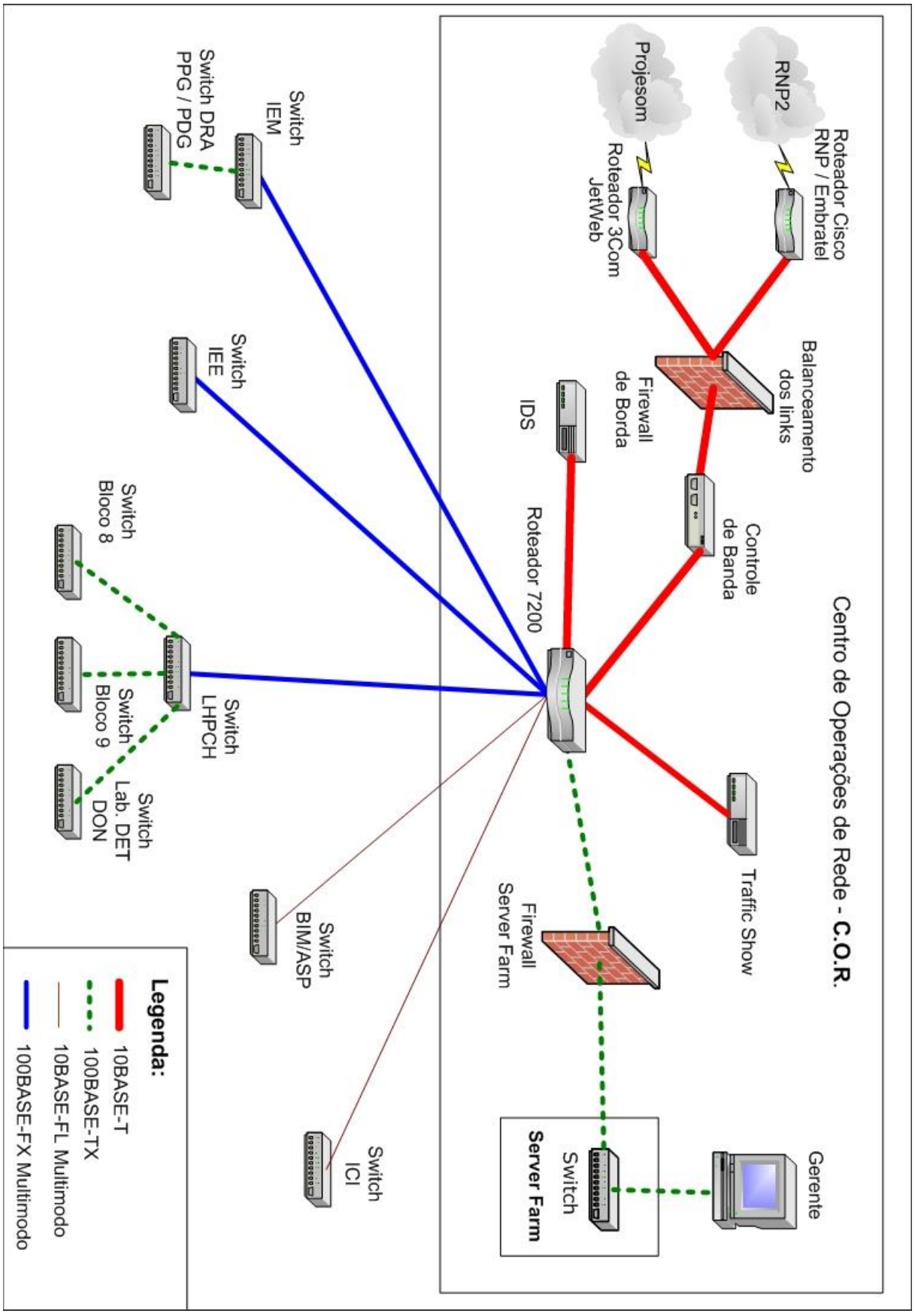

Figura 19 – Proposta de uma topologia física da rede.

O primeiro, denominado *firewall* de borda, está situado entre a rede externa e a rede interna. Já o segundo, denominado *firewall* Server *Farm,* está situado entre os servidores corporativos e a rede interna, restringindo o acesso a estes servidores, conforme se pode verificar na figura 19.

O *firewall* de borda irá atuar como a primeira linha de defesa, filtrando o tráfego de entrada ou de saída da rede. Este equipamento também executará o balanceamento de carga nos *links* de Internet.

O *firewall Server Farm* possui a característica de proteger os servidores corporativos tanto do tráfego externo como do tráfego interno. Este *firewall* tem a função de evitar ataques originados tanto na rede externa quanto na rede interna, criando uma região segura para os servidores corporativos e públicos. Esta região é chamada de *Demilitarized Zone* ou DMZ [25].

A zona desmilitarizada (DMZ) é uma rede situada entre a rede interna da instituição e a rede pública. Esta região protege os servidores que estão disponíveis ao mundo externo como, por exemplo, servidores de DNS, *web* e de correio eletrônico.

Esta região concentra todos os servidores corporativos da universidade, e caso estes servidores venham a sofrer algum ataque, a rede interna continuará intacta e segura.

O acesso à Internet é o gargalo da rede e o principal motivo de reclamação do desempenho da rede. Portanto, para ajudar os administradores no monitoramento da rede, esta proposta sugere a utilização de um equipamento chamado *traffic show* ou analisador de tráfego, que mostrará o comportamento do tráfego dos usuários.

O *traffic show* é conectado ao roteador, em uma de suas interfaces de 10Mbps. Todo tráfego da rede que circular pelo *backbone* ou tiver como destino uma rede externa, será analisado por este equipamento. Logo, será possível obter diversas informações importantes para a tomada de decisões, que serão utilizadas por outro equipamento na rede, o controlador de banda.

Uma outra funcionalidade muito importante do roteador é a sua utilização para implementar o recurso de *traffic show*, através da tecnologia *NetFlow*, disponível neste equipamento. Portanto, se a administração da rede desejar, este

serviço pode ser implantado no roteador, evitando assim, o uso de outro equipamento.

Com o intuito de garantir o uso racional da rede, propõe-se o emprego de um dispositivo, controle de banda, que irá priorizar e limitar a utilização dos *links* de acesso à Internet, baseado em dados capturados pelo *traffic show*.

O equipamento de controle de banda permitirá que os administradores criem regras e políticas, que irão priorizar uma maior banda para os aplicativos mais importantes para os usuários como, por exemplo, correio eletrônico e *web*.

As demais aplicações terão uma prioridade bem menor, mas não serão bloqueadas. Este equipamento é conectado à rede através do roteador, e está localizado entre o *firewall* de borda e o roteador, de acordo com a figura 19.

7.4.1 Equipamento de gerência da rede

A figura 20 mostra a topologia da gerência dos equipamentos. Cada equipamento será conectado ao *switch* da gerência. Isto dará aos administradores da rede condições para um melhor gerenciamento desses equipamentos, local ou remotamente. O switch da gerência deverá possuir no mínimo 12 portas, padrão 10BASE-T / 100BASE-TX para conectar todos os equipamentos que serão instalados na rede.

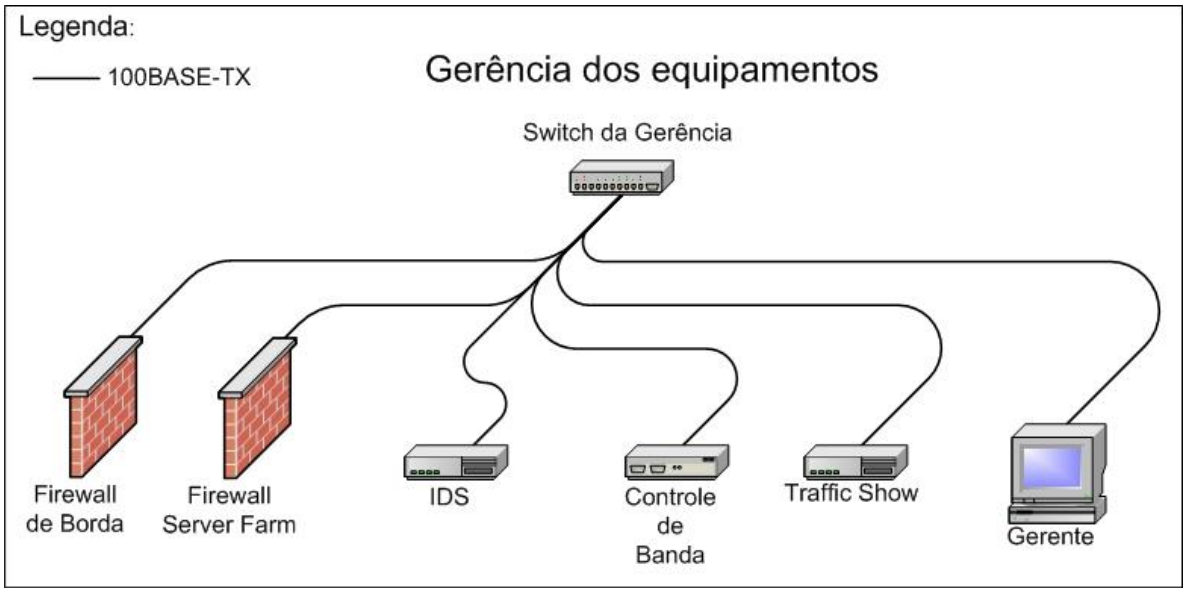

Figura 20 – Topologia física da gerência de rede.

Além dos equipamentos que ajudarão a melhorar o gerenciamento da rede e a implementação de medidas proativas de segurança, existe também, o equipamento gerente.

A função principal deste equipamento é prover uma interface entre o administrador da rede e todos os equipamentos mostrados nas figuras 20 e 21. Com a utilização deste *host* gerente, as tarefas de configuração e visualização de todo o ambiente de rede será centralizado em um único terminal.

Um recurso que pode ser adicionado a este equipamento é o acesso discado via modem. Isso permitirá acessar o *host* gerente caso a rede ou algum outro equipamento esteja com problemas, causando a interrupção de qualquer acesso à rede UNIFEI.

7.4.2 Server Farm

Com a centralização dos serviços corporativos, a universidade pode alocar todos os servidores em um único local. Esta localidade é representada pelo *Server Farm*.

Cada servidor terá sua função na rede e executará um determinado serviço. Todos eles serão conectados à rede através do switch *Server Farm*, que deverá possuir pelo menos 12 portas padrão 100BASE-TX.

Esses servidores corporativos serão gerenciados e monitorados pelo *host* gerente, mostrado nas figuras 20 e 21. A função básica de cada servidor é descrita a seguir:

- O servidor de arquivos irá fornecer atualizações dos *softwares* utilizados pelos usuários, bem como outros tipos arquivos ou *softwares* que por ventura sejam necessários aos usuários.
- O servidor de *Intranet* proverá o acesso dos usuários à rede interna da universidade.
- O servidor de *web* fornecerá o serviço de hospedagem de páginas de toda a universidade.

- O servidor DHCP será responsável por fornecer dinamicamente os parâmetros de configuração de um host como, por exemplo, o endereço IP e o endereço do DNS *Server*. Este serviço pode ser implementado no roteador.
- O servidor de DNS executará o serviço de resolução de nomes de domínio. Ele responderá às solicitações dos usuários para traduzir um nome de domínio para um endereço IP associado.
- O servidor de correio eletrônico será responsável pelo envio e recebimento de mensagens de correio eletrônico dos usuários da rede. Neste servidor deverá ser instalado um bom *software* antivírus para verificar os e-*mails* dos usuários.
- A finalidade principal do servidor de FTP é transferir arquivos de um *host* para outro, copiando e movendo arquivos do servidor para o cliente e vice-versa.
- A função do servidor do sistema acadêmico será proporcionar aos alunos, professores e funcionários acesso ao programa que irá controlar as notas, matrículas e outras informações sobre os registros acadêmicos dos alunos.

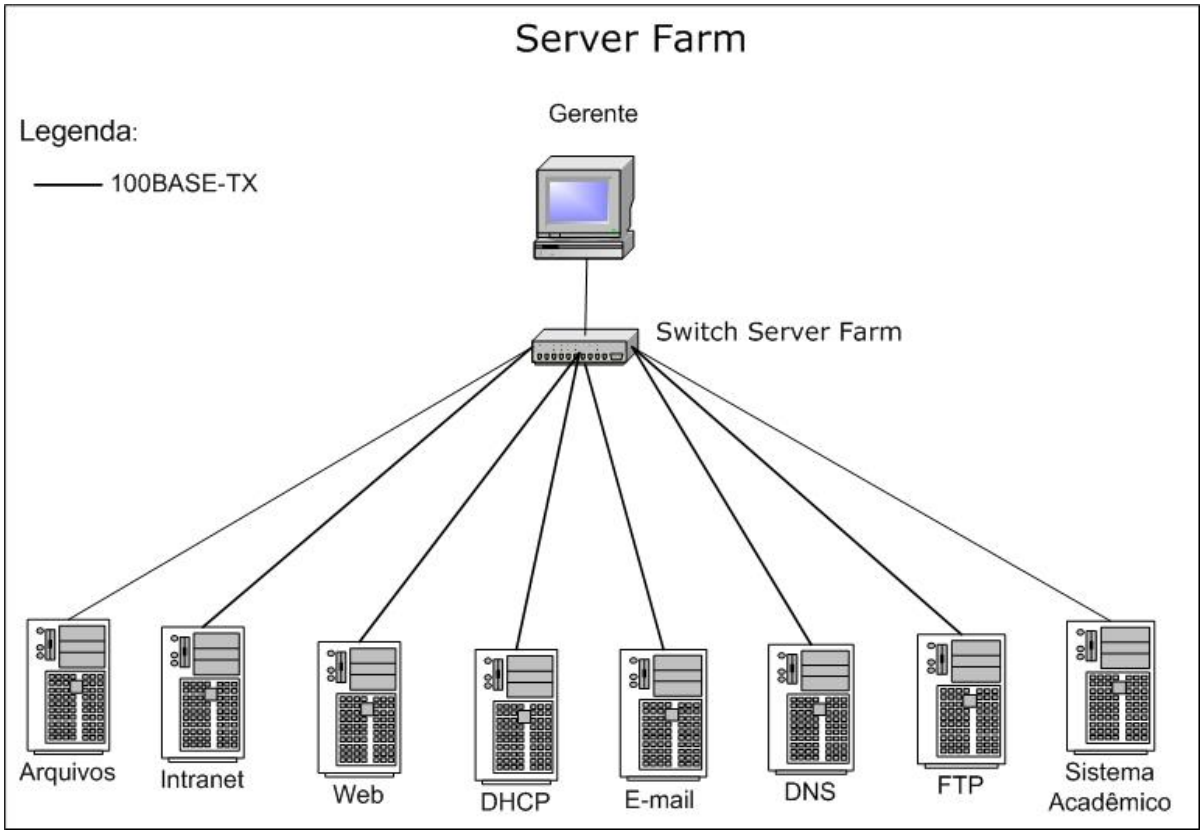

Figura 21 – Topologia física dos servidores corporativos - *Server Farm*.

8 CONCLUSÕES

Esta proposta de reestruturação da rede UNIFEI baseou-se no desenvolvimento de projetos em camadas. A primeira tarefa realizada foi o levantamento e análise dos requisitos dos usuários e da universidade, onde foi possível verificar as necessidades atuais e futuras dos usuários. Na etapa seguinte, foram levantadas e analisadas diversas informações sobre as características atuais da rede e sobre as características do tráfego da rede UNIFEI.

Depois de levantadas estas informações, foi possível constatar que a atual topologia e alguns equipamentos da rede não precisam ser trocados ou substituídos por outros, como acreditam alguns administradores da rede. Concluiu-se também, que os *links* de acesso à Internet são suficientes para prover um bom serviço aos usuários.

Portanto, um dos pontos principais da elaboração de projetos em camadas é a realização de um planejamento eficiente antes da sua implementação. Logo, antes de escolher quais tecnologias e equipamentos seriam utilizados, pode-se descobrir as reais necessidades dos usuários e da universidade e assim, desenvolver uma proposta coerente de reestruturação da rede.

Com o aumento do número de alunos e dos computadores na universidade, tornou-se fundamental uma administração eficiente da rede UNIFEI, pois atualmente tanto os recursos técnicos quanto os recursos humanos são insuficientes, para atender à atual demanda.

A administração da universidade deve elaborar um plano de capacitação dos funcionários da administração da rede, bem como aumentar o quadro efetivo dos funcionários que trabalham na gerência e administração da rede, que atualmente é formado por cerca três a quatro pessoas.

Esta proposta foi desenvolvida com o intuito de mostrar alguns recursos existentes que podem fornecer um melhor gerenciamento da rede. Entretanto, a decisão de se utilizar um ou outro dispositivo de rede será dos administradores da rede UNIFEI.

Um assunto muito discutido atualmente é o uso de *software open source* em instituições públicas, e este é o momento ideal para a universidade refletir sobre a utilização destes recursos e também, fomentar esta idéia junto aos seus alunos, funcionários e professores.

Atualmente os administradores da rede UNIFEI já utilizam alguns *softwares open source*, entre eles estão: o software para gerenciar a taxa de ocupação dos servidores, o *software* antivírus e a ferramenta para monitoramento dos *links*.

8.1 Plano de teste básico de desempenho da rede

Após a implementação desta proposta é muito importante a elaboração de testes básicos de desempenho da rede, que irão representar a medida da rapidez e da confiabilidade de uma rede.

A combinação de *software*, *hardware* e o cabeamento da rede terão um desempenho em conjunto diferente dos seus desempenhos individuais. Portanto, deve-se elaborar um conjunto de parâmetros ou medidas para descobrir se o desempenho de uma rede está de acordo com o estabelecido. Esses parâmetros são chamados de *baseline* ou linha de base [5]. Essa linha de base é estabelecida após toda rede ter sido implantada e configurada corretamente pelos administradores.

Para elaborar uma linha de base pode-se utilizar uma ferramenta de monitoramento do tráfego na rede. Essa ferramenta irá armazenar diversas informações sobre os pacotes de dados que circulam na rede como, por exemplo, a

contagem de colisão de pacotes, taxa de utilização de rede, tráfego de broadcast, erros de quadro, etc.

Com o estabelecimento da linha de base da rede UNIFEI será possível realizar testes na rede para verificar se o atual desempenho está dentro dos parâmetros aceitáveis estabelecidos na linha de base.

Deve-se ficar atento com a linha de base, pois à medida que a rede cresce e é alterada, a linha de base também irá se modificar como qualquer outra documentação que necessite de uma atualização periódica.

8.2 Documentação da rede

A documentação é a tarefa mais discutida e a que menos é executada em um projeto de rede. Esta proposta procurou estabelecer alguns temas, na elaboração da documentação da rede, os quais incluirão os tópicos descritos a seguir.

8.2.1 Documentação do cabeamento da rede

Esta etapa deve envolver os seguintes requisitos [1]:

- Topologia lógica e física do cabeamento principal e também do cabeamento secundário ou horizontal.
- As especificações dos tipos e comprimentos dos cabos utilizados no cabeamento principal ou *backbone*.
- As especificações dos tipos e comprimentos dos cabos utilizados no cabeamento horizontal dentro de cada instituto, laboratório, etc.
- A localização dos armários de telecomunicações dentro de cada instituto ou laboratório. Estes armários são responsáveis por abrigar os equipamentos de rede.

8.2.2 Manual de cabeamento de rede

Este tópico propõe a elaboração de um manual de cabeamento da rede de computadores da universidade, onde serão definidas as normas de cabeamento para a rede interna. Este manual irá guiar as futuras instalações e atualizações do cabeamento da rede UNIFEI.

8.3 Proposta de estudos futuros

Este trabalho propõe a reestruturação da rede UNIFEI, entretanto para completar esta proposta serão necessários outros estudos mais aprofundados, que podem ser desenvolvidos por alunos em outras dissertações. Estes estudos são:

8.3.1 Projeto do backbone redundante

A tecnologia de redes sem fio pode ser utilizada para o desenvolvimento de um cabeamento de *backbone* redundante, que compreende as metas de disponibilidade e escalonamento. Com isto, a rede UNIFEI poderá melhorar a meta técnica de disponibilidade da rede interna, caso ocorra algo com o cabeamento principal de fibra óptica.

Outro uso interessante para esta tecnologia é o fornecimento de acesso à rede do campus para usuários externos, fora do campus da universidade como, por exemplo, o prédio central da UNIFEI ou até mesmo conectar todos os professores e alunos da universidade.

8.3.2 Projeto de segurança da informação

A proposta de reestruturação da rede aborda apenas o *hardware* para auxiliar a segurança da informação na universidade, mas é importante ter em mente que segurança não é só a instalação de equipamentos de segurança. A universidade deve criar uma política que atenda suas metas de segurança da informação e também a segurança física da rede.

Este projeto deve abranger a criação de um plano gestor de informática, bem como a criação de uma política de segurança da informação, entre outros assuntos citados anteriormente neste trabalho.

8.3.3 Projeto de gerenciamento da rede

Esta proposta de reestruturação envolve apenas a especificação de equipamentos para auxiliar o gerenciamento da rede, mas não desenvolveu nenhum projeto de gerenciamento da rede.

O gerenciamento envolve técnicas para auxiliar no monitoramento e na solução dos diversos problemas de uma rede. Portanto, esta proposta aborda os equipamentos a serem inseridos em uma rede, mas existe ainda, a necessidade da elaboração de um projeto de gerenciamento, que pode ser desenvolvido por outros estudos ou propostas de dissertação.

O gerenciamento de redes é um tema muito extenso e complexo, por isso é recomendável a elaboração de uma proposta mais aprofundada sobre este assunto, que envolverá diversas etapas como, por exemplo:

- Detalhes de configuração dos *hosts* e dos servidores corporativos e de grupo de trabalho.
- Listas dos *softwares* utilizados pelos usuários.
- Registros de suporte aos usuários e da manutenção da rede.
- Diretrizes de uso racional dos recursos da rede.
- Recuperação de dados.
- Operações de *backup*.
- Técnicas de redundância para os servidores.

Estes itens são apenas algumas etapas a serem desenvolvidas para a elaboração de um projeto de gerenciamento da rede e suporte para os usuários.

APÊNDICE A

Formulários para levantamento dos requisitos de rede

FORMULÁRIO PARA LEVANTAMENTO DE REQUISITOS DOS ADMINISTRADORES DA UNIFEI

1) Atualmente, a rede de dados tem desempenho suficiente para atender suas necessidades?

Intranet		**Internet**	
Sim	( )	Sim	( )
Não	( )	Não	( )
Lenta	( )	Lenta	( )
Vírus	( )	Vírus	( )
Falta de Suporte	( )	Falta de Suporte	( )
Instável	( )	Instável	( )
_____	( )	_____	( )
_____	( )	_____	( )

2) Há algum plano para se implementar outras aplicações de rede como, por exemplo, vídeo conferência e voz sobre IP?

Intranet		**Internet**	
Vídeo conferência	( )	Vídeo conferência	( )
Voz sobre IP	( )	Voz sobre IP	( )
Ensino a distância	( )	Ensino a distância	( )
_____	( )	_____	( )
_____	( )	_____	( )

3) Quais as metas da instituição em relação à rede Intranet e Internet?

4) Qual o investimento estimado para a área de tecnologia da informação da instituição?

FORMULÁRIO PARA LEVANTAMENTO DE REQUISITOS DOS ADMINISTRADORES DA REDE UNIFEI

1) Nível dos recursos humanos

Suficiente	Sim ( )	Não ( )
Capacitação técnica	Sim ( )	Não ( )

2) Nível dos recursos técnicos

2.1)Micros para os usuários

Suficiente (em número)	Sim ( )	Não ( )
Atende às necessidades quanto ao tipo e capacidade	Sim ( )	Não ( )

2.2) Servidores

Suficiente (em número)	Sim ( )	Não ( )
Atende às necessidades quanto ao tipo e capacidade	Sim ( )	Não ( )

2.3) Infra-estrutura da rede

Suficiente (em número)	Sim ( )	Não ( )
Atende aos requisitos mínimos de rede	Sim ( )	Não ( )

2.4) Equipamentos de rede

Suficiente (em número)	Sim ( )	Não ( )
Atende aos requisitos mínimos de rede	Sim ( )	Não ( )

3) Propostas

3.1) Centralização

Necessária	Sim ( )	Não ( )
Adequada	Sim ( )	Não ( )
Desnecessária	Sim ( )	Não ( )
Inadequada	Sim ( )	Não ( )

3.2) Políticas no tratamento da informação

Necessária	Sim ( )	Não ( )
Adequada	Sim ( )	Não ( )
Desnecessária	Sim ( )	Não ( )
Inadequada	Sim ( )	Não ( )

FORMULÁRIO PARA LEVANTAMENTO DE REQUISITOS DOS USUÁRIOS DA UNIFEI

1) Quais são as três principais atividades desenvolvidas por você, que dependem da rede da UNIFEI?	
1	
2	
3	

2) Das três atividades escolhidas anteriormente, quais delas dependem da Internet?	
1	
2	
3	

3) Classifique o desempenho da rede em relação às suas atividades.
( ) Atende completamente minhas necessidades
( ) Atende parcialmente minhas necessidades
( ) Não atende minhas necessidades

4) Se o desempenho não está em um nível aceitável, aponte alguns fatores	
1	
2	
3	

5) Cite três atividades desenvolvidas por você, que utilizarão a rede no futuro.	
1	
2	
3	

6) Quais serão as tecnologias envolvidas nestas atividades?

REFERÊNCIAS BIBLIOGRÁFICAS

[1] OPPENHEIMER, Priscilla. **Top-Down Network Design**. 1. ed. USA: MacMillan Technical Publishing, 1997.

[2] TANENBAUM, Andrew S. **Redes de Computadores**. Rio de Janeiro: Editora Campus, 1994.

[3] SOARES, Luiz F.; COLCHER, Sérgio; LEMOS, Guido. **Redes de Computadores**: das LANs, MANs e WANs às redes ATM. 2. ed. Rio de Janeiro: Editora Campus, 1995.

[4] CHIOZZOTTO, Mauro; SILVA, Luis A. Pinto. **TCP/IP Tecnologia e Implantação**. 1. ed. São Paulo: Editora Érica, 1999.

[5] **CISCO Certified Network Associate Curriculum**. USA: Cisco Systems Inc., 2001.

[6] COMER, Douglas E. **Internetworking with TCP/IP:** Principles, Protocols and Architecture. 2. ed. Englewood Cliffs, Nova Jersey: Prentice Hall, Inc., 1995.

[7] COMER, Douglas E. **Computer Networks and Internets.** 2. ed. Nova Jersey: Prentice Hall, Inc., 1995.

[8] ODOM, Wendell. **CCNA Exam Certification Guide**. Indianápolis, USA: Lacidar Unlimited Inc., 1999.

[9] **INTERNETWORKING Technologies Handbook. USA:** Cisco Systems Inc., 2003.

[10] VACCA, John. **The Cabling Handbook**. USA: Prentice Hall, Inc., 1998.

[11] RIBEIRO, José A. Justino. **Fundamentos de Comunicações Ópticas**. Santa Rita do Sapucaí - MG, 2001.

[12] LAMMLE, Todd. **CCNA Cisco Certified Network Associate Study Guide**. Califórnia, USA: Sybex Inc., 2002.

[13] SWARTZ, John; LAMMLE, Todd. **CCIE Cisco Certified Internetwork Expert Study Guide**. Califórnia, USA: Sybex Inc., 2003.

[14] INSTITUTE OF ELECTRICAL AND ELECTRONIC ENGINEERS. **IEEE 802.3**. USA, 2000.

[15] BARKL, Andy; LAMMLE, Todd. **CCDA Cisco Certified Design Associate Study Guide**. 2. ed. Califórnia, USA: Sybex Inc., 2003.

[16] REKHTER, Y. et al. **Address Allocation for Private Internets**. RFC 1918. feb. 1996. Disponível em: <www.rfc-editor.org>. Acesso em: 15 jan. 2004.

[17] ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 17799**. Tecnologia da informação - Código de prática para a gestão da segurança da informação. Rio de Janeiro, 2001.

[18] CARVALHO, Daniel B. **Segurança de Dados com Criptografia**. Rio de Janeiro: Editora Book Express, 2000.

[19] KISSER, Scott. **A Hardware Based Firewall Option for the SOHO User.** SANS Institute, 2000. Disponível em: <www.sans.org>. Acesso em 22 jan. 2004.

[20] NAKAMURA, Emilio T.; GEUS, Paulo L. **Segurança de Redes em Ambientes Cooperativos**. 2. ed. São Paulo: Editora Futura, 2003.

[21] CISCO´s NetFlow. Disponível em: <www.cisco.com/warp/public/732/Tech/nmp/net-flow/index.shtml>. Acesso em: 11 mar. 2004.

[22] MRTG (Multi Router Traffic Grapher). Disponível em: <http://people.e.ethz.ch/õeitker/webtools/mrtg>. Acesso em: 11 mar. 2004.

[23] UNIVERSIDADE FEDERAL DE ITAJUBÁ. Disponível em <www.unifei.edu.br>. Acesso em: 20 mar. 2004.

[24] EGEVANG, K.; FRANCIS, P. **The IP Network Address Translator (NAT)**. RFC 1631. May. 1994. Disponível em: <www.rfc-editor.org>. Acesso em: 17 mai 2004.

[25] LARSON, Robert E; COCKCROFT, Lance. **CCSP - Cisco Certified Security Professional**. Osborne, USA: McGraw-Hill, 2003.

[26] SHINDER, Thomas W.; SHIMONSKI, Robert J.; SHINDER, Debra L. **The Best Damn Firewall Book Period**. Rockland, USA: Syngress Publishing, Inc., 2003.

[27] SHIREY, R. **Internet Security Glossary**. RFC 2828. May, 2000. Disponível em: <www.rfc-editor.org>. Acesso em: 22 mai. 2004.

[28] RANUM, Marcus J. **Coverage in Intrusion Detection Systems**. NFR Security, Inc.**, 2001.**

[29] BAIJU, Shah. **How to Choose Intrusion Detection Solution.** SANS Institute, 2001. Disponível em <www.sans.org>. Acesso em 22 mai. 2004.

[30] BACE, Rebecca. **An Introduction to Intrusion Detection and Assessment**. ICSA, Inc., 1999.

[31] BIERMANN, E.; CLOETE, E.; VENTER, L. M. A comparison of Intrusion Detection system. **Computer & Security**, 2001.

[32] NUKHERJEE, B.; HEBERLEIN, L.T.; LEVITT K. Network Intrusion Detection. **IEEE Network**, Jun 1994.

[33] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO/IEC DIS 10040**. Information technology - Open Systems Interconnection - Systems management overview. Geneva, 1991.

[34] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO 8073**. Information Processing Systems - Open Systems Interconnection - Connection-Oriented Transport Protocol Specification. Geneva, 1988.

[35] GÜN, L.; GUÉRIN, R. Bandwidth management and congestion control framework of the broadband network architecture. **Computer Networks and ISDN System**, North-Holland, 1993.

[36] VAN DEN NIEUWELLAR, M; HUNT, R. Real-time carrier network traffic measurement, visualization and Topology modeling. **Computer Communications**, 2004.

[37] LIN, T.; SUN, Y. S.; CHANG, S.; CHU, S.; CHOU, Y.; LI, M. Management of abusive and unfair Internet Access by quota-based priority control. **Computer Networks**, 2004.