



UNIVERSIDADE FEDERAL DE PELOTAS  
BACHARELADO EM CIÊNCIA DA COMPUTAÇÃO

OUTROS TRABALHOS EM:  
[www.projetoderedes.com.br](http://www.projetoderedes.com.br)

**ANÁLISE DE INFRA-ESTRUTURA DE REDE PARA SUPORTE À  
VIDEOCONFERÊNCIA: UM ESTUDO DE CASO**

**VERÔNICA BURMANN DA SILVA**

Pelotas, 2005

**VERÔNICA BURMANN DA SILVA**

**ANÁLISE DE INFRA-ESTRUTURA DE REDE PARA SUPORTE À  
VIDEOCONFERÊNCIA: UM ESTUDO DE CASO**

Monografia apresentada ao Curso de Bacharelado em Ciência da computação do Instituto de Física e Matemática da Universidade Federal de Pelotas, como requisito parcial à obtenção do título de Bacharel em Ciência da Computação.

**Orientador:** Prof Dr. Ricardo Azambuja Silveira  
Universidade Federal de Pelotas

**Co-orientador:** Prof. João Ladislau Lopes  
Diretor do Centro de Informática da  
Universidade Federal de Pelotas

Pelotas, 2005

# **ANÁLISE DE INFRA-ESTRUTURA DE REDE PARA SUPORTE À VIDEOCONFERÊNCIA: UM ESTUDO DE CASO**

Por

**VERÔNICA BURMANN DA SILVA**

Monografia defendida e aprovada em 14 de julho de 2005 pela banca examinadora constituída pelos seguintes integrantes:

BANCA EXAMINADORA:

---

Prof. Dr. Ricardo Azambuja Silveira (UFPel)

---

Prof. Msc. Leonardo Ribeiro (UFPel)

---

Profa. Msc. Eliane Diniz (UFPel)

---

Prof. João Ladislau Lopes (Diretor do CI da UFPel)

## **AGRADECIMENTOS**

Aos meus pais, Victor e Liane, pelo amor e ensinamentos valiosos que me ajudam durante minha vida.

Aos meus irmãos, pelo carinho e amor dedicados a mim.

Ao meu noivo Christian que dividiu comigo, nesta trajetória, minhas frustrações e alegrias.

Aos amigos Heloisa e Alfredo, pela ajuda e incentivo nos momentos difíceis.

Aos professores do curso, pela sabedoria transmitida.

Ao professor Ricardo pela orientação neste trabalho.

E principalmente a Deus, pela vida e tudo que sou.

*Escuto e esqueço;  
vejo e recordo;  
faço e entendo.*

Tao Te King

## SUMÁRIO

LISTA DE FIGURAS.....	8
Capítulo IV.....	8
Capítulo VI.....	8
Capítulo VIII.....	8
Capítulo IX.....	8
Capítulo X.....	9
Capítulo XI.....	9
LISTA DE TABELAS.....	11
Capítulo VII.....	11
Capítulo VIII.....	11
RESUMO.....	12
ABSTRACT.....	13
I INTRODUÇÃO.....	14
1.1 Motivação.....	14
1.1.1 Pesquisa-Ação.....	15
1.2 Objetivos.....	17
1.2.1 Objetivos Específicos.....	17
1.3 Contribuição Esperada.....	18
II CONCEITOS SOBRE VIDEOCONFERÊNCIA.....	20
2.1 Introdução geral sobre videoconferência.....	20
2.2 Modalidades de videoconferência.....	24
2.3 Características de sistemas de videoconferência.....	26
2.4 Procedimentos para videoconferência.....	28
III Áudio e Vídeo streaming.....	30
IV Estudo dos Cenários do ambiente de videoconferência.....	33
4.1 Ambiente dos Participante.....	33
4.2 Salas de Videoconferência.....	34
4.3 Cenários.....	38
V Parâmetros de avaliação.....	43
VI. Configuração de sistemas de videoconferência.....	44
6.1 Fundamentos da Rede para Videoconferência.....	44
6.2 Conceitos de Rede de Computadores.....	46
6.3 Equipamentos de Rede de Computadores.....	47
6.3.10 Gateway.....	51
6.3.11 Multipoint Control Unit.....	52
6.3.12 Gatekeeper (Controle de Rede).....	52
6.3.13 Domain Name Service/Domain Name System.....	53
6.3.14 Firewall.....	54
6.3.15 Network Address Translation.....	55
6.3.16 Ethernet.....	57
6.3.17 Asymmetric Digital Subscriber Line.....	59
6.4 Gerenciando os serviços de videoconferência.....	63
VII Estudo das aplicações dos protocolos de redes.....	64
7.1 Internet Protocol.....	64
7.2 Transmission Control Protocol.....	64
7.3 User Datagram protocol.....	65
7.4 TCP/IP (Transmission Control Protocol / Internet Protocol).....	65
7.5 Dynamic Host Configuration Protocol.....	66

7.6	Internet Group Management Protocol .....	67
7.7	Real Time Transport Protocol .....	67
7.8	Real Time Control Protocol .....	67
7.9	Session Initiation Protocol.....	68
7.10	Real Time Streaming Protocol .....	68
7.11	Transmissão Multicamadas.....	68
7.12	Padrão H.323 .....	69
7.13	Áudio.....	70
7.14	Outras Tecnologias Existentes.....	72
VIII	Infra-estrutura de redes da UFPel .....	76
8.1	Arquitetura do Ambiente de Videoconferência .....	76
8.2	Topologia de Rede da Universidade Federal de Pelotas .....	79
8.3	UFPELNET: Serviços & Equipamentos de Abrangência Institucional.....	83
8.4	Principais Tipos de Equipamentos que Interligam a UFPelNET .....	84
IX	Análise do tráfego da rede .....	88
9.1	Multi Router Traffic Grapher .....	88
9.1.1	Características .....	89
9.1.2	Exemplos de Gráficos Gerados .....	90
9.2	Nagios .....	94
9.2.1	Características.....	94
9.2.2	Configuração mínima.....	95
9.2.3	Licença .....	95
9.2.4	Exemplos de Gráficos Gerados .....	96
X	Testes Realizados na Universidade Federal de Pelotas .....	99
XI	Estudo de uma solução de videoconferência a ser implantada na Universidade Federal de Pelotas.....	119
XII	CONCLUSÕES .....	125
XIII	Referências Bibliográficas .....	127

## **LISTA DE FIGURAS**

### **CAPÍTULO IV**

Figura 4.2.1: Luminárias utilizadas num estúdio de transmissão	35
Figura 4.2.2: Sala utilizando materiais de isolamento	35
Figura 4.2.3: Sala de Reuniões tipo Mesa Redonda.	36
Figura 4.2.4: Layout de um Auditório de Videoconferência	37
Figura 4.2.5: Modelo de Aterramento	38
Figura 4.3.1: Cenário A Videoconferência Computador para Computador usando o NetMeeting	39
Figura 4.3.2: Cenário B - Videoconferência Computador para Câmera	40
Figura 4.3.3: Cenário C - Câmera para Câmera	40
Figura 4.3.4: Cenário D - Diversos Computadores comunicando com uma Sala	41
Figura 4.3.5: Cenário E – Videoconferência em Salas de Aula	42

### **CAPÍTULO VI**

Figura 6.3.11: Videoconferência de Modelo Centralizado MCU	52
Figura 6.3.16: Estrutura Ethernet	58

### **CAPÍTULO VIII**

Figura 8.1: Mapa de velocidades dos Prédios do Campus Capão do UFPel.	77
Figura 8.2: Sistema de Videoconferência UFPel	78
Figura 8.3: Mapa Lógico da Infra-estrutura de rede da Universidade Federal de Pelotas.	80
Figura 8.4: Mapa da Rede do Instituto de Informática da UFRGS	81
Figura 8.5: Mapa da Rede da UCPel	82

### **CAPÍTULO IX**

Figura 9.1.2.1: Gráfico do Roteador (eth0) no dia 04 de Julho	91
Figura 9.1.2.2: Gráfico do Roteador (PPP/0) no dia 04 de Julho	91



Figura 9.1.2.3: Gráfico do Roteador (PPP/1) no dia 04 de Julho	91
Figura 9.1.2.4: Gráfico do Roteador (PPP/2) no dia 04 de Julho	91
Figura 9.1.2.5: Gráfico do Roteador (PPP/3) no dia 04 de Julho	92
Figura 9.1.2.6: Gráfico do Roteador (eth0) no dia 29 de Abril	92
Figura 9.1.2.7: Gráfico do Roteador (PPP/0) no dia 29 de Abril	92
Figura 9.1.2.8: Gráfico do Roteador (PPP/1) no dia 29 de Abril	93
Figura 9.1.2.9: Gráfico do Roteador (PPP/2) no dia 29 de Abril	93
Figura 9.1.2.10: Gráfico do Roteador (PPP/3) no dia 29 de Abril	93
Figura 9.2.4.1: Gráfico Nagios da Rede da UFPel	96
Figura 9.2.4.2: Mapa Nagios do Status da Rede da UFPel	98

## **CAPÍTULO X**

Figura 10.1: Configuração de IP e DNS	102
Figura 10.2: Configuração de IP particular	102
Figura 10.3: Esquema do funcionamento de videoconferência por streaming	103
Figura 10.4: Configuração do Agendamento	104
Figura 10.5: Configuração do RealProducer	105
Figura 10.6: Configuração das Audiências do RealProducer	106
Figura 10.7: Visualização do Real Producer Basic 10	107
Figura 10.8: Esquema do funcionamento da Aula Remota	109
Figura 10.9: Visualização do RealPlayer	109
Figura 10.10: Configuração NetMeeting	113
Figura 10.11: Configuração das opções, aba geral	114
Figura 10.12: Configuração Avançada	114
Figura 10.13: Configuração Vídeo	115
Figura 10.14: Configuração de chamada	116

## **CAPÍTULO XI**

Figura 11.1: Layout da sala de multimeios para utilização de videoconferência que poderá ser adota pela UFPel	120
---	-----

Figura 11.2: Projeto de Layout da sala de reunião no Centro de Informática da UFPel	121
Figura 11.3: Foto da sala de Cursos do Centro de Informática da UFPel	123

## **LISTA DE TABELAS**

### **CAPÍTULO VII**

Tabela 7.1: Recomendações ITU-T que suportam a sinalização H.323	69
--	----

### **CAPÍTULO VIII**

Tabela 8.4: Circuitos FRAME-RELAY contratados a Brasil Telecom.	85
---	----

## **RESUMO**

Neste trabalho pretende-se realizar um trabalho de pesquisa sobre o conceito de videoconferência, as suas modalidades e as respectivas infra-estruturas necessárias para a sua realização.

Para estudar os casos realizados na Universidade Federal de Pelotas foi necessário que o trabalho tivesse um maior enfoque nos aspectos de projeto de rede, configuração de topologias, dispositivos e protocolos.

Pretende-se com isso, ser possível estabelecer e validar um conjunto de parâmetros para avaliação que possibilite a escolha de um sistema de videoconferência de acordo com necessidades específicas e recursos disponíveis.

Palavras Chave: Sistemas de Videoconferência, Redes de Computadores e Sistemas Multimídia.

## **ABSTRACT**

In this term paper it is propoused to carry out a research that focus on the video conference's concept, its modalities and the necessary infrastructures for its realization.

In order to study a number of cases carried out at the Federal University of Pelotas,it became necessary a broader approach that could focus on the aspects of net projects,topology configurations, devices and protocols.

It is intended by this work, to establish and to validate a set of parameters for evaluation that could make possible the right choice of a video conference system according to its specific necessities along with available resources.

**Keywords:** Systems of Video Conference, Computer networks and Systems of Multimedia.

## **I INTRODUÇÃO**

### **1.1 Motivação**

Uma das maiores necessidades dos seres humanos é a comunicação. Desde o mais remoto dos tempos, essa necessidade se faz presente.

Com o avanço da tecnologia, chegamos hoje até a Internet formada por milhões de usuários, ligados a ela por meio de diversos dispositivos que evoluem a cada dia. Esse avanço, impensável até alguns anos atrás, nos coloca diante de um mundo de informações e, ao mesmo tempo, pode provocar um descontrole na seleção das mesmas.

Como uma nova possibilidade de comunicação, a videoconferência veio à tona com a evolução da Internet. Esta modalidade de comunicação proporciona a sensação de estar comunicando-se "ao vivo" com uma pessoa, só que com o auxílio de equipamentos. Essa nova maneira de se comunicar abre a perspectiva de realizar, em tempo real, por exemplo, a Educação a Distância.

Com a Internet, tem-se a possibilidade de comunicação síncrona, em tempo real ou "on-line", como é conhecida. Isso possibilita uma maior interação professor/aluno, estando o professor disponível para orientações no momento exato em que surgirem as dúvidas, permitindo aos alunos ter uma atitude ativa.

A videoconferência também é um novo meio de promover reuniões, permitindo que grupos de profissionais, com escritórios em locais fisicamente distantes, reúnam-se sem sair de suas respectivas salas. Praticamente é como se estivessem falando com a tela de televisão.

A videoconferência possibilita a comunicação, em tempo real, entre pessoas situadas em locais diferentes, enviando e recebendo imagem, voz e dados. Desta forma, mais cedo ou mais tarde, a videoconferência vai se tornando mais acessível e

passa a fazer parte da vida das pessoas, como aconteceu com o computador pessoal e com o correio eletrônico.

Embora uma grande quantidade de ferramentas e recursos seja disponível, a implementação de um projeto de videoconferência com fins institucionais, seja com objetivos educativos ou comerciais, não é algo trivial. Muitas técnicas devem ser empregadas e um bom conhecimento de protocolos, dispositivos e configurações de rede é necessário.

Durante a execução de vários experimentos nesta área, percebeu-se a necessidade de um estudo mais profundo e sistematizado neste sentido e o desenvolvimento de um material que possa ser utilizado como guia e relato de experiência para futuros projetos nesta área.

Neste contexto, surgiu a idéia de desenvolver este trabalho, relacionado a análise dos aspectos relativos à configuração de rede para suporte a videoconferência, utilizando a rede da UFPel, assim como (Kelly,2005) com o estudo das ferramentas que são utilizadas na viabilização dos modelos de videoconferência, visar reunir e relatar as experiências realizados na UFPel.

### **1.1.1 Pesquisa-Ação**

A metodologia utilizada neste trabalho foi a pesquisa-ação, que se mostrou mais adequada para o tipo de estudo em questão.

A pesquisa-ação foi usada pela primeira vez por Kurt Lewin, nos anos 40. Segundo Kurt (apud, SERRANO, 1990), pesquisa-ação é um posicionamento realista da ação, sempre seguida por uma reflexão crítica-objetiva e uma avaliação de resultados. Nem ação sem investigação, nem investigação sem ação.

A pesquisa-ação, como linha de pesquisa associada a diversas formas de ação coletiva, foi utilizada neste trabalho, nas resoluções de problemas, pois a mesma, ofereceu meios de uma pesquisa participante, que busca alternativas para

que aconteça a apropriação do conhecimento, conduzindo com isso, a uma busca constante do querer saber, valorizando assim a pesquisa, tendo como objetivo a ação, a concretização do aprendizado.

Com a utilização dessa metodologia, pesquisa-ação, foi possível analisar os resultados das experiências de transmissões de videoconferência e replanejar as próximas ações ao refletir.

A pesquisa-ação segundo Roech (1992 apud THIOLENT, 1999) e em (ROECH, 1987 apud JONES, 1999) é definida:

Na pesquisa-ação, o pesquisador desempenha um papel ativo no equacionamento dos problemas encontrados, no acompanhamento e na avaliação das ações desencadeadas em função destes problemas. A pesquisa-ação é uma estratégia metodológica da pesquisa social que possibilita a interação entre pesquisador e pessoas implicadas na situação investigada, resultando na ordem de prioridade dos problemas a serem pesquisados e nas soluções a serem encaminhadas sob forma de ação concreta (THIOLENT, 1992).

Pesquisa-ação é uma estratégia de pesquisa que permite obter conhecimento de primeira mão sobre a realidade social empírica. Permite ao pesquisador “chegar perto dos dados” e, portanto, desenvolver os componentes analíticos, conceituais e categóricos de explicação, a partir dos dados, e não a partir de técnicas estruturadas, preconcebidas e altamente quantificadas que enquadram a realidade em definições operacionais que o pesquisador construiu. O enfoque requer que o pesquisador interprete o mundo real a partir da respectiva dos sujeitos de sua investigação. (JONES, 1987).

O que distingue a pesquisa-ação - segundo considera Jones (1987) – dos demais enfoques da pesquisa qualitativa é a relação teoria com a prática.



Diferentemente dos métodos tradicionais de pesquisa qualitativa que combinam observação com entrevista, na pesquisa-ação os pesquisadores se preocupam em construir teoria para a prática.

Acredita-se que usando a metodologia pesquisa-ação, de uma maneira tranqüila, observa-se, além de um envolvimento no trabalho, em busca de soluções para os problemas apresentados, sem tentar sufocá-los, em busca de respostas corretas e imediatas, como também a orientação em busca de ações que condizem com o aprendizado, tendo como fundo a observação dos fatos e a vontade de alcançar os objetivos propostos.

## **1.2 Objetivos**

O objetivo geral deste trabalho é modelar uma infra-estrutura adequada para a viabilização de projetos de videoconferência, enfocando os aspectos de projeto de rede, configuração de topologias, dispositivos e protocolos, tendo como base para estudo de caso, a rede da Universidade Federal de Pelotas.

### **1.2.1 Objetivos Específicos**

Para alcançar o objetivo geral do trabalho, foram estabelecidos os seguintes objetivos específicos:

- Estudar e analisar a configuração da rede da Universidade, verificando a viabilidade das diversas modalidades de técnicas de videoconferência.
- Analisar os diversos protocolos utilizados em cada uma das modalidades de videoconferência e analisar a infra-estrutura necessária.
- Estudar, a partir da rede da Universidade, os casos de erros, entendendo-os e resolvendo-os;

- Avaliar as principais ferramentas de software para configuração de rede para suporte a videoconferência com a possibilidade de configuração na rede envolvida.

### **1.3 Contribuição Esperada**

Com a conclusão deste trabalho, são fornecidos alguns importantes subsídios necessários para a implantação de uma infra-estrutura de videoconferência adequada à rede Universidade. Além disso, com o sistema de videoconferência em pleno funcionamento, podendo assim haver a reativação o canal de TV da UFPel, bem como poderão ser desenvolvidas atividades inerentes tanto à área acadêmica como à administrativa, tais como: apresentações de seminários, semanas acadêmicas, trabalhos de conclusão de curso, defesas de teses e dissertações, treinamentos, formação continuada e reuniões de trabalho.

Ainda é importante ressaltar que, com a implantação de uma infra-estrutura de videoconferência, decorrente dos estudos realizados neste trabalho e com o aproveitamento das características inerentes a esta modalidade de comunicação, espera-se reduzir custos com deslocamentos, proporcionar melhor aproveitamento do tempo e aumentar a produtividade e a rapidez nas atividades acadêmicas e administrativas da Universidade.

### **1.4 Metodologia Empregada**

Como início do trabalho, foi estudada a bibliografia encontrada com a finalidade de ter-se uma base teórica para a continuidade do trabalho que irá seguir no seu decorrer.

A partir desse estudo, os usuários foram contextualizados para a escolha de um sistema de videoconferência adequados as suas possibilidades e necessidades. Para que isso tivesse acontecido foi preciso tornar mais claras as características dos sistemas de videoconferência tal como os aspectos importantes de procedimentos,

configurações, infra-estrutura e protocolos. Foi feito em seguida a avaliação dos parâmetros e o estudo de alguns padrões para a videoconferência.

O trabalho é contemplado com as experiências práticas de videoconferência que foram realizadas durante o período acadêmico como, por exemplo, a realização da nossa Semana Acadêmica do Curso de Ciência da Computação, a apresentação de trabalhos de conclusão de curso, palestras, entre outros, sempre utilizando algum tipo de sistema de videoconferência.

Foi realizado também o estudo do caso particular da Universidade Federal de Pelotas onde é proposto uma possível solução para a implantação de uma sala de videoconferência para a utilização de toda a comunidade universitária.

## **II CONCEITOS SOBRE VIDEOCONFERÊNCIA**

### **2.1 Introdução geral sobre videoconferência**

Desde os primórdios tempos o homem necessitava de algum meio para sua comunicação com os demais. No início se utilizava à comunicação através das pinturas nas cavernas, dos gestos, da fala, da escrita de cartas, depois temos o telégrafo, o telefone e agora temos a Internet que nos possibilita a comunicação com pessoas de qualquer parte remota do mundo numa rapidez nunca vista antes.

Na sua natureza social e para adquirir conhecimentos, o ser humano necessita de grande interação com seus semelhantes. Com o desenvolvimento da espécie e a sua dispersão em lugares cada vez mais longínquos se tornou mais difícil a tão necessária troca de informações. Este problema começou a ser amenizado quando se criaram métodos de troca de mensagens como, por exemplo, na fumaça feita pela fogueira dos nossos primitivos ancestrais e hoje na utilização dos equipamentos atuais de telecomunicação.

Antigamente, os grandes reis buscavam homens sábios para que pudessem ensinar seus filhos desde a infância. Há pouco tempo atrás, quando existia a necessidade de uma reunião para troca de informações era necessário o deslocamento de alguma das partes. Este procedimento acarretava um certo desperdício tanto de tempo como de dinheiro, além de outros fatores de riscos externos. Hoje, quando há necessidade de uma troca de conhecimentos, ela pode ser feita através dos dispositivos atuais que tornam a comunicação cada vez mais real e imediata.

Vários grupos de pesquisa iniciaram estudos objetivando desenvolver um conjunto de serviços de comunicação, assim surgiu os serviços de teleconferência para melhorar este quadro.

São definidos por Soares, Martins & Bastos (1988) e por Fluckiger (1995) como serviços de teleconferência, um conjunto de facilidades de telecomunicações que permite aos participantes, em duas ou mais localidades distintas, estabelecer uma comunicação bidirecional através de dispositivos eletrônicos de comunicação,

enquanto compartilham, simultaneamente, seus espaços acústicos e visuais, tendo a impressão de estarem todos em um único ambiente.

Os serviços de teleconferência são classificados pela literatura (ITU-T,1993) como:

- **Áudio Conferência** – Como diz o nome, são sistemas onde só os sinais de áudio e controles são transmitidos entre os participantes.
- **Conferência Áudio-Documentária** – Adicionado a Áudio Conferência o tratamento de documentos de texto entra essa nova classificação. Um exemplo, de certa forma desta categoria, se pode encaixar o software Skype, que possibilita a troca de informações através da voz e também o tratamento de textos;
- **Conferência Audiográfica** – Similar a Conferência Áudio-Documentaria, mas com mais um serviço, o de transmissão de imagens estáticas;
- **Freeze-Frame Videoconferência** – Igual a Áudio conferência acrescida de envio periódico de imagens estáticas dos participantes como se fosse fotos deles naquele momento da transmissão;
- **Teleseminário** - Serviço que consiste da distribuição dos eventos ocorridos num local (áudio e vídeo) para todos os demais participantes, sendo o áudio o único sinal de retorno, para perguntas de dúvidas ou comentários, por exemplo;
- **Videoconferência** - Serviço similar à conferência audiográfica acrescida do envio, em tempo real, de sinais de vídeo entre os vários participantes.

Outros serviços audiovisuais também se destacam, e tem características bastante próximas, como o compartilhamento dos mesmos padrões e soluções desenvolvidas para teleconferência. São eles:

- **Telefonia Convencional** - Serviço com transmissão full-duplex. Incluída com o intuito de levantar considerações sobre interoperabilidade com os demais serviços;
- **Videofonia** - Serviço com transmissão ponto-a-ponto bidirecional de sinais de áudio e vídeo;

- **Telemonitoramento** - Serviço de transmissão unidirecional de sinais com o intuito de efetuar observação de ambientes. Como exemplo, temos a babá eletrônica, câmeras de vigilância, etc. Ainda não existe proposta de padrão para este tipo de serviço.

O caso particular do serviço de videoconferência inclui diversos serviços como, por exemplo, a conferência audiográfica que não emprega transmissão de vídeo. Por isso a videoconferência, nesse sentido, ocupa um local de destaque.

A videoconferência é uma forma de comunicação interativa que permite que duas ou mais pessoas que estejam em locais diferentes possam se encontrar face a face através da comunicação áudio-visual em tempo real. Reuniões, cursos, conferências, debates e palestras, com a origem e destino de qualquer lugar, são conduzidas como se todos os participantes estivessem juntos no mesmo local.

Com os recursos da videoconferência, pode-se conversar com os participantes e ao mesmo tempo visualizá-los na tela do monitor (telão ou televisão, dependendo dos recursos utilizados), trocando informações como se fosse pessoalmente.

Com a ajuda de um sistema de videoconferência, é possível compartilhar programas de computador, dialogar através de canais de bate-papo, apresentar slides, vídeos, desenhos e fazer anotações em um quadro-branco compartilhado. Nos diversos meios de aplicação, a videoconferência tem trazido inúmeras vantagens, despertando cada vez mais o interesse das pessoas em fazer uso desta tecnologia.

A videoconferência se torna uma ferramenta de apoio no meio educacional, nas escolas, bibliotecas, universidades e em projetos de ensino a distância. Algumas das vantagens trazidas pelo uso desse sistema podem ser percebidas no compartilhamento de recursos com comunidades distantes, a realização de experiências virtuais, quando as reais não são possíveis; a possibilidade de trazer aos alunos as opiniões de importantes especialistas através de palestras; a aplicação de atividades conjuntas como debates e exercícios em grupo e a perspectiva de trazer uma variedade de formas novas de aprendizagem com diversas mídias.

Sem dúvida a utilização de compartilhamento interativo de documentos, de gráficos e de recursos de áudio e vídeo em tempo real, traz motivação no processo

de aprendizagem fazendo com que a matéria dada em aula se torne mais interessante e menos cansativa.

Reuniões empresariais que antes não poderiam ser realizadas por motivo de distância ou por causa dos muitos gastos com viagens e estadias, podem ser feitas utilizando a videoconferência. Além do mais, num momento de crise, a videoconferência poderá auxiliar fazendo a comunicação de empresas matriz e suas filiais para a troca de informações urgentes.

Com o aumento das pesquisas em torno desta nova tecnologia de comunicação, nesses últimos anos, nota-se que ela se encontra operacional. Mas para tal, sabe-se que os protótipos de videoconferência sofrem algumas limitações.

Por exemplo, para se ter qualidade de transmissão e sincronismo de áudio e vídeo a videoconferência deve adotar alguns padrões. Padrão de codificação de mídia não é tudo, caso se deseje um sistema de videoconferência aberto. Deve ser seguida também a codificação de informações multimídia/hipermídia incluindo o sincronismo espacial e temporal das mídias e a descrição da apresentação.

O uso de padrões adequados é muito importante, pois além de permitir a portabilidade do sistema, permite a interoperabilidade com sistemas afins.

A compatibilidade dos serviços de transmissão de mídia pode ser realizada por filtragem se forem adotados e seguidos os padrões.

Um grande problema na implementação de um sistema de videoconferência é a sobrecarga gerada no sistema de comunicação pela transmissão das várias mídias. O sistema deve prover mecanismos de diminuição no fluxo das mídias, em especial o áudio e vídeo, que mais utilizam recursos de banda passante da rede. Tais mecanismos devem evitar, por exemplo, que um vídeo seja transmitido mais de uma vez para uma mesma sub-rede, se possível.

Durante a pré-conferência, que é outra facilidade que o sistema deve oferecer, realiza-se o agendamento e configuração do ambiente, facilidades para manipulação de documentos e trabalho cooperativo, suporte à votação, facilidades para troca de mensagens entre os usuários, possibilidade de gravação da conferência para posterior assistência e, em todas as suas funções, mecanismos de segurança, facilitando assim o momento da videoconferência.

Nos sistemas de videoconferência, o controle de acesso ao ambiente é de difícil implementação. Fazem parte deste mecanismo chave, o gerenciamento de quais participantes tem direito à fala, à manipulação de documentos, etc. em um

dado instante, bem como o controle do período máximo de tempo que cada participante tem, quando detém um controle específico do ambiente. Um sistema ideal deve permitir a configuração completa do acesso às suas facilidades, e se encarregar de gerenciar as regras estabelecidas.

No decorrer deste trabalho será mostrado algumas experiências de implementação do sistema de videoconferência na Universidade Federal de Pelotas.

## 2.2 Modalidades de videoconferência

Existem várias maneiras de dividir os tipos de sistemas de videoconferência, Segundo (WILLEBEEK-LEMAIR & SHAE, 1997) uma divisão desses sistemas pode ser feita da seguinte forma:

- **Baseado em circuito:** utilizam uma conexão dedicada, geralmente RDSI (do inglês, *Integrated Services Digital Network* - ISDN) e padrões codec H.320, não sofrendo interferência do tráfego de outros dados. No entanto, requerem equipamentos adicionais.

Unidades de Controle Multipontos (*Multipoint Control Unit* - MCU) são usadas para conectar as partes em uma mesma videoconferência e controlar como o áudio e o vídeo serão distribuídos para todos os participantes.

- **Baseado em pacotes:** utilizam conexão de dados normais para videoconferência, por exemplo, Ethernet, Token Ring e Frame Relay, entre outros. Não necessitam de MCUs, assim todos os participantes recebem todos os dados da videoconferência. Se for este o caso, os próprios participantes devem fazer o papel do MCU e decidir o que querem ver e ouvir. Nestes sistemas, a videoconferência está sujeita a interrupções causadas pelo tráfego de outras aplicações na rede. O *Multicast Backbone* (Mbone) é um exemplo disto.

Nesta divisão de sistemas de videoconferência baseado em pacotes encontramos a modalidades de conferências ponto-a-ponto e multicast. Na conferência ponto-a-ponto cada um deve rodar o software de videoconferência em seu equipamento através da Internet ou rede conectando-se diretamente através do



número IP. Já na conferência multicast podemos destacar dois tipos de conferência como mostrado abaixo:

- **Conferência em grupo** - é uma conferência interativa onde todos os usuários que estão conectados podem enviar e receber áudio e vídeo
  - proporciona um ambiente colaborativo
  - grupo conecta-se a um software servidor (refletor)
  - grupo tem um endereço IP ou "*host name*"
- **Conferência Cybercast** (ou conferência "*one-way*") - somente o criador da conferência pode enviar vídeo e áudio demais podem ver e ouvir os dados enviados, mas não os podem enviar.

Em sistemas de videoconferência pode-se citar que os principais elementos são (BATES & GREGORY, 1997):

- **Participante:** usuário da conferência com direitos, controlados pelo coordenador, à fala e demais recursos da conferência;
- **Organizador:** indivíduo que tem como tarefa agendar a conferência e, se necessário, divulgar aos participantes a existência da conferência (pode ser um participante, ou não);
- **Coordenador:** participante com direitos especiais sobre todo o controle da conferência (uma conferência pode ser realizada sem a presença deste indivíduo, quando o controle de acessos for realizado pelo próprio sistema);
- **Interlocutor:** participante que detém, em um dado instante, o direito a fala e a alteração dos documentos multimídia/hipermídia (o direito de alteração de documentos pode ser delegado a um secretário);
- **Secretário:** usuário da conferência para quem se delega o direito de escrita nos documentos multimídia/hipermídia da base compartilhada (pode ser um participante ou não);
- **Assento:** dispositivo lógico que pode ser preenchido por um participante ou secretário;
- **Base privada:** sessão de trabalho de um usuário, de acesso e controle restrito a este;

- **Hiperbase ou hiperbase pública:** depósito de documentos persistentes de acesso a todos os usuários da conferência, de acordo com seus direitos;
- **Base compartilhada:** depósito volátil de documentos que possibilita o trabalho cooperativo entre os participantes da conferência (é visível por todos os participantes, mas com controle de alteração realizado pelo sistema).

### 2.3 Características de sistemas de videoconferência

A União de Telecomunicação Internacional (ITU) faz parte da Organização de Nações Unidas, e se encarga no desenrolar das recomendações formais para assegurar que as comunicações a nível mundial se cumpram de maneira efetiva e eficiente. Em 1984 se estabeleceram as primeiras recomendações.

Algumas recomendações e características que podem ser seguidas caso se deseja que o sistema ofereça suporte a videoconferência, são elas: (ITU-T,1992)

- **Qualidade de áudio e vídeo** – na transmissão de mídias de áudio e vídeo os sistemas de videoconferência devem prover os dois tipos de qualidade, a básica e a alta. A básica fornece uma transmissão de sinais de áudio e vídeo com qualidade reduzida, por exemplo, o G.711 e H.261, e a de alta qualidade fornece uma qualidade de áudio e vídeo similar à difusão de sinais de televisão entre outros.
- **Transmissão de imagens estáticas de alta resolução** – permite a troca de imagens de alta definição, por exemplo, num diagnóstico médico o envio de uma radiografia ou exame em ISO JPEG.
- **Criptografia para garantir privacidade** – característica muito importante para sistemas que precisam manter a privacidade e segurança dos participantes da videoconferência. Evitando assim que intrusos decodifiquem mensagens trocadas ou roubem arquivos dos vários participantes. É, portanto essencial em qualquer tipo de serviço de comunicação e fundamental em sistemas de comunicação militares.

- **Transmissão de dados em geral** – pode permitir a transmissão de mensagens textuais, documentos ou dados de banco de dados entre os participantes se o sistema for capaz de manipular e suportar esses tipos de informação.
- **Utilização de câmeras auxiliares** – o sistema de videoconferência pode dar suporte a outras câmeras, onde o usuário escolher qual das várias imagens ele deseja difundir. É interessante o uso das câmeras, como por exemplo, quando um professor deseja mostrar algum experimento a todos os alunos.
- **Gravação da conferência** – gravando a transmissão possibilitará que um usuário seja capaz de assistir uma conferência antiga quantas vezes desejar e possibilitará ao participante que esteve ausente assistir o que perdeu.
- **Existência de um coordenador** (*chairman*) – o coordenador tem direitos especiais sobre todo o ambiente da conferência, algumas das funções são: modificar a prioridade na passagem de permissão, desabilitar qualquer função de qualquer usuário ou mesmo expulsar da conferência um usuário.
- **Identificação do interlocutor** - o sistema oferece algum método que indica qual dos diversos participantes da conferência é o interlocutor do momento.
- **Compatibilidade** - um sistema de videoconferência deve ser capaz de trocar informações com outros sistemas. Sem isso não há transmissão de áudio, vídeo, mensagens instantâneas e muito menos a troca de arquivos. Com uso de padrões comuns como para a codificação de áudio, de vídeo e estrutura do quadro (*frame*) torna possível a compatibilidade entre os sistemas de videoconferência. Exemplos desses padrões são G.711, H.261 e H.221, respectivamente.
- **Controle de acesso** – existem algoritmos que o próprio sistema pode implementar para garantir que apenas um usuário fale ou modifique alguma coisa num determinado instante, indicando qual participante pode acessar os recursos da conferência e com quais direitos. Um sistema ideal deve prover mecanismo de controle de acesso à voz e a manipulação em documentos. O controle de acesso pode ser por acionamento de botão ou por detecção de silêncio.
- **Manipulação cooperativa de documentos** – se durante uma videoconferência, os participantes desejarem ter ferramentas que possibilitem

a manipulação fácil e eficiente dos documentos compartilhados, devem dispor de um completo mecanismo de controle de alterações no documento de forma a evitar inconsistências.

- **Minimização na utilização do sistema de comunicação** - as mídias utilizadas, principalmente áudio e vídeo requisitam muitos recursos do sistema de comunicação, por isso um sistema de videoconferência deve prover mecanismos, como as técnicas de multicasting ou o uso do MCU, para minimizar o uso da banda passante do meio.

## 2.4 Procedimentos para videoconferência

Antes de começar a videoconferência, é necessário serem feitos alguns procedimentos para ajudar na viabilização da transmissão. Dentre eles pode-se citar:

- **Reserva de mecanismo:** onde se aloca equipamentos e salas para a realização da conferência. Nas experiências realizadas na Universidade Federal de Pelotas as câmeras eram emprestadas do NADARTE (Núcleo de Apoio ao Desenvolvimento e à Aplicação de Recursos Telemáticos na Educação) e as salas que já possuíam os demais equipamentos eram utilizadas no CI (Centro de Informática da Universidade) ou o auditório do Prédio da Lagoa Mirim no Campus Pelotas.
- **Pré-conferência:** nesta etapa, que um sistema ideal implementa antes da conferência, o organizador configura o ambiente, agenda a conferência, a divulga aos seus componentes, determina quais participantes terão acesso à mesma, quais os tipos de acessos que cada participante possui, quem é o coordenador (se existir um) e informações para o algoritmo de controle de acesso, dentre outras informações. Assim se houver alguma alteração de informações a tempo de avisar todos os participantes. Por exemplo, no caso de mudança de horário de uma determinada conferência ou ausência de um dos participantes.
- **Conexão do cliente:** é o momento que é inicializado o software do equipamento cliente para assim dar início da participação do usuário na

sessão de videoconferência. Lembrando que o equipamento deve estar habilitado.

- **Gerenciamento da conferência:** pode ser dirigido, quando um usuário é escolhido para ser o coordenador da conferência, ou não dirigido, quando nenhum dos terminais tem prioridade sobre os demais. O coordenador, antes e durante a execução da conferência, pode ter acesso à configuração, em tempo de execução. Como exemplo tem-se a inclusão ou exclusão de um participante, a configuração de acesso de cada usuário e até intervindo no algoritmo de controle de acesso implementado pelo sistema.
- **Muting:** está opção permite que cada participante possa desabilitar as funções de áudio e vídeo na sua sessão de trabalho. Tal desabilitação é ainda mais indicada quando a videoconferência utiliza esquema de detecção de nível de fala para seleção da imagem a ser difundida como nas câmeras que se movem de acordo com a detecção da voz do interlocutor.
- **Início e Término da Conferência:** normalmente a conferência inicia quando o coordenador determinar o momento planejado no agendamento. O término, voluntariamente ou pelo sistema, dá-se quando o último participante se desconectar da mesma, ou quando se esgotar o tempo previsto na pré-conferência, conforme agendado. Quando qualquer participante quiser deixar a conferência, os outros participantes ou, no mínimo o coordenador, devem ser informados. Dá mesma forma acontece quando um participante retornar: o coordenador deve permitir sua entrada.

### III ÁUDIO E VÍDEO STREAMING

O termo streaming vem do inglês que significa algo como “fluxo contínuo”, logo, quer dizer transmissão de áudio e/ou vídeo pela rede. A transmissão de vídeo streaming possibilita a reprodução de dados de mídia contínua em tempo real, sem a necessidade de aguardar a transferência completa do arquivo.

Abaixo estão listados os métodos mais conhecidos de transmissão em vídeo streaming:

#### 3.1 Métodos

Os métodos de Streaming foram baseados pelo material de (MARTINS, 2005) e são eles:

- **Streaming de áudio e vídeo ao vivo** - Nesse tipo de streaming, a informação é gerada em tempo real, ou seja, o computador vai recebendo as informações continuamente enquanto o áudio e vídeo é mostrado ao usuário.
- **Streaming de áudio e vídeo armazenado** - Com o streaming de vídeo armazenado os clientes requisitam arquivos de vídeo que estão armazenados em servidores. Assim o usuário pode controlar o vídeo mostrado à distância, ou seja, no vídeo armazenado o usuário terá controle como, por exemplo, dar pause, play ou stop. A transmissão do conteúdo multimídia só acontecerá sob demanda do cliente, podendo existir vários clientes conectados ao servidor simultaneamente, cada um visualizando um conteúdo diferente.

#### 3.2 Exemplo de Aplicação

##### - Vídeo sob demanda

Permite que os usuários selecionem arquivos multimídia de um servidor central para visualizarem em sua televisão ou tela do computador. Pode ser usado para entretenimento, educação e apoio à videoconferência. Um sistema de vídeo sob demanda é constituído por um servidor, um software cliente e um repositório de dados multimídia. O servidor proporciona uma plataforma completa para integração de áudio e vídeo em aplicações online, utilizando uma arquitetura cliente-servidor para oferecer áudio, vídeo e/ou áudio.

## **- Multicast**

O processo de comunicação de dados multicast oferece vantagens principalmente em aplicações multimídia compartilhadas porque ele é um serviço de rede no qual um único fluxo de dados, proveniente de uma determinada fonte, pode ser enviado simultaneamente para diversos destinatários. O multicast é voltado para aplicações do tipo um-para-muitos e muitos-para-muitos.

O serviço de transmissão unicast é fornecido pela maioria dos protocolos de alto nível (TCP). Com este serviço se um determinado ponto deseja enviar a mesma informação para vários destinatários através deste serviço, então será preciso enviar uma cópia da informação para cada um dos destinatários.

Diferente do que acontece no serviço realizado no transporte multicast, que no tráfego multicast, utiliza-se um endereço IP especial para o envio dos pacotes, que são enviados para endereços de grupo multicast. Caso as estações queiram receber os pacotes que estão sendo transmitidos a um determinado endereço de grupo, estas devem se juntar a este grupo através de procedimentos especiais, como a definição do servidor multicast em seu aplicativo de recepção de áudio e vídeo.

A grande vantagem do tráfego é que ele permite que várias estações vinculadas a um mesmo grupo possam receber simultaneamente os pacotes enviados por um servidor, com isto há economia de banda necessária para suportar uma transmissão de qualidade.

Então como requisito básico para o funcionamento da transmissão é que todos os equipamentos envolvidos suportem o tráfego multicast. Principalmente quando vários sítios estão envolvidos simultaneamente, a utilização do envio de pacotes de maneira seletiva fornece um ganho de processamento de CPU e largura de banda.

Os pacotes no tráfego multicast são enviados em endereços de classe D e recebidos pelas estações que se uniram a grupos multicast. Quando um grupo de

máquinas deseja se comunicar, elas escolhem um endereço multicast para que esta comunicação ocorra. As interfaces de rede são configuradas para reconhecer o endereço selecionado, e todas as máquinas pertencentes ao grupo passam a receber uma cópia de cada quadro enviado para o endereço multicast. IP Multicast é um protocolo para transmissão de datagramas de uma fonte para vários destinatários, em uma rede local ou rede WAN (Wide Area Network.), onde as estações envolvidas utilizam o conjunto de protocolos TCP/IP.

### **Aplicações do serviço nos Negócios**

- Possibilidade de redução de despesas com viagens;
- Gerar, promover e transferir conhecimento e tecnologia;
- Integração das empresas matriz e filiais;
- Possibilidade de fornecimento de serviço a outros órgãos.

### **Aplicações do serviço no Treinamento e Educação**

- Maior abrangência na formação e capacitação de funcionários;
- Economia de tempo e despesas com deslocamento;
- Realização de educação a distância.



## **IV ESTUDO DOS CENÁRIOS DO AMBIENTE DE VIDEOCONFERÊNCIA**

Este capítulo contém algumas pertinentes considerações sobre o ambiente dos participantes, salas de videoconferência e alguns cenários do ambiente de videoconferência.

### **4.1 Ambiente dos Participante**

Tendo em vista o custo benefício, para uma videoconferência de até três participantes, os equipamentos básicos suficientes são: computador pessoal e uma câmera tipo webcam. Um detalhe que deve-se preocupar, com esses recursos, é focar o participante ou o objeto que se deseja mostrar. Já na transmissão de uma reunião, por exemplo, para mostrar outros participantes ou objetos da sala o melhor é a utilização de câmeras com mais recursos de ajustes de foco e zoom.

A câmera utilizada nos experimentos na Universidade possui diversos outros recursos, além dos de ajustes de autofocar, zoom, movimento com a detecção de movimento do interlocutor, entre outros. De acordo com (Cookbook, 2000) “para salas de conferências ou auditórios, uma câmera com mais recursos é essencial e também pode-se ter câmeras auxiliares”.

Também com experiências passadas nas transmissões de videoconferência na Universidade verificou-se a falta de alguns equipamentos de extrema importância e consideração, quando se deseja uma ótima qualidade de comunicação. São eles os microfones e caixas de som.

Quando se trata de um participante que utiliza o computador, para garantir o sistema sem interferência de ecos, fones de ouvido e microfone preso à cabeça é uma solução. Com a câmera utilizada, que oferece o recurso de cancelamento de eco, usar microfones do tipo profissional e autôfalantes tornam a qualidade de áudio melhor. Em mesa redonda com transmissão de videoconferência, por exemplo, a que se utilizou na transmissão da História, ter vários microfones de desktops previne a necessidade de elevação de vozes durante a videoconferência.

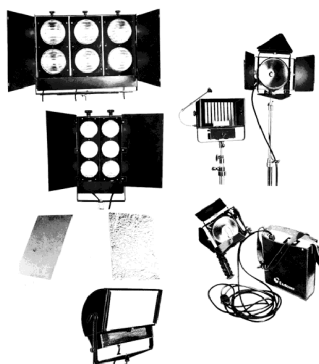
Outro recurso utilizado nas salas de videoconferência, dependendo do tipo de aplicação, é o quadro branco (whiteboard). Nesses quadros, qualquer participante pode interagir com os demais, que visualizarão tudo o que for escrito por teclado ou por mouse.

## 4.2 Salas de Videoconferência

As Salas de Videoconferência são concebidas para uma utilização interativa em rede. Por isso, e também por ser um serviço corporativo dinâmico, uma Sala de Videoconferência deverá ser de uso exclusivo. Algumas características operacionais necessárias são (Neto,1999):

- **Dimensionamento** - Geralmente, as salas para videoconferência são definidas a partir de um layout com capacidade para um público de cerca de 20 pessoas, as dimensões variam conforme o caso.
- **Localização** – No interior de uma sala de videoconferência, o áudio pode ser prejudicado com variadas fontes de ruídos. Por isso, a distancia dessas fontes deve ser relevante para assim reduzir outros custos referentes ao tratamento acústico do ambiente.
- **Iluminação** – Para uma qualidade melhor da imagem é importante seguir esse quatro conselhos referentes à iluminação:
  1. Evitar, sempre que possível, uma sala com janelas. O uso de cortinas pode neutralizar as fontes externas de luz.
  2. A Fonte de luz deve ser do tipo homogênea, preferencialmente como as lâmpadas fluorescentes.
  3. Não deve haver áreas de sombreamento em qualquer extensão da Sala a uniformidade da luz deve se estender em todo o ambiente.
  4. A Intensidade luminosa do ambiente de videoconferência deve estar situada na faixa de 600 a 800 lux.

A figura 4.2.1, mostra alguns equipamentos de iluminação utilizados em estúdios de transmissão.



**Figura 4.2.1:** Luminárias utilizadas num estúdio de transmissão.

- **Acústica** – Não deve existir fontes de interferências internas ou externas que possam afetar a qualidade, já que esta é de extrema importância no serviço de videoconferência. Caso isso não seja possível existe a possibilidade do tratamento acústico do ambiente, garantindo segurança, sigilo da informação dos assuntos abordados. O tratamento acústico consiste no isolamento acústico e o eco na reverberação. O primeiro é a técnica utilizando materiais de isolamento, o segundo tem o objetivo de reduzir as reflexões sonoras no interior de uma sala com tapetes, cortiças ou cortinas, por exemplo. Abaixo na figura 4.2.2 tem-se um exemplo da técnica utilizando materiais de isolamento.



**Figura 4.2.2:** Sala utilizando materiais de isolamento.

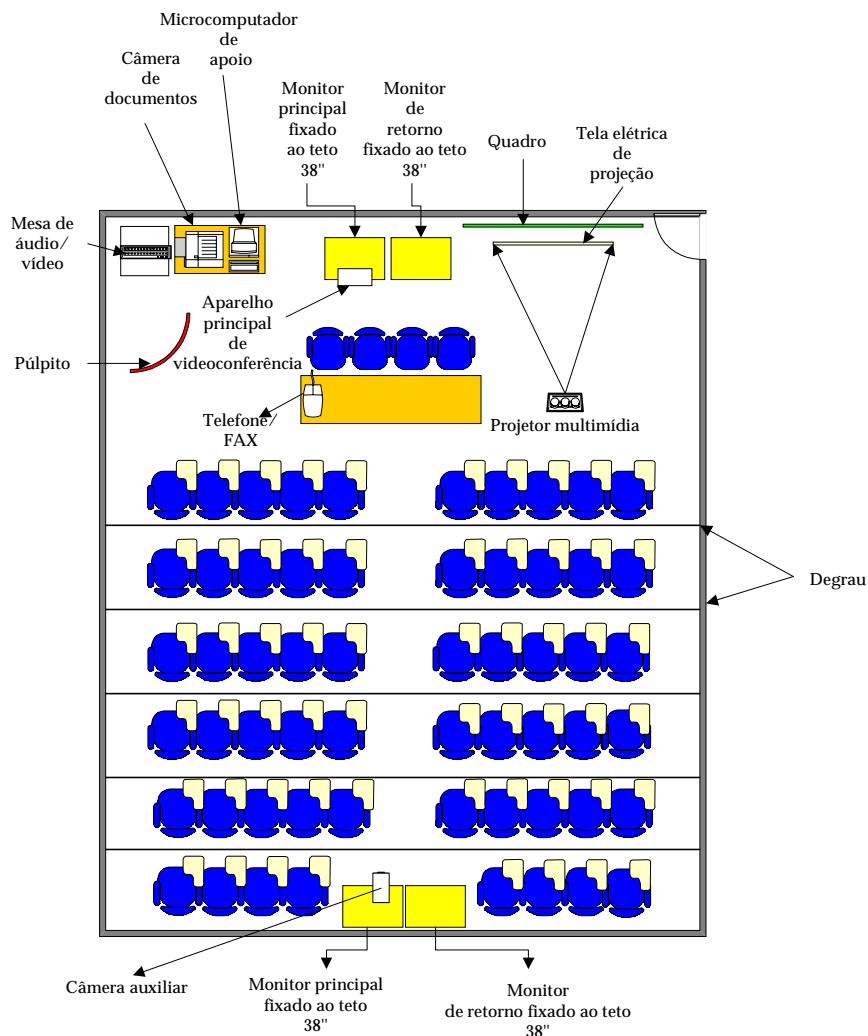
- **Decoração** – A decoração deve ser discreta sem objetos decorativos que chamem atenção dos participantes do evento. Normalmente, uma Sala de Videoconferência poderá dispor de pequenos quadros de avisos, desde que instalados em paredes fora do campo visual da câmera. As cores das

paredes, do material de tratamento acústico, das cortinas, dos móveis, do teto e do piso, deverão ser uniformes, suaves, neutras, claras e todas foscas.

- **Layout** – A ocupação do espaço no interior de uma Sala de Videoconferência define as posições de câmeras, microfones e participantes, as áreas de circulação de pessoas, o posicionamento do mobiliário e dos equipamentos de modo a que os participantes tenham uma visão livre e confortável dos monitores de vídeo, a dimensão da sala segundo à finalidade a que se destina, entre outros. Na figura 4.2.3 e na figura 4.2.4 são mostrados *layouts* de exemplo de salas de videoconferência.



**Figura 4.2.3:** *Layout* da Sala de Reuniões tipo Mesa Redonda.  
Fonte: Núcleo de Multimídia e Internet da Universidade de Brasília.

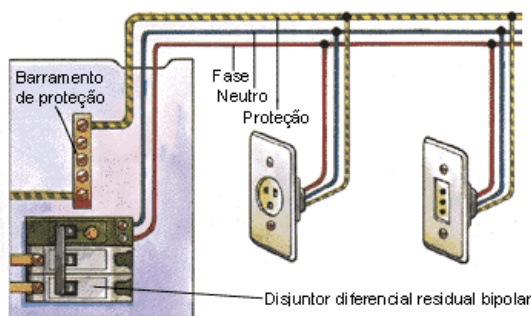


**Figura 4.2.4:** Layout de um Auditório de Videoconferência.

Fonte: NMI da UnB (Núcleo de Multimídia e Internet da Universidade de Brasília).

- **Mobiliário** – A quantidade de mobiliário deve ser definida de acordo com o tamanho da sala. Exemplos de mobiliários são mesa para impressora, mesa para computador, mesa em formato de U com estrutura em madeira ou metal com tampo em madeira de lei clara, sem vidro. As cadeiras e/ou poltronas devem ser confortáveis, com encosto e apoio de braço (com tampo para escrita dependendo da necessidade), podem ser fixas, giratórias e com altura ajustável.
- **Infra-estrutura** - A infra-estrutura é dividida em energia, aterramento e cabeamento para conexão à rede. Abaixo está como cada uma deve seguir:

1. Energia - Uma Sala de Videoconferência deverá ser dotada de tomadas de energia, tipo 3 pinos, com alimentação de 110V ou 220V (de acordo com o projeto a ser definido), localizados conforme o caso em estudo. As tomadas deverão informar a carga máxima possível.
2. Aterramento - Todas as tomadas deverão ter o terceiro pino conectado à malha de aterramento da instalação e isolado do pino "neutro". Abaixo na figura 4.2.5 mostra como deve ser o aterramento:



**Figura 4.2.5: Modelo de Aterramento.**

Fonte: Site da Hidropan Segurança <[www.hidropan.com.br/seguranca10.htm](http://www.hidropan.com.br/seguranca10.htm)>

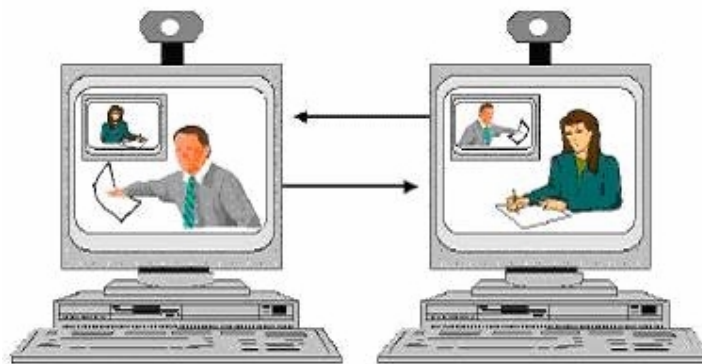
3. Cabeamento de conexão à rede - O cabeamento de acesso à rede de Videoconferência deverá terminar em algum ponto atrás do "rack" da estação de videoconferência.
4. Terminal - Uma Sala de Videoconferência deverá dispor de terminais privilegiados da rede telefônica, para o serviço de FAX e telefonia, conforme projeto.

### 4.3 Cenários

Um cenário é formado por uma ou mais salas e por objetos do ambiente de videoconferência (microfones, câmeras, whiteboards, etc) compostos de acordo com o tipo de encontro desejado entre os participantes, ou seja, quantas pessoas podem

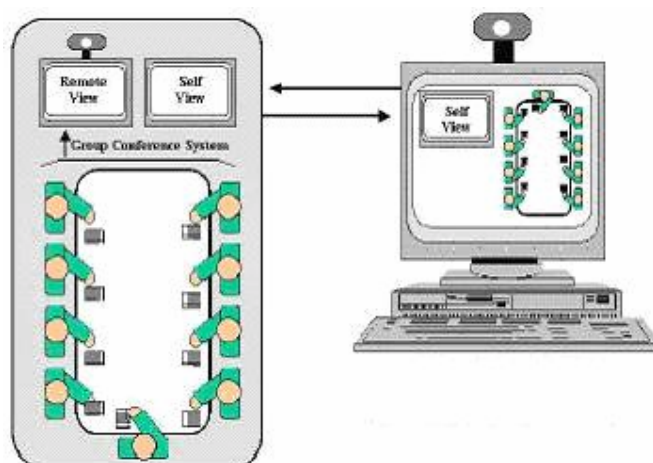
estar participando da sessão de videoconferência e de que forma se sozinhas ou em grupos. A seguir serão apresentados os tipos sugeridos por (Cookbook, 2000):

- **Cenário A:** é aquele no qual a comunicação se dá entre duas pessoas apenas, sendo que cada uma utiliza um computador pessoal devidamente equipado. Geralmente, quando o cenário utilizado é deste tipo, a comunicação estabelecida é ponto a ponto. A Figura 4.3.1 apresenta um esboço deste tipo de cenário, chamado nesta dissertação, de cenário A. Este cenário é o que requer menor custo com equipamentos e preparação do ambiente dos participantes.



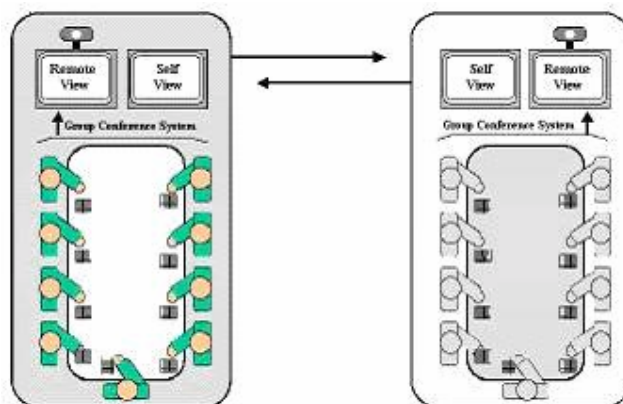
**Figura 4.3.1:** Cenário A Videoconferência Computador para Computador usando o NetMeeting.

- **Cenário B:** é aquele no qual a comunicação se estabelece entre uma pessoa e um grupo. O cenário B, que é mostrado na Figura 4.3.2, é semelhante ao anterior, podendo ter um custo um pouco mais elevado devido à necessidade de ter-se uma sala de videoconferência para comportar o grupo, e considerando que esta será devidamente equipada. Como este cenário envolve um grupo de pessoas em um dos lados, pode ser exigida das sessões de videoconferência um pouco mais de qualidade que no cenário anterior o que justificaria uma seleção mais minuciosa do sistema.



**Figura 4.3.2:** Cenário B Videoconferência Computador para Câmera (de um para um grupo).

- **Cenário C:** envolve comunicação entre grupos, sendo apresentado na Figura 4.3.3. Em termos de comunicação é semelhante aos dois anteriores, mas exigem um sistema de videoconferência com mais recursos. O ideal é que os dois grupos utilizem salas devidamente equipadas para sessões de videoconferência.

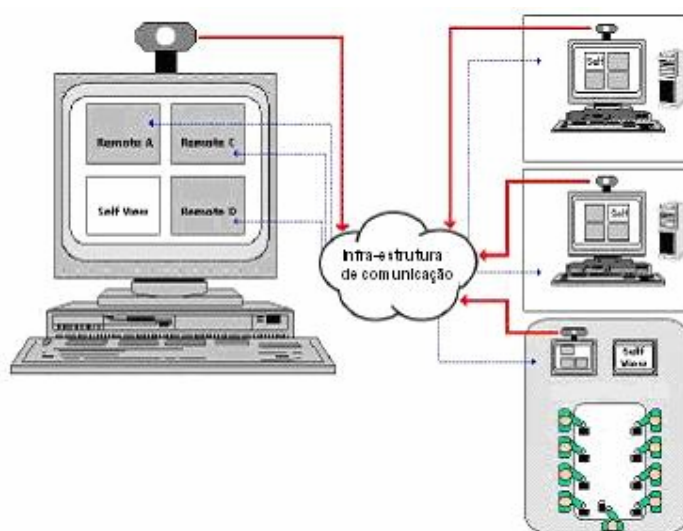


**Figura 4.3.3** Cenário C - Câmera para Câmera (grupo para outro grupo).

- **Cenário D:** este cenário é utilizado na comunicação entre várias pessoas, sendo que cada uma usa um computador pessoal devidamente equipado, e também um grupo que participa em uma sala de videoconferência. A diferença deste cenário para o cenário B é que neste existem mais de dois participantes, justificando a necessidade de um sistema com um controle de acesso mais rigoroso. Quanto maior o número de participantes em pontos remotos, mais difíceis se torna o controle de "quem" estará ativo em um

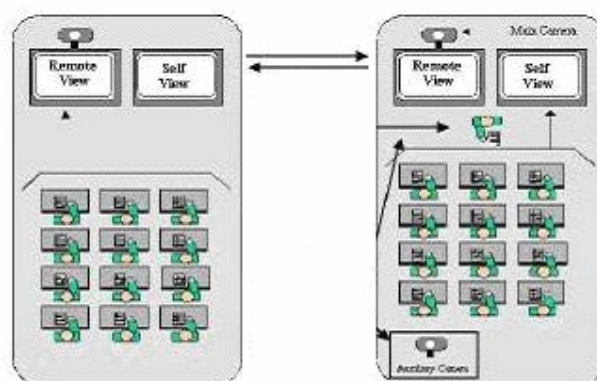


determinado instante da sessão. Um esboço deste tipo de cenário é apresentado na Figura 4.3.4. Exemplo desse cenário é a transmissão da organização do encontro do ALFA-FADO (Formação Avançada e Desenvolvimento Organizacional). O Alfa-Fado tem como objetivo fundamental definir uma estratégia comum para Instituições de Ensino Superior (IES) Européias e Latino-Americanas que lhes permita proporcionar oportunidades de qualificação ao longo da vida, através de formação avançada suportada por e-learning.



**Figura 4.3.4** Cenário D - Diversos Computadores comunicando com uma Sala.

- **Cenário E:** a Figura 4.3.5 mostra um cenário no qual a comunicação, apesar de ser também entre grupos, representa um outro tipo de aplicação de videoconferência que é utilizado para aulas remotas. Neste caso, na maior parte do tempo existe um participante ativo e demais passivo. Um tipo de sistema indicado para este cenário é aquele que, por exemplo, disponibiliza aos alunos remotos um método de acesso por texto, através do qual possam enviar perguntas ao professor. Uma janela aparece na tela do professor com a pergunta, e ele tem a escolha de rejeitá-la ou respondê-la oralmente. Um recurso bastante interessante em cenários deste tipo é o uso de câmeras que, baseadas na detecção de voz, focalizam o interlocutor automaticamente. Neste cenário, poder-se-ia citar o exemplo da aula remota do professor Raymundo Ferreira Filho, caso na sala da disciplina de Inteligência Artificial tivesse os equipamentos de câmera como na figura 4.3.5.



**Figura 4.3.5** Cenário E – Videoconferência em Salas de Aula.

## V PARÂMETROS DE AVALIAÇÃO

Nesta seção se pretende abordar os parâmetros de avaliação de sistemas de videoconferência na Universidade Federal de Pelotas com o intuito de facilitar o trabalho de implantação de sistemas deste tipo. Deve ser lembrado que esses parâmetros dependem das reais necessidades de aplicação e da disponibilidade de recursos para equipamentos e softwares. Os parâmetros estabelecidos são mostrados a seguir (ITU-T, 1992):

- **Recursos disponíveis:** com referência a quantidade de recursos que estão disponíveis no sistema de videoconferência, como por exemplo, a comunicação por áudio, vídeo e dados, além de outros recursos como bate-papo, transferência de arquivos, controle remoto de *desktop*.
- **Qualidade de áudio e vídeo:** avaliar os sistemas de videoconferência quanto à qualidade do áudio e vídeo de acordo com a característica de sua classificação seja ela “básica” ou “alta” como apresentado no item 2.3.
- **Controle de acesso:** como atua em cada um e quais as formas disponíveis - por detecção de silêncio ou outra forma. Este parâmetro está relacionado com a característica "implementação do controle de acesso".
- **Modelo de comunicação:** existem programas que apresentam um melhor desempenho quando utilizado em modelo centralizado, enquanto outros suportam apenas o modelo descentralizado, e todos podem ser utilizados em conjunto, suportando o modelo híbrido.
- **Plataformas suportadas:** é importante saber quais plataformas o software suporta já que atualmente existe uma grande variedade de Sistemas Operacionais.
- **Licença:** este parâmetro avaliará se o software é gratuito ou proprietário. Esta informação pode ajudar quem estiver pretendendo implementar uma solução de videoconferência de baixo custo.
- **Cenário:** serão avaliados para cada software quais os cenários que melhor se adequar. Este parâmetro foi escolhido pelo fato do tipo de cenário estar relacionado ao tipo de comunicação. Assim, para cada tipo de comunicação existe(m) o(s) cenário(s) que melhor se adequa(m).

## VI. CONFIGURAÇÃO DE SISTEMAS DE VIDEOCONFERÊNCIA

Alguns aspectos relativos à rede são pertinentes serem abordados para o melhor entendimento dos testes e transmissões de serviços de videoconferência que foram realizados durante esta monografia. A seguir, serão conceituados alguns fundamentos de rede de computadores para esclarecer os principais problemas relacionados à infra-estrutura básica em relação aos sistemas de videoconferência.

### 6.1 Fundamentos da Rede para Videoconferência

Originalmente, os serviços de videoconferência foram desenvolvidos em redes dedicadas como a ISDN (Integrated Services Digital Network). Esse tipo de rede dedicada fornece alguma garantia sobre o nível do serviço que seria dado as aplicações.

Logo após surgiu a videoconferência baseada em padrão IP, para uma rede de dados sem nenhum padrão de qualidade de serviço com a Internet. Como elas são redes programadas a entrega de aplicações sensíveis pode-se ter aplicações de quase tempo real como no caso a videoconferência IP e também podem ser usada para e-mails, navegação na *Web*, entre outras.

A informação de áudio/vídeo dentro da videoconferência é segmentada em blocos pela aplicação, codificada e comprimida, colocada em uma série de pacotes de dados e enviada pela rede até terminais remotos em intervalos constantes. Os pacotes de dados chegam até seus destinos em um tempo variado, geralmente fora de ordem. Para manter a impressão de “tempo real” de uma videoconferência interativa, os pacotes devem chegar na hora e a tempo de serem reordenados para serem entregues através do terminal de videoconferência.

Na videoconferência através da rede Internet existem cinco problemas de redes fundamentais, são eles: Largura de banda, perda de pacotes, latência, tremulação e políticas.

O requisito fundamental para que se tenha espaço suficiente no curso da rede para que todos os seus pacotes passem desimpedidos é a largura de banda. Numa videoconferência por ISDN para ter idéia de quantidade, usa de 128 a 384

Kbps (kilobits por segundo) já sistemas de vídeo H.323 baseados em IP podem usar a mesma largura de banda, embora normalmente tendem a ir mais alto pela rede ser barata atingindo uma largura de banda de 384 a 768 Kbps.

Perda de pacotes é quando os pacotes falham e não chegam corretamente. Isso pode ocorrer devido à largura de banda insuficiente ao longo do caminho (quando congestionamento ocorre, os *routers* derrubarão pacotes) ou talvez erro na transmissão. Os erros ocorrem mais comumente em conexões *wireless* (sem fios) como microondas, satélites ou *Ethernet* local *wireless*. Eles também podem ocorrer em cobre e mesmo em conexões de fibra. A perda de pacotes resulta em efeitos como “*tiling*” dentro da janela de vídeo, perda de pedaços ou áreas em branco dentro da janela de vídeo e/ou interrupção no áudio.

Outro problema de rede é a latência, ou seja, o atraso de tempo entre o acontecimento de um evento e o terminal remoto vendo ele. A latência é introduzida pelos processos de codificação/decodificação e, portanto, depende do equipamento usado e também pelo tempo que os pacotes levam para atravessar a rede.

Quando ocorre latência excessiva há uma maior chance de um interlocutor sobrepor o outro, ou seja, os dois interlocutores falarem ao mesmo tempo sem perceber. Em chamadas com menos de 50 ms de latência de rede isso torna-se menos significativo já em chamadas maiores com uma latência de 150 ms tornar-se muito enervante. Outro problema é que a latência para o áudio e o vídeo pode ser diferente, e, então, o movimento dos lábios não aparece sincronizado com o áudio.

Tremulação é a variação aleatória na latência devido a coisas como processos que competem rodando no terminal (por exemplo, no *desktop* de seu computador pessoal), outro tráfego bloqueando temporariamente o caminho através dos *routers* ou mesmo a mudança de caminho da rede durante a videoconferência. A variação aleatória é um dos vários aspectos que faz os pacotes chegarem fora de ordem de que foram transmitidos. A tremulação resulta em qualidade irregular e imprevisível dentro de uma videoconferência, e o terminal cliente tentará compensar isso fazendo *buffering* do tráfego por algum tempo limitado antes de rodá-lo para você. Isso aumenta mais ainda a latência.

As políticas são introduzidas por meios como *firewalls* e dispositivos de tradução de endereço de rede (NAT) que são geralmente usados para tentar esconder ou proteger os elementos da rede da Internet mais ampla. O H.323 usa portas alocadas dinamicamente e, desse modo, não é muito amigável a *firewalls*.

## 6.2 Conceitos de Rede de Computadores

De acordo com (SOARES,1995) uma rede de computadores é formada por um conjunto de módulos processadores capazes de trocar informações e compartilhar recursos, interligados por um sistema de comunicação.

Os componentes básicos em uma rede de computadores são:

- Software de rede – É encarregado pelo controle de mais alto nível da comunicação de uma rede de computadores.
- Camadas de rede – Serve para simplificar o projeto da rede.
- Protocolos – É um conjunto de regras sobre o modo como se dará à comunicação entre as partes envolvidas.
- Hierarquia de rede – É a maneira como as camadas da rede se comunicam entre si.

As redes de computadores podem ser divididas em LANs (Local Area Network) são aquelas em que os recursos se localizam num espaço físico comum (um andar de escritório, um edifício etc), MAN (Metropolitan Area Network) são redes de abrangência metropolitana restringindo-se às conexões dentro de uma cidade (com velocidades em torno de 10 Mbps), depois tem-se o meio termo que são as WANs (Wide Area Network) que possuem uma abrangência geográfica grande e dispersa com diversos equipamentos interligados ao longo da rede.

As transmissões que ocorrem no canal da rede podem ser definidas de acordo com o sentido como:

- Simplex: A transmissão é feita em um único sentido.
- Half-duplex: A transmissão é feita nos dois sentidos, mas não ao mesmo tempo.
- Full-duplex: A transmissão é feita nos dois sentidos simultaneamente.

Segundo (WIRTH,2001) a maneira como um nó envia um pacote pode ser:

**Multicast** - Quando um nó (qualquer dispositivo conectado a rede) envia um pacote endereçado a um grupo especial de endereços. Um exemplo seria um roteador enviando atualizações para todos os outros roteadores.

**Broadcast** – Quando um nó envia um pacote, que deve ser transmitido para todos os outros nós da rede.

### 6.3 Equipamentos de Rede de Computadores

Nesta subseção farei um breve resumo de alguns equipamentos que fazem com que a rede esteja habilitada para o serviço de videoconferência.

#### 6.3.1 Host

*Host* é um servidor que disponibiliza e os clientes, ou *guests* acessam os recursos disponibilizados.

Na internet é um computador que tem acesso bidirecional completo a outros computadores. Um *host* tem um número específico que, somado ao número da rede, formam seu endereço IP. O *host* armazena, centraliza e distribui arquivos ou recursos (modem, impressora, etc.), serviços de correio eletrônico, redes de impressão entre outros serviços que serão acessados pelos demais micros da rede. Numa rede como a Internet todos os computadores são chamados de *host*, independentemente de disponibilizarem algo. Sua capacidade vai de um micro a um supercomputador.

#### 6.3.2 Hub

*Hub* é um equipamento que é o ponto de conexão central para o cabeamento de uma rede. O *Hub* permite conectar dois ou mais segmentos *Ethernet*. Quando os sinais de transmissão se começam a deteriorar, o que é causado pela limitação do comprimento dos cabos, o *Hub* simplesmente repete e amplifica o sinal para todas as portas que lhe estão conectadas. Um *Hub*, também chamado de *Repeater* (Repetidor), permite apenas que os utilizadores compartilhem *Ethernet*. Os pontos em uma rede partilhada podem apenas obter uma porcentagem da banda de rede, pelo que uma rede de *Repeaters* é muitas vezes apelidada de

"*Shared Ethernet*". Todos os nós do segmento *Ethernet* irão partilhar o mesmo domínio de colisão.

Um domínio simples de colisão consiste em um ou mais *Hubs Ethernet* e nós conectados entre eles. Cada aparelho dentro do domínio de colisão partilha a banda de rede disponível com os outros aparelhos no mesmo domínio. *Switches* e *Bridges* são utilizados para separar domínios de colisão que são demasiado grandes de forma a melhorar a performance e a estabilidade da rede.

### 6.3.3 Switch

A função de um *Switch* é conectar diferentes redes. Um *Switch* mapeia endereços *Ethernet* dos nós que residem em cada segmento da rede e permite apenas a passagem do tráfego necessário. Quando um *Switch* recebe um pacote, determina qual o destino e a origem deste, e encaminha-o para a direção certa. O *Switch* larga o pacote se a origem e o destino são no mesmo segmento de rede. Os *Switches* também previnem que pacotes danificados se alastrem por toda a rede, melhorando assim a eficiência da transmissão dessa rede.

Existem duas arquiteturas básicas de *Switches* de rede: "cut-through" e "store-and-forward". Os *Switches* "Cut-through" apenas examinam o endereço de destino antes de reencaminhar o pacote. Um *Switch* "store-and-forward" aceita e analisa o pacote inteiro antes de o reencaminhar. Este método permite detectar alguns erros, evitando a sua propagação pela rede. Hoje em dia, existem diversos tipos de *Switches* híbridos que misturam ambas as arquiteturas.

### 6.3.4 Diferença entre Hub e Switch

Embora aparentemente ambos sirvam para conectar computadores em rede, há uma diferença significativa entre ambos. O *hub* é um mero repetidor. Se o computador pessoal ligado à porta 1 quiser trocar informações com o computador pessoal ligado à porta 4, as informações (pacotes de rede) serão replicadas para todas as outras portas do *hub* ao mesmo tempo. Isto causa dois problemas. Primeiro, baixa o desempenho da rede, como o *hub* replica as informações para todas as suas portas, é como se todos os computadores pessoais estivessem ligados em um único cabo, e se o cabo está sendo usado, nenhum outro PC pode



usar o cabo ao mesmo tempo. Ou seja, no exato momento que o primeiro PC estiver se comunicando com o quarto computador pessoal, nenhum outro computador pessoal poderá usar o cabeamento da rede (note que as transmissões de dados em uma rede são divididas em pequenos fragmentos chamados quadros; este impedimento que descrevemos refere-se à transmissão de um quadro e não à totalidade dos dados que estão sendo transmitidos). O segundo problema é em relação à segurança da rede. Como os dados são replicados para todas as portas, um PC conectado a uma das portas do *hub* pode facilmente ver todo o tráfego da rede – incluindo tudo o que você faz na Internet que não seja criptografado –, através de um programa do tipo *sniffer*. Já um *switch* é como se fosse um *hub* que analisa os quadros. Nele, se o primeiro PC da rede quiser se comunicar com o quarto PC da rede, ele irá chavear a comunicação somente entre estas duas máquinas, não replicando os quadros para todas as demais máquinas da rede. Assim, o *switch* tem duas grandes vantagens sobre um *hub*. Primeiro, faz com que a rede não baixe o seu desempenho quando duas máquinas estão trocando informações entre si. E, segundo, oferece mais segurança, já que em um ponto de rede um hacker não encontrará todos os quadros que circulam na rede, somente os quadros direcionados àquela máquina específica.

### 6.3.5 Roteador

Um dispositivo de rede que permite interligar redes distintas. A Internet é composta por inúmeros roteadores interligados entre si. Ao acessar um site qualquer, a requisição trafega por vários roteadores, até chegar ao destinatário e os dados enviados por ele fazem o caminho inverso para chegar ao seu micro. O nome "roteador" é bastante sugestivo, pois os roteadores são capazes de definir a melhor rota para os pacotes de dados, evitando roteadores que estejam sobrecarregados ou que não estejam funcionando. Um roteador pode ser tanto um dispositivo dedicado (no caso dos roteadores de maior porte) quanto um computador pessoal com duas ou mais placas de rede rodando um sistema operacional com suporte a esta função.

Os roteadores são capazes de unir os *backbones* da Internet e encaminhar milhões de pacotes de dados por segundo. Pode também ser utilizado para unir duas redes que utilizem protocolos de rede distintos, já que estes aparelhos operam

na camada de protocolo do modelo OSI, eles são capazes de entender os pacotes de dados e alterá-los caso necessário, eles podem endereçar os pacotes tanto baseados no endereço TCP/IP quando no endereço físico (MAC) das placas de rede. Os *bridges* e *switches* por sua vez operam na camada física da rede, ou seja, são capazes de reconhecer apenas o endereço MAC das placas, mas não os endereços ou dados transmitidos. É por isso que ao contrário dos roteadores eles não são capazes trabalhar com duas redes distintas, ao unir duas redes através de um *switch* elas passam a formar uma única rede.

### 6.3.6 Bridge

Para Wirth as “*Bridges*” manipulam pacotes diferentemente dos “*repeaters*” que só tratam de sinais elétricos e desta forma possuem a vantagem sobre os “*repeaters*” de não retransmissão de erros, ruídos ou quadros mal formados. São Usadas para reduzir tráfego, fracionar uma rede local em sub-redes e converter diferentes tipos de LANs.

### 6.3.7 Diferença entre Roteador e “Bridge”

Uma “*bridge*” é usada como um repetidor, quando se deseja interligar dois segmentos de rede, atuando na camada de enlace, ou seja, uma “*bridge*” possui software próprio, que analisa os endereços físicos de origem e de destino dos computadores envolvidos na conexão e só faz a retransmissão para o outro segmento, se o segundo computador estiver neste outro segmento.

Uma “*bridge*” só pode unir segmentos de rede que possuam a mesma tecnologia , ou seja, os dois segmentos de rede precisam utilizar o mesmo tipo de pacote e controle, como por exemplo utilizar os mesmos tipos de placas de rede.

Um roteador também une dois ou mais segmentos de rede, porém atua na camada de rede, o que possibilita a união de dois ou mais segmentos de rede com tecnologias diferentes (*gateways*).

### 6.3.8 ALPINE

De acordo com o Professor Adenauer Yamin, que trabalha no gerenciamento da rede da UFPel, o *Alpine* é um chassis equipado com *switches* destinado a gerenciar o meio físico (usado na interligação de prédios) não local.

O chassis dos *switches Alpine 3800* são ideais por fornecer serviços IP de banda larga para redes de Área Metropolitana (MANs), provedor de serviço, data centers empresariais e edifícios *multi-tenant*. A plataforma *Alpine* fornece total cobertura *Ethernet* com suporte para as medias Categoria 5 padrão e fibra ótica bem como as tecnologias que estendem o alcance de *Ethernet* sobre tecnologias VDSL e WAN.

No *Alpine 3804* há cinco *slots* com capacidade *non blocking* de 32Gbps. O primeiro *slot* de cada chassis é utilizado para o módulo de gerenciamento do *switch* (SMMi), o qual executa todas as funções de gerenciamento, controla o encaminhamento da base de dados e tabelas de roteamento, e processa todas as atualizações dos protocolos de roteamento. Os *slots* restantes de cada *switch* da série *Alpine 3800* são utilizados para módulos permutáveis.

### 6.3.9 Frame Relay

Frame Relay é uma técnica de comutação de pacotes baseada em um conjunto de protocolos especificados pelo ITU-T, sendo a técnica mais recomendada para implementação de redes WAN para conectividade entre hosts e redes locais.

As principais vantagens do Frame Relay são: tamanho variável de pacotes; controle de tráfego, evitando situações de congestionamento da rede; apenas um nível de encapsulamento e menor tráfego.

A tecnologia Frame-Relay permite a multiplexação de várias conexões lógicas (circuitos virtuais entre equipamentos ligados à rede) através de um único meio físico. Essas conexões podem ser do tipo permanentes ou comutadas, embora a maioria das redes Frame Relay existentes opere apenas em modo permanente.

### 6.3.10 Gateway

O “gateway” por sua tradução é um “portão de entrada” que faz a ligação de redes diferentes através de duas maneiras: num computador com no mínimo duas

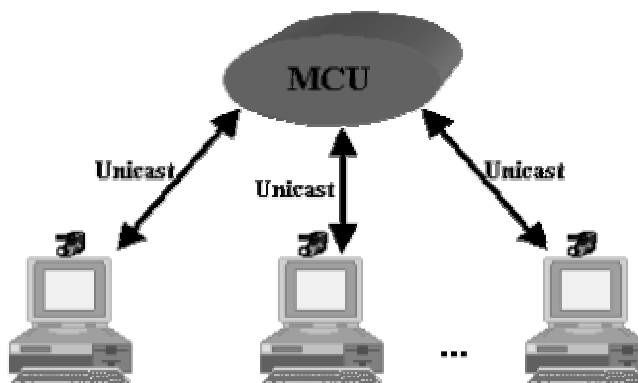
placas de rede ou simplesmente através de um dispositivo dedicado. Com o gateway é possível unir duas redes com protocolos diferentes e até mesmo compartilhar a conexão de Internet entre diversos computadores se configurado corretamente.

Para WIRTH um “gateway” é um elemento de rede, que atua como um ponto de entrada para uma outra rede. Um acesso “gateway” é um “gateway” entre a rede telefônica e outras redes, como por exemplo, a Internet.

O gateway é um elemento da conferência que promove vários serviços, sendo o mais importante à função de tradução de algoritmos de terminais de videoconferência H.323 para outros tipos de terminais (H.320, por exemplo). Esta função inclui tradução entre transmissão formata e entre procedimentos de comunicações. Além disso, o Gateway também traduz entre codecs de áudio e vídeo e executa configuração de chamada (TAROUCO, 2003).

### 6.3.11 Multipoint Control Unit

O MCU (Multipoint Control Unit) cria salas de reuniões virtuais com participantes de várias localizações. O propósito de um MCU é conectar três ou mais sistemas de videoconferência na mesma conferência, administrando o áudio e o vídeo de cada participante de forma que a comunicação de grupo seja alcançada. Abaixo na figura 6.3.11 está o exemplo de uma videoconferência de modelo centralizado com o MCU.



**Figura 6.3.11:** Videoconferência de Modelo Centralizado MCU.

**Fonte:** Site <<http://www.cirp.usp.br/secoes/screde/videoconf/videoconf.html>>

### 6.3.12 Gatekeeper (Controle de Rede)

Segundo (WIRTH, 2001) o conceito de “gatekeeper” é o cérebro de rede H.323, o qual executa um controle essencial, com funções administrativas e

gerenciais, a fim de manter a integridade da rede, tanto em ambiente de empresa, como em ambiente de distribuição.

O “gatekeeper” é o ponto chave de redes multimídia baseadas em H.323, que é uma norma implementada em redes através de zonas. Zonas são o conjunto de pontos finais sobre o poder de um e apenas de um “gatekeeper”. Na zona podem estar inclusas quaisquer números de terminais, “gateways” e Unidades de Conferência Multiponto.

São quatro funções que o “gatekeeper” deve obrigatoriamente fazer:

- 1) Tradução de endereço – proporciona a tradução de endereços entre o nome e o endereço de transporte referente a uma solicitação de um terminal para um serviço.
- 2) Controle de admissão – autorizam o acesso enviando mensagens de acordo com as diretrizes de policiamento, que o administrador de rede selecionou, quando fez a configuração do “gatekeeper” e/ou zona.
- 3) Controle da banda passante – monitora e controla o uso de banda passante da rede e assegura que o tráfego de áudio e vídeo, não exceda a carga máxima da rede.
- 4) Gerenciamento da rede – usa um modelo de sinalização roteada de chamada, para rotear sinalização de chamada e controle de canais para uma entidade apropriada na rede.

O gatekeeper que gerencia é uma aplicação na forma de um programa que segue a recomendação H.323 do ITU-T e, apesar de ser um elemento opcional para videoconferência, é essencial para o gerenciamento da rede multimídia sob IP.

Segundo (TAROUCO, 2003), um Gatekeeper é o componente mais importante de uma rede H.323. Ele age como o ponto central para todas as chamadas dentro de sua zona e provê serviços de controle de chamada para estações registradas. Em muitas implementações, um Gatekeeper H.323 age como um interruptor virtual.

### **6.3.13 Domain Name Service/Domain Name System**

De acordo com (WIRTH, 2001) o serviço de nome de domínio ou DNS (Domain Name Service/Domain Name System) como é comumente conhecido, é um dos mais importantes da Internet. Quando se acessa uma página em algum servidor Web através de um browser ou se envia um e-mail, para citar dois exemplos práticos

do dia-a-dia, o DNS está sempre presente traduzindo os nomes de domínio usados em seus respectivos endereços IP. Ou seja, traduzir um endereço do tipo `www.ufpel.edu.br` num endereço IP do tipo `200.255.253.1`.

#### 6.3.14 Firewall

À medida que o uso de tecnologias da computação avança, a proteção dessas informações e sistemas requerem a aplicação de ferramentas e conceitos de segurança eficientes. O *firewall* é uma opção praticamente imprescindível. É obrigação de todo administrador de rede manter essa barreira de proteção.

*Firewall* para (Soares) pode ser visto como um monitor de referências para uma rede, sendo seu objetivo garantir a integridade dos recursos ligados a ela. O *firewall* controla o tráfego de dados entre um computador e a Internet (ou entre a rede onde este computador está instalado e a Internet). Seu objetivo é permitir somente a transmissão e a recepção de dados autorizados. Existem *firewalls* baseados na combinação de hardware e software e *firewalls* baseados somente em software. Este último é o tipo recomendado ao uso doméstico e também é o mais comum.

Explicando de maneira mais precisa, o *firewall* é um mecanismo que atua como "defesa" de um computador ou de uma rede, controlando o acesso ao sistema por meio de regras e a filtragem de dados. A vantagem do uso de *firewalls* em redes, é que somente um computador pode atuar como *firewall*, não sendo necessário instalá-lo em cada máquina conectada.

Há mais de uma forma de funcionamento de um *firewall*, que varia de acordo com o sistema, aplicação ou do desenvolvedor do programa. No entanto, existem três categorias principais: filtros de pacotes, *gateways* de circuitos e *gateways* de aplicação.

- **Filtros de Pacote** – para redes pequenas ou de médio porte, utilizam endereços IP de origem e destino, e portas UDP (Protocolo para usuário de conjunto de dados) e TCP (Protocolo para Controle de Transmissão) para tomar decisões de controle de acesso. Uma desvantagem é que as regras aplicadas podem ser muito complexas e causar perda de desempenho da rede ou não serem eficazes o suficiente.

- **Gateways de Aplicação** – voltado a redes de porte médio ou grande, utilizam implementações especiais das aplicações, desenvolvidas especificamente para funcionar de forma segura.
- **Gateways de circuitos** – atua como intermediário de conexões TCP, funcionando como um Proxy TCP (um TCP modificado).

### **Razões para utilizar um firewall**

As três razões principais são:

- 1) Para ajudar a impedir que sua rede ou seu computador seja acessado sem autorização. Assim, é possível evitar que informações sejam capturadas ou que sistemas tenham seu funcionamento prejudicado pela ação de *hackers*;
- 2) No combate a vírus e cavalos-de-troia, uma vez que é capaz de bloquear portas que eventualmente sejam usadas pelas "pragas digitais" ou então bloquear acesso a programas não autorizados;
- 3) Evitar que os usuários de redes corporativas acessem serviços ou sistemas indevidos, além de ter o controle sobre as ações realizadas na rede, sendo possível até mesmo descobrir quais usuários as efetuaram.

Através dos estudos realizados na rede da Universidade descobriu-se que o *firewall* também é responsável pelo roteamento da rede interna.

### **6.3.15 Network Address Translation**

O NAT (Network Address Translation - Tradução de Endereço de Rede) possibilita troca de informações, pois é um recurso que permite converter endereços da rede interna em endereços da Internet. O uso mais comum deste recurso é compartilhar a conexão com a Internet. O compartilhamento pode ser feito usando um computador pessoal com duas placas de rede, um modem ADSL com hub embutido, um roteador, etc. Segundo (WIRTH, 2001) o NAT simplesmente faz a tradução de endereços válidos na Internet para os endereços reservados e vice-versa. Com isso, todos os equipamentos de rede interna/fechada passam a ter acesso a Internet. O NAT pode fazer uma tradução de endereços no estilo um-para-

um, no qual cada endereço interno tem um respectivo válido na Internet, ou uma tradução no estilo vários-para-um, no qual todos os endereços internos são traduzidos para um único endereço válido globalmente. Enquanto a primeira prática não é muito comum e em nada contribui para a economia de endereços IP, a segunda é a mais indicada e muito popular.

Existem vários programas que permitem compartilhar a conexão usando o NAT, uma opção é o Internet Connection Sharing do Windows, mas existem proxys com recursos semelhantes, como por exemplo o Wingate. A vantagem destes sobre os proxys manuais é o fato da conexão ser quase totalmente transparente. Todos os computadores pessoais podem ser configurados para acessar diretamente a Internet, usando o servidor NAT como “gateway”, dispensando a configuração manual de proxy em cada programa.

O servidor fica conectado simultaneamente às duas redes, à Internet e à rede local onde estão os demais computadores pessoais. Ele pode ter o endereço IP 224.217.65.34 na Internet e o IP 192.168.0.1 na rede local, por exemplo. Se um dos computadores pessoais da rede local abre uma página no <http://www.ufpel.edu.br> por exemplo, o pedido será enviado ao servidor, que por sua vez o encaminhará para o endereço correspondente na Internet e devolverá a resposta para o computador pessoal da rede local.

O mais interessante é que o computador pessoal local enxerga apenas o servidor de conexão e fica invisível para todos os demais computadores pessoais da Internet, que novamente verá apenas o servidor e não os computadores pessoais da rede local. É por isso que o provedor de acesso não pode fazer nada para impedir que os usuários compartilhem a conexão via NAT, eles simplesmente não têm como obter nenhuma prova de que a conexão está sendo compartilhada.

O NAT, de maneira geral, pode ser implementado junto ao roteador ou a um computador executando um software firewall (de segurança). Qualquer um destes dois equipamentos seja um computador ou um roteador, que possua pelo menos duas interfaces de rede, ligando a rede pública (a Internet e, possivelmente, a parte externa da rede da empresa) à rede privada (rede interna/fechada da empresa). Com isso, as vantagens são muitas. Além da economia dos endereços IP válidos globalmente, pode-se destacar também (SOARES, 1995):

- \* Segurança dos computadores e da própria rede interna, uma vez que usuários na Internet não terão como acessá-los diretamente, pois os endereços



reservados não são válidos para uso na Internet. Todos os equipamentos internos ficarão “escondidos”.

\* Facilidade de reconfiguração do NAT, em caso de mudança no bloco de endereços IP válidos na Internet. A numeração interna não é afetada. A mesma facilidade se aplica no caso da rede fechada já suportar o TCP/IP, tendo seus computadores já numerados com endereços reservados, e for ligada à Internet pela primeira vez. Nesse último caso, não haverá praticamente mudanças na rede existente.

Embora apresente muitas vantagens, o NAT também tem suas desvantagens. A principal talvez seja o fato de que o uso do NAT degrada a performance da comunicação. Uma vez que toda a troca de informações terá que passar pelo equipamento que está implementando o NAT e este terá que realizar a tradução, o equipamento em questão sofrerá uma expressiva sobrecarga, entretanto, um hardware robusto minimiza este problema. É bom lembrar mais uma vez, que o NAT traz mais segurança à rede interna, um aspecto cada vez mais importante para qualquer empresa que já ligou ou pretende ligar a sua rede à Internet.

### **6.3.16 Ethernet**

A Ethernet<sup>1</sup> é uma rede de computadores pessoais que surgiu junto com os primeiros microcomputadores, o Altair e o Apple. Um padrão muito usado para a conexão física de redes locais. Descreve protocolo, cabeamento, topologia e mecanismos de transmissão. A informação pode ser transmitida em modo Broadcast. É de relativa facilidade de instalação e manutenção em redes de pequeno porte, o que a tornou popular. Para redes maiores, a instalação do cabeamento, e a administração podem ser mais complexas, especialmente porque nestes casos, vários cabos diferentes podem estar interconectados, com diferentes velocidades e tecnologias de comunicação, além da necessidade de possuir Servidores com grandes capacidades. A velocidade nominal da tecnologia Ethernet varia de 10 a 1000 megabits por segundo, onde Fast Ethernet compreende a taxa de transferência de dados com 100 megabits por segundo e Giga Ethernet a 1000 megabits por segundo.

---

<sup>1</sup> A Ethernet foi desenvolvida na Xerox em 1976, por Bob Metcalfe e David Boggs.

A Ethernet foi definida pelo IEEE (Institute of Electric and Electronic Engineers) como a norma 802.3, que permite um débito normalizado de 10 megabits por segundo, além de outros débitos consoante o suporte utilizado. Muitas vezes o termo Ethernet também é utilizado para designar uma rede que funciona segunda esta tecnologia.

Estrutura do quadro Ethernet, figura 6.3.16 segundo (TANENBAUM,1989):

<b>Preâmbulo</b>	<b>End. Destino</b>	<b>End. Origem</b>	<b>Tipo</b>	<b>Dados</b>	<b>CRC</b>
------------------	---------------------	--------------------	-------------	--------------	------------

Figura 6.3.16: Estrutura Ethernet.

- Preâmbulo (8 bytes): bytes responsáveis pela sincronização inicial da transmissão.
- Endereço de destino (6 bytes): endereço físico de destino (para broadcasting, todos os bits setados);
- Endereço de origem (6 bytes): endereço físico do adaptador que transmite o quadro;
- Campo de Tipo (2 bytes): identificador do protocolo da camada de rede;
- Campo de Dados (46 a 1500 bytes): carrega o datagrama IP;
- Verificação de Redundância Crítica (CRC - 4 bytes);

Características da Ethernet:

- A Ethernet fornece à camada de rede um serviço não orientado á conexão;
- Não há confirmação de recebimento de quadros;
- Falha na verificação do CRC resulta em rejeição do quadro, sem retransmissão;
- Os dados podem ter lacunas, podendo ser recebidos ou não conforme o protocolo de transporte usado;
- Por sua simplicidade, a Ethernet é uma tecnologia barata.

A Ethernet usa o protocolo CSMA-CD

- Um adaptador de rede pode transmitir quando quiser;
- O protocolo usa detecção de portadora;
- Usa detecção de colisões;
- Antes de tentar a transmissão, espera um tempo aleatório (menor que o tempo de quadro).

### **6.3.17 Asymmetric Digital Subscriber Line**

ADSL (Asymmetric Digital Subscriber Line), tecnologia de acesso rápido que usa as linhas telefônicas oferecida em várias cidades. As velocidades variam em geral de 256 kbits a 2 mbps, dependendo do plano de acesso escolhido. A principal virtude é não usar o sistema telefônico comutado, dispensando o assinante de pagar pulsos, apenas a tarifa mensal.

Para isso, é instalado um modem ADSL na casa do assinante e outro na central telefônica. Os dois modems estabelecem uma comunicação contínua, usando frequências mais altas que as utilizadas nas comunicações de voz, o que permite falar no telefone e usar o ADSL ao mesmo tempo. O modem instalado na central é ligado diretamente ao sistema do provedor, sem passar por outras centrais telefônicas.

O sistema ADSL (SOARES,1995) está baseado em um avançado processamento de sinais digitais e de algoritmos, para comprimir as informações, possibilitando a transmissão de altas taxas de transmissão, através de um par trançado de cobre, usado na telefonia fixa. Adicionalmente, muitos avanços na tecnologia ADSL devem-se ao aperfeiçoamento de transformadores, filtros analógicos e codificadores A/D.

Podemos entender o sistema ADSL (WIRTH, 2001), como sendo vários canais transparentes de transmissão, com varias taxas de transmissão através de um par trançado de cobre, entretanto, dentro dos equipamentos, onde está a telefonia, é um verdadeiro milagre da moderna tecnologia.

Para criar múltiplos canais, os modems ADSL dividem a faixa passante disponível de uma linha telefônica através de uma das duas maneiras: FDM (Frequency Division Multiplex) ou o Cancelamento e eco. O sistema FDM atribui uma banda para o sentido "Uplink" e outra banda para o sentido "Downlink". O sentido

“Downlink” é dividido através de multiplexação TDM (Time Division Multiplexing), em um ou mais canais mais rápidos e em um ou mais canais lentos. No sentido “Uplink” também existe multiplexação em canais de dados mais lentos.

O sistema de Cancelamento de eco atribui a banda para “Uplink” para sobrepor-se a faixa de “Downlink” e separa as duas faixas por meio de cancelamento local de eco, uma técnica utilizada pelos modems V.32(Padrão da ITU para modulação de dados, usado por modems analógicos nas transmissões a 4.800 bps e a 9.600 bps) e V. 34(Padrão da ITU para modulação de dados, usado por modems analógicos nas transmissões a 28.800 bps, 24.000bps e 19.200 bps).

Através destas duas técnicas o sistema ADSL também separa a região da banda em POTS de 4Khz.

Um modem ADSL organiza os dados criados pela multiplexação no sentido “Downlink”, os canais duplex e os canais de manutenção em blocos e anexa uma codificação de controle de erro para cada bloco.

O receptor pode corrigir erros que ocorrem durante a transmissão, usando a codificação para correção de erros.

#### **6.3.18 Assynchronous Transfer Mode**

O ATM (Modo de Transferência Assíncrono) foi proposto pela Bellcore, uma entidade que está ligada à AT&T nos EUA e à várias empresas de telecomunicações na Europa. É uma tecnologia de transmissão e comutação de dados que pode ser usada para a transmissão de informações em aplicações de natureza e requisitos de performance distintos, englobando desde TV, telefonia, som e dados de computadores.

No que se refere à transmissão de dados de computadores, a tecnologia ATM pode ser aplicada tanto em redes de computadores locais (LAN) como em redes de longo alcance (WAN), o que é muito útil para a criação de internetworking, ou seja, a criação de backbones baseados em ATM.

A tecnologia ATM foi desenvolvida pela organização internacional ITU-T durante o desenvolvimento da arquitetura B-ISDN (Broadband Integrated Services Digital Network), que por sua vez foi à evolução para banda-larga da ISDN, cujo

objetivo foi o de integrar todos os possíveis serviços de comunicação (TV, telefone, fax, transmissão de dados) sob uma única tecnologia.

O ATM é baseado na transmissão de pequenos pacotes de tamanho fixo, estrutura definida chamados de células e na multiplexação por divisão de tempo assíncrona (ATDM), não havendo alocação fixa de intervalos de tempo nas conexões. Aqui é dispensado o uso de protocolos de correção de erros, porém, para que a integridade dos dados seja assegurada, ele depende da integridade das linhas digitais. Com o ATM é possível trabalhar a velocidades que variam desde 50 Mbit/s até mais que 1 Gbit/s. Estas células são transmitidas através de conexões de circuitos virtuais estabelecidos, sendo sua entrega e comutação feitas pela rede baseado na informação contida no cabeçalho da mesma.

### **Transmissão em Redes ATM**

A tecnologia ATM (SOARES, 1995) é baseada na técnica de comutação de pacotes (packet switching) e de multiplexação estatística de circuitos – alocação de largura de banda conforme a demanda. As informações a serem transmitidas são agrupadas em células de tamanho fixo e com identificadores de conexão, cujo fluxo ordenado constitui o que se convencionou chamar de circuito virtual, que substitui o circuito de banda passante das técnicas TDM e FDM.

A camada ATM fornece um serviço do tipo orientado a conexão (connection-oriented) para as camadas superiores através dos circuitos virtuais, que deve ser estabelecido antes de qualquer transmissão de dados.

Existem várias tecnologias de transmissão no meio físico que suportam ATM, entre as quais SONET, fibras óticas, cabos STP/UTP, etc.

### **Mercado da ATM**

Atualmente o uso mais comum do ATM é para workgroup LANs. Esta é uma LAN na qual cada uma das workstations estão conectadas a um comutador ATM local. Um adaptador para ATM LAN é instalado em cada workstation, tipicamente esta conexão trabalha na ordem de 51 Mbit/s, 100 Mbit/s ou 155 Mbit/s.

O emprego tímido do ATM em WANs deve-se a duas razões. Primeiro, por ser considerada nova, necessita que padronizações e implementações sejam estabelecidas; segundo está relacionado ao custo. Em contraste com tecnologias

hoje utilizadas (backbones FDDI ou Switch Ethernet), o ATM é ainda muito caro por ser uma tecnologia nova.

### **Vantagens e Desvantagens da Tecnologia ATM**

Uma das vantagens da tecnologia ATM (SOARES, 1995) é que ela não utiliza a alocação e nem monopoliza canais. Outras vantagens são obtidas com o uso de células com tamanho tão reduzido. Quanto maior o tamanho da célula, maior é o tempo de empacotamento, resultando em um atraso na transferência desta. Para os serviços sensíveis ao tempo de atraso, como vídeo e áudio, o alongamento do tempo de atraso provoca uma queda na qualidade, gerando distorções e eco na transmissão de voz.

Por outro lado (WIRTH, 2001), os pacotes ATM apresentam uma certa ineficiência. Como 48 dos 53 bytes das células que estão disponíveis para os dados, as cargas úteis em cada célula é de apenas 90% (48/53), tendo um desperdício de 10% com informações contidas no cabeçalho. Isto torna-se mais grave, quando 49 bytes em dados são transferidos, pois são utilizados duas células de 53 bytes. Como a segunda célula carregará apenas 1 byte de informação, a eficiência neste caso é de apenas 45%.

### **Futuro do ATM**

A tecnologia ATM foi desenvolvida para o tráfego de dados em redes de alta velocidade, principalmente dados multimídia como voz e vídeo em tempo real. Para atingir estes objetivos, foi necessário o desenvolvimento de comutadores rápidos e eficientes. Estes comutadores podem apresentar uma gama muito variada de formas de implementação dependentes do fabricante.

Embora o custo dos comutadores e equipamentos básicos para a montagem de uma rede ATM sejam bastante elevados, a escalabilidade, banda de passagem e alta velocidade compensam os gastos com a tecnologia.

Esta nova tecnologia, filosoficamente semelhante ao sistema telefônico, levará a uma mudança extrema nas redes de comunicação atuais, tornando possível à integração das mídias mais populares como TV, telefonia e computadores.

## 6.4 Gerenciando os serviços de videoconferência

Para descrever como funciona o sistema de videoconferência como um todo, pode-se destacar os seguintes etapas (COOKBOOK, 2005): primeiramente tem-se as entradas de *mixers* de áudio (microfone e auto-falante), da câmera, do monitor (vídeo ou VGA) e podendo se necessário ter os *whiteboards*. Em seguida os *codecs* (Codificador/Decodificador) que fazem a administração e também a compressão do áudio, vídeo e o conteúdo de dados e enviam os dados comprimidos para fora do terminal remetente até o terminal receptor. Outra etapa necessária é processo de habilitar a comunicação interativa entre participantes através da rede para fornecer um meio para se conectar com os outros terminais. Para melhorar a funcionalidade dos serviços de videoconferência existem alguns componentes como os “*gatekeepers*” (servidores de chamadas), os “*gateways*” e os MCUs ( Unidade de conferência Multiponto). Logo a seguir será explicado cada um deles.

Com relação à topologia física, projetistas de redes comutadas por pacotes devem procurar:

- A obtenção do menor número de saltos possível entre os dois pontos finais de conexão, de forma a diminuir a probabilidade de perdas e congestionamentos;
- A largura de banda em cada trecho da conexão, de forma a garantir o recurso requisitado pela aplicação;
- O uso de *multicast*, para evitar a necessidade de maior largura de banda (e custo, conseqüentemente) na WAN, e permitir o uso de soluções multiponto na LAN;
- Topologias que favoreçam a QoS (Qualidade de Serviço). Na LAN *Ethernet*, a colisão deve ser totalmente evitada (ainda que exija o uso de um segmento *Ethernet* exclusivo para o CODEC);
- Projetos que adotem ativos de rede, topologias e protocolos que permitam isolar na mesma rede o tráfego multimídia dos demais, favorecendo o QoS.

## **VII ESTUDO DAS APLICAÇÕES DOS PROTOCOLOS DE REDES**

Neste capítulo será abordado os protocolos principais para a comunicação de sistemas de videoconferência. Alguns desses protocolos não foram utilizados durante as experiências realizadas enquanto ocorreram testes e transmissões, mas são protocolos muito utilizados na transmissão de áudio e vídeo, por isso se tornou necessário abordar algo sobre esses protocolos.

### **7.1 Internet Protocol**

O IP (protocolo de Internet) é um conjunto de 32 bits que atribui o endereço de um computador em redes TCP/IP com o propósito de localizá-lo dentro da internet. É o protocolo da camada 3 de rede na arquitetura ISO (FALBRIARD, 2002). Entre suas funções. Proporciona uma conexão para protocolos de nível superior, assumindo funções como rastrear endereços de nós, rotas para envio de mensagens recebidas, além de se responsabilizar por localizar e manter o melhor caminho de tráfego na topologia da rede. O IP, nada mais é que a um protocolo de identificação do seu computador na Internet.

Existem dois tipos de IP, IP dinâmico e IP fixo ou estático, o IP dinâmico é aquele que muda ou varia dentre determinados endereços IP a cada conexão, já para se obter um IP fixo precisa pagar para um provedor. A única desvantagem do IP fixo é que deixa o computador que o tem mais identificável na rede.

### **7.2 Transmission Control Protocol**

O TCP (Transmission Control Protocol) é um protocolo de transporte padronizado para a interligação de redes baseadas em IP. Operando no topo do IP, é responsável pela multiplexagem de sessões, recuperação de erros, confiabilidade



da ligação extremo a extremo e controle de fluxo. É um protocolo padrão da Internet de camada de transporte orientado à conexão e orientado a stream, ao contrário do UDP.

De acordo com (FALBRIARD, 2002), o propósito do protocolo TCP é fornecer um circuito lógico robusto com serviços de conexão entre um par de processos. O protocolo não espera encontrar rede e enlaces com transporte garantido ou livre de erros, mas tenta fornecer a robustez exigida pelos próprios mecanismos do protocolo de transporte.

### **7.3 User Datagram protocol**

O UDP (User Datagram protocol), protocolo padrão da Internet de camada de transporte não orientado à conexão que adiciona um nível de confiabilidade e multiplexação ao IP. O UDP é um protocolo bem mais simples e o serviço por ele fornecido é apenas a multiplexação/demultiplexação do acesso ao nível inter-rede

Segundo (FALBRIARD, 2002), o UDP fornece serviços de entrega sem conexão e por intenção sem nenhum controle de transmissão ou tentativa de recuperação. O UDP utiliza os datagramas IP para o transporte das mensagens entre vários equipamentos até com a possibilidade de distribuí-las para vários participantes da rede.

### **7.4 TCP/IP (Transmission Control Protocol / Internet Protocol)**

O TCP/IP (rede de multiserviço) é a plataforma de protocolos originária da rede ARPA, também conhecida como conjunto de protocolos da Internet, que combina o TCP e o IP.

A arquitetura TCP/IP baseia-se num serviço de transporte orientado à conexão, fornecido pelo TCP (Transmission Control Protocol), e em um serviço de rede não orientado à conexão (datagrama não confiável), fornecido pelo protocolo IP. A arquitetura TCP/IP dá uma ênfase toda especial à interligação de diferentes tecnologias de redes.

No nível de aplicação, os usuários usam programas de aplicação para acessar os serviços disponíveis na rede. Algumas aplicações disponíveis na Internet TCP/IP (SOARES, 1995) são:

- Simple Mail Transfer Protocol (SMTP) que oferece um serviço store-and-forward para mensagens que carregam correspondências contendo textos.
- File Transfer Protocol (FTP) que fornece o serviço de transferência de arquivos.
- TELNET que oferece o serviço de terminal virtual.
- Domain Name System (DNS) que oferece um serviço de nomes em endereços de rede.

Nos serviços de transporte com várias opções de conexão e confiabilidade (os protocolos TCP e UDP), a função básica é permitir a comunicação fim-a-fim entre aplicações.

O nível de inter-rede é o responsável pela transferência de dados através da inter-rede, desde a máquina de origem até a máquina destino. Por exemplo, tem o serviço de entrega dos pacotes sem conexão (datagrama IP, ICMP e ARP).

Quaisquer tipos de rede podem ser ligados, bastando para isso que seja desenvolvida uma interface que compatibilize a tecnologia de rede com o protocolo IP, essa é a função do nível de interface de rede.

## **7.5 Dynamic Host Configuration Protocol**

O DHCP (Dynamic Host Configuration Protocol) segundo (WIRTH, 2001) tem o papel fundamental de facilitar a configuração de computadores de uma rede. Ele centraliza e gerencia a alocação a configurações TCP/IP a todos os computadores de uma rede que estejam configurados como clientes DHCP.

O DHCP é uma ferramenta para controle dinâmico de IPs em uma rede interna. Ele permite que um administrador defina dinamicamente características aos clientes que conectarem a rede.

Isso elimina a necessidade de se configurar informações de rede como DNS, Gateway e endereços de IP nos clientes, ficando tudo de uma maneira fácil, e automática. O DHCP é também vital quando utilizado em grandes redes, onde

manter sob controle todos os endereços e configurar novos clientes pode gerar uma grande dor de cabeça.

Outra vantagem é a reutilização de endereços IP, tão logo um cliente se desconecte da rede, o mesmo endereço usado por ele pode ser utilizado para o próximo cliente.

## **7.6 Internet Group Management Protocol**

O protocolo de gerenciamento de grupo, IGMP, é usado pelas estações de trabalho para reportarem seus participantes de grupos de estações, a roteadores multicast vizinhos. É um protocolo assimétrico e é parte integral do IP, sendo um requisito básico de implementação a todas as estações de trabalho que desejam enviar e receber pacotes multicast. A distribuição de tráfego multicast em uma rede é efetuada inicialmente pela configuração das estações, para recebimento do tráfego. Esta configuração é feita pelo IGMP que usa datagramas IP para transmitir suas mensagens.

## **7.7 Real Time Transport Protocol**

- Protocolo RTP de transporte para aplicações transmite dados em tempo real;
- Não fornece garantia de qualidade em tempo real;
- O transporte de dados é acrescido por um protocolo de controle – RTCP, que permite o monitoramento da entrega dos dados;

## **7.8 Real Time Control Protocol**

- O protocolo RTCP (Real Time Control Protocol) é usado para comunicação entre as origens e os destinos, carregando avaliações na qualidade de entrega de dados e informações dos membros, trabalhando junto com o protocolo RTP.
- Informações de controle da sessão para manter a alta qualidade das sessões;

- Apresenta relatórios dos pacotes que foram enviados.

## **7.9 Session Initiation Protocol**

- Criação, modificação e finalização de sessões;
- Gerenciamento dos participantes das chamadas: durante a sessão, um participante pode “trazer” outros usuários para dentro da sessão, pode transferir uma chamada ou pode cancelar conexões. Esse tipo de característica permite a criação de serviços avançados associados à sinalização, de modo simples e rápido.

## **7.10 Real Time Streaming Protocol**

- Ao invés de armazenar grandes arquivos de multimídia, estes são usualmente enviados através da rede em fluxos.
- Os dados são quebrados em pacotes em tamanhos determinados pelo emissor e o receptor, assim um cliente pode “tocar” o primeiro pacote, descomprimir o segundo e estar recebendo o terceiro.
- Deste modo o usuário não precisa esperar que todo o conjunto de dados chegue a sua máquina.
- Prove as funcionalidades como de um controle remoto. (avanço, retrocesso, pausa,...) e pode ser usado tanto em dados ao vivo como em mídias armazenadas.
- Também trabalha com muitos usuários em um ambiente multicast ou apenas um usuário em *unicast*.

## **7.11 Transmissão Multicamadas**

- A transmissão multicamadas visa transmitir para o cliente o dado separado em  $n$  camadas, onde a primeira tem o vídeo representado em uma qualidade de vídeo mais baixa;

- Conseqüentemente necessitando uma largura de banda menor e com uma prioridade mais elevada, a cada nova camada a qualidade do vídeo vai aumentando.

## 7.12 Padrão H.323

- É um padrão aprovado pela International Telecommunication Union (ITU) que define como um dado audiovisual é transmitido por uma rede.
- O H.323 é parte de uma série de padrões de comunicações que permitem videoconferência através de redes e também a compatibilidade com dezenas de aplicações de telefonia pela Internet.
- Provê uma arquitetura, ação de dados multimídia, para redes baseadas no protocolo IP.
- Permite que produtos multimídia e aplicações de fabricantes diferentes possam interoperar de forma eficiente e que os usuários possam se comunicar sem preocupação com a velocidade da rede.
- O fluxo e dados em redes podem ser administrados. O gerente de rede pode restringir a quantidade de largura de banda disponível para conferências.

### 7.12.1 Modo de Operação

O H.323 é um documento base que faz referencia a um conjunto de protocolos e formatos de mensagens definidos em outros documentos. Verifique na tabela 7.1 abaixo, a relação das recomendações ITU-T definidas para dar suporte à sinalização H.323.

**Tabela 7.1:** Recomendações ITU-T que suportam a sinalização H.323

<b>Recomendação ITU</b>	<b>Título</b>
H.225.0	Call Signaling protocols and Media Stream Packetization form Packet-Based Multimedia Communication Systems
H.235	Security and Encryption of H-Series Multimedia Terminals
H.245	Control Protocol for Multimedia Communication
H.350.x	Directory Services Architecture for Multimedia Conferencing

H.450.x	Supplemental Services for H.323
H.460.x	Guidelines for the Use of the Generic Extensible Framework
Série T.120	Data Protocols for Multimedia Conferencing

Também temos o H.248 conhecido como protocolo Megaco, é um padrão desenvolvido cooperativamente entre o ITU e a IETF para permitir que um media gateway controller (MGC) controle um media gateway (MG). Competindo com outros protocolos como o MGCP e MDCP, é considerado um protocolo complementar ao H.323 e ao SIP, no qual o MGC controla os MGs via H.248 mas comunicará com outro via H.323 ou SIP.

O protocolo H.245, transmitido através de TCP, é utilizado para interligar todas as entidades H.323. É utilizado para negociar facilidades entre os participantes de uma chamada H.323, tais como abertura e fechamento de canais lógicos (portas UDP para transporte de fluxos RTP- Real-Time Protocol e RTCP – Real-Time Control Protocol).

### 7.12.2 Benefícios

- Padrões de *codec*: H.323 (ITU-T, 1992) estabelece padrões para compressão e descompressão de dados de áudio e vídeo;
- Interoperabilidade: comunicação sem preocupação de velocidade;
- Administração de largura de banda: tráfego de vídeo e áudio demandam alta largura de banda -> congestionamento da rede
- Flexibilidade
- Suporte multiponto
- Independência de plataforma e aplicação
- Independência entre redes
- Segurança

### 7.13 Áudio

Existem ainda os codecs, protocolos extras que adicionam funcionalidades e maior qualidade à comunicação. Entre os tipos possíveis de áudio especificados pelo padrão H.320, tem-se:

- **G.703** - É uma recomendação (ITU-T, 1992) que trata das especificações da interface física a quatro fios e para transmissão digital a 2,048 Mbps. Geralmente, é utilizado para se referir à interface de transmissão européia a 2,048 Mbps.
- **G.704** - Recomendação do ITU para estruturas de quadros síncronos usados nos seguintes níveis hierárquicos: 1544, 6312, 2048, 8488 e 44736 kbit/s.
- **G.711** - Padrão do ITU (Union International telecommunication) para compressão de voz;
- **G.722** – codec de áudio que consomem 128 Kbps de largura de banda;
- **G.723** - Algoritmo utilizado para compressão de voz e supressão de silêncio de um sinal digital cuja variante mais conhecida é o G-723.1, que consegue converter um sinal PCM de entrada de 64 kbps em uma saída que pode variar de 5,3 a 6,4 kbps.
- **G.726** - Especificação do ITU-T para codificador de voz ADPCM trabalhando na faixa de 16 a 40 kbps.
- **G.728** - codec de áudio em canais com banda de 16 kbps.
- **G.729** - Algoritmo utilizado para compressão de voz e supressão de silêncio de um sinal digital, que consegue converter um sinal PCM de entrada de 64 kbps em uma saída de 8 kbps.

O que os diferencia são os algoritmos usados, a média de atraso e principalmente a qualidade da voz. Neste último aspecto, o G.711 é considerado excelente.

Os sistemas que possuem uma qualidade mínima de áudio e vídeo suportam apenas áudio G.711. O áudio G.711 possui qualidade de telefonia (banda estreita, 3Khz) e consome 48-64 Kbps de largura de banda. Já os sistemas que possuem a qualidade mínima e todos os fatores opcionais suportam áudio G.722, o qual possui qualidade estéreo (banda larga, 7Khz), e consomem 128 Kbps de largura de banda. Os sistemas que possuem qualidade mínima e alguns fatores opcionais, opcionalmente podem implementar áudio G.722. O áudio G.728 surge com uma opção para sistemas com baixas taxas de transmissão. Este tipo de áudio consome apenas 16 Kbps de banda. Os melhores produtos para videoconferência permitem ao usuário escolher o tipo do áudio a ser utilizado.

### 7.14 Outras Tecnologias Existentes

Outra tecnologia existente e que foi desenvolvido pelo ITU é o padrão H.320. Trata-se de um conjunto de protocolos que especifica a comunicação multimídia de áudio e vídeo fim-a-fim, cujo principal componente é o protocolo H.261.

O H.261 é o responsável pela codificação e compactação de sons e imagens. Seu algoritmo é bastante similar ao da técnica MPEG, e prevê a geração de taxa constante de bits - ainda que para isto a qualidade do vídeo se torne variável (há alteração no número de quadros por segundo) - para uso com taxas de bits medidas em múltiplos de 64 Kbps.

O H.320 também pode ser utilizado sobre ambiente ATM. A vantagem é a alta largura de banda, muito mais caro que as interfaces ATM. Com alta largura de banda disponível, o algoritmo de compactação não necessita funcionar com eficiência máxima, o que diminui também o retardo de CODEC. E, finalmente, o ATM provê QoS (Qualidade de Serviço) fim-a-fim. Este é, sem dúvida, o ambiente ideal para suportar aplicações multimídia.

Enquanto utilizado como tecnologia de LAN, o ATM provê o QoS necessário para garantir o funcionamento da aplicação multimídia mesmo em uma rede com alto tráfego de dados. O problema do uso de videoconferência sobre ATM é o alto custo de links ATM de longa distância, pois os maiores benefícios da aplicação são obtidos justamente no uso em WANs. Caso o projetista opte por utilizar ATM neste cenário, deve considerar ainda o uso de CODECs padrão H.321 – este padrão é ligeiramente diferente do H.320, na verdade é uma otimização específica para o ambiente ATM. Outro aspecto a se considerar é a existência de uma rede pública baseada em ATM, condição necessária para organizações viabilizarem interconexão (e a realização de sessões de videoconferência com estas conexões) sem que tenham que fazer parte de uma mesma rede privada.

Mas o cenário mais comum no ambiente corporativo é formado pela utilização de redes padrão Ethernet e do protocolo TCP/IP. A grande base instalada e a tendência de mercado de convergência para estas tecnologias impõem aos fornecedores de soluções multimídia para redes a necessidade de se adaptar a este ambiente, sob pena de perder mercado.



A implementação de redes multiserviços com Ethernet e TCP/IP é um desafio, pois estes protocolos não oferecem suporte aos requisitos de QoS exigidos (largura de banda, atraso, variação do atraso e taxa máxima de perda de pacotes). A substituição dos protocolos por outros com capacidades de QoS resolve um problema mas cria outro – perde-se interoperabilidade.

Assim, dotar ambientes Ethernet e TCP/IP de capacidades de QoS exigidas por aplicações de videoconferência significa agregar mecanismos e recursos que permitam garantir banda, priorizar o tráfego, evitar colisões, segmentar a rede e rotear o tráfego de forma otimizada (uso de multicast, por exemplo). Alguns destes itens serão obtidos com cuidados de projeto (segmentação da rede, por exemplo), outros implicam em uso de protocolos e/ou ativos de rede que possuam capacidades de QoS.

De forma bastante resumida, pode-se citar como cuidados mínimos o uso dos protocolos RTP (Real Time Protocol) e o RTCP (Real Time Control Protocol) para suporte à priorização do tráfego, o RSVP (Resource Reservation Protocol) para reserva de banda, e uso de multicast na LAN. Além disso, os roteadores deverão ter capacidade para priorizar o tráfego (por protocolo, porta, interface ou criando um circuito virtual dedicado à conexão multimídia) e os switches deverão suportar recursos de camada 4 ou superior (para realizar a priorização do tráfego). Estas exigências sugerem o uso destes serviços na rede privada da organização (intranet), uma vez que é dentro de sua área de autonomia que o administrador da rede terá autonomia para configurar os componentes de forma a atender aos requisitos necessários.

O padrão desenvolvido pelo ITU para a utilização de multimídia em redes comutadas por pacotes é o H.323, cujo principal componente é o protocolo de compactação H.263. Este último é baseado no (e compatível com) protocolo H.261.

Utilizado em ambiente TCP/IP, fica clara a necessidade do H.263 ser mais eficiente que o H.261 para trafegar os dados da sessão de videoconferência com a mesma largura de banda, uma vez que o TCP/IP impõe maior overhead de encapsulamento.

Além das vantagens já citadas anteriormente (custo e base instalada do ambiente Ethernet e TCP/IP), deve-se considerar também a possibilidade de uso de soluções baseadas em computador (CODEC de software instalado em um microcomputador acoplado a uma câmera e kit multimídia), o menor custo dos

equipamentos e dos links (utiliza-se o mesmo link WAN da rede de dados, tarifada da forma mais conveniente – custo fixo, variável ou combinado) e a facilidade de integração com outras aplicações (Vídeo sob demanda, distribuição de vídeo para Internet).

As principais desvantagens estão no menor grau de QoS, a dificuldade de interoperar com pontos conectados por meio de núvens públicas, maiores exigências de performance dos CODECs em relação aos padrões H.320 e H.321 e necessidade de cuidados de projeto para a implementação dos serviços.

#### **7.14.1 Interoperabilidade**

Quando utilizadas soluções que adotam protocolos proprietários, a interoperabilidade fica comprometida ou limitada ao suporte oferecido pelo fabricante.

Supondo que a escolha da solução tenha adotado padrões abertos (como o H.320 e o H.323, por exemplo), duas questões devem concentrar a atenção do projetista em relação à interoperabilidade.

A primeira se refere à necessidade de realizar uma sessão de videoconferência utilizando equipamentos baseados em diferentes padrões, quando será necessário o uso de gateways. Tipicamente este é o caso de uma expansão do parque multimídia instalado, onde os equipamentos mais novos em geral implementam padrão H.323 e os mais antigos utilizam H.320. Este também é o caso quando se torna necessário fazer com que um microcomputador ligado a uma rede TCP/IP consiga interoperar com um CODEC H.320 em uma rede ISDN.

Finalmente, quando o administrador de rede é requisitado a implementar uma sessão de videoconferência entre um CODEC baseado em hardware e uma solução baseada em software, deve ter em mente que a qualidade de áudio e vídeo estará limitada à menor das capacidades, ou seja, ao tamanho de janela, quantidade de cores e taxa de quadros por segundo atingida pelo componente de menor performance. Recomenda-se também o uso da configuração de computador mais potente disponível à época, para minimizar o atraso introduzido pelo processamento da digitalização e da compactação realizada pelo software de videoconferência.

### 7.14.2 Tendência

A tendência de convergência atual aponta para o uso de TCP/IP, e na área de videoconferência não é diferente. Os fabricantes mais antigos, voltados para soluções baseadas em H.320 já possuem ao menos um modelo disponível no padrão H.323, e há fornecedores exclusivamente focados neste padrão.

Com o crescente aprimoramento dos mecanismos de QoS para redes Ethernet e TCP/IP, e o custo de links WAN caindo, o uso de H.323 na intranet é a solução mais indicada. Na extranet, porém, o padrão H.320 é a escolha obrigatória, uma vez que a Internet não oferece o QoS necessário. Os padrões para a Internet2 ainda estão sendo definidos, mas é provável que esta substitua os enlaces ISDN para a realização de videoconferências na Extranet em um futuro próximo.

Enquanto o cenário das redes públicas não fica definido, a melhor opção é adquirir equipamentos que suportem os dois padrões, ou seja, compatíveis com H.320 e com H.323. Assim, o investimento fica preservado, uma vez que é possível utilizá-lo na Intranet com TCP/IP e na Extranet com ISDN ou X.21, mas não de forma simultânea – não se trata de um gateway, mas sim de um CODEC compatível com mais de um padrão. Sessões multiponto serão o passo seguinte à implementação do serviço, isto quando não fazem parte da especificação inicial.

Na LAN o uso de multicast evita a necessidade de envio de vários pacotes unicast, um para cada CODEC destino. Na WAN otimiza a topologia de distribuição dos pacotes (spanning tree). O multicast, entretanto, é uma capacidade de redes comutadas por pacotes.

Algumas soluções de software possuem suporte a sessões multiponto onde apenas um participante pode transmitir a cada instante do tempo. O controle da sessão é realizado por um dos pontos (o "administrador da conferência"), dispensando os custos de aquisição de um MCU – um dos componentes mais caros da arquitetura de vídeo para redes.

## VIII INFRA-ESTRUTURA DE REDES DA UFPEL

Muitos problemas enfrentados pelos sistemas de videoconferência poderiam ser eliminados quando se tem operadores que conhecem os conceitos fundamentais de rede de computadores. Assim poderão resolver os problemas que ocorrerem com o funcionamento na utilização da infra-estrutura de rede.

É necessário que a infra-estrutura de rede utilizada nos sistemas de videoconferência forneça os serviços de transmissão e conectividade de dados com uma determinada qualidade.

Segundo (TAROUÇO, 2003) os sistemas de videoconferência rodam sobre a infra-estrutura de redes, logo, quaisquer problemas operacionais existente nos diversos elementos da infra-estrutura acabam influenciando diretamente no desempenho das sessões de videoconferência. Apesar de as estruturas específicas para videoconferência serem complexas por si só, prestar atenção somente em tais estruturas não é suficiente para garantir o sucesso das comunicações: a infra-estrutura de redes também precisa do mesmo nível de atenção.

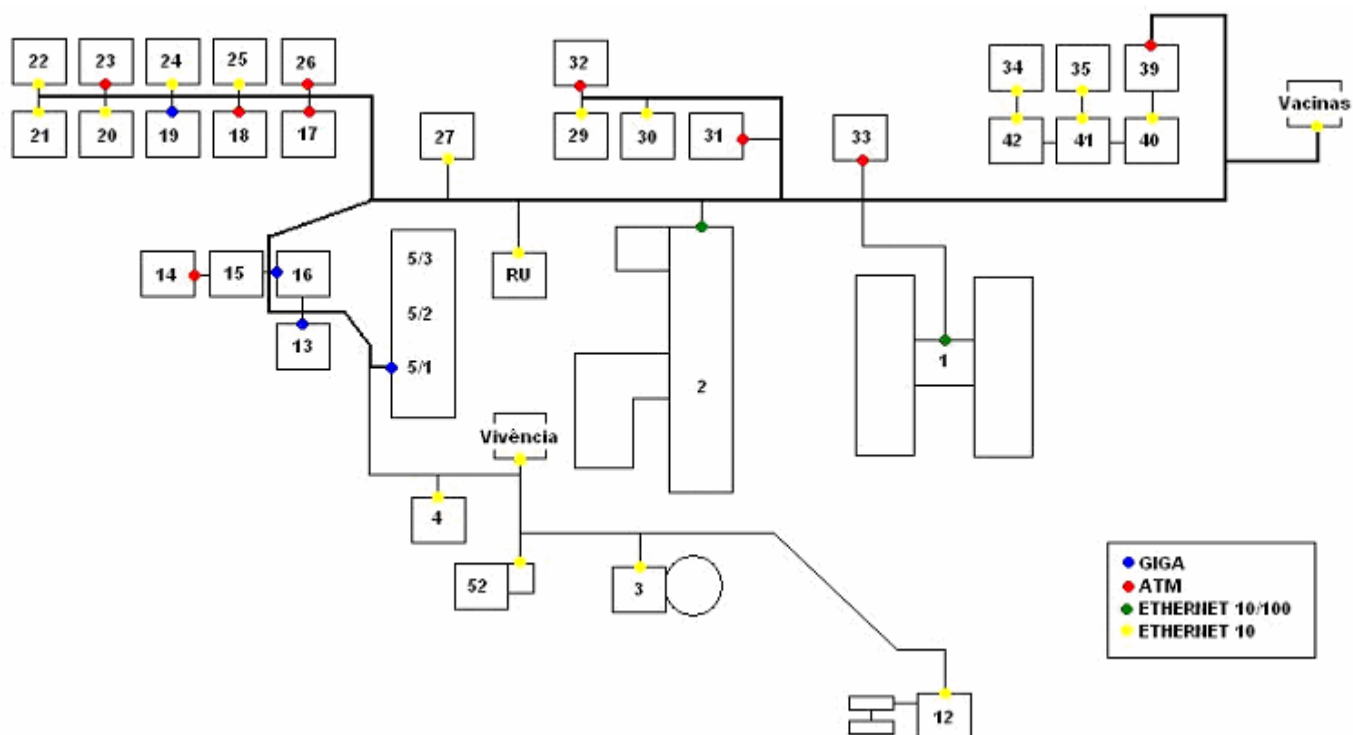
Neste capítulo, mostra-se o estudo da infra-estrutura de redes da Universidade Federal de Pelotas como estudo em questão.

### 8.1 Arquitetura do Ambiente de Videoconferência

A estrutura física do ambiente está distribuída da seguinte maneira: No Campus do Capão do Leão temos três salas Multimeios localizadas no prédio da Nutrição (5), uma Sala de Reunião e uma Sala de Treinamento ambas localizadas no prédio do Centro de Informática (15). E pertencente ao Campus Pelotas um Estúdio de Transmissão localizado no prédio da Lagoa Mirim.

O serviço de rede comutada por pacotes implantado no prédio da Lagoa Mirim, situado no Campus Pelotas, é também um serviço da Embratel – Empresa Brasileira de Telecomunicações. Este serviço faz parte de uma *backbone* Internet da Embratel o qual tem conectividade mundial. No caso do estúdio de transmissão temos uma largura de banda de um link Frame Relay de 2 Mbps.

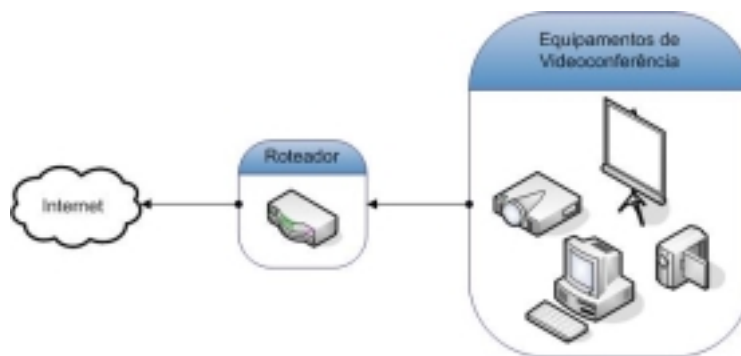
Abaixo temos a Figura 8.1 dos prédios do Campus Capão do Leão.



**Figura 8.1:** Mapa de velocidades dos Prédios do Campus Capão do Leão UFPel.

A rede local do Centro de Informática é composta de uma rede específica para videoconferência, onde temos equipamentos de videoconferência e estações de gerência da rede e uma rede virtual de computadores, onde estão todas as demais estações do prédio.

As redes utilizam a mesma estrutura física de cabeamento, mas estão separadas por redes diferentes. Esta decisão foi tomada para não haver concorrência entre o tráfego das estações com o tráfego multimídia da videoconferência, pois estamos em um meio onde não há garantia de qualidade do serviço. De acordo com a Figura 8.2, se observa que o sistema de videoconferência está diretamente ligado ao roteador.



**Figura 8.2:** Sistema de Videoconferência UFPel.

Os mais importantes fatores para a escolha da rede de acesso para o ambiente multimídia, principalmente com o tráfego de áudio e vídeo em tempo real são: os protocolos escolhidos, a expectativa de tempo de uso do enlace de acesso e a largura de banda disponível para este acesso.

Por essa razão foi projetada a rede comutada por pacotes (IP). No caso da Sala de Reunião e da Sala de Treinamento temos uma saída direta a 1Gbps.

Com esta disponibilidade montamos uma rede local para videoconferência baseada no protocolo IP. Esta rede tem saída para a internet sendo possível realizar videoconferências com qualquer outro ponto ligadas à rede mundial, desde que haja disponibilidade de banda para isto.

### 8.1.1 Equipamentos Terminais de Videoconferência

Os equipamentos terminais da rede se referem aos *codecs* de videoconferência. Estes *codecs* são dispositivos que captam áudio e vídeo, codificam e comprimem/descomprimem estes sinais para transmissão na rede de acesso disponível. Para a definição dos equipamentos foram analisados fatores como custo, operação, configuração, capacidade de *upgrade*, facilidade na instalação e capacidade de comunicação usando a recomendação H.263 e H264. Analisando estes fatores, optamos por adquirir equipamentos da marca View Station V500 – POLYCOM.

### **8.1.2 Equipamentos de Interconexão de Redes – Gateway**

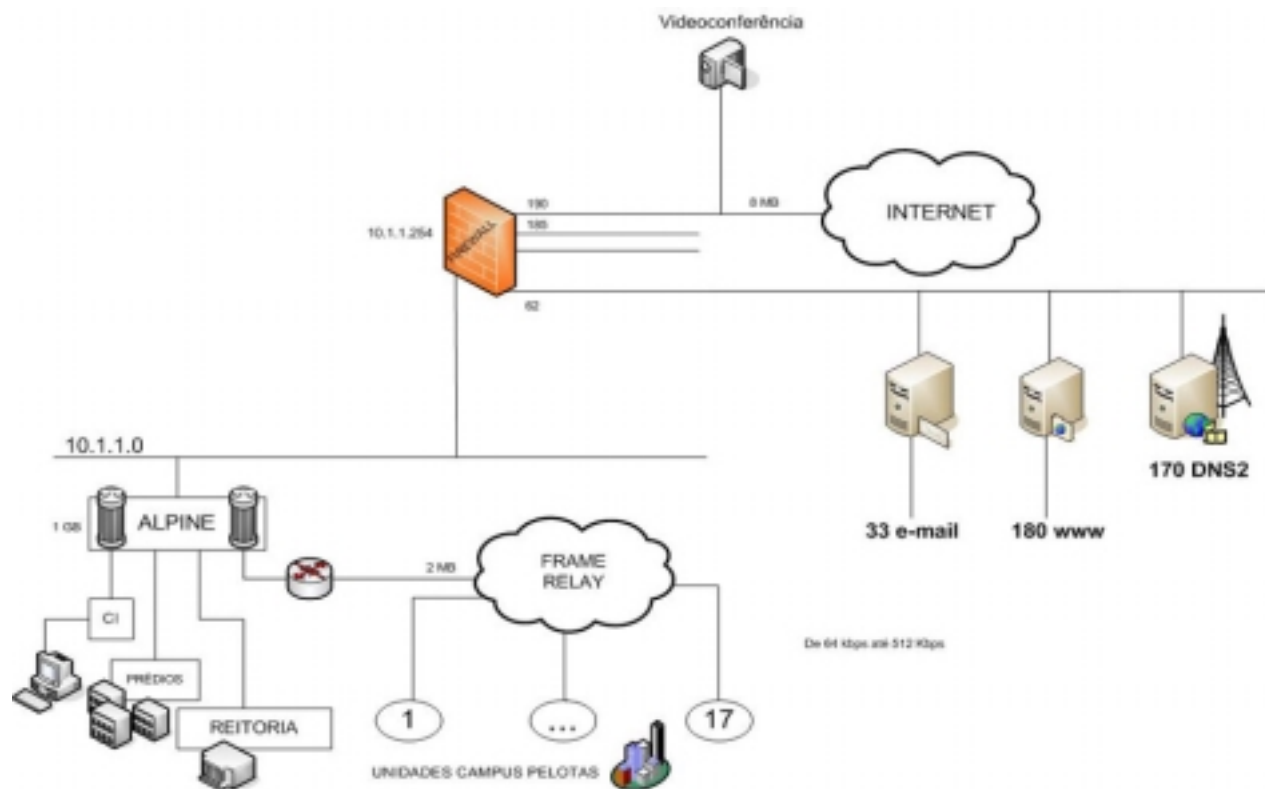
O gateway é um elemento essencial em uma rede, pois tem a capacidade de interligar sistemas que utilizam diferentes protocolos de comunicação, podendo ainda oferecer outros serviços suplementares conforme o modelo e fabricante. O gateway existente no Centro de Informática é o próprio roteador da UFPel, um CISCO modelo 2620. O gateway possui quatro portas WAN de 2 Mbps e uma porta fast Ethernet.

### **8.1.3 Equipamentos de Multiponto – MCU (Multipoint Control Unit)**

Na verdade a utilização do MCU neste trabalho foi através do servidor TCHE da UFRGS (Universidade Federal do Rio Grande do Sul). O MCU existente na UFRGS é da marca CISCO. Ele permite aos usuários participarem de conferências multiponto, seja de voz apenas seja com áudio e vídeo, sem a necessidade de configuração adiantada. O usuário que deseja transmitir multimídia para outros participantes deve ter os equipamentos da videoconferência e agendar o serviço com o servidor. Os demais usuários que queiram acessar esta conferência devem entrar no site <<http://www.tche.br/eventos>>. O MCU se encarrega de alocar recursos e mixar áudio e vídeo configurando assim a conferência.

## **8.2 Topologia de Rede da Universidade Federal de Pelotas**

Na figura 8.3 podemos verificar como está distribuída a infra-estrutura lógica de rede da UFPel:



**Figura 8.3:** Mapa Lógico da Infra-estrutura de rede da Universidade Federal de Pelotas.

As velocidades da rede variam dependendo das necessidades de cada prédio/departamento como o número de usuários, tipo de usuário (se só acessa a Internet, webmail, rede interna, etc...) e do *switch* de cada prédio. Ainda neste capítulo as velocidades serão mostradas.

Externamente os endereços são da classe C, os endereços dos prédios são da classe B e os demais endereços internos são da classe A.

No servidor de rádio está instalado um software *trial* do Helix Server, com limitação de recursos e também de duração de utilização, mas ainda não foi testado com mais de duas máquinas como, por exemplo, na opção de *videostreaming*. Pretende-se em breve investir na aquisição de um software próprio para a Universidade.

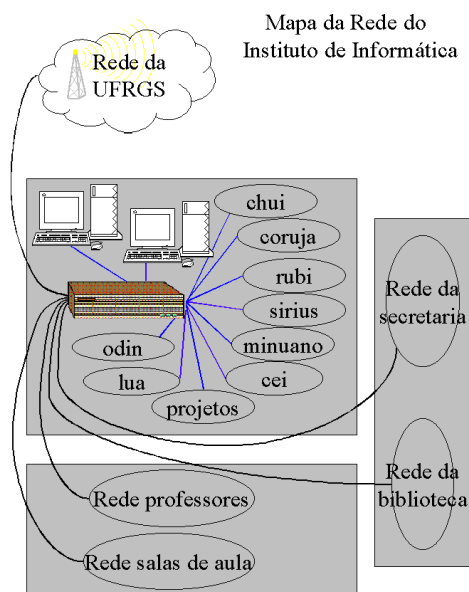
O que dificulta a possibilidade de termos salas de videoconferência também nos prédios do Auditório da Agronomia e das salas de Multímeios é o endereçamento IP (falso, NAT estático) que o administrador de rede nos libera, isso porque os protocolos de videoconferência têm dificuldades para serem roteados. Por enquanto no Auditório da Agronomia não seria somente o problema do IP, também a



infra-estrutura do prédio esta sendo modificada. Mas infra-estrutura não é a pior coisa neste caso. Nas salas multimeios, que são administradas pelo Departamento de Informática, dependendo de como está a configuração já pode ser possível ter sistemas de videoconferência. Já nas salas da Lagoa Mirim teria que verificar com a possibilidade de um acordo da UFPel com a Brasil Telecom.

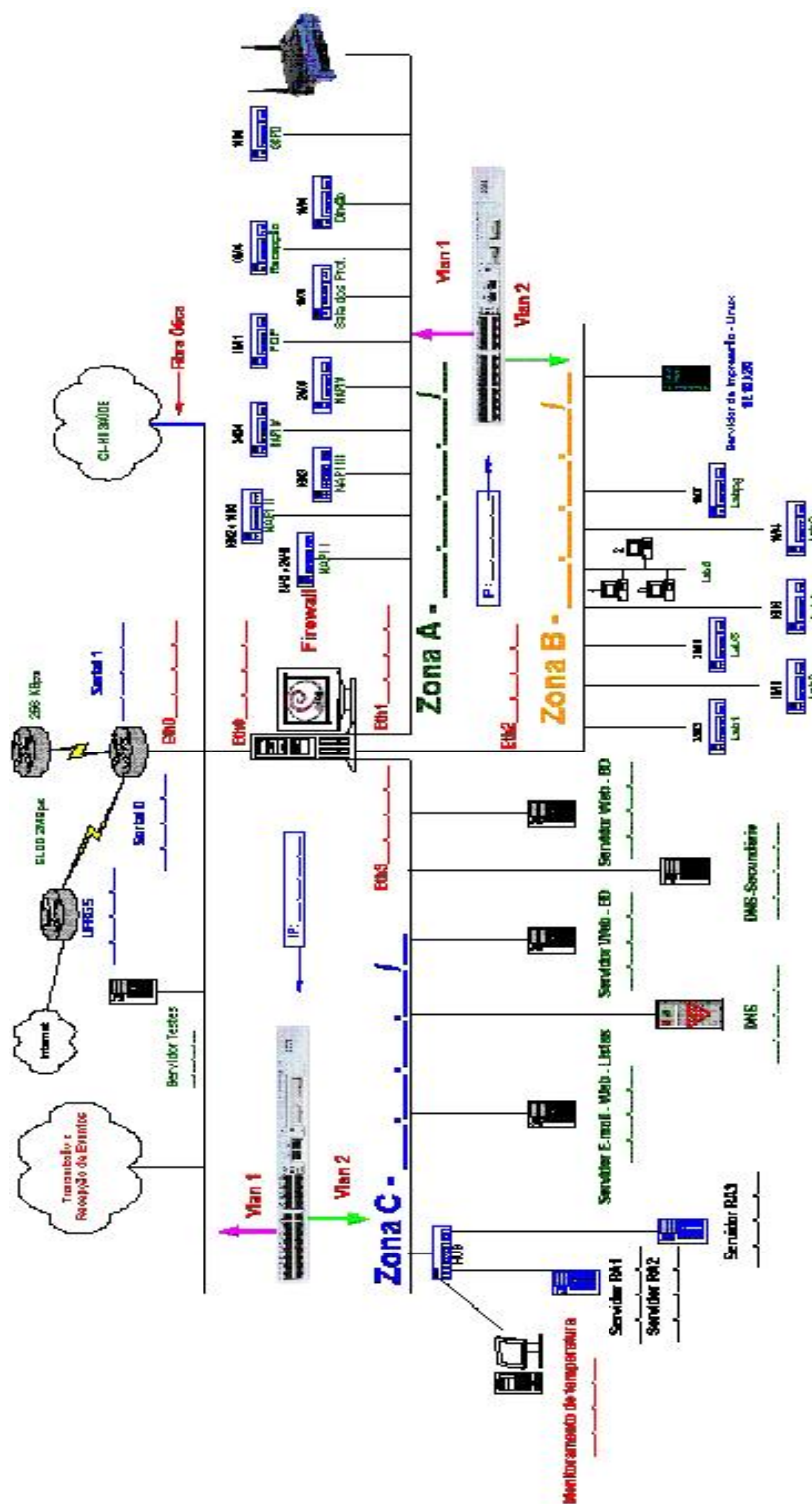
Pode-se verificar que nossas transmissões realizadas no CI, os equipamentos estavam diretamente ligados ao roteador, assim conseguíamos ter um IP estático e todas os métodos de videoconferência podiam ser realizados sem ter interferências de áudio ou vídeo ocasionados pelo IP dinâmico, *firewall* e NAT.

Na figura 8.4 pode-se ver o mapa da rede do Instituto de Informática da UFRGS. Podemos ver que existe um equipamento principal, onde provavelmente tenha seu *firewall* e NAT para segurança, que distribui para as demais redes (em preto), salas e servidores (em azul). Esse mapa não há como verificar velocidades e classes de endereços.



**Figura 8.4:** Mapa da Rede do Instituto de Informática da UFRGS.  
Fonte: Universidade Federal do Rio Grande do Sul.

A seguir está bem detalhado o Mapa da Rede da Universidade Católica de Pelotas na Figura 8.5, onde pode-se verificar classes de endereços, servidores, roteadores, *firewall*, outros equipamentos de rede e as conexões dos prédios e salas. Esse mapa é mais um modelo porque os espaços de endereços estão incompletos.



**Figura 8.5:** Mapa da Rede da UCPel.  
Fonte: Universidade Católica de Pelotas.

### 8.3 UFPELNET: Serviços & Equipamentos de Abrangência Institucional

- **Serviços Internet da UFPel: WWW Server e FTP Server**

Um Processador Intel Pentium III, 1Ghz, memória RAM de 512 Mbytes, três discos SCSI 36 GB. Emprega sistema operacional Linux, distribuição RED HAT.

- **Serviço de FireWall da UFPel**

O serviço de Firewall além de proteger os equipamentos da Intranet contra intrusos, permite que a nível local da UFPel tenha uma rede classe A com autonomia de gerenciamento. Um Processador Intel Pentium III, 1Ghz, memória RAM de 1GB, três discos SCSI 36 GB. Emprega sistema operacional Linux, distribuição RED HAT.

- **Serviço de DNS secundário da UFPel (EAD- Teleduc, Rádio)**

Um Processador Intel Pentium III, 1Ghz, memória RAM de 512 Mbytes, três discos SCSI 36 GB. Emprega sistema operacional Linux, distribuição RED HAT.

- **Serviços Internet da UFPel: E-mail (Minerva)**

Dois Processador Intel Pentium Xeon, 2.8 Ghz, memória RAM de 3GB, dois discos SCSI 36 GB. Emprega sistema operacional Linux, distribuição Debian.

- **Serviço de Aplicativos: Banco de Dados (Pro-Reitoria, DRA, etc...)**

Dois processadores Intel Pentium III 1Ghz, memória RAM de 2 GB, dois discos SCSI 36 GB. Emprega sistema operacional Linux, distribuição NT Server.

- **Serviço de DNS da UFPel:**

Um processador IntelPentium III, 800 Mhz, 1 GB RAM, disco SCSI 36 GB. Emprega sistema operacional Linux, distribuição Debian.

#### **8.4 Principais Tipos de Equipamentos que Interligam a UFPeINET**

- **Roteador Cisco 2620 (INTERNET)**

Quatro portas WAN de 2Mbps e uma porta fast Ethernet.

- **Servidores de Comunicação Livingston**

Para conexão via dial-up (usuários residenciais).

- **Roteador Cisco 2600 (FRAME RELAY)**

Uma porta de 2Mbps.

- **ALPINE**

Interconexão dos prédios do Campus do Capão do Leão. Permite até 1Gbps.

- **ATM**

Faz a conexão entre os prédios a 155 Mbps.

### Circuitos FRAME-RELAY contratados a Brasil Telecom

**Tabela 8.4:** Circuitos FRAME-RELAY contratados a Brasil Telecom.

Local	Endereço	Telefone	Contato	Nº SAC	Velocidade	IP
UFPeI (Campus)	Campus Universitário	3275-7421	Bayard	410670	1Mb	
Ciências Sociais	R. Cel Alberto Rosa, 154	3278-6653	Joana	410667	512K	10.30.0.254
Medicina	Av. Dq Caxias, 250	3221-3554	Renato	410671	256K	10.31.0.254
Direito	Pc cons Maciel, 215	3225-1221	Marcos/ Nelson	410672	128K	10.32.0.254
ESEF	R. Luiz de Camões, 625	3273-3851	João	410673	128K	10.33.0.254
CAVG	Av.Eng Ildefonso Simões Lopes, 2791	3277-6584	Marcelo	410674	128K	10.34.0.254
Coperve	R Gonçalves Chaves, 3126	3222-4060	Mateus/ Bayard	410675	128K	10.35.0.254
Mercosul	R Andrade Neves, 1529	3222-0404	Névio	410676	128K	10.36.0.254
Lagoa Mirim	R Lobo da Costa, 477	3227-2268	Zé Pedro/ Elmo	410757	128K	10.37.0.254
Odontologia	R Gonçalves Chaves, 457	32224439		410758	128K	10.38.0.254
Ciências Domésticas	R Alm Barroso, 1734	3225-4573	Terezinha / Jane	410759	128K	10.39.0.254
ILA	Av Bento Gonçalves, 3395	3222-4318	Fernando	410760	128K	10.40.0.254
Assistência Judiciária	R Gonçalves Chaves, 660	3222-4918	Vera	410761	128K	10.41.0.254
Conservatório	R Felix da Cunha, 651	3222-2562		410771	64K	10.42.0.254
CAEC	R Três de Maio, 852	3227-7509	Carmem	410899	64K	10.43.0.254
CPMet	Av.Eng Ildefonso Simões Lopes, 2791	3277-6690	Rogério	411042	128K	10.45.0.254
MALG	R Gen Osório	3225-9144	Eliana	411004	64K	10.44.0.254
Museu Carlos Ritter	Deodoro esq Cassiano	3222-0880	Derly		64K	
Casa do Estudante	R Andrade Neve	3225-8552	Ana/ Ari	411422	128K	
Reitoria (IP Dedicado)	Campus Universitário	3275-7421	Bayard	410890	128K	200.180.249.105

## **Especificações dos Serviços e Equipamentos da UFPel**

### **Roteador Frame Relay**

Endereço: 10.1.1.1

Parent Hosts: Bridge

Filhos: 17 (todos os roteadores do Campus Pelotas)

### **Bridge**

Endereço: 10.1.1.254

Parent Hosts: none (this is a root host)

Filhos: 3 (Roteador Frame Relay, Livinston e Nagios)

### **Alpine – 3804 (BackBone)**

Endereço: 10.1.1.10

Parent Hosts: Bridge

Filhos: 7 (os switchs do Campus Capão do Leão)

### **Bridge1 (Placa eth1#1)**

Endereço: 200.17.161.62

Parent Hosts: none (this is a root host)

Filhos: 2

### **Bridge2 (Placa eth2#1)**

Endereço: 200.17.161.126

Parent Hosts: none (this is a root host)

Filhos: 0

### **Bridge3 (Placa eth3#1)**

Endereço: 200.17.161.189

Parent Hosts: none (this is a root host)

Filhos: 0

### **Bridge4 (Placa eth4#1)**

Endereço: 200.17.161.254

Parent Hosts: none (this is a root host)

Filhos: 3 (nodo1, nodo2, nodo3)

### **Nodo01 (Servidor DNS Mail Usuários #1)**

Endereço: 200.17.161.195

Parent Hosts: Bridge4

Filhos: 0

**Nodo2 (Servidor DNS Mail Usuários #1)**

Endereço: 200.17.161.196

Parent Hosts: Bridge4

Filhos: 0

**Nodo03 (Servidor DNS Mail Usuários #1)**

Endereço: 200.17.161.197

Parent Hosts: Bridge4

Filhos: 0

**Minerva (Servidor DNS Mail Usuário #1)**

Endereço: 200.17.161.33

Parent Hosts: Bridge1

Filhos:

**Livinston (Host Servidor de Conexões #2)**

Endereço: 200.17.161.40

Parent Hosts: Bridge

Filhos:

**Router\_Campus (Roteador Remoto CampusXCampus #3)**

Endereço: 10.1.1.250

Parent Hosts: Bridge

Filhos: 1(router\_net)

## IX ANÁLISE DO TRÁFEGO DA REDE

No decorrer das transmissões que foram feitas, notou-se que havia certo congestionamento na rede. A partir daí, houve a necessidade de realizar uma análise do tráfego da rede da Universidade.

A análise de tráfego propicia um diagnostico para uma melhor utilização dos recursos da rede, exercendo influência direta sobre o roteamento e garantindo a banda necessária para uma determinada aplicação, no caso, a videoconferência.

A escolha das ferramentas do Multi Router Traffic Grapher e do Nagios, para a análise do tráfego e monitoramento da rede, respectivamente, foi devido à facilidade de eles já estarem instalados nos computadores do Centro de Informática onde aconteceu a maioria dos testes de transmissão de videoconferência.

Em qualquer lugar dentro da rede interna da Universidade qualquer pessoa pode ter acesso pelo *browser* do computador a imagem dos gráficos do MRTG de como está o tráfego através do seguinte link: <http://10.1.1.3/trafego>, enquanto que no Nagios pelo link: <http://10.1.1.3/nagios/> é requerido um nome de usuário e senha para então poder manipular com o monitoramento da rede.

O MRTG e o Nagios estão instalados em uma das máquinas de servidor em Linux. A seguir é explicado mais detalhadamente o MRTG, bem como o Nagios, ambos representados com exemplos de gráficos gerados a partir rede da Universidade.

### 9.1 Multi Router Traffic Grapher

O Multi Router Traffic Grapher (MRTG), de acordo com o próprio site (<http://people.ee.ethz.ch/~oetiker/webtools/mrtg/>), é uma ferramenta para monitorar a carga de tráfego em *links* de rede. O MRTG gera páginas HTML contendo imagens gráficas do formato PNG que possibilitam uma representação visual "ao vivo" deste tráfego.

MRTG consiste em um script em *Perl* que usa SNMP (Protocolo de Gestão Simples de Rede). É um protocolo de gestão de rede da camada de aplicação que facilita o intercâmbio de informação entre os dispositivos de rede e possibilita aos



administradores de rede gerir a performance da rede, encontrar e resolver problemas de rede, e planejar o crescimento desta, para ler os contadores de tráfego de seus roteadores e um rápido programa em C que *loga* os dados do tráfego e cria belos gráficos representando o tráfego da conexão de rede monitorada. Estes gráficos são incluídos em páginas *web* que podem ser visualizadas de qualquer *Browser* moderno.

Somadas a detalhada visão diária, o MRTG também cria representações visuais do tráfego durante os últimos sete dias, das últimas quatro semanas e dos últimos doze meses. Isto é possível porque o MRTG mantém um *log* de todos os dados que ele conseguiu do roteador. Este *log* é automaticamente consolidado, e com isso ele não cresce com o tempo, mas ainda contém todos os dados relevantes de todo o tráfego dos últimos dois anos. Isto tudo é realizado de uma maneira muito eficiente. Então é possível monitorar mais de 200 *links* de rede de qualquer estação UNIX decente.

O MRTG não se limita a monitorar somente tráfego, é possível monitorar qualquer variável SNMP que você escolher. Você pode até usar um programa externo para pegar os dados que você deve monitorar via MRTG. É possível usar o MRTG, para monitorar coisas como Carga do Sistema, Sessões *Logadas*, Disponibilidade de *Modems* e muito mais.

### **9.1.1 Características**

#### **Portabilidade**

MRTG trabalha na maior parte das plataformas UNIX e Windows NT.

#### **Perl**

MRTG é escrito em Perl e vem com todo o código fonte.

#### **Portabilidade SNMP**

MRTG usa uma implementação SNMP de alta portabilidade escrita toda em Perl. Não é necessário instalar qualquer pacote SNMP externo.

#### **Suporte a SNMPv2c**

MRTG pode ler os novos contadores de 64 bits do SNMPv2c. Os contadores não serão mais problemas.

#### **Interface de Identificação Confiável**

As interfaces dos roteadores podem ser identificadas pelo Endereço IP, Descrição e Endereço *Ethernet* em adição ao número da interface normal.

### **Tamanho dos arquivos de Log Fixos**

Os arquivos de log do MRTG NÃO crescem. Graças ao uso de um algoritmo de consolidação de dados único.

### **Configuração Automática**

MRTG vem com um conjunto de ferramentas de configuração que faz a configuração muito simples.

### **Desempenho**

As rotinas mais críticas foram escritas em C.

### **Livre de Gráficos GIF**

Os gráficos são gerados diretamente no formato PNG.

### **Customizável**

A aparência das páginas produzidas pelo MRTG é altamente configurável.

## **9.1.2 Exemplos de Gráficos Gerados**

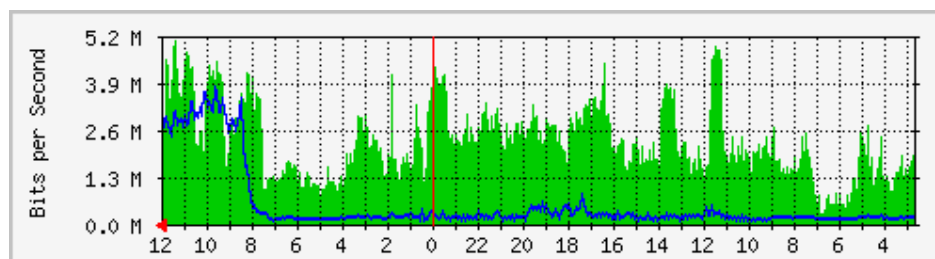
Os gráficos abaixo foram gerados durante um dia normal (4 de julho de 2005) e numa transmissão da videoconferência com a UNICAMP no dia 29 de abril de 2005.

O gráfico está em função de tempo e da transferência, a cor azul indica o tráfego de saída em bits por segundo e a verde indica o tráfego de entrada em bits por segundo. Existem quatro roteadores, mas só foi capturado os gráficos dos roteadores que tinham importância ou relação com a rede durante a videoconferência.

Na interface do MRTG, pode-se selecionar no mouse em cima do gráfico e aparecerá outra janela detalhando-o diariamente, semanalmente, mensalmente e anualmente. Diariamente o gráfico faz uma média de 5 em 5 minutos de tráfego, semanalmente é feito uma média de tráfego de 30 em 30 minutos, mensalmente de 2 em 2 horas e anualmente de dia a dia.

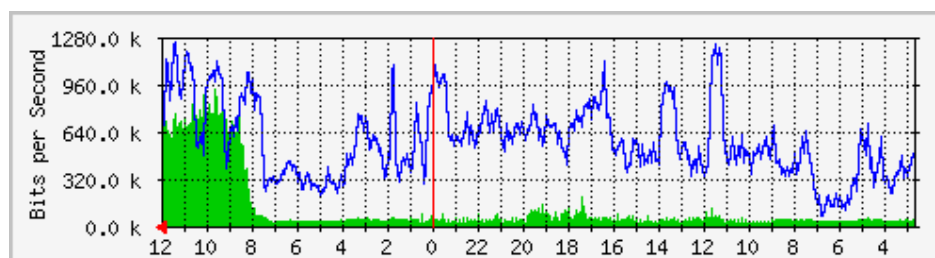
Nos gráficos abaixo, dos roteadores do dia 04 de Julho de 2005 às 12h, verifica-se o andamento da rede num dia de funcionamento normal da Universidade e sem transmissão de videoconferência.

Roteador (eth0) - roteador de rede, principal roteador neste caso, é nele que passam todas as entradas e saídas da rede interna.



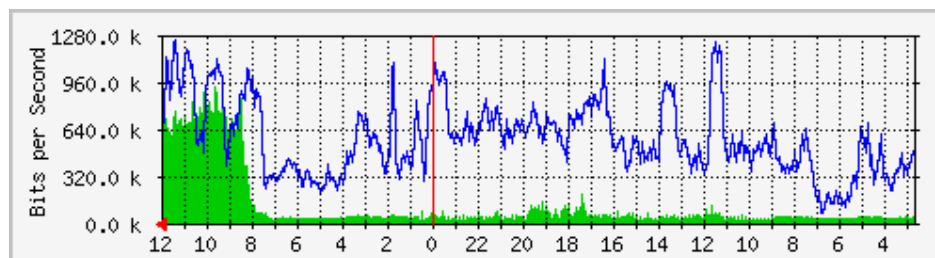
**Figura 9.1.2.1:** Gráfico do Roteador (eth0) no dia 04 de Julho de 2005.

Roteador (PPP/0) – os roteadores PPP's são portas do Roteador (eth0), tudo o que passa do tráfego interno pelos *modems* dos PPP's é passado para o roteador (eth0).



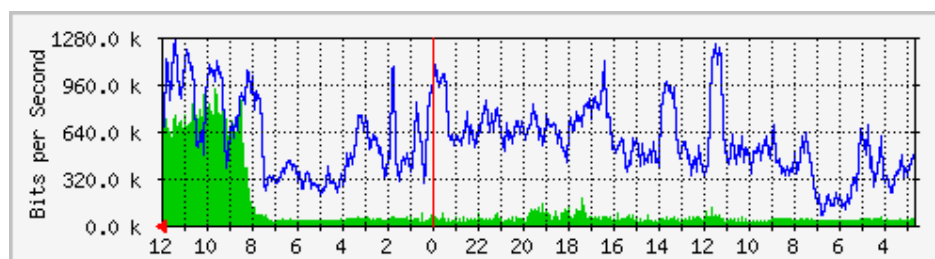
**Figura 9.1.2.2:** Gráfico do Roteador (PPP/0) no dia 04 de Julho de 2005.

Roteador (PPP/1)



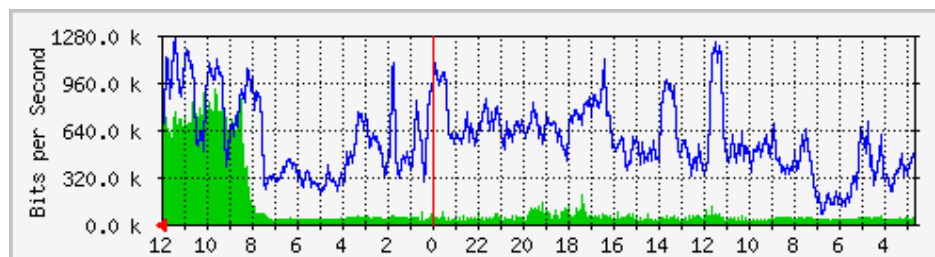
**Figura 9.1.2.3:** Gráfico do Roteador (PPP/1) no dia 04 de Julho de 2005.

Roteador (PPP/2)



**Figura 9.1.2.4:** Gráfico do Roteador (PPP/2) no dia 04 de Julho de 2005.

Roteador (PPP/3)

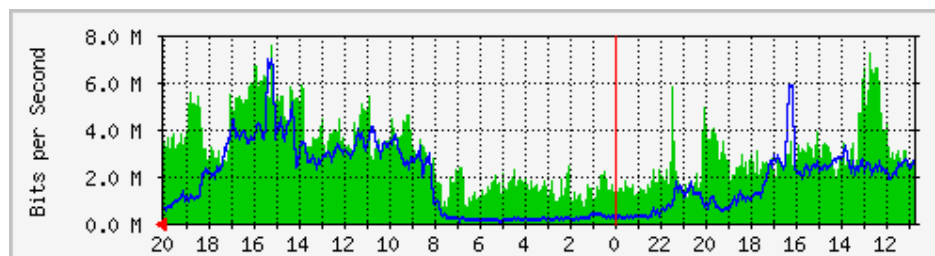


**Figura 9.1.2.5:** Gráfico do Roteador (PPP/3) no dia 04 de Julho de 2005.

Neste caso foi avaliado no roteador principal (eth0). A maior taxa de entrada de bits (verde) foi por volta das 11h30min atingindo 5.2 M já a maior taxa de saída de bits (azul) foi 3.9M às 9h30min.

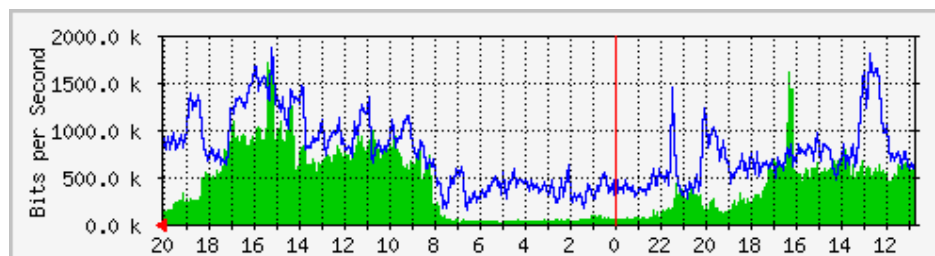
Abaixo estão os gráficos do dia 29 de Abril de 2005, capturado às 20h13min. Neste dia teve-se transmissão de videoconferência a partir das 18h até às 20h.

Roteador (eth0)



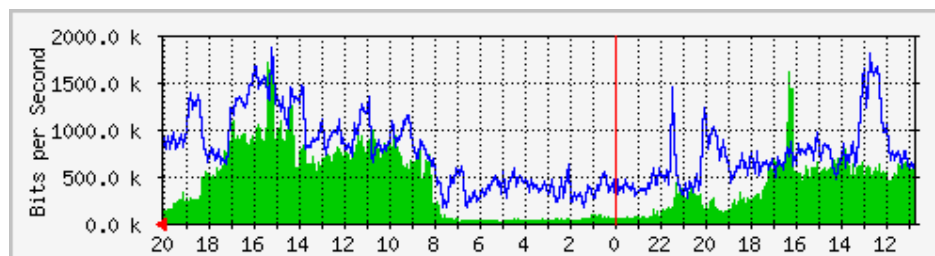
**Figura 9.1.2.6:** Gráfico do Roteador (eth0) no dia 29 de Abril de 2005.

Roteador (PPP/0)



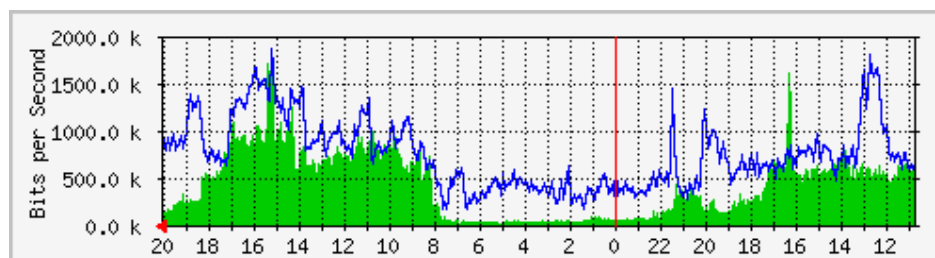
**Figura 9.1.2.7:** Gráfico do Roteador (PPP/0) no dia 29 de Abril de 2005.

Roteador (PPP/1)



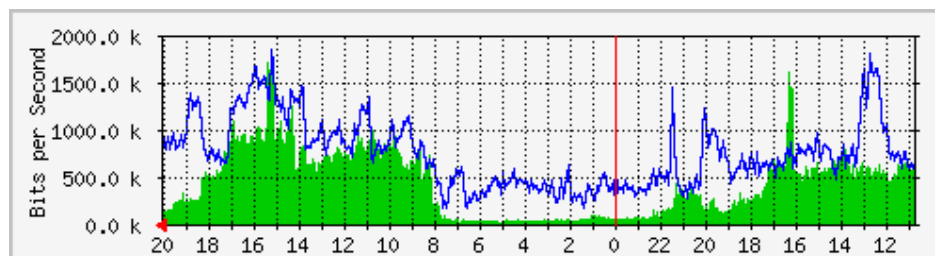
**Figura 9.1.2.8:** Gráfico do Roteador (PPP/1) no dia 29 de Abril de 2005.

Roteador (PPP/2)



**Figura 9.1.2.9:** Gráfico do Roteador (PPP/2) no dia 29 de Abril de 2005.

Roteador (PPP/3)



**Figura 9.1.2.10:** Gráfico do Roteador (PPP/3) no dia 29 de Abril de 2005.

Neste caso foi avaliado no roteador principal (eth0) que o pico no tráfego foi aproximadamente numa taxa para entrada de 7.3M às 15h15min e de saída 7M no mesmo horário. Nota-se que nos demais horários as taxas de entrada e saída são bem menores principalmente durante a madrugada.

Baseando-se no roteador (eth0) foi comparados o tráfego do dia 04 de Julho com o da transmissão da videoconferência do dia 29 de Abril pode-se notar que das 18h até às 20h:

- **Dia 04 de Julho** – A maior taxa de entrada de bits (verde) foi por volta das 19h30min atingindo aproximadamente 3.5 M, já a maior taxa de saída de bits (azul) foi aproximadamente 0.7 M às 19h.

- **Dia 29 de Abril** – A maior taxa de entrada de bits (verde) foi por volta das 19h atingindo aproximadamente 5.5 M, já a maior taxa de saída de bits (azul) foi de aproximadamente 2.3 M às 18h.

## 9.2 Nagios

O Nagios, de acordo com o <http://www.nagios.org/>, é considerado uma das ferramentas mais poderosas para gerenciar uma rede de computadores. Através dele se consegue tirar relatórios de acesso, status das máquinas, problemas que podem estar ocorrendo na sua máquina antes que eles afetem gravemente o sistema, etc.

Através da configuração do Nagios para telefone celular se pode receber mensagens quando houver erros na rede como por exemplo, uma mensagem dizendo que o seu servidor de e-mails está com problemas.

O Nagios é um aplicativo de monitoramento de sistemas e de redes. Ele checka clientes e serviços, por você especificados, alertando quando as coisas estão indo mal ou se restabelecendo.

O Nagios foi originalmente desenhado para rodar no Linux, apesar dele poder funcionar na maioria dos unix.

### 9.2.1 Características

Algumas das várias ferramentas do Nagios incluem:

- Monitoramento de rede e serviços (SMTP, POP3, HTTP, NNTP, PING, etc.);
- Monitoramento dos recursos de clientes (carga de processador, uso de disco, etc.);
- Organização simples de plugins que permite aos usuários facilmente desenvolverem seus próprios serviços de checagem;
- Checagem paralela de serviços;

- Habilidade para definir hierarquia de redes de clientes usando clientes pais (parent hosts), permitindo a detecção e distinção entre clientes que estão desativados e aqueles que estão inalcançáveis;
- Notificação de contatos quando problemas em serviços e clientes ocorrerem ou forem resolvidos (via email, pager, ou métodos definidos pelo usuário);
- Habilidade para definir tratadores de eventos (event handlers) que serão executados durante eventos de serviços ou clientes na tentativa de resolução de problemas;
- Rotatividade automática de arquivos de logs;
- Suporte para implementação de clientes de monitoramento redundantes;
- Interface web opcional para visualização do status atual da rede, histórico de notificações e problemas, arquivos de log, etc;

### **9.2.2 Configuração mínima**

A única exigência para rodar o Nagios é ter um computador rodando Linux (ou variantes do UNIX) e um compilador C. Será provável a necessidade de ter o TCP/IP configurado já que a maioria das checagens de serviços serão feitas através da rede.

### **9.2.3 Licença**

Nagios é distribuído sob os termos da GNU General Public License Versão 2 como foi publicado pela Free Software Foundation. Isto lhe garante permissão de copiar, distribuir e modificar o Nagios sob certas condições.

### 9.2.4 Exemplos de Gráficos Gerados

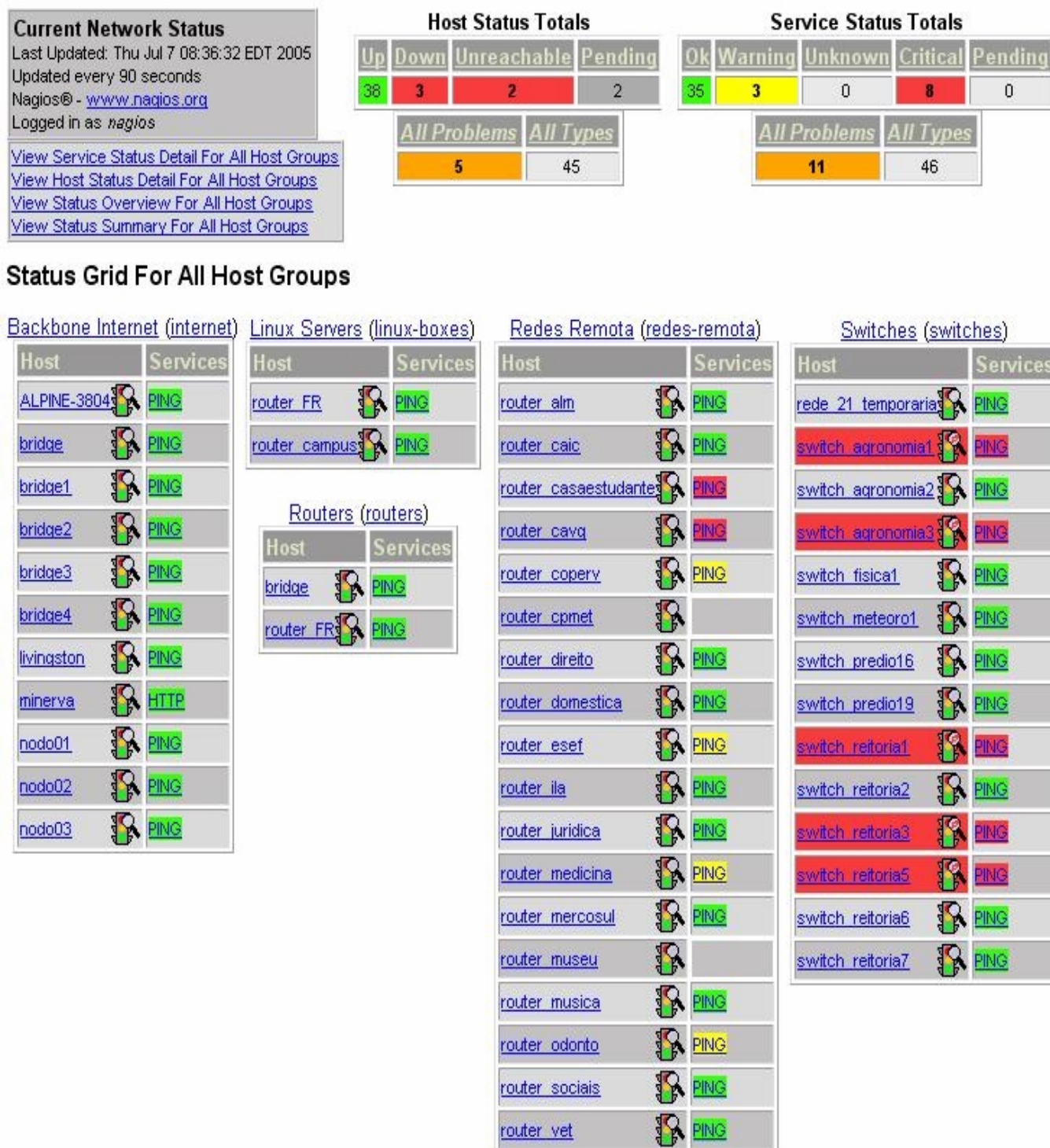


**Figura 9.2.4.1:** Gráfico Nagios da Rede da UFPEl.

Acima, na figura 9.2.4.1, mostra um exemplo de gráfico gerado pelo Nagios. Todos os pontos de interrogação são selecionáveis pelo mouse, e neles se podem saber maiores detalhes sobre o equipamento de rede. Por exemplo, clicando na interrogação do router\_Fr (Frame Relay) abre-se uma janelinha com o seu endereço “10.1.1.1”, qual equipamento que ele está conectado “Bridge” e qual são os equipamentos nele conectados neste caso são os “dezessete” roteadores do Campus Pelotas entre outras informações.



Há também outro tipo de mapa gerado pelo Nagios, figura 9.2.4.2, que mostra como está o status dos equipamentos/serviço ou serviços da rede. As cores do semáforo verde, amarelo e vermelho significam respectivamente que o equipamento/serviço está funcionando corretamente, o equipamento/serviço está com problemas, mas ainda está funcionando ou o equipamento/serviço está não está funcionando. Abaixo se pode visualizar no mapa o status da rede.



**Figura 9.2.4.2:** Mapa Nagios do Status da Rede da UFPel.

## **X TESTES REALIZADOS NA UNIVERSIDADE FEDERAL DE PELOTAS**

### **Relatório dos Testes e da Apresentação dos Trabalhos de Conclusão do Vinícius e da Helena**

Participantes:

Apresentadores de trabalhos: Vinícius e Helena

Banca Avaliadora: Professores Amauri Machado, Ricardo Silveira, Leonardo Fossati, Eliane Diniz, Raymundo Ferreira Filho e o Diretor do CI, João Ladislau.

Técnicas responsáveis pela transmissão: Verônica e Kelly

Data: Setembro de 2004

Equipamentos:

Microfone

Câmera de videoconferência Sony PCS 1600

Computador Athlon XP 2000, 512 Mb de RAM, Placa de Vídeo

Televisão 29"

Softwares:

Skype: <http://www.skype.com>

Netmeeting: <http://www.microsoft.com/windows/netmeeting>

MSN- messenger: <http://messenger.msn.com.br>

Helix Server: <http://forms.real.com/rnforms/products/tools/producerbasic/>

Configuração dos equipamentos:

Gateway da câmera e computador: 200.17.161.62

DNS da câmera e computador: 200.17.161.33

Máscara da câmera e computador: 255.255.255.192

IP computador : 200.17.161.39

IP câmera: 200.17.161.37

Como foi nosso primeiro contato com a aparelhagem de videoconferência se teve realmente muita dificuldade, pois não tínhamos quem nos ensinasse a utilizar esse sistema e equipamentos. A seguir será detalhada toda a etapa, inclusive com as dificuldades, até conseguirmos fazer o sistema funcionar. A videoconferência era ponto-a-ponto, nós no CI e o Professor Amauri em São Paulo.

- A primeira sala que foi-nos dada para a transmissão não estava habilitada com Internet, por isso tivemos que mudar para a sala de cursos do CI.
- A princípio o sistema de videoconferência não funcionou, não entendíamos porque razão.
- Quando conseguimos a ajuda da pessoa responsável pela rede da Universidade, descobrimos que precisávamos de endereços IP diferentes do que estávamos usando. O IP que estávamos utilizando era o mesmo utilizado para acessar a rede interna da universidade.
- Conseguimos então um IP com o responsável, só que este IP não era exatamente um IP externo, ele ainda passava pela firewall e NAT então esse número era transformado.
- A saída do som estava configurada para sair na própria televisão.
- Por causa desse IP o áudio não funcionou e também nossa câmera não conseguia chamar o outro equipamento. O professor Amauri que estava participando da banca avaliadora foi que nos chamou com sua câmera. Já para comunicação de voz foi utilizado o programa Skype.

### **Teste Utilizando o Programa Helix Server**

No outro teste, estávamos testando a utilização de outro método de transmissão, usando o Helix Server. O professor Raymundo Ferreira Filho estava nos ensinando. Nesse tipo de videoconferência multiponto, a transmissão é enviada para um servidor. No caso, estávamos testando com o servidor da rede *tche* para todas as pessoas que acessassem a transmissão *online*.

Com o IP que tínhamos nosso teste foi um fracasso, pois nosso IP modificava antes de chegar no servidor e não se estabelecia a comunicação com o servidor de lá.

Então para resolver esse problema, com a ajuda do Diretor do Centro de Informática João Ladislau, foi conectado o nosso cabo diretamente no roteador assim nosso IP não passava mais no *firewall* e NAT.

Após essa mudança conseguimos enviar nossa videoconferência com áudio que até então não tínhamos conseguido para o servidor *tche* sem mais problemas.

### **Relatório Transmissão Semana Acadêmica**

Durante a Semana Acadêmica do Curso de Ciência da Computação, foi transmitido o evento *online* através do servidor da rede tche.

Servidor: <http://www.tche.br/eventos>

Link: <http://mcu.ufrgs.br:8080/ramgen/encoder/live.rm>

Internet: ADSL 1.5 Mb fornecido pela Brasil Telecom

Equipamento utilizado:

- Microcomputador: Athlon XP 2000, 512 Mb de RAM, Placa de Vídeo
- Câmera: Sony- Compact Conference Package- PCS 1600
- Microfone desktop (qualidade de transmissão ruim)
- Placa de captura de vídeo: Pixelview Play TV Pro.

Software utilizado:

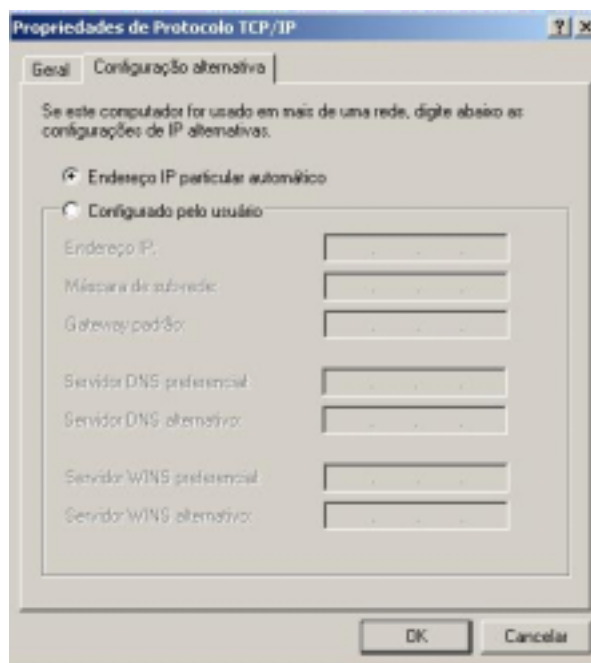
- Real Producer Basic 10
- Real One Player (para visualizar)

O computador teve a sua configuração de rede modificada, pois estávamos utilizando, um acesso ADSL à Internet, fornecido por uma operadora de Telefonia. Nas figuras 10.1 mostra-se como ficou. No painel de controle na configuração de conexões de rede temos que entrar em propriedades TCP/IP, na aba geral devemos selecionar a opção de obter um IP e um endereço de servidores DNS automaticamente.



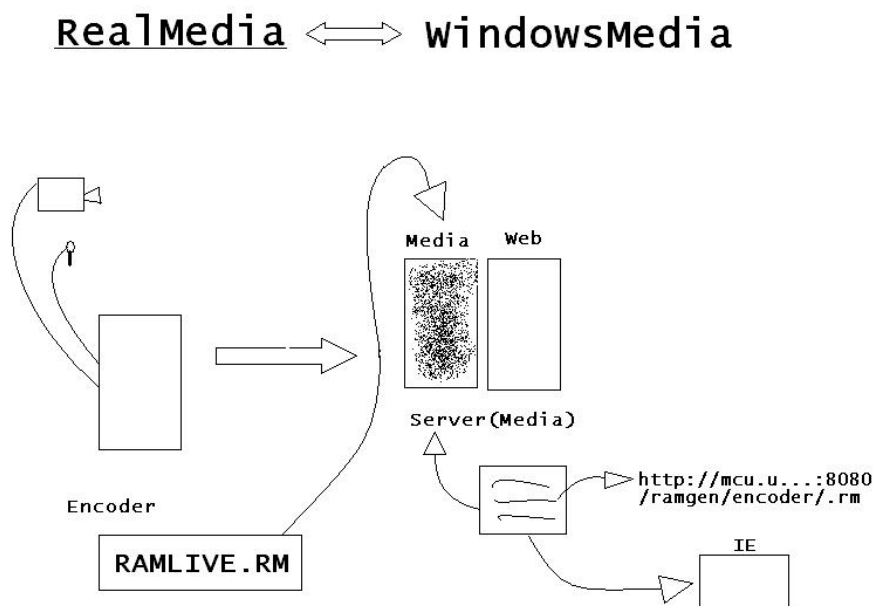
**Figura 10.1:** Configuração de IP e DNS.

Na aba configuração alternativa, figura 10.2, selecionar a opção endereço IP particular automático.



**Figura 10.2:** Configuração de IP particular.

Para entender como será realizada a videoconferência por videostreaming ver a figura 10.3:



**Figura 10.3:** Esquema do funcionamento de videoconferência por streaming.

De acordo com a figura, o áudio e o vídeo é enviado para o servidor e dele qualquer usuário poderá acessar a transmissão em tempo real em seu computador através do seu *browser*. Lembrando que o computador que deseja ver a videoconferência deve ter instalado o programa RealPlayer.

Para realizar uma transmissão ao vivo, pela Rede Tche, é necessário fazer o agendamento da transmissão, o qual é feito no link:

<http://www.tche.br/eventos/altera> , mediante uso de uma senha fornecida para a UFPEL. Abaixo, figura 10.4, tem-se um agendamento:

Agendamento de eventos	
Data do evento:	2004-11-12 (aaaa/mm/dd)
Hora de início:	18:00 (hh:mm)
Hora de término:	22:00 (hh:mm)
Resumo do evento:	Clique aqui para criar link de uma url <a href="#">http://</a> <pre>&lt;a href="http://mcu.ufrgs.br:8080/rangen/encoder/live.rm"&gt;Semana Acadêmica UFPEL&lt;/a&gt;</pre>
Link para vídeo:	Clique aqui para criar um link de vídeo <a href="#">rtsp://</a> UFPEL
Link para vod:	Clique aqui para criar um link de vod <a href="#">rtsp://</a>

**Figura 10.4:** Configuração do Agendamento.

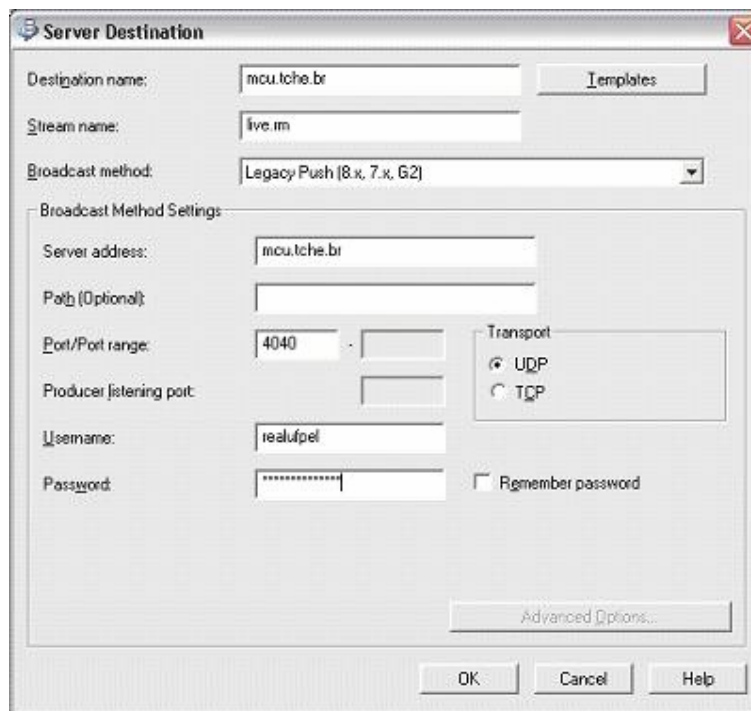
OBS: o tamanho que o vídeo aparecerá no Real One Player é definido nas configurações da placa de captura de vídeo.

O comentário de como foram as transmissões em geral é mostrado abaixo:

### **Configuração do Real Producer:**

O Real Producer é um software que envia a transmissão da videoconferência para o servidor. Como é um software básico, possui algumas limitações. A figura 10.5 mostra como ficou a configuração do software para transmitir ao servidor.

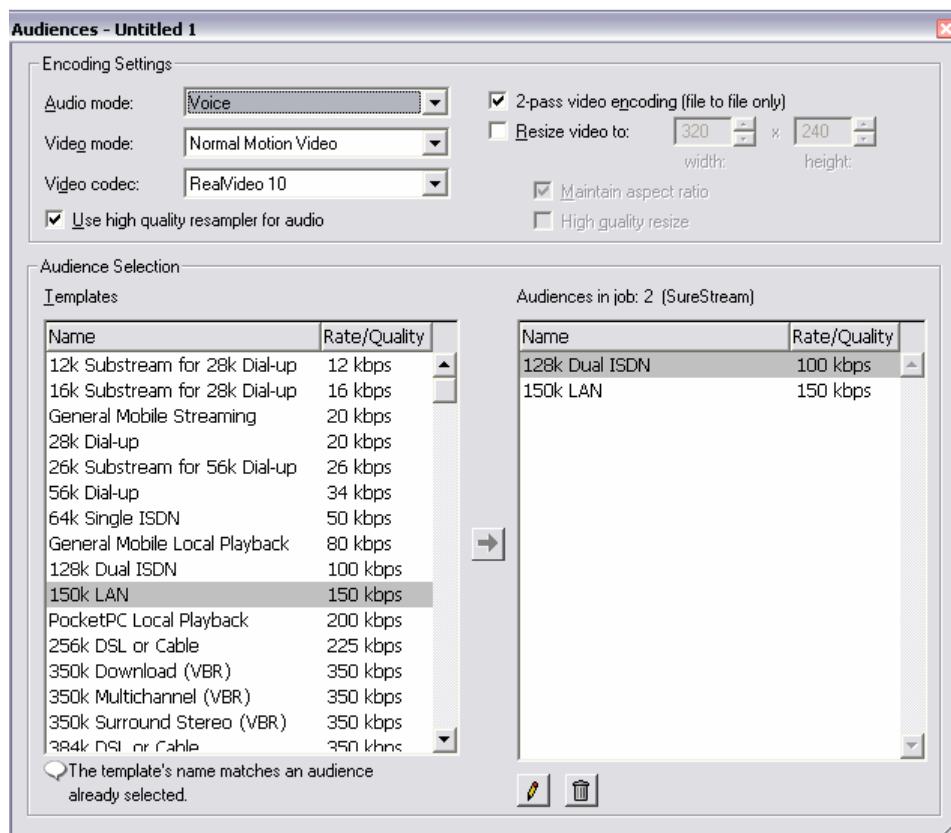




**Figura 10.5:** Configuração do RealProducer.

De cima para baixo, no primeiro espaço devemos preencher com o nome do destino, depois com o nome do arquivo que estamos transmitindo, logo em seguida devemos selecionar o método de transmissão. Após o preenchimento dessas informações devemos colocar o endereço do servidor, a porta que se deseja enviar o tipo de transporte e por último o login e senha.

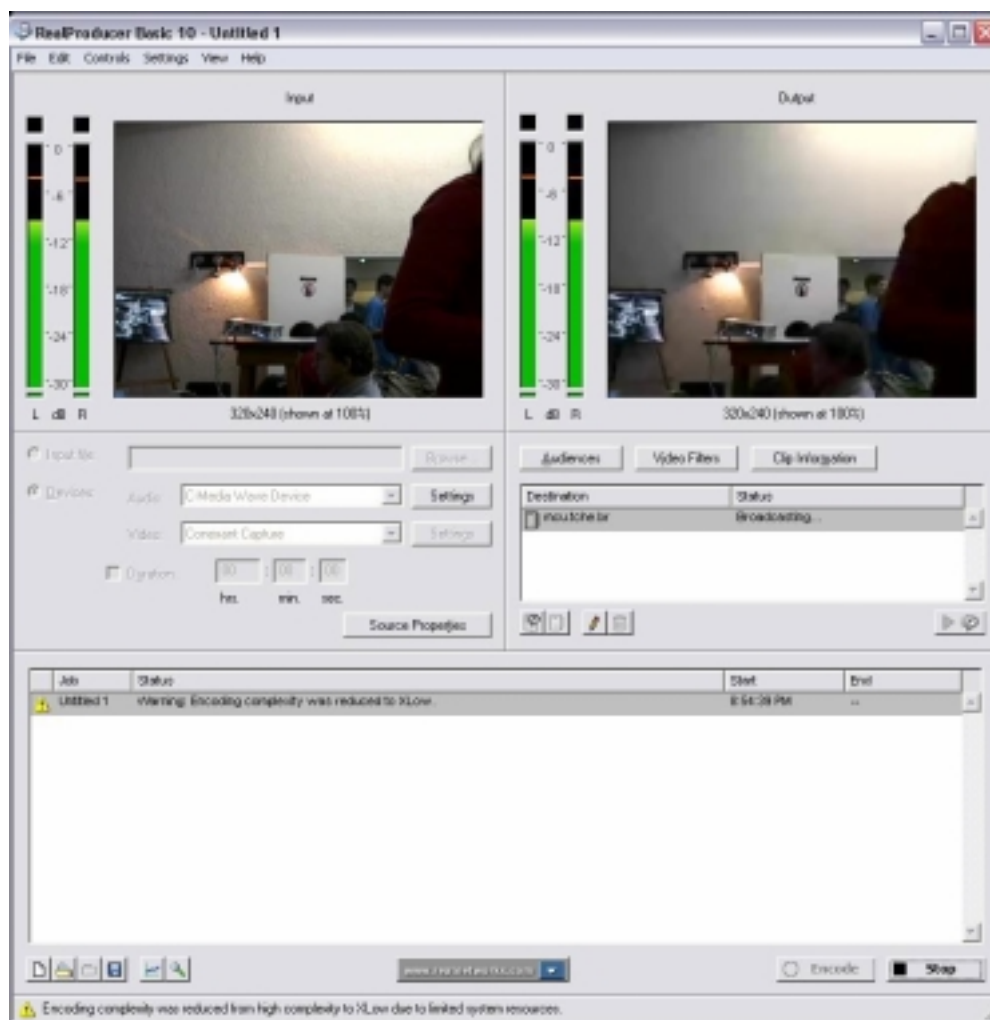
A figura 10.6 mostra a tela das audiências, onde se pode configurar o áudio, vídeo e em que software o usuário poderá assistir a transmissão. Mais abaixo temos a opção de escolha das velocidades dos usuários que podem ver a transmissão, de acordo com essa escolha depende a qualidade do áudio e vídeo.



**Figura 10.6:** Configuração das Audiências do RealProducer.

### **Visualização do Real Producer Basic 10:**

A figura 10.7 a seguir, mostra a tela com a interface do software transmitindo para o servidor.



**Figura 10.7:** Visualização do Real Producer Basic 10.

Algumas dificuldades encontradas foram:

- Os telefones do local onde foi realizada a Semana Acadêmica (Lagoa Mirim) são interligados por uma central Pabx, o que dificultou a instalação da ADSL.
- Com o uso desta câmera e do Helix Producer Basic, não é possível manter o palestrante e os slides aparecendo ao mesmo tempo. Por este motivo, constatou-se a necessidade de algum programa para manter os slides aparecendo ao mesmo tempo em que se mostra o palestrante. Ou então, o Helix Producer Basic poderia permitir que pudéssemos mandar mensagens curtas, online, para quem estiver assistindo. Isto é, que houvesse a possibilidade de digitar um link, onde as pessoas que estiverem assistindo possam baixar os slides e acompanhar a palestra.
- A falta de um bom microfone tornou o áudio com muito ruído e eco.

Observações quanto ao Helix Producer Basic 10:

- Seria útil que o software permitisse guardar imagens da apresentação que está sendo transmitida, ou seja, ele não permite salvar ao mesmo tempo em que está transmitindo.
- O fato de não poder escrever uma mensagem para os usuários que ficassem sobrepostos à apresentação, o qual já foi citado anteriormente.

Existe no mercado também o Helix Universal Server, que é um programa pago, que possui mais recursos que o Helix producer Basic. Este programa está disponível para servidores, que operam em sistemas múltiplos, e oferece todas as características requeridas de *streaming* do servidor para usuário *unicast* incluindo:

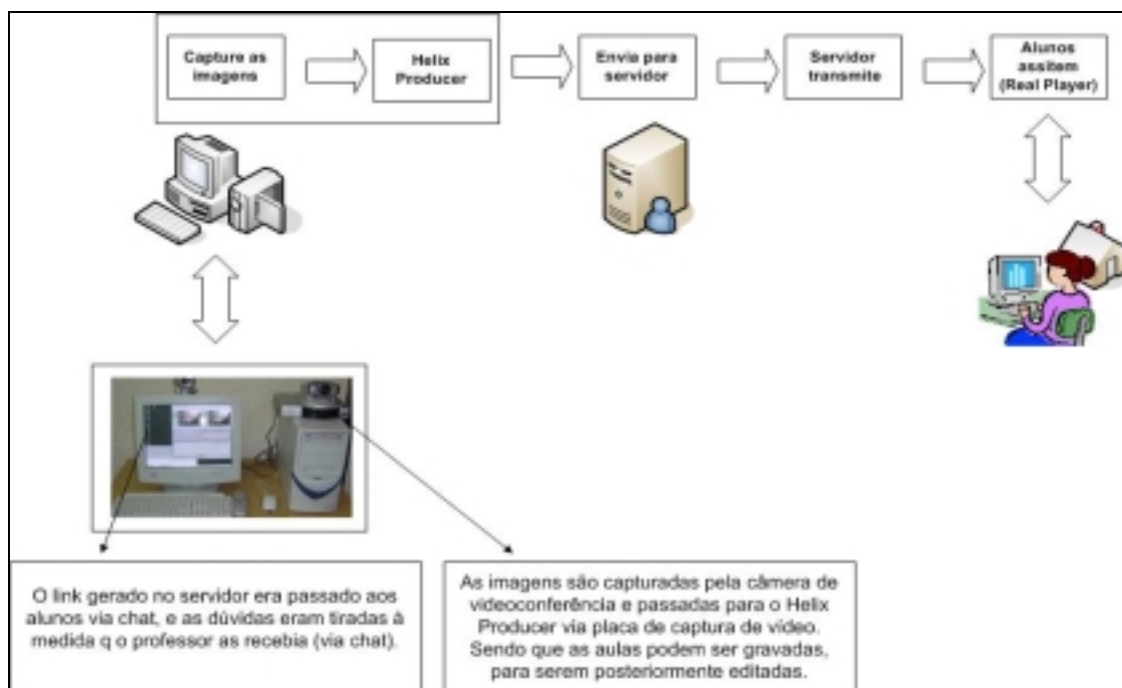
- Entrega ao vivo e sob demanda para as audiências;
- Transmissão por Broadcasting com SureStream para assegurar a melhor experiência possível para os usuários que alcançam índices de acesso diferentes;
- Salva transmissões para serem revistos sob demanda;
- Autenticação para assegurar o controle de quem acessa a transmissão;
- Entre outras.

### **Aula Professor Ricardo Silveira em Inteligência Artificial I**

Palestra por: Raymundo Ferreira Filho

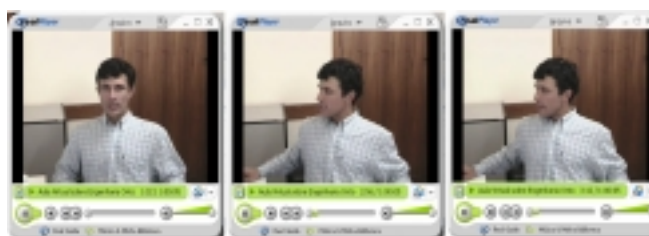
Novembro de 2004

A figura 10.8 mostra o esquema da Aula Remota:



**Figura 10.8:** Esquema do funcionamento da Aula Remota.

- Acessamos "<http://mcu.ufrgs.br:8080/ramgen/encoder/cinted.rm>"
- Para acessar o arquivo dos slides "[iate.ufrgs.br/lms/IA/document/ontologia.ppt](http://iate.ufrgs.br/lms/IA/document/ontologia.ppt)"
- A palestra era visualizada pelo real player, como mostra a figura 10.9:



**Figura 10.9:** Visualização do RealPlayer.

- O palestrante tem áudio e vídeo, os participantes somente áudio.
- A interação dos alunos com o palestrante era feita por mensagens instantâneas pelo MSN messenger.
- Com base no aprendizado que obtivemos (Tarouco) com esse tipo de transmissão fizemos um artigo relacionado a este evento sobre aula remota.
- Poderíamos ter utilizado uma pessoa, no nosso caso o próprio professor Ricardo seria uma ótima opção, para ser o secretário da interação. Ele poderia ter adicionado

os ouvintes da palestra no Messenger dele, assim o interlocutor poderia selecionar as perguntas significativas que foram feitas durante a videoconferência. Com isso, foi observado como sendo um ponto negativo da palestra, que a todo o momento alguém da aula era adicionado na Lista do Messenger do interlocutor, trazendo interrupções durante a maioria do tempo da aula remota.

### **Relatório da transmissão dia 19/01/2005**

Apresentação de Seminário “**Studies on Rooster Sperm**” por Denise Bongalhardo, PhD

Professora Adjunta do Departamento de Fisiologia e Farmacologia

Instituto de Biologia

Universidade Federal de Pelotas

Contato:

Tel : (53) 275 7337

e-mail: [denisecb@ufpel.tche.br](mailto:denisecb@ufpel.tche.br)

Informações Técnicas destino da transmissão:

GWCC Information (Laboratório de Biotecnologia e Germoplasma do Departamento de Agricultura dos Estados Unidos da América, localizado em Beltsville, Maryland).

Technical Contact Name: Tony Koontz

Technical Contact Telephone Number: 301-504-1097

Alternate Name: Maureen Harris

Alternate Telephone Number: 301-504-1088

Room Number Meeting will be held in: 4-2293

Telephone number in the Meeting Room: 301-504-4569

Type of Video System: Polycom

Speed 384kb

Video System's Telephone Numbers: 301-504-1138

IP Address: [199.133.23.224](http://199.133.23.224)

Date of Meeting: Jan 19 2005

Start Time: 8:30 am

End Time: 10:30 am

Time Zone: Eastern Day Light Time

Informações técnicas da origem da transmissão (UFPEL):

Sistema de vídeo: Compact Conference Package – Sony PCS-1600

IP da Câmera: 200.17.161.181

IP do computador: 200.17.161.183

Speed: 384Kb

Data da transmissão: 19 de janeiro de 2005

Horário de início: 11:30 am

Horário de término: 1:30 pm

Responsáveis técnicas: Verônica Burmann da Silva e Kelly Hannel

Contatos: [vebs@ufpel.edu.br](mailto:vebs@ufpel.edu.br), [hkelly@ufpel.edu.br](mailto:hkelly@ufpel.edu.br)

Tel: (0XX55)53-275 7127

(0XX55)53-2757414

### **Equipamentos e softwares utilizados na videoconferência e nos testes**

Câmera PCS-1600 Sony

Microfone profissional com fio ligado na entrada de microfone da câmera

Caixas de som ligadas na saída de áudio da câmera

TV 29" da Panasonic ligada na saída de vídeo da câmera

Retroprojeto da marca Próxima conectado ao microcomputador com os slides

Microcomputador (Athlon XP 2200, 512 Mb de RAM, HD 40, Windows XP

Profissional)

Softwares: Net Meeting 3.01(4.4.3400)

**Transmissão realizada no dia 22 de fevereiro de 2005.**

**Reunião do Grupo de Pesquisa do Alfa-Fado**

Durante a troca de mensagens anteriormente a reunião, nos foi esclarecido que iríamos utilizar um novo tipo de transmissão de videoconferência, iríamos utilizar um refletor. Então se começou na semana anterior a data da transmissão a

configurar o equipamento para o funcionamento adequado. Foi instalado o refletor VRVS que é um sistema de salas virtuais para videoconferência. No anexo desse trabalho é mostrado como fizemos passo a passo a instalação do VRVS.

Apesar do trabalho que se teve com a configuração do refletor, na hora da videoconferência acabaram não o utilizando. Utilizaram o NetMeeting para realizar essa reunião. O motivo da troca do método da transmissão foi a dificuldade encontrada na configuração do refletor por alguns participantes da reunião.

Como ainda não tínhamos utilizado essa modalidade que o NetMeeting proporciona, essa transmissão contribuiu para um estudo maior dos sistemas possíveis de videoconferência.

Na transmissão apareciam quatro janelas sendo que uma das janelas fazia rodízio com outras câmeras, pois tinha aproximadamente sete participantes conectados.

Utilizamos a webcam (Vídeo Blaster WebCam Go Plus WDM) ao invés da câmera (Sony 1600) pois o NetMeeting não detectou a placa de captura de vídeo e como também não se teve tempo foi o que deu no momento. Achamos que deveríamos ter instalado a placa de captura antes de instalar o NetMeeting para que assim o programa a detectasse.

O professor Ricardo Silveira foi quem participou da transmissão no prédio do Centro de Informática.

#### **Dados dos Computador:**

IP do computador: 200.17.161.181

Gateway: 200.17.161.190

Máscara: 255.255.255.192

DNS: 200.17.161.33

#### **Os dados fornecidos pelo Vicente Goya para a conexão foram:**

IP Gatekeeper: 193.144.34.146

IP MCU: 193.144.34.147

Serv: 259



Para ISDN:

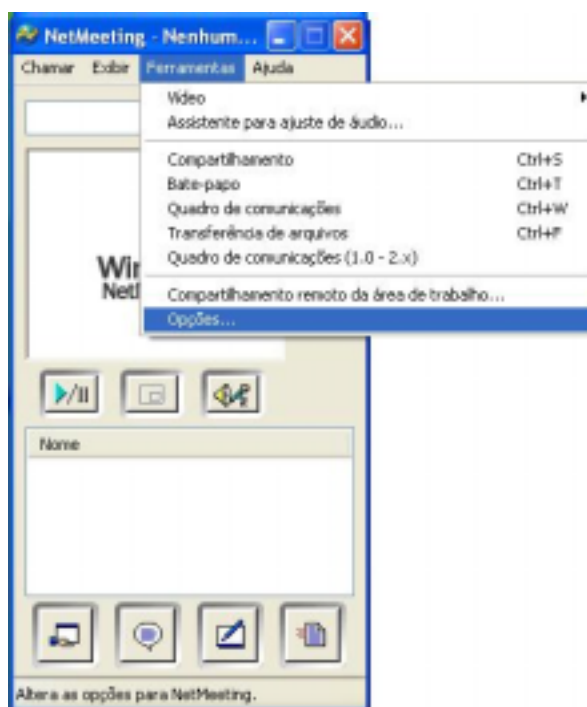
ISDN1: +34 981 553 565

ISDN2: +34 981 553 094

\* Só são possíveis 2 conexões por ISDN.

### Como foi feita a chamada pelo NetMeeting

Clicando em Iniciar+Executar+ digitar conf – Abre o programa netmeeting. No menu Ferramentas, clicar em opções conforme a figura 10.10:



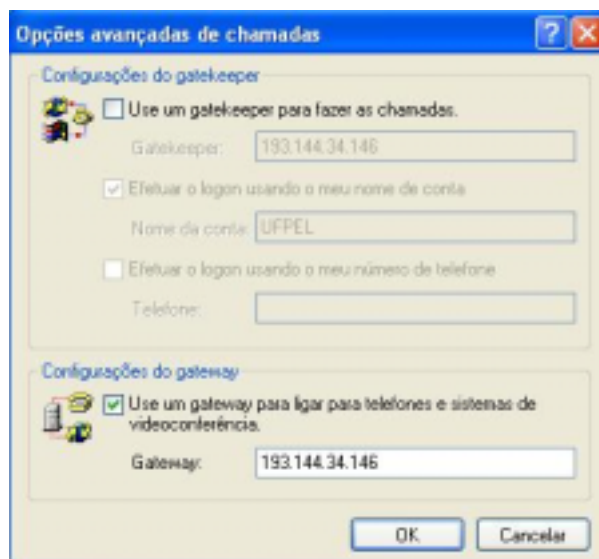
**Figura 10.10:** Configuração NetMeeting.

Na aba Geral, clicar em chamadas avançadas como mostra a figura 10.11:



**Figura 10.11:** Configuração das opções, aba geral.

Na configuração do Gateway, selecionar a opção que diz “Use um gateway para ligar para telefones e sistemas de videoconferência”, conforme a figura 10.12.



**Figura 10.12:** Configuração Avançada.

No nosso caso digitamos 193.144.34.146 como número do gateway dado pelo responsável técnico Vicente.

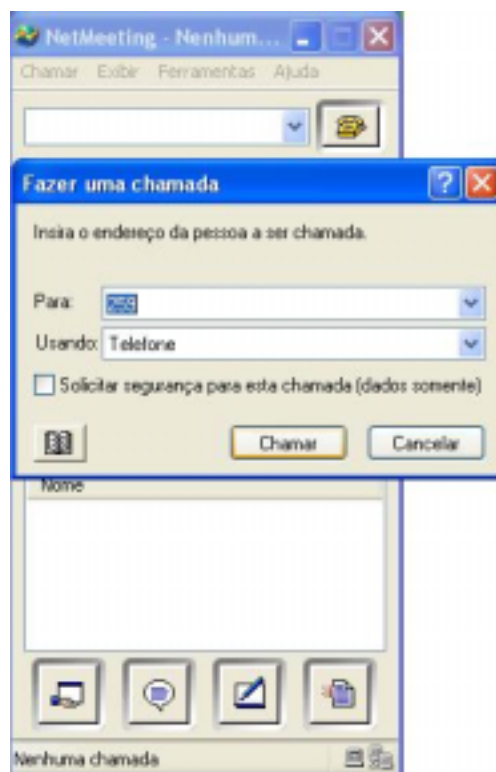
Na aba Vídeo, nas propriedades da câmera de vídeo, pode-se selecionar o dispositivo de captura de vídeo. A figura 10.13, mostra a seleção da WebCam.



**Figura 10.13:** Configuração Vídeo.

Agora, dando *ok* e voltando na janela principal do programa NetMeeting, clicando no telefone para fazer a chamada.

Digitamos o número do servidor 259 e usando telefone, isso no nosso caso como mostra a figura 10.14:



**Figura 10.14:** Configuração de chamada.

### **Relatório da transmissão dia 29/04/2005 Mesa Redonda História**

Mesa Redonda:

Brasil Império: estado da arte em História da Educação

Participantes convidados:

Rita Filomena A. Januário Bettini, UNESP

Maria Cristina Gomes Machado, UEM

Nicanor Pachares Sá, UFMT

Elizabeth Madureira Siqueira, UFMT

Elomar Tambara, UFPel

Informações Técnicas destino da transmissão:

Local: Sala de Videoconferência da FE - UNICAMP

Nome do Responsável Técnico: Engº. Gilberto Oliani

Contatos:

e-mail: [gilberto@unicamp.br](mailto:gilberto@unicamp.br) e pelo telefone: (0xx19)3788 7977 ou (19) 3788-5690  
(sala de edição da videoconferência)

Sistema de vídeo: equipamento Tandberg modelo Educator 6000

IP do equipamento: 143.106.58.210

Speed: 3 Mbps

ISDN: 07801919000

Speed: 2 Mbps (disponível atualmente 384 kbps)

Data de TESTE: 25 de abril de 2005

Horário de início: 9:30 am

Data da transmissão: 29 de abril de 2005

Horário de início: 5:00 pm

Horário de término: 8:30 pm

Informações técnicas da origem da transmissão (UFPEL):

Professor: Elomar Tambara, [tambara@ufpel.edu.br](mailto:tambara@ufpel.edu.br)

Telefones: (0XX55)53-275 9053 e (0XX55)53-276 6653

Local: Centro de Informática da UFPel

Responsáveis técnicas:

Verônica Burmann da Silva – Estagiária do Centro de Informática UFPel

Kelly Hannel – Estagiária do NADARTE UFPel

Contatos: [vebs@ufpel.edu.br](mailto:vebs@ufpel.edu.br) e [hkelly@ufpel.edu.br](mailto:hkelly@ufpel.edu.br) , respectivamente ou pelos telefones

Tel: (0XX55)53-275 7127

(0XX55)53-2757414

Sistema de vídeo: Compact Conference Package – Sony PCS-1600

IP da Câmera: 200.17.161.181

IP do computador: 200.17.161.183

Speed: 384Kb

Data de TESTE: 25 de abril de 2005

Horário de início: 9:30 am

Data da transmissão: 29 de abril de 2005

Horário de início: 5:00 pm

Horário de término: 8:30 pm

### Equipamentos utilizados na videoconferência

Câmera PCS-1600 Sony

Microfone de Lapela ligado na entrada de microfone da câmera

Caixas de som ligadas na saída de áudio da câmera

TV 29" da Panasonic ligada na saída de vídeo da câmera

Retroprojektor Próxima conectado ao microcomputador com os slides

Microcomputador (Athlon XP 2200, 512 Mb de RAM, HD 40, Windows XP Professional)

### Equipamentos e Softwares utilizados nos testes

Câmera PCS-1600 Sony

Microfone de lapela ligado na entrada de microfone da câmera

Caixas de som ligadas na saída de áudio da câmera

TV 29" da Panasonic ligada na saída de vídeo da câmera

Retroprojektor Próxima conectado ao microcomputador com os slides

Microcomputador (Athlon XP 2200, 512 Mb de RAM, HD 40, Windows XP Professional)

Softwares: Net Meeting 3.01(4.4.3400) e Messenger 7.0

## **XI ESTUDO DE UMA SOLUÇÃO DE VIDEOCONFERÊNCIA A SER IMPLANTADA NA UNIVERSIDADE FEDERAL DE PELOTAS**

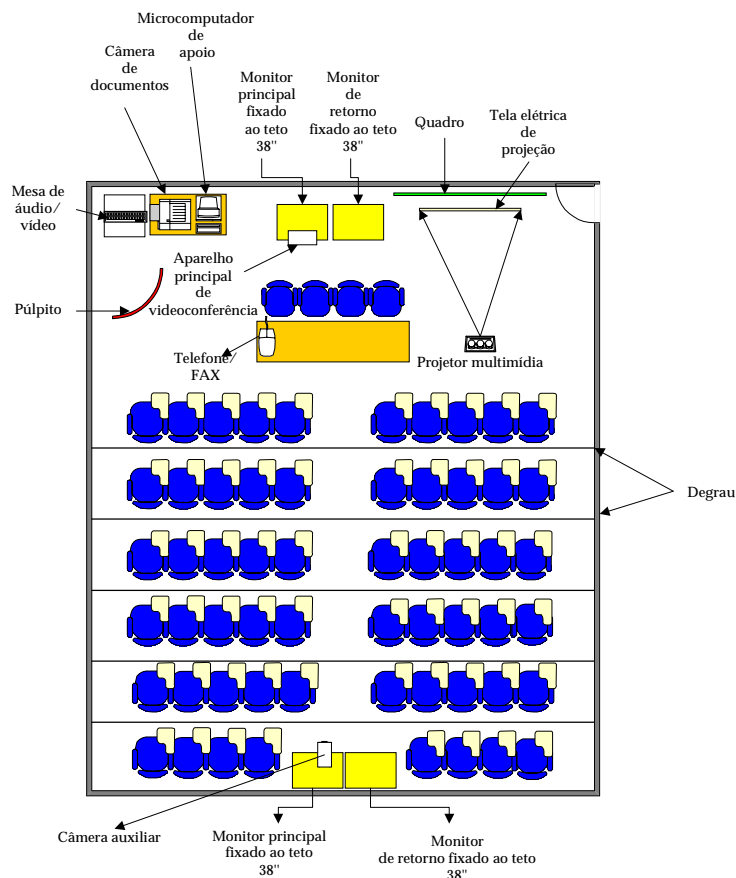
### **Ambientes de múltiplos usos**

Este capítulo foi elaborado para mostrar os exemplos de uso dos diversos ambientes de videoconferência na UFPel.

#### **11.1 Multimeios**

A sala pode ser preparada para servir de auditório e tem a capacidade de por volta umas 50 pessoas sentadas em cadeiras com pranchetas. Esta platéia está dividida em 6 fileiras com aproximadamente 10 cadeiras em cada uma. Os monitores e câmeras principais, monitores e câmeras auxiliares se situarão dispostos de uma forma tal que otimize o espaço da sala e proporcione um ótimo ângulo de visão para todos os participantes, sejam eles apresentadores ou platéia.

A velocidade da rede que chega no prédio que está localizado a sala multimeios é de 1 Giga. Na figura 11.1 mostra o desenho da pretensa sala de multimeios.



**Figura 11.1:** Layout da sala de multimeios para utilização de videoconferência que poderá ser adotada pela UFPel.

### 11.1.1 Exemplo de Uso

O primeiro exemplo de uso é no campo da telemedicina. O propósito era a demonstração de técnicas cirúrgicas. A conexão deverá ser realizada na velocidade mínima de 384 kbps entre o hospital universitário que estará mostrando a cirurgia com a sala de multimeios da UFPel. Esta conexão será feita usando a rede comutada por circuitos digital para se obter uma qualidade de imagem próxima à televisão (25 quadros por segundo). Os participantes localizados na multimeios poderão ter uma visão tanto do médico quanto da cirurgia em questão, pois a configuração com vários monitores permite esta facilidade. A interação entre o cirurgião e os participantes será feita em tempo real através de 2 microfones multidirecionais localizados estrategicamente na sala.

O segundo exemplo pode ser o uso em outras disciplinas como no evento que tivemos da Física, quando se tinha os alunos presentes e também os que estavam assistindo o evento a distância puderam ver os experimentos que foram



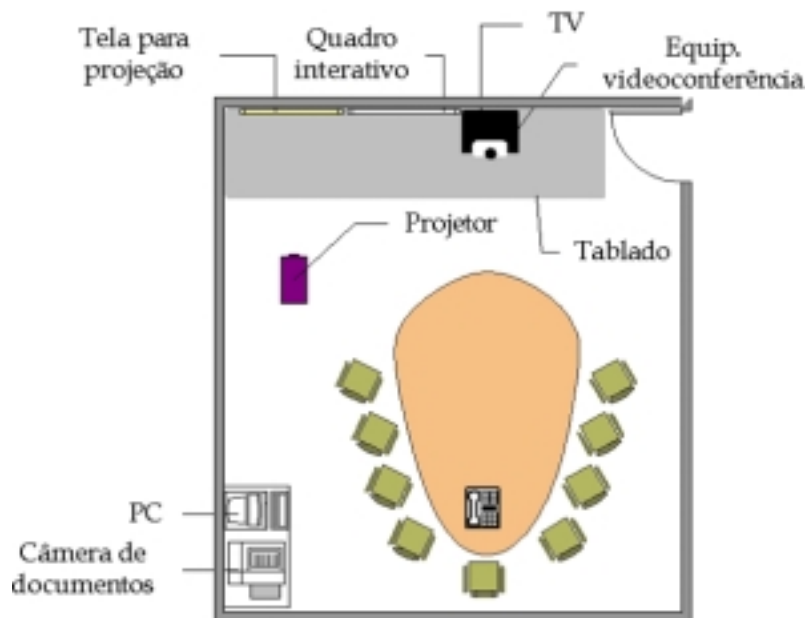
realizados. Foi realizada uma conexão na velocidade de 512 kbps entre a sala de multimeios e o servidor Tche.

Neste caso tínhamos na sala multimeios apresentadores sentados na mesa em frente à platéia e através do uso de câmeras auxiliares poderíamos ter a visualização frontal tanto das autoridades na mesa quanto da platéia e também da mesa com as experiências. A interação entre os participantes presentes era feita com perguntas com microfone para quem estava presente e por mensagem escrita para os distantes.

Portanto, esta configuração de auditório permite usos variados seja para apenas recepção de videoconferência seja para apresentação e recepção.

## 11.2 Sala de Reunião

A sala de videoconferência no Centro de Informática configurada para servir de sala de reunião permite que pessoas discutam assuntos diversos usando vários recursos de videoconferência. A sala será projetada de uma forma tal que todos os participantes ficassem dentro do ângulo de visão da câmera, pois a visualização de todos os participantes é fundamental. A velocidade de rede que temos no prédio do centro de informática para a transmissão de videoconferência chega a 1 Giga. A figura 11.2 a seguir mostra o desenho de uma sala de reunião.



**Figura 11.2:** Projeto do layout da sala de reunião no Centro de Informática da UFPel.

Fonte: NMI da UnB (Núcleo de Multimídia e Internet da Universidade de Brasília)

A configuração desta sala é otimizada tanto para o uso de reuniões presenciais quanto para reuniões à distância.

### **11.2.1 Exemplo de Uso**

Um exemplo comum de utilização desta sala é a realização de reuniões entre professores, servidores, estudantes da nossa entidade educacional com demais pessoas de diferentes localidades e também para o público fora da Universidade sob pagamento e agendamento. A reunião é realizada da sala de reunião do CI (Centro de Informática) na Universidade Federal de Pelotas para qualquer sistema de videoconferência também habilitado com os mesmos serviços que dispusermos. A conexão foi feita utilizando a rede de acesso IP, ou seja, pela Internet na velocidade de 512 kbps. Os participantes poderão interagir em tempo real e compartilhar documentos usando o computador.

### **11.3 Sala de Treinamento**

O ambiente preparado para servir de sala de treinamento no CI tem uma configuração mista, ou seja, preparada tanto para treinamentos presenciais quanto para treinamentos à distância. A sala é equipada com nove computadores, sendo todos com acesso à Internet. O instrutor possui uma estação própria a qual tem a capacidade de controlar todas as demais.

Para aulas à distância, a sala de treinamento possui um equipamento de videoconferência, uma televisão de 29 polegadas como monitor principal, uma tela para projeção, um projetor e 2 microfones localizados estrategicamente no local. A Figura 11.3 mostra a foto da sala de treinamento do CI.



**Figura 11.3:** Foto da sala de Cursos do Centro de Informática da UFPel.

### **11.3.1 Exemplo de Uso**

A aplicação mais usada para esta sala é a de treinamento presencial. O instrutor ministra cursos usando a televisão de 40 polegadas ou através de apresentação de material preparado no computador e projetado na tela, assim os alunos podem, desta forma, acompanhar seus passos. Atualmente, temos um ministrado cursos de Microsoft Office para cinco pessoas.

No caso de um treinamento à distância os alunos iam visualizar o computador e a imagem do professor na tela. Neste esquema é sugerido que a conexão seja feita em pelo menos 384 kbps, pois a partir desta velocidade conseguiremos obter vídeo Full Motion da tela do computador do professor e da sua própria imagem. Esta é uma configuração típica usando sala de treinamento à distância e estúdio de transmissão.

### **11.4 Estúdio de Transmissão**

O estúdio de transmissão de videoconferência que se pretende implantar no NADARTE (Núcleo de Apoio ao Desenvolvimento e à Aplicação de Recursos Telemáticos na Educação) na Universidade Federal de Pelotas é semelhante a um estúdio de televisão. Teremos uma sala preparada com tratamento acústico, iluminação e cenários apropriados, de tal forma que as transmissões tenham a melhor qualidade de áudio e vídeo possíveis.

Dentro do estúdio alguns recursos serão disponibilizados para o apresentador, tais como: computador, câmera de documentos e quadro digital. O estúdio usa a configuração com 2 monitores, sendo um principal e outro secundário e uma câmera principal, estrategicamente localizada a fim de se obter o melhor

enquadramento do apresentador. A imagem transmitida será em modo Dual Stream Vídeo, isto é, as pessoas receberão a imagem do professor e a imagem de uma câmera auxiliar ou a tela do computador de apoio.

#### **11.4.1 Exemplo de Uso**

O estúdio de transmissão tem a função principal de gerar aulas. Os exemplos práticos de uso do estúdio do NADARTE são as aulas ministradas para diversos cursos de graduação e inclusive os cursos de mestrado profissionalizante à distância para alunos da Universidade Federal de Pelotas. As aulas serão geradas usando uma conexão ponto a ponto ou multiponto de acordo com a necessidade e a velocidade também será variada dependendo da utilização e os alunos poderão interagir com o professor em tempo real, se a velocidade for de 128 kbs a imagem possuirá baixa qualidade (15 quadros por segundo). Com isto, o uso dos recursos disponibilizados é feito de maneira cautelosa, quanto maior a movimentação e troca de câmeras mais borradas ficarão a imagem.

## **XII CONCLUSÕES**

Aplicações como educação à distância, reuniões virtuais, seminários e palestras à distância e telemedicina são algumas das muitas aplicações já desenvolvidas em um sistema de videoconferência. A cada dia surge, com o avanço das tecnologias, diferentes recursos para videoconferência. Mais e mais usuários desejam fazer uso deste recurso, deparando-se, conseqüentemente, com a necessidade de escolher uma aplicação que lhe seja ideal.

O trabalho do projetista é de fundamental importância para apontar a escolha mais adequada, e deve iniciar determinando a qualidade de áudio e vídeo desejada, seguido do estudo da capacidade da rede existente em atender à aplicação de vídeo na qualidade especificada.

Esta escolha é, contudo, facilitada quando são levados em consideração alguns parâmetros para avaliação de tais aplicações e foi para auxiliar na definição desses parâmetros que este trabalho foi realizado. Ao utilizar determinados parâmetros, o usuário pode escolher a aplicação que melhor se adeque às suas necessidades.

Atualmente o uso de serviços de vídeo nas redes de computadores depende mais de projetos adequados e de justificativas de custo e benefício do que de desenvolvimento tecnológico. O mercado oferece ampla variedade de soluções, mas a implementação de videoconferência exige decisões de projeto com relação à escolha de padrões.

Esta escolha deve ser realizada partindo do parâmetro "cenário" e em seguida o parâmetro de "recursos disponíveis". Após as aplicações que oferecem subsídios a tais parâmetros terem sido escolhidas, "modelos de comunicação", "controle de acesso" e "qualidade de áudio e vídeo" são parâmetros auxiliares que permitirão um refinamento da escolha.

Deverá incluir também a realização de estudos de retorno de investimentos, simulações de custo com o uso de tecnologias e links diversos como nos parâmetros "licença" e "plataformas suportadas, previsão necessidades futuras e demandas de

interoperabilidade, na rede privada (intranet) ou pública (extranet). Sendo assim, escolher uma aplicação que seja a ideal, dependerá deste conjunto de parâmetros.

Esta monografia foi realizada objetivando uma contribuição para melhorar a qualidade das sessões de videoconferência, amenizando problemas, tais como congestionamento de rede e sincronismo das mídias.

### XIII REFERÊNCIAS BIBLIOGRÁFICAS

BATES, R.J. and GREGORY, D. **Voice and Data Communications Handbook**, McGraw-Hill Series on Computer Communications, 1997.

COOKBOOK, **Video Conferencing Cookbook**. Disponível no site <<http://www.vide.gatech.edu/cookbook2.0>> acesso em: 23/03/2005.

FALBRIARD, Claude. **Protocolos e Aplicações para Redes de Computadores**. São Paulo: Editora Erica, 2002.

FLUCKIGER, F. - **“Understanding Networked Multimedia - Applications and Technology”** - Prentice Hall, 1995.

ITU-T (F.730, 1992 F.730, International Telecommunication Union, Telecommunication Standardization Sector, **Telematic, Data Transmission, ISDN Broadband, Universal, Personal Communications and Teleconference Services: Operation and Quality of Serviço - Videoconference Service - General**, ITU-T Recommendation F.730, agosto de 1992;)

JONES, S. Choosing action research: a rationale. In: **MANGHAM, I. L.** (Org.). *Organization analysis and development*. Chichester: John Wiley, 1987.

KOTLER, Philip; FOX, Karen F.A. **Marketing Estratégico para Instituições Educacionais**. São Paulo: Atlas, 1994.

MARTINS, Ricardo Ferreira Martins.  
**“Streaming”** <<http://www.das.ufsc.br/redes/redes00/multicast/index-texto.html>>  
 acesso em 17/05/2005.

NETO, C. C. **Salas de Videoconferência**. Disponível no site <<http://www.cciencia.ufrj.br/educnet/salavide.htm>> acesso em: 15/04/2005.

ROECH, Sylvia Maria Azevedo. **Projetos de Estágio e de Pesquisa em Administração** 2º Edição Publicação Editora Atlas S.A. 1999.

SOARES, L.F.G, LEMOS, G e COLCHER, S. **Redes Computadores das LANs, MANs e WANs às Redes ATM** 2 ed. Rio de Janeiro: Editora Campus, 1995.

SOARES, L.F.G.; Martins, S. de L.; Bastos, T.L.P. - **"Lan Based Real Time Audio-Graphics Conferencing System, General Overview"** - CCR066 TR Rio Scientific Center-IBM Brasil, Novembro de 1988.

SOUSA, Lindberg Barros. **Redes: Transmissão de dados, voz e imagem** São Paulo: Editora Erica, 2000.

TANENBAUM, Andrews S. **Rede de Computadores** Rio de Janeiro: Editora Campus, 1989.

TAROUCO, Liane M. R.; et alii. **Videoconferência**. In: Rede Nacional de Pesquisas(RNP) - Grupo de Trabalho Aplicações Educacionais em Rede, 2003.

THIOLLENT, M. **Metodologia da pesquisa-ação**. 10.ed. São Paulo: Cortez: Autores Associados, 1992.

WILLEBEEK-LEMAIR, M.H. & SHAE, Z. "**Distributed video conferencing systems**" **Computer Communications**, vol. 20, pp. 157-168,1997.

WIRTH, Almir **Telecomunicações Multimídia - Internet, LAN's e WAN's** Rio de Janeiro: Editora Book Express, 2001.

#### **Links Relacionados:**

**RealProducer**<<http://www.realnetworks.com/products/discreteserver/index.html>>

**MRTG**<<http://people.ee.ethz.ch/~oetiker/webtools/mrtg/>>

**Nagios** <<http://www.nagios.org/>>

**ALFA -FADO**<<http://www.alfafado.com/>>

**Skype**<<http://web.skype.com/home.pt.html>>

**Alpine**<<http://www.extremenetworks.com.br/alpine3800.asp>>

**OUTROS TRABALHOS EM:**  
[www.projetoderedes.com.br](http://www.projetoderedes.com.br)