GEORGE MARCEL MONTEIRO ARCURI SMETANA

**UM SISTEMA DE CONFERÊNCIA CENTRALIZADA COM CONTROLE
DE POSSE DA PALAVRA PARA EDUCAÇÃO A DISTÂNCIA**

Dissertação apresentada à Escola
Politécnica da Universidade de São Paulo
para obtenção do Título de Mestre em
Engenharia

São Paulo
2004

GEORGE MARCEL MONTEIRO ARCURI SMETANA

**UM SISTEMA DE CONFERÊNCIA CENTRALIZADA COM CONTROLE
DE POSSE DA PALAVRA PARA EDUCAÇÃO A DISTÂNCIA**

Dissertação apresentada à Escola
Politécnica da Universidade de São Paulo
para obtenção do Título de Mestre em
Engenharia

Área de Concentração:
Sistemas Digitais

Orientador:
Profa. Dra. Tereza Cristina Melo de Brito
Carvalho

São Paulo
2004

Consagro este trabalho a Jesus Cristo, meu Senhor, Salvador,
Pai, Irmão e Amigo, para quem e por quem tenho vivido.

AGRADECIMENTOS

Em primeiro lugar, a Deus, por seu amor, carinho e cuidado por mim.

À Profa. Dra. Tereza Cristina Melo de Brito Carvalho, minha orientadora neste trabalho, pelas orientações, conselhos, amizade e motivação.

Ao Prof. Dr. Wilson Vicente Ruggiero, pela sua liderança e pela oportunidade que me foi dada no LARC.

Ao amigo e companheiro de projeto Reinaldo Matushima, pela sua competência, inteligência e empenho, sem os quais este trabalho seria extremamente dificultado.

A Ricardo Komatsu, da Scopus Tecnologia S.A., e à Profa. Dra. Regina Melo Silveira, pelas discussões relacionadas ao sistema de conferência multiponto.

Aos amigos do LARC, em especial, a Leonardo Augusto Martucci, companheiro de tantos trabalhos e de tantos momentos alegres.

Aos amigos do colégio, da faculdade e do clube, inesquecíveis e marcantes.

Aos amigos e irmãos em Cristo, pelas suas orações, intercessão, orientações, lições de vida, apoio, amizade e companheirismo.

Aos meus pais, George e Maria Lúcia, que me proporcionaram meios de chegar até aqui e aos meus irmãos, Giselle, Patrick e Michelle. Amo a todos vocês. Tudo se fará novo, em nome de Jesus.

À Maria Leonor e sua família, por todas as coisas. Deus o sabe.

RESUMO

Este trabalho apresenta um sistema de conferência multiponto centralizada com controle de posse da palavra, que oferece comunicação por voz e por texto, desenvolvido para dar suporte a ferramentas de educação a distância baseadas em tecnologia *web*.

Além do sistema de conferência multiponto, este trabalho introduz, também, conceitos de voz sobre IP (VoIP), *codecs* de áudio, tráfego de tempo real sobre redes IP, mecanismos de distribuição de pacotes em redes IP, conferências multimídia sobre redes IP, criação e controle de conferências e mecanismos para se controlar a transmissão de pacotes de voz em conferências multiponto, como detecção de atividade de voz (VAD) e controle de posse da palavra.

O controle de posse da palavra ou moderação é uma metodologia para coordenar o acesso a recursos de mídia contínua, como os canais de áudio e vídeo em conferências, resolvendo eventuais conflitos e condições de corrida e garantindo o uso exclusivo dos mesmos por um participante da conferência. O controle de posse da palavra é apropriado para a dinâmica de uma sala de aula, onde na maioria das vezes, o professor exerce o papel de um moderador e de principal interlocutor. Além de regular o fluxo de informação na sala de aula virtual, o controle de posse da palavra também ajuda a reduzir a utilização dos recursos da rede. Como principal resultado deste trabalho, uma arquitetura para o sistema de conferência multiponto foi proposta, implementada e testada.

Verificou-se que o sistema é escalável e que o controle de posse da palavra reduz o grau de interatividade entre os participantes da conferência, mas funciona eficazmente como mecanismo para reduzir a utilização dos recursos de rede. A comunicação adicional por texto ajuda a reduzir o impacto do controle de posse da palavra no grau de interatividade. Neste trabalho, o uso de uma topologia centralizada para a realização de conferências multiponto mostrou-se bastante vantajoso, principalmente porque o tráfego *multicast* não era suportado.

ABSTRACT

This work presents a centralized multipoint conference system with floor control, which offers voice and text communication capability, developed to support distance learning tools based on web technology.

This work also brings concepts about voice over IP (VoIP), audio codecs, real-time traffic over IP networks, packet distribution mechanisms in IP networks, multimedia conferences over IP networks, establishment and control of conferences and mechanisms to control voice packets transmission in multipoint conferences, as Voice Activity Detection (VAD) and floor control.

Floor control is a suitable methodology for coordinating access to continuous media resources, such as audio and video channels in conferences, solving resource conflicts and race conditions and guaranteeing their mutually exclusive use by one participant of the conference. Floor control is appropriate for the classroom's dynamics, where the teacher, mostly, has the role of a moderator and main talker.

Besides regulating the information flow in the virtual classroom, floor control helps reducing the need for network resources.

As main result, an architecture for the multipoint conference system was proposed, implemented and tested. It was found that the system is scalable and that floor control reduces the interactivity among the conference's participants, but works efficiently as a mechanism for reducing the need for network resources. Text communications help lowering the impact of floor control on interactivity. In this work, the deployment of a centralized topology for multipoint conferences showed to be very advantageous, mainly because multicast traffic was not supported.

SUMÁRIO

1.	INTRODUÇÃO	1
1.1	Motivação.....	2
1.2	Objetivos	2
1.3	Organização do trabalho	3
2.	VISÃO GERAL DOS PRINCIPAIS CONCEITOS.....	5
2.1	Voz sobre IP.....	6
2.1.1	Características dos <i>codecs</i> de áudio utilizados para codificar voz.....	11
2.1.1.1	Os <i>codecs</i> de áudio baseados em amostras	11
2.1.1.2	Os <i>codecs</i> de áudio baseados em <i>frames</i>	13
2.1.1.3	Qualidade subjetiva de um <i>codec</i> de áudio	13
2.1.1.4	Comparação entre os <i>codecs</i> de áudio	15
2.1.2	O protocolo de transporte de tempo real em redes IP	16
2.1.3	Mecanismos de distribuição de pacotes em redes IP	17
2.1.3.1	IP Unicast	18
2.1.3.2	IP Broadcast	18
2.1.3.3	IP Multicast	18
2.2	Conferências multimídia sobre redes IP	19
2.2.1	Unidade de controle multiponto e conferências centralizadas	22
2.2.1.1	Utilização de banda nos pontos da conferência multiponto centralizada	25
2.2.1.2	Utilização de banda na unidade de controle multiponto	26
2.2.1.3	Utilização de banda na rede da conferência multiponto centralizada	28
2.2.2	Criação e controle de conferências	28
2.2.3	Mecanismos para controle de transmissão de pacotes de voz.....	30
2.2.4	Detecção de silêncio.....	31
2.3	Ambientes virtuais multimídia colaborativos	32
2.3.1	Controle de posse de palavra em ambientes colaborativos.....	34
2.4	Tradutores de endereços de rede e de portas.....	37
2.4.1	O NAT básico	38
2.4.2	O NAPT	39
2.4.3	Problemas com o NAT e o NAPT.....	39
2.4.4	Uma solução genérica para o problema do NAPT.....	43
2.5	Considerações finais.....	44
3.	ESPECIFICAÇÃO DO SISTEMA	47
3.1	Definições	47
3.2	Requisitos funcionais do sistema	48
3.2.1	Requisitos gerais do sistema	48
3.2.2	Requisitos funcionais das salas virtuais de conferência.....	52
3.2.2.1	Representação das salas virtuais de conferência.....	52
3.2.2.2	Políticas de acesso às salas virtuais de conferência	53
3.2.2.3	Papéis sociais dentro da conferência.....	54

3.2.3	Requisitos funcionais do gerenciamento do sistema.....	56
3.2.4	Requisitos funcionais da base de dados do sistema	57
3.2.5	Requisitos funcionais de comunicação de tempo real.....	58
3.2.6	Integração com outros sistemas	59
3.3	Especificação técnica da comunicação de tempo real do sistema.....	60
3.3.1	Mecanismo de distribuição de pacotes.....	61
3.3.2	Tipo de conferência multiponto	61
3.3.3	Mecanismo de controle de transmissão de pacotes.....	63
3.3.4	Protocolo criação e controle de conferências.....	63
3.3.5	<i>Codec</i> de áudio	64
3.3.6	Utilização de portas UDP e portas base	64
3.3.7	Apresentação e justificativa da solução adotada para a comunicação de tempo real	65
3.3.8	Análise crítica da solução adotada para a comunicação de tempo real..	66
3.4	Especificação técnica do controle de sessão e de posse da palavra	68
3.4.1	Aspectos relacionados ao sistema	68
3.4.1.1	Classificação do mecanismo de controle de posse da palavra	68
3.4.1.2	Políticas e mecanismos de controle de sessão e de posse da palavra.	68
3.4.2	Aspectos relacionados ao usuário	71
3.4.2.1	Interface homem-máquina da sala virtual de conferência.....	72
3.4.2.2	Indicações e representações audiovisuais	72
3.4.3	Análise crítica da solução adotada para o controle de sessão e de posse da palavra	75
3.5	Considerações finais.....	75
4.	ARQUITETURA E IMPLEMENTAÇÃO DO SISTEMA	76
4.1	Arquitetura do sistema de conferência multiponto	76
4.1.1	Interação entre os subsistemas	78
4.2	Implementação do sistema de conferência multiponto	79
4.3	Detalhamento da implementação do sistema	82
4.3.1	Base de dados	83
4.3.2	Subsistemas de gerenciamento e de acesso às salas virtuais de conferência	83
4.3.2.1	Funcionalidades oferecidas	84
4.3.2.2	Informações dinâmicas dos subsistemas de gerenciamento e de acesso às salas virtuais de conferência.....	85
4.3.2.3	Segurança nos <i>sites</i> do sistema	86
4.3.2.4	Página <i>web</i> do usuário e sala virtual de conferência.....	86
4.3.2.5	Modos de integração com outros sistemas.....	91
4.3.3	Subsistema de comunicação de tempo real.....	93
4.3.3.1	O servidor de unidades de controle multiponto	94
4.3.3.2	A unidade de controle multiponto.....	99
4.3.3.2.1	Funcionamento da unidade de controle multiponto.....	100
4.3.3.2.2	A estrutura de dados da unidade de controle multiponto.....	101
4.3.3.3	A <i>applet</i> Java do usuário	103
4.3.3.4	Portas base e portas UDP da unidade de controle multiponto e da <i>applet</i> Java.....	108

4.3.3.5	Solucionando o problema da tradução de endereços e portas.....	111
4.4	Controle de sessão e de posse da palavra.....	112
4.4.1	Aspectos relacionados ao sistema	112
4.4.1.1	Sincronismo de informações e distribuição dos pacotes de controle.	113
4.4.2	Aspectos relacionados ao usuário	115
4.4.3	Diagramas de tempo de troca de mensagens de controle de conferência	116
4.4.4	Resolvendo problemas de consistência durante a conferência	120
4.5	Processamento de pacotes	122
4.5.1	Processamento de pacotes de controle de sessão	122
4.5.2	Processamento de pacotes de controle de posse da palavra.....	125
4.5.3	Processamento de pacotes RTP.....	126
4.5.4	Processamento de pacotes RTCP.....	132
4.6	O <i>chat</i> de texto	133
4.7	Análise de escalabilidade do sistema	133
4.8	Considerações finais.....	136
5.	RESULTADOS EXPERIMENTAIS	139
5.1	Ambientes de testes.....	143
5.2	Testes funcionais.....	145
5.2.1	Testes das funcionalidades do administrador do sistema.....	146
5.2.1.1	Acesso ao sistema de gerenciamento	146
5.2.1.2	Listagem, criação, modificação e exclusão de salas	147
5.2.1.3	Listagem, criação, modificação e exclusão de usuários.....	152
5.2.1.4	Associação de usuários a salas	155
5.2.1.5	Início e término de salas.....	159
5.2.2	Testes das funcionalidades do usuário do sistema	164
5.2.2.1	Acesso ao sistema	164
5.2.2.2	Participação em conferências virtuais.....	166
5.2.3	Testes das funcionalidades gerais	167
5.2.3.1	Testes do controle de posse da palavra	167
5.2.3.2	Teste de integração com outro sistema	172
5.2.3.3	Testes com NAPT	179
5.3	Testes quantitativos.....	185
5.3.1	Caracterização da transmissão de pacotes RTP pela <i>applet</i> Java do usuário	186
5.3.2	Avaliação do desempenho do controle de posse da palavra	188
5.3.3	Medição da banda consumida pela unidade de controle multiponto	193
5.3.4	Avaliação do desempenho de uma unidade de controle multiponto isolada	196
5.3.5	Avaliação do desempenho de duas unidades de controle multiponto em abordagem multitarefa.....	200
5.3.6	Avaliação do desempenho de duas unidades de controle multiponto em abordagem multiprocesso.....	202
5.3.7	Avaliação da utilização de recursos computacionais pela unidade de controle multiponto e pela <i>applet</i> Java.....	203
5.4	Testes qualitativos.....	205
5.4.1	Testes remotos.....	205

5.4.2	Avaliação subjetiva	208
5.5	Considerações finais.....	210
6.	CONCLUSÕES E TRABALHOS FUTUROS.....	213
6.1	Avaliação do sistema.....	213
6.2	Resultados alcançados.....	215
6.3	Trabalhos futuros e sugestões	216
6.4	Contribuições	217
A.	TABELAS DA BASE DE DADOS DO SISTEMA DE CONFERÊNCIA	218
B.	FORMATOS DOS PACOTES DE CONTROLE DE CONFERÊNCIA	226
C.	DIAGRAMA DE TROCA DE MENSAGENS DE CONTROLE DE CONFERÊNCIA.....	235
C.1	Diagramas de tempo de troca de mensagens de controle de posse da palavra.....	236
C.1.1	Participante comum pedindo a posse da palavra.....	236
C.1.2	Participante comum desistindo de pedir a posse da palavra	238
C.1.3	Participante comum devolvendo a posse da palavra.....	239
C.1.4	Moderador concedendo a posse da palavra de um participante para outro	240
C.1.5	Moderador concedendo a posse da palavra para um participante....	242
C.1.6	Moderador tomando de volta a posse da palavra	243
C.1.7	Moderador pedindo a posse da palavra.....	245
C.1.8	Moderador desistindo do pedido de posse da palavra.....	246
C.1.9	Moderador bloqueando o recebimento de áudio de um participante	246
C.1.10	Moderador liberando o recebimento de áudio de um participante...	248
C.2	Diagramas de tempo de troca de mensagens de controle de sessão.....	249
C.2.1	Moderador pedindo para entrar na conferência	249
C.2.2	Participante comum pedindo para entrar na conferência	252
C.2.3	Moderador admitindo um participante na conferência	253
C.2.4	Moderador rejeitando um participante na conferência.....	254
C.2.5	Moderador expulsando um participante da conferência	255
C.2.6	Moderador expulsando o participante da conferência com a posse da palavra	256
C.2.7	Moderador anistiando um participante que foi expulso da conferência	257
C.2.8	Participante abandonando a conferência.....	259
C.2.9	Participante com a posse da palavra abandonando a conferência....	260
C.2.10	Moderador abandonando a conferência	261
C.2.11	Moderador tentando eleger um participante como o novo moderador da conferência	263
C.2.12	Participante aceitando ser o novo moderador da conferência.....	265
C.2.13	Participante não aceitando ser o novo moderador da conferência...	266
C.2.14	Moderador com problemas de comunicação com a unidade de controle multiponto	267
C.2.15	Participante com problemas de comunicação com a unidade de controle multiponto	269
	LISTA DE REFERÊNCIAS	271

LISTA DE FIGURAS

Figura 2.1 – Transmissão e recepção de pacotes de voz.....	8
Figura 2.2 – Encapsulamento dos pacotes de áudio sobre os protocolos da arquitetura TCP/IP.....	9
Figura 2.3 – Ilustração de uma conferência multiponto centralizada utilizando IP <i>unicast</i> com uma unidade de controle multiponto e seis participantes.	23
Figura 2.4 – Cenário de uma aplicação de rede <i>peer-to-peer</i> em uma rede com NAT.	41
Figura 3.1 – Ambiente de utilização do sistema de conferência multiponto.	49
Figura 3.2 – Diagrama de transição de indicações para o moderador.	74
Figura 3.3 – Diagrama de transição de indicações para o participante comum.....	74
Figura 4.1 – Subsistemas do sistema de conferência multiponto.....	77
Figura 4.2 – Arquitetura do sistema de conferência multiponto proposto.....	78
Figura 4.3 – Implementação da arquitetura do sistema de conferência proposto.	81
Figura 4.4 – Interface homem-máquina do tipo <i>janela inteira</i>	88
Figura 4.5 – Interface homem-máquina do tipo <i>janela mínima</i>	88
Figura 4.6 – Interface homem-máquina do tipo <i>janela flutuante</i>	89
Figura 4.7 – Sala virtual de conferência ambientada em um porto.....	91
Figura 4.8 – Requisição atendida com sucesso para iniciar uma sala virtual de conferência.	95
Figura 4.9 – Requisição bem sucedida para se fechar a unidade de controle multiponto de uma sala virtual de conferência.	96
Figura 4.10 – Consulta ao servidor de unidades de controle multiponto a respeito das salas virtuais de conferência abertas.	96
Figura 4.11 – Consulta ao servidor de unidades de controle multiponto a respeito dos participantes de uma conferência em uma determinada sala.	97
Figura 4.12 – A unidade de controle multiponto de uma sala virtual sendo iniciada e depois terminada.	98
Figura 4.13 – Ilustração das abordagens multitarefa (a), multiprocesso (b) e híbrida (c) para o uso de unidades de controle multiponto simultâneas.....	99
Figura 4.14 – Sistema de conferência com unidades de controle multiponto distribuídas atrás de um NAT/NAPT com encaminhamento estático de portas.....	105
Figura 4.15 – Participante comum pedindo a posse da palavra.	117
Figura 4.16 – Moderador, com a posse da palavra, concedendo-a a um participante comum.....	119
Figura 4.17 – Processamento de pacotes RTP.	129
Figura 4.18 – Rotina de transmissão de pacotes RTP.....	131
Figura 5.1 – Topologia da maior parte dos testes.	144
Figura 5.2 – Tela de acesso ao <i>site</i> de gerenciamento.	147
Figura 5.3 – Tela inicial do <i>site</i> de gerenciamento do sistema, listando as salas existentes.....	148
Figura 5.4 – Criação de uma sala virtual de conferência.	149
Figura 5.5 – Sala criada com sucesso.....	150
Figura 5.6 – Sala modificada com sucesso.	151

Figura 5.7 – Tela para confirmação de exclusão de sala.....	151
Figura 5.8 – Sala excluída com sucesso.....	152
Figura 5.9 – Usuários cadastrados no sistema.	153
Figura 5.10 – Cadastro de usuário.	154
Figura 5.11 – Sala virtual sem nenhum usuário associado a ela.....	155
Figura 5.12 – Processo de associação de usuários a uma sala.	156
Figura 5.13 – Escolha do moderador da sala com moderador fixo.....	157
Figura 5.14 – Mensagem recebida por um usuário cadastrado tentando acessar uma sala virtual do tipo <i>fechada</i> sem estar associado a ela.	157
Figura 5.15 – Participante da sala virtual do tipo <i>fechada</i> tentando entrar na conferência antes que o moderador.....	158
Figura 5.16 – Sala iniciada com sucesso.....	159
Figura 5.17 – Sala fechada com sucesso.....	160
Figura 5.18 – Servidor de unidades de controle multiponto iniciando e fechando com sucesso a unidade de controle multiponto associada à sala virtual.....	161
Figura 5.19 – Sala iniciada, mas com problemas de comunicação com o servidor de unidades de controle multiponto.	161
Figura 5.20 – Sala fechada, mas com problemas de comunicação com o servidor de unidades de controle multiponto.	162
Figura 5.21 – Sala fechada, mas com problemas para destruir as variáveis de aplicação do servidor <i>web</i>	163
Figura 5.22 – Várias salas abertas no servidor de unidades de controle multiponto.	163
Figura 5.23 – Tela de acesso ao <i>site</i> de conferências.....	164
Figura 5.24 – Tela de escolha de salas virtuais de conferência para os usuários cadastrados no sistema.	165
Figura 5.25 – Tela de escolha de salas virtuais de conferência para os usuários não cadastrados no sistema.	166
Figura 5.26 – Mensagem de erro avisando ao usuário que ele já está participando de uma conferência.	167
Figura 5.27 – Bandas de transmissão e de recepção medidas na unidade de controle multiponto durante o roteiro de testes #1.....	169
Figura 5.28 – Bandas de transmissão e de recepção medidas na unidade de controle multiponto durante o roteiro de testes #2.....	170
Figura 5.29 – Página <i>web</i> criada para teste de integração com o COL, contendo os <i>links</i> para o professor e para os alunos.....	174
Figura 5.30 – Aluno tentando acessar a sala de aula virtual sem ela ter sido iniciada pelo professor.	174
Figura 5.31 – Página <i>web</i> para o aluno confirmar suas informações pessoais e preencher as demais informações necessárias.....	175
Figura 5.32 – Primeira tela para o professor: configuração da sala de aula virtual.	176
Figura 5.33 – Sala de aula virtual iniciada pelo professor.	177
Figura 5.34 – Sala de aula virtual fechada pelo professor.	177
Figura 5.35 – Página <i>web</i> para confirmação dos dados do professor.	178
Figura 5.36 – Sala de aula virtual com um professor e um aluno presentes.	179
Figura 5.37 – Topologia de rede utilizada para os testes com NAPT.....	179
Figura 5.38 – Configurações de NAPT do roteador Cisco 2514.	180
Figura 5.39 – Pacotes da rede interna do NAPT capturados no <i>software sniffer</i>	182

Figura 5.40 – Tradução de endereços IP e de portas UDP no NAPT feita pelo roteador Cisco 2514.	182
Figura 5.41 – Captura de portas pela unidade de controle multiponto.	183
Figura 5.42 – Pacotes RTP de áudio GSM capturados no transmissor (<i>software sniffer</i> Netasyst WLX).	187
Figura 5.43 – Avaliação de <i>jitter</i> e perda de pacotes RTP do transmissor (<i>software sniffer</i> Advisor LAN).	187
Figura 5.44 – O participante <i>Marcel</i> como moderador da conferência e com a posse da palavra.	189
Figura 5.45 – O participante <i>Reinaldo</i> com a posse da palavra.	189
Figura 5.46 – Captura de pacotes no <i>software sniffer</i> Advisor LAN mostrando a concessão da posse da palavra do moderador (endereço IP 192.168.2.2) para um participante comum (endereço IP 192.168.2.4), através dos quadros capturados #161, #162, #163, #164 e # 184).	190
Figura 5.47 – Bandas de transmissão e de recepção da unidade de controle multiponto.	193
Figura 5.48 – Pacotes RTP de áudio capturados pelo <i>software sniffer</i> Netasyst WLX no servidor da unidade de controle multiponto. Notar as portas UDP de destino na coluna “ <i>Summary</i> ”.	197
Figura 5.49 – Pacotes RTP de áudio capturados de duas salas virtuais de conferência hospedadas em um mesmo servidor de unidades de controle multiponto. Notar as portas UDP de destino e de origem na coluna “ <i>Summary</i> ”.	200
Figura 5.50 – Pacotes RTP de áudio capturados de três salas concorrentes em abordagem multitarefa. Notar as portas UDP de destino e de origem na coluna “ <i>Summary</i> ”.	202
Figura 5.51 – Pacotes RTP de áudio capturados de duas salas concorrentes em abordagem multiprocesso. Notar as portas UDP de destino e de origem na coluna “ <i>Summary</i> ”.	203
Figura 5.52 – Topologia de rede do teste #1, com um <i>cable modem</i>	206
Figura 5.53 – Topologia de rede dos testes #2 e #3, com um <i>modem</i> analógico.	206
Figura A.1 – Relacionamento entre as três tabelas do sistema.	219
Figura B.1 – Pacote para pedido de entrada na conferência (controle de sessão). ..	226
Figura B.2 – Pacote de controle de sessão.	230
Figura B.3 – Pacote do protocolo controle de posse da palavra.	230
Figura B.4 – Pacote do protocolo de <i>chat</i> de texto.	233
Figura C.1 – Participante comum pedindo a posse da palavra.	236
Figura C.2 – Participante comum desistindo de pedir a posse da palavra.	238
Figura C.3 – Participante comum devolvendo a posse da palavra para o moderador.	239
Figura C.4 – Moderador concedendo a posse da palavra de um participante para outro.	240
Figura C.5 – Moderador concedendo a posse da palavra para um participante que a esteja requisitando ou não.	242
Figura C.6 – Moderador tomando de volta a posse da palavra.	243
Figura C.7 – Moderador pedindo a posse da palavra.	245
Figura C.8 – Moderador desistindo do pedido de posse da palavra.	246
Figura C.9 – Moderador bloqueando o recebimento de áudio de um participante. ..	247
Figura C.10 – Moderador liberando o recebimento de áudio de um participante.	248

Figura C.11 – Moderador pedindo para entrar na conferência e sendo aceito pela unidade de controle multiponto.....	249
Figura C.12 – Moderador pedindo para entrar na conferência e sendo rejeitado pela unidade de controle multiponto.....	251
Figura C.13 – Participante comum pedindo para entrar na conferência.	252
Figura C.14 – Moderador admitindo um participante na conferência.	254
Figura C.15 – Moderador rejeitando um participante na conferência.	255
Figura C.16 – Moderador expulsando um participante da conferência.	256
Figura C.17 – Moderador expulsando um participante que estava com a posse da palavra.	257
Figura C.18 – Moderador anistiando um participante que foi expulso da conferência.	258
Figura C.19 – Participante abandonando a conferência.	259
Figura C.20 – Participante com a posse da palavra abandonando a conferência.....	260
Figura C.21 – Moderador abandonando a conferência.	261
Figura C.22 – Moderador tentando eleger um participante como o novo moderador da conferência.	263
Figura C.23 – Moderador tentando eleger um participante como o novo moderador da conferencia, mas não recebe a confirmação de recebimento do participante	264
Figura C.24 – Participante aceitando ser o novo moderador da conferência.....	265
Figura C.25 – Participante não aceitando ser o novo moderador da conferência. ...	266
Figura C.26 – Moderador restabelecendo a comunicação com a unidade de controle multiponto.	268
Figura C.27 – Moderador não conseguindo restabelecer comunicação com a unidade de controle multiponto.	269
Figura C.28 – Participante restabelecendo a comunicação com a unidade de controle multiponto.	270
Figura C.29 – Participante não conseguindo restabelecer a comunicação com a unidade de controle multiponto.....	270

LISTA DE TABELAS

Tabela 2.1 – Critérios utilizados para MOS em avaliações de áudio	14
Tabela 2.2 – Comparação entre alguns <i>codecs</i> utilizados em conferências.....	16
Tabela 2.3 – Ferramentas multimídia colaborativas e suas classificações.....	33
Tabela 3.1 – Indicações audiovisuais do usuário e seus significados.....	73
Tabela 4.1 – Ambientes disponíveis para as salas virtuais de conferência.....	90
Tabela 4.2 – Ações e parâmetros das requisições HTTP enviados pelo gerenciador ao servidor de unidades de controle multiponto	94
Tabela 4.3 – Faixa de portas UDP para o sistema de conferência	109
Tabela 5.1 – Configuração do servidor utilizado como unidade de controle multiponto, servidor <i>web</i> e servidor de banco de dados	144
Tabela 5.2 – Roteiro de teste para conferência com dois participantes	168
Tabela 5.3 – Roteiro de teste para conferência com três participantes	168
Tabela 5.4 – Tempos medidos na troca de posse da palavra.	192
Tabela 5.5 – Medições realizadas para caracterizar os cenários dos testes remotos.	207
Tabela 5.6 – Resumo dos resultados obtidos nos testes.....	212
Tabela B.1 – Tipos de mensagem do protocolo de controle de conferência.....	229
Tabela B.2 – Tipos de mensagem de controle de posse da palavra	232

ACRÔNIMOS

ACK	A cknowledgement Packet
ADSL	A symmetric D igital S ubscriber L ine
ASN.1	A btract S yntax N otation O ne (X.680 – X.693)
COL	C ursos on L ARC
DTX	D iscontinuous T ransmission
FIFO	F irst I n F irst O ut
FCFS	F irst C ome F irst S erved
FTP	F ile T ransfer P rotocol (RFC 238)
GSM	G roup S péciale M obile/ G lobal S ystem for M obile C ommunications
HTTP	H ypertext T ransfer P rotocol (RFC 2616)
HTTPS	H TTP over S ecure S ocket L ayer (RFC 2818)
IANA	I nternet A ssigned N umbers A uthority
IETF	I nternet E ngineering T ask F orce
IGMP	I nternet G roup M anagement P rotocol
IP	I nternet P rotocol (RFC 791)
ITU	I nternational T elecommunication U nion
ITU-T	I TU T elecommunication S tandardization S ector
JMF	J ava M edia F ramework
LARC	L aboratório de A rquitetura e R edes de C omputadores
LRS	L east R ecently S erved
MMUSIC	M ultiparty M ultimedia S ession C ontrol
MC	M ultipoint C ontroller (Controlador multiponto)
MCU	M ultipoint C ontrol U nit (Unidade de controle multiponto)
MIPS	M ilhões de I nstruções p or s egundo
MOS	M ean O pinion S core
MP	M ultipoint P rocessor (Processador multiponto)
MTU	M aximum T ransmission U nit (Máxima unidade de transmissão)
NAT	N etwork A ddress T ranslator (Tradutor de endereço de rede)
NAPT	N etwork A ddress and P ort T ranslator (Tradutor de endereço de rede e de porta)
PCI	P eripheral C omponent I nterconnect
PER	P acked E ncoding R ules (ASN.1) (X.691)
pps	P acotes p or s egundo
QoS	Q uality o f S ervice (Qualidade de serviço)
RAM	R andom A ccess M emory (Memória de acesso aleatório)
RDSI	R ede D igital de S erviços I ntegrados
RFC	R equest for C omments
RSVP	R esource R eservation P rotocol (RFC 2205 a 2210)
RTCP	R TCP C ontrol P rotocol (RFC 1889)
RTP	R eal-Time T ransport P rotocol (RFC 1889)
RTT	R ound-Trip T ime
SID	S ilence I nsertion D escriptor
SIP	S ession I nitiation P rotocol (RFC 3261)

TCP	T ransport C ontrol P rotocol (RFC 793)
UDP	U ser D atagram P rotocol (RFC 768)
URI	U niform R esource I ndicator (RFC 2396)
URL	U niform R esource L ocator (RFC 2396)
VAD	V oice A ctivity D etection
VoIP	V oice o ver I P
WFQ	W eighted F air Q ueueing
WYSIWIMS	W hat Y ou S ee I s W hat I M ay S ee
WYSIWIS	W hat Y ou S ee I s W hat I S ee

1. INTRODUÇÃO

“Ainda que eu fale a língua dos homens e dos anjos, se não tiver amor, serei como o bronze que soa ou como o címbalo que retine. Ainda que eu tenha o dom de profetizar e conheça todos os mistérios e toda a ciência; ainda que eu tenha tamanha fé, a ponto de transportar os montes, se não tiver amor, nada serei. E ainda que eu distribua todos os meus bens entre os pobres e ainda que entregue o meu próprio corpo para ser queimado, se não tiver amor, nada disso me aproveitará.”

1 Coríntios 13.1-3

Com o crescimento da área de educação a distância, as ferramentas para essa finalidade têm se tornado mais sofisticadas, incorporando tecnologias e técnicas de ambientes colaborativos virtuais para superar barreiras naturais decorrentes da separação espacial entre as pessoas, como a falta de interação homem-a-homem. Comunicações não-verbais, como gestos e contato visual, são responsáveis por grande parte da transmissão da mensagem em interações face-a-face (DOMMEL, GARCIA-LUNA-ACEVES, 1997 apud HAYNE, PENDERGAST, GREENBERG, 1993/94).

Uma sala de aula virtual para educação a distância é um dos paradigmas para ambientes colaborativos propostos por Qiu, Kuhns e Cox (2002). Nesse paradigma, a interação entre os participantes é assimétrica, isto é, o áudio e o vídeo do professor são transmitidos para os alunos e, ocasionalmente, um aluno recebe a permissão do professor para se dirigir à classe, com a finalidade de realizar ou responder uma pergunta ou fazer algum comentário. O paradigma da sala de aula virtual é, na verdade, uma especialização do paradigma de uma conferência moderada, com o professor se comportando como o moderador e os estudantes, como a audiência.

Este trabalho descreve um sistema de conferência multiponto centralizada com controle de posse de palavra desenvolvido para dar suporte a ferramentas de educação a distância baseadas em tecnologia *web*. O sistema desenvolvido oferece comunicação por áudio e por texto. O controle de posse da palavra foi utilizado no

sistema para regular a interação entre os participantes da conferência e para controlar o acesso ao canal de áudio de forma a se utilizar mais eficientemente os recursos de rede.

O sistema de conferência multiponto proposto neste trabalho foi desenvolvido dentro do contexto de um projeto do LARC – Laboratório de Arquitetura e Redes de Computadores (LARC, 2003) em parceria com a empresa Scopus Tecnologia S. A¹.

1.1 Motivação

A motivação deste trabalho é oferecer recursos de comunicação multiponto por voz para sistemas baseados em tecnologia *web*, em especial, para sistemas de ensino a distância. A comunicação por voz permite uma maior interatividade e uma experiência mais rica para o usuário de sistemas de ensino a distância.

Embora o foco seja a educação a distância, nada impede que o sistema de conferência sugerido seja utilizado em outros cenários onde a mesma dinâmica de conversação é aplicável, como em uma conferência onde um dos participantes exerce o papel social do moderador e de interlocutor principal.

1.2 Objetivos

Os objetivos principais deste trabalho são a proposta e o desenvolvimento de um sistema de conferência multiponto por voz voltado para a área de educação a distância, reproduzindo em um ambiente virtual a dinâmica de conversação de uma sala de aula real.

O sistema de conferência multiponto deve:

¹ Scopus Tecnologia S. A. Disponível em: <<http://www.scopus.com.br>>. Acesso em: 28 jan. 2004.

- Garantir um grau mínimo de interatividade entre o professor e os alunos, permitindo a comunicação entre eles por voz e, opcionalmente, por texto;
- Ser funcional em ambientes típicos de ensino a distância, podendo ser acessado localmente, através de uma *intranet*, ou remotamente, através de uma conexão discada ou de banda larga;
- Ser de fácil utilização;
- Ser escalável, com relação ao número de alunos em uma sala de aula virtual e à utilização de salas de aula virtuais simultâneas;
- Requerer recursos computacionais simples, compatíveis com o perfil de usuários domésticos.

1.3 Organização do trabalho

Este primeiro capítulo descreve o contexto, os objetivos e o foco do trabalho.

O segundo capítulo apresenta conceitos de voz sobre IP (VoIP), *codecs* de áudio, tráfego de tempo real sobre redes IP, mecanismos de distribuição de pacotes em redes IP, conferências multimídia sobre redes IP, criação e controle de conferências e mecanismos para se controlar a transmissão de pacotes de voz. Esses conceitos foram necessários para o desenvolvimento do sistema de conferência proposto. Leitores familiarizados com os conceitos citados podem ir direto ao terceiro capítulo, enquanto que é recomendável aos leitores não familiarizados lerem o segundo capítulo para obterem uma melhor compreensão desta dissertação.

O problema central deste trabalho é o desenvolvimento de um sistema de conferência voltado para ensino a distância, capaz de oferecer comunicação multiponto por voz. No terceiro capítulo, esse problema é abordado, levantando-se os requisitos do tal sistema e realizando uma discussão em torno das abordagens possíveis. A solução adotada é definida e defendida.

O quarto capítulo descreve a arquitetura, os componentes, a implementação e as funcionalidades do sistema de conferência desenvolvido.

No quinto capítulo, são apresentados os testes realizados para demonstrar as funcionalidades do sistema e para mostrar que o sistema atende aos requisitos levantados no terceiro capítulo. Os resultados obtidos são discutidos, interpretados e confrontados com o comportamento esperado.

No sexto capítulo são expostas as conclusões e considerações finais sobre o trabalho, além de algumas sugestões para melhorar o sistema desenvolvido.

Os anexos apresentam mais detalhes a respeito da implementação do sistema.

A lista de referências fecha o trabalho, com o material que serviu de suporte para o mesmo.

2. VISÃO GERAL DOS PRINCIPAIS CONCEITOS

“O amor jamais acaba; mas, havendo profecias, desaparecerão; havendo línguas, cessarão; havendo ciência, passará; porque, em parte, conhecemos e, em parte, profetizamos. Quando, porém, vier o que é perfeito, então, o que é em parte será aniquilado.”

1 Coríntios 13.8-10

O principal objetivo deste trabalho é o desenvolvimento de um sistema de conferência multiponto por voz em redes IP, voltado para a área de educação a distância. Tendo essa definição em mente, é necessário se identificar quais são as áreas de conhecimento necessárias para solucioná-lo, desdobrando-as a partir do polinômio <voz, conferência, redes IP, educação a distância>.

Como o sistema utiliza comunicação por voz em redes IP, certamente que o assunto voz sobre IP (VoIP) deve ser abordado. Um pouco de conhecimento a respeito de *codecs* de áudio é um requisito para se compreender as principais características do tráfego de voz em uma rede como a Internet. A tecnologia de voz sobre IP está intimamente ligada ao protocolo aberto para tráfego de tempo real desenvolvido pela *Internet Engineering Task Force* (IETF) (IETF, 2002), o *Real-Time Transport Protocol* (RTP) (SCHULZRINNE et al., 1996).

A utilização da Internet como rede de comunicação para tráfego de tempo real leva a uma breve discussão a respeito de banda, atraso, taxa de perda de pacotes e dos possíveis mecanismos de distribuição dos pacotes de voz em redes IP. Sendo a banda um fator crítico para o sucesso de comunicações pela Internet, faz-se necessário a apresentação de alguns mecanismos para restrição do uso da banda em conferências. Surgem daí os assuntos controle de posse da palavra (*floor control*) e detecção de atividade de voz.

Para se compreender conferências multimídia sobre redes IP é necessário se discutir um pouco sobre as topologias possíveis e suas implicações, os elementos que as constituem e os principais protocolos de estabelecimento e sinalização em uso: o

Session Initiation Protocol (SIP) (ROSENBERG et al., 2002) e a recomendação H.323 (ITU-T, 2003b).

Conferências virtuais podem ser inseridas no assunto de ambientes virtuais multimídia colaborativos, sendo que o foco em educação a distância direciona a discussão para o paradigma da sala de aula virtual, onde a interação entre professor e alunos pode ser regida pelas teorias de controle de posse da palavra, que novamente surge em cena neste trabalho.

Como os usuários do sistema podem estar localizados atrás de roteadores que utilizam a tecnologia de tradução de endereços de rede e/ou de portas (*Network Address Translator* – NAT/*Network Address and Port Translator* – NAPT) (HOLDREGE, SRISURESH, 1999) é inevitável se discutir o funcionamento de NATs e NAPT, bem como os problemas decorrentes do seu uso e as possíveis soluções para contorná-los (HOLDREGE, SRISURESH, 2001) e (SENIE, 2002).

Portanto, nesse capítulo serão discutidos os seguintes assuntos:

- Voz sobre IP;
- RTP e RTCP em redes IP;
- Mecanismos de distribuição de pacotes em redes IP;
- Conferências multimídia sobre redes IP;
- Mecanismos para controle de banda em conferências multimídia sobre redes IP;
- Ambientes multimídia virtuais colaborativos;
- Controle de posse da palavra;
- Funcionamento de NAT/NAPT, problemas associados e possíveis soluções.

2.1 Voz sobre IP

Como as redes IP não fornecem qualidade de serviço (*Quality of Service* – QoS) (CISCO, 1999) de forma nativa, a *Internet Engineering Task Force* (IETF) (IETF,

2002) desenvolveu um protocolo de transporte de tempo real, o *Real-Time Transport Protocol* (RTP) (SCHULZRINNE et al., 1996), e seu protocolo de controle, o *RTP Control Protocol* (RTCP) (SCHULZRINNE et al., 1996). O RTP e o RTCP são utilizados em aplicações de transmissão de voz e vídeo sobre IP.

O RTP adiciona a cada cabeçalho *User Datagram Protocol* (UDP) (POSTEL, 1980) um cabeçalho contendo uma marca de tempo (*timestamp*), um número de seqüência e um número de identificação da fonte de sincronismo. O número de seqüência serve para eliminar os pacotes duplicados e reordenar os pacotes recebidos fora de ordem. O *timestamp* permite a sincronização e a reprodução de cada pacote de voz no instante correto, o que é muito importante, visto que os pacotes podem sofrer atrasos variáveis (*jitter*) pelo caminho. Os pacotes recebidos são reordenados, armazenados e reproduzidos no instante correto. A fonte de sincronismo identifica quem originou cada *stream* (canal de mídia). Essa informação é vital em conferências entre vários pontos, porque os *timestamps* e números de seqüência são próprios a cada originador de *stream*. Resumidamente, o RTP oferece meios para os pacotes de áudio serem reordenados e reproduzidos nos instantes corretos.

O RTCP é utilizado como controle do RTP e também é transmitido sobre UDP. O RTCP contém estatísticas de transmissão e recepção, além de informações gerais a respeito de cada participante da conferência.

A transmissão de voz sobre IP envolve os seguintes processos:

1. Conversão da onda mecânica de voz para um sinal elétrico, através de um transdutor mecânico-elétrico.
2. Conversão analógico-digital do sinal de voz (filtragem do sinal analógico, amostragem, quantização uniforme ou não-uniforme e representação binária do sinal quantizado).
3. Codificador (compressão digital é opcional, mas desejável).
4. Transformação do sinal digitalizado em pacotes.
5. Adição de informações de controle de tempo real aos pacotes (cabeçalho RTP).

6. Encapsulamento dos pacotes sobre protocolos da arquitetura TCP/IP (cabeçalhos UDP e IP).
7. Transmissão dos pacotes.

O codificador pode mudar a codificação do sinal original digitalizado, para deixá-lo mais robusto à transmissão em um determinado meio físico, por exemplo, ou para representá-lo de forma mais eficiente, eliminando informações redundantes e informações que estão além da percepção psicoauditiva humana através de algum algoritmo de compressão. A Figura 2.1 ilustra o processo completo.

Figura 2.1 – Transmissão e recepção de pacotes de voz.

Estando o sinal de áudio já representado de forma binária, ele é dividido em pacotes e encapsulado em cima do RTP, que por sua vez é encapsulado em cima do UDP. Os pacotes de áudio não são transportados utilizando o *Transport Control Protocol* (TCP) (POSTEL, 1981c), porque o mecanismo de retransmissão dos dados não se

aplica para transmissão de voz em tempo real. A Figura 2.2 mostra o encapsulamento dos pacotes de áudio sobre os protocolos da arquitetura TCP/IP.

Áudio	Variável
RTP	12 a 72 B
UDP	12 B
IP	20 a 60 B
Camada de enlace	Variável

Figura 2.2 – Encapsulamento dos pacotes de áudio sobre os protocolos da arquitetura TCP/IP.

A expressão “tempo real” implica que o tráfego possui requisitos com relação ao tempo. Quando se transmite voz, vídeo ou qualquer outro tráfego de tempo real sobre uma rede de pacotes, é necessário atender alguns requisitos:

- *Bit rate* mínimo e/ou *bit rate* constante;
- Baixo atraso;
- Baixa variação do atraso (*jitter*);
- Reordenação de pacotes;
- Baixa perda de pacotes².

Para atender a esses requisitos de qualidade de serviço (QoS), pode ser necessário:

- Utilizar esquemas de priorização de tráfego na camada de rede, através do uso do campo *Type of Service* (TOS) do cabeçalho IPv4 (POSTEL, 1981a), cuja interpretação foi alterada, passando a ser chamado de *Differentiated Services* (*DiffServ*) (BLAKE et al., 1998) e (NICHOLS et al., 1998);

² Ao contrário do tráfego de dados normal, o tráfego de voz e de vídeo aceita uma certa porcentagem de pacotes perdidos.

- Em redes locais, utilizar na camada de enlace o padrão IEEE 802.1p (IEEE, 1998) para priorização de quadros;
- Utilizar mecanismos de reserva de banda, através do *Resource Reservation Protocol* (RSVP) (BRADEN et al., 1997);
- Configurar todos os equipamentos de rede para suportarem esses mecanismos.

O atraso constante ou ausência de *jitter* é uma característica desejada, mas não fundamental, para se garantir a reprodução das amostras no instante correto. A maioria dos *codecs* e das implementações possuem *jitter buffers*, isto é, possuem uma certa quantidade de memória alocada para armazenar os pacotes recebidos, eliminando os efeitos prejudiciais da variação do atraso e permitindo a decodificação dos pacotes armazenados em instantes regulares. A influência do *jitter* na decodificação e reconstrução do sinal só é sentida se o pacote chegar após o instante no qual ele deveria ser reproduzido. Nesse caso, o pacote seria descartado e ocorreria uma descontinuidade na reprodução do áudio.

Garantir baixo atraso é fundamental para o sucesso de comunicações bidirecionais e interativas entre pessoas. Um *round-trip time* (RTT) acima de 300 ms já começa a dificultar comunicações com essas características (ITU-T, 2000a), porque para se dar seqüência a uma conversa é necessária uma confirmação do ouvinte. Se o locutor achar que essa confirmação demorou a chegar, ele irá repetir sua locução e a conversa não avançará.

Uma situação em que pacotes seqüenciais de mesma prioridade podem chegar fora da ordem de sua transmissão (era para seguir o esquema *First In First Out* – FIFO) ocorre quando os pacotes são transmitidos por enlaces diferentes. Os pacotes poderiam tomar caminhos diferentes em enlaces com balanceamento de carga sem identificação de fluxo, com balanceamento *round-robin* por pacote, ou em situações de congestionamento de rede, onde um roteador pode redefinir a melhor rota para um destino subitamente. Raramente há inversão na ordem dos pacotes, mas, se ocorrer, os pacotes são reordenados, contanto que cheguem antes do seu instante de reprodução. Se não chegarem a tempo, são descartados.

Como não há retransmissão de pacotes, a perda deles prejudica a reconstrução dos sinais de áudio. Dependendo do *codec* utilizado, uma perda de 5% dos pacotes já é suficiente para prejudicar sensivelmente a inteligibilidade do sinal reconstruído³.

Fundamentalmente, se o pacote chegar a tempo de ser reproduzido, ele será reproduzido, independentemente de *jitter*, de ter chegado fora da ordem ou de ter sido duplicado. Se o pacote chegar após o instante de reprodução, tudo se passa como se ele tivesse sido perdido.

2.1.1 Características dos *codecs* de áudio utilizados para codificar voz

A maioria dos *codecs* de áudio utilizados para codificar voz utiliza uma frequência de amostragem de 8.000 Hz e um filtro passa-faixa de 30 a 3.400 Hz, semelhante ao utilizado na telefonia convencional. Outros valores de frequência de amostragem comumente utilizados são: 11.025, 16.000, 22.050, 24.000, 32.000, 44.100 e 48.000 Hz. Normalmente, esses *codecs* trabalham com pacotes de tamanhos fixos com taxas de 20 a 50 pacotes por segundo e *bit rates* constantes (SCHULZRINNE, 1996).

Os *codecs* de áudio podem ser baseados em amostras ou em *frames*. Em ambos os tipos de *codecs*, um certo número de amostras é agrupado, podendo a seguir ser aplicado algum algoritmo de compressão ou não, gerando um pacote de áudio a ser transportado pelo RTP. O *timestamp* RTP do pacote de áudio gerado corresponde ao *timestamp* da primeira amostra do pacote (SCHULZRINNE et al., 1996).

2.1.1.1 Os *codecs* de áudio baseados em amostras

Nos *codecs* baseados em amostras, cada amostra é representada por um número inteiro de *bits*, sendo que esse número de *bits* pode ser variável, porém, deve-se garantir um alinhamento de 8 *bits* para cada pacote de áudio gerado (SCHULZRINNE, 1996).

Definindo-se o atraso (A) desejado para o *codec* e a frequência de amostragem (f_A), determina-se o número de amostras por pacote (N_A). Quanto maior o número de

³ Verificado pelo autor em laboratório com o *codec* G.723.1.

amostras em um pacote, maior o atraso inserido. Dado um número de amostras por pacote, fica definido o número de pacotes por segundo (PPS), segundo a Equação (1). Dependendo do fator de compressão utilizado o pacote será maior ou menor, isto é, o número de *bits* utilizado para representar cada amostra será maior ou menor. Pode-se calcular o número médio de *bits* por amostra (BPA), segundo a Equação (2), dividindo o tamanho do pacote em *bits* (T_P) pelo número de amostras (N_A). Multiplicando-se o tamanho do pacote (T_P) pelo número de pacotes por segundo (PPS), tem-se o *bit rate* do *codec* de áudio baseado em amostras (BR_{CAA}). As Equações (1), (2) e (3) servem para calcular o *bit rate* de um *codec* de áudio baseado em amostras.

$$A = \frac{N_A}{f_A} = \frac{1}{PPS} \quad (1)$$

$$T_P = N_A \cdot BPA \quad (2)$$

$$BR_{CAA} = PPS \cdot T_P \quad (3)$$

Adicionando-se a cada pacote gerado os cabeçalhos RTP (C_{RTP}), UDP (C_{UDP}), IP (C_{IP}) e os *bytes* da camada de enlace (C_{ENLACE}), tem-se o *bit rate* do canal (BR_{CANAL}), como mostra a Equação (4).

$$BR_{CANAL} = PPS \cdot (T_P + 8 \cdot (C_{RTP} + C_{UDP} + C_{IP} + C_{ENLACE})) \quad (4)$$

Um *codec* hipotético baseado em amostras utilizando uma frequência de amostragem de 8 kHz, 8 *bits* por amostra e gerando um pacote a cada 25 ms, produz 40 pacotes por segundo (pps) e cada pacote transporta 200 amostras. Sem compressão, essas 200 amostras ocupariam 200 B. Nesse caso, o *bit rate* do *codec* seria 64 kbps. Se o *codec* possuir um fator de compressão de 10 vezes, cada amostra seria representada em média, por 0,8 *bits*, o *codec* passaria a ser de 6,4 kbps e cada pacote carregaria apenas 20 B de dados. Considerando-se 12 B de cabeçalho RTP, 8 B de cabeçalho UDP, 20 B de cabeçalho IP e 18 B ocupados na camada de enlace (no caso de uma rede Ethernet), cada pacote de áudio comprimido ocuparia 78 B, resultando em um *bit rate* do canal de 24,960 kbps, um valor 3,9 vezes maior que o *bit rate* do *codec*.

Em cada quadro transmitido, há 20 B de áudio codificado e 58 B de cabeçalhos RTP, UDP, IP e Ethernet.

2.1.1.2 Os *codecs* de áudio baseados em *frames*

Nos *codecs* baseados em *frames*, um bloco de amostras de tamanho fixo é comprimido em um bloco geralmente de tamanho fixo também. Um ou mais *frames* podem ser encapsulados em um mesmo pacote RTP, mas quanto maior o número de *frames* em um pacote RTP, maior o atraso inserido, porque mais tempo precisa ser esperado antes de se gerar e transmitir o pacote (SCHULZRINNE, 1996).

Um *codec* hipotético semelhante ao exemplo do *codec* baseado em amostras, trabalhando com *frames* de 20 ms e produzindo blocos de 20 B, transmitindo um bloco desses por pacote, apresentaria o mesmo comportamento do *codec* do exemplo anterior. Se ele transmitisse um número N_B de blocos por pacote, o pacote seria maior e o *overhead* diminuiria, mas o atraso entre pacotes aumentaria N_B vezes.

Pode-se calcular o *bit rate* de um *codec* baseado em *frames* de forma análoga ao cálculo do *bit rate* de um *codec* baseado em amostras, necessitando-se apenas do tamanho do pacote e da taxa de pacotes por segundo.

2.1.1.3 Qualidade subjetiva de um *codec* de áudio

A qualidade subjetiva de um *codec* de áudio pode ser definida pela fidelidade com relação ao áudio original, pela inteligibilidade do áudio codificado e pela facilidade de reconhecimento e identificação do locutor.

Uma forma padronizada de avaliação da qualidade subjetiva do áudio codificado foi concretizada na recomendação P.800 – *Methods for Subjective Determination of Transmission Quality* (ITU-T, 1996a) e (RADCOM, 1999), que emprega pontuação média por opinião, *Mean Opinion Score* (MOS). Amostras de voz gravadas pré-selecionadas de acordo com as recomendações da série P.50 – *Test Signals* (ITU-T, 1998c) são reproduzidas para homens e mulheres sob condições controladas, que atribuem notas de 1 (pior) a 5 (excelente) para cada critério estabelecido. Um *codec* de voz com MOS igual a 4 possui uma qualidade subjetiva comparável à de uma

chamada de longa distância em telefonia. Os critérios adotados para se dar notas para a qualidade de voz são apresentados na Tabela 2.1 abaixo (ITU-T, 1996a) e (RADCOM, 1999):

Tabela 2.1 – Critérios utilizados para MOS em avaliações de áudio

Pontuação	Tipo de teste			
	Escala de opinião para teste de conversação (MOS _C)	Escala de opinião para teste auditivo (MOS)	Escala de esforço para a audição (MOS _{LE})	Escala de preferência de volume (MOS _{LP})
5	Excelente	Excelente	Relaxamento completo possível, não requer esforço.	Muito mais alto que o preferível.
4	Bom	Bom	É necessário prestar atenção, mas não precisa de um esforço considerável para a compreensão do significado.	Mais alto que o preferível.
3	Razoável	Razoável	É necessário um esforço moderado.	Preferível
2	Pobre	Pobre	É necessário um esforço moderado.	Mais baixo que o preferível.
1	Ruim	Ruim	Não é possível compreender o significado.	Muito mais baixo que o preferível.

Através de modelos matemáticos dos aparelhos auditivo e fonador humano foram criados métodos mais objetivos e reproduzíveis para se avaliar a qualidade subjetiva do áudio codificado, de forma a substituir a recomendação P.800 (ITU-T, 1996a).

Dentre esses métodos, destacam-se a *Perceptual Analysis/Masurement System* (PAMS) (PSYTECHNICS, 2004) e as recomendações P.861 – *Objective Quality Measurement of Telephone-Band (300-3.400 Hz) Speech Codecs/Perceptual Speech Quality Measurement (PSQM)* (ITU-T, 1998b) e a P.862 – *Perceptual Evaluation of Speech Quality (PESQ), an Objective Method for End-to-End Speech Quality Assessment of Narrowband Telephone Networks and Speech Codecs* (ITU-T, 2001a).

2.1.1.4 Comparação entre os *codecs* de áudio

A escolha do *codec* de áudio é realizada de acordo com o cenário de utilização do mesmo e os principais critérios considerados são: a banda ocupada pela *codec*, seu atraso e a sua qualidade subjetiva. Cada cenário oferece bandas e atrasos diferentes. Exemplos de cenários são uma rede local, uma comunicação por satélite e acesso à Internet por meio de uma conexão discada.

Dois *codecs* podem ter *bit rates* iguais, mas um possuir uma qualidade subjetiva melhor que o outro. Em um cenário onde banda não é um fator crítico, o *codec* de melhor qualidade subjetiva deve ser escolhido. Se ambos possuírem qualidades subjetivas próximas, pode-se escolher o *codec* de menor atraso.

A Tabela 2.2, extraída de informações contidas em (ADAPTATIVE, 2002); (KIVILUOTO, 2002); (OPENH323, 2002); (PACKETIZER, 2002); (RADCOM, 1999) e (VOCAL, 2002), compara alguns *codecs* de voz utilizados.

O PCM 8 kHz mono não utiliza nenhum mecanismo de compressão além das leis de compansão A ou μ . O PCM apenas quantiza e codifica cada amostra. A quantidade de bits utilizada na codificação pode ser 6, 7 ou 8, resultando em taxas de transmissão de 48, 56 e 64 kbps, respectivamente. Sendo assim, as perdas no PCM são devidas à quantização, à baixa frequência de amostragem e ao uso de filtros.

O atraso algorítmico *codecs* de áudio baseados em amostras e em *frames* depende de quantas amostras ou *frames* há em cada pacote de áudio, respectivamente. Na Tabela 2.2, há apenas um *frame* por pacote de áudio e o atraso está sendo considerado somente em um lado da comunicação.

Os *codecs* de voz possuem baixo *bit rate*, de 2,4 kbps a 64 kbps, mas o *overhead* introduzido pelos protocolos RTP, UDP, IP e pela camada de enlace elevam muito o *bit rate* do canal.

Tabela 2.2 – Comparação entre alguns *codecs* utilizados em conferências

<i>Codec</i>	Algoritmo ⁴ (amostra/frame)	Bit rate (kbps)	Atraso algorítmico ⁵ (ms)	MOS	Complexidade (MIPS)
G.711	PCM (amostra)	48, 56 e 64	0,125 por amostra	4,3	0,01
G.722	SB-ADPCM (amostra)	48, 56 e 64	< 2	4,1	5
G.723.1	MP-MLQ/ACELP (frame)	5,3 e 6,4	30 ⁶	3,7 e 4,0	11
G.726	ADPCM (amostra)	16, 24, 32 , 40	0,125 por amostra	4,1	2
G.727	EADPCM (amostra)	16, 24, 32 , 40	0,125 por amostra	4,1	2
G.728	LD-CELP (frame)	16	2,5	3,4	30
G.729	CS-ACELP (frame)	8	10 ⁷	4,0	20
G.729 anexo A	CS-ACELP (frame)	8	15	3,8	11
GSM ⁸ 06.10	RPE-LTP (frame)	13,2	20	3,5 a 3,9	6

2.1.2 O protocolo de transporte de tempo real em redes IP

O RTP (SCHULZRINNE et al., 1996) é um protocolo desenvolvido pela IETF (IETF, 2002) para fornecer mecanismos de transporte fim-a-fim próprios para aplicações transmitindo áudio, vídeo ou outros tipos de dados que precisem de tratamento em tempo real, utilizando serviços de distribuição de pacotes *multicast* ou *unicast*. O RTP não realiza reserva de banda nem assegura a qualidade de serviço. O

⁴ *Pulse Code Modulation* (PCM) (ITU-T, 1988a), *Adaptative Differential Pulse Code Modulation* (ADPCM) (ITU-T, 1990a), *Embedded ADPCM* (EADPCM) (ITU-T, 1990b), *Sub-Band ADPCM* (SB-ADPCM) (ITU-T, 1988b), *Multipulse Maximum Likelihood Quantization/Algebraic-Code-Excited Linear-Prediction* (MP-MLQ/ACELP) (ITU-T, 1996b), *Low-Delay Code-Excited Linear-Prediction* (LD-CELP) (ITU-T, 1992), *Conjugate-Structure Algebraic CELP* (CS-ACELP) (ITU-T, 1996c), *Regular Pulse Excited Long-Term Prediction* (RPE-LTP) (ETSI, 1998).

⁵ Schulzrinne et al. (1996) define que é necessário pelo menos o recebimento de dois pacotes para se validar uma sequência de pacotes RTP. Portanto, em média, o atraso total fim-a-fim acaba sendo o dobro do atraso algorítmico.

⁶ Nas estações origem e destino há 30 ms de atraso do algoritmo do *codec* e na estação destino, há mais 7,5 ms de *jitter buffer* totalizando pelo menos 67,5 ms de atraso fim-a-fim (ITU-T, 1996b).

⁷ Em cada estação há 10 ms de atraso do algoritmo do *codec* e na estação destino, há mais 5,0 ms de *jitter buffer* totalizando pelo menos 25 ms de atraso fim-a-fim (ITU-T, 1996c).

⁸ *Group Spéciale Mobile* ou *Global System for Mobile Communications*.

RTCP (SCHULZRINNE et al., 1996) é o protocolo de controle associado ao RTP e permite o monitoramento de estatísticas de transmissão e recepção, identificação dos pontos participantes na conferência e a sinalização de abandono de conferência.

A RFC 1889 – *Real-Time Transport Protocol* (SCHULZRINNE et al., 1996) especifica o RTP e o RTCP, devendo ambos ser preferencialmente transportados sobre UDP, via IP *multicast*, conferindo maior escalabilidade às conferências, contudo, o mecanismo de distribuição *unicast* também pode ser utilizado.

A RFC 1889 define que o RTP e o RTCP devem utilizar portas UDP diferentes e consecutivas para recepção e envio de pacotes, sendo a porta UDP do RTP um número par. A RFC 1890 – *RTP Profile for Audio and Video Conferences with Minimal Control* (SCHULZRINNE, 1996) define as portas UDP número 5004 e 5005, para a recepção de pacotes RTP e RTCP, respectivamente. Nada impede, porém, que outros valores de portas sejam utilizados.

Uma sessão RTP é definida como sendo a associação entre os participantes de uma conferência que se comunicam utilizando o RTP. Para cada participante, a sessão RTP é definida pelo par de endereços de destino (de rede e de transporte) do RTP e do RTCP. Cada mídia é carregada em sessões RTP diferentes, isto é, o áudio é carregado em uma sessão e o vídeo em outra, sendo reservadas portas UDP de destino diferentes para o RTP e o RTCP de cada mídia. Em conferências sobre *multicast*, os endereços destino do RTP e do RTCP são comuns a todos os participantes. Portanto, mídias diferentes não podem ser multiplexadas em uma mesma porta UDP de destino, mas pacotes de uma mesma mídia originados por participantes diferentes podem.

2.1.3 Mecanismos de distribuição de pacotes em redes IP

Há três formas de se distribuir pacotes em uma rede IP: via *unicast*, *multicast* ou *broadcast*.

2.1.3.1 IP Unicast

No *unicast*, um pacote é gerado para um único destinatário na rede, identificado por um endereço IP de *host*, isto é, um endereço IP pertencente à faixa de endereços 0.0.0.0 a 223.255.255.255, desde que não seja um endereço de *broadcast* ou de uma rede qualquer. Os protocolos TCP e UDP podem utilizar pacotes do tipo *unicast*.

2.1.3.2 IP Broadcast

O *broadcast* serve para endereçar todos os sistemas dentro de uma rede, devendo ser usado somente em casos especiais, como, por exemplo, para se descobrir o endereço MAC de uma estação, cujo endereço IP é conhecido. Seu uso indiscriminado pode levar ao congestionamento da rede, causando degradação no desempenho dela.

2.1.3.3 IP Multicast

A idéia por trás do *multicast* é a de se transmitir um único pacote que será recebido por muitos pontos dentro ou fora da sub-rede considerada, mas não por todos. Os endereços do tipo *multicast* pertencem à faixa de endereços 224.0.0.0 a 239.255.255.255. A faixa de endereços utilizada para o IP *multicast* é identificada pelos 4 *bits* mais significativos do endereço IP: 1110, em binário. Grupos de estações são identificados pelos 28 *bits* menos significativos. A RFC 1112 – *Host Extensions for IP Multicasting* (DEERING, 1989) define que um endereço IP *multicast* seja mapeado em um endereço MAC destino da seguinte forma: os 23 *bits* menos significativos do endereço IP *multicast* são sobrescritos aos 23 *bits* menos significativos do endereço MAC 01-00-5E-00-00-00, em hexadecimal. Por se estar desconsiderando os 5 *bits* mais significativos que identificam o grupo de *host*, pode haver colisão no mapeamento de endereços IP *multicast* em endereços MAC destino.

Quando uma estação deseja receber pacotes destinados a um certo endereço *multicast*, isto é, quando ela deseja fazer parte de um grupo *multicast*, ela pede para o seu *gateway* transmitir os pacotes que ele receber com o endereço *multicast* em questão para o seu segmento de rede. Os roteadores propagam entre si informações e solicitações de adesão a grupos *multicast*, utilizando protocolos como o IGMPv3, definido na RFC 3376 – *Internet Group Management Protocol, Version 3* (FENNER, 2002).

O endereço 224.0.0.2, por exemplo, foi definido para endereçar todos os roteadores dentro de uma sub-rede (IANA, 2002).

Somente o UDP pode ser transportado sobre pacotes do tipo *multicast*, porque os mecanismos de confiabilidade do TCP não podem ser aplicados diretamente.

Há algumas tentativas de se criar um protocolo confiável de transporte para ser utilizado sobre *multicast*, como descrito em (ARMSTRONG, FREIER, MARZULLO, 1992); (BRAUDES, ZABELE, 1993); (MANKIN et al., 1998); (HANDLEY, 2000); (WHETTEN et al., 2001) e (KERMODE, VICISANO, 2002), mas nada ainda utilizado largamente. Esses mecanismos propostos utilizam pacotes de confirmação (ACKs) negativos ou ACKs agregados por subgrupos para obter confiabilidade na distribuição de pacotes.

2.2 Conferências multimídia sobre redes IP

A terminologia sobre conferências empregada neste trabalho foi adaptada de (ITU-T, 2003b), Rosenberg et al. (2002) e Malkin (1996).

Um conjunto de transmissores e receptores multimídia trocando canais de mídia (áudio, vídeo e dados) e de controle em tempo real compõe uma sessão multimídia. Uma conferência multimídia virtual é um exemplo de uma sessão multimídia. Cada canal de mídia e de controle é transportado por canais lógicos diferentes. Os canais de áudio e vídeo são normalmente transportados sobre o RTP (SCHULZRINNE et al., 1996), que por sua vez utiliza os serviços da camada de transporte da arquitetura TCP/IP.

O controle de uma conferência pode ser decomposto em controle de sessão e controle de posse da palavra, como proposto em (QIU, KUHNS, COX, 2002). Controle de sessão envolve, basicamente: o estabelecimento, sinalização e gerenciamento da sessão; autenticação, admissão, localização de usuários, bem como a descoberta das suas capacidades multimídia de recepção e transmissão. Exemplos de protocolos de controle de sessão são o *Session Initiation Protocol* (SIP) (ROSENBERG et al., 2002) da IETF (IETF, 2002) e a recomendação H.323 (ITU-T, 2003b) da *International Telecommunications Union Telecommunication Standardization Sector* (ITU-T) (ITU-T, 2003a).

As conferências podem ser classificadas primariamente entre conferências ponto-a-ponto e conferências multiponto. A conferência ponto-a-ponto é a forma mais simples de conferência possível, com um ponto transmitindo diretamente para o outro. As seguintes entidades podem estar presentes em uma conferência multiponto:

- **Terminal:** Um terminal é um sistema capaz de estabelecer comunicações multimídia em tempo real sobre uma rede IP. O suporte a áudio é obrigatório, enquanto o suporte a vídeo e a dados é opcional. O terminal oferece uma interface homem-máquina para os usuários do sistema.
- **Controlador multiponto (MC):** O controlador multiponto é obrigatório em uma conferência multiponto, porque é a entidade responsável pelo tratamento dos canais de controle dos participantes da conferência. O controlador multiponto pode estar presente em um terminal ou em uma unidade de controle multiponto.
- **Processador multiponto (MP):** O processador multiponto é a entidade responsável por distribuir o canal de mídia recebido de um participante para os demais participantes na conferência. Transcodificação e mixagem de mídia são opcionais. O processador multiponto pode estar presente em um terminal ou em uma unidade de controle multiponto.
- **Unidade de controle multiponto (MCU):** A unidade de controle multiponto é composta por pelo menos um controlador multiponto e zero ou mais processadores multiponto, para tratar diferentes tipos de mídia.

As conferências multiponto podem ser classificadas de acordo com a forma na qual seus canais são distribuídos entre os seus participantes (ITU-T, 2003b):

- **Conferências multiponto descentralizadas:** Nesse tipo de conferência, tanto os pacotes de mídia como os de controle são transportados sobre IP *multicast*. O IP *unicast* pode ser utilizado no lugar do IP *multicast*, quando este último não puder ser utilizado, em uma configuração chamada “*full-mesh*”⁹, extremamente ineficiente sob o ponto de vista de utilização de banda da rede.
- **Conferências multiponto centralizadas:** Nesse tipo de conferência, há um elemento centralizador, a unidade de controle multiponto, responsável por estabelecer conexões ponto-a-ponto com cada participante da conferência e transmitir os pacotes de mídia recebidos para os demais participantes. Tanto os pacotes de mídia como os de controle são transportados sobre IP *unicast*.
- **Conferência multiponto mista:** Conferência na qual alguns participantes comportam-se como em uma conferência centralizada, enquanto outros participantes agem como se estivessem em uma conferência descentralizada. A conexão entre a parte centralizada e a parte descentralizada da conferência pode ser feita por uma unidade de controle multiponto. Os participantes não precisam ter a consciência da natureza mista da conferência.
- **Conferência híbrida:** Conferência na qual alguns canais são transportados via IP *multicast* e outros canais via IP *unicast*. A diferença entre a conferência mista e a conferência híbrida, é que na híbrida, um mesmo ponto transmite tanto via IP *multicast* quanto via IP *unicast*, enquanto que na mista, dois ou mais pontos transmitem unicamente via *multicast*, enquanto os outros transmitem unicamente via IP *unicast* (com exceção do elemento que conecta a conferência centralizada à conferência descentralizada, que transmite de ambas as formas). Em uma conferência híbrida, por exemplo, os canais de áudio e vídeo poderiam ser

⁹ Na configuração *full-mesh*, cada ponto transmite um pacote IP *unicast* para cada um dos demais pontos.

distribuídos via IP *multicast* e os canais de controle, via IP *unicast*, para um ponto encarregado do gerenciamento da conferência.

Embora o IP *multicast* consuma menos banda do que o IP *unicast* em conferências multiponto, nem sempre é possível utilizá-lo, porque tanto a infra-estrutura de rede quanto o sistema de conferência multimídia (*hardware* e *software*) precisam suportar tráfego *multicast*. Além disso, conferências com abrangência global precisam de endereços IP *multicast* globais, que devem ser requisitados junto à *Internet Assigned Number Authority* (IANA) (IANA, 2003) e (IANA, 2000). Independentemente da conferência utilizar IP *unicast* ou *multicast*, se o número de transmissores simultâneos não for restringido através do uso de mecanismos de controle de posse da palavra, por exemplo, a banda consumida passa rapidamente a ser o principal fator limitante da escalabilidade da conferência.

2.2.1 Unidade de controle multiponto e conferências centralizadas

A unidade de controle multiponto é responsável por redistribuir os pacotes recebidos de cada participante para os demais em uma conferência centralizada. A unidade de controle multiponto estabelece conferências ponto-a-ponto com cada participante. Para isso, ela deve suportar os protocolos de estabelecimento e sinalização de conferências sendo utilizados.

A Figura 2.3 ilustra uma conferência multiponto centralizada com uma unidade de controle multiponto atendendo a seis participantes remotos pela Internet, utilizando IP *unicast*. Um dos participantes está transmitindo seus pacotes RTP para a unidade de controle multiponto, que encaminha os pacotes RTP para os outros cinco participantes.

Figura 2.3 – Ilustração de uma conferência multiponto centralizada utilizando IP *unicast* com uma unidade de controle multiponto e seis participantes.

A unidade de controle multiponto não gera novos pacotes RTP (a menos que realize mixagem ou transcodificação de *streams*), apenas altera e encaminha os pacotes RTP recebidos de cada participante para os demais, mas ela gera seus próprios pacotes RTCP. Cada participante inicia sua transmissão com um número aleatório de sequência e de *timestamp* no cabeçalho RTP (SCHULZRINNE et al., 1996). Para não confundir os receptores, a unidade de controle multiponto pode gerar seu próprio número de sequência e *timestamp* para cada participante, visto que eles podem receber um número diferente de pacotes (o participante transmitindo não recebe seu próprio áudio de volta¹⁰).

Os pacotes RTCP precisam ser gerados pela unidade de controle multiponto e transmitidos para cada ponto conectado a ela.

¹⁰ Quando a unidade de controle multiponto possui a função de *loop back*, o participante transmitindo recebe o seu próprio áudio de volta. Quando não há *loop back*, utiliza-se menos banda.

Desde que a unidade de controle multiponto não realize transcodificação ou mixagem, ela é independente de *codec*, isto é, não importa qual *codec* o RTP está transportando, porque ela só precisa das informações do RTP e do RTCP. Para uma unidade de controle multiponto independente de *codec*, o *stream* de mídia criptografado é como um *stream* de mídia qualquer.

Quando todos os participantes da conferência utilizam o mesmo *codec*, não há a necessidade de se realizar transcodificação na unidade de controle multiponto, simplificando seu projeto e funcionamento. Como cada participante estabelece uma conexão ponto-a-ponto com a unidade de controle multiponto, ela pode exigir o uso de um determinado *codec* na fase de negociação da abertura do canal de áudio, forçando todos os participantes da conferência a usarem o *codec* definido por ela. A negociação do *codec* só é necessária, quando não há um *codec* pré-definido para a conferência.

A mixagem dos sinais recebidos pela unidade de controle multiponto é opcional e deve ser evitada, porque é uma operação bastante custosa computacionalmente, dependente de *codec* e por aumentar o atraso fim-a-fim. Os pacotes recebidos precisariam ser decodificados, somados linearmente e o áudio resultante precisaria ser codificado e transmitido. O número de canais de áudio a ser mixado seria um fator limitante da escalabilidade da unidade de controle multiponto. Se a unidade de controle multiponto realizar mixagem, deve haver uma ponderação no ganho dos sinais de áudio recebidos, para que o ruído ambiente não mascare o áudio da pessoa falando.

Em uma conferência com a presença de um moderador, os terminais dos participantes enxergam a unidade de controle multiponto como sendo o próprio moderador, porque ela é a origem e destino dos pacotes.

A seguir são realizadas análises sobre o impacto da banda da rede nos pontos da conferência, na unidade de controle multiponto e na rede como um todo. Para simplificar a análise em cada caso, somente será considerada a transmissão do canal de áudio (pacotes RTP e RTCP), utilizando *bit rate* constante. A unidade de controle multiponto não retransmite o canal de áudio para o participante que o originou.

Antes, porém, deve ser analisada a conferência ponto-a-ponto, por ser a forma mais simples de conferência possível. Sua análise é importante, porque a conferência multiponto centralizada assemelha-se à sobreposição de várias conferências ponto-a-ponto. Em uma conferência ponto-a-ponto, cada ponto transmitirá um canal RTP, com *bit rate* constante¹¹ A e um canal RTCP, com *bit rate* constante¹² B , mostrado na Equação (5) e a taxa de transmissão (TX_{pp}) de um ponto será P , segundo a Equação (6). A taxa de recepção (RX_{pp}) também será P , pela Equação (7). Como a RFC 1889 (SCHULZRINNE et al., 1996) define que a banda ocupada pela transmissão de pacotes RTCP seja uma fração da banda ocupada pela transmissão de pacotes RTP (normalmente inferior a 5%), temos que $A \gg B$.

$$P = A + B, A \gg B \quad (5)$$

$$TX_{pp} = P \quad (6)$$

$$RX_{pp} = P \quad (7)$$

2.2.1.1 Utilização de banda nos pontos da conferência multiponto centralizada

Para os participantes da conferência multiponto centralizada, tudo se passa como se a conferência fosse ponto-a-ponto. Dessa forma, a taxa de transmissão (TX_{MPCU})¹³ e de recepção (RX_{MPCU}) de pacotes são iguais às taxas de um participante em uma conferência ponto-a-ponto, como mostram as Equações (8) e (9).

$$TX_{MPCU} = P \quad (8)$$

$$RX_{MPCU} = P \quad (9)$$

¹¹ Pelas características dos *codecs* de áudio apresentados anteriormente, o *bit rate* do canal de áudio (canal RTP) será considerado como sendo constante.

¹² Para simplificar o modelamento de um participante em uma conferência, o *bit rate* do canal RTCP será considerado constante.

¹³ O acrônimo MPCU vem de conferência **m**ultiponto **c**entralizada utilizando IP **u**nicast.

A taxa de transmissão de pacotes RTCP deveria decair com o aumento do número de participantes (N), conforme (SCHULZRINNE et al., 1996), mas se o *software* do usuário não for informado da natureza multiponto da conferência, ele continuará transmitindo com a mesma taxa, independentemente do número de participantes na conferência. Se um mecanismo para restringir a banda dos pacotes RTCP for implementado, tanto a taxa de transmissão (TX'_{MPCU}) quanto a taxa de recepção (RX'_{MPCU}) de pacotes RTCP diminuiria, como mostram as Equações (10)¹⁴ e (11) abaixo. O aumento do intervalo de tempo de recebimento de pacotes RTCP prejudica a resolução das estatísticas, mas a banda de transmissão de pacotes RTCP da unidade de controle multiponto permaneceria fixa.

$$TX'_{MPCU} = A + \frac{B}{N} \leq P, N \geq 2 \quad (10)$$

$$RX'_{MPCU} = A + \frac{B}{N} \leq P, N \geq 2 \quad (11)$$

Para as demais análises feitas, não será considerado o decaimento da taxa de transmissão de pacotes RTCP por participante, portanto, serão consideradas as Equações (8) e (9) como as equações que regem a recepção e a transmissão de um participante em uma conferência multiponto.

2.2.1.2 Utilização de banda na unidade de controle multiponto

Pela própria natureza centralizadora da unidade de controle multiponto, ela receberá os pacotes de todos os participantes da conferência e terá de repassá-los aos demais, devendo, portanto, ser acessível através de um enlace com banda larga.

As bandas necessárias para transmissão (TX_{MCU}) e recepção (RX_{MCU}) de pacotes pela unidade de controle multiponto em uma conferência com N participantes são

¹⁴ Poderia se utilizar outro cálculo para diminuir a taxa de transmissão de pacotes RTCP.

mostradas nas Equações (12) e (13), considerando as Equações (10) e (11) e sem considerar o canal de *loop back*.

$$TX_{MCU} = A \cdot N \cdot (N - 1) + B \cdot N < N^2 \cdot P, N \geq 2 \quad (12)$$

$$RX_{MCU} = A \cdot N + B \cdot N = N \cdot P, N \geq 2 \quad (13)$$

Pode-se reduzir a taxa de pacotes recebidos e transmitidos pela unidade de controle multiponto com um mecanismo de controle de posse da palavra que impeça a transmissão de pacotes RTP dos participantes sem a posse da palavra. Em outras palavras, somente o participante com a posse da palavra transmitirá pacotes RTP. Nesse caso, as taxas de recepção (RX'_{MCU}) e de transmissão (TX'_{MCU}) de pacotes da unidade de controle multiponto obedecem às Equações (14) e (15), respectivamente.

$$TX'_{MCU} = A \cdot (N - 1) + B \cdot N \approx (N - 1) \cdot P, N \geq 2 \quad (14)$$

$$RX'_{MCU} = A + B \cdot N > P \quad (15)$$

Nessa situação, a unidade de controle multiponto possui bandas assimétricas em cada sentido, sendo que a banda de *upstream* é a maior. Essa assimetria é inversa à da tecnologia *Asymmetric Digital Subscriber Line* (ADSL), que proporciona uma banda de *downstream* maior do que a de *upstream*, portanto a tecnologia ADSL não é a mais indicada para servir a uma unidade de controle multiponto.

Pode-se perceber que tanto a banda na unidade de controle multiponto quanto o *codec* utilizado são fatores que podem limitar o número de participantes em uma conferência. Um *codec* que gera pacotes a cada 20 ms é mais impactante para a unidade de controle multiponto, do que um *codec* que gera pacotes a cada 40 ms, porque o tempo disponível para processamento e encaminhamento de pacotes para todos os participantes cai pela metade.

2.2.1.3 Utilização de banda na rede da conferência multiponto centralizada

Como todos os pacotes serão encaminhados para a unidade de controle multiponto e dela para os demais participantes, a banda na rede (RD_{MPCU}) será a somatória da banda transmitida pelos participantes, mais a banda de transmissão da unidade de controle multiponto, como pode ser observado na Equação (16):

$$\begin{aligned} RD_{MPCU} &= (A \cdot N \cdot (N - 1) + B \cdot N) + (A \cdot N + B \cdot N) \\ &= A \cdot N^2 + 2 \cdot B \cdot N < N^2 \cdot P, N \geq 2 \end{aligned} \quad (16)$$

Se somente um participante transmitir por vez, a banda na rede (RD'_{MPCU}) fica sendo a soma das bandas de transmissão da unidade de controle multiponto, do canal do falador ativo e dos canais RTCP transmitidos por todos os participantes, mostrada na Equação (17) abaixo.

$$\begin{aligned} RD'_{MPCU} &= (A \cdot (N - 1) + B \cdot N) + (A) + (B \cdot N) \\ &= A \cdot N + 2 \cdot B \cdot N \approx N \cdot P, N > 2 \end{aligned} \quad (17)$$

Nessa situação, a banda na rede passa a crescer de forma linear com o número de participantes.

2.2.2 Criação e controle de conferências

Quando uma conferência não possui um protocolo específico de criação e controle, ela é chamada de conferência fracamente controlada. Um exemplo de uma conferência fracamente controlada seria uma conferência onde as únicas informações necessárias para se tomar parte nela, seria o seu horário, seu endereço IP *multicast* e as portas UDP utilizadas para o RTP e para o RTCP.

Os principais protocolos para estabelecimento e gerenciamento de conferências são o SIP (ROSENBERG et al., 2002) da IETF (IETF, 2002) e o definido na recomendação H.323 (ITU-T, 2003b) da ITU-T (ITU-T, 2003a). Ambos utilizam o RTP e o RTCP para os *streams* de mídia.

O SIP é um protocolo da camada de aplicação da arquitetura TCP/IP, desenvolvido pelo grupo de trabalho *Multiparty Multimedia Session Control* (MMUSIC) (IETFAWG, 2002) da IETF especialmente para estabelecer, manipular e desfazer sessões multimídia. O conceito do SIP é extremamente semelhante ao do *Hypertext Transfer Protocol* (HTTP) (FIELDING et al., 1999), possuindo requisições e respostas em formato texto, com códigos de respostas e uso de localizadores/indicadores uniformes de recurso (*Uniform Resource Locators – URLs/Uniform Resource Indicators – URIs*) (BERNERS-LEE et al., 1998).

A primeira versão do SIP foi publicada em 1999, como a RFC 2543 – SIP: *Session Initiation Protocol* (HANDLEY et al., 1999). A segunda versão do SIP foi publicada em 2002, sob o mesmo título, através da RFC 3261 (ROSENBERG et al., 2002). O SIP é complementado ainda por outras RFCs.

A recomendação H.323 foi publicada primeiramente em 1996 sob o título “*Visual Telephone Systems and Equipment for Local Area Networks which provide a non-guaranteed Quality of Service*” (ITU-T, 1996d). A versão atual, a quinta, publicada em 2003, é intitulada “*Packet-Based Multimedia Communications Systems*” (ITU-T, 2003b).

A recomendação H.323 define os requisitos técnicos e as entidades que oferecem comunicação multimídia sobre redes de pacotes sem qualidade de serviço garantida. A H.323 é independente das camadas de enlace e de rede e trata também da interoperabilidade com outros tipos de rede, como a Rede Digital de Serviços Integrados (RDSI)¹⁵ e a rede pública de telefonia.

A H.323 oferece mais funcionalidades que o SIP e suporta aplicações colaborativas como *whiteboarding* e compartilhamento de *desktop*. A utilização da *Abstract Syntax Notation One* (ASN.1) (ITU-T, 2002b) com *Packed Encoding Rules* (PER) (ITU-T, 2002c) confere ao protocolo H.323 uma representação muito eficiente de seus

¹⁵ Em inglês, *Integrated Services Digital Network* (ISDN).

pacotes, mas a complexidade adicionada à codificação e decodificação dos pacotes é uma grande desvantagem. Outra desvantagem é o curto período de vida de cada versão da H.323, dificultando o desenvolvimento de aplicações compatíveis.

Já o SIP é mais leve e a sua semelhança com o HTTP (FIELDING et al., 1999) facilitam o desenvolvimento de aplicações, bem como a codificação e a decodificação de seus pacotes. Entretanto, o *overhead* de comunicação é maior, por utilizar uma representação em modo texto ao invés de uma representação binária, como no H.323. O fato do SIP não ser tão poderoso quanto o H.323 não é um problema para a principal aplicação para o qual ele é utilizado, a telefonia IP como substituta da telefonia convencional.

Tanto o SIP quanto o H.323 possuem grande aceitação na indústria. O H.323 está presente desde 1996 e já está na sua quarta versão, enquanto a primeira especificação do SIP só apareceu em 1999 e a segunda, em 2002. Vários equipamentos oferecem suporte a ambos, mas os clientes de conferência utilizam um ou outro. Há alguns *gateways* SIP-H.323 disponíveis no mercado. O SIP vem obtendo espaço na telefonia IP, enquanto o H.323 é o preferido para videoconferências com suporte a dados, já que o SIP não endereça diretamente essa questão.

2.2.3 Mecanismos para controle de transmissão de pacotes de voz

O pior cenário possível em termos de banda consumida em uma conferência multiponto ocorre quando todos os participantes transmitem pacotes RTP simultaneamente, independentemente da conferência ser descentralizada ou centralizada. O número de *streams* de áudio recebido por um participante seria igual ao número de participantes na conferência menos um. Para resolver essa situação, algum mecanismo de controle de transmissão de pacotes RTP precisa ser implementando nos terminais dos usuários e também na unidade de controle multiponto, no caso da conferência multiponto centralizada. Os dois mecanismos mais comuns são:

- Detecção de silêncio;
- Controle de posse de palavra (*floor control*).

Para economizar banda, sistemas de conferência que não suportam detecção de silêncio ou controle de posse da palavra geralmente requerem que o usuário deixe o seu microfone mudo, enquanto ele não quiser falar nada, ou então, que mantenham pressionada uma tecla ou o *mouse* enquanto falam, simulando o mecanismo “*push to talk*” normalmente encontrado em *walkie-talkies* e interfones. Mecanismos “*push to talk*” costumam ser bastante desconfortáveis em conferências de longa duração, enquanto que o pedido para se deixar o microfone mudo nem sempre é respeitado por todos os participantes.

2.2.4 Detecção de silêncio

O transmissor pode determinar se o sinal de áudio deve ser ou não encaminhado pela potência do sinal de áudio capturado, de acordo com um certo modelo matemático, tentando-se avaliar se o participante está em silêncio ou não (*Voice Activity Detection* – VAD) (BRANDY, 1965) e (ITU-T, 1997).

A detecção de silêncio deve preferencialmente ser realizada no terminal do usuário, mas pode ser feita na unidade de controle multiponto, decodificando-se o áudio recebido e realizando-se o cálculo da potência. Estabelece-se um limiar dinâmico ou estático para a detecção de atividade de voz (ou de presença de silêncio), sendo que esse limiar é calibrado de acordo com o nível do ruído de fundo do ambiente no qual o terminal se localiza. Quando um período de silêncio é detectado, nenhum pacote contendo áudio é transmitido, economizando-se banda.

Para que o participante receptor não tenha uma sensação artificial e desconfortável de quietude, o terminal receptor pode reproduzir um “ruído de conforto” (ITU-T, 2000b). Os *codecs* G.711 (ITU-T, 1988a), G.726 (ITU-T, 1990a), G.727 (ITU-T, 1990b), G.728 (ITU-T, 1992) e G.722 (ITU-T, 1988b) não possuem em suas especificações a detecção de ativação de voz, a descontinuidade da transmissão de

pacotes (*Discontinuous Transmission* – DTX) (LUTHI, 2001), nem a geração de um ruído de conforto. Nada impede, porém, que implementações específicas de cada *codec* lidem com essas questões.

A RFC 3389 – *Real-time Transport Protocol (RTP) Payload for Comfort Noise (CN)* (ZOPF, 2002) sugere um tipo de *payload* específico para o transporte de informações de silêncio para o RTP, de forma a reduzir a banda ocupada. Essa técnica também é conhecida como inserção de descrição de silêncio (*Silence Insertion Descriptor* – SID) (LUTHI, 2001) e (ZOPF, 2002).

Algumas implementações de *codecs* de áudio indicam a presença de silêncio ou simplesmente não transmitem pacotes nessa situação. Porém, em ambientes muito ruidosos ou com conversas em paralelo no ambiente do usuário, a detecção de silêncio pode não funcionar satisfatoriamente, transmitindo-se *bursts* espúrios de pacotes de áudio.

2.3 Ambientes virtuais multimídia colaborativos

Um ambiente virtual multimídia colaborativo é a representação digital de um espaço de trabalho para permitir a interação entre pessoas separadas geograficamente para a realização de uma tarefa em colaboração, dispondo para isso de ferramentas e recursos multimídia compartilhados para a comunicação e percepção mútua dos envolvidos na sua execução (CHURCHILL, SNOWDON, 1998).

Há diferentes abordagens para a representação das ferramentas e recursos multimídia em um ambiente colaborativo (ANTUNES, GUIMARÃES, 1994). Uma abordagem comum para a interface homem-máquina de ambientes virtuais colaborativos compartilhados é a WYSIWIS (*What You See Is What I See* – O Que Você Vê É O Que Eu Vejo), onde todos os usuários utilizando a ferramenta colaborativa possuem a mesma visão dos recursos que os demais. Os recursos são representados com as mesmas formas, cores e disposições na interface de todos os usuários. Uma forma um pouco mais relaxada do WYSIWIS é o WYSIWIMS (*What You See Is What I May See* – O Que Você Vê É O Que Eu Posso Estar Vendo). No WYSIWIMS, o

usuário possui uma maior flexibilidade com relação à disposição e à representação dos recursos na sua interface.

As ferramentas multimídia colaborativas podem ser classificadas de acordo com o estado de prontidão no tempo (síncrona ou assíncrona) e de acordo com o padrão de relacionamento dos usuários (não-interativa/transacional ou interativa/reativa) (DOMMEL, GARCIA-LUNA-ACEVES, 1997). Exemplos de ferramentas multimídias e suas classificações são apresentados na Tabela 2.3.

Tabela 2.3 – Ferramentas multimídia colaborativas e suas classificações

Ferramenta	Grau de prontidão		Padrão de relacionamento	
	Síncrona	Assíncrona	Não-interativa ou Transacional	Interativa ou Reativa
Banco de dados		X	X	
Edição de texto	X		X	
E-mail		X		X
Videoconferência	X			X

O acesso às ferramentas multimídia precisa ser coordenado e controlado de forma a resolver possíveis conflitos de uso. Os tipos de conflitos e os mecanismos mais indicados para resolvê-los depende da classificação da ferramenta multimídia (DOMMEL, GARCIA-LUNA-ACEVES, 1997). Para este trabalho em particular, interessam as ferramentas síncronas interativas, como a videoconferência. Os recursos compartilhados disponíveis em uma videoconferência são justamente os canais de áudio e de vídeo. O conflito em uma videoconferência ocorre quando mais de um participante deseja transmitir o seu canal de vídeo e de áudio e o mecanismo utilizado para a resolução desse tipo de conflito é o controle de posse da palavra (*floor control*). Outros mecanismos podem ser utilizados, mas de uma forma ou de outra, eles podem ser encarados genericamente como políticas de uso do recurso em questão.

Qiu, Kuhns e Cox (2002) citam alguns paradigmas de ambientes colaborativos multimídia: videoconferência interativa, videofone, reuniões de grupos e salas de

aula virtuais. Os paradigmas citados diferem entre si pelos graus de escalabilidade e de interatividade entre os participantes do ambiente colaborativo.

Para este trabalho, o paradigma da sala de aula virtual é o foco e nele, há uma interatividade não muito alta, porque a forma de comunicação é predominantemente assimétrica, com o professor se dirigindo à classe na maior parte do tempo e, ocasionalmente, um aluno se dirige à classe e ao professor, para fazer ou responder uma pergunta ou realizar um comentário. A sala de aula virtual deve ser capaz de suportar até algumas dezenas de alunos e é fundamental que o professor tenha a percepção da presença deles na sala, sendo secundária a percepção dos alunos por outros alunos.

2.3.1 Controle de posse de palavra em ambientes colaborativos

Em uma conferência ou reunião presidida, a posse da palavra concede o direito à pessoa que a detém de se dirigir às demais pessoas presentes (DOMMEL, GARCIA-LUNA-ACEVES, 1997). A pessoa que preside a conferência é o moderador e é ele quem concede a posse da palavra às pessoas, controlando o dinamismo da conferência.

O controle de posse da palavra aplica-se aos canais de áudio ou de vídeo, mas, de forma mais abstrata, seu conceito e funcionamento podem ser aplicados a qualquer outro recurso síncrono e interativo que precise de acesso coordenado, resolvendo conflitos no seu uso, como condições de corrida e *deadlocks*. A forma mais abstrata do controle de posse da palavra é um controle de posse de um recurso de um ambiente virtual colaborativo. Exemplos de recursos da conferência que precisam de acesso coordenado são os canais de áudio e vídeo, *whiteboard* e edição de documentos por múltiplos autores simultaneamente. Cada recurso pode ter o seu controle de posse ou um único controle pode gerenciar o acesso a múltiplos recursos. Um único controle de posse de palavra pode estar associado aos canais de áudio e de vídeo.

O controle de posse da palavra pode ser otimista ou pessimista. O controle otimista espera até que um conflito de recurso ocorra e, então, o resolve, enquanto o controle pessimista tenta impedir que conflitos de recursos ocorram, por exclusão mútua (DOMMEL, GARCIA-LUNA-ACEVES, 1997) e (QIU, KUHNS, COX, 2002).

Em ambientes colaborativos virtuais, o controle de posse da palavra pode ser realizado de forma autônoma por um agente de *software* com regras ou políticas explícitas de concessão da posse da palavra, ou de forma assistida por um dos participantes fazendo o papel social do moderador, com regras implícitas e subjetivas de concessão de posse da palavra, derivadas das conversações face-a-face do mundo real.

A política de controle de posse da palavra define quem possuirá o controle de posse da palavra. No caso de um mecanismo autônomo de controle de posse da palavra, a política deve ser explícita, conhecida por todos os participantes da conferência, deve assegurar que qualquer participante possa deter a posse da palavra e deve possuir um mecanismo de recuperação em caso de falha. A maior desvantagem do controle de posse da palavra autônomo decorre do fato dele não considerar a dinâmica natural de uma conversação como base para tomada de decisões. Dommel e Garcia-Luna-Aceves (1995) e (1997), sugerem algumas políticas para o controle de posse da palavra autônomo e para o assistido:

- **Conferência moderada:** Um usuário faz o papel de moderador e decide subjetivamente quem terá a posse da palavra.
- **Sob agendamento:** A sequência de atribuições da posse da palavra é definida antes do início da conferência, por agendamento.
- **Por tempo:** As requisições de posse da palavra e a própria posse da palavra são controladas por temporizadores, podendo seus intervalos de tempo ser determinados por eventos e condições do sistema.
- **Ordem pré-definida:** A posse da palavra é oferecida a cada participante a partir de uma ordem pré-definida. A política *First Come First Served* (FCFS) é um exemplo de política com ordem pré-definida.

- **Reordenação *ad hoc*:** As requisições de posse da palavra são reordenadas, baseadas em prioridades, critérios de qualidade de serviço e uso. Exemplos desse tipo de política são as políticas *Least Recently Served* (LRS) e *Weighted Fair Queueing* (WFQ).
- **Eleição:** Os participantes da conferência elegem quem será o próximo participante a ter a posse da palavra.
- **Loteria:** Sorteia-se a posse da palavra entre os participantes que a requisitaram.

A implementação do controle de posse da palavra pode ser dividida em questões relacionadas ao sistema e questões relacionadas ao usuário (DOMMEL, GARCIA-LUNA-ACEVES, 1997).

Questões relacionadas ao sistema discorrem sobre:

- A arquitetura do próprio sistema;
- O formato dos pacotes;
- O mecanismo de distribuição dos pacotes;
- A consistência e coerência dos estados do controle de posse de palavra;
- O tratamento de exceções e de falhas.

Questões relacionadas ao usuário discorrem sobre:

- A representação na interface homem-máquina dos recursos disponíveis e do seu estado atual;
- A forma pela qual o controle de posse da palavra é requisitado, concedido e representado.

Os aspectos de sistema do controle de posse da palavra estão relacionados ao mecanismo de controle de posse da palavra, enquanto que os aspectos de usuário estão relacionados à política do controle de posse da palavra, como a posse da palavra é requisitada e concedida (CROWLEY et al., 1990).

Se a conferência for do tipo centralizada, a unidade de controle multiponto precisa suportar o controle de posse da palavra e conhecer o moderador da conferência, no caso de controle de posse da palavra assistida, ou implementar o mecanismo de controle de posse de palavra autônomo. No primeiro caso, a unidade de controle multiponto recebe as requisições de posse de palavra e as encaminha para o moderador. Então, a resposta do moderador é encaminhada para os participantes que solicitaram a posse da palavra.

Se a conferência for do tipo descentralizada com transmissão de pacotes sobre IP *unicast*, todos os participantes precisam saber quem é o moderador da conferência, para encaminharem suas requisições de palavra e esperarem uma resposta.

2.4 Tradutores de endereços de rede e de portas

A tradução de endereços de redes é um método utilizado para mapear endereços de um domínio de rede para outro (HOLDREGE, SRISURESH, 1999). O tradutor de endereço de rede (*Network Address Translator* – NAT) separa uma rede privada (rede interna), de uma rede global (rede externa). Utiliza-se o NAT quando o espaço de endereçamento da rede privada não é válido para a rede global ou quando se deseja esconder a rede privada da rede global.

Geralmente, as redes internas ao NAT, também chamadas de redes privadas, utilizam os espaços de endereçamento 10.0.0.0/16, 172.16.0.0/12 e 192.168.0.0/16, segundo (REKHTER, 1996).

O NAT oferece uma solução provisória para a escassez de endereços IPv4, mas cria problemas para as aplicações de rede, como será visto mais adiante.

Há várias versões de NAT, mas só serão abordadas o NAT básico e o NAPT (*Network Address and Port Translator* – Tradutor de endereço de rede e de porta) (HOLDREGE, SRISURESH, 1999).

2.4.1 O NAT básico

Pacotes da rede interna com destino à rede externa têm seus endereços IP de origem inválidos trocados pelo NAT por endereços IP de origem de uma faixa de endereços pré-determinada válida na rede externa. O NAT pode ser alcançado externamente por qualquer um dos endereços IP dessa faixa.

O mapeamento de endereços pode ser realizado de forma dinâmica ou estática. Na forma estática, o endereço IP interno falso sempre é mapeado para o mesmo endereço IP verdadeiro e na forma dinâmica, para o primeiro endereço IP verdadeiro disponível.

Quando o mapeamento é feito, o NAT cria internamente uma sessão, caracterizada pela tripla <endereço IP origem interno, endereço IP destino, protocolo superior à camada de rede IP>. Essa tripla está associada ao endereço IP traduzido. As sessões são desfeitas um certo tempo depois que a comunicação entre os pontos externo e interno à rede do NAT é finalizada, o que pode ser difícil de se determinar para sessões utilizando o UDP (HOLDREGE, SRISURESH, 1999).

O equipamento da rede externa ao qual o pacote se destina deve transmitir os seus pacotes para o novo endereço IP de origem do pacote. Quando o NAT recebe um pacote da rede externa, ele verifica se há alguma sessão que mapeia o endereço IP destino do pacote com um endereço da rede interna. Caso haja, o pacote tem seu endereço IP destino alterado e o NAT o transmite para a rede interna. Caso contrário, o pacote é descartado.

Quando um endereço IP verdadeiro do NAT está sendo utilizado por uma sessão, somente a estação à qual pertence o endereço IP falso pode utilizar o endereço IP verdadeiro, pelo menos se o protocolo transportado pela camada de rede for o mesmo, para que o NAT consiga identificar corretamente a quem se destina o pacote

recebido da rede externa. O NAT básico restringe o número de equipamentos que pode acessar simultaneamente a rede externa ao número de endereços IP verdadeiros disponíveis e também não permite que um equipamento da rede externa inicie uma comunicação com um equipamento da rede interna. Isso ocorre, porque a estação externa não tem como endereçar o endereço IP falso da estação na rede interna, já que a sessão no NAT só é criada quando os pacotes são transmitidos da rede interna para a rede externa. Então, não haverá uma sessão no NAT capaz de fazer o mapeamento.

2.4.2 O NAPT

O NAPT permite multiplexar os endereços IP verdadeiros disponíveis através da tradução de endereços e de portas. A sessão passa a ser representada pela tupla <endereço IP de origem, porta TCP/UDP de origem, endereço IP de destino, porta TCP/UDP de destino>. Dessa forma, pode-se criar um número muito maior de sessões, dependendo somente do número de portas disponíveis para a tradução.

Algumas implementações de NAPT utilizam como porta de origem o próprio número de porta de origem do pacote recebido, desde que ela ainda esteja disponível nele, passando a utilizar uma porta aleatória ou a primeira porta disponível de uma faixa de portas ao receber um pacote de uma outra estação com a mesma porta de origem.

Para o cenário anterior e na maioria dos casos, um único endereço IP verdadeiro seria suficiente para resolver o problema da empresa.

2.4.3 Problemas com o NAT e o NAPT

O NAT e o NAPT apresentam vários problemas para as aplicações de rede (HOLDREGE, SRISURESH, 1999); (HOLDREGE, SRISURESH, 2001) e (SENIE, 2002) e há algumas soluções propostas, que utilizam protocolos adicionais (ROSENBERG et al., 2003) ou heurísticas (DAIGLE, 2002).

Sob o ponto de vista das aplicações de rede, o maior problema causado pelo NAT tradicional ou pelo NAPT é a impossibilidade de se iniciar uma conexão de rede originada a partir da rede externa, porque o NAT tradicional e o NAPT não têm como determinar a qual estação interna os pacotes da conexão se destinam. Uma solução para esse problema é o encaminhamento estático de endereço IP, no caso do NAT, ou de portas, no caso do NAPT. Isto é, pode-se configurar o NAT tradicional para encaminhar todo pacote recebido em um determinado endereço IP válido da sua faixa de endereços para uma única estação da rede interna. De forma semelhante, pode-se configurar o NAPT para encaminhar todo pacote recebido em um endereço IP e em uma porta TCP/UDP para uma determinada porta de uma estação da rede interna. Entretanto, essa solução para o NAPT só é viável quando a porta TCP/UDP da aplicação de rede for definida de forma estática e quando somente um equipamento interno utilizar essa aplicação. Essa solução estática não se aplica a aplicações que utilizam portas TCP/UDP dinâmicas ou que necessitam da abertura de conexões subseqüentes na mesma direção, como o *File Transfer Protocol* (FTP).

Uma aplicação de rede que dependa de configurações especiais no NAT ou no NAPT pode ser inviabilizada, porque o usuário pode não ter domínio sobre o equipamento ou mesmo conhecimento de como fazê-lo.

Protocolos que encapsulam informações de camada de rede e de transporte para a negociação da abertura de novas conexões, como o H.323 (ITU-T, 2003b), encontram problemas com NAT e com o NAPT, não só pela questão da abertura de conexões a partir da rede externa, mas também porque a estação da rede interna encapsulará um endereço IP falso e portas que serão inatingíveis para a rede externa. Alguns NATs e NAPTs implementam o conceito de *gateways* de camada de aplicação. Os *gateways* de camada de aplicação são específicos para cada aplicação (H.323, FTP, etc.) e analisam continuamente os pacotes de uma conexão, realizando conversões de endereços de rede e de portas encapsuladas para endereços e portas válidos e vice-versa. Os *gateways* de camada de aplicação aumentam consideravelmente o processamento em NATs e NAPTs. Quando os fabricantes de NAT/NAPT incluem *gateways* de aplicação nos seus equipamentos, somente algumas poucas aplicações mais populares são atendidas.

O cenário ilustrado na Figura 2.4 ajuda a compreender o problema com o NAPT: uma aplicação de rede com arquitetura *peer-to-peer*, que usa a porta UDP 5.000 para se comunicar bidirecionalmente, é utilizada por duas estações, A e B, atrás de um mesmo NAPT e por uma terceira estação, C, na rede externa.

Figura 2.4 – Cenário de uma aplicação de rede *peer-to-peer* em uma rede com NAPT.

As três estações estão esperando receber conexões na porta UDP 5.000. Nesse cenário, temos as seguintes situações:

- A estação A consegue enviar um pedido de conexão para as estações B e C;
- A estação B consegue enviar um pedido de conexão para as estações A e C;
- A estação C não consegue enviar um pedido de conexão para A e para B, porque não há nenhuma sessão mapeando o caminho de C para A e/ou de C para B.

Se o NAPT realizar encaminhamento estático da porta 5.000 para a estação A, por exemplo, a estação B nunca seria alcançada externamente. Ainda que A e B consigam enviar um pedido de conexão para C, C tem que responder para a porta UDP pela

qual o NAPT transmitiu o pacote, e não mais a porta 5.000, para que a comunicação seja completada.

Suponha que o pacote de pedido de conexão transmitido de *A* para *C* possua o endereço IP de origem IP_A , porta UDP de origem 5.000, endereço IP de destino IP_C e porta UDP destino 5.000. Ao passar pelo NAPT, o endereço IP de origem do pacote passa a ser $IP_{NAPT\ EXTERNO}$ e a porta UDP de origem continua sendo 5.000, por ela estar disponível. Uma sessão identificada pela tupla $\langle IP_A, 5.000, IP_C, 5.000 \rangle$ é criada e associada à porta UDP 5.000 do NAPT. Se a aplicação *peer-to-peer* incluir no seu pedido de conexão o endereço IP de *A*, IP_A , e a estação *C* tentar utilizar essa informação como o endereço IP destino do pacote, *A* nunca receberá a resposta de *C*, porque *C* estará transmitindo seu pacote para um endereço IP inválido. Para dar prosseguimento ao exemplo, suponha que *C* detecte o endereço IP de origem do pacote recebido e transmita seus pacotes para esse endereço. Quando a estação *C* responder ao pedido de conexão, ela enviará um pacote com IP de origem IP_C , porta UDP de origem 5.000, endereço IP destino $IP_{NAPT\ EXTERNO}$ e porta UDP destino 5.000. O NAPT receberá o pacote e, pela sessão identificada pela tupla $\langle IP_A, 5.000, IP_C, 5.000 \rangle$, modifica o endereço IP destino $IP_{NAPT\ EXTERNO}$ para IP_A e deixa a porta UDP inalterada, visto que é a mesma. A estação *A* recebe o pacote e a comunicação entre *A* e *C* fica estabelecida.

Agora, suponha que a estação *B* também deseje se comunicar com a estação *C* e envie um pacote de pedido de conexão com IP de origem IP_B , porta UDP de origem 5.000, endereço IP destino IP_C e porta UDP destino 5.000. Quando o NAPT recebe esse pacote, ele troca o endereço IP de origem para $IP_{NAPT\ EXTERNO}$, mas a porta UDP de origem não pode ser a 5.000, porque ela está sendo utilizada pela sessão da estação *A* com a estação *C*. Então, o NAPT passa a utilizar a primeira porta UDP disponível de uma determinada faixa de endereços, a porta 1.024, por exemplo. Então, a sessão é criada, identificada pela tupla $\langle IP_B, 5.000, IP_C, 5.000 \rangle$ e é associada à porta UDP 1.024 do NAPT. Se a estação *C* enviar a sua resposta para a porta 5.000 do NAPT, o pacote será encaminhado erroneamente para estação *A*, ao invés da estação *B*. Para evitar esse problema, a aplicação de rede deve capturar a porta UDP de origem do pacote recebido e usá-la como porta UDP destino. Dessa forma, a estação *C* deve enviar um pacote para o endereço IP destino $IP_{NAPT\ EXTERNO}$,

porta UDP destino 1.024, endereço IP de origem IP_C e porta UDP de origem 5.000. Quando o NAPT receber esse pacote, ele o encaminhará corretamente para a estação *B*.

Os *firewalls* apresentam os mesmos problemas do NAT e do NAPT, podendo ainda bloquear explicitamente ou implicitamente o tráfego necessário para o funcionamento de uma aplicação de rede.

2.4.4 Uma solução genérica para o problema do NAPT

Para uma aplicação de rede com arquitetura cliente-servidor, estando o cliente localizado atrás de um NAPT e o servidor atrás de outro NAPT ou NAT, os seguintes requisitos são necessários para o funcionamento transparente da aplicação de rede, pelo menos sob o ponto de vista do cliente:

1. Os *sockets* envolvidos na comunicação precisam ser bidirecionais, isto é, as portas TCP/UDP da aplicação precisam ser utilizadas tanto para a transmissão (porta de origem) quanto para a recepção de dados (porta de destino).
2. A rotina de recepção de pacotes precisa detectar o endereço IP de origem e a porta TCP/UDP de origem e utilizá-los como endereço IP destino e porta TCP/UDP destino. Conseqüentemente, não se deve encapsular informações a respeito de endereços IP e portas TCP/UDP para serem utilizadas como endereços e portas destino nos pacotes transmitidos.
3. Toda comunicação deve ser iniciada a partir do cliente, na rede interna do NAPT, para que este crie a sessão e a associe à porta traduzida transmitida pelo NAPT para a rede externa.
4. O NAT/NAPT do servidor deve estar configurado para encaminhar estaticamente para o servidor os pacotes recebidos nas portas utilizadas pela aplicação de rede em questão e não deve realizar tradução de portas nos pacotes transmitidos pelo servidor, para que o *software* no cliente não seja confundido.

No caso de aplicações *peer-to-peer*, se as estações estiverem atrás de NAPT's diferentes, outros requisitos são necessários para resolver o problema de comunicação, como um *gateway* de camada de aplicação em um NAPT que resolva nomes em endereços de rede, por exemplo.

2.5 Considerações finais

A partir das informações contidas neste capítulo, pode-se identificar como aspectos mais relevantes em voz sobre IP:

- O tráfego de voz sobre IP é transportado utilizando-se o protocolo RTP sobre UDP e possui características de tempo real;
- Os *codecs* comumente utilizados em voz sobre IP produzem uma taxa constante de pacotes de tamanho fixo;
- Os *codecs* de áudio possuem características diferentes com relação à banda utilizada, atraso algorítmico e qualidade subjetiva. A escolha do *codec* a ser utilizado depende do cenário em questão, caracterizado pela banda disponível e pelo atraso médio dos pacotes na rede;

Já com relação aos mecanismos de distribuição de pacotes em redes IP, pode-se afirmar:

- A utilização de IP *multicast* somente é possível quando a infra-estrutura de rede, o sistema operacional do terminal multimídia e a própria aplicação o suportarem, mas sempre é possível utilizar-se IP *unicast*;
- Em geral, é difícil obter-se um endereço IP *multicast* global;

A respeito de conferências multimídia, conclui-se:

- Conferências multimídia podem ser realizadas com ou sem a utilização de um protocolo de controle de conferência (SIP, H.323 e protocolos proprietários), como em uma conferência fracamente controlada;
- Para se realizar uma conferência multimídia utilizando IP *unicast* é recomendável a utilização de uma unidade de controle multiponto (conferência multiponto centralizada);
- Transcodificação e mixagem são operações dependentes de *codecs* e custosas computacionalmente;

Dentre o que foi apresentado sobre mecanismos para controle de banda em conferências multimídia sobre redes IP e controle de posse da palavra, as seguintes observações podem ser colocadas:

- A detecção de atividade de voz deve ser realizada no *software* do cliente e não na unidade de controle multiponto, para se distribuir o processamento necessário e se economizar os recursos de rede;
- O mecanismo de controle de posse da palavra consegue restringir a banda utilizada tanto em conferências multimídia centralizadas quanto em descentralizadas;
- Em conferências centralizadas com um mecanismo de controle de posse da palavra que permita um único participante transmitindo por vez, o crescimento da banda utilizada deixa de ser quadrático e passa a ser linear com relação ao número de participantes nela;
- O mecanismo de controle de posse da palavra reproduz o comportamento típico em uma sala de aula, porque o papel do professor assemelha-se ao de um moderador e interlocutor em uma conferência. Portanto, tal mecanismo é apropriado para regular as interações em uma sala de aula virtual;

Com relação a aplicações de redes e NATs/NAPTs, pode-se ressaltar os seguintes pontos:

- O usuário de uma aplicação de rede qualquer pode se encontrar atrás de um NAT/NAPT;
- Aplicações com arquitetura cliente-servidor conseguem contornar os problemas com NAT/NAPT de forma mais simples que aplicações com arquitetura *peer-to-peer*;
- A aplicação de rede deve ser projetada de forma que o NAT/NAPT não a inviabilize. Para tanto, é necessário que a comunicação sempre seja iniciada pela estação na rede interna ao NAT/NAPT, que sempre seja feita a detecção de portas e de endereços IP dos pacotes recebidos e que os *sockets* sejam bidirecionais. No caso do servidor estar atrás de um NAT/NAPT, o NAT/NAPT deve realizar encaminhamento estático de portas para o servidor e não realizar tradução das portas dos pacotes originados pelo servidor.

O próximo capítulo levanta os requisitos do sistema de conferência multiponto por voz e com base nas informações trazidas neste capítulo, define e propõe a solução a ser adotada.

3. ESPECIFICAÇÃO DO SISTEMA

“Vinde a mim, todos os que estais cansados e sobrecarregados, e eu vos aliviarei. Tomai sobre vós o meu jugo e aprendei de mim, que sou manso e humilde de coração; e achareis descanso para a vossa alma. Porque o meu jugo é suave, e o meu fardo é leve.”

Mateus 11.28-30

Neste capítulo, são apresentados os requisitos e as especificações do sistema multiponto por voz proposto para se enriquecer a experiência de usuários de ferramentas de ensino a distância pela Internet. Algumas definições são colocadas primeiramente. As abordagens possíveis para a arquitetura e implementação do sistema são discutidas, tendo como base principal as informações contidas no capítulo anterior. Finalmente, a solução adotada é apresentada, expondo suas vantagens e desvantagens. O capítulo é encerrado com algumas considerações finais.

3.1 Definições

As seguintes definições servirão como base para o texto:

- **Sala virtual de conferência:** Espaço virtual representado no sistema proposto por uma página *web* onde são realizadas conferências virtuais. A sala virtual de conferência tem um número finito de cadeiras virtuais (lotação da sala).
- **Usuário do sistema:** Qualquer pessoa com acesso ao sistema de conferência.
- **Usuário cadastrado no sistema:** Pessoa com acesso ao sistema de conferência e cujas informações particulares encontram-se cadastradas na base de dados do sistema.

- **Usuário não cadastrado no sistema:** Pessoa com acesso ao sistema de conferência, mas cujas informações particulares não se encontram cadastradas na base de dados do sistema.
- **Administrador do sistema:** Usuário especial do sistema com acesso ao sistema de gerenciamento.
- **Participante:** Usuário do sistema presente em uma conferência.
- **Participante comum:** Participante de uma conferência que não exerce o papel de moderador.
- **Moderador:** Participante de uma conferência com que controla a interação entre os demais participantes e a admissão deles na mesma.
- **Cadeira virtual:** Cada participante de uma conferência possui uma cadeira virtual na conferência.
- **Cadeira reservada:** Associação de um usuário cadastrado no sistema a uma sala virtual de conferência de forma a assegurar sua participação em conferências na sala em questão, independentemente da lotação dela.

3.2 Requisitos funcionais do sistema

Os requisitos do sistema podem ser divididos em requisitos gerais, requisitos para as salas virtuais de conferência, requisitos de gerenciamento, requisitos referentes à base de dados e requisitos para a comunicação de tempo real.

Qualidade de serviço de rede, segurança e um estudo profundo sobre a escalabilidade e disponibilidade do sistema não pertencem ao escopo deste trabalho, portanto, seus requisitos não foram levantados, embora o sistema possa apresentar funcionalidades que atendam indiretamente a um desses itens.

3.2.1 Requisitos gerais do sistema

O sistema de conferência multiponto deve ser um sistema completamente independente. Entretanto, o sistema de conferência multiponto deve poder também ser integrado a sistemas externos a ele, como por exemplo, ferramentas de educação a distância também baseadas em tecnologia *web*.

O sistema de conferência multiponto deve ser desenvolvido para ambientes de redes baseados na arquitetura TCP/IP.

O sistema de conferência multiponto deve poder ser acessado tanto por usuários remotos, através da Internet, quanto por usuários locais, na mesma rede do servidor hospedando o sistema, como mostra a Figura 3.1.

Figura 3.1 – Ambiente de utilização do sistema de conferência multiponto.

Os seguintes requisitos funcionais gerais foram definidos para o sistema:

- **Reprodução da dinâmica de conversação de uma sala de aula:** A principal atividade em uma sala de aula é a comunicação do professor com os alunos e, ocasionalmente, dos alunos com o professor ou entre os próprios alunos. Portanto, na maior parte do tempo há um fluxo assimétrico de informações. Há a

definição clara de papéis sociais distintos, aluno (participante comum) e professor (moderador), que deverão ser tratados de forma distinta pelo sistema.

- **Suporte a comunicação por áudio e, opcionalmente, por texto:** O sistema deve suportar o tráfego de áudio e de texto, sendo que ambos possuem requisitos de tempo real. A comunicação por texto ajuda a aumentar a interatividade dentro da conferência.
- **Limitação da banda consumida:** O sistema deve permitir somente que um participante fale por vez em uma sala virtual de conferência, para limitar a utilização de banda na rede e orquestrar a conversação na conferência.
- **Implementação baseada em tecnologia *web*, para facilitar a integração com ferramentas de ensino a distância para a Internet:** O sistema deve ser implementado utilizando-se tecnologias difundidas e disponíveis no mercado. A sala de aula virtual será representada para cada usuário através de uma página *web* e a interface homem-máquina deve possuir recursos multimídia especiais para captura e reprodução de áudio. A utilização de tecnologia *web* é justificada por sua grande aceitação, difusão, popularidade e por facilitar a integração com outros sistemas, como os próprios *sites* e *intranets* de faculdades, escolas e empresas.
- **Acesso ao sistema a partir de um terminal (uma estação) com recursos multimídia simples:** O sistema deve ser implementado em *software*, de forma que o usuário consiga utilizar o sistema com um computador multimídia doméstico, sem a utilização de equipamentos caros e dedicados. Um computador com um processador de 350 MHz, 128 MB de memória RAM e placa de som *full-duplex* padrão PCI deve ser suficiente para a utilização do sistema.
- **Acesso remoto ao sistema:** Considerando que um usuário doméstico pode utilizar uma conexão com a Internet por acesso discado, há uma restrição da banda disponível para o usuário. Supondo-se a banda máxima limitada em cerca de 50 kbps, a somatória da banda decorrente dos pacotes de áudio, de texto e de controle de conferência precisa ser inferior a esse valor. Desses três tipos de tráfego, o mais crítico é o dos pacotes de áudio o que certamente restringe os *codecs* de áudio que podem ser utilizados a *codecs* de baixo *bit rate*.

- **Suporte a comunicação através de NAT/NAPT:** O usuário deve ser capaz de utilizar o sistema ainda que ele se encontre atrás de um *Network Address Translator* (NAT), de um *Network Address and Port Translator* (NAPT) (HOLDREGE, SRISURESH, 1999) ou de um *firewall*, apesar das barreiras que esses equipamentos podem representar para aplicações de rede (HOLDREGE, SRISURESH, 1999); (HOLDREGE, SRISURESH, 2001) (vide Capítulo 2.4.3).
- **Utilização simultânea de mais de uma sala de aula virtual:** O sistema deve permitir que conferências ocorram em paralelo e que o usuário escolha em qual delas ele deseja tomar parte.
- **Limitação de uma conferência por usuário:** O usuário deve ser capaz de participar somente de uma conferência por vez.
- **Visualização das salas virtuais de conferência:** O sistema deve permitir ao usuário visualizar as salas virtuais de conferência às quais ele tem direito de acesso, para que ele possa escolher em qual sala entrar.
- **Cada sala de aula virtual deve suportar um número limitado de usuários:** O número de alunos de alunos em uma sala de aula virtual causa impacto na banda de rede consumida pela aplicação, principalmente se não for utilizado o IP *multicast* como mecanismo de distribuição de pacotes (vide Capítulo 2.1.3).
- **Capacidade do sistema:** Sem limitação de banda, o sistema deve suportar no mínimo duas salas virtuais de conferência com pelo menos cinco participantes em cada conferência, mas é desejável que cada sala virtual de conferência consiga atender até algumas dezenas de participantes. A capacidade máxima do sistema (o número máximo de salas virtuais de conferência simultâneas e o número máximo de participantes em cada sala) certamente não é ilimitada, mas quanto maior for a sua capacidade, melhor. Se a capacidade máxima do sistema fosse ilimitada, o moderador da sala virtual de conferência limitaria o número máximo de participantes na conferência, porque não conseguiria atender a um número ilimitado de participantes.
- **O sistema deve possibilitar o uso de *codecs* de áudio diferentes:** A aplicação deve ser independente de *codec* de áudio e permitir que cada sala de aula virtual possa usar o *codec* que se desejar. Cada *codec* de áudio possui características

diferentes com relação à banda, ao atraso e à qualidade subjetiva. Se o administrador do sistema souber que uma determinada sala virtual de conferência é utilizada somente por usuários da rede local, então ele pode configurar esta sala para utilizar um *codec* com uma qualidade subjetiva melhor, sem se preocupar tanto com a banda consumida. Se a sala, porém, for utilizada predominantemente por usuários remotos, o administrador do sistema pode escolher um *codec* de áudio com uma banda menor.

- **Suporte a futuras extensões:** O sistema deve ser implementado de forma a suportar extensões futuras, como o uso de vídeo ou de um outro protocolo de controle de conferência.

3.2.2 Requisitos funcionais das salas virtuais de conferência

As salas virtuais de conferência possuem requisitos quanto à forma como elas são representadas, acessadas e como os participantes da conferência interagem entre si.

3.2.2.1 Representação das salas virtuais de conferência

A sala virtual de conferência deve ser implementada como uma página *web* e cada participante nela deve ser representado através de duas imagens, uma para representá-lo quando estiver presente na conferência (imagem ativo – em cores) e outra, quando estiver ausente (imagem inativo – em escala de cinza). Quando um usuário possui uma cadeira reservada na sala virtual de conferência e ele não estiver ainda presente na conferência, a sua imagem inativa deve ser visualizada por todos os participantes.

A interface homem-máquina deve ser personalizável, através de alterações na página *web* que representa a sala virtual de conferência. A interface homem-máquina deve ser capaz de ocupar toda a tela disponível no terminal do usuário ou somente uma

parte dela, de forma que outros aplicativos possam ser visualizados simultaneamente com o sistema de conferência multiponto.

Os participantes em uma conferência devem ser capazes de visualizar pelo menos a imagem e o nome dos demais participantes.

Somente um participante poderá falar por vez e deve haver uma indicação visual do participante que está falando. Deve também haver uma indicação visual para cada uma das situações possíveis para um participante dentro de uma conferência:

- Fora da conferência;
- Pedindo para entrar na conferência;
- Dentro da conferência;
- Com problemas de comunicação de rede;
- Expulso da conferência;
- Pedindo para falar;
- Falando;
- Com o áudio bloqueado pelo moderador.

A interface homem-máquina deve ser do tipo *What You See Is What I See* (WYSIWIS – vide Capítulo 2.3), isto é, todos os participantes na conferência devem possuir uma mesma visão da sala virtual de conferência em suas interfaces homem-máquina. Portanto, é necessário se garantir o sincronismo de informações a respeito do estado de cada participante.

3.2.2.2 Políticas de acesso às salas virtuais de conferência

As salas podem ou não possuir usuários cadastrados associados a elas. Os usuários podem estar associados a mais de uma sala virtual de conferência, mas só podem

participar de uma conferência por vez. Quando um usuário está associado a uma sala virtual de conferência, ele torna-se dono de uma cadeira virtual naquela sala, passando a ser o único usuário que pode sentar virtualmente nela, como se a cadeira ficasse permanentemente reservada a ele.

O sistema deve oferecer diferentes políticas de acesso às salas virtuais de conferência:

- Deve ser possível reservar cadeiras virtuais em salas virtuais de conferência para usuários cadastrados no sistema;
- Deve haver três tipos diferentes de salas virtuais de conferência: salas que só podem ser acessadas por usuários com cadeira reservada; salas que podem ser acessadas somente por usuários cadastrados (com ou sem cadeira reservada) e salas que podem ser acessadas por usuários cadastrados ou não no sistema. Dessa forma, tanto usuários cadastrados quanto não cadastrados no sistema podem participar de conferências.

Essas políticas devem ser implementadas, de forma que o sistema de conferência atenda a diferentes cenários, como os descritos abaixo:

- Disponibilização de salas virtuais de conferência para alguns usuários cadastrados de um sistema;
- Disponibilização de salas virtuais de conferência para todos os usuários cadastrados de um sistema;
- Disponibilização irrestrita de salas virtuais de conferência.

3.2.2.3 Papéis sociais dentro da conferência

Deve haver dois papéis sociais bem distintos dentro da conferência:

- Participante comum;
- Moderador.

O participante comum pode:

- Pedir para entrar na conferência;
- Deixar a qualquer instante a sala virtual de conferência;
- Sinalizar que deseja falar (requisitar a posse da palavra);
- Desistir de pedir para falar (desistir de requisitar a posse da palavra);
- Devolver a posse da palavra para o moderador, após tê-la recebido.

O moderador é um participante com poderes especiais para:

- Admitir, rejeitar e expulsar participantes comuns na/da conferência;
- Permitir ou negar a posse da palavra a qualquer participante comum;
- Tomar a posse da palavra no momento em que desejar, sinalizando ou não que deseja falar;
- Permitir ou não que um determinado participante na conferência ouça o que estiver sendo discutido;
- Eleger um novo moderador.

Deve haver uma indicação visual para destacar o moderador da conferência.

Quando o moderador abandonar a conferência, ela deve ser terminada.

O sistema deve possibilitar que uma sala virtual de conferência possua um moderador definido previamente ou que ele seja o primeiro participante a entrar nela.

Dois cenários que ilustram a necessidade desses dois mecanismos diferentes para se definir o moderador são: uma sala de aula virtual, onde o professor deve sempre ser o moderador e uma sala virtual de conferência onde os alunos podem discutir livremente entre si.

Um terceiro mecanismo, opcional, poderia fazer com que o participante com a posse da palavra seja um moderador com poderes limitados somente para definir quem será o próximo participante a ter a posse da palavra. Os participantes seriam admitidos automaticamente na conferência e não poderiam ser expulsos pelo moderador.

3.2.3 Requisitos funcionais do gerenciamento do sistema

O gerenciamento do sistema deve ser realizado por um usuário do sistema com o papel de administrador. O administrador do sistema pode:

- Criar, listar, modificar e excluir usuários;
- Criar, listar, modificar, excluir, monitorar, iniciar e terminar salas virtuais de conferência;
- Associar e desassociar usuários a salas virtuais de conferência.

Para se realizar uma conferência, deve ser necessário antes iniciar uma sala virtual de conferência.

A capacidade de monitorar uma sala virtual de conferência deve simplesmente informar se ela está iniciada ou não e, em caso positivo, deve informar quantos participantes estão presentes nela.

O sistema deve permitir a um novo usuário cadastrar-se e posteriormente alterar seus dados no sistema.

3.2.4 Requisitos funcionais da base de dados do sistema

A base de dados deve conter somente informações estáticas a respeito de usuários, salas e cadeiras virtuais reservadas de usuários. Informações dinâmicas, como os estados dos participantes dentro de uma conferência ou o texto trocado entre eles, devem ser armazenadas em variáveis voláteis, que devem ser destruídas quando a sala virtual de conferência for terminada.

Deseja-se armazenar o seguinte conjunto de informações estáticas a respeito do usuário do sistema:

- Nome;
- *Login* e senha;
- Apelido;
- E-mail;
- Telefone;
- Imagem ativo e imagem inativo, para representá-lo na conferência.
- Data de nascimento;
- Sexo;
- Nacionalidade;
- Endereço residencial;
- Empresa onde trabalha.

Com relação às salas virtuais de conferência, deve-se armazenar:

- Nome da sala;
- Número;

- Número de cadeiras virtuais (lotação da sala);
- Assunto da conferência;
- Política de acesso;
- Forma de representação da sala;
- Configurações de áudio (*codec* utilizado);
- Configurações de rede (portas UDP utilizadas pela sala virtual de conferência, endereço IP do servidor);
- Moderador;
- Utilização de comunicação também por texto;
- Ambiente da sala.

Uma tabela da base de dados deve armazenar o número das salas virtuais de conferência e o *login* dos usuários associados a ela.

3.2.5 Requisitos funcionais de comunicação de tempo real

Deve haver um mecanismo de controle de banda, encaminhando somente o áudio de um participante para os demais. A comunicação por texto, quando presente em uma conferência, deve estar disponível a todos os participantes.

As mensagens de controle de conferência devem ser distribuídas para todos os participantes da conferência, de forma a manter as interfaces homem-máquina deles sincronizadas.

O sistema deve permitir que conferências sejam realizadas simultaneamente, isto é, deve permitir que várias salas virtuais de conferência sejam executadas em paralelo.

Todo o tráfego de uma sala virtual de conferência deve ser completamente isolado e independente do tráfego das demais salas.

3.2.6 Integração com outros sistemas

A integração com outros sistemas deve ser realizada modificando-se o mínimo possível o funcionamento e a base de dados do sistema de conferência multiponto.

O grau de integração com outros sistemas deve depender das funcionalidades originais do sistema de conferência multiponto que forem mantidas. Os seguintes graus de integração devem ser possíveis:

- **Integração no nível de usuários:** Nesse nível de integração, o gerenciamento do sistema de conferência multiponto seria utilizado para criar as salas virtuais de conferência e o sistema externo a ele forneceria as informações a respeito dos usuários de cada sala.
- **Integração no nível de salas:** Nesse nível de integração, o gerenciamento do sistema de conferência multiponto seria utilizado para criar os usuários e o sistema externo a ele forneceria as informações a respeito de cada sala virtual de conferência.
- **Integração do nível de usuários e salas:** Nesse nível de integração, o gerenciamento do sistema de conferência multiponto não seria utilizado e o sistema externo a ele forneceria as informações a respeito das salas virtuais de conferência e dos usuários de cada sala.

A integração deve poder ser realizada acessando-se a base de dados do sistema externo ou recebendo as informações de salas ou usuários como parâmetros em requisições HTTP, visto que o sistema de conferência multiponto deve ser baseado em tecnologia *web*.

Se o conjunto de informações a respeito do usuário ou da sala virtual de conferência fornecido pelo sistema externo não for suficiente para o sistema de conferência multiponto, então as informações deverão ser completadas em uma ou mais etapas

intermediárias, antes de se iniciar a sala virtual de conferência e/ou antes de o usuário poder tomar parte em uma conferência.

3.3 Especificação técnica da comunicação de tempo real do sistema

A especificação técnica da parte de comunicação de tempo real do sistema de conferência multiponto depende da tomada de algumas decisões decorrentes dos requisitos anteriormente levantados:

- **Mecanismo de distribuição de pacotes:** IP *unicast* ou IP *multicast* (vide Capítulo 2.1.3).
- **Tipo de conferência multiponto:** Centralizada, híbrida, mista ou descentralizada (vide Capítulo 2.2).
- **Mecanismo de controle de transmissão de pacotes:** Controle de posse da palavra autônomo ou assistido (com a presença de um moderador), otimista ou pessimista, com ou sem detecção de silêncio (vide Capítulo 2.2.3).
- **Protocolo de criação e controle de conferências:** *Session Initiation Protocol* (SIP), H.323, outro protocolo de controle de conferência ou realização de conferências fracamente controladas (vide Capítulo 2.2.2).
- **Codec de áudio:** GSM, G.723.1, G.729A, G.728, etc. (vide Capítulo 2.1.1).
- **Utilização de portas:** Definição de portas UDP a serem utilizadas para cada tipo de tráfego (voz, texto e controle de conferência).

Essas questões são discutidas a seguir e estão de certa forma interligadas. A escolha do mecanismo de distribuição de pacotes afeta a escolha do tipo de conferência e vice-versa. Independentemente do tipo de conferência utilizado, o uso de um mecanismo de controle de transmissão de pacotes dos participantes é extremamente benéfico, fazendo com que somente um participante da conferência transmita seu áudio por vez. Com isso, o nível de interatividade da conferência é reduzido, mas a

natureza assimétrica de conversação do paradigma da sala de aula virtual comporta essa situação.

3.3.1 Mecanismo de distribuição de pacotes

Embora o IP *multicast* pareça ser o melhor mecanismo de transporte para conferências pelo fato da origem transmitir um único pacote, independentemente do número de receptores, nem sempre é possível utilizá-lo, porque os seguintes pré-requisitos são necessários:

- Os equipamentos de rede por onde passam os pacotes da conferência precisam suportar tráfego IP *multicast* e serem configurados para isso;
- O sistema operacional do terminal precisa oferecer suporte a IP *multicast*;
- O *software* de conferência precisa implementar a comunicação por IP *multicast*;
- Conferências globais precisam requisitar um endereço IP *multicast* válido globalmente à *Internet Assigned Numbers Authority* (IANA) (IANA, 2003), de difícil obtenção (IANA, 2000).

Entretanto, sempre é possível utilizar o IP *unicast* como mecanismo de distribuição de pacotes. O IP *unicast* não possui nenhuma dessas restrições e, em uma conferência multiponto centralizada, a banda de transmissão e de recepção de cada participante é igual à banda quando se utiliza o IP *multicast*, independentemente do número de participantes, porque para os participantes desse tipo de conferência há somente um *stream* de áudio de saída e/ou um de entrada. A grande desvantagem do IP *unicast* é a banda do elemento centralizador (vide Capítulo 2.2.1.2).

3.3.2 Tipo de conferência multiponto

A conferência descentralizada utilizando IP *unicast*, em uma configuração *full-mesh*, é inviável, porque cada participante transmitiria para todos os outros, utilizando a banda da rede da forma mais ineficiente possível e obrigando cada participante a possuir uma banda elevada de transmissão e de recepção, proporcional ao número de participantes da conferência.

A conferência descentralizada utilizando IP *multicast* é uma solução atraente, mas depende dos pré-requisitos citados para esse mecanismo de distribuição.

A conferência híbrida e a mista necessitam dos pré-requisitos do IP *multicast*.

A conferência centralizada simplifica o *software* do usuário, transformando uma conferência multiponto em várias conferências ponto-a-ponto, mas depende de uma unidade de controle multiponto para distribuir os pacotes da conferência para todos os participantes. O maior problema dessa abordagem é a banda necessária à unidade de controle multiponto, que cresce quadraticamente com relação ao número de participantes na conferência se não for restringido o número de transmissores simultâneos através do uso de um mecanismo de controle de transmissão de pacotes (controle de posse da palavra). Na presença desse mecanismo, a banda de recepção da unidade de controle multiponto passa a ser igual ao de uma conferência ponto-a-ponto e a banda de transmissão passa a ser linear com relação ao número de participantes da conferência. O tráfego na unidade de controle multiponto torna-se assimétrico (vide Capítulo 2.2.1.2). A presença da unidade de controle multiponto facilita o gerenciamento do controle da conferência, centralizando-o. Fica mais simples determinar quem pode ou não participar da conferência, quem pode ou não transmitir ou receber pacotes.

Em uma solução utilizando conferência centralizada, cada sala virtual de conferência deve possuir sua própria unidade de controle multiponto associada a ela, para garantir um maior isolamento entre salas.

Se o uso do IP *multicast* não for um problema para um determinado sistema de conferência, então a conferência multiponto híbrida utilizando *stream* distribuído e controle centralizado pode ser uma boa solução, por combinar as vantagens do IP *multicast* com a centralização do controle da conferência.

3.3.3 Mecanismo de controle de transmissão de pacotes

O uso de um controle de posse da palavra assistido pessimista (vide Capítulo 2.3.1), com a presença de um moderador na conferência, é um mecanismo relativamente simples e eficaz para se determinar qual participante irá transmitir para os demais os seus pacotes de áudio e para se prevenir conflitos no uso do canal de voz.

A detecção de silêncio é custosa computacionalmente. Quando implementada na unidade de controle multiponto pode causar o chaveamento involuntário do transmissor, caso a potência de algum sinal de áudio recebido seja maior do que a do sinal do interlocutor. Quando implementada no cliente, pode causar a transmissão espúria de pacotes de áudio, caso o nível de potência do sinal de áudio ultrapasse o limiar de silêncio estabelecido.

O uso de um controle de posse de palavra autônomo permite um controle involuntário da posse da palavra, bastante democrático, mas, ao mesmo tempo, bastante inconveniente, pois o mecanismo não é suscetível ao dinamismo da conferência, não sabendo se o interlocutor acabou o que tinha para falar e quem deve ter a posse da palavra a seguir, para dar continuidade à conversa. Um mecanismo de votação dos participantes poderia auxiliar quem deve ter a palavra a seguir.

3.3.4 Protocolo criação e controle de conferências

O H.323 é extremamente poderoso, sob o ponto de vista de funcionalidades, mas sua implementação é bastante complexa, principalmente devido ao uso da notação ASN.1 PER (ITU-T, 2002c).

O SIP é mais simples, porém não há muita clareza sobre o seu funcionamento em uma conferência multiponto centralizada (ROSENBERG, SCHULZRINNE, 2002).

O uso de um protocolo de criação e controle de conferências específico e mais simples não só atende aos propósitos deste trabalho, como também confere uma maior liberdade, flexibilidade e simplicidade de desenvolvimento. Além disso, o

software do terminal do usuário também faz parte do sistema especificado, portanto, a compatibilidade com outros protocolos não é crítica. De qualquer forma, o H.323 e o SIP não possuem um mecanismo explícito para controle de posse da palavra e ele precisaria ser desenvolvido.

3.3.5 *Codec de áudio*

O *codec* de áudio G.711, por exemplo, não pode ser usado em uma conferência por um participante que possua uma conexão com a Internet por acesso discado pela banda disponível ser insuficiente (vide Capítulo 2.1.1). No entanto, uma conferência sendo realizada dentro da *intranet* de uma empresa pode usá-lo, tirando proveito da sua melhor qualidade subjetiva comparada aos demais *codecs* de voz. Em uma conferência centralizada, onde a unidade de controle multiponto faz a distribuição do canal de áudio recebido para os demais participantes, a banda ocupada pelo *codec* possui um impacto ainda maior, pois qualquer diferença entre a taxa de transmissão de dois *codecs* diferentes é multiplicada pelo número de canais transmitidos e recebidos por ela. Portanto, a escolha do *codec* de áudio a ser utilizado depende da banda disponível para cada cliente e da forma como o canal de áudio será distribuído entre os participantes.

Para que a aplicação seja verdadeiramente independente de *codec* de áudio, mixagem e transcodificação não serão realizadas pela unidade de controle multiponto.

3.3.6 *Utilização de portas UDP e portas base*

Deve haver um número suficiente de portas para os tráfegos de áudio, texto e controle de conferência. O canal de áudio utiliza duas portas UDP, uma para o *Real-Time Transport Protocol* (RTP) *Real-Time Transport Protocol* (RTP) (SCHULZRINNE et al., 1996) e outra para o *RTP Control Protocol* (RTCP) (SCHULZRINNE et al., 1996). O tráfego de controle de conferência pode ser separado em controle de sessão e controle de posse da palavra, mas ambos podem

multiplexar a mesma porta UDP. Pode-se utilizar uma porta UDP exclusiva ou multiplexar a porta de controle de conferência para a comunicação por texto. Portanto, para uma conferência com comunicações por voz e texto, com controle de sessão e de posse da palavra são necessárias de três a seis portas UDP. A utilização de vídeo obrigaria no uso de mais duas portas UDP (uma para o RTP, outra para o RTCP) e a conferência precisaria de cinco a oito portas UDP.

Para facilitar o gerenciamento do uso de portas UDP, será definida uma faixa de dez portas UDP para cada sala virtual de conferência e cada faixa começará em uma porta múltipla de dez. A porta que define o início da faixa recebe o nome de *porta base*.

3.3.7 Apresentação e justificativa da solução adotada para a comunicação de tempo real

O sistema de conferência multiponto será implementado usando a topologia centralizada, com IP *unicast* e tendo uma unidade de controle multiponto para cada sala virtual de conferência.

Um mecanismo de controle de posse da palavra assistido (com a presença de um moderador) e pessimista (evitando conflitos do uso de canal de voz) será implementado, por ser uma forma simples e eficiente de se obter o resultado desejado: restringir a banda consumida e regular a conversação na conferência. Para isso, um protocolo de controle de conferência com controle de sessão e de posse da palavra será desenvolvido.

A não utilização do SIP e do H.323 foi decidida para simplificar o desenvolvimento da unidade de controle multiponto e do *software* do terminal do usuário. Porém, ambos podem suportar futuramente tanto o SIP quanto o H.323.

O protocolo de controle de conferência será o responsável por garantir o sincronismo de informações das interfaces homem-máquina dos participantes em uma conferência, de forma que eles todos tenham a mesma visão dos acontecimentos dentro dela.

A unidade de controle multiponto só encaminhará os pacotes de áudio do participante da conferência a quem for concedida a posse da palavra. Os pacotes de controle de conferência e de texto serão, normalmente, encaminhados para todos os participantes.

O transporte dos pacotes de áudio será feito sobre RTP, enquanto um tipo de pacote do protocolo de controle de conferência será utilizado para se transportar os pacotes do *chat* de texto, multiplexando a porta UDP de controle de conferência.

A unidade de controle multiponto não realizará mixagem, nem transcodificação, garantindo a independência de *codecs*, e será implementada em *software*.

A conferência multiponto centralizada associada ao uso do IP *unicast* é uma solução viável e universal, porque atende a ambientes sem suporte a *multicast* e não necessita um endereço IP *multicast* global.

3.3.8 Análise crítica da solução adotada para a comunicação de tempo real

Para um sistema de conferência multiponto, a escalabilidade está relacionada ao número máximo possível de participantes em uma conferência e relacionada ao número máximo de conferências simultâneas. Os dois fatores limitantes para a escalabilidade da solução adotada são a banda de transmissão da unidade de controle multiponto e o seu desempenho.

Duas medições podem ser utilizadas para se avaliar o desempenho de uma unidade de controle multiponto. A primeira medição informa o tempo que a unidade de controle multiponto leva para começar a encaminhar os pacotes RTP a partir do instante em que ela recebeu um pacote RTP. A segunda medição verifica o número de pacotes RTP que ela consegue encaminhar (número de participantes que ela consegue servir) até que ela receba o próximo pacote RTP.

Os *codecs* de áudio mais utilizados transmitem pacotes igualmente espaçados no tempo, sendo que o intervalo entre dois pacotes consecutivos costuma estar entre 20 e 50 ms, resultando em 20 a 50 pacotes por segundo sendo recebidos. Portanto, a

unidade de controle multiponto possui apenas alguns milissegundos para transmitir os pacotes para os demais participantes.

O desempenho da unidade de controle multiponto depende de vários fatores: implementação em *hardware* ou em *software*, eficiência da implementação do seu próprio código fonte, desempenho do sistema operacional, processador utilizado, quantidade de memória disponível, tempo de processador disponível para a unidade de controle multiponto, prioridade do processo e desempenho da interface de rede, entre outros.

A implementação em *software* da unidade de controle multiponto confere uma maior flexibilidade e reduz os custos de desenvolvimento em relação a uma unidade de controle multiponto em *hardware*.

A banda de transmissão da unidade de controle multiponto do sistema proposto crescerá proporcionalmente ao número de participantes na conferência, devido ao uso do IP *unicast* como mecanismo de transmissão. Uma versão futura do sistema poderia utilizar unidades de controle multiponto distribuídas, mais próximas aos usuários, atenuando o problema da banda.

Entre a banda de transmissão e o desempenho da unidade de controle multiponto, a banda disponível será o principal fator limitante para a sua escalabilidade na maioria das situações. Para um *codec* de áudio genérico ocupando 25 kbps por canal, incluindo o *overhead* dos protocolos RTP, UDP, IP e da camada de enlace, a unidade de controle multiponto precisaria de uma banda de transmissão de pelo menos 250 kbps para atender a 10 participantes remotos. Se todos os usuários estiverem dentro de uma rede local, o desempenho da unidade de controle passa a ser o fator limitante do número de participantes. De qualquer forma, uma conferência centralizada com centenas de participantes pode tornar-se complexa para o moderador gerenciar.

Alguns testes com a unidade de controle multiponto serão realizados e relatados, para se avaliar o número máximo de participantes em uma conferência para um computador com uma certa configuração (processador, memória, sistema operacional, etc.), embora um estudo profundo sobre a escalabilidade do sistema não faça parte do escopo deste trabalho.

3.4 Especificação técnica do controle de sessão e de posse da palavra

Os aspectos de sistema e de usuário para os controles de sessão e de posse da palavra são especificados a seguir.

3.4.1 Aspectos relacionados ao sistema

Os controles de sessão e de posse da palavra deverão ser implementados como um único protocolo de controle de conferência, por apresentarem várias características semelhantes, como a necessidade de serem distribuídos para todos os participantes e a diferenciação entre pacotes do moderador e do participante comum.

Os pacotes de controle utilizarão o UDP como protocolo de transporte, para facilitar o uso futuro de IP *multicast*.

3.4.1.1 Classificação do mecanismo de controle de posse da palavra

O sistema desenvolvido empregará o mecanismo de controle de posse da palavra assistido (vide Capítulo 2.3.1), com um dos participantes da conferência no papel de moderador da mesma e os demais, no papel de participantes comuns.

3.4.1.2 Políticas e mecanismos de controle de sessão e de posse da palavra

Como o mecanismo de controle de posse da palavra será assistido e não autônomo, a política de concessão da posse da palavra será subjetiva e implícita (vide Capítulo 2.3.1). Qualquer participante pode requisitar a posse da palavra e o moderador pode concedê-la a quem ele desejar, sem obedecer alguma regra pré-determinada.

Deverão ser implementados nas salas virtuais de conferência duas variantes do mecanismo de controle de posse da palavra (a terceira variante é opcional):

- **Moderador fixo:** Um usuário pré-determinado é definido como moderador da sala. Exemplo de uso: o professor na sala de aula virtual.
- **Moderador flexível:** O primeiro usuário que entrar na sala de conferência torna-se o moderador. Se o moderador abandona a sala, o próximo usuário que pedir para entrar nela torna-se o moderador. Exemplo de uso: uma sala virtual de conferência para os alunos se reunirem e discutirem a respeito da matéria, sem a presença do professor ou mesmo para professores se reunirem.
- **Moderador dinâmico (opcional):** O usuário que está com a posse da palavra torna-se o moderador. O mesmo exemplo do moderador flexível aplica-se nesse caso, mas o mecanismo de moderador dinâmico confere menos formalidade, maior interatividade e igualdade para os participantes. A versão inicial do sistema não implementará esse mecanismo.

O moderador deve sempre receber a posse da palavra ao entrar na sala.

Nos mecanismos de moderador fixo e flexível, quando o moderador abandonar a conferência, os demais participantes devem abandoná-la também, porque a unidade de controle multiponto não implementará controle de posse da palavra de forma autônoma. O moderador deverá poder, no entanto, eleger outro moderador antes de abandonar a conferência, para que ela não precise ser encerrada. Se o participante com a posse da palavra abandonar a conferência, a posse da palavra deve retornar automaticamente para o moderador. No caso do moderador dinâmico, essas mesmas situações devem ser resolvidas pela unidade de controle multiponto, determinando um novo moderador de forma aleatória ou não.

Haverá quatro tipos de salas de conferência:

- **Sala fechada:** A sala do tipo fechada precisa estar cadastrada na base de dados. Somente usuários cadastrados e associados a ela podem entrar nela. Exemplo de uso: somente usuários inscritos no curso podem participar da aula virtual.

- **Sala aberta:** A sala do tipo aberta precisa estar cadastrada na base de dados. Somente usuários cadastrados no sistema de conferência podem entrar nela. Exemplo de uso: somente usuários cadastrados no sistema podem participar da aula virtual sendo ministrada.
- **Sala livre:** A sala do tipo livre precisa estar cadastrada na base de dados. Qualquer usuário, cadastrado ou não, pode entrar nela, desde que a lotação máxima da sala virtual de conferência não tenha sido atingida. Exemplo de uso: uma aula virtual aberta a qualquer um, como atrativo para as pessoas se inscreverem nos cursos.
- **Sala temporária:** A sala do tipo temporária não precisa estar cadastrada na base de dados. Qualquer um pode entrar nela, contanto que o limite do número de usuários configurado para ela não seja ultrapassado. A sala temporária sempre utiliza o mecanismo de moderador fixo e o moderador é o usuário que a criou e quando ele a abandona, ela é destruída. Exemplo de uso: sala criada por um aluno para discutir com seus colegas sobre a matéria ministrada.

A existência de diferentes tipos de salas de conferência atende a diferentes cenários e diferentes níveis de integração com outros sistemas, oferecendo também diferentes políticas de acesso para participação em conferências. Os cenários colocados estão dentro do paradigma da sala de aula virtual, mas os diferentes tipos de sala também atendem a outros cenários mais genéricos. A sala do tipo *aberta*, por exemplo, poderia ser uma sala de *chat* exclusiva para os assinantes de um provedor de acesso à Internet. A sala do tipo *livre* poderia ser oferecida por esse mesmo provedor para qualquer visitante do seu *site*. Assinantes desse mesmo provedor poderiam criar salas do tipo *temporária* para conversar com seus amigos, assinantes ou não. Semelhantemente a um fórum de discussão, salas dos tipos *temporária* e *livre* poderiam estar associadas a notícias de um *site* ou à página de um produto.

O controle de sessão refere-se à forma pela qual os usuários do sistema são admitidos, rejeitados, expulsos ou desligados na/da sala virtual de conferência.

As salas poderão ser configuradas para admitir automaticamente os participantes que possuírem acesso a ela ou para encaminhar todo pedido de admissão ao moderador.

Somente o administrador do sistema pode criar salas virtuais de conferência.

Para usuários não cadastrados tomarem parte em conferências (em salas do tipo *livre* ou *temporária*), um conjunto mínimo de informações pessoais deverá ser passado para a sala de conferência, através do envio de um formulário HTML ou de parâmetros no *link* contendo a URL (*Uniform Resource Locator*) que leva à sala.

Os seguintes passos são necessários para um usuário participar de uma conferência em uma sala do tipo *fechada*:

1. O administrador do sistema entra no gerenciamento do sistema de conferência.
2. O administrador do sistema cria a sala do tipo *fechada*.
3. O administrador do sistema cria um ou mais usuários.
4. O administrador do sistema associa pelo menos dois usuários à sala.
5. Se a sala criada estiver configurada para utilizar o mecanismo de controle de posse da palavra com moderador fixo, o moderador deve ser escolhido pelo administrador do sistema.
6. O administrador do sistema inicia a sala virtual de conferência e a unidade de controle multiponto associada a ela.
7. O usuário (com direito de acesso) visualiza a sala virtual de conferência.
8. O usuário entra na sala virtual de conferência.

O protocolo de controle de conferência deve permitir ao participante comum e ao moderador da conferência realizar as tarefas relacionadas no Capítulo 3.2.2.3.

Os formatos dos pacotes de controle de conferência são descritos no Anexo B.

3.4.2 Aspectos relacionados ao usuário

Os aspectos do sistema relacionados ao usuário, como sua interface homem-máquina e a forma como ele interage com o sistema, como a posse da palavra é requisitada e concedida são expostos aqui.

3.4.2.1 Interface homem-máquina da sala virtual de conferência

A sala virtual de conferência será representada pelas imagens de cada participante da conferência utilizando o conceito WYSIWIS (vide Capítulo 2.3), sendo necessário manter as interfaces homem-máquina de todos os participantes sincronizadas.

A interface homem-máquina deve permitir ao participante comum e ao moderador da conferência realizar as tarefas relacionadas no Capítulo 3.2.2.3.

3.4.2.2 Indicações e representações audiovisuais

As indicações visuais do usuário serão representadas por bordas coloridas em torno da sua imagem. Indicações auditivas são importantes para chamar a atenção do usuário a mudanças na interface homem-máquina, principalmente quando a atenção dele é necessária em diferentes partes da tela. As indicações auditivas serão ouvidas pelo participante comum:

- Quando ele recebe ou perde a posse da palavra;
- Quando ele está pedindo para entrar na conferência.

As indicações auditivas serão ouvidas pelo moderador:

- Quando ele toma, recebe de volta ou concede a posse da palavra;
- Quando ele está esperando para entrar na conferência;

- Quando algum participante está pedindo para entrar na conferência.

A Tabela 3.1 mostra as indicações de controle de conferência e suas representações, enquanto a Figura 3.2 e a Figura 3.3 mostram as transições de indicação possíveis para o moderador e para o participante comum, respectivamente.

Tabela 3.1 – Indicações audiovisuais do usuário e seus significados

Indicação	Significado	Representação audiovisual
<i>Normal</i>	O participante está na conferência e não há nenhuma outra indicação mais apropriada.	Sem borda colorida. Se a indicação anterior do usuário era <i>possePalavra</i> , ele ouve um efeito sonoro indicando a perda da posse da palavra.
<i>pedindoPalavra</i>	O participante está pedindo a posse da palavra.	Borda verde.
<i>possePalavra</i>	O participante está com a posse da palavra.	Borda vermelha. O usuário ouve um efeito sonoro indicando o recebimento da posse da palavra.
<i>semInformacao</i>	O participante está com problemas de comunicação.	Borda amarela.
<i>semAudio</i>	O moderador bloqueou o encaminhamento de pacotes de áudio para o participante.	Borda azul clara.
<i>Expulso</i>	O participante foi expulso da conferência e não pode requisitar uma nova admissão nela, enquanto o moderador não liberá-lo.	Borda preta e imagem semitransparente.
<i>pedindoEntrar</i>	O participante está pedindo para entrar na conferência.	Borda azul. Na interface homem-máquina do participante pedindo para entrar é tocado um tom de chamada telefônica e na do moderador, um telefone tocando.
<i>foraConferencia</i>	O usuário está fora da conferência, mas possui uma cadeira reservada na sala.	Sem borda e imagem semitransparente.

“Qualquer indicação” na Figura 3.2 e na Figura 3.3 serve para representar uma indicação audiovisual válida qualquer e simplificar os diagramas.

Figura 3.2 – Diagrama de transição de indicações para o moderador.

Figura 3.3 – Diagrama de transição de indicações para o participante comum.

3.4.3 Análise crítica da solução adotada para o controle de sessão e de posse da palavra

A adoção de se unir o controle de sessão com o controle de posse da palavra em um único protocolo de controle de conferência visa simplificar o processamento de pacotes, reduzir a quantidade de código necessária e o reduzir o número de portas UDP.

A utilização do protocolo UDP para o transporte do controle de conferência poderá causar problemas de sincronismo entre as interfaces homem-máquina dos participantes da conferência, mas o sistema deve ser capaz de minimizar as possíveis inconsistências decorrentes da perda de pacotes de controle de conferência.

As indicações audiovisuais ajudarão na utilização do sistema de conferência e na compreensão do mecanismo de controle de posse da palavra.

3.5 Considerações finais

Esse capítulo apresentou os requisitos funcionais e técnicos para o sistema de conferência multiponto desejado.

A partir dos requisitos e do que foi apresentado no capítulo anterior, foi definida a solução para se oferecer comunicação multiponto por voz: um sistema de conferência multiponto centralizada com controle de posse da palavra assistido.

O próximo capítulo traz o sistema desenvolvido que atende aos requisitos colocados.

4. ARQUITETURA E IMPLEMENTAÇÃO DO SISTEMA

“Jesus chorou.”

João 11.35

Este capítulo apresenta a arquitetura e a implementação do sistema que atende às especificações e requisitos levantados no capítulo anterior.

Como foi definido no capítulo anterior, o sistema de conferência multiponto é centralizado (vide Capítulo 2.2), utilizando como mecanismo de distribuição de pacotes de conferência (RTP/RTCP e pacotes de controle) o IP *unicast* (vide Capítulo 2.1.3) e uma unidade de controle de conferência (vide Capítulo 2.2.1). O sistema de conferência oferece comunicação por áudio através do protocolo RTP/RTCP (vide Capítulo 2.1.2) entre os participantes de uma conferência e, adicionalmente, comunicação por texto. O sistema utiliza um protocolo de controle de conferência próprio, que implementa controle de sessão e controle de posse da palavra (vide Capítulos 2.2.2 e 2.3.1)

4.1 Arquitetura do sistema de conferência multiponto

O sistema de conferência multiponto foi organizado em quatro subsistemas: subsistema de gerenciamento, subsistema de acesso às salas virtuais de conferência, base de dados e o subsistema efetivamente responsável pela comunicação por voz em tempo real, como mostrado na Figura 4.1.

Através do subsistema de acesso às salas virtuais de conferência, os usuários visualizam as salas virtuais de conferência disponíveis e podem participar em conferências, através de uma interface homem-máquina que oferece uma representação da sala virtual de conferência e recursos multimídia para comunicação em tempo real.

Figura 4.1 – Subsistemas do sistema de conferência multiponto.

O subsistema de gerenciamento oferece recursos para o administrador do sistema gerenciar usuários e salas virtuais de conferência.

A base de dados armazena as informações a respeito dos usuários, as configurações das salas virtuais de conferência e eventuais associações de usuários a salas (cadeiras virtuais reservadas).

O subsistema de comunicação de tempo real deve permitir a comunicação dos participantes entre si, através da unidade de controle multiponto e a criação e destruição de unidades de controle multiponto, conforme as conferências são iniciadas ou terminadas pelo subsistema de gerenciamento.

O subsistema de acesso às salas virtuais de conferência está exposto aos usuários do sistema de conferência multiponto, enquanto que o subsistema de gerenciamento é acessado somente pelo administrador do sistema. Ambos são protegidos por *login* e senha, mas, inicialmente, sem a utilização de criptografia de senhas e HTTPS (HTTP over Secured Socket Layer – SSL) (RESCORLA, 2000); (FREIER, KARLTON, KOCHER, 1996) e (ALLEN, DIERKS, 1999). A base de dados e o subsistema de comunicação de tempo real são acessados pelos usuários do sistema através dos dois subsistemas mencionados anteriormente.

4.1.1 Interação entre os subsistemas

A Figura 4.2 apresenta a arquitetura do sistema de conferência multiponto, onde podem ser identificados os subsistemas descritos anteriormente, em um grau maior de detalhamento.

Figura 4.2 – Arquitetura do sistema de conferência multiponto proposto.

Toda sala e usuário criados pelo subsistema de gerenciamento são armazenados na base de dados. Quando uma sala virtual de conferência é iniciada, as suas configurações e os usuários associados a ela são carregados em variáveis voláteis que podem ser acessadas pelo subsistema de acesso às salas virtuais de conferência. Ainda quando uma sala virtual de conferência é iniciada, o subsistema de comunicação de tempo real se prepara para começar a receber o tráfego dela,

alocando os recursos necessários. Quando a sala virtual de conferência é terminada, essas variáveis voláteis são destruídas e o subsistema de comunicações de tempo real desaloca os recursos dela.

O subsistema de acesso às salas virtuais de conferência consulta a base de dados para conhecer quais salas virtuais de conferência foram criadas e acessa as variáveis voláteis para saber quais salas foram iniciadas. Somente as salas que tiverem sido iniciadas são exibidas aos usuários do sistema. Quando o usuário entra em uma sala virtual de conferência, a sua parte do subsistema de comunicação de tempo real é iniciada, alocando os recursos de comunicação multimídia e de rede. Quando o usuário sai de uma sala virtual de conferência, os recursos de comunicação multimídia e de rede são desalocados.

4.2 Implementação do sistema de conferência multiponto

O sistema de conferência multiponto, desenvolvido segundo os requisitos levantados no capítulo anterior, é descrito mais detalhadamente a seguir, juntamente com sua implementação e arquitetura.

A Figura 4.3 mostra a implementação da arquitetura descrita anteriormente. O sistema de conferência multiponto proposto é implementado pelos elementos:

- **Servidor de banco de dados:** É responsável pelo subsistema da base de dados. Armazena as configurações das salas virtuais de conferência, as informações a respeito dos usuários e as associações entre usuários e salas.
- **Servidor *web*:** Engloba os subsistemas de gerenciamento e de acesso às salas virtuais de conferência. Como um dos requisitos do sistema de conferência é a utilização de tecnologia *web*, o subsistema de gerenciamento foi implementado através de um *site* de gerenciamento, enquanto que o subsistema de acesso às salas virtuais de conferência foi implementado através de um *site* de conferência, que são hospedados neste servidor. O *site* de gerenciamento é restrito ao administrador do sistema, e permite a ele gerenciar os usuários do sistema e as

salas virtuais de conferência. O *site* de conferência permite aos usuários visualizar as salas virtuais de conferência disponíveis e acessá-las.

- **Servidor de unidades de controle multiponto:** Faz parte do subsistema de comunicação de tempo real. Cada servidor de unidades de controle multiponto gerencia uma ou mais unidades de controle multiponto. O servidor de unidades multiponto recebe requisições HTTP do servidor *web* (*site* de gerenciamento) para iniciar e terminar as unidades de controle multiponto associadas a cada sala virtual de conferência. A resposta à requisição é enviada ao servidor *web* utilizando HTTP, com dados em XML informando se a ação foi bem sucedida ou não. O sistema de conferência poderá ter múltiplos servidores de unidades de controle multiponto espalhados pela rede, para aumentar a sua escalabilidade.
- **Unidade de controle multiponto (MCU):** Faz parte do subsistema de comunicação de tempo real. Cada unidade de controle multiponto está associada a somente uma sala virtual de conferência e estabelece comunicações ponto-a-ponto com cada participante da conferência virtual, provendo comunicação entre todos os participantes dela, encaminhando os pacotes RTP/RTCP e os pacotes de controle de conferência (controle de sessão e controle de posse da palavra). Internamente, a unidade de controle multiponto é composta por um controlador multiponto (MC) e por um processador multiponto (MP). O controlador multiponto trata e encaminha os pacotes de controle de conferência, enquanto que o seu processador multiponto lida com os pacotes RTP/RTCP de áudio.
- **Página *web* do usuário:** Faz parte do subsistema de acesso às salas virtuais de conferência. A página *web* do usuário é carregada a partir do servidor *web* e oferece a interface homem-máquina e a representação da sala virtual de conferência para o usuário.
- ***Applet* Java do usuário:** Faz parte do subsistema de comunicação de tempo real. A *applet* Java fica embutida na página *web* do usuário e comunica-se com a unidade de controle multiponto. Ela oferece captura, codificação, decodificação e reprodução de áudio, além de transmissão e recepção de pacotes RTP/RTCP e de controle de conferência.

Figura 4.3 – Implementação da arquitetura do sistema de conferência proposto.

Relacionando a arquitetura do sistema de conferência da Figura 4.2 com a sua implementação, apresentada na Figura 4.3, podemos fazer as seguintes associações:

- Base de dados
 - Servidor de banco de dados
- Subsistema de gerenciamento
 - Servidor *web* (*site* de gerenciamento)
- Subsistema de acesso às salas virtuais de conferência
 - Servidor *web* (*site* de conferência)
 - Página *web* do usuário
- Subsistema de comunicação de tempo real
 - Servidor de unidades de controle multiponto
 - Unidade de controle multiponto

➤ *Applet* Java do usuário

A implementação do sistema de conferência é baseada na arquitetura cliente-servidor. Pelo lado do servidor, o sistema de conferência é composto pelo servidor *web*, pelo servidor da base de dados, pelos servidores de unidades de controle multiponto e pelas unidades de controle multiponto. Pelo lado do cliente, o sistema é composto pela página *web* e pela *applet* Java do usuário.

4.3 Detalhamento da implementação do sistema

Os servidores *web* e de banco de dados foram implementados em Microsoft Internet Information Services 5.0 (MICROSOFT, 2000b), utilizando Active Server Pages 3.0 (ASP) (MICROSOFT, 1999), e em Microsoft SQL Server 2000 (MICROSOFT, 2000d), respectivamente, hospedados no sistema operacional Microsoft Windows 2000 Server (MICROSOFT, 2000a), por serem *softwares* amplamente utilizados.

As páginas *web* foram desenvolvidas tendo como base o *browser* Microsoft Internet Explorer versão 5.5 ou superiores (MICROSOFT, 2000d), porque são os *browsers* bastante populares. Devido às particularidades de outros *browsers*, a compatibilidade do sistema com eles depende de ajustes em alguns trechos do código em HTML (NETSCAPE, 1998a) e (W3C, 2003a), JavaScript (NETSCAPE, 1998b) e (MICROSOFT, 2003b) e HTML dinâmico (DHTML) (MICROSOFT, 2003a).

A unidade de controle multiponto foi implementada utilizando a linguagem Java (SUN, 2003b) versão 1.4.2 da Sun Microsystems (SUN, 2003a), por ser aberta e pela sua portabilidade.

A linguagem Java foi escolhida também para a implementação da comunicação de tempo real embutida na interface homem-máquina do usuário através de uma *applet* Java, pela disponibilidade da biblioteca gratuita chamada Java Media Framework (JMF) (SUN, 2003c), que facilita a implementação de tráfego multimídia sobre redes IP em tempo real, por implementar tanto o RTP/RTCP (SCHULZRINNE et al., 1996) quanto à parte de captura, codificação, decodificação e reprodução de áudio e

vídeo. A *applet* Java do usuário foi implementada utilizando linguagem Java 1.4.2 e a biblioteca Java Media Framework 2.1.1e.

A implementação de cada um dos subsistemas é descrita a seguir.

4.3.1 Base de dados

A base de dados foi implementada em um banco de dados relacional. Através das informações contidas na base de dados, as salas virtuais de conferência são carregadas e construídas. As tabelas da base de dados guardam somente informações estáticas sobre as salas de conferência e sobre os usuários (vide Capítulo 3.2.4) e possíveis associações entre usuários e salas (cadeiras virtuais reservadas). Informações dinâmicas, como o número atual de participantes na conferência e o estado de um participante dentro de uma sala de conferência, são armazenadas em variáveis de aplicação do servidor *web*.

O Anexo A traz informações mais completas a cerca da base de dados do sistema de conferência.

4.3.2 Subsistemas de gerenciamento e de acesso às salas virtuais de conferência

Os subsistemas de gerenciamento e de acesso às salas virtuais de conferência são compostos pelos *sites* de gerenciamento e de conferência, respectivamente.

O acesso ao sistema de conferência dá-se através de uma página *web*, onde o usuário pode escolher entre ir para o *site* de gerenciamento ou para o *site* de conferência. Na versão atual do sistema, somente o administrador do sistema possui acesso ao *site* de gerenciamento. Se o usuário não estiver cadastrado no sistema, é oferecida a ele a oportunidade de fazê-lo. O usuário não cadastrado também pode participar de conferências, desde que estas não imponham restrição quanto aos participantes.

4.3.2.1 Funcionalidades oferecidas

O *site* de gerenciamento foi projetado para ser monousuário, isto é, há somente uma única conta de administrador do sistema. No entanto, um usuário pode se cadastrar no sistema e posteriormente alterar seus dados.

No *site* de gerenciamento, os usuários podem ser pelo administrador:

- Criados;
- Listados;
- Modificados;
- Apagados;
- Associados e desassociados a salas de conferência.

As salas podem ser:

- Criadas;
- Listadas;
- Modificadas;
- Apagadas;
- Monitoradas;
- Iniciadas e finalizadas.

Quando uma sala é iniciada, sua configuração e associação de usuários são carregadas da base de dados para variáveis de aplicação do servidor *web* e a sua unidade de controle multiponto é iniciada, enviando-se uma requisição HTTP com a ação desejada para o servidor de unidades de controle multiponto, que responde, em

formato XML (*Extensible Markup Language*) (W3C, 2003b), o resultado da ação solicitada. Quando a configuração de uma sala é alterada na base de dados, ela só se torna ativa na próxima vez que a sala de conferência for iniciada.

Quando uma sala é finalizada no subsistema de gerenciamento, as variáveis de aplicação referentes a ela no servidor *web* são destruídas e a sua unidade de controle multiponto associada é terminada, enviando-se uma requisição HTTP com a ação desejada para o servidor de unidades de controle multiponto. As informações do banco de dados permanecem inalteradas.

A sala virtual de conferência só deve ser finalizada no subsistema de gerenciamento após o término da conferência. Se uma sala virtual de conferência for finalizada enquanto a conferência estiver em andamento, os resultados podem ser imprevisíveis, porque no decorrer da conferência as interfaces homem-máquina dos participantes podem tentar acessar e modificar as variáveis de aplicação que foram destruídas. Essa situação está sendo tratada, mas é recomendável terminar a conferência antes de finalizá-la.

O *site* de conferência oferece ao usuário acesso às salas de conferência às quais ele possui permissão de acesso e a possibilidade de modificar seus dados pessoais. O *site* de conferência é responsável por obter as informações do usuário para a página *web* da sala de conferência.

4.3.2.2 Informações dinâmicas dos subsistemas de gerenciamento e de acesso às salas virtuais de conferência

As informações dinâmicas dos subsistemas de gerenciamento e de acesso às salas virtuais de conferência são armazenadas em variáveis de aplicação no servidor *web* e são utilizadas pelos seus respectivos *sites*. As principais informações dinâmicas são:

- **Salas virtuais de conferência iniciadas:** Para cada sala virtual de conferência iniciada, há uma variável de aplicação correspondente contendo uma estrutura de dados com informações trazidas a partir da base de dados.

- **Participantes da sala:** Cada sala de conferência possui uma estrutura de dados associada a ela, informando quem está participando da conferência virtual em andamento e o seu estado com relação ao controle de posse da palavra.

4.3.2.3 Segurança nos *sites* do sistema

A segurança nos *sites* do sistema foi implementada somente com *logins* e senhas em texto plano, sem a utilização de criptografia. Como a versão atual do *site* de gerenciamento é monousuário, a senha e o *login* do administrador do sistema são armazenados em um arquivo de configuração do próprio *site* do sistema. As senhas dos usuários do sistema são armazenadas na base de dados, juntamente com as demais informações relativas a eles. A versão atual do sistema não utiliza HTTPS (HTTP sobre *Secured Socket Layer* – SSL) (RESCORLA, 2000); (FREIER, KARLTON, KOCHER, 1996) e (ALLEN, DIERKS, 1999), mas sua utilização não demandaria alterações muito significativas. Uma vez que o *site* de conferências esteja utilizando HTTPS, pode-se distribuir chaves de criptografia através da página *web* da sala de conferência de cada usuário para eles criptografarem seus canais de áudio e de controle.

Cabe ao *site* de conferência assegurar que as cadeiras reservadas em salas virtuais de conferência sejam ocupadas somente pelos seus donos e que a lotação máxima da sala seja respeitada, porque essas informações não são passadas para a unidade de controle multiponto.

4.3.2.4 Página *web* do usuário e sala virtual de conferência

A página *web* do usuário representa a sala virtual de conferência propriamente dita, contém a interface homem-máquina e oferece recursos de comunicação de rede, captura e reprodução de áudio através da *applet* Java.

A página *web* do usuário é construída a partir das informações armazenadas nas variáveis de aplicação do servidor *web* sobre a sala virtual de conferência e sobre o usuário. A página *web* utiliza HTML (NETSCAPE, 1998a) e (W3C, 2003a), DHTML (MICROSOFT, 2003a) e JavaScript (MICROSOFT, 2003b) e (NETSCAPE, 1998b) para fazer a representação audiovisual da sala e disponibilizar para o usuário controles para participação em uma conferência.

As informações essenciais a respeito do usuário e da sala que são passadas para a página *web* do usuário são:

- **Sala:** número.
- **Usuário:** nome, e-mail, telefone, apelido, *login*, senha, imagem ativo e imagem inativo.

Se o sistema de conferência estiver sendo utilizado de forma independente, essas informações são passadas de forma automática. Se o sistema de conferência estiver sendo utilizado de forma integrada com outro sistema, usando uma base de dados externa e essas informações não estiverem disponíveis nela, elas precisam ser obtidas através de páginas *web* adicionais (vide Capítulo 4.3.2.5 mais adiante).

Os aspectos da interface homem-máquina da sala virtual de conferência relacionados ao controle de posse da palavra e de conferência são apresentados mais adiante neste trabalho. Fora esses aspectos, a sala virtual de conferência pode ser representada de três formas distintas:

- **Janela inteira:** A página *web* ocupa toda a tela disponível para o usuário (Figura 4.4). Essa forma é recomendada quando o sistema de conferência estiver sendo utilizado independentemente de outros sistemas ou quando for utilizado também o *chat* de texto.
- **Janela mínima:** A página *web* ocupa o mínimo de espaço possível (Figura 4.5). Essa forma é recomendada quando o sistema de conferência estiver sendo

utilizado como ferramenta de apoio a outros sistemas, com o usuário necessitando visualizar outras janelas simultaneamente.

- **Janela flutuante:** A página *web* ocupa apenas uma parte da janela (Figura 4.6). Essa forma é recomendada para as mesmas situações da *janela mínima*.

Figura 4.4 – Interface homem-máquina do tipo *janela inteira*.

Figura 4.5 – Interface homem-máquina do tipo *janela mínima*.

Figura 4.6 – Interface homem-máquina do tipo *janela flutuante*.

A interface homem-máquina oferece controles de volume para o microfone e para o alto-falante do usuário. Quando a sala está configurada para utilizar também comunicação através de *chat* de texto, a interface homem-máquina disponibiliza uma área para digitação do texto e uma área para a visualização das mensagens recebidas, com identificação do usuário que a transmitiu e o horário de transmissão da mesma. Essas informações são adicionadas à mensagem digitada antes do seu envio pela *applet* Java. A área de visualização das mensagens recebidas pode ser ocultada temporariamente, mas a área de digitação, não.

A página *web* do usuário comunica-se com a *applet* Java através do JavaScript e vice-versa. Comandos disparados pelo usuário na interface homem-máquina são recebidos e transformados em ações apropriadas pela *applet* Java e pacotes recebidos da rede pela *applet* Java são refletidos apropriadamente na interface homem-máquina. Por exemplo, o usuário pode diminuir o volume do seu microfone e do seu alto-falante através da interface homem-máquina, e quem executa tais tarefas é a *applet* Java. O usuário pode, também, deixar o seu microfone mudo através da sua interface homem-máquina. Se ele estiver com a posse da palavra, a *applet* Java não transmitirá nenhum pacote de áudio até que o seu microfone seja desbloqueado.

A determinação do moderador da sala virtual depende do mecanismo de moderação sendo utilizado. Dependendo do mecanismo utilizado, o moderador pode ser o primeiro participante a entrar na sala virtual de conferência (*moderador flexível*) ou um participante pré-determinado (*moderador fixo*) (vide Capítulo 3.4.1.2).

A informação a respeito do moderador da sala é obtida pela página *web* a partir da variável de aplicação do servidor *web* que armazena informações sobre a sala. A página *web* informa para a *applet* Java qual o papel do participante na conferência, se de moderador ou se de participante comum. Se já houver um moderador na conferência e a *applet* Java, por engano, tentar entrar nela como moderador, a unidade de controle multiponto informa a *applet* Java quem é o atual moderador, e ela passa a operar como se o participantes fosse um participante comum.

A sala virtual de conferência pode ainda ser representada através da metaforização de ambientes geográficos. De acordo com o ambiente selecionado para a sala no *site* de gerenciamento, essa sala possuirá, ao fundo, uma imagem e efeitos sonoros característicos. A versão atual do *site* de gerenciamento não permite a adição ou personalização de ambientes, mas traz os ambientes pré-definidos mostrados na Tabela 4.1. Essa funcionalidade pode ser interessante para sistemas de ensino a distância direcionados a crianças, por exemplo.

Tabela 4.1 – Ambientes disponíveis para as salas virtuais de conferência

Ambiente	Observação
Nenhum	A sala não possui nenhum esquema de ambiente definido.
Selva	A sala possui a imagem de fundo de uma selva e ruídos de animais.
Praia	A sala possui a imagem de fundo de uma praia e ruídos de ondas.
Porto	A sala possui a imagem de fundo de um porto e ruídos de gaivotas e apitos de navios.
Espaço	A sala possui a imagem de fundo de uma estação espacial e efeitos sonoros típicos de filmes de ficção científica.
Tempestade	A sala possui a imagem de fundo de uma tempestade e ruídos de trovões.
Estádio	A sala possui a imagem de fundo de um estádio de futebol e ruídos típicos de uma torcida.
Aplausos	A sala não possui imagem de fundo, somente ruídos de aplausos.

A Figura 4.7 mostra uma sala virtual de conferência configurada para reproduzir o ambiente de um porto.

Figura 4.7 – Sala virtual de conferência ambientada em um porto.

4.3.2.5 Modos de integração com outros sistemas

O sistema foi desenvolvido para ser um sistema independente, possuindo uma base de dados própria e completa autonomia. A integração com outros sistemas de ensino a distância ou qualquer outro sistema onde se aplique o paradigma de uma sala virtual de conferência com a presença de um moderador pode ser feita das seguintes formas:

- **Alimentação da base de dados do sistema a partir de dados externos:** A base de dados do sistema de conferência é conhecida e pode ser preenchida com dados externos da base do sistema ao qual se deseja integrar. Nesse caso, é necessário: assegurar a compatibilidade dos tipos de dados de cada campo das tabelas; preencher com informações válidas os campos obrigatórios, mas inexistentes na

base de dados externa e sincronizar as informações sempre que houver mudanças na base de dados externa, como a exclusão de um usuário. Geralmente, os dados a respeito dos usuários, como informações para contatos pessoais e identificação única, são comuns, mesmo em sistemas diferentes. A principal vantagem desse modo de integração é a ausência de alterações no sistema de conferência. Por outro lado, a principal desvantagem é a necessidade de se atualizar a base de dados do sistema de conferência sempre que a base de dados do sistema externo sofrer alteração.

- **Uso de base de dados externa:** Nesse caso, o sistema de conferência precisa ser modificado para importar dados de uma base de dados externa toda vez que a sala for iniciada. A base de dados do sistema de conferência não seria utilizada, nem o subsistema de gerenciamento. Portanto, as ações de iniciação e término das salas e das unidades de controle multiponto precisam ser executadas em lugar do subsistema de gerenciamento. Cada sistema diferente exigiria diferentes modificações no sistema de conferência para se realizar a integração. A vantagem desse modo de integração é a existência de apenas uma base de dados, evitando a necessidade de sincronizá-las quando uma das bases for alterada. A desvantagem é a necessidade de se alterar o sistema de conferência de forma a compatibilizá-lo com o sistema externo. Algumas páginas *web* para obtenção das informações obrigatórias foram desenvolvidas para facilitar esse modo de integração.
- **Criação de um subsistema de gerenciamento específico:** Um subsistema de gerenciamento específico para o sistema externo em questão seria criado. A vantagem desse modo de integração é a total personalização do sistema de conferência multiponto de acordo com as características do sistema externo. A grande desvantagem é a necessidade de alterações profundas no sistema de conferência multiponto, desviando-se dos requisitos levantados no Capítulo 3.2.6.

Independentemente do modo de integração, algumas informações certamente não estarão disponíveis previamente na base de dados do sistema externo, como as portas UDP da unidade de controle multiponto e o *codec* de áudio a ser utilizado, por serem informações extremamente particulares do sistema de conferência multiponto. Dessa

forma, essas informações precisam ser fornecidas em algum momento para que se possa realizar uma conferência.

As partes vitais do sistema de conferência são a página *web* que representa a sala de conferência, a *applet* Java embutida nela, as variáveis de aplicação utilizadas para a construção da página e a integração da unidade de controle multiponto com as informações e o estado da sala. Assegurando-se que as informações essenciais a respeito do usuário e da sala estejam disponíveis e que a unidade de controle multiponto seja iniciada e terminada juntamente com a sala, não importa qual a forma de integração optada.

4.3.3 Subsistema de comunicação de tempo real

O subsistema de comunicação de tempo real é composto pelos servidores de unidades de controle multiponto, pelas unidades de controle multiponto e pela *applet* Java embutida na página *web* do usuário.

A escolha da linguagem Java para a implementação do servidor de unidades de controle multiponto e da unidade de controle multiponto foi feita pela sua portabilidade. Como o servidor de unidades de controle multiponto foi implementado em Java, ele pode ser hospedado transparentemente em servidores Linux, Unix, Apple, Sun e outros, embora ele apenas tenha sido testado em servidores com sistema operacionais Microsoft Windows 2000 Server e Windows XP.

As linguagens C e C++ também poderiam ser utilizadas para a implementação do servidor de unidades de controle multiponto e da unidade de controle multiponto. Ganharia-se em desempenho, mas perderia-se a portabilidade.

Conferências onde a maior parte dos usuários estão localizados fora da rede da unidade de controle multiponto tem como gargalo principal do sistema de conferência a banda de transmissão disponível para a unidade de controle multiponto e não o desempenho dela. Como a arquitetura proposta para o sistema de conferência multiponto permite que os servidores de unidades de controle multiponto sejam

distribuídos pela rede, a questão do desempenho da implementação da unidade de controle multiponto tem sua importância reduzida.

4.3.3.1 O servidor de unidades de controle multiponto

O servidor de unidades de controle multiponto é o responsável pela comunicação entre uma ou mais unidades de controle multiponto com o *site* de gerenciamento do sistema. O sistema de conferência permite que mais de um servidor de unidades de controle multiponto seja instanciado. Cada servidor de unidades de controle multiponto deve ser iniciado manualmente, sendo informada uma porta TCP, na qual são esperadas requisições HTTP vindas do *site* de gerenciamento no servidor *web*.

O servidor de unidades de controle multiponto pode estar localizado tanto no próprio servidor *web* quanto em uma máquina remota. O endereço IP e a porta TCP do servidor de unidades de controle multiponto responsável pela unidade de controle multiponto associada à sala virtual de conferência são definidos na configuração da sala virtual de conferência, no *site* de gerenciamento.

A requisição HTTP deve informar a ação desejada e o número da sala. As ações disponíveis e os parâmetros da requisição HTTP são apresentados na Tabela 4.2.

Tabela 4.2 – Ações e parâmetros das requisições HTTP enviados pelo gerenciador ao servidor de unidades de controle multiponto

Ação	Parâmetros
iniciar	<ul style="list-style-type: none"> ▪ Número da sala ▪ Nome da sala ▪ Assunto da sala ▪ Portas base UDP da <i>applet</i> Java do usuário e da unidade de controle multiponto da sala (vide Capítulos 3.3.6 e 4.3.3.4).
fechar	<ul style="list-style-type: none"> ▪ Número da sala
consultar	<ul style="list-style-type: none"> ▪ Número da sala

Quando uma sala é iniciada no subsistema de gerenciamento, uma requisição HTTP é enviada ao servidor de unidades de controle multiponto especificado (Figura 4.8), que inicia uma nova unidade de controle multiponto.

Figura 4.8 – Requisição atendida com sucesso para iniciar uma sala virtual de conferência.

Quando a sala é terminada no *site* de gerenciamento, uma requisição HTTP é enviada ao servidor de unidades de controle multiponto especificado para finalizar a unidade de controle multiponto (Figura 4.9)

Figura 4.9 – Requisição bem sucedida para se fechar a unidade de controle multiponto de uma sala virtual de conferência.

Quando a requisição HTTP estiver solicitando uma consulta e o número da sala for igual a “-1”, o servidor de unidades de controle multiponto responde um XML informando quais salas estão abertas dentro dele, como mostrado na Figura 4.10.

```

Requisição:
http://macadamia:8080/xml.asp?acao=consultar&sala=-1

Resposta XML:
<?xml version="1.0" encoding="ISO-8859-1" ?>
<salas>
  <sala id="0">
    <nome>Sala de redes de computadores</nome>
    <assunto>Tudo sobre redes de computadores</assunto>
    <status>Aberta</status>
    <moderador>admin@macauba</moderador>
    <cadeiraModerador>2</cadeiraModerador>
    <numeroParticipantes>5</numeroParticipantes>
  </sala>
  <sala id="2">
    <nome>Outra sala de redes de computadores</nome>
    <assunto>Mais ainda que tudo sobre redes de computadores</assunto>
    <status>Aberta</status>
    <moderador>admin@macadamia</moderador>
    <cadeiraModerador>1</cadeiraModerador>
    <numeroParticipantes>2</numeroParticipantes>
  </sala>
</salas>
  
```

Figura 4.10 – Consulta ao servidor de unidades de controle multiponto a respeito das salas virtuais de conferência abertas.

Quando a requisição de consulta informar um número de sala válido, o servidor de unidades de controle multiponto obtém da unidade de controle multiponto correspondente as informações a respeito dos participantes da conferência da sala em questão, como mostrado na Figura 4.11.

```

Requisição:
http://<endereço do servidor>:8080/xml.asp?acao=consultar&sala=2

Resposta XML:
<?xml version="1.0" encoding="ISO-8859-1" ?>
<sala id="2">
  <nome>Outra sala de redes de computadores</nome>
  <assunto>Mais ainda que tudo sobre redes de computadores</assunto>
  <status>Aberta</status>
  <moderador>admin@macadamia</moderador>
  <cadeiraModerador>1</cadeiraModerador>
  <numeroParticipantes>2</numeroParticipantes>
  <participantes>
    <participante id="0">
      <nome>Reinaldo Matushima</nome>
      <cadeira>0</cadeira>
      <cname>matushim@macauba</cname>
      <ssrc>654654065</ssrc>
      <status>1</status>
      <indicacao>possePalavra</indicacao>
    </participante>
    <participante id="0">
      <nome>Marcel</nome>
      <cadeira>1</cadeira>
      <cname>admin@macadamia</cname>
      <ssrc>798840605</ssrc>
      <status>1</status>
      <indicacao>normal</indicacao>
    </participante>
  </participantes>
</sala>

```

Figura 4.11 – Consulta ao servidor de unidades de controle multiponto a respeito dos participantes de uma conferência em uma determinada sala.

A interface homem-máquina do servidor de unidades de controle multiponto é meramente informativa e consiste em uma janela de console em modo texto, para minimizar o processamento necessário. Nela são mostradas as requisições HTTP recebidas pelo servidor de unidades de controle multiponto e a execução de cada ação (Figura 4.12). Também são mostradas as saídas das unidades de controle multiponto de cada sala.

```

C:\WINNT\system32\java.exe
[SocketServerMCU] Porta para servidor nao definida. Porta alocada default: 8080
[SocketServerMCU] Porta alocada para o servidor: 8080
[SocketServerMCU] Requisicao: GET /xml.asp?acao=iniciar&sala=2004&nome=Sala+2004&assunto=Sala+2004&p...
[Sala: 2004] Iniciando MCU
[Sala: 2004] Porta Base MCU:8080
[Sala: 2004] Porta Base Usuario:7000
[Sala: 2004] Trafficclass:false
[Sala: 2004] SSRC_MCU: 814136256
[Sala: 2004] MCU iniciada
[SocketServerMCU] Requisicao: GET /xml.asp?acao=fechar&sala=2004 HTTP/1.0
[Sala: 2004] MCU Finalizada

```

Figura 4.12 – A unidade de controle multiponto de uma sala virtual sendo iniciada e depois terminada.

O sistema de conferência desenvolvido aceita três tipos diferentes de abordagem para a criação de unidades de controle multiponto:

- **Abordagem multitarefa¹⁶:** Um único servidor de unidades de controle multiponto é responsável por pelo menos uma unidade de controle multiponto.
- **Abordagem multiprocesso¹⁷:** Cada servidor de unidades de controle multiponto é responsável por uma única unidade de controle multiponto.
- **Abordagem híbrida¹⁸:** Cada servidor de unidades de controle multiponto é responsável por pelo menos uma unidade de controle multiponto.

A abordagem multiprocesso é mais robusta do que a multitarefa, por haver uma maior isolamento entre as salas virtuais de conferência e permitir que as unidades de controle multiponto sejam distribuídas pela rede, em diversas máquinas. Porém, a abordagem multiprocesso ocupa mais memória e mais processamento no servidor, porque instancia novos objetos que poderiam ser comuns a todas as salas virtuais e cria processos que concorrem entre si pelo tempo do processador.

¹⁶ Em abordagens multitarefa, um único processo possui várias tarefas que compartilham o espaço de memória do processo e concorrem entre si pelo tempo de processador dele.

¹⁷ Em abordagens multiprocesso, vários processos com uma única tarefa concorrem entre si pelo tempo de processador. Cada processo é executado em um espaço de memória separado.

¹⁸ Em abordagens híbridas, há vários processos com várias tarefas sendo executados paralelamente.

A Figura 4.13 mostra as abordagens multitarefa, multiprocesso e híbrida para a execução de unidades de controle multiponto simultâneas.

Figura 4.13 – Ilustração das abordagens multitarefa (a), multiprocesso (b) e híbrida (c) para o uso de unidades de controle multiponto simultâneas.

Para se ter dois ou mais servidores de unidades de controle multiponto sendo executados em uma mesma máquina, basta especificar portas TCP diferentes para cada um deles como parâmetro de iniciação, enquanto que para se ter servidores de unidades de controle multiponto distribuídos pela rede, basta especificar endereços IP diferentes para cada um deles nas configurações da sala virtual de conferência no *site* de gerenciamento.

4.3.3.2 A unidade de controle multiponto

Cada unidade de controle multiponto é independente entre si e é iniciada e terminada pelo servidor de unidades de controle multiponto ao qual ela está associada.

Internamente, a unidade de controle multiponto é dividida em controlador multiponto e processador multiponto. O controlador multiponto trata os pacotes de controle de

conferência (controle de posse da palavra e controle de sessão), enquanto que o processador multiponto trata os pacotes RTP/RTCP.

Os canais RTP, RTCP e de controle de conferência são independentes e utilizam portas UDP diferentes (*sockets* diferentes). Cada unidade de controle multiponto possui, então, três tarefas concorrentes, uma para cada tipo de pacote.

Os *sockets* são bidirecionais (vide Capítulo 2.4.4). A utilização de *sockets* bidirecionais pela *applet* Java e pela unidade de controle multiponto é fundamental para superar os problemas causados quando o usuário se encontra atrás de um NAT (*Network Address Translators*) ou de um NAPT (*Network Address and Port Translators*), conforme exposto no Capítulo 2.4.3, porque as implementações de NAPT só costumam aceitar o tráfego entrante se o endereço IP e a porta UDP de origem do pacote corresponder ao endereço IP e à porta UDP destino do pacote interno ao NAPT que causou a tradução de porta e de endereço IP.

4.3.3.2.1 Funcionamento da unidade de controle multiponto

Quando a unidade de controle multiponto é iniciada, ela passa a esperar a recepção de pacotes de controle de sessão, de pacotes de controle de posse da palavra e de pacotes RTP/RTCP nas portas UDP correspondentes.

A unidade de controle multiponto é basicamente reativa, isto é, ela só realiza alguma ação após a recepção de um pacote em um dos seus canais. Para todo pacote de controle de conferência recebido, a unidade de controle multiponto transmite um pacote de confirmação de recebimento.

A unidade de controle multiponto não garante a entrega dos pacotes de controle de sessão, de controle de posse da palavra, dos pacotes de *chat* de texto e muito menos dos pacotes RTP de áudio.

Pela forma como o controle de conferência foi projetado, o próprio usuário torna-se o mecanismo de retransmissão dos pacotes, simplificando o desenvolvimento e o processamento da unidade de controle multiponto e da *applet* Java. Se o pedido para entrar na conferência de um participante comum não for recebido pelo moderador,

ele não será admitido na conferência, mas poderá pedir novamente para entrar na conferência. Se o moderador permitiu a entrada do participante comum na conferência e este não recebeu a mensagem contendo a permissão, quando ele pedir novamente para entrar na conferência, a interface homem-máquina do moderador mostrará a ele que o usuário está pedindo para entrar na conferência. Se o moderador concede a posse da palavra a um participante e este não a recebe, o áudio do participante não será ouvido pelo moderador e ele acabará tomando alguma atitude a respeito.

4.3.3.2.2 A estrutura de dados da unidade de controle multiponto

Quando a unidade de controle multiponto é iniciada, sua estrutura de dados de participantes da conferência está vazia, mesmo que a sala possua cadeiras virtuais reservadas para alguns usuários. A estrutura de dados dos participantes da conferência da unidade de controle multiponto possui as seguintes informações dinâmicas e, portanto, voláteis:

- **SSRC do participante:** Identifica o SSRC dos pacotes de áudio do participante. O SSRC (*Synchronization Source Identifier* – Identificador de fonte de sincronismo) (SCHULZRINNE et al., 1996) é uma das informações que identifica unicamente o participante para a unidade de controle multiponto.
- **Número da cadeira virtual do participante na sala virtual de conferência:** Informa qual o número da cadeira virtual do participante dentro da sala virtual de conferência. Corresponde a uma forma a mais de identificação do participante.
- **Tipo de usuário:** Informa qual o papel do usuário dentro da conferência, se de moderador ou de participante comum. Essa informação é utilizada pela unidade de controle multiponto para validar os pacotes de controle de sessão e de controle de posse da palavra.
- **Indicação do participante:** Informa a atual indicação audiovisual do usuário referente aos protocolos de controle de sessão e de controle de posse da palavra.

- **Endereço IP do participante:** Informa o endereço IP do participante. Esse endereço é capturado a partir do endereço IP de origem do pacote de pedido para entrar na conferência. Essa informação é utilizada na transmissão de pacotes da unidade de controle multiponto para o participante e na validação de pacotes recebidos do participante.
- **Porta UDP de recepção do canal de controle:** Informa qual a porta UDP utilizada pela *applet* Java do usuário para a recepção do canal de controle de conferência.
- **Porta UDP de transmissão do canal de controle:** Informa qual a porta UDP utilizada pela *applet* Java do usuário para a transmissão do canal de controle de conferência.
- **Porta UDP de recepção dos pacotes RTP de voz:** Informa qual a porta UDP utilizada pela *applet* Java do usuário para a recepção dos pacotes RTP de voz.
- **Porta UDP de transmissão dos pacotes RTP de voz:** Informa qual a porta UDP utilizada pela *applet* Java do usuário para a transmissão dos pacotes RTP de voz.
- **Porta UDP de recepção dos pacotes RTCP de voz:** Informa qual a porta UDP utilizada pela *applet* Java do usuário para a recepção dos pacotes RTCP referentes ao canal de voz.
- **Porta UDP de transmissão dos pacotes RTCP de voz:** Informa qual a porta UDP utilizada pela *applet* Java do usuário para a transmissão dos pacotes RTCP referentes ao canal de voz.
- **SDS CNAME (Source Description Canonical Name – Nome canônico de descrição da fonte):** Ajuda a identificar unicamente o participante (SCHULZRINNE et al., 1996) para a unidade de controle multiponto na recepção de pacotes de controle de sessão e de controle de posse da palavra.
- **Estatísticas de recepção e de transmissão de pacotes RTP e RTCP:** Armazena as estatísticas de recepção e transmissão de pacotes RTP e RTCP recomendados por (SCHULZRINNE et al., 1996), como número de pacotes enviados, número de pacotes recebidos, taxa de perdas, *jitter*, etc.

- **Último número de seqüência recebido de pacote de áudio:** Armazena o número de seqüência do cabeçalho RTP do último pacote de áudio recebido desse participante.
- **Último *timestamp* transmitido de pacote de áudio:** Armazena o *timestamp* do cabeçalho RTP do último pacote de áudio transmitido da unidade de controle multiponto para esse participante.
- **Último número de seqüência transmitido de pacote de áudio:** Armazena o número de seqüência do cabeçalho RTP do último pacote de áudio transmitido da unidade de controle multiponto para esse participante.
- **Último *timestamp* recebido de pacote de áudio:** Armazena o *timestamp* do cabeçalho RTP do último pacote de áudio recebido desse participante.
- **Informações para o *chat* de texto:** Armazena as informações necessárias para o protocolo do *chat* de texto.
- **Outras informações:** Outras informações auxiliares a respeito do participante.

Quando um participante é admitido na conferência, a unidade de controle multiponto gera uma entrada para ele na sua estrutura de dados. O endereço IP e as portas UDP são iniciados com valores inválidos, nulos, para posterior preenchimento pelo algoritmo de detecção de NAT/NAPT (vide Capítulo 4.3.3.5 mais adiante).

4.3.3.3 A *applet* Java do usuário

A *applet* Java é carregada pela página *web* da sala virtual de conferência e oferece recursos de comunicação de rede, captura e reprodução de áudio para o usuário.

Applets Java impõem algumas restrições de segurança, para impedir o acesso a dados particulares dos usuários e eventuais estragos nos computadores dos mesmos. Uma das restrições impostas impede que a *applet* Java abra uma conexão de rede com um endereço IP diferente daquele de onde a página *web* que a contém tenha sido carregada. Essa restrição impõe que, aos olhos da página *web*, a unidade de controle

multiponto possua o mesmo endereço IP que o servidor *web*. Há três formas de se atender a esse requisito:

- Com a unidade de controle multiponto hospedada na mesma máquina que o servidor *web*;
- Com a unidade de controle multiponto e o servidor *web* hospedados em máquinas diferentes, só que atrás de um NAT/NAPT (HOLDREGE, SRISURESH, 1999), porque todo pacote sairia com o endereço IP do NAT, independentemente se vindo da unidade de controle multiponto ou do servidor *web*.
- Com a *applet* Java do usuário hospedada na mesma máquina que a unidade de controle multiponto;

A alternativa com o NAT/NAPT possui maior escalabilidade que a primeira alternativa, pois possibilita a distribuição de unidades de controle multiponto em servidores de unidades de controle multiponto em máquinas pertencentes à rede interna do NAT/NAPT. O NAT/NAPT precisa ser configurado para encaminhar estaticamente o tráfego de cada sala virtual de conferência para a máquina hospedando a respectiva unidade de controle multiponto e o tráfego do *site* de gerenciamento originado na rede externa para o servidor *web*.

A Figura 4.14 ilustra o cenário do sistema de conferência com unidades de controle multiponto distribuídas atrás de um NAT/NAPT. Há um servidor *web*, um servidor de banco de dados, um NAT/NAPT e duas conferências sendo realizadas (duas salas virtuais de conferência em uso), uma delas nas portas base 7.000 e 5.000 para a unidade de controle multiponto e para *applet* Java do usuário, respectivamente, e a outra, nas portas base 8.000 e 6.000.

Figura 4.14 – Sistema de conferência com unidades de controle multiponto distribuídas através de um NAT/NAPT com encaminhamento estático de portas.

Na solução com o NAT, a alteração da porta base UDP da unidade de controle multiponto de uma sala requer a alteração do encaminhamento de portas do NAT, a menos que as portas base UDP estejam associadas às máquinas que hospedam as unidades de controle multiponto, ou seja, dependendo da faixa de portas utilizada por uma sala virtual de conferência, ela seria hospedada em uma máquina ou em outra. Nesse caso, ao se alterar a porta base UDP de uma sala, pode ser necessário alterar o endereço IP falso da unidade de controle multiponto no *site* de gerenciamento, evitando-se a alteração da configuração do NAT, se ela mapear faixas de portas para cada máquina a ser utilizada para hospedar as unidades de controle multiponto.

Applets Java assinadas com certificados aliviam as restrições de segurança, mas o usuário precisa confirmar se deseja ou não executá-las no momento em que elas são carregadas, porque elas passam a ter acesso irrestrito de leitura, escrita e abertura de conexões. O sistema implementado não utiliza *applets* assinadas.

A terceira alternativa apresentada é a que oferece maior escalabilidade, pois dispensa o artifício do NAT/NAPT e também não necessita de *applets* Java assinadas, permitindo-se distribuir os servidores de unidade de controle multiponto em redes diferentes. A diferença entre a primeira e a última alternativa, é que na última somente a *applet* Java seria hospedada juntamente com a unidade de controle multiponto, e não os *sites* de gerenciamento e de acesso às salas virtuais de conferência inteiros.

A página *web* do usuário continuaria a ser carregada a partir do servidor *web*, mas os arquivos binários da *applet* Java seriam carregados a partir de outro servidor *web*, onde também está o servidor de unidades de controle multiponto. O próprio servidor de unidade de controle multiponto, com pequenas modificações, poderia fazer o papel de um servidor *web* e responder às requisições HTTP da página *web* solicitando os arquivos binários da *applet* Java.

Essa alternativa só não foi implementada por ter sido idealizada após a finalização do servidor de unidades de controle multiponto. Uma versão futura do sistema de conferência multiponto poderá implementar essa solução.

A *applet* Java da interface homem-máquina do usuário implementa:

- Captura, codificação, transmissão, recepção, decodificação e reprodução do áudio;
- Controle do volume do áudio capturado e reproduzido;
- Controle de transmissão dos pacotes de áudio involuntário, associado ao controle de posse da palavra, e voluntário, deixando o microfone mudo na interface homem-máquina;
- Os protocolos RTP/RTCP, de controle de conferência (controle de sessão e de posse da palavra) e de *chat* de texto;

- Comunicação com a página *web*, através da chamada de funções JavaScript, para atualizar a interface homem-máquina do usuário de acordo com os pacotes recebidos da rede.

Quando a página *web* e a *applet* Java são carregadas do servidor *web* no *browser* do usuário, as seguintes informações são passadas da página *web* para a *applet* Java:

- **Papel do usuário na conferência:** O comportamento da *applet* Java depende se o usuário for o moderador da conferência ou um participante comum.
- **Número da cadeira do usuário:** O número da cadeira do usuário dentro da sala de conferência é utilizado pela *applet* Java para alterar a interface homem-máquina do usuário corretamente de acordo com os pacotes de controle de conferência recebidos. Quando a *applet* Java envia a requisição para entrar na conferência, a informação a respeito da cadeira do usuário é enviada, juntamente com outro identificador, o SSRC (*Synchronization Source Identifier* – Identificador de fonte de sincronismo) (SCHULZRINNE et al., 1996) utilizado pelo canal RTP de áudio do participante.
- **Número da cadeira do moderador:** Essa informação é utilizada para validar os pacotes de controle de sessão e de posse da palavra do moderador recebidos pelo participante, quando o usuário for um participante comum. Quando o participante comum é eleito novo moderador da conferência, a informação a respeito da cadeira do moderador é alterada na *applet* Java e na página *web*.
- **Portas base UDP do usuário e da unidade de controle multiponto:** Com essas informações, a *applet* Java abre as portas UDP corretas para recepção de pacotes RTP, RTCP, de controle de conferência e de *chat* de texto e aprende para quais portas na unidade de controle multiponto deve direcionar cada tipo de pacote.
- **Endereço IP da unidade de controle multiponto:** Informação necessária para que a *applet* Java transmita seus pacotes e valide os pacotes recebidos. Por causa da restrição de segurança embutida na *applet* Java, o endereço IP da unidade de controle multiponto precisa ser o mesmo do endereço IP do servidor *web*.

- **Codec de áudio:** Informa qual o *codec* de áudio utilizado na conferência. A *applet* Java deve codificar o áudio e esperar recebê-lo no formato especificado.

Quando a página *web* da sala virtual de conferência é carregada, a *applet* Java transmite a requisição para entrar na conferência para a unidade de controle multiponto e inicia também a transmissão dos pacotes RTP e RTCP de áudio, de forma que se o usuário estiver atrás de um NAPT (HOLDREGE, SRISURESH, 1999), as portas externas do NAPT serão abertas e o NAPT passará a admitir tráfego entrante nelas e encaminhará corretamente os pacotes para a máquina do usuário. A transmissão de pacotes de áudio é cessada quando a *applet* Java recebe do moderador a confirmação de recebimento da sua requisição para entrar na conferência.

Internamente, a *applet* Java utiliza abordagem multitarefa para tratar cada tipo de pacote: pacotes RTP de áudio, pacotes RTCP de áudio e pacotes de controle de conferência. Os canais RTP, RTCP e de controle de conferência são independentes e utilizam portas UDP diferentes, sendo que o RTP e o RTCP são tratados pelos objetos do JMF e o canal de controle por um objeto especificamente criado para o protocolo de controle de conferência desenvolvido. Os *sockets* são bidirecionais (vide Capítulo 2.4.4).

4.3.3.4 Portas base e portas UDP da unidade de controle multiponto e da *applet* Java

A sala virtual de conferência pode ser caracterizada pelas portas UDP utilizadas pela sua unidade de controle multiponto e pela *applet* Java do usuário. A cada sala é atribuída exclusivamente uma faixa de dez portas UDP consecutivas para a unidade de controle multiponto e uma faixa para o usuário, sendo que a porta base da faixa é sempre um número múltiplo de dez. A faixa de portas da unidade de controle multiponto não precisa ser a mesma faixa de portas da *applet* Java do usuário. Usando faixas diferentes de portas, permite-se que uma mesma máquina hospede tanto a unidade de controle multiponto quanto a *applet* Java do usuário. Dessa forma,

não é necessário possuir um equipamento exclusivo para a unidade de controle multiponto, embora isso seja desejável. A Tabela 4.3 mostra a finalidade de cada porta dentro da faixa alocada.

Tabela 4.3 – Faixa de portas UDP para o sistema de conferência

Porta UDP	Finalidade
Porta base	Canal de controle de conferência (controle de sessão e controle de posse da palavra) e <i>chat</i> de texto.
Porta base + 1	Porta reservada para uso futuro.
Porta base + 2	Porta reservada para uso futuro.
Porta base + 3	Porta reservada para uso futuro.
Porta base + 4	Porta do RTP do canal de áudio.
Porta base + 5	Porta do RTCP do canal de áudio.
Porta base + 6	Porta reservada para uso futuro do RTP do canal de vídeo.
Porta base + 7	Porta reservada para uso futuro do RTCP do canal de vídeo.
Porta base + 8	Porta reservada para uso futuro.
Porta base + 9	Porta reservada para uso futuro.

Se para uma determinada sala for definida a porta base UDP 8.000 e para a *applet* Java do usuário, a porta base UDP 5.000, por exemplo, então o cliente esperará receber pacotes RTP de áudio na sua porta UDP 5.004 e transmitirá seus pacotes RTP de áudio para a porta UDP 8.004 da unidade de controle multiponto.

A unidade de controle multiponto não pode assumir que essas portas devem ser utilizadas como portas UDP destino de seus pacotes, porque o usuário pode se encontrar atrás de um NAPT, que pode alterar de forma imprevisível as portas UDP de origem dos pacotes originados pelo usuário. Dessa forma, a unidade de controle multiponto deve transmitir seus pacotes sempre para as portas UDP de origem dos pacotes recebidos a partir da porta UDP de destino desses mesmos pacotes. Assim, o NAPT encaminhará os pacotes recebidos da unidade de controle multiponto para a máquina correta dentro da sua rede privada, devido ao mapeamento da tupla <endereço IP de origem local, porta UDP de origem local, endereço IP de destino, porta UDP de destino> realizado quando o pacote do usuário atravessou o NAPT com destino à unidade de controle multiponto.

A porta base está sendo multiplexada pelos canais de controle de sessão, de posse da palavra e *chat* de texto, pela forma como foram desenvolvidos esses protocolos. Porém, para facilitar a utilização de outros protocolos de controle de sessão, como o *Session Initiation Protocol* (SIP) (ROSENBERG et al., 2002) ou o H.323 (ITU-T, 2003b), convém que o controle de sessão, o controle de posse da palavra e o *chat* de texto utilizem portas diferentes. O uso de canais separados para cada uma dessas funcionalidades simplifica o decodificador associado à porta de recepção e permite que esses protocolos evoluam de forma independente.

Pelo fato da unidade de controle multiponto desenvolvida ser independente de *codec*, adicionar um canal de vídeo a ela envolve poucas modificações, entre elas, a aplicação do controle de posse da palavra também a esse canal. A parte mais complexa da adição de vídeo ao sistema é relativa à *applet* Java do usuário, porque envolve um esforço de programação maior e há a necessidade de se testar a compatibilidade com câmeras diferentes.

A utilização do UDP como protocolo da camada de transporte afeta o controle de sessão, o controle de posse da palavra e o *chat* de texto, devido à ausência de um mecanismo confiável de entrega dos pacotes, mas permite o uso futuro do IP *multicast*. Entretanto, o controle de sessão e o controle de posse da palavra são menos sensíveis à perda de pacotes do que o *chat* de texto, porque a perda de um pacote contendo texto prejudica a conversação. O usuário que transmitiu o pacote contendo texto imagina que todos o receberam e estão cientes do que foi escrito. A perda de um pacote de controle ou de posse da palavra pode produzir um estado inconsistente na interface dos usuários, mas que pode ser rapidamente detectado e corrigido através de mensagens de sincronismo e pelo recebimento de pacotes mais atuais, enquanto que o pacote de texto precisaria ser reenviado pelo usuário. Pelo prosseguimento da conversa, o usuário pode perceber que sua mensagem de texto não foi recebida.

A perda de pacotes pode ocorrer entre o usuário e a unidade de controle e entre a unidade de controle multiponto e o usuário. No primeiro caso, a *applet* Java do usuário tem o conhecimento do sucesso ou não na entrega de um pacote de controle através do recebimento de uma confirmação por parte da unidade de controle

multiponto. No segundo caso, a unidade de controle multiponto tem o conhecimento do sucesso ou não da entrega de um pacote de controle de forma análoga, mas a *applet* Java do usuário que transmitiu o pacote inicial não possui meios de saber se todos os demais participantes da conferência receberam o seu pacote. Portanto, o sistema deve suportar eventuais perdas de pacotes de controle. Como o usuário é o mecanismo de retransmissão do controle de conferência, a inclusão de um mecanismo de confiabilidade sobre o UDP não é necessária, mas pode ser benéfica.

4.3.3.5 Solucionando o problema da tradução de endereços e portas

O sistema desenvolvido aproxima-se da arquitetura cliente-servidor, porque o usuário inicia a comunicação carregando uma página *web* a partir do servidor *web* e quando a *applet* Java é carregada, ela envia para a unidade de controle multiponto um pedido para entrar na conferência. Porém, quando o usuário entra na conferência, a menos que ele entre com a posse da palavra, a unidade de controle multiponto passa a encaminhar para ele os pacotes RTP de áudio em um novo canal de comunicação. O problema do NAPT decorre justamente pela unidade de controle multiponto estar originando esse novo canal. Se o usuário não iniciar a transmissão nesse novo canal, o NAPT não irá criar a sessão e associar uma porta UDP externa a ela. Esse problema foi resolvido da seguinte forma: quando a *applet* Java do usuário é carregada e transmite para a unidade de controle multiponto pelo canal de controle o pedido para entrar na conferência, simultaneamente ela inicia a transmissão de pacotes RTP de áudio, forçando o NAPT a criar uma nova sessão. Quando a *applet* Java recebe a permissão ou negação do pedido para entrar na conferência, ela pára a transmissão de pacotes RTP, a menos que ela receba a posse da palavra de forma explícita.

De uma forma geral para resolver o problema do NAPT, o sistema desenvolvido possui as seguintes características:

- Os *sockets* da *applet* Java e da unidade de controle multiponto são bidirecionais (vide Capítulo 2.4.4).
- As rotinas de recepção de pacotes detectam o endereço IP e a porta UDP de origem dos pacotes de cada canal e comparam se as informações contidas na estrutura de dados do participante são válidas (se já foi realizada a detecção anteriormente).
- Os canais de comunicação são sempre iniciados pela *applet* Java do usuário.
- As informações encapsuladas de endereço IP e de portas UDP no pacote de pedido de entrada na conferência ajudam na detecção do NAPT, através do confronto com as informações capturadas dos cabeçalhos IP e UDP dele.

4.4 Controle de sessão e de posse da palavra

A implementação do controle de sessão e de posse da palavra é exposta a seguir e são diferenciados os aspectos relacionados ao sistema dos relacionados ao usuário.

4.4.1 Aspectos relacionados ao sistema

Os controles de sessão e de posse da palavra foram implementados como um único protocolo de controle de conferência.

Os pacotes de controle utilizam o UDP como protocolo de transporte, para facilitar o uso futuro de IP *multicast*.

O sistema desenvolvido emprega o mecanismo de controle de posse da palavra assistido (vide Capítulo 2.3.1), com um dos participantes da conferência no papel de moderador da mesma e os demais, no papel de participantes comuns.

A autenticação de usuários é feita no nível do *site*, com senhas e *logins*. Após o usuário ser identificado, são mostradas as salas às quais ele possui permissão de acesso.

O protocolo de controle de conferência permite ao participante comum:

- Pedir para entrar em uma sala virtual de conferência;
- Deixar a sala de conferência;
- Requisitar a posse da palavra;
- Desistir de requisitar a posse da palavra;
- Devolver a posse da palavra para o moderador, após tê-la recebido.

O moderador controla a admissão na sessão e a posse da palavra e pode:

- Iniciar, terminar e configurar as salas virtuais de conferência¹⁹;
- Admitir, rejeitar e expulsar participantes;
- Permitir ou negar a posse da palavra a qualquer participante;
- Tomar a posse da palavra no momento em que desejar. Ele pode também requisitá-la, apenas para avisar ao atual detentor da posse da palavra que o moderador a quer de volta;
- Permitir ou não que a unidade de controle multiponto encaminhe áudio para um determinado participante;
- Eleger um novo moderador.

4.4.1.1 Sincronismo de informações e distribuição dos pacotes de controle

Como a interface homem-máquina utiliza o conceito WYSIWIS (*What You See Is What I See* – O Que Você Vê É O Que Eu Vejo) (vide Capítulo 2.3), precisa-se manter consistentes as interfaces homem-máquina de todos os participantes. Esse sincronismo de informações é feito pela transmissão e recepção de pacotes de

¹⁹ Na versão atual do sistema, essas funções cabem somente ao administrador do sistema.

controle de conferência. Mesmo quando um pacote de controle de conferência destina-se a um único participante, seja ele o moderador ou um participante comum, a unidade de controle multiponto encaminha para os demais participantes uma cópia do pacote, de forma a atualizar as interfaces homem-máquina deles.

O destinatário do pacote de controle de conferência sempre responde ao pacote recebido com um pacote de confirmação (*Ack*). A unidade de controle multiponto também gera seus pacotes de confirmação na recepção dos pacotes de controle de conferência. Dependendo da indicação audiovisual atual do participante (moderador ou participante comum), a alteração da interface homem-máquina ocorre no recebimento do pacote de confirmação do moderador, do participante comum ou da unidade de controle multiponto (vide Anexo C).

Como o protocolo de controle de conferência foi implementado sobre o UDP, que não garante a entrega dos dados, o sistema foi desenvolvido para que o próprio usuário seja o mecanismo de retransmissão, quando ele percebe que a sua requisição não foi recebida, isto é, quando a sua ação não causou a mudança esperada na sua interface homem-máquina.

Toda ação do moderador implica em uma reação compatível da unidade de controle multiponto. Se o moderador concede a posse da palavra para um participante, a unidade de controle multiponto encaminha a concessão da posse da palavra para os demais participantes, para as suas interfaces homem-máquina serem atualizadas. As ações dos participantes comuns são encaminhadas pela unidade de controle multiponto para os demais participantes pelos mesmos motivos.

Um mecanismo duplo de sincronização foi implementado para manter a interface homem-máquina do usuário coerente: pelo protocolo de controle de conferência e por requisições e respostas HTTP. Primariamente, a indicação do usuário na interface é alterada quando a *applet* Java recebe um pacote de controle ou uma confirmação de recebimento de pacote por parte da unidade de controle multiponto. Após a alteração da indicação audiovisual de um usuário, sua nova indicação é enviada por ele para o servidor *web* através de uma requisição HTTP, de forma a manter também o servidor *web* atualizado. Dessa forma, quando um novo usuário entrar na conferência, sua

interface será carregada com informações atualizadas e ele terá ciência dos participantes na sala virtual de conferência.

Problemas de sincronismo ocorrem quando pacotes de controle são perdidos, recebidos fora de ordem ou quando a informação do servidor se torna inconsistente. O mecanismo duplo de sincronização pode ser substituído por pacotes explícitos de sincronismo periodicamente enviados pela unidade de controle multiponto, informando a novos participantes quem está presente na conferência e qual sua indicação. O pacote de sincronismo implementado na versão atual do sistema é transmitido pela *applet* Java do usuário e não informa a sua indicação, servindo apenas para indicar que o participante está presente na conferência.

Quando um usuário entra na conferência, ele inicia a transmissão de seus pacotes de áudio para a unidade de controle multiponto, para forçar uma entrada na tabela de tradução de endereços de um eventual NAT/NAPT (HOLDREGE, SRISURESH, 2001); (SENIE, 2002) (vide Capítulo 2.4.3) presente na rede. Após a permissão ou negação da sua admissão, ele pára de transmitir, a menos que ele receba de forma explícita a posse da palavra. Caso ele não pare de transmitir os pacotes de áudio, ele receberá periodicamente pacotes de controle de posse da palavra para parar a transmissão.

4.4.2 Aspectos relacionados ao usuário

A sala de conferência é representada pelas imagens de cada participante da conferência. Quando o usuário clica na imagem de um participante, um *menu* aparece na sua tela com as ações e informações disponíveis. As ações disponíveis variam de acordo com o papel desempenhado pelo usuário na conferência e a sua indicação audiovisual atual na conferência.

A *applet* Java da interface homem-máquina do usuário é informada a respeito do papel do participante na conferência, se de participante comum ou se de moderador, através de parâmetros passados para ela na sua iniciação. Quando o moderador elege um novo moderador, a sua *applet* e a do novo moderador são alteradas internamente

para refletir a mudança no papel desempenhado. Dessa forma, a *applet* Java gera os pacotes adequados a cada um dos papéis.

Quando a *applet* Java de um participante recebe da unidade de controle multiponto uma ordem para cessar a transmissão de pacotes de voz, a *applet* Java interrompe o transmissor e solicita à interface homem-máquina uma transição para uma pseudo-indicação chamada *semPossePalavra*. A interface homem-máquina do participante só é alterada se a sua indicação atual for *possePalavra*. Nesse caso, sua nova indicação passa a ser *normal*.

4.4.3 Diagramas de tempo de troca de mensagens de controle de conferência

O protocolo de controle de conferência foi implementado segundo os diagramas de troca de mensagens apresentados integralmente no Anexo C. Os diagramas mostram as mensagens trocadas entre a unidade de controle multiponto e as *applets* Java do participante comum e do moderador. A título de exemplo, dois casos de uso de controle de posse da palavra estão relatados neste capítulo: um participante pedindo a posse da palavra e o moderador concedendo a posse da palavra a um participante.

As trocas de mensagens, suas correspondentes ações desencadeadoras e desencadeadas na unidade de controle multiponto, nas *applets* Java e interfaces homem-máquina dos participantes foram projetadas de forma que o usuário seja o mecanismo de retransmissão das mensagens, aliviando o processamento da unidade de controle multiponto e das *applets*, simplificando seu funcionamento e implementação.

Quando um pacote de controle de conferência é enviado ou recebido, ele pode ou não provocar mudanças na interface-homem máquina dos participantes da conferência.

Por causa do duplo mecanismo de sincronismo, toda vez que um participante tem sua indicação alterada, ele envia sua nova indicação para o servidor *web*, através de uma requisição HTTP. As únicas exceções ocorrem quando o moderador expulsa um participante da conferência e quando o moderador concede anistia ao participante

expulso. Nessas duas situações, o moderador envia para o servidor *web* as novas indicações do participante expulso e anistiado.

Para os diagramas a seguir, a unidade de controle multiponto será identificada por *MCU*, o moderador será identificado por *M*, o participante em questão por *P* e os demais participantes da conferência, por *Participantes*. As mensagens de confirmação de recebimento da unidade de controle multiponto, da *applet* Java do moderador e do participante serão chamadas de ACK_{MCU} , ACK_M e ACK_P , respectivamente.

A Figura 4.15 ilustra um participante comum pedindo a posse da palavra para o moderador.

Figura 4.15 – Participante comum pedindo a posse da palavra.

Estando o participante comum *P* já admitido na conferência, ele pode requisitar a posse da palavra sempre que sua indicação estiver *normal*, isto é, sempre que ele estiver na conferência sem a posse da palavra (indicação *possePalavra*), sem o seu áudio bloqueado (indicação *semAudio*) pelo moderador e sem problemas de comunicação (indicação *semInformacao*) com a unidade de controle multiponto. Essa restrição decorre do fato de o *menu* de cada participante na sala virtual de

conferência apresentar somente as opções compatíveis com a sua indicação atual e seu papel na conferência. Através da sua interface homem-máquina ele requisita a posse da palavra. Há três momentos possíveis para P mudar sua interface homem-máquina para *pedindoPalavra*:

- **No instante em que o pedido é enviado:** Nessa situação, P não tem como saber se M recebeu a sua requisição, porque ela pode ter se perdido entre P e a MCU ou entre a MCU e M . Se a indicação do participante fosse alterada para *pedindoPalavra* e o moderador não a tivesse recebido, a única forma de P reenviar a requisição é enviando uma mensagem de desistência do pedido de posse da palavra, voltando para a indicação *normal* e enviando uma nova requisição.
- **No recebimento do ACK_{MCU} :** Nessa situação, P sabe que a MCU recebeu a sua requisição, mas também não tem como saber se o moderador a recebeu.
- **No recebimento do ACK_M :** Nessa situação, P tem a certeza que M recebeu a sua requisição. O tempo de resposta da ação do participante é o *round-trip time* da camada de aplicação (RTT_{APP}) entre P e M . Isto é, o tempo que se leva para a interface homem-máquina de P ser atualizada a partir do instante em que ele requisitou a posse da palavra depende do tempo de processamento e de transmissão da requisição e do ACK_M pela unidade de controle multiponto e pelas *applets* Java de P e de M , mais o atraso inserido pela rede. Se RTT_{APP} for estimado em aproximadamente um segundo para conferências sendo realizadas através da Internet, esse será aproximadamente o tempo que levará para a interface homem-máquina de P ser atualizada. A interface homem-máquina de M e dos demais participantes serão atualizadas antes que a de P . Se ACK_M não for recebido por P , ou se P enviar uma nova requisição antes do seu recebimento, não haverá problemas, porque as interfaces homem-máquina de M e dos *Participantes* continuará consistente e a *applet* Java de M transmitirá um novo ACK_M .

Pela discussão apresentada para a situação em questão, é mais seguro, em termos de consistência, atualizar a interface homem-máquina de P no recebimento de ACK_M . Na maioria das demais situações que serão apresentadas, as atualizações das interfaces homem-máquina são feitas da mesma forma, no recebimento de ACK_M .

A Figura 4.16 mostra o moderador, com a posse da palavra, concedendo-a a um participante comum.

Figura 4.16 – Moderador, com a posse da palavra, concedendo-a a um participante comum.

Quando a MCU recebe a concessão de posse da palavra para P , ela pára de encaminhar os pacotes RTP de áudio de M , e passa a esperar pelos pacotes RTP de áudio de P . Se M não receber logo ACK_P , ele continuará a transmitir áudio até que a MCU ordene explicitamente que ele pare, através de uma mensagem de perda de posse da palavra (pseudo-indicação *semPossePalavra*).

Se o moderador não receber o ACK_P , sua interface homem-máquina continuará indicando P sem a posse da palavra, permitindo que o moderador novamente envie a concessão de posse da palavra a ele, até que ACK_P seja recebido.

As interfaces homem-máquina de todos os participantes devem alterar dois participantes simultaneamente, M e P , quando for recebida a concessão de posse da palavra para P .

Analisando o caso quando há sucesso na troca de mensagens: quando a MCU recebe a concessão de posse da palavra para P , ela pára de encaminhar os pacotes RTP de áudio de M e passa a esperar pelos pacotes de P . A banda de transmissão de pacotes RTP da MCU cai a zero, enquanto a de recepção permanece igual a um canal de áudio. Quando P receber a posse da palavra e iniciar seu transmissor, por um curto intervalo de tempo, a MCU receberá os pacotes RTP de M e de P , porque M ainda não recebeu o ACK_P e por isso continua a transmitir, a menos que M receba nesse intervalo de tempo uma notificação para parar de transmitir. Durante esse período de tempo, a banda de recepção de pacotes RTP da MCU dobra e a de transmissão é restabelecida. Esse comportamento pode também ser observado nos gráficos de banda de recepção e de transmissão da MCU discutidos no capítulo seguinte.

4.4.4 Resolvendo problemas de consistência durante a conferência

Caso um determinado participante da conferência não receba uma requisição enviada P , sua interface homem-máquina ficará momentaneamente inconsistente, até que a indicação do participante inconsistente seja alterada. A inconsistência só é problemática quando ocorre na interface homem-máquina do moderador ou quando o participante inconsistente na interface homem-máquina for o próprio participante ou o moderador. Ainda assim, a inconsistência tende a ser resolvida ao longo do tempo. Os diagramas de tempo foram projetados de forma a prevenir e minimizar as ocorrências de inconsistências das interfaces homem-máquina.

Há diferentes níveis de inconsistências. Uma interface homem-máquina inconsistente que não indica que P está com o áudio bloqueado só é uma inconsistência grave se

interface homem-máquina em questão for a de M . Ainda assim, ela pode ser resolvida com M enviando uma mensagem bloqueando o áudio de P e outra desbloqueando em seguida, se assim o desejar.

Outra inconsistência grave ocorre quando a interface homem-máquina de P informá-lo que ele está com a posse da palavra, quando na verdade ela está com outro participante. Nesse caso, a MCU resolverá esse estado inconsistente transmitindo para P uma mensagem para que ele pare de transmitir pacotes de áudio. Essa inconsistência pode ser resolvida também por M , concedendo a posse da palavra para outro participante ou tomando-a para si próprio.

Se a interface homem-máquina de M estiver inconsistente, com nenhum participante com a posse da palavra, ele pode concedê-la para alguém. Se a interface homem-máquina de M indicar todos os participantes com a posse da palavra, ele pode resolver essa inconsistência retirando a posse da palavra do participante que realmente está com a posse da palavra, mas terá que descobrir quem ele é, por tentativa e erro.

Praticamente todo problema de consistência pode ser resolvido através do envio de mensagens de sincronismo pela unidade de controle multiponto, porque a palavra final cabe a ela. A unidade de controle multiponto sempre sabe quem é o moderador da conferência, quem está com a posse da palavra e quem está ou não na conferência.

Se um participante imagina estar na conferência, mas não possui uma entrada na estrutura de dados da unidade de controle multiponto, ele não receberá pacote algum. Então, importa conhecer o que se passa na unidade de controle multiponto. Os pacotes de sincronismo são transmitidos esporadicamente pela unidade de controle multiponto. Poderia-se alterá-la, de forma a transmitir os pacotes de sincronismo também quando ela detecta uma possível inconsistência ou, então, para explicitar transições de indicações implícitas, como o abandono da conferência de um participante com a posse da palavra. A versão atual da unidade de controle multiponto não realiza essas funções, para simplificar o seu processamento interno e para minimizar o uso de banda.

O problema de se explicitar todas as transições implícitas de indicação é o aumento da banda consumida pela unidade de controle multiponto pelo envio de mais mensagens.

Se a inconsistência da interface homem-máquina não puder ser resolvida através das mensagens de controle de conferência, o participante pode forçar o sincronismo explícito com o servidor através de uma opção na sua interface homem-máquina ou abandonar a conferência, retornando em seguida. Em último caso, torna-se necessário o reinício da conferência.

4.5 Processamento de pacotes

Os dois elementos do sistema de conferência que realizam processamento de pacotes de áudio e de controle de conferência são a unidade de controle multiponto e a *applet* Java do usuário.

Na unidade de controle multiponto, o controlador multiponto lida com os pacotes de controle de conferência (controle de sessão e controle de posse da palavra), enquanto o processador multiponto cuida da recepção e encaminhamento dos pacotes RTP/RTCP.

Na *applet* Java, os objetos desenvolvidos utilizando o JMF cuidam da recepção e transmissão de pacotes RTP/RTCP, além da captura, codificação, decodificação e reprodução do áudio.

O processamento de cada tipo de pacote é descrito a seguir.

4.5.1 Processamento de pacotes de controle de sessão

Os pacotes de controle de sessão compreendem os pacotes que carregam mensagens de pedido de admissão na conferência, aceitação ou rejeição do pedido de entrada na conferência, abandono de conferência e expulsão de participante da conferência.

A tarefa de recebimento de pacotes de controle de sessão na unidade de controle multiponto fica em um laço infinito, esperando por eles.

Quando o *browser* do participante carrega a página *web* da sala de conferência, sua *applet* Java transmite para a unidade de controle multiponto uma mensagem de pedido para entrar na conferência. A página *web* informa à *applet* Java qual o papel do participante e os parâmetros de configuração, como as portas base e o *codec* de áudio. Se o papel do participante na conferência for a de moderador, a unidade de controle multiponto automaticamente admite-o na conferência, transmitindo para ele uma permissão de entrada na conferência, desde que já não haja um moderador presente. Nesse caso e no caso do papel do participante na conferência for a de um participante comum, a unidade de controle multiponto encaminha o pedido para entrar na conferência para o moderador e para todos os demais participantes. Após o moderador ter sido admitido na conferência, todo pacote de controle de sessão transmitido por ele é validado pela unidade de controle multiponto pelo endereço IP de origem e pelos campos SSRC, User ID e User Type (vide Anexo B).

Quando a unidade de controle multiponto recebe um pedido de entrada na conferência de um participante comum, ela verifica se não se trata de um participante que foi expulso da conferência. Se não houver nenhum registro de que ele foi expulso da conferência, as informações contidas no pacote recebido são armazenadas temporariamente na estrutura de dados da unidade de controle multiponto e uma versão simplificada do pacote é encaminhada para os demais participantes da conferência. Se o moderador aceita a entrada do participante na conferência, as informações a respeito do participante comum são passadas para a estrutura de dados definitiva. Se o participante não for aceito, suas informações são destruídas, a menos que ele seja explicitamente vetado na conferência pelo moderador. Nesse caso, suas informações são retidas para que a unidade de controle multiponto não encaminhe mais pacotes desse participante.

Ainda no recebimento do pedido para entrar na conferência, a unidade de controle multiponto executa um algoritmo para detectar se o participante encontra-se atrás de um NAT ou de um NAPT. O pacote de pedido de entrada na conferência carrega informações encapsuladas a respeito do endereço IP e das portas UDP originalmente

utilizados pela *applet* Java do participante. Essas informações são confrontadas com o endereço IP e a porta UDP de origem do pacote recebido. Se o endereço IP do pacote recebido for diferente do endereço IP original, o participante provavelmente se encontra atrás de um NAT ou de um NAPT. Se a porta UDP originalmente utilizada para o canal de controle for diferente da porta UDP de origem do pacote recebido, então o participante provavelmente se encontra atrás de um NAPT.

Mesmo que o NAT/NAPT não seja detectado, a unidade de controle multiponto sempre irá transmitir pacotes de controle de sessão para a porta UDP de origem e para o endereço IP de origem do pacote de pedido de entrada na conferência recebido, a partir da porta UDP de destino desse mesmo pacote. Dessa forma, um eventual NAPT no usuário encaminhará corretamente para ele o tráfego recebido da unidade de controle multiponto.

Quando um participante da conferência é expulso pelo moderador, além da unidade de controle multiponto encaminhar a mensagem de expulsão para todos os participantes, ela não encaminha mais nenhuma mensagem recebida desse participante, nem o pedido para entrar na conferência. A entrada nele na estrutura de dados da unidade de controle multiponto não é destruída, justamente para verificar se o pedido para entrar na conferência vem de um participante que foi expulso da conferência. Para que a unidade de controle multiponto volte a encaminhar o pedido para entrar na conferência desse participante para o moderador, ela precisa antes receber uma mensagem do moderador anistiando o participante em questão.

Quando o usuário pede para entrar na conferência, sua *applet* Java transmite o pedido para entrar na conferência em intervalos de tempo regulares, por um número determinado de vezes, até que ela receba um pacote de confirmação de recebimento de pedido de entrada na conferência por parte do moderador ou então um pacote de permissão ou negação de entrada na conferência.

Quando a unidade de controle multiponto fica um determinado tempo sem receber pacote algum de um participante, ela transmite um pacote de controle de sessão para todos os participantes, inclusive para ele, avisando que aquele participante encontra-se com problemas de comunicação. Quando a *applet* Java do participante em questão recebe esse pacote, um pacote de sincronismo é enviado para a unidade de controle

multiponto. Quando a unidade de controle multiponto recebe qualquer pacote desse participante, os demais participantes são avisados que o participante está novamente ativo na conferência.

A única mensagem de controle de sessão respondida com uma mensagem de confirmação é o pedido para entrar na conferência e quem gera essa confirmação é a *applet* Java do moderador. As demais mensagens simplesmente são encaminhadas para todos os participantes.

4.5.2 Processamento de pacotes de controle de posse da palavra

Todos os pacotes de controle de posse da palavra recebidos pela unidade de controle multiponto são validados por ela através da verificação do endereço IP de origem e do SSRC. Os pacotes válidos são encaminhados para os demais participantes da conferência.

Quando a unidade de controle multiponto recebe um pacote do moderador concedendo a posse da palavra para algum participante, imediatamente a unidade de controle multiponto pára de encaminhar os pacotes RTP de áudio do participante que estava com a posse da palavra e passa a esperar pelos pacotes RTP de áudio do novo dono da posse da palavra. Caso o participante que estava com a posse da palavra não pare de transmitir, ele receberá mensagens vindas da unidade de controle multiponto para interromper a sua transmissão.

Quando a *applet* Java do participante que estava com a posse da palavra recebe uma mensagem indicando um novo participante com a posse da palavra ou um pedido para parar de transmitir, ela pára a transmissão de pacotes RTP de áudio e muda a interface homem-máquina do participante para a indicação *normal*.

Quando a unidade de controle multiponto recebe do moderador uma mensagem para bloquear o áudio de algum participante, ela deixa de encaminhar os pacotes RTP de áudio para o participante em questão, até o momento em que o moderador transmita para ela a mensagem desbloqueando o áudio do participante. Essas mensagens também são encaminhadas pela unidade de controle multiponto para todos os

participantes, para que eles saibam que determinado participante não ouvirá o que estiver sendo falado por aquele que está com a posse da palavra. Entretanto, esse participante continua a receber mensagens do *chat* de texto.

Quando um participante está com o seu áudio bloqueado pelo moderador, ele fica impedido de requisitar a posse da palavra.

4.5.3 Processamento de pacotes RTP

A tarefa de recepção de pacotes RTP fica esperando receber pacotes na porta UDP apropriada, em um laço infinito. Quando um pacote é recebido, primeiramente é feita uma validação do seu cabeçalho RTP, verificando a versão do protocolo RTP, o *bit* de extensão, o *bit* de marca, o *codec* utilizado, a presença de *padding* e os campos que indicam o número de fontes que contribuíram para a formação do áudio sendo transportado (SCHULZRINNE et al., 1996). Mesmo que o pacote recebido possua um cabeçalho RTP válido ainda é necessário verificar outras informações para decidir se ele será ou não encaminhado para os demais participantes. As outras informações para completar a validação do pacote são:

- **Endereço IP de origem do pacote (IP_X):** O endereço IP de origem do pacote é confrontado contra o endereço IP do participante que possui SSRC igual a $SSRC_X$.
- **Porta UDP de origem do pacote (UDP_X):** A porta UDP de origem é confrontada com a porta UDP RTP do participante que possui SSRC igual a $SSRC_X$. Se as portas UDP de recepção e transmissão do participante X na estrutura de dados da unidade de controle multiponto possuírem valor nulo (valor inválido pré-determinado), isto é, se esse for o primeiro pacote RTP recebido do participante X, a porta UDP_X é inserida na estrutura de dados.
- **SSRC do cabeçalho RTP do pacote ($SSRC_X$):** A unidade de controle multiponto verifica se o participante que possui o $SSRC_X$ está com a posse da palavra.

Se o pacote for válido, a unidade de controle multiponto atualiza as suas estatísticas de recepção para o participante X. A seguir, a unidade de controle multiponto verifica se as portas UDP do RTP do participante X contêm valores válidos, não nulos. Caso os valores sejam nulos, a unidade de controle multiponto captura a porta UDP de transmissão do pacote recebido (UDP_X) e coloca-a na estrutura de dados para o participante X. Desse momento em diante, todo pacote RTP que a unidade de controle multiponto vier a transmitir para o participante X será direcionado para a porta UDP_X capturada. A captura de porta UDP de origem serve para solucionar problemas com NAPT. O endereço IP e a porta UDP para onde a unidade de controle multiponto deve transmitir os pacotes de controle de sessão e de posse da palavra já eram conhecidos, pelo recebimento do pacote de pedido para entrar na conferência, mas faltava conhecer as portas UDP para o RTP e para o RTCP.

Não se pode assumir que a porta UDP do RTP para a qual a unidade de controle multiponto irá transmitir seja uma porta par, como sugerido em (SCHULZRINNE et al., 1996), porque se o pacote RTP atravessar um NAPT em seu trajeto do participante para a unidade de controle multiponto, a porta UDP de origem será alterada de forma imprevisível.

Se o participante X não está com a posse da palavra e o número de sequência RTP (SCHULZRINNE et al., 1996) recebido for múltiplo de um certo valor ou se encaixar em outro critério desejado, a unidade de controle multiponto pede para o participante parar de transmitir. A validação sobre o número de sequência recebido é feita, para que a unidade de controle multiponto não transmita um pedido para o participante X parar de transmitir a cada pacote recebido. Caso ele esteja com a posse da palavra, o pacote recebido é modificado antes de ser encaminhado para os demais participantes da conferência.

O número de sequência (NS_X) e o *timestamp* ($Timestamp_X$) dos pacotes RTP recebidos do participante X pela unidade de controle multiponto não são validados, eles apenas são recalculados antes dos pacotes serem transmitidos para cada participante, deixando a validação desses campos a cargo da *applet* Java do usuário. Se o pacote RTP recebido estiver fora de ordem, ela o retransmitirá dessa forma,

deixando para a *applet* Java a tarefa de reordená-lo, aliviando o processamento da unidade de controle multiponto.

Os pacotes RTP são transmitidos somente para os participantes que não estejam com seus receptores de áudio bloqueados pelo moderador e que possuam uma porta RTP de recepção válida na estrutura de dados da unidade de controle multiponto. O participante com a posse da palavra só receberá o seu próprio áudio se a unidade de controle multiponto estiver com o *loopback* habilitado (opcional). Depois, as estatísticas de transmissão da unidade de controle multiponto e de recepção dos participantes são atualizadas.

A Figura 4.17 ilustra todo o processamento de pacotes RTP feito pela unidade de controle multiponto e a Figura 4.18 detalha a parte do envio do pacote RTP para cada participante.

Figura 4.17 – Processamento de pacotes RTP.

A unidade de controle multiponto gera seus próprios valores desses campos de forma relativa para cada um dos demais participantes, calculando-os segundo as Equações (20) e (21), respectivamente, utilizando as estatísticas de recepção e transmissão de cada participante.

$$\Delta NS_x[m] = NS_x[m] - NS_x[m-1] \quad (18)$$

$$\Delta Timestamp_x[m] = Timestamp_x[m] - Timestamp_x[m-1] \quad (19)$$

$$NS_{MCU \rightarrow Y}[n] = NS_{MCU \rightarrow Y}[n-1] + \Delta NS_x[m] \quad (20)$$

$$Timestamp_{MCU \rightarrow Y}[n] = \begin{cases} Timestamp_{MCU \rightarrow Y}[n-1] + \left(\frac{\Delta Timestamp_x[m]}{\Delta NS_x[m]} \right), \\ \text{para } \Delta NS_x[m] \neq 0 \\ Timestamp_{MCU \rightarrow Y}[n-1], \text{ para } \Delta NS_x[m] = 0 \end{cases} \quad (21)$$

Os valores iniciais do *timestamp* e do número de sequência dos pacotes RTP transmitidos da unidade de controle multiponto para cada um dos demais participantes, $Timestamp_{MCU \rightarrow Y}[0]$ e $NS_{MCU \rightarrow Y}[0]$, respectivamente, são números aleatórios, segundo a recomendação de (SCHULZRINNE et al., 1996). Cada um dos participantes recebe um número de sequência e um *timestamp* independente, porque eles podem receber uma quantidade de pacotes RTP diferentes, de acordo com a dinâmica da conferência. Quando um participante está com a posse da palavra ou com o áudio bloqueado pelo moderador, ele não recebe pacotes RTP de áudio, então, o último número de sequência e o último *timestamp* recebidos por ele permanecem inalterados, enquanto os dos demais participantes continuam a serem atualizados. Para esse participante, tudo se passa como se a unidade de controle multiponto tivesse parado temporariamente o seu transmissor. Embora o tempo absoluto esteja correndo, o *timestamp* desse participante está parado (SCHULZRINNE et al., 1996). Quando ele voltar a receber pacotes de áudio, a reprodução será realizada normalmente.

Figura 4.18 – Rotina de transmissão de pacotes RTP.

Como o *timestamp* do cabeçalho RTP não reflete o tempo absoluto, a diferença entre um participante que pára o seu transmissor RTP e após algum tempo volta a transmitir áudio e uma sequência de pacotes atrasada é muito sutil, depende de um limite de tempo imposto pelo receptor para determinar a diferença nas duas situações e da rigidez da sua implementação. Se o receptor RTP determinar que os pacotes estão atrasados, eles não serão reproduzidos e o participante que os recebe não ouvirá

nada. Se o receptor RTP interpretá-los como o reinício do transmissor após um período de silêncio, eles serão reproduzidos. Dependendo do tempo absoluto decorrido sem o recebimento dos pacotes RTP, o receptor pode inclusive interpretar os novos pacotes recebidos como uma nova sessão RTP do transmissor, que por acaso possui o número de sequência seguintes da sequência anterior.

4.5.4 Processamento de pacotes RTCP

Os pacotes RTCP recebidos pela unidade de controle multiponto estão sendo ignorados na versão atual do sistema de conferência, a informação contida neles não está sendo utilizada para a unidade de controle multiponto modificar suas características de transmissão.

A unidade de controle multiponto também não está gerando pacotes RTCP na versão atual do sistema, embora praticamente todas as informações necessárias estejam disponíveis. O não envio de pacotes RTCP não prejudica o funcionamento da conferência, como foi verificado em testes práticos.

Embora os pacotes RTCP sejam ignorados, a unidade de controle multiponto também executa o algoritmo de detecção da porta UDP utilizada para os pacotes RTCP de cada participante, permitindo que uma versão futura do sistema transmita corretamente esses pacotes. Quando um pacote RTCP é recebido pela unidade de controle multiponto, ela verifica se a porta UDP RTCP do participante na sua estrutura de dados possui portas válidas para transmissão e recepção RTCP. Se não possuir, a porta UDP de origem do pacote recebido é capturada.

Não se pode assumir que a porta UDP do RTCP seja a porta ímpar imediatamente acima da porta UDP do RTP (SCHULZRINNE et al., 1996), porque dependerá da forma pela qual um eventual NAPT no participante mapeará as portas dos pacotes UDP saindo por ele.

4.6 O *chat* de texto

O *chat* de texto foi implementado como mais uma ferramenta de comunicação entre alunos e entre alunos e professor, para aumentar a interatividade na conferência, permitindo comunicações paralelas à conversação central e servindo como um canal de retorno simples, evitando a necessidade de se conceder a posse da palavra a cada participante da conferência simplesmente para se verificar se todos concordam ou se todos entenderam o que foi colocado, por exemplo.

A menos que ocorra alguma falha na distribuição dos pacotes contendo texto, todos os participantes recebem o pacote enviado, menos aquele que o enviou, mas sua interface homem-máquina do *chat* de texto é atualizada com o texto enviado. Embora o pacote de texto ofereça meios para ser direcionado exclusivamente para um subconjunto dos participantes da conferência, a interface homem-máquina ainda não implementa essa funcionalidade, nem a unidade de controle multiponto.

A utilização de *chat* de texto em uma sala virtual de conferência é opcional e configurável através do *site* de gerenciamento.

4.7 Análise de escalabilidade do sistema

Os principais pontos discutidos a respeito da escalabilidade do sistema são:

- **Bandas de transmissão e de recepção da unidade de controle multiponto:**
Cada unidade de controle multiponto recebe 1 canal de áudio, N canais de controle e transmite $N - 1$ canais de áudio e N canais de controle. A banda de cada canal de áudio depende do *codec* sendo utilizado. A banda de transmissão disponível para a unidade de controle multiponto restringe o número máximo de participantes em salas virtuais de conferência, enquanto que a banda de recepção disponível restringe o número de salas virtuais de conferência simultâneas,

porque a banda de recepção necessária é diretamente proporcional ao número de conferências simultâneas.

- **Número de portas UDP:** O número de portas UDP disponível em uma estação restringe o número máximo de salas virtuais de conferência que ela pode hospedar. Sendo as portas UDP identificadas por um número de 16 *bits* sem sinal, há 65.535 portas disponíveis em uma estação, mas, geralmente, somente as portas acima do número 1.024 estão disponíveis para aplicações genéricas. Como cada sala ocupa uma faixa de 10 portas UDP, tendo como porta base uma porta múltipla de 10, a primeira porta base que pode ser utilizada é a 1.030, e a última, a 65.520. Dessa forma, uma única estação poderia hospedar 6.417 salas, um número de salas certamente maior do que a banda disponível pode atender caso todas as salas estejam em uso simultaneamente.
- **Número de salas virtuais de conferência:** Para a abordagem multitarefa, o número de salas suportadas por um único servidor de unidades de controle multiponto depende do número de tarefas que podem ser disparados por um processo na linguagem Java. Para as abordagens multiprocesso e híbrida, a restrição passa a ser a capacidade do sistema operacional e de recursos computacionais. O *site* de gerenciamento restringe o espaço de endereçamento de salas a 6.417 faixas de endereço, devido ao conceito das portas base UDP.
- **Número de conferências simultâneas:** Os principais fatores limitantes que restringem o número de salas virtuais de conferência em uso simultaneamente dependem do cenário em questão. Para conferência na Internet, os principais fatores limitantes são a banda de recepção e a de transmissão do servidor. Para conferências simultâneas sendo realizada em uma mesma rede local de alta velocidade, a capacidade de processamento da máquina hospedando as unidades de controle multiponto passa a ser o principal fator limitante, porque as tarefas de recepção e transmissão de cada sala concorrem entre si pelos recursos compartilhados de processamento. A distribuição de unidades de controle multiponto pela rede alivia às restrições impostas pela capacidade de processamento de uma única máquina.

- **Número de participantes simultâneos:** O número máximo de participantes simultâneos é restringido primeiramente pela banda de transmissão disponível para a unidade de controle multiponto e depois pela capacidade de processamento da máquina que a hospeda. A forma como esses participantes estão distribuídos em salas virtuais de conferência afeta a escalabilidade do sistema. O desempenho do sistema atendendo a 10 salas com 10 participantes cada certamente não é o mesmo do sistema atendendo a 100 participantes em uma única sala. No primeiro caso, há 10 participantes transmitindo pacotes RTP de áudio, 90 participantes recebendo-os e as tarefas de recepção e transmissão de cada sala concorrem entre si pelo tempo do processador. Já no segundo caso, há somente 1 participante transmitindo pacotes RTP de áudio, 99 participantes recebendo-os e as tarefas da sala só concorrem com tarefas de outros processos pelo tempo do processador.

Pelas características do sistema apresentadas, pode-se afirmar que os principais gargalos do sistema são a banda utilizada pela unidade de controle multiponto e o desempenho das unidades de controle multiponto e não a capacidade de armazenamento de salas ou de usuários do sistema.

A banda utilizada pela unidade de controle multiponto é crítica para conferências realizadas na Internet, enquanto que o desempenho dela é o ponto crítico para conferências com menos restrições de banda, como em redes locais Gigabit Ethernet.

Para se avaliar a escalabilidade com respeito à banda consumida para recepção e transmissão da unidade de controle multiponto, basta conhecer a banda ocupada pelo *codec* de áudio utilizado na conferência e a banda ocupada pelo canal de controle.

A escalabilidade do sistema segundo o desempenho da unidade de controle multiponto é mais difícil de ser avaliada, porque depende de muitas variáveis, como recursos de *hardware*, de *software* e da eficiência da sua implementação. Porém, a influência desse conjunto de variáveis resume-se à observação do tempo que a unidade de controle multiponto leva para encaminhar para os pacotes recebidos.

O comportamento da unidade de controle multiponto depende se a abordagem é multitarefa ou multiprocessos e do número de salas virtuais abertas simultaneamente,

pela forma como o tempo de processamento passa a ser distribuído entre os processos e tarefas concorrentes.

4.8 Considerações finais

O sistema de conferência foi desenvolvido de forma a reproduzir a dinâmica conversacional dentro de uma sala de aula: o professor dirigindo-se aos alunos na maior parte do tempo e, às vezes, um aluno falando à sala de aula, com a devida autorização do professor.

O sistema de conferência foi projetado para funcionar transparentemente com NATs e NAPT's, visto que os usuários do sistema podem encontrar-se atrás desses equipamentos. O sistema de conferência pode ser utilizado de forma independente ou de forma integrada a um sistema externo.

O sistema de conferência multiponto foi subdividido em quatro subsistemas: subsistema de acesso às salas virtuais de conferência, subsistema de gerenciamento, subsistema de comunicação de tempo real e a base de dados. Essa subdivisão permitiu uma melhor direção na implementação do sistema.

A arquitetura do sistema de conferência derivada da arquitetura cliente-servidor. Do lado do servidor, a arquitetura do sistema de conferência é composta pelo servidor *web*, pelos servidores da base de dados, pelo servidor de unidades de controle multiponto e pelas unidades de controle multiponto. Pelo lado do cliente, ela é composta pela página *web* e pela *applet* Java do usuário.

O sistema de conferência é centralizado, utilizando como mecanismo de distribuição de pacotes de conferência (RTP/RTCP e pacotes de controle) o IP *unicast* e uma unidade de controle de conferência. O sistema de conferência oferece comunicação por áudio através do protocolo RTP/RTCP entre os participantes de uma conferência e, adicionalmente, comunicação por texto.

Foi implementado um protocolo de controle de conferência para realizar controle de sessão e controle de posse da palavra. O controle de posse da palavra é utilizado para coordenar a conversação dentro da conferência e a utilização de banda. Devido à

existência do mecanismo de controle de posse da palavra, dois papéis sociais distintos surgem dentro da conferência, o de moderador e o de participante comum.

O moderador pode ser definido de três formas distintas: previamente, na configuração da sala virtual de conferência (*moderador fixo*); o primeiro participante que entrar na conferência torna-se o moderador (*moderador flexível*) e o participante com a posse da palavra torna-se o moderador (*moderador dinâmico*). Somente as duas primeiras formas estão disponíveis na versão atual do sistema de conferência.

O sistema de conferência oferece diferentes tipos de salas virtuais de conferência, de forma a atender diferentes políticas de acesso: *salas fechadas*, restritas aos usuários cadastrados e associados a elas; *salas abertas*, acessíveis somente pelos usuários cadastrados; *salas livres*, disponíveis para usuários cadastrados e não cadastrados, e *salas temporárias*, semelhantes às *salas livres*, mas são criadas dinamicamente e destruídas quando o moderador a abandona.

O servidor *web* hospeda o *site* de gerenciamento e o *site* de conferência. Somente o administrador do sistema pode acessar o *site* de gerenciamento, onde ele pode gerenciar os usuários do sistema e as salas virtuais de conferência. O *site* de conferência permite aos usuários visualizar as salas virtuais de conferência disponíveis e acessá-las.

O servidor da base de dados armazena as informações a respeito dos usuários, as configurações das salas virtuais de conferência e as associações entre usuários e salas.

O servidor de unidades multiponto recebe requisições HTTP do servidor *web* para iniciar e terminar as unidades de controle multiponto associadas a cada sala virtual de conferência. As unidades de controle multiponto são iniciadas e terminadas instanciando-se e destruindo-se objetos internamente ao servidor de unidades de controle multiponto. Servidores de unidades de controle multiponto podem ser distribuídos pela rede, de forma a se aumentar a escalabilidade do sistema de conferência, desde que se contorne as restrições de segurança impostas pela *applet* Java do usuário.

A unidade de controle multiponto provê a comunicação entre todos os participantes da conferência, encaminhando os pacotes RTP/RTCP e os pacotes de controle de

conferência recebidos para os demais participantes. A unidade de controle multiponto implementa o mecanismo de controle de posse da palavra, reagindo conforme as determinações do moderador da conferência. A unidade de controle multiponto é completamente independente de *codec*, porque que ela não realiza mixagem, nem transcodificação. Essa independência de *codec* confere a ela uma maior flexibilidade de uso e maior escalabilidade, visto que essas operações são bastante custosas computacionalmente.

A página *web* do usuário oferece uma representação da sala virtual de conferência para ele. A interface homem-máquina foi implementada em uma página *web*, utilizando o conceito WYSIWIS (*What You See Is What I See* – O Que Você Vê É O Que Eu Vejo) (vide Capítulo 2.3). Conseqüentemente, as interfaces homem-máquina de todos os participantes na conferência precisam estar sincronizadas. A sincronização é feita através dos pacotes de controle de conferência, mas também pode ser feita a partir de uma sincronização explícita consultando-se o servidor *web*.

Por ser implementada com tecnologia *web*, a interface homem-máquina do usuário pode ser facilmente personalizada. Três variantes da interface homem-máquina foram desenvolvidas, de forma a atender diferentes casos de uso: *janela inteira*, para quando o sistema de conferência for utilizado de forma independente; *janela flutuante* e *janela mínima*, para quando o sistema for utilizado de forma integrada a um sistema externo, onde o usuário necessita visualizar outras informações simultaneamente.

A *applet* Java fica embutida na página *web* do usuário e oferece captura, codificação, decodificação e reprodução de áudio, além de transmissão e recepção de pacotes RTP/RTCP e de controle de conferência de e para a unidade de controle multiponto.

No próximo capítulo são relatados testes que demonstram o funcionamento do sistema de conferência, comprovando que ele atende aos requisitos levantados no capítulo anterior e descritos neste capítulo. Também são expostos testes que avaliam o desempenho do sistema de conferência, sob aspectos objetivos e subjetivos.

5. RESULTADOS EXPERIMENTAIS

“Qual é mais fácil? Dizer ao paralisado: Estão perdoados os teus pecados, ou dizer: Levanta-te, toma o teu leito e anda?”

Marcos 2.9

Dentre as principais características do sistema de conferência, as quatro mais importantes para um usuário são:

- **Usabilidade:** Depende de quão bem foi projetado e implementado o sistema de conferência como um todo, principalmente a interface-homem máquina do usuário na sala virtual de conferência.
- **Interatividade:** Depende do tempo de resposta do sistema de conferência, que por sua vez depende dos tempos de resposta da unidade de controle multiponto e da *applet* Java do usuário, mas acima de tudo, das condições da rede e dos canais de comunicação disponibilizados pelo sistema de conferência para o usuário. Um grande atraso na rede tornará mais lenta a interação entre os usuários, prejudicando a interatividade.
- **Qualidade subjetiva de voz:** Depende do *codec* de áudio utilizado, da taxa de perdas de pacotes, do atraso da rede e do *jitter* (vide Capítulo 2.1.1).
- **Banda utilizada:** Depende da banda utilizada pelo *codec* de áudio (RTP e RTCP), pelo protocolo de controle de conferência e pelo protocolo HTTP. Essa característica permite a um usuário em potencial do sistema de conferência avaliar se a banda ao seu dispor é suficiente para participar de uma conferência.

Entretanto, para a pessoa ou empresa proprietária do sistema de conferência, as principais características do sistema de conferência são:

- **Banda utilizada por usuário:** Conhecer a banda utilizada por usuário em conferência é necessário para se dimensionar a banda a ser contratada para atender a um certo número de usuários simultâneos.
- **Capacidade de processamento necessário:** Conhecer qual a capacidade de processamento demandada por uma unidade de controle multiponto para atender um certo número de usuários simultâneos também é importante.
- **Capacidade do sistema:** Dada uma determinada banda disponível e uma determinada capacidade de processamento, descobrir quantos usuários simultâneos podem estar em conferências é importante para o proprietário do sistema de conferência.
- **Escalabilidade do sistema:** Descobrir onde estão os gargalos do sistema de conferência, os fatores que afetam a sua escalabilidade, ajuda a direcionar novos esforços para aumentar a sua capacidade. A banda ou a capacidade de processamento disponível será o gargalo do sistema de conferência.

Para o proprietário do sistema de conferência, essas características afetam o custo do sistema. As vantagens de negócio que podem ser proporcionadas pelo sistema de conferência não pertencem ao escopo deste trabalho e, portanto, não serão discutidas.

A avaliação do sistema de conferência depende de métricas subjetivas:

- Usabilidade;
- Interatividade;
- Qualidade subjetiva do áudio.

E métricas objetivas:

- Bandas de recepção e de transmissão da unidade de controle multiponto e da *applet* Java;

- Tempo de resposta da unidade de controle multiponto (atraso do primeiro pacote encaminhado e intervalo de tempo entre os demais pacotes encaminhados);
- Utilização de processador e de memória pela unidade de controle multiponto e pela applet Java;

Para se avaliar as métricas e características do sistema de conferência descritas acima, foram elaborados os seguintes testes:

- **Testes de utilização de banda:** Utilizando uma rede Fast Ethernet em um cenário controlado, o mecanismo de controle de posse da palavra foi avaliado no papel de mecanismo de restrição da banda consumida pelo sistema de conferência. Foram realizadas medições para se revelar qual a banda consumida pelos participantes da conferência e pela unidade de controle multiponto.
- **Testes de desempenho:** Utilizando o mesmo cenário anterior, o desempenho da unidade de controle multiponto foi avaliado com relação aos seus tempos de resposta, utilização de capacidade de processamento, oferecendo indicações da capacidade do sistema de conferência.
- **Testes remotos:** Utilizando cenários reais de uso, onde ocorrem restrição de banda, atraso e perda de pacotes mais pronunciados, pode-se avaliar o impacto desses fatores na interatividade, na qualidade subjetiva de áudio e na experiência geral de uso do sistema de conferência.
- **Avaliação subjetiva:** Nesses testes, a experiência geral de uso do sistema é relatada, dando as impressões com relação à usabilidade, interatividade e qualidade subjetiva de voz, norteando melhorias futuras para o sistema de conferência.

Os demais testes também foram realizados para completar a investigação a respeito do sistema de conferência:

- **Testes das funcionalidades oferecidas:** As principais funcionalidades descritas no Capítulo 4 foram testadas, para mostrar que o sistema as suporta.
- **Testes com o controle de posse da palavra:** Esses testes visam: comprovar sua função de controle de fluxo conversacional; avaliá-lo como mecanismo de restrição de banda em conferências multiponto; descobrir o seu tempo de resposta e verificar como ele afeta a interatividade de uma conferência.
- **Testes com NAPT:** Foram realizados testes com participantes da conferência atrás de um NAPT (*Network Address and Port Translator*) (HOLDREGE, SRISURESH, 1999), para se comprovar o funcionamento transparente do sistema de conferência na presença desse equipamento (vide Capítulo 2.4.3).

Os testes foram agrupados da seguinte forma:

- Testes funcionais
 - Testes das funcionalidades do administrador do sistema
 - Testes das funcionalidades do usuário do sistema
 - Testes das funcionalidades gerais (controle de posse da palavra, integração com outro sistema e funcionamento com NAPT)
- Testes quantitativos
 - Testes de utilização de banda
 - Testes de desempenho (tempo de resposta do controle de posse da palavra, tempo de resposta da unidade de controle multiponto e utilização de recursos computacionais)
- Testes qualitativos
 - Testes remotos
 - Avaliação subjetiva (interatividade, usabilidade e qualidade subjetiva de voz)

5.1 Ambientes de testes

O *codec* de áudio em todos os testes foi o GSM (ETSI, 1998), com três *frames* de áudio de 20 ms sendo carregados em cada pacote RTP. Cada *frame* de áudio GSM ocupa 33 B, então, o tamanho (S) do quadro Ethernet resultante é dado pela Equação (22).

$$\begin{aligned} S &= 14 B \text{ (cabeçalho Ethernet)} + 20 B \text{ (cabeçalho IP)} + 8 B \text{ (cabeçalho UDP)} \\ &\quad + 12 B \text{ (cabeçalho RTP)} + 3 \cdot 33 B \text{ (áudio GSM)} + 4 B \text{ (FCS Ethernet)} \\ &= 157 B \end{aligned} \quad (22)$$

Pelo fato do GSM produzir um *frame* de áudio a cada 20 ms, 50 *frames* de áudio são produzidos por segundo. Como o RTP está transportando três *frames* GSM por pacote, são gerados 50/3 pacotes RTP por segundo, aumentando o atraso do *codec* de 20 ms para 60 ms, mas reduzindo a banda consumida por um canal de áudio de 36.400 bps ($B_{1 \text{ GSM}}$) para 20.933,3 bps ($B_{3 \text{ GSM}}$), devido à redução do *overhead* dos protocolos, como mostrado nas Equações (23) e (24), respectivamente.

$$B_{1 \text{ GSM}} = 91 B \cdot 8 \cdot 50 = 36.400,0 \text{ bps} \quad (23)$$

$$B_{3 \text{ GSM}} = 157 B \cdot 8 \cdot \frac{50}{3} = 20.933,3 \text{ bps} \quad (24)$$

A maioria dos testes utilizam a topologia da Figura 5.1: uma rede local Fast Ethernet. Quando o teste utilizar uma topologia diferente desta, ela será mostrada.

Figura 5.1 – Topologia da maior parte dos testes.

O mesmo servidor *S* é o servidor *web*, servidor de banco de dados e unidade de controle multiponto e a Tabela 5.1 traz as suas configurações de *hardware* e *software*. Nenhuma requisição foi feita ao banco de dados e somente o tráfego HTTP referente ao mecanismo de sincronismo dos participantes da sala estava presente durante os testes, com exceção do teste das funcionalidades do sistema.

Tabela 5.1 – Configuração do servidor utilizado como unidade de controle multiponto, servidor *web* e servidor de banco de dados

Configurações de <i>hardware</i>	
Processador	Intel Pentium III 600 MHz (slot 1)
Placa mãe	Asus P3B-F
Memória	512 MB PC133
Placa de rede	3Com EtherLink 10/100 PCI TX NIC (3C905B-TX)
Placa de vídeo	nVidia TNT2 M64 16 MB AGP 2x
Disco rígido	Seagate ST38410A 8.4 GB 5.400 rpm Ultra ATA 66
Configurações de <i>software</i>	
Sistema operacional	Microsoft Windows 2000 Server 5.00.2195 em inglês, Service Pack 4
Servidor <i>web</i>	Microsoft Internet Information Services 5.0
Servidor de banco de dados	Microsoft SQL Server 2000
Máquina virtual Java	Sun Microsystems Java(TM) 2 Runtime Environment, Standard Edition (build 1.4.1_02-b06)

As demais estações foram empregadas como terminais multimídia do usuário, utilizando sistema operacional Microsoft Windows 2000 Professional ou Microsoft Windows XP Professional, a mesma máquina virtual Java de *S*, Java Media Framework 2.1.1e (JMF) (SUN, 2003c), *browser* Microsoft Internet Explorer 5.5 ou superior e configurações de *hardware* variadas, sendo que a estação com menos recursos computacionais possuía um processador Intel Pentium 166 MHz, 64 MB de memória RAM, placa de som Creative Labs SoundBlaster PCI 128 e placa de rede 3Com EtherLink 10/100 PCI TX NIC (3C905B-TX). Porém, essa configuração com menos recursos computacionais demonstrou-se inapropriada para o uso do JMF, havendo lentidão no uso do sistema de conferência. Um computador com um processador superior a 350 MHz e pelo menos 128 MB de memória RAM é recomendável.

5.2 Testes funcionais

O objetivo desses testes é mostrar que o sistema executa corretamente as seguintes funcionalidades básicas apresentadas no Capítulo 4:

- Funcionalidades do administrador do sistema
 - Acesso ao sistema de gerenciamento
 - Listagem, criação, modificação e exclusão de salas
 - Listagem, criação, modificação e exclusão de usuários
 - Associação de usuários a salas
 - Início e término de salas
- Funcionalidades do usuário do sistema
 - Acesso ao sistema
 - Participação em conferências virtuais
- Funcionalidades gerais

- Funcionamento do controle de posse da palavra
- Integração outros sistemas
- Funcionamento transparente com NAPT

Os testes utilizaram salas virtuais de conferência do tipo *livre* com moderador flexível, isto é, o primeiro participante a entrar na sala torna-se o moderador. Quando for utilizado outro tipo de sala virtual e de mecanismo de moderação, as modificações serão explicitadas.

5.2.1 Testes das funcionalidades do administrador do sistema

Nesses testes, as principais funcionalidades do administrador do sistema levantadas no Capítulo 4 são executadas, para comprovar que o sistema de conferência desenvolvido atende aos requisitos especificados.

5.2.1.1 Acesso ao sistema de gerenciamento

O acesso ao sistema de gerenciamento é feito pela tela de acesso mostrada na Figura 5.2 e somente o administrador do sistema pode acessá-lo.

Figura 5.2 – Tela de acesso ao *site* de gerenciamento.

5.2.1.2 Listagem, criação, modificação e exclusão de salas

A Figura 5.3 mostra a tela inicial do *site* de gerenciamento do sistema. Nesta tela, pode-se observar as salas já existentes, com seu número, nome, assunto, tipo e ações possíveis de serem tomadas. O *menu*, comum a todas as telas do *site* de gerenciamento, mostra as tarefas básicas disponíveis para o administrador do sistema.

Figura 5.3 – Tela inicial do *site* de gerenciamento do sistema, listando as salas existentes.

Para se criar uma nova sala, basta escolher a opção *Criar uma nova sala* no *menu*, preencher corretamente as informações pedidas, escolhendo o tipo de sala (*livre*, *fechada*, *aberta* ou *temporária*) e o mecanismo de controle de posse da palavra, como pode ser visto na Figura 5.4.

Gerenciamento do sistema de audiokonferência LARC-SCOPUS - Nova sala - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address http://macademia/controle/salas.asp?numero=-1&acao=criar Links

LARC **Gerenciamento do sistema de conferências** **SCOPUS**

Listar salas | Criar uma nova sala | Listar os usuários cadastrados | Criar um novo usuário | Ajuda | Sair
 Variáveis de aplicação | Importar dados de usuários | Importar dados de salas | Atualizar janela

Criar | Cancelar | Voltar

Configurações gerais	
Número da sala	<input type="text"/>
Tipo da sala	Fechada
Interface homem-máquina	Janela inteira
Nome da sala	<input type="text"/>
Assunto da sala	<input type="text"/>
Número de cadeiras na sala	<input type="text"/> (Tem que ser maior ou igual ao número atual de participantes: 0)
Admitir automaticamente os participantes	☒ Sim ☐ Não
Início da conferência	<input type="text"/> (dd.mm.aaaa hh:mm:ss)
Fim da conferência	<input type="text"/> (dd.mm.aaaa hh:mm:ss)
Ambiente da sala	Definido pelo usuário

Configurações de segurança	
Dono da sala	Depois de associar os participantes a esta sala, você deve escolher o dono dela.
Sala protegida por senha	☐ Sim ☒ Não (A senha é utilizada somente para salas temporárias)
Senha	<input type="text"/>
Confirme a senha	<input type="text"/>

Configurações de portas UDP	
Porta base UDP do usuário	<input type="text"/> (Precisa ser um valor inteiro, múltiplo de 10 entre 1030 e 40000)
Porta base UDP da MCU	<input type="text"/> (Precisa ser um valor inteiro, múltiplo de 10 entre 1030 e 40000)

Configurações de áudio	Configurações de vídeo
Habilitar áudio ☒ Sim ☐ Não	Habilitar vídeo ☐ Sim ☒ Não
Codec de áudio GSM	Codec de vídeo H.263

Configurações de chat de texto	
Habilitar chat de texto	☐ Sim ☒ Não

Configurações de controle de transmissão de pacotes RTP	
Tipo de controle utilizado	Moderador fixo (somente o participante escolhido será o moderador)
Moderador da sala	Depois de associar os participantes a esta sala, você deve escolher o moderador dela, caso você deseje utilizar o mecanismo de moderador fixo.
Endereço IP do moderador	0.0.0.1 (xxx.xxx.xxx.xxx) (Não utilizado)

Configurações avançadas	
Conferência limitada à rede local da MCU	☐ Sim ☒ Não (Não utilizado)
Endereço IP e porta TCP do servidor de MCUs	143.107.111.14:8080 (xxx.xxx.xxx.xxx:yyyyy)
Máscara de rede	0 (Número de bits para o endereço de rede) (Não utilizado)
Endereço IP multicast da conferência	224.0.0.3 (224.xxx.xxx.xxx) (Não utilizado)
TTL do cabeçalho IPv4	32 (Não utilizado)
TOS do cabeçalho IPv4	224 (Não utilizado)

Criar | Cancelar | Voltar

Local intranet

Figura 5.4 – Criação de uma sala virtual de conferência.

A Figura 5.5 mostra a saída para uma sala do tipo *livre* criada com sucesso, no caso, a sala número 4, chamada “A Rocha”, cujo assunto central é “Lições para a vida”.

Figura 5.5 – Sala criada com sucesso.

Para se alterar uma sala, basta selecioná-la no *menu* da Figura 5.5. A tela para a modificação de salas é a mesma tela utilizada para a criação de salas. A Figura 5.6 mostra uma alteração de uma sala realizada com sucesso. No caso, alterou-se o assunto da sala número 4 para “Lições para a vida – Acesso gratuito!”.

Figura 5.6 – Sala modificada com sucesso.

O menu da Figura 5.5 permite que uma sala seja excluída através da opção “Excluir”. Uma tela pedindo a confirmação da exclusão é mostrada ao administrador do sistema, para que a sala não seja excluída equivocadamente (Figura 5.7).

Figura 5.7 – Tela para confirmação de exclusão de sala.

Após a confirmação, a sala é excluída e as salas são listadas, como mostrado na Figura 5.8.

Figura 5.8 – Sala excluída com sucesso.

5.2.1.3 Listagem, criação, modificação e exclusão de usuários

O administrador do sistema pode visualizar os usuários cadastrados a partir da opção *Listar os usuários cadastrados* no menu. A Figura 5.9 mostra os usuários cadastrados no sistema. A tela onde os usuários cadastrados são listados informa também quais usuários estão ativos no sistema, quais podem ser moderadores de salas virtuais de conferência (definido no cadastro do usuário) e oferece, ainda, a opção de enviar um e-mail para todos os usuários, caso deseje-se informá-los a respeito de modificações no sistema. O administrador tem o poder de desabilitar usuários ativos no sistema, caso ocorra algum problema que necessite desse tipo de intervenção.

Figura 5.9 – Usuários cadastrados no sistema.

Há duas formas de se cadastrar usuários no sistema: através do *site* de gerenciamento, pelo administrador do sistema, e através da tela de escolha de salas virtuais de conferência para os usuários não cadastrados. As opções disponíveis no *menu* superior na tela de cadastro de usuário são diferentes para o usuário não cadastrado e para o administrador do sistema. Para o usuário que está se cadastrando no sistema, as únicas opções disponíveis são desistir do cadastro ou cadastrar-se e depois ir para a tela de escolha de salas virtuais, só que agora como usuário cadastrado. A Figura 5.10 mostra a tela de criação de usuário para o administrador do sistema (distinguida pelas opções disponíveis no *menu* superior).

Gerenciamento do sistema de audiokonferência LARC-SCOPIUS - Novo usuário - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address http://macadamia/controle/usuarios.asp?numero=-1&acao=criar Links

LARC **Gerenciamento do sistema de conferências** **SCOPIUS**

Listar salas | Criar uma nova sala | Listar os usuários cadastrados | Criar um novo usuário | Ajuda | Sair
Variáveis de aplicação | Importar dados de usuários | Importar dados de salas | Atualizar janela

Criar | Cancelar | Voltar

Informações pessoais

Nome

Data de nascimento (dd.mm.aaaa)

Sexo Selecione uma opção

Cidade São Paulo

Estado SP

País Brasil

Nacionalidade brasileira

Informações de acesso

Login

Senha

Confirme sua senha

Informações para a conferência

Apelido

Enviar foto? ☐ Sim (**Formatos:** gif, jpeg ou png; **tamanho máximo:** 6.000 bytes; **dimensões (L x A):** 79 x 90 ou 40 x 45).
☒ Não. (Ao invés de enviar uma foto sua, você pode escolher uma imagem da nossa coleção.)

Foto do usuário ativo Browse...
Visualizar imagem | Voltar imagem

Foto do usuário inativo Browse...
Visualizar imagem | Voltar imagem

Pode ser moderador ☒ Sim ☐ Não

Criar | Cancelar | Voltar

Done Local intranet

Figura 5.10 – Cadastro de usuário.

Os processos de modificação e exclusão de usuários são análogos aos mesmos processos para as salas virtuais de conferência.

5.2.1.4 Associação de usuários a salas

Para esse teste, foi utilizada uma sala virtual do tipo *fechada* com moderador fixo. Quando uma sala é criada, ela ainda não possui nenhum usuário associado a ela, devendo essa tarefa ser realizada. No *site* de gerenciamento, para se associar usuários a salas, precisa-se entrar na tela de configuração da sala e escolher a opção *Modificar associação de participantes desta sala* ou então, escolher a opção *Participantes* na tela onde as salas cadastradas são apresentadas. A Figura 5.11 mostra uma sala virtual do tipo *fechada* com moderador fixo e nenhum usuário associado a ela ainda.

Figura 5.11 – Sala virtual sem nenhum usuário associado a ela.

A Figura 5.12 mostra o processo de associação de usuários às salas virtuais. A tela apresenta, à esquerda, os usuários cadastrados no sistema que não estão associados à sala e, à direita, os que foram associados a ela. Para se associar um usuário ou conjunto de usuários à sala, basta selecioná-lo(s) e realizar a operação de associação, pressionando o botão [**>>**], respeitando-se a capacidade máxima de cadeiras virtuais da sala. Para desassociar um usuário ou conjunto de usuários de uma sala, basta selecioná-lo(s) e pressionar o botão [**<<**]. A ordem em que os usuários forem associados será a ordem de apresentação deles na página *web* da sala virtual de

conferência. Após as alterações, o administrador do sistema deve confirmá-las, selecionando a opção *Modificar*.

Figura 5.12 – Processo de associação de usuários a uma sala.

Como a sala em questão utiliza o mecanismo de moderador fixo, é necessário agora definir quem será o moderador da sala, na tela de conferência da sala virtual. A Figura 5.13 mostra a escolha do moderador. Enquanto o moderador não for definido para a sala virtual com mecanismo de moderador fixo, a sala não pode ser iniciada.

Figura 5.13 – Escolha do moderador da sala com moderador fixo.

Após a sala do tipo *fechada* ser iniciada, somente os usuários associados a ela conseguem acessá-la na tela de escolha de salas virtuais no *site* de conferência. A Figura 5.14 mostra um usuário cadastrado no sistema, mas não associado à sala, tentando acessá-la. Uma possível modificação do sistema pode fazer a tela de escolha de salas virtuais do *site* de conferência apresentar somente as salas às quais o usuário possui acesso. Escolheu-se mostrar todas as salas para os usuários cadastrados, para que ele tenha conhecimento de todas as salas (iniciadas) disponíveis no sistema.

Figura 5.14 – Mensagem recebida por um usuário cadastrado tentando acessar uma sala virtual do tipo *fechada* sem estar associado a ela.

Quando se utiliza o mecanismo de moderador fixo, não há como um participante ser admitido na conferência, antes que o moderador entre na sala virtual de conferência. Se o participante tenta entrar na conferência antes que o moderador, ele recebe um aviso, informando que o moderador não respondeu ao pedido dele para entrar na conferência, como mostrado na Figura 5.15. Isso não ocorre quando o mecanismo de moderador flexível é utilizado, porque o primeiro participante que entrar na sala virtual torna-se o moderador dela. A Figura 5.15 mostra ainda as cadeiras virtuais reservadas dos demais participantes. A interface homem-máquina utilizada nesse teste é do tipo *janela inteira*, que mostra todas as informações disponíveis a respeito da conferência.

Figura 5.15 – Participante da sala virtual do tipo *fechada* tentando entrar na conferência antes que o moderador.

Outros tipos de salas virtuais também podem ter cadeiras virtuais reservadas e aceitar usuários que não estejam associados explicitamente à sala, desde que seja respeitada a lotação da sala virtual definida na configuração dela no *site* de gerenciamento.

5.2.1.5 Início e término de salas

Quando uma sala virtual de conferência é iniciada no *site* de gerenciamento, suas informações na base de dados são carregadas e armazenadas em variáveis de aplicação do servidor *web* e o servidor de unidades de controle multiponto recebe uma requisição HTTP para iniciar a unidade de controle multiponto associada à sala virtual. A Figura 5.16 mostra a mensagem recebida pelo administrador do sistema quando esse processo é bem sucedido.

Gerenciamento do sistema de conferências

Listar salas | Criar uma nova sala | Listar os usuários cadastrados | Criar um novo usuário | Ajuda | Sair
Variáveis de aplicação | Importar dados de usuários | Importar dados de salas | Atualizar janela

A operação 'iniciar' foi realizada com sucesso para a sala 2004.
A MCU da sala 2004 foi iniciada com sucesso.
 Clique aqui para criar uma nova sala.

Número	Nome	Assunto	Tipo	Status	Opções
1	Sala 1	Sala 1	Aberta	Fechada	Participantes Iniciar Excluir
2	Sala 2	Sala 2	Livre	Fechada	Participantes Iniciar Excluir
4	A Rocha	Lições para a vida - Acesso gratuito!	Livre	Fechada	Participantes Iniciar Excluir
5	Sala 5	Sala Demonstracao	Livre	Fechada	Participantes Iniciar Excluir
2004	Sala 2004	Sala 2004	Livre	Iniciada (0)	Participantes Fechar Excluir

Há 5 salas cadastradas.

Figura 5.16 – Sala iniciada com sucesso.

Quando a sala virtual de conferência é fechada com sucesso (Figura 5.17), suas variáveis de aplicação no servidor *web* são destruídas e a unidade de controle multiponto associada a ela é fechada.

Figura 5.17 – Sala fechada com sucesso.

A Figura 5.18 mostra o servidor de unidades de controle multiponto recebendo e executando com sucesso as requisições para iniciar (linha: “[SocketServerMCU] Requisição: GET /xml.asp?ação=iniciar&sala=2004...””) e terminar (linha: “[SocketServerMCU] Requisição: GET /xml.asp?acao=fechar&sala=2004 HTTP/1.0”) a unidade de controle multiponto associadas à sala virtual de conferência número 2004.

```

C:\WINNT\system32\java.exe
[SocketServerMCU] Porta para servidor nao definida. Porta alocada default: 8080
[SocketServerMCU] Porta alocada para o servidor: 8080
[SocketServerMCU] Requisicao: GET /xml.asp?acao=iniciar&sala=2004&nome=Sala+2004&assunto=Sala+2004&p
ortaBaseMCU=8000&portaBaseUsuario=7000&tos=false HTTP/1.0
[Sala: 2004] Iniciando MCU.....
[Sala: 2004] Porta Base MCU:8000
[Sala: 2004] Porta Base Usuario:7000
[Sala: 2004] Trafficclass:false
[Sala: 2004] SSRC_MCU: 1767362432
[Sala: 2004] MCU iniciada
[SocketServerMCU] Requisicao: GET /xml.asp?acao=fechar&sala=2004 HTTP/1.0
[Sala: 2004] MCU Finalizada.....

```

Figura 5.18 – Servidor de unidades de controle multiponto iniciando e fechando com sucesso a unidade de controle multiponto associada à sala virtual.

Se o servidor de unidades de controle multiponto estiver indisponível no momento em que uma sala virtual de conferência é iniciada, obtém-se o resultado mostrado na Figura 5.19. Não é possível realizar conferências sem a unidade de controle multiponto. Nesse caso, a solução é fechar a sala e tentar iniciá-la novamente.

Gerenciamento do sistema de conferências

Listar salas | Criar uma nova sala | Listar os usuários cadastrados | Criar um novo usuário | Ajuda | Sair
Variáveis de aplicação | Importar dados de usuários | Importar dados de salas | Atualizar janela

A operação 'iniciar' foi realizada com sucesso para a sala 2004.

Erro número -2147012867 - A connection with the server could not be established
Ocorreu um erro ao se conectar com a MCU.

Clique aqui para criar uma nova sala.

Número	Nome	Assunto	Tipo	Status	Opções
1	Sala 1	Sala 1	Aberta	Fechada	Participantes Iniciar Excluir
2	Sala 2	Sala 2	Livre	Fechada	Participantes Iniciar Excluir
4	A Rocha	Lições para a vida - Acesso gratuito!	Livre	Fechada	Participantes Iniciar Excluir
5	Sala 5	Sala Demonstracao	Livre	Fechada	Participantes Iniciar Excluir
2004	Sala 2004	Sala 2004	Livre	Iniciada (0)	Participantes Fechar Excluir

Há 5 salas cadastradas.

Figura 5.19 – Sala iniciada, mas com problemas de comunicação com o servidor de unidades de controle multiponto.

A Figura 5.20 mostra uma sala virtual sendo fechada, mas com problemas para se comunicar com o servidor de unidades de controle multiponto.

Figura 5.20 – Sala fechada, mas com problemas de comunicação com o servidor de unidades de controle multiponto.

Se por algum motivo as variáveis de aplicação da sala virtual não forem encontradas no momento em que se requisitar o seu fechamento, recebe-se a mensagem apresentada na Figura 5.21.

Figura 5.21 – Sala fechada, mas com problemas para destruir as variáveis de aplicação do servidor *web*.

Esse problema pode ocorrer, se o administrador do sistema requisitar o fechamento da sala virtual, não esperar a resposta do servidor e fazer uma nova requisição. Como a sala já estava sendo fechada, as variáveis de aplicação já foram destruídas.

A Figura 5.22 mostra a iniciação pelo servidor de unidades de controle multiponto das unidades de controle multiponto das salas números 2004, 4 e 2, nessa ordem.

Figura 5.22 – Várias salas abertas no servidor de unidades de controle multiponto.

Cada sala virtual de conferência opera independentemente das outras salas abertas em paralelo.

5.2.2 Testes das funcionalidades do usuário do sistema

O objetivo dos testes a seguir é comprovar que o usuário é capaz de se cadastrar no sistema e de participar de conferências estando ou não cadastrado.

5.2.2.1 Acesso ao sistema

A Figura 5.23 mostra a tela de acesso ao *site* de conferências.

Figura 5.23 – Tela de acesso ao *site* de conferências.

A tela de acesso ao *site* de conferências conduz os usuários cadastrados à tela de escolha de salas virtuais de conferência e os não cadastrados a uma tela onde eles podem tomar parte de conferências virtuais, mediante o preenchimento de determinadas informações, e também se cadastrar no sistema. Somente as salas virtuais que foram iniciadas são apresentadas para os usuários do sistema na tela de escolha de salas no *site* de conferência (Figura 5.24).

Figura 5.24 – Tela de escolha de salas virtuais de conferência para os usuários cadastrados no sistema.

Para o usuário cadastrado, somente as salas do tipo *fechada* às quais ele não está explicitamente associado não estão à sua disposição, isto é, ele não poderá participar de uma conferência em uma sala virtual do tipo *fechada* à qual ele não está associado.

Acesso ao sistema de audioconferência - Opções disponíveis - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address <http://macademia/opcoes.asp> Links

Sistema de conferências **SCOPLUS**
Atualizar janela | Sair

O que você deseja fazer?

- Desejo me cadastrar no sistema (se você já é cadastrado e está lendo essa mensagem, sua sessão pode ter expirado. Clique aqui)
- Desejo entrar em uma sala

Passo 1: Sem estar cadastrado, você precisa digitar suas informações para entrar em uma sala.

Seu nome: **Sexo:**
Login provisório: **Seu apelido:** **Escolha uma imagem:**
Senha provisória: **Confirme a senha:**
Seu e-mail: **Seu telefone:**
Outras informações:
Ambiente da sala:

Passo 2: Escolha uma sala.

Salas do tipo 'livre' disponíveis: 2.

Nome	Assunto	Número de participantes	Início	Fim
Sala 2	Sala 2	0	12.09.2003	12.09.2003
Sala 2004	Sala 2004	4	12.09.2003	12.09.2003

Se você se cadastrar, você poderá criar salas temporárias e acessar as seguintes salas:

Salas do tipo 'aberta' disponíveis: 1.

Nome	Assunto	Número de participantes	Início	Fim
Sala 1	Sala 1	0	12.09.2003	12.09.2003

Applet Aplicacao initied Local intranet

Figura 5.25 – Tela de escolha de salas virtuais de conferência para os usuários não cadastrados no sistema.

Para o usuário não cadastrado, somente as salas virtuais de conferência do tipo *livre* estão disponíveis para ele, mas as salas do tipo *aberta* também são apresentadas (Figura 5.25). Quando o usuário cadastrado e o não cadastrado abandonam uma sala virtual de conferência, eles retornam às suas respectivas telas de escolha de salas.

5.2.2.2 Participação em conferências virtuais

Tendo por base o conjunto de testes realizados em todo este capítulo, fica claro que o usuário consegue tomar parte em conferências realizadas em salas virtuais. O sistema

foi projetado para que o usuário só consiga entrar em uma única sala virtual de conferência por vez. A Figura 5.26 mostra a mensagem de erro apresentada ao usuário, quando ele tenta entrar em uma segunda sala virtual de conferência.

Figura 5.26 – Mensagem de erro avisando ao usuário que ele já está participando de uma conferência.

5.2.3 Testes das funcionalidades gerais

Nos testes a seguir, são avaliados: o funcionamento do controle de posse da palavra; a integração do sistema de conferência com outro sistema e o funcionamento do sistema de conferência, quando um ou mais participantes da conferência encontram-se atrás de um NAPT.

5.2.3.1 Testes do controle de posse da palavra

Os roteiros de testes apresentados na Tabela 5.2 e na Tabela 5.3 foram executados para mostrar o funcionamento do controle de posse da palavra e o seu impacto na banda utilizada em uma conferência centralizada. Modificou-se a unidade de controle multiponto, para ela registrar todos os seus pacotes recebidos e transmitidos. O roteiro de teste #1 é para uma conferência com dois participantes, enquanto que o roteiro de teste #2 é para uma conferência com três participantes.

Tabela 5.2 – Roteiro de teste para conferência com dois participantes

Roteiro de teste #1	
Tempo (s)	Ações
0	Iniciação da unidade de controle multiponto da sala.
20	Participante <i>A</i> entra na conferência como moderador.
40	Participante <i>B</i> entra na conferência.
60	Moderador bloqueia a sua transmissão de áudio por 10 s deixando o seu microfone mudo, através da sua interface homem-máquina.
80	Moderador bloqueia a recepção de áudio do participante <i>B</i> por 10 s.
100	Moderador concede a posse da palavra ao participante <i>B</i> .
120	Participante <i>B</i> bloqueia a sua transmissão de áudio por 10 s deixando o seu microfone mudo, através da sua interface homem-máquina.
140	Moderador toma a posse da palavra de volta do participante <i>B</i> .
160	Participante <i>B</i> abandona a sala de conferência.
180	Moderador encerra a conferência e abandona a sala.

Tabela 5.3 – Roteiro de teste para conferência com três participantes

Roteiro de teste #2	
Tempo (s)	Ações
0	Iniciação da unidade de controle multiponto da sala.
20	Participante <i>A</i> entra na conferência como moderador.
40	Participante <i>B</i> entra na conferência.
60	Participante <i>C</i> entra na conferência.
80	Moderador bloqueia a recepção de áudio do participante <i>B</i> por 10 s.
100	Moderador bloqueia a recepção de áudio do participante <i>C</i> por 10 s.
120	Moderador concede a posse da palavra ao participante <i>B</i> .
140	Moderador concede a posse da palavra ao participante <i>C</i> .
150	Moderador bloqueia a recepção de áudio do participante <i>B</i> .
160	Moderador bloqueia a recepção de áudio do participante <i>C</i> . Ambos os participantes <i>B</i> e <i>C</i> têm suas recepções de áudio bloqueadas pelo moderador.
170	Moderador permite que o participante <i>B</i> receba áudio.
180	Moderador permite que o participante <i>C</i> receba áudio.
190	Participante <i>B</i> abandona a sala de conferência.
200	Participante <i>C</i> abandona a sala de conferência.
210	Moderador encerra a conferência e abandona a sala.

Para os testes de banda realizados, a unidade de controle multiponto será identificada por *MCU*, o moderador será identificado por *M* e os participantes serão identificados por *A* e *B*, no roteiro de testes #1, e por *A*, *B* e *C*, no roteiro de testes #2, sendo que o participante *A* sempre entra como moderador da conferência. As mensagens de confirmação de recebimento da unidade de controle multiponto, da *applet* Java do moderador e dos participantes serão chamadas de ACK_{MCU} , ACK_M , ACK_A , ACK_B e ACK_C , respectivamente. A banda de transmissão RTP da unidade de controle multiponto será identificada por *RTP_TX* e a banda de recepção RTP por *RTP_RX*.

A Figura 5.27 mostra as bandas de transmissão e de recepção de pacotes RTP da unidade de controle multiponto decorrentes do roteiro de teste #1 e a Figura 5.28 mostra as mesmas bandas para o roteiro de teste #2.

Há uma pequena diferença de tempo entre o instante previsto no roteiro para o instante real de cada evento, porque os testes foram controlados manualmente e não por uma ferramenta de testes autônoma.

Figura 5.27 – Bandas de transmissão e de recepção medidas na unidade de controle multiponto durante o roteiro de testes #1.

Figura 5.28 – Bandas de transmissão e de recepção medidas na unidade de controle multiponto durante o roteiro de testes #2.

No roteiro de testes #1, quando *A* entra na conferência (ao redor de 20s), ele se torna o moderador, *M*, recebe implicitamente a posse da palavra e começa a transmitir seus pacotes RTP de áudio para a *MCU*, mas a *MCU* não tem para quem encaminhar esses pacotes. Por esse motivo RTP_TX é nulo.

Quando *B* pede para entrar na conferência (ao redor de 40s), ele começa a transmitir seus pacotes RTP de áudio, para superar eventuais problemas com o NAPT, causando a elevação de RTP_RX até receber ACK_{MCU} ou uma notificação para parar de transmitir, quando ele pára seu transmissor.

Quando *B* é admitido na conferência, RTP_TX sobe para a banda ocupada por um canal de áudio. Em uma situação onde a *MCU* possa estar recebendo mais de um canal de áudio, somente os pacotes RTP do participante com a posse da palavra é encaminhado, evitando o crescimento de RTP_TX.

No instante em que M bloqueia o seu próprio microfone através da sua interface homem-máquina (ao redor de 60s), parando o seu transmissor, a MCU deixa de receber seus pacotes RTP, causando RTP_RX e, conseqüentemente, RTP_TX a se tornarem nulos. Quando M bloqueia o áudio de B (ao redor de 80s), novamente a MCU não tem para quem encaminhar os pacotes de áudio de M e RTP_TX cai a zero, o mesmo acontecendo a partir do instante em que B abandona a conferência (ao redor de 160 s).

Pode-se observar nos gráficos as diferenças no comportamento de cada transição de posse da palavra, dependendo de quem estava com a posse da palavra e para quem ela foi concedida.

Quando M está com a posse da palavra e a concede para o participante comum B (ao redor de 100s no gráfico do teste #1 e ao redor de 120s no gráfico do teste #2), a unidade de controle multiponto responde com um ACK_{MCU} (vide Anexo C) e passa a esperar os pacotes RTP de áudio do novo dono da posse da palavra, fazendo RTP_TX cair. A seguir, a MCU encaminha a concessão de posse da palavra para os demais participantes e quando B a recebe, ele transmite ACK_B e inicia seu transmissor. Quando o ACK_B é recebido por M , ele pára o seu transmissor e muda sua indicação. Entretanto, se a MCU perceber que M continua transmitindo embora não esteja mais com a posse da palavra, isto é, se B não receber logo a concessão de posse da palavra e se M não receber logo ACK_B , a MCU enviará para M uma notificação para parar de transmitir e ninguém estaria transmitindo, porque M já teria parado seu transmissor e B ainda não teria iniciado o seu, provocando uma queda em RTP_RX.

Quando o participante comum está com a posse da palavra e M a concede para outro (ao redor de 140s no gráfico do teste #1 e ao redor de 200s no gráfico do teste #2), a unidade de controle multiponto responde para M com ACK_{MCU} ao receber a concessão de posse da palavra e passa a esperar pelos pacotes RTP de áudio do novo detentor da posse da palavra, que ainda não começou a transmitir. Enquanto o antigo detentor da posse da palavra não receber a concessão da posse da palavra para o outro participante, ele continua a transmitir pacotes RTP, o que explica a queda de RTP_TX da unidade de controle multiponto, enquanto a RTP_RX permanece

constante. Então, por um curto período de tempo, a unidade de controle multiponto continua a receber o áudio dele, mas não encaminha mais seus pacotes. Se o novo detentor da posse da palavra começar a transmitir antes do antigo detentor parar, a unidade de controle multiponto receberá o tráfego equivalente a dois canais de áudio, aumentando RTP_RX, mas somente os pacotes RTP do novo detentor serão encaminhados, mantendo RTP_TX limitado a um canal de áudio.

A principal diferença entra os roteiros de testes #1 e #2 é RTP_TX em todas as situações, devido à presença de um número maior de participantes na conferência. Ambos os testes mostram que RTP_RX está continuamente restrito a um único canal de áudio, exceto por curtos períodos de tempo, quando os participantes estão pedindo para entrar na conferência, devido aos possíveis problemas com NAPT, e durante transições de posse da palavra. Isso mostra que o controle de posse da palavra é eficaz para o controle da banda em uma conferência multiponto.

5.2.3.2 Teste de integração com outro sistema

Para ilustrar a integração do sistema desenvolvido com qualquer outro sistema capaz de abrir uma janela de um *browser* e passar os parâmetros necessários, desenvolveu-se uma página *web* simples, mostrada na Figura 5.29. O teste foi realizado visando uma futura integração com a ferramenta de ensino a distância do LARC (LARC, 2003), o COL – Cursos On LARC (COL, 2003). A página *web* contém *links* que simulam os *links* a serem colocados no COL, na página de cada usuário. O *link* do professor o conduz a uma tela onde ele pode iniciar e encerrar a sala virtual de conferência do tipo *temporária* associada à matéria ministrada por ele. A sala utiliza o mecanismo de moderador fixo e o professor exerce o papel de moderador. Quando o professor abandona a sala de aula virtual, ela é fechada e a conferência é encerrada.

O *link* do professor passa os seguintes parâmetros para o sistema desenvolvido:

- **Login:** O parâmetro *login* refere-se ao *login* do professor no COL.
- **Senha:** O parâmetro *senha* refere-se à senha do professor no COL.

- **Ação:** Esse parâmetro refere-se à ação desejada com relação à sala. A primeira ação passada é a de configuração da sala, portanto o professor é conduzido à tela de configuração da sala.
- **Número da sala:** Informa o número da sala virtual do tipo *temporária*.
- **Nome da sala:** Informa o nome da sala. No caso do COL, informa o nome da matéria ministrada pelo professor.
- **Assunto da sala:** Informa o assunto da matéria ministrada pelo professor.
- **Número de cadeiras na sala:** Informa qual o número máximo de alunos que podem entrar na sala de aula virtual.

Os *links* dos alunos passam os seguintes parâmetros para o sistema desenvolvido:

- **Login:** Refere-se ao *login* do aluno no COL.
- **Senha:** Refere-se à senha do aluno no COL.
- **Origem:** Informa se as demais informações sobre aluno deverão ser obtidas acessando à base de dados do COL ou se elas estão sendo passadas como parâmetros para a página alvo do *link*.
- **Número da sala:** Informa qual a sala de aula virtual que o aluno está tentando acessar.
- **Destino:** Define se a sala de aula virtual deve ser aberta em uma nova janela do *browser* ou na mesma.

Figura 5.29 – Página web criada para teste de integração com o COL, contendo os links para o professor e para os alunos.

O aluno não pode entrar na conferência antes que o professor, senão seu pedido para entrar na conferência não será respondido. Se o aluno tentar entrar na sala antes mesmo do professor iniciá-la, ele receberá a mensagem mostrada na Figura 5.30.

Figura 5.30 – Aluno tentando acessar a sala de aula virtual sem ela ter sido iniciada pelo professor.

Se a sala de aula virtual já tiver sido iniciada pelo professor, quando o aluno seguir o seu *link*, ele será conduzido a uma página web onde ele deve confirmar suas informações pessoais e completar as demais informações necessárias para que ele tome parte em uma conferência. A quantidade de informações que ele terá ainda que

preencher depende da presença ou não no sistema a ser integrado, o COL, no caso, das informações obrigatórias para o sistema de conferência. Essa página *web* é mostrada na Figura 5.31. O COL, por exemplo, não possui fotos dos seus usuários em sua base de dados e o sistema de conferência precisa de uma imagem para representar cada participante dentro da conferência e fora dela na interface homem-máquina. Pensando nessa questão, foi desenvolvido um banco de imagens para o usuário escolher a imagem que o representará dentro da sala virtual de conferência.

COL - Acesso ao sistema de conferência - Microsoft Internet Explorer

Antes de entrar na sala de conferência é necessário:

- Que você confirme os seus dados e escolha uma imagem.
- Que seja verificada a sua instalação do Java Media Framework (JMF).

Seu nome:	Reinaldo Matushima		Sexo:	Masculino
Login:	reinaldo.matushi	Seu apelido:	reinaldo.matushi	Escolha uma imagem:
Senha:	*****	Confirme a senha:	*****	
Seu e-mail:	reinaldo.matushime	Seu telefone:	25525558	
Outras informações:				

Verificando a instalação do Java Media Framework:

JMF Versao... 2.1.1e

Win32 Build

Bibliotecas Encontradas - Instalacao OK

Entrar na sala de conferência

Download do Java Media Framework 2.1.1e da Sun Microsystems | Site do Java Media Framework

Download da Java Virtual Machine 1.4.2 da Sun Microsystems | Site do Java

Figura 5.31 – Página *web* para o aluno confirmar suas informações pessoais e preencher as demais informações necessárias.

Para o professor, o primeiro passo é a configuração da sala, onde ele pode alterar os parâmetros passados, configurar uma senha de acesso para a sala, habilitar ou não o *chat* de texto entre outras possibilidades.

Sala temporária - Microsoft Internet Explorer

LARC **Gerenciamento do sistema de conferências** **SCOPLUS**
Fechar

Iniciar sala

Configurações gerais	
Número da sala temporária	40010
Nome da sala	Laboratório de Redes de Computadores - Experiência de camada de rede
Assunto da sala	Nessa experiência, o aluno conhecerá melhor o protocolo IPv4 e o funciona
Número de cadeiras na sala	20 (A sala tem que ter entre 2 e 50 cadeiras)
Admitir automaticamente os participantes	☐ Sim ☒ Não
Início da conferência	10.10.2003 (dd.mm.aaaa hh:mm:ss)
Fim da conferência	10.10.2003 (dd.mm.aaaa hh:mm:ss)

Configurações de segurança	
Dono da sala	wilson
Sala protegida por senha	☒ Sim ☐ Não
Senha	*****
Confirme a senha	*****

Configurações de chat de texto	
Habilitar chat de texto	☒ Sim ☐ Não

Figura 5.32 – Primeira tela para o professor: configuração da sala de aula virtual.

Estando a sala de aula virtual já configurada, o professor deve iniciá-la, através da opção *Iniciar sala*. Depois que a sala for iniciada, o professor pode fechá-la ou entrar nela. Se o professor desejar alterar alguma informação, ela deve ser encerrada primeiramente. A Figura 5.33 mostra uma sala de aula virtual iniciada com sucesso.

Figura 5.33 – Sala de aula virtual iniciada pelo professor.

A Figura 5.34 mostra uma sala de aula virtual encerrada pelo professor.

Figura 5.34 – Sala de aula virtual fechada pelo professor.

Se o professor decidir entrar na sala de aula virtual, ele é levado agora a uma página *web* semelhante à dos alunos, para confirmar suas informações pessoais.

COL - Acesso ao sistema de conferência - Microsoft Internet Explorer

Antes de entrar na sala de conferência é necessário:

- Que você confirme os seus dados e escolha uma imagem.
- Que seja verificada a sua instalação do Java Media Framework (JMF).

Seu nome:	Wilson Ruggiero		Sexo:	Masculino
Login:	wilson	Seu apelido:	wilson	Escolha uma imagem:
Senha:	XXXXXXXXXXXXXXXXXXXX	Confirme a senha:	XXXXXXXXXXXXXXXXXXXX	
Seu e-mail:	wRug@larc.usp.br	Seu telefone:	84258425	
Outras informações:	LARC-EPUSP			

Verificando a instalação do Java Media Framework:

JMF Versao... 2.1.1e

Win32 Build

Bibliotecas Encontradas - Instalacao OK

Entrar na sala de conferência

Download do Java Media Framework 2.1.1e da Sun Microsystems | Site do Java Media Framework

Download da Java Virtual Machine 1.4.2 da Sun Microsystems | Site do Java

Figura 5.35 – Página *web* para confirmação dos dados do professor.

A Figura 5.36 mostra a sala de aula virtual já com o professor e o aluno presentes. A página *web* da sala virtual de conferência desse teste de integração foi configurada para utilizar a interface homem-máquina do tipo *flutuante*, porque ocupa menos espaço que a do tipo *janela inteira*, mas também mostra o nome dos participantes. Por esse motivo, são omitidas as informações a respeito do nome, assunto e capacidade da sala.

Figura 5.36 – Sala de aula virtual com um professor e um aluno presentes.

5.2.3.3 Testes com NATP

O objetivo desse teste é mostrar que o sistema funciona mesmo quando um ou mais usuários encontram-se atrás de um NATP.

A Figura 5.37 mostra a topologia de rede utilizada para os testes com o NATP.

Figura 5.37 – Topologia de rede utilizada para os testes com NATP.

A estação *S* é o servidor *web*, servidor de banco de dados e unidade de controle multiponto, enquanto que as estações *A* e *B* são o moderador e um participante

comum, respectivamente. A estação *C* foi utilizada para se monitorar o tráfego da conferência no *hub* de 100 Mbps e para isso foi utilizado o *software sniffer* Advisor Lan da Agilent Technologies, versão 15.0.0.1000 (AGILENT, 2003).

Utilizou-se um roteador Cisco 2514 com o Cisco IOS™ 2500 (C2500-I-L) versão 12.1(20) (CISCO, 2003) como NAPT. As configurações de NAPT do roteador são apresentadas na Figura 5.38.

```
version 12.1
!
hostname ChatVoz
!
ip subnet-zero
!
ip dhcp pool 0
network 192.168.2.0 255.255.255.0
dns-server 143.107.111.43 143.107.255.3
netbios-name-server 143.107.111.6
netbios-node-type h-node
default-router 192.168.2.1
domain-name larc.usp.br
lease infinite
!
interface Ethernet0
ip address 192.168.2.1 255.255.255.0
ip nat inside
no ip mroute-cache
no cdp enable
!
interface Ethernet1
ip address 143.107.111.15 255.255.255.0
ip nat outside
no ip mroute-cache
no cdp enable
!
ip nat translation udp-timeout 3600
ip nat inside source list 1 interface Ethernet1 overload
ip classless
ip route 0.0.0.0 0.0.0.0 143.107.111.1
!
access-list 1 permit 192.168.2.0 0.0.0.255
no cdp run
```

Figura 5.38 – Configurações de NAPT do roteador Cisco 2514.

O motivo de se utilizar a topologia da Figura 5.37 ou, mais explicitamente, o motivo de se colocar duas estações atrás do mesmo NAPT, deve-se ao fato dos problemas com o NAPT surgirem principalmente quando há uma ou mais aplicações em

estações diferentes na sua rede interna necessitando utilizar a mesma porta TCP ou UDP.

Se houvesse apenas uma estação, o problema com o NAPT poderia não ocorrer, porque alguns NAPTs só realizam tradução de portas a partir do instante em que a mesma já está em uso. O roteador Cisco 2514 utilizado funciona dessa forma: quando possível, o NAPT mantém a porta UDP de origem inalterada. Outra característica do roteador utilizado, é que ele divide as portas em três faixas: [0, 511], [512, 1.023] e [1.024, 65.535]. Dessa forma, se a porta TCP ou UDP de origem precisar ser traduzida, será utilizada a primeira porta disponível dentro da faixa de portas à qual ela pertence.

Há algumas formas possíveis para se demonstrar que o sistema funciona com NAPT. A forma mais trivial é simplesmente utilizar a topologia acima e verificar que usuários nas estações *A* e *B* conseguem se comunicar um com o outro.

Outra forma seria apresentar gráficos de transmissão e recepção de pacotes RTP capturados nas estações *A* e *B* e mostrar, através do funcionamento do mecanismo de controle de posse da palavra, mas seria necessário alinhar os gráficos no tempo, apesar de não haver um sincronismo perfeito entre as estações *A* e *B*.

A forma escolhida para se comprovar o funcionamento do sistema com NAPT foi através da captura em um *software sniffer* do tráfego da rede interna ao NAPT e da apresentação da tradução de endereços IP e de portas UDP no NAPT. Através dos pacotes capturados pelo *software sniffer*, pode-se ver claramente que uma estação transmite pacotes RTP para *S* enquanto a outra recebe de *S* outros pacotes RTP. Para isso, ambas as estações precisam estar participando da conferência e a unidade de controle multiponto precisa estar encaminhando os pacotes de controle de conferência e os pacotes RTP para o endereço IP do NAPT e para suas portas UDP corretas. Então, a captura de endereços IP e de portas UDP na unidade de controle multiponto precisa obrigatoriamente estar funcionando de forma correta e o NAPT também. A Figura 5.39 mostra os pacotes da conferência capturados na rede interna do NAPT, enquanto a Figura 5.40 mostra a tradução de endereços IP e de portas UDP no NAPT e a mostra as portas capturadas pela unidade de controle multiponto.

Capture Buffer : Decode : Decode Data

Frame	Len	Absolute Time	Source	Destination	Prot	Description
3569	157	18:48:01.826276	192.168.2.2	143.107.111.14	RTP	Payload=GSM
3570	157	18:48:01.826402	143.107.111.14	192.168.2.4	RTP	Payload=GSM
3571	157	18:48:01.926420	192.168.2.2	143.107.111.14	RTP	Payload=GSM
3572	157	18:48:01.926546	143.107.111.14	192.168.2.4	RTP	Payload=GSM
3573	157	18:48:01.976492	192.168.2.2	143.107.111.14	RTP	Payload=GSM
3574	157	18:48:01.976618	143.107.111.14	192.168.2.4	RTP	Payload=GSM
3575	157	18:48:02.016550	192.168.2.2	143.107.111.14	RTP	Payload=GSM
3576	157	18:48:02.016676	143.107.111.14	192.168.2.4	RTP	Payload=GSM
3577	157	18:48:02.066622	192.168.2.2	143.107.111.14	RTP	Payload=GSM
3578	157	18:48:02.076636	143.107.111.14	192.168.2.4	RTP	Payload=GSM
3579	157	18:48:02.106680	192.168.2.2	143.107.111.14	RTP	Payload=GSM
3580	157	18:48:02.116694	143.107.111.14	192.168.2.4	RTP	Payload=GSM

Figura 5.39 – Pacotes da rede interna do NAPT capturados no *software sniffer*.

O tráfego foi capturado na rede interna do NAPT. Pela Figura 5.39 pode-se afirmar que *A* (endereço IP 192.168.2.2) está com a posse da palavra, já que ele está transmitindo seus pacotes de RTP de áudio (*codec* GSM) para a *MCU* (endereço IP 143.107.111.14) (*frames* ímpares) e ela está encaminhando esses pacotes para *B* (endereço IP 192.168.2.4) (*frames* pares). Certamente que a tradução de endereços e portas foi feita corretamente, caso contrário a comunicação de *A* e *B* com a *MCU* não teria sido estabelecida.

Command Prompt - telnet 143.107.111.15

```

ChatVoz#show ip nat translations | include udp
Pro Inside global      Inside local      Outside local      Outside global
udp 143.107.111.15:1025 192.168.2.4:7000  143.107.111.14:8000 143.107.111.14:8000
udp 143.107.111.15:1024 192.168.2.4:7004  143.107.111.14:8004 143.107.111.14:8004
udp 143.107.111.15:1026 192.168.2.4:7005  143.107.111.14:8005 143.107.111.14:8005
udp 143.107.111.15:7000 192.168.2.2:7000  143.107.111.14:8000 143.107.111.14:8000
udp 143.107.111.15:7004 192.168.2.2:7004  143.107.111.14:8004 143.107.111.14:8004
udp 143.107.111.15:7005 192.168.2.2:7005  143.107.111.14:8005 143.107.111.14:8005

```

Figura 5.40 – Tradução de endereços IP e de portas UDP no NAPT feita pelo roteador Cisco 2514.

No roteador Cisco 2514, a coluna “*Inside global*” revela quais são o endereço IP e a porta UDP de destino originais do pacote transmitido por uma estação interna (*A* ou *B* nesse teste) ao NAPT que causou a formação da tupla. A coluna “*Inside local*”

indica quais são o endereço IP e a porta UDP de origem originais do mesmo pacote. Por sua vez, a coluna “*Outside local*” registra o endereço IP e a porta UDP de origem traduzidos, isto é, o endereço IP e a porta UDP de origem do pacote transmitido pelo NAPT para a rede externa. Por último, a coluna “*Outside global*” informa o endereço IP e a porta UDP de destino traduzidos, isto é, o endereço IP e a porta UDP de destino do pacote transmitido pelo NAPT para a rede externa. Somente em casos excepcionais o endereço IP e a porta UDP destino são traduzidos. No caso do teste realizado, essas informações permaneceram inalteradas.

```

C:\WINNT\system32\java.exe
[SocketServerMCU] Porta para servidor nao definida. Porta alocada default: 8080
[SocketServerMCU] Porta alocada para o servidor: 8080
[SocketServerMCU] Requisicao: GET /xml.asp?acao=iniciar&sala=2004&nome=Sala+2004&assunto=Sala+2004&p
ortaBaseMCU=8000&portaBaseUsuario=7000&tos=false HTTP/1.0
[Sala: 2004] Iniciando MCU.....
[Sala: 2004] Porta Base MCU:8000
[Sala: 2004] Porta Base Usuario:7000
[Sala: 2004] Trafficclass:false
[Sala: 2004] SSRC MCU: 1812379264
[Sala: 2004] MCU iniciada
[MCU - Processa Controle] Endereco IP encapsulado no pacote de pedido
para entrar na conferencia: /192.168.2.2
[MCU - Processa Controle] SSRC: 411307365->Endereco IP de origem do pacote recebido: /143.107.111.15
[MCU - Processa Controle] SSRC: 411307365->Porta UDP de Controle de Conferencia capturada: 7000
[MCU - Processa Controle] Participante: 0 SSRC: 411307365 solicitou entrada na Conferencia
[MCU - Processa RTP] SSRC: 411307365->Porta UDP do RTP capturada: 7004
[MCU - Processa RTCP] SSRC: 411307365->Porta UDP do RTCP capturada: 7005
[MCU - Processa Controle] Endereco IP encapsulado no pacote de pedido
para entrar na conferencia: /192.168.2.4
[MCU - Processa Controle] SSRC: 411756171->Endereco IP de origem do pacote recebido: /143.107.111.15
[MCU - Processa Controle] SSRC: 411756171->Porta UDP de Controle de Conferencia capturada: 1025
[MCU - Processa Controle] Participante: 1 SSRC: 411756171 solicitou entrada na Conferencia
[MCU - Processa Controle] Participante: 1 SSRC: 411756171 entrou na conferencia
[MCU - Processa RTP] SSRC: 411756171->Porta UDP do RTP capturada: 1024
[MCU - Processa RTCP] SSRC: 411756171->Porta UDP do RTCP capturada: 1026
[MCU - Processa Controle] Participante: 1 SSRC: 411756171 saiu da conferencia
[MCU - Processa Controle] Moderador encerrou a conferencia
[SocketServerMCU] Requisicao: GET /xml.asp?acao=fechar&sala=2004 HTTP/1.0
[Sala: 2004] MCU Finalizada.....
  
```

Figura 5.41 – Captura de portas pela unidade de controle multiponto.

Como se pode observar pela Figura 5.40 e pela Figura 5.41, o primeiro participante a entrar na conferência (A), no caso, o moderador, teve suas portas UDP do protocolo de controle de conferência, do RTP e do RTCP inalteradas: 7.000, 7.004 e 7.005, respectivamente. O segundo participante a entrar na conferência (B) teve suas portas traduzidas. Os pacotes RTP de áudio são transmitidos antes do que o pacote de pedido para entrar na conferência, para garantir que a unidade de controle multiponto possa encaminhar pacotes RTP para ele ao ser admitido na conferência. Por esse motivo, a porta UDP de origem do RTP foi traduzida para 1.024 e a de controle de

conferência, para 1.025, já que o NAPT recebeu primeiro os pacotes RTP. A porta do RTCP foi traduzida para 1.026. Apenas como observação, se a estação *B* estivesse participando de uma conferência em uma sala virtual atendida por uma unidade de controle multiponto hospedada também em *S*, o NAPT do roteador Cisco 2514 não traduziria as portas UDP de *B*, porque elas estariam associadas a outras portas UDP de *S*, gerando uma nova tupla, mapeada de forma não conflitante com a tupla de *A* com *S*.

A Figura 5.41 mostra que a unidade de controle multiponto da sala 2004 capturou corretamente as informações de *A* (endereço traduzido: 143.107.111.15; endereço IP encapsulado: 192.168.2.2; portas UDP de controle de conferência, RTP e RTCP: 7.000, 7.004 e 7.005, respectivamente) e de *B* (endereço traduzido: 143.107.111.15; endereço IP encapsulado: 192.168.2.4; portas UDP de controle de conferência, RTP e RTCP: 1.025, 1.024 e 1.026, respectivamente), como pode ser observado pelas linhas “[MCU - Processa Controle] SSRC: ...”, “[MCU - Processa RTP] SSRC: ...” e “[MCU - Processa RTCP] SSRC: ...”.

O usuário doméstico, que é um usuário potencial do sistema, provavelmente não terá em sua casa um roteador Cisco 2514, mas um roteador doméstico, com menos opções de configuração, comumente chamado de *broadband router* ou de *home gateway*, utilizado para compartilhar o acesso à Internet em sua rede. A mesma topologia foi utilizada para outro teste com um roteador doméstico ORiNOCO BG-2000 Wireless Broadband Gateway (dados do *firmware*: “Application Code: Gateway_1.1.1; Bootloader 0.09; WiFi: 8.42”) (PROXIM, 2003) no lugar do Cisco 2514. O teste foi realizado com sucesso, mas o roteador doméstico não possui a funcionalidade de mostrar a tabela de tradução de endereços e portas. Esses equipamentos domésticos nem sempre possuem compatibilidade total com os protocolos padrões, podendo o mesmo equipamento possuir comportamentos diferentes com versões diferentes de seus *firmwares*. Com o NAPT não é diferente e por isso não se pode garantir que todos esses roteadores domésticos façam corretamente a tradução de portas.

5.3 Testes quantitativos

Para os testes quantitativos, foi alterada a forma de atribuição de portas base para a *applet* Java do usuário, para que mais de uma instância da *applet* pudesse ser carregada em uma mesma estação, diminuindo o número de estações necessárias para os testes. As portas base UDP da *applet* Java foram atribuídas a partir da porta base UDP original configurada para a sala virtual de conferência no *site* de gerenciamento, acrescentando-se um deslocamento numérico segundo o número da cadeira do participante dentro da conferência.

Foram realizados os seguintes testes para se avaliar o sistema:

- Caracterização da transmissão de pacotes RTP pela *applet* Java do usuário;
- Avaliação do desempenho do controle de posse da palavra;
- Medição da banda total de transmissão e recepção consumida pela unidade de controle multiponto;
- Avaliação do desempenho de uma unidade de controle multiponto;
- Avaliação do desempenho de duas unidades de controle multiponto hospedadas em um mesmo servidor de unidades de controle multiponto (abordagem multitarefa);
- Avaliação do desempenho de duas unidades de controle multiponto hospedadas em diferentes servidores de unidades de controle multiponto (abordagem multiprocesso);
- Avaliação da utilização de recursos computacionais por uma unidade de controle multiponto e pela *applet* Java do usuário.

Nos testes a seguir, foram utilizados os *softwares sniffer* Advisor LAN versão 15.0.0.1000 da Agilent Technologies (AGILENT, 2003) e o Netasyst WLX versão 1.0.003 da Network Associates Technology (NAI, 2003). Foram utilizados alguns recursos de análise de tráfego do primeiro, enquanto que o segundo foi utilizado por

oferecer uma apresentação mais consolidada dos pacotes capturados. Deve ser observado, que o *software sniffer* Netasyst WLX não considera os 4 B do FCS no tamanho do quadro Ethernet, como resultado, os quadros Ethernet transportando um pacote RTP com três *frames* GSM de áudio são apresentados com 153 B, ao invés de 157 B, podendo induzir a erros nos cálculos de utilização de banda.

5.3.1 Caracterização da transmissão de pacotes RTP pela *applet* Java do usuário

Antes dos testes para se avaliar o desempenho da unidade de controle multiponto foi realizado um teste para se caracterizar o transmissor utilizado, a *applet* Java do usuário. Para tanto, foram capturados os pacotes RTP de áudio do moderador por um *software sniffer* na sua própria estação, estando ele sozinho na conferência.

Foi constatado no teste que a *applet* Java do usuário não consegue transmitir os pacotes de áudio em intervalos de tempo regulares (sem *jitter*). Como cada pacote RTP está transportando três *frames* GSM de 20 ms de áudio, a *applet* Java deveria gerar um pacote RTP a cada 60 ms e a unidade de controle multiponto teria em média 60 ms para encaminhar os pacotes para os demais participantes. Porém, pela Figura 5.42 (Netasyst WLX) pode-se notar pela coluna “*Delta Time*”, que os pacotes RTP de áudio são transmitidos com grande variação de atraso.

A Figura 5.43 (Advisor LAN) mostra não somente que o *jitter* médio é de aproximadamente 17 ms, um valor alto (SCHULZRINNE et al., 1996), mas também que a *applet* Java do usuário deixa de transmitir em média cerca de 17% dos pacotes, provocando degradação na reprodução do áudio. Esse comportamento é do próprio JMF²⁰ (SUN, 2003c).

²⁰ O mesmo comportamento foi observado em um programa de exemplo fornecido juntamente com o JMF.

Netasyst WLX (Trial Mode) - Local, Ethernet (Line speed at 100 Mbps) - [Sniff: Filtered 2, 1/441 Ethernet Frames, Filter: Def...

File Monitor Capture Display Tools Database Window Help

Default

No.	Source Address	Dest Address	Summary	Len (Bytes)	Delta Time	Rel. Time
1	[143.107.111.15]	[143.107.111.14]	UDP: D=20004 S=20004	153	0.000.000	0:00:00.000
2	[143.107.111.15]	[143.107.111.14]	UDP: D=20004 S=20004	153	0.044.208	0:00:00.044
4	[143.107.111.15]	[143.107.111.14]	UDP: D=20004 S=20004	153	0.055.626	0:00:00.099
5	[143.107.111.15]	[143.107.111.14]	UDP: D=20004 S=20004	153	0.046.027	0:00:00.145
6	[143.107.111.15]	[143.107.111.14]	UDP: D=20004 S=20004	153	0.093.972	0:00:00.239
7	[143.107.111.15]	[143.107.111.14]	UDP: D=20004 S=20004	153	0.059.046	0:00:00.298
8	[143.107.111.15]	[143.107.111.14]	UDP: D=20004 S=20004	153	0.044.231	0:00:00.343
9	[143.107.111.15]	[143.107.111.14]	UDP: D=20004 S=20004	153	0.059.752	0:00:00.402
10	[143.107.111.15]	[143.107.111.14]	UDP: D=20004 S=20004	153	0.045.662	0:00:00.448
11	[143.107.111.15]	[143.107.111.14]	UDP: D=20004 S=20004	153	0.093.268	0:00:00.541
12	[143.107.111.15]	[143.107.111.14]	UDP: D=20004 S=20004	153	0.059.309	0:00:00.601
15	[143.107.111.15]	[143.107.111.14]	UDP: D=20004 S=20004	153	0.044.638	0:00:00.645
16	[143.107.111.15]	[143.107.111.14]	UDP: D=20004 S=20004	153	0.056.601	0:00:00.702
17	[143.107.111.15]	[143.107.111.14]	UDP: D=20004 S=20004	153	0.042.530	0:00:00.744
18	[143.107.111.15]	[143.107.111.14]	UDP: D=20004 S=20004	153	0.089.870	0:00:00.834
19	[143.107.111.15]	[143.107.111.14]	UDP: D=20004 S=20004	153	0.065.088	0:00:00.899
21	[143.107.111.15]	[143.107.111.14]	UDP: D=20004 S=20004	153	0.037.434	0:00:00.937
23	[143.107.111.15]	[143.107.111.14]	UDP: D=20004 S=20004	153	0.060.609	0:00:00.997
24	[143.107.111.15]	[143.107.111.14]	UDP: D=20004 S=20004	153	0.044.544	0:00:01.042
25	[143.107.111.15]	[143.107.111.14]	UDP: D=20004 S=20004	153	0.107.582	0:00:01.149
28	[143.107.111.15]	[143.107.111.14]	UDP: D=20004 S=20004	153	0.044.195	0:00:01.194
29	[143.107.111.15]	[143.107.111.14]	UDP: D=20004 S=20004	153	0.047.836	0:00:01.242
30	[143.107.111.15]	[143.107.111.14]	UDP: D=20004 S=20004	153	0.043.929	0:00:01.285
31	[143.107.111.15]	[143.107.111.14]	UDP: D=20004 S=20004	153	0.059.408	0:00:01.345
34	[143.107.111.15]	[143.107.111.14]	UDP: D=20004 S=20004	153	0.104.540	0:00:01.449
35	[143.107.111.15]	[143.107.111.14]	UDP: D=20004 S=20004	153	0.043.782	0:00:01.493
36	[143.107.111.15]	[143.107.111.14]	UDP: D=20004 S=20004	153	0.046.254	0:00:01.539
37	[143.107.111.15]	[143.107.111.14]	UDP: D=20004 S=20004	153	0.052.110	0:00:01.592
38	[143.107.111.15]	[143.107.111.14]	UDP: D=20004 S=20004	153	0.044.324	0:00:01.636
40	[143.107.111.15]	[143.107.111.14]	UDP: D=20004 S=20004	153	0.109.758	0:00:01.746

Expert Decode Matrix Host Table Protocol Dist. Statistics Filtered 2 /

For Help, press F1

Figura 5.42 – Pacotes RTP de áudio GSM capturados no transmissor (*software sniffer* Netasyst WLX).

Figura 5.43 – Avaliação de *jitter* e perda de pacotes RTP do transmissor (*software sniffer* Advisor LAN).

5.3.2 Avaliação do desempenho do controle de posse da palavra

Para se avaliar o desempenho do controle de posse da palavra, foi escolhida uma situação de concessão de posse da palavra, por ser uma situação bastante completa sob o ponto de vista de elementos da conferência envolvidos.

O tempo (T_{Total}) entre o momento em que a posse da palavra foi concedida a um participante, até o momento em que ele começa a transmitir pacotes RTP foi medido. Esse tempo sempre será maior ou igual do que a soma dos *round-trip time* (RTT) entre o participante comum e a unidade de controle multiponto (MCU) ($RTT_{Participante-MCU}$) e entre o moderador e a MCU ($RTT_{Moderador-MCU}$), com o tempo de processamento dos pacotes de controle de conferência pelas *applets* Java dos usuários e pela MCU ($T_{Processamento}$). Deve-se, ainda, acrescentar o tempo para se iniciar o transmissor do novo detentor da posse da palavra ($T_{IniciarTransmissor}$), segundo mostra a Equação (27). O tempo efetivamente gasto no controle de posse da palavra ($T_{ControlePossePalavra}$) não inclui $T_{IniciarTransmissor}$, segundo informa a Equação (26), mas somente a diferença de tempo entre a transmissão do pacote de controle de posse da palavra e o recebimento do ACK correspondente. Os RTTs podem ser medidos com a utilização de mensagens ICMP *Echo Request*.

$$T_{Total} \geq RTT_{Participante-MCU} + RTT_{Moderador-MCU} + T_{Processamento} + T_{IniciarTransmissor} \quad (25)$$

$$T_{ControlePossePalavra} \geq RTT_{Participante-MCU} + RTT_{Moderador-MCU} + T_{Processamento} \quad (26)$$

O teste de desempenho do controle de posse da palavra foi feito utilizando a mesma topologia de teste com o NAPT, apresentada na Figura 5.37, com dois participantes: o participante *Marcel* (na estação *A*, endereço IP 192.168.2.2), como moderador da conferência e o participante *Reinaldo* (na estação *B*, endereço IP 192.168.2.4). A MCU está hospedada no servidor *S* (endereço IP 143.107.111.14). A estação *C* capturou o tráfego no *hub* de 100 Mbps, que se encontra na rede interna do NAPT, com um *software sniffer*.

Figura 5.44 – O participante *Marcel* como moderador da conferência e com a posse da palavra.

A Figura 5.44 mostra a sala virtual de conferência já com os participantes *Marcel*, à esquerda, e *Reinaldo*, à direita. O moderador *Marcel* está com a posse da palavra (indicação *possePalavra*) enquanto que o participante *Reinaldo* está com a indicação *normal*, visto que não há nenhuma borda colorida em torno da sua foto. A Figura 5.45 mostra o participante *Reinaldo* já com a posse da palavra. A interface homem-máquina utilizada nesse teste é a do tipo *janela mínima*, que utiliza o mínimo espaço possível.

Figura 5.45 – O participante *Reinaldo* com a posse da palavra.

Para demonstrar a concessão de posse da palavra, o moderador *Marcel* concedeu a posse da palavra para o participante *Reinaldo* e os pacotes foram capturados no *software sniffer*. Foi aplicado um filtro para mostrar somente os pacotes com o

protocolo de transporte UDP, visto que tanto o RTP quanto o protocolo de controle de posse da palavra são transportados sobre UDP. O resultado da captura está apresentado na Figura 5.46.

Frame	Len	Absolute Time	Source	Destination	Prot	Description
156	157	12:18:56.296866	143.107.111.14	192.168.2.4	RTP	Payload=GSM
157	157	12:18:56.376856	192.168.2.2	143.107.111.14	RTP	Payload=GSM
158	157	12:18:56.386870	143.107.111.14	192.168.2.4	RTP	Payload=GSM
159	157	12:18:56.436942	192.168.2.2	143.107.111.14	RTP	Payload=GSM
160	157	12:18:56.446956	143.107.111.14	192.168.2.4	RTP	Payload=GSM
161	78	12:18:56.466985	192.168.2.2	143.107.111.14	RTCP	APP
162	78	12:18:56.467048	143.107.111.14	192.168.2.2	RTCP	APP
163	78	12:18:56.467110	143.107.111.14	192.168.2.4	RTCP	APP
164	64	12:18:56.477000	192.168.2.4	143.107.111.14	RTCP	APP
184	64	12:18:56.477872	143.107.111.14	192.168.2.2	RTCP	APP
185	157	12:18:56.607187	192.168.2.2	143.107.111.14	RTP	Payload=GSM
186	157	12:18:56.617201	192.168.2.2	143.107.111.14	RTP	Payload=GSM
196	157	12:18:56.717345	192.168.2.2	143.107.111.14	RTP	Payload=GSM
200	157	12:18:56.737374	192.168.2.2	143.107.111.14	RTP	Payload=GSM
215	157	12:18:57.147964	192.168.2.2	143.107.111.14	RTP	Payload=GSM
217	157	12:18:57.208051	192.168.2.4	143.107.111.14	RTP	Payload=GSM
218	157	12:18:57.208176	192.168.2.4	143.107.111.14	RTP	Payload=GSM
219	157	12:18:57.208302	143.107.111.14	192.168.2.2	RTP	Payload=GSM
226	157	12:18:57.278152	192.168.2.4	143.107.111.14	RTP	Payload=GSM
228	157	12:18:57.278731	143.107.111.14	192.168.2.2	RTP	Payload=GSM

Figura 5.46 – Captura de pacotes no *software sniffer* Advisor LAN mostrando a concessão da posse da palavra do moderador (endereço IP 192.168.2.2) para um participante comum (endereço IP 192.168.2.4), através dos quadros capturados #161, #162, #163, #164 e # 184).

Como se pode observar na Figura 5.46, *Marcel* (endereço IP 192.168.2.2) estava com a posse da palavra e transmitira seus pacotes RTP para a *MCU* (endereço IP 143.107.111.14) e esta encaminhava os pacotes para *Reinaldo* (endereço IP 192.168.2.4). O participante com a posse da palavra não recebe o seu áudio de volta da *MCU*, visto que nenhum pacote RTP de áudio é transmitido dela para o detentor da posse da palavra. O quadro capturado #161 (no instante 12:18:56.466985), interpretado pelo *software sniffer* como se fosse um pacote RTCP do tipo APP, é na verdade um pacote de controle de posse da palavra que *Marcel* transmitiu para

Reinaldo (no nível da camada de aplicação da arquitetura TCP/IP), mas endereçado para a *MCU* (no nível da camada de rede da arquitetura TCP/IP).

Quando a *MCU* recebe mensagem com a concessão de posse da palavra para *Reinaldo*, ela responde para *Marcel* com um ACK_{MCU} (quadro capturado #162 no instante 12:18:56.467048), encaminha mensagem com a concessão de posse da palavra para *Reinaldo* (quadro capturado #163 no instante 12:18:56.467110) e pára de encaminhar os pacotes RTP de áudio de *Marcel*. Percebe-se claramente que *Marcel* continua a transmitir seus pacotes RTP de áudio até o instante em que ele recebe o $ACK_{Reinaldo}$ (quadro capturado #184 no instante 12:18:56.477872), transmitido de *Reinaldo* para a *MCU* e desta para ele. Os pacotes RTP de áudio transmitidos por *Marcel* após a recepção de $ACK_{Reinaldo}$ são decorrentes do tempo necessário para que a sua *applet* Java efetivamente pare o seu transmissor. Semelhantemente, o participante *Reinaldo* leva algum tempo para iniciar o seu transmissor e, por isso, não começa a transmitir logo em seguida de ter recebido a posse da palavra.

A partir do quadro capturado #217 (instante 12:18:57.208051), *Reinaldo* está transmitindo pacotes RTP de áudio para a *MCU* que os encaminha para *Marcel*, caracterizando o controle da posse da palavra.

Como os pacotes foram capturados dentro da rede interna do NAPT e o *software sniffer* registra o instante no qual o pacote foi capturado, os RTTs estão embutidos no tempo de captura de cada pacote.

Portanto, $T_{ControlePossePalavra}$ foi medido pela diferença entre o instante da transmissão de $ACK_{Reinaldo}$, da *MCU* para *Marcel* (quadro #184, instante 12:18:56.477872) e o instante em que a concessão da posse da palavra foi transmitida de *Marcel* para *MCU* (quadro #161, instante 12:18:56.466985).

Já T_{Total} foi medido pela diferença entre o instante da transmissão do primeiro pacote originado por *Reinaldo*, encaminhado da *MCU* para *Marcel* (quadro #219, instante 12:18:57.208302) e o instante em que a concessão da posse da palavra foi transmitida de *Marcel* para *MCU* (quadro #161, instante 12:18:56.466985).

Por sua vez, $T_{IniciarTransmissor}$ foi medido subtraindo-se o instante em que *Reinaldo* transmite a confirmação referente à concessão de posse da palavra (quadro #164,

instante 12:18:56.477000), do instante de transmissão do primeiro pacote RTP de *Reinaldo* para a *MCU* (quadro #217, instante 12:18:57.208051).

A Figura 5.46 também permite calcular o tempo que o moderador *Marcel* leva para parar o seu transmissor ($T_{PararTransmissor}$), subtraindo-se o instante da transmissão de $ACK_{Reinaldo}$, da *MCU* para *Marcel* (quadro #184, instante 12:18:56.477872) do instante em que seu último pacote RTP é transmitido para a *MCU* (quadro #215, instante 12:18:57.147964).

Pode-se também calcular o tempo em que a *MCU* fica sem encaminhar pacotes RTP ($T_{SemAudio}$), devido à troca de posse da palavra, pela diferença entre os instantes da transmissão do ACK_{MCU} da *MCU* para *Marcel* (quadro #162, instante 12:18:56.467048) e da transmissão do primeiro pacote RTP originado por *Reinaldo*, também da *MCU* para *Marcel* (quadro #219, instante 12:18:57.208302).

Tabela 5.4 – Tempos medidos na troca de posse da palavra.

Variável	Tempo (ms)
$T_{ControlePossePalavra} = \text{Quadro \#184} - \text{Quadro \#161}$	10,887
$T_{Total} = \text{Quadro \#219} - \text{Quadro \#161}$	741,317
$T_{IniciarTransmissor} = \text{Quadro \#217} - \text{Quadro \#164}$	731,051
$T_{PararTransmissor} = \text{Quadro \#215} - \text{Quadro \#184}$	670,092
$T_{SemAudio} = \text{Quadro \#219} - \text{Quadro \#162}$	741,254

Devido à topologia de testes utilizada, $RTT_{Moderador-MCU}$ e $RTT_{Participante-MCU}$ são inferiores a 10 ms e não são informados com precisão pelo sistema operacional. O *software sniffer* informa que os RTTs são inferiores a 100 μ s.

Pelos resultados acima, pode-se concluir que $T_{Processamento}$ é inferior a 10 ms e que $T_{ControlePossePalavra}$ só é significativo para RTTs altos.

Devido à troca de posse da palavra, os participantes ficam aproximadamente 740 ms sem receber áudio.

5.3.3 Medição da banda consumida pela unidade de controle multiponto

A análise da banda consumida pela unidade de controle multiponto será feita sobre o teste realizado com três participantes. Na Figura 5.47 é apresentado um gráfico contendo a banda total de recepção (seqüência Total_RX), a banda total de transmissão (seqüência Total_TX), as bandas de recepção e de transmissão ocupadas pelos protocolos de controle de conferência e RTCP (seqüências Outros_RX e Outros_TX, respectivamente) e as porcentagens da banda total ocupada pelo tráfego de voz recebido e transmitido (seqüências RTP_RX/Total_RX e RTP_TX/Total_TX, respectivamente).

Figura 5.47 – Bandas de transmissão e de recepção da unidade de controle multiponto.

A análise porcentual das bandas de recepção e transmissão de controle de conferência não deve ser feita em situações transitórias, mas na situação mais corriqueira, onde o participante com a posse da palavra está com o seu transmissor

ativo e todos os participantes estão recebendo áudio (nenhum deles está com o áudio bloqueado pelo moderador). Nas demais situações, as bandas ocupadas são inferiores, porque ou nada está sendo transmitido ou alguém não está recebendo pacotes RTP de áudio. Exemplos de situações adequadas para análise estão nos intervalos aproximados [68, 80], [94, 100], [112, 119], [122, 138], [140, 150] e [182, 90] s. Durante esses intervalos, os pacotes que não carregam RTP ocuparam no máximo cerca de 13% da banda de recepção e nem 7% da de transmissão.

A banda total de transmissão da unidade de controle multiponto não ultrapassou 44 kbps (menos de 22 kbps sendo transmitido para cada participante) e a de recepção, ficou abaixo de 26 kbps. O gráfico da Figura 5.47 confirma a Equação (14) (vide Capítulo 2.2.1.2).

Pelo mecanismo de controle de posse da palavra, a unidade de controle multiponto recebe somente um canal de áudio, independentemente do número de participantes em uma sala virtual de conferência. Porém, a banda de recepção ocupada pelos pacotes de controle de conferência e RTCP aumenta com o número de participantes.

Eventuais pacotes RTCP transmitidos pela unidade de controle multiponto são particulares a cada participante. O crescimento da banda de transmissão ocupada pelos pacotes de controle de conferência é mais preocupante, porque praticamente todo pacote de controle de conferência recebido pela unidade de controle multiponto é respondido com um pacote de confirmação e depois é propagado para os demais participantes, semelhantemente aos pacotes RTP de áudio. Os pacotes de controle de conferência não possuem periodicidade definida e sua distribuição temporal depende da dinâmica da conferência e do grau de participação das pessoas envolvidas.

Considerando-se que os pacotes de controle de conferência possuem tamanho inferior aos pacotes de voz, para que a banda de transmissão da unidade de controle multiponto ocupada por esses pacotes supere a dos pacotes RTP de áudio, é necessário que o número de participantes na conferência seja maior do que o número de pacotes de voz transmitidos por unidade de tempo. Exemplificando: suponha uma conferência com dez participantes utilizando um *codec* que acarreta na transmissão de 16,6 quadros de 157 B por segundo. Se cada quadro Ethernet transportando um pacote de controle de conferência ocupar 82 B, em média, seria necessário que a

unidade de controle multiponto recebesse aproximadamente 28,6 pacotes por segundo, para igualar ambas as bandas. Esse valor foi obtido a partir da Equação (27), onde N é o número de participantes na conferência, $T_{Controle}$ é a taxa média de pacotes de controle de conferência recebidos, $B_{Controle}$ é o tamanho médio dos quadros Ethernet transportando pacotes de controle de conferência, T_{Voz} é a taxa média de pacotes RTP de áudio recebidos e B_{Voz} é o tamanho médio dos quadros Ethernet transportando pacotes RTP de áudio.

$$(N - 1) \cdot T_{Voz} \cdot B_{Voz} = N \cdot T_{Controle} \cdot B_{Controle}, N \geq 2 \quad (27)$$

A Equação (27) desconsidera os pacotes de confirmação de recebimento, visto que estes são dirigidos a um único participante.

Na verdade, a pergunta a ser feita é: dado o tamanho médio dos quadros transportando pacotes de controle de conferência, qual é o número mínimo de participantes que produz na unidade de controle multiponto uma taxa de recebimento desses quadros, de modo que a banda de transmissão deles se iguale à dos pacotes RTP de áudio. Essa pergunta é válida, porque os participantes da conferência não estão constantemente enviando pacotes de controle de conferência. O intervalo de tempo entre duas interações consecutivas de um mesmo participante é da ordem de vários segundos, ou mesmo de minutos. Um participante que venha a pedir a posse da palavra, só desistirá do seu pedido depois de um certo tempo.

No caso do exemplo dado, para que os dez participantes gerassem 28,6 pacotes de controle de conferência por segundo, seria necessário que cada um deles interagisse mais de duas vezes por segundo com a sua interface homem-máquina, um ritmo impraticável. Qual deveria ser o número de participantes para que a unidade de controle multiponto receba 28,6 pacotes de controle de conferência por segundo? Simplificando-se a situação para se responder a esta pergunta: se as interações dos participantes estiverem igualmente espaçadas no tempo e cada participante fizer, em média, uma interação a cada 10 s, seriam necessários 286 participantes.

Essa análise indica que é necessário um número grande de participantes para se dobrar a banda transmitida pela unidade de controle multiponto, como se ela estivesse distribuindo dois canais de áudio simultaneamente para os participantes.

O mecanismo de controle de posse da palavra mostrou-se útil tanto para o usuário quanto para o proprietário do sistema de conferência, com relação à economia de recursos de rede.

5.3.4 Avaliação do desempenho de uma unidade de controle multiponto isolada

O objetivo desse teste é estimar o número máximo de participantes que a unidade de controle multiponto consegue servir para uma determinada configuração de *software* e *hardware*. Para isso, foi iniciada uma única sala virtual de conferência com dez participantes e foram realizadas medições com um *software sniffer* instalado no mesmo servidor que a unidade de controle multiponto. A topologia do teste é a mesma utilizada com o NAPT.

O tamanho do pacote RTP depende do *codec* sendo utilizado e da duração do áudio sendo encapsulado em cada pacote RTP na correspondente implementação. O tamanho do pacote RTP interfere no tempo de transmissão do mesmo. Como o ambiente de testes é baseado em uma rede Fast Ethernet, o tempo de transmissão (T_T) de um quadro Ethernet de 157 B é dado pela Equação (28).

$$T_T = \frac{157 \text{ B} \cdot 8}{100 \text{ Mbps}} = 12,56 \mu s \quad (28)$$

Se forem considerados o preâmbulo de sincronismo (*PRE*), o delimitador de início de quadro (*SFD*) e o *interframe gap* (*IFG*) (SEIFERT, 2000), tudo se passa como se fossem transmitidos 177 B e o tempo de transmissão (T_T') de um quadro Ethernet de 157 B passa a ser dado pela Equação (29).

$$T_T = \frac{(PRE + SFD + 157B + IFG) \cdot 8}{100Mbps} = \frac{(7B + 1B + 157B + 12B) \cdot 8}{100Mbps} = 14,16\mu s \quad (29)$$

Para o teste especificado, uma unidade de controle multiponto com tempo de resposta nulo para encaminhar os pacotes RTP de áudio para os demais participantes e máxima eficiência conseguiria servir 4.237 participantes, segundo a Equação (30).

$$N = \frac{60ms}{14.16\mu s} \approx 4.237 \text{ participantes} \quad (30)$$

Netstumbler WXL (Trial Mode) - Local, Ethernet (Line speed at 100 Mbps) - [1sala10participantes.cap: Decode, 32/708 Ethernet...

File Monitor Capture Display Tools Database Window Help

Default

No.	Source Address	Dest Address	Summary	Len (Bytes)	Delta Time	Rel. Time
1	[143.107.111.15]	[143.107.111.14]	UDP: D=20004 S=20004	153	0.000.000	0:00:00.000
2	[143.107.111.14]	[143.107.111.15]	UDP: D=20064 S=20004	153	0.000.453	0:00:00.000
3	[143.107.111.14]	[143.107.111.15]	UDP: D=1058 S=20004	153	0.000.160	0:00:00.000
4	[143.107.111.14]	[143.107.111.15]	UDP: D=20024 S=20004	153	0.000.143	0:00:00.000
5	[143.107.111.14]	[143.107.111.15]	UDP: D=20034 S=20004	153	0.000.146	0:00:00.000
6	[143.107.111.14]	[143.107.111.15]	UDP: D=20044 S=20004	153	0.000.142	0:00:00.001
7	[143.107.111.14]	[143.107.111.15]	UDP: D=20054 S=20004	153	0.000.145	0:00:00.001
8	[143.107.111.14]	[143.107.111.15]	UDP: D=20074 S=20004	153	0.000.145	0:00:00.001
9	[143.107.111.14]	[143.107.111.15]	UDP: D=20084 S=20004	153	0.000.145	0:00:00.001
10	[143.107.111.14]	[143.107.111.15]	UDP: D=20114 S=20004	153	0.000.146	0:00:00.001
11	[143.107.111.15]	[143.107.111.14]	UDP: D=20004 S=20004	153	0.087.973	0:00:00.089
12	[143.107.111.14]	[143.107.111.15]	UDP: D=20064 S=20004	153	0.000.447	0:00:00.090
13	[143.107.111.14]	[143.107.111.15]	UDP: D=1058 S=20004	153	0.000.162	0:00:00.090
14	[143.107.111.14]	[143.107.111.15]	UDP: D=20024 S=20004	153	0.000.144	0:00:00.090
15	[143.107.111.14]	[143.107.111.15]	UDP: D=20034 S=20004	153	0.000.146	0:00:00.090
16	[143.107.111.14]	[143.107.111.15]	UDP: D=20044 S=20004	153	0.000.143	0:00:00.090
17	[143.107.111.14]	[143.107.111.15]	UDP: D=20054 S=20004	153	0.000.146	0:00:00.090
18	[143.107.111.14]	[143.107.111.15]	UDP: D=20074 S=20004	153	0.000.145	0:00:00.090
19	[143.107.111.14]	[143.107.111.15]	UDP: D=20084 S=20004	153	0.000.144	0:00:00.091
20	[143.107.111.14]	[143.107.111.15]	UDP: D=20114 S=20004	153	0.000.148	0:00:00.091
21	[143.107.111.15]	[143.107.111.14]	UDP: D=20004 S=20004	153	0.064.468	0:00:00.155
22	[143.107.111.14]	[143.107.111.15]	UDP: D=20064 S=20004	153	0.000.389	0:00:00.156
23	[143.107.111.14]	[143.107.111.15]	UDP: D=1058 S=20004	153	0.000.160	0:00:00.156
24	[143.107.111.14]	[143.107.111.15]	UDP: D=20024 S=20004	153	0.000.144	0:00:00.156
25	[143.107.111.14]	[143.107.111.15]	UDP: D=20034 S=20004	153	0.000.147	0:00:00.156
26	[143.107.111.14]	[143.107.111.15]	UDP: D=20044 S=20004	153	0.000.145	0:00:00.156
27	[143.107.111.14]	[143.107.111.15]	UDP: D=20054 S=20004	153	0.000.145	0:00:00.156
28	[143.107.111.14]	[143.107.111.15]	UDP: D=20074 S=20004	153	0.000.144	0:00:00.156
29	[143.107.111.14]	[143.107.111.15]	UDP: D=20084 S=20004	153	0.000.145	0:00:00.157
30	[143.107.111.14]	[143.107.111.15]	UDP: D=20114 S=20004	153	0.000.146	0:00:00.157
31	[143.107.111.15]	[143.107.111.14]	UDP: D=20004 S=20004	153	0.045.276	0:00:00.202

Expert Decode Matrix Host Table Protocol Dist Statistics

For Help, press F1

Figura 5.48 – Pacotes RTP de áudio capturados pelo *software sniffer* Netasyst WLX no servidor da unidade de controle multiponto. Notar as portas UDP de destino na coluna “*Summary*”.

A Figura 5.48 mostra os pacotes RTP de áudio recebidos (quadros capturados #1, #11, #21 e #31) e transmitidos pela unidade de controle multiponto (endereço IP 143.107.111.14).

Pode-se perceber que a unidade de controle multiponto (endereço IP 143.107.111.14) recebe um quadro Ethernet de 157 B transportando um pacote RTP de áudio com o *codec* GSM, transmitido pelo NAPT (endereço IP 143.107.111.15).

A partir do instante em que a unidade de controle multiponto recebe o pacote RTP e realiza a sua validação, o pacote é encaminhado para a rotina de transmissão de pacotes RTP onde a estrutura de dados de participantes é percorrida e os pacotes RTP são modificados e encaminhados para os demais participantes.

A unidade de controle multiponto processa o pacote RTP e após cerca de 450 μ s, começa a encaminhar os pacotes RTP modificados para cada participante (ver os quadros capturados de #1 a #10). Como os dez participantes encontram-se atrás do NAPT, estando um deles com a posse da palavra, são enviados nove pacotes RTP para o NAPT, cada um destinado a um participante, visivelmente diferenciados pela porta UDP destino do pacote RTP transmitido pela unidade de controle multiponto. O intervalo de tempo entre o primeiro e o segundo pacote RTP de áudio encaminhados é cerca de 160 μ s. A partir do segundo pacote, o intervalo passa a ser cerca de 145 μ s. Esse é o tempo que a unidade de controle multiponto está levando para iterar pela sua estrutura de dados de participantes, alterar e transmitir o pacote RTP de cada participante.

Após 87,973 ms que o pacote RTP (quadro capturado #1) foi recebido pela unidade de controle multiponto, chegou o próximo pacote (quadro capturado #11).

O próprio *software sniffer* insere atraso nos quadros Ethernet, distorcendo os números reais de atraso, devido ao seu processamento interno.

Pela observação da Figura 5.48, estimando-se de forma conservadora o atraso médio para a unidade de controle multiponto processar um pacote RTP (A) em 500 μ s e o intervalo de tempo médio entre a transmissão de dois quadros consecutivos (D) em 160 μ s. Considerando-se o intervalo médio entre o recebimento de pacotes RTP (I) como sendo 60 ms, o número máximo de participantes que a unidade de controle

multiponto atenderia em uma conferência utilizando o *codec* GSM transportando três *frames* de áudio de 20 ms por quadro Ethernet é dado pela Equação (31).

$$N = \frac{I - A}{D} = \frac{60 \text{ ms} - 0,500 \text{ ms}}{0,160 \text{ ms}} \approx 371 \text{ participantes} \quad (31)$$

Para simplificar a análise da escalabilidade, foi assumido um comportamento linear do desempenho da unidade de controle multiponto, isto é, não foi considerada uma possível degradação de seu desempenho com o aumento do número de participantes servidos e o aumento do tráfego de controle, de *chat* de texto e de RTCP.

O número de participantes que podem ser atendidos simultaneamente é razoável, visto que o sistema operacional utilizado não trabalha em tempo real, o servidor de unidades de controle multiponto e a unidade de controle multiponto foram implementados em Java e concorrem com outros processos pelos recursos disponíveis. Além disso, devem ser considerados os processamentos de cada pacote RTP, RTCP e de controle de conferência realizados pela unidade de controle multiponto e o mecanismo de detecção de portas UDP para funcionamento transparente do sistema com NAPT.

Esse teste revela que a banda disponível para a conferência será, normalmente, o principal fator limitante da sua escalabilidade, mesmo porque o número de participantes que satura a unidade de controle multiponto pode ser elevado utilizando-se um processador melhor, já que os parâmetros *A* e *D* dependem do desempenho do processador, do sistema operacional e da eficiência do código da unidade de controle multiponto.

Não se observou alteração no desempenho da unidade de controle multiponto elevando-se o nível de prioridade do processo do servidor de unidades de controle multiponto.

5.3.5 Avaliação do desempenho de duas unidades de controle multiponto em abordagem multitarefa

Os dez participantes do teste anterior foram divididos em duas salas virtuais de conferência, sala #1 (porta base UDP 20.000) e sala #2 (porta base UDP 2.000), servidas por duas unidades de controle multiponto hospedadas em um mesmo servidor de unidades de controle multiponto para se avaliar o impacto de unidades de controle multiponto concorrentes em abordagem multitarefa. A sala #1 foi iniciada primeiramente. A Figura 5.49 mostra os pacotes RTP de áudio capturados na unidade de controle multiponto.

No.	Source Address	Dest Address	Summary	Len (Bytes)	Delta Time	Rel. Time
1	[143.107.111.15]	[143.107.111.14]	UDP: D=20004 S=20034	153	0.000.000	0:00:00.000
2	[143.107.111.14]	[143.107.111.15]	UDP: D=20004 S=20004	153	0.000.402	0:00:00.000
3	[143.107.111.14]	[143.107.111.15]	UDP: D=20054 S=20004	153	0.000.211	0:00:00.000
4	[143.107.111.14]	[143.107.111.15]	UDP: D=20164 S=20004	153	0.000.145	0:00:00.000
5	[143.107.111.14]	[143.107.111.15]	UDP: D=20134 S=20004	153	0.000.143	0:00:00.000
6	[143.107.111.15]	[143.107.111.14]	UDP: D=2004 S=2154	153	0.017.567	0:00:00.018
7	[143.107.111.14]	[143.107.111.15]	UDP: D=2114 S=2004	153	0.000.514	0:00:00.018
8	[143.107.111.14]	[143.107.111.15]	UDP: D=2194 S=2004	153	0.000.165	0:00:00.019
9	[143.107.111.14]	[143.107.111.15]	UDP: D=2084 S=2004	153	0.000.146	0:00:00.019
10	[143.107.111.14]	[143.107.111.15]	UDP: D=2014 S=2004	153	0.000.144	0:00:00.019
12	[143.107.111.15]	[143.107.111.14]	UDP: D=20004 S=20034	153	0.016.381	0:00:00.035
13	[143.107.111.14]	[143.107.111.15]	UDP: D=20004 S=20004	153	0.000.327	0:00:00.036
14	[143.107.111.14]	[143.107.111.15]	UDP: D=20054 S=20004	153	0.000.194	0:00:00.036
15	[143.107.111.14]	[143.107.111.15]	UDP: D=20164 S=20004	153	0.000.147	0:00:00.036
16	[143.107.111.14]	[143.107.111.15]	UDP: D=20134 S=20004	153	0.000.143	0:00:00.036
17	[143.107.111.15]	[143.107.111.14]	UDP: D=2004 S=2154	153	0.030.405	0:00:00.067
18	[143.107.111.14]	[143.107.111.15]	UDP: D=2114 S=2004	153	0.000.452	0:00:00.067
19	[143.107.111.14]	[143.107.111.15]	UDP: D=2194 S=2004	153	0.000.163	0:00:00.067
20	[143.107.111.14]	[143.107.111.15]	UDP: D=2084 S=2004	153	0.000.144	0:00:00.067
21	[143.107.111.14]	[143.107.111.15]	UDP: D=2014 S=2004	153	0.000.145	0:00:00.067
23	[143.107.111.15]	[143.107.111.14]	UDP: D=20004 S=20034	153	0.056.792	0:00:00.124
24	[143.107.111.14]	[143.107.111.15]	UDP: D=20004 S=20004	153	0.000.436	0:00:00.125
25	[143.107.111.14]	[143.107.111.15]	UDP: D=20054 S=20004	153	0.000.209	0:00:00.125
26	[143.107.111.14]	[143.107.111.15]	UDP: D=20164 S=20004	153	0.000.143	0:00:00.125
27	[143.107.111.14]	[143.107.111.15]	UDP: D=20134 S=20004	153	0.000.144	0:00:00.125
28	[143.107.111.15]	[143.107.111.14]	UDP: D=2004 S=2154	153	0.038.315	0:00:00.163
29	[143.107.111.14]	[143.107.111.15]	UDP: D=2114 S=2004	153	0.000.425	0:00:00.164
30	[143.107.111.14]	[143.107.111.15]	UDP: D=2194 S=2004	153	0.000.162	0:00:00.164
31	[143.107.111.14]	[143.107.111.15]	UDP: D=2084 S=2004	153	0.000.145	0:00:00.164
32	[143.107.111.14]	[143.107.111.15]	UDP: D=2014 S=2004	153	0.000.143	0:00:00.164

Figura 5.49 – Pacotes RTP de áudio capturados de duas salas virtuais de conferência hospedadas em um mesmo servidor de unidades de controle multiponto. Notar as portas UDP de destino e de origem na coluna “Summary”.

A unidade de controle multiponto (endereço IP 143.107.111.14) recebe um quadro Ethernet de 157 B transportando um pacote RTP de áudio com o *codec* GSM transmitido pelo NAPT (endereço IP 143.107.111.15) de cada sala. Como há cinco participantes em cada sala, quatro pacotes RTP de áudio são transmitidos de volta para o NAPT. Pode-se perceber um comportamento temporal semelhante ao do teste anterior com uma só sala.

Como o recebimento, validação e alteração de um pacote RTP de áudio insere um atraso cerca de três vezes maior que cada iteração na estrutura de dados de participantes da unidade de controle multiponto, isso deve ser considerado no cálculo do número total de participantes que pode ser atendido. Tudo se passa como se houvesse dois participantes a mais em cada sala virtual. Simplificando a análise de salas concorrentes, sem considerar o efeito do entrelaçamento dos pacotes RTP transmitidos pelas unidades de controle multiponto, o número máximo de participantes que poderia ser atendido cai em função do número de salas virtuais concorrentes (m) em um mesmo servidor, segundo a Equação (32).

$$N(m) = \frac{I - m \cdot A}{D}, m \cdot A \leq I = \frac{60 \text{ ms} - 2 \cdot 0,500 \text{ ms}}{0,160 \text{ ms}} \approx 368 \text{ participantes} \quad (32)$$

As duas unidades de controle multiponto estarem concorrendo entre si pelo tempo do processador e pela banda disponível não afetou de forma significativa o desempenho individual delas, mostrando que a abordagem multitarefa pode ser utilizada sem receios em relação a desempenho. Foi então iniciada uma terceira sala (sala #3, porta base UDP 10.000) com mais cinco participantes para se verificar esse comportamento. Os pacotes RTP de áudio capturados podem ser vistos na Figura 5.50.

No.	Source Address	Dest Address	Summary	Len (Bytes)	Delta Time	Rel. Time
1	[143.107.111.15]	[143.107.111.14]	UDP: D=10004 S=10174	153	0.000.000	0:00:00.000
2	[143.107.111.14]	[143.107.111.15]	UDP: D=10024 S=10004	153	0.000.447	0:00:00.000
3	[143.107.111.14]	[143.107.111.15]	UDP: D=10044 S=10004	153	0.000.167	0:00:00.000
4	[143.107.111.14]	[143.107.111.15]	UDP: D=10064 S=10004	153	0.000.146	0:00:00.000
5	[143.107.111.14]	[143.107.111.15]	UDP: D=10074 S=10004	153	0.000.146	0:00:00.000
6	[143.107.111.15]	[143.107.111.14]	UDP: D=20004 S=20034	153	0.013.738	0:00:00.014
7	[143.107.111.14]	[143.107.111.15]	UDP: D=20004 S=20004	153	0.000.382	0:00:00.015
8	[143.107.111.14]	[143.107.111.15]	UDP: D=20054 S=20004	153	0.000.214	0:00:00.015
9	[143.107.111.14]	[143.107.111.15]	UDP: D=20164 S=20004	153	0.000.146	0:00:00.015
10	[143.107.111.14]	[143.107.111.15]	UDP: D=20134 S=20004	153	0.000.145	0:00:00.015
11	[143.107.111.15]	[143.107.111.14]	UDP: D=2004 S=2154	153	0.002.044	0:00:00.017
12	[143.107.111.14]	[143.107.111.15]	UDP: D=2114 S=2004	153	0.000.284	0:00:00.017
13	[143.107.111.14]	[143.107.111.15]	UDP: D=2084 S=2004	153	0.000.154	0:00:00.018
14	[143.107.111.14]	[143.107.111.15]	UDP: D=2014 S=2004	153	0.000.149	0:00:00.018
15	[143.107.111.15]	[143.107.111.14]	UDP: D=20004 S=20034	153	0.027.391	0:00:00.045
16	[143.107.111.14]	[143.107.111.15]	UDP: D=20004 S=20004	153	0.000.419	0:00:00.045
17	[143.107.111.14]	[143.107.111.15]	UDP: D=20054 S=20004	153	0.000.223	0:00:00.046
18	[143.107.111.14]	[143.107.111.15]	UDP: D=20164 S=20004	153	0.000.145	0:00:00.046
19	[143.107.111.14]	[143.107.111.15]	UDP: D=20134 S=20004	153	0.000.145	0:00:00.046
20	[143.107.111.15]	[143.107.111.14]	UDP: D=2004 S=2154	153	0.028.956	0:00:00.075
21	[143.107.111.14]	[143.107.111.15]	UDP: D=2114 S=2004	153	0.000.484	0:00:00.075
22	[143.107.111.14]	[143.107.111.15]	UDP: D=2084 S=2004	153	0.000.172	0:00:00.076
23	[143.107.111.14]	[143.107.111.15]	UDP: D=2014 S=2004	153	0.000.148	0:00:00.076
24	[143.107.111.15]	[143.107.111.14]	UDP: D=10004 S=10174	153	0.028.097	0:00:00.104
25	[143.107.111.14]	[143.107.111.15]	UDP: D=10024 S=10004	153	0.000.448	0:00:00.104
26	[143.107.111.14]	[143.107.111.15]	UDP: D=10044 S=10004	153	0.000.198	0:00:00.104
27	[143.107.111.14]	[143.107.111.15]	UDP: D=10064 S=10004	153	0.000.149	0:00:00.105
28	[143.107.111.14]	[143.107.111.15]	UDP: D=10074 S=10004	153	0.000.147	0:00:00.105
29	[143.107.111.15]	[143.107.111.14]	UDP: D=2004 S=2154	153	0.003.165	0:00:00.108
30	[143.107.111.14]	[143.107.111.15]	UDP: D=2114 S=2004	153	0.000.376	0:00:00.108
31	[143.107.111.14]	[143.107.111.15]	UDP: D=2084 S=2004	153	0.000.162	0:00:00.108
32	[143.107.111.14]	[143.107.111.15]	UDP: D=2014 S=2004	153	0.000.147	0:00:00.109
33	[143.107.111.15]	[143.107.111.14]	UDP: D=10004 S=10174	153	0.039.884	0:00:00.149

Figura 5.50 – Pacotes RTP de áudio capturados de três salas concorrentes em abordagem multitarefa. Notar as portas UDP de destino e de origem na coluna “Summary”.

Durante o teste com as três salas, a sala #2 perdeu um participante, ficando somente com quatro participantes, totalizando catorze participantes simultâneos. O comportamento das três unidades de controle multiponto continuou semelhante ao de uma unidade de controle multiponto isolada.

5.3.6 Avaliação do desempenho de duas unidades de controle multiponto em abordagem multiprocesso

Um novo teste com dez participantes distribuídos igualmente em duas salas foi realizado, mas com a unidade de controle multiponto de cada uma delas em dois

servidores de unidades de controle multiponto diferentes, para se avaliar a abordagem multiprocesso.

No.	Source Address	Dest Address	Summary	Len (Bytes)	Delta Time	Rel. Time
1	[143.107.111.15]	[143.107.111.14]	UDP: D=2004 S=2004	153	0.000.000	0:00:00.000
2	[143.107.111.14]	[143.107.111.15]	UDP: D=2034 S=2004	153	0.000.475	0:00:00.000
3	[143.107.111.14]	[143.107.111.15]	UDP: D=2164 S=2004	153	0.000.167	0:00:00.000
4	[143.107.111.14]	[143.107.111.15]	UDP: D=2134 S=2004	153	0.000.148	0:00:00.000
5	[143.107.111.14]	[143.107.111.15]	UDP: D=2184 S=2004	153	0.000.148	0:00:00.000
6	[143.107.111.15]	[143.107.111.14]	UDP: D=20004 S=20154	153	0.009.615	0:00:00.010
7	[143.107.111.14]	[143.107.111.15]	UDP: D=20014 S=20004	153	0.000.431	0:00:00.010
8	[143.107.111.14]	[143.107.111.15]	UDP: D=20114 S=20004	153	0.000.158	0:00:00.011
9	[143.107.111.14]	[143.107.111.15]	UDP: D=20174 S=20004	153	0.000.141	0:00:00.011
10	[143.107.111.14]	[143.107.111.15]	UDP: D=20044 S=20004	153	0.000.149	0:00:00.011
11	[143.107.111.15]	[143.107.111.14]	UDP: D=2004 S=2004	153	0.087.812	0:00:00.099
12	[143.107.111.14]	[143.107.111.15]	UDP: D=2034 S=2004	153	0.000.477	0:00:00.099
13	[143.107.111.14]	[143.107.111.15]	UDP: D=2164 S=2004	153	0.000.165	0:00:00.099
14	[143.107.111.14]	[143.107.111.15]	UDP: D=2134 S=2004	153	0.000.149	0:00:00.100
15	[143.107.111.14]	[143.107.111.15]	UDP: D=2184 S=2004	153	0.000.149	0:00:00.100
16	[143.107.111.15]	[143.107.111.14]	UDP: D=20004 S=20154	153	0.012.032	0:00:00.112
17	[143.107.111.14]	[143.107.111.15]	UDP: D=20014 S=20004	153	0.000.439	0:00:00.112
18	[143.107.111.14]	[143.107.111.15]	UDP: D=20114 S=20004	153	0.000.159	0:00:00.112
19	[143.107.111.14]	[143.107.111.15]	UDP: D=20174 S=20004	153	0.000.143	0:00:00.112
20	[143.107.111.14]	[143.107.111.15]	UDP: D=20044 S=20004	153	0.000.146	0:00:00.113
21	[143.107.111.15]	[143.107.111.14]	UDP: D=2004 S=2004	153	0.031.373	0:00:00.144
22	[143.107.111.14]	[143.107.111.15]	UDP: D=2034 S=2004	153	0.000.391	0:00:00.144
23	[143.107.111.14]	[143.107.111.15]	UDP: D=2164 S=2004	153	0.000.163	0:00:00.145
24	[143.107.111.14]	[143.107.111.15]	UDP: D=2134 S=2004	153	0.000.146	0:00:00.145
25	[143.107.111.14]	[143.107.111.15]	UDP: D=2184 S=2004	153	0.000.148	0:00:00.145
26	[143.107.111.15]	[143.107.111.14]	UDP: D=20004 S=20154	153	0.018.238	0:00:00.163
27	[143.107.111.14]	[143.107.111.15]	UDP: D=20014 S=20004	153	0.000.359	0:00:00.163
28	[143.107.111.14]	[143.107.111.15]	UDP: D=20114 S=20004	153	0.000.153	0:00:00.164
29	[143.107.111.14]	[143.107.111.15]	UDP: D=20174 S=20004	153	0.000.143	0:00:00.164
30	[143.107.111.14]	[143.107.111.15]	UDP: D=20044 S=20004	153	0.000.146	0:00:00.164

Figura 5.51 – Pacotes RTP de áudio capturados de duas salas concorrentes em abordagem multiprocesso. Notar as portas UDP de destino e de origem na coluna “Summary”.

O comportamento observado foi semelhante ao da abordagem multitarefa.

5.3.7 Avaliação da utilização de recursos computacionais pela unidade de controle multiponto e pela *applet* Java

A finalidade desse teste é observar o comportamento do servidor de unidades de controle multiponto e das unidades de controle multiponto em operação, com relação à utilização do tempo do processador e de memória. Também foi observado o

comportamento da *applet* Java do usuário para se avaliar melhor os requisitos computacionais para o usuário.

Pelo gerenciador de tarefas do sistema operacional Microsoft Windows 2000 Server (MICROSOFT, 2000a), observa-se que o servidor de unidades de controle multiponto (aplicação “Servidor MCU”, imagem “java.exe”) utiliza inicialmente 13 tarefas e ocupa aproximadamente 12 MB. Quando a primeira sala é aberta, o número de tarefas sobe para 17 (cada unidade de controle multiponto utiliza três tarefas) e a utilização de memória, para 14 MB, aproximadamente. Quando a segunda sala é aberta, o número de tarefas sobe para 20 e a utilização de memória, para 14,4 MB, aproximadamente. Quando mais salas são abertas, o número de tarefas é incrementado de 3 unidades, enquanto o uso de memória fica praticamente inalterado em cerca de 14,5 MB. Para a unidade de controle multiponto, cada participante representa um acréscimo inferior a 100 kB no uso de memória.

A porcentagem de utilização do tempo do processador manteve-se abaixo de 10% na maior parte dos testes. A utilização ficou um pouco maior quando uma nova unidade de controle multiponto era iniciada pelo servidor de unidades de controle multiponto. Com uma conferência em andamento, o servidor de unidades de controle multiponto utilizava menos de 5% do processador. Com duas e três conferências em andamento, a utilização do tempo do processador ficou em torno de 10%. Quando as unidades de controle multiponto não são utilizadas, o servidor de unidades de controle multiponto consome cerca de 0% do processador. Aumentando-se a prioridade do processo do servidor de unidades de controle multiponto de *normal* para qualquer classificação mais prioritária não produziu nenhum ganho perceptível de desempenho.

Como a unidade de controle multiponto necessita de um baixo tempo de resposta, ela praticamente pára de responder quando passa a ser executada em memória virtual. Portanto, é fundamental garantir que o servidor, no qual as unidades de controle multiponto são executadas, possua memória suficiente para evitar o uso de memória além da memória física disponível. A mesma recomendação é válida para a *applet* Java do usuário, que pode chegar a ocupar 40 MB de memória. A *applet* Java chegou a utilizar cerca de 15% do processador, quando recebendo ou transmitindo áudio.

Pelas observações feitas, recomenda-se que o computador do usuário possua, pelo menos, 80 MB de memória RAM e 30% a mais de poder de processamento disponível além das recomendações do sistema operacional e demais *softwares* utilizados em conjunto. Semelhantemente, recomenda-se que o servidor possua 20 MB de memória RAM (no caso da abordagem multiprocesso) e 10% a mais de poder de processamento, para cada sala virtual de conferência.

5.4 Testes qualitativos

Os testes qualitativos oferecem uma impressão geral sobre a usabilidade e a interatividade do sistema de conferência.

5.4.1 Testes remotos

Três testes remotos foram realizados para se avaliar o impacto de um cenário mais realista no sistema de conferência: teste #1, utilizando o serviço de banda larga de um provedor de acesso à Internet via *cable modem* (provedor X); testes #2 e #3, com um *modem* analógico, utilizando o acesso discado de dois provedores de acesso à Internet gratuitos populares (provedores Y e Z, respectivamente)²¹. Os *modems* analógicos que seguem a recomendação ITU-T V.90 (ITU-T, 1998a) possuem uma taxa máxima de *downstream* de 56.000 bps e 33.600 bps de *upstream*, restringindo os *codecs* de voz que podem ser utilizados.

No teste #1, cuja topologia de rede é apresentada na Figura 5.52, os usuários remotos A e B estão localizados através de um mesmo NAPT, enquanto que o servidor S pertence a uma rede diferente. O equipamento utilizado como NAPT foi um SMC Barricade 7004 ABR (dados do *firmware*: “Runtime Code Version: V1.42.012; Boot Code Version: V1.00; Hardware Version: 01”) (SMC, 2003). O acesso à Internet foi

²¹ Os três provedores oferecem serviço de acesso à Internet na cidade de São Paulo – SP – Brasil.

realizado através de um *cable modem* Terayon TeraPro (TERAYON, 2003), conectado à taxa de 256 kbps.

Figura 5.52 – Topologia de rede do teste #1, com um *cable modem*.

A topologia de rede utilizada nos testes #2 e #3 é apresentada na Figura 5.53. Em ambos os testes, o usuário A pertence à rede remota, enquanto o usuário B e o servidor S pertencem à mesma rede.

Figura 5.53 – Topologia de rede dos testes #2 e #3, com um *modem analógico*.

Medições²² foram feitas para se caracterizar os cenários dos testes transmitindo-se mensagens ICMP *Echo Request* (POSTEL, 1981b) com 32 B de dados ICMP do servidor S (endereço IP 143.107.111.14) para a interface externa do NAPT no teste

²² As medições foram realizadas no dia 28 nov. 2003, das 16:50:00 às 17:50:00.

#1, e diretamente para o usuário remoto nos testes #2 e #3. A distância em *hops* entre as redes do servidor *S* e do usuário remoto foi medida transmitindo-se, também, mensagens ICMP *Echo Request* e variando-se o valor do campo *Time to Live* (TTL) do cabeçalho IPv4, até que fossem recebidas mensagens ICMP *Echo Reply* de sucesso, ao invés de mensagens ICMP *TTL Expired In-Transit*. O impacto do uso de priorização de tráfego foi avaliado configurando-se o campo *Type of Service* (TOS)/*Differentiated Service (DiffServ)*²³ do cabeçalho IPv4 (POSTEL, 1981a); (BLAKE et al., 1998) e (NICHOLS et al., 1998). Não foi possível determinar a rota exata entre as redes do servidor *S* e do usuário remoto em cada um dos testes, porque nem todos os roteadores intermediários respondiam às mensagens ICMP *Echo Request*. A Tabela 5.5 apresenta o resultado das medições realizadas.

Tabela 5.5 – Medições realizadas para caracterizar os cenários dos testes remotos.

Teste	Endereço IP	Tecnologia e taxa de recepção/transmissão	TOS	Distância em número de hops	Perda de pacotes (%)	Round-trip time (ms)			Avaliação subjetiva
						Mínimo	Médio	Máximo	
#1	200.185.X.X ²⁴	Cable modem @ 256/256 kbps (provedor X)	0	13	6,5	20	40	110	OK
			224	13	12,5	20	41	120	
#2	200.234.93.100	Conexão discada @ 52,0/33,6 kbps (provedor Y)	0	12	56,5	761	827	841	NOK
			224	12	71,2	180	189	240	
#3	200.207.179.98	Conexão discada @ 50,6/33,6 kbps (provedor Z)	0	10	0,0	160	170	183	OK
			224	10	0,0	160	166	181	

Nas medições do teste #2, pode-se afirmar, baseando-se no alto atraso e na altíssima taxa de perda de pacotes, que o caminho entre o servidor *S* e a rede do provedor *Y* estava bastante congestionado. Já os caminhos entre o servidor *S* e as redes dos

²³ Em computadores com sistema operacional da família Microsoft Windows, o comando `ping -i <TTL> -v <TOS> <endereço de destino>` configura os campos TTL e TOS no cabeçalho IPv4 transportando a mensagem ICMP. A mensagem ICMP *Echo Reply* é retornada com o mesmo valor de TOS.

²⁴ O endereço IP completo foi omitido propositalmente, por motivos de segurança.

provedores X e Z parecem estar menos carregadas. A diferença de carga nos enlaces dos testes pode explicar o porquê da priorização de tráfego ser mais impactante no teste #2 do que nos demais. Por outro lado, a priorização de tráfego parece ter um efeito negativo nos testes #1 e #2 com relação à taxa de perda de pacotes. As medições do teste #3 foram refeitas mais algumas vezes para se confirmar a ausência de perda de pacotes, constatando a qualidade do serviço oferecido pelo provedor Z.

Como o sistema de conferência não implementa priorização de tráfego, a experiência subjetiva no teste #2 foi definitivamente insatisfatória, principalmente pela alta taxa de perda de pacotes e não tanto pelo altíssimo atraso. Os testes #1 e #3 foram muito satisfatórios. No teste #1, a perda de pacotes causou pequenas interrupções no áudio e alguns problemas de sincronização não-críticos, isto é, problemas de sincronismo que foram resolvidos normalmente durante o andamento da conferência ou através de um pedido de sincronismo explícito através da interface homem-máquina. Os testes #1 e #3 foram bastante semelhantes e praticamente indistinguíveis, apesar do teste #3 possuir um atraso maior e do teste #1 possuir uma taxa de perdas não nula.

Os testes remotos mostram que a perda de pacotes tem um impacto mais significativo do que o atraso no sistema de conferência. O sistema de conferência funcionou sem problemas e transparentemente com o NAPT do teste #1. A qualidade do áudio nos testes #1 e #3 estava normal. A interatividade entre os participantes estava excelente nos testes #1 e #3, mas impraticável no teste #2, devido às condições da rede do provedor Y.

5.4.2 Avaliação subjetiva

A avaliação subjetiva consiste no relato sobre a experiência conversacional com o sistema desenvolvido e da sua observação com relação ao comportamento de outros usuários do sistema.

Quando o participante acessa pela primeira vez a página *web* da sala virtual de conferência, ele tende a explorar cada item gráfico com o *mouse*, esperando aparecer alguma descrição do mesmo. Quando o participante descobre que ao clicar nas

imagens dos participantes da conferência surge um *menu*, ele clica na sua própria imagem e lê as ações e informações disponíveis. As representações visuais das indicações não são tão intuitivas, mas o participante rapidamente consegue entender as associações de cores ao pedir a posse da palavra e ao recebê-la.

A indicação auditiva auxilia o participante a identificar quando recebeu a posse da palavra, mas a partir desse instante, há uma estranha sensação de silêncio, já que ele não recebe o seu próprio áudio. Como não há interação visual na versão atual do sistema, o participante que acabou de receber a posse da palavra costuma testar o canal de comunicação perguntando “Vocês estão me ouvindo?” ou “Se vocês estão me ouvindo, mandem uma mensagem de texto”. Nesse ponto, a comunicação por texto auxilia bastante o andamento da conversa.

Como as pessoas estão acostumadas a canais de comunicação por voz bidirecionais e simultâneos, elas ficam inseguras de falarem e não estarem sendo ouvidas. A ausência de um canal de retorno que ofereça percepção contínua da presença de todos participantes produz uma certa inquietação no participante com a posse da palavra, levando-o continuamente a pedir alguma forma de manifestação dos demais participantes.

Muitas vezes o interlocutor esquece que sua pergunta só será respondida se a posse da palavra for passada para outro participante. Por sua vez, o ouvinte muitas vezes se esquece que suas palavras não estão sendo ouvidas e tenta responder ao interlocutor sem receber a posse da palavra e quando a posse da palavra lhe é concedida, a indicação sonora o lembra que somente agora lhe ouvirão.

Os maiores problemas de comunicação ocorrem quando os participantes tentam usar o sistema em uma conversa com alta interatividade, sendo que ele foi desenvolvido visando a dinâmica de uma sala de aula e não de um telefonema, mas no decorrer da conversa, os participantes acabam se adaptando à nova dinâmica conversacional.

O mecanismo de controle de posse da palavra cria uma certa expectativa no interlocutor e no moderador com relação a mudanças na interface homem-máquina, esperando que algum participante peça a posse da palavra. A ausência de comunicações visuais faz com que os participantes acabem se distraindo, desviando suas visões da interface homem-máquina, principalmente quando não há troca de

interlocutor por longos períodos de tempo. Quando a sala virtual de conferência não está utilizando *chat* de texto, os participantes se distraem ainda mais facilmente.

Entretanto, quando o sistema é utilizado como uma sala de aula virtual, com o professor falando na maior parte do tempo, após um pouco de prática todos os participantes se mostram mais confortáveis com o controle de posse da palavra.

5.5 Considerações finais

Os testes funcionais mostraram que o sistema de conferência atende aos requisitos levantados no Capítulo 3. O sistema de conferência pode ser integrado a sistemas externos e funciona transparentemente com NAPT's. O mecanismo de controle de posse da palavra mostrou-se bastante eficiente para controlar a banda utilizada tanto pelos participantes quanto pela unidade de controle multiponto na conferência.

Os testes quantitativos revelaram que, normalmente, o principal gargalo do sistema de conferência será a banda disponível para a unidade de controle multiponto e não a capacidade de processamento do servidor que a hospeda.

Na configuração do servidor utilizada nos testes, a unidade de controle multiponto demorava aproximadamente 450 μ s antes de começar a encaminhar um pacote RTP válido. Depois de encaminhado o primeiro pacote, havia um intervalo de cerca de 145 μ s entre os pacotes RTP encaminhados para os demais participantes. Em uma sala com 100 participantes, a diferença de tempo entre o recebimento do pacote de áudio pela unidade de controle multiponto e o encaminhamento dele para todos os participantes da conferência ocorreria em menos de 15 ms. Em termos práticos, esse atraso é desprezível.

Aparentemente, não foi observada degradação no desempenho de unidades de controle multiponto operando simultaneamente, nem diferenças significativas entre as abordagens multitarefa e multiprocessamento.

Foi estimado que o servidor utilizado nos testes conseguiria servir aproximadamente 370 participantes simultâneos. Não foi possível determinar um ponto de saturação no processamento da unidade de controle multiponto, por falta de recursos

computacionais disponíveis. Aumentando-se a capacidade de processamento do servidor possibilitaria que um número ainda maior de participantes simultâneos seja servido, pela redução do tempo de processamento na unidade de controle multiponto.

A *applet* Java do usuário requer uma capacidade de processamento considerável, devido à utilização do JMF, enquanto que a unidade de controle multiponto mostrou-se leve, para o baixo número de usuários simultâneos dos testes.

Os testes qualitativos indicam que a interatividade é mais afetada pela falta de um canal de retorno apropriado para a comunicação dos demais participantes com o participante com a posse da palavra, do que por outros fatores, como o atraso. O uso de comunicação por texto ameniza, mas não resolve completamente o problema da interatividade, já que o detentor da posse da palavra continua sem ter a percepção instantânea dos demais participantes na conferência. Enquanto o mecanismo de controle de posse da palavra é benéfico para se economizar banda, ele é o responsável pelo baixo grau de interatividade entre os participantes, restringindo o uso do sistema de conferência a casos de uso como o da sala de aula virtual.

A usabilidade do sistema pode ser aprimorada, através de melhorias na interface homem-máquina, deixando-a mais intuitiva e auto-explicativa e através de um canal de retorno de áudio, permitindo a comunicação em modo *full-duplex* entre alguns participantes da conferência, em algumas situações específicas.

Os testes remotos mostraram que a taxa de perda de pacotes tem um efeito mais negativo do que um alto atraso no sistema de conferência, por causar a perda de pacotes de controle de conferência e de pacotes de áudio, prejudicando a inteligibilidade e a comunicação. Esses testes também mostraram que mesmo um usuário utilizando uma conexão discada pode participar de conferências.

No geral, os resultados dos testes realizados foram bastante positivos. O resumo dos resultados obtidos é apresentado na Tabela 5.6, para as configurações apresentadas no Capítulo 5.1.

Tabela 5.6 – Resumo dos resultados obtidos nos testes.

Sistema de conferência multiponto	
Métricas (capítulos)	Avaliação
Usabilidade (5.4.1 e 5.4.2)	Boa
Interatividade (5.3.2, 5.4.1 e 5.4.2)	Baixa (pela ausência de um canal de retorno e não pelo atraso da rede ou do controle de posse da palavra)
Qualidade subjetiva do áudio (5.4.1 e 5.4.2)	Boa
Capacidade máxima (5.3.4)	< 371 participantes simultâneos
Unidade de controle multiponto	
Métricas (capítulos)	Avaliação
Tempo de resposta (pacotes RTP) (5.3.4)	< 500 (~ 450) μ s para encaminhar o primeiro pacote < 160 (~ 145) μ s para encaminhar os demais
Tempo de resposta (mecanismo de controle de posse da palavra) (5.3.2)	< 10 ms (sem contar atraso da rede)
Banda de recepção (5.2.3.1 e 5.3.3)	~ 26 kbps
Banda de transmissão (5.2.3.1 e 5.3.3)	~ 22 kbps por usuário
Utilização de processador (5.3.7)	< 10%, com uma conferência sendo realizada (normalmente abaixo de 5%) ~ 0%, quando a unidade de controle multiponto não estiver sendo utilizada
Utilização de memória (5.3.7)	~ 12 MB para a máquina virtual Java ~ 2 MB para o servidor de unidades de controle multiponto ~ 400 kB por unidade de controle multiponto ~ 100 kB por usuário em conferência
Applet Java	
Métricas (capítulos)	Avaliação
Banda de recepção (5.2.3.1 e 5.3.3)	~ 22 kbps
Banda de transmissão (5.2.3.1 e 5.3.3)	~ 26 kbps, com a posse da palavra ~ 1 kbps, sem a posse da palavra (somente tráfego de controle de conferência, estatísticas RTCP e pacotes do chat de texto)
Utilização de processador (5.3.7)	~ 15%
Utilização de memória (5.3.7)	~ 40 MB

6. CONCLUSÕES E TRABALHOS FUTUROS

“Porque Deus amou ao mundo de tal maneira que deu o seu Filho unigênito para que todo o que nele crê não pereça, mas tenha a vida eterna.”

João 3.16

“Respondeu-lhe Jesus: Eu sou o caminho, e a verdade, e a vida; ninguém vem ao Pai senão por mim.”

João 14.6

Esse capítulo apresenta a avaliação geral do sistema de conferência multiponto desenvolvido, as contribuições feitas, os resultados alcançados, trabalhos futuros e sugestões para melhorá-lo.

6.1 Avaliação do sistema

Os testes realizados mostram que o sistema de conferência desenvolvido atende às especificações levantadas no Capítulo 3 e que o seu comportamento corresponde ao descrito no Capítulo 4: o sistema de conferência possibilita comunicação multiponto por voz e o mecanismo de controle de posse da palavra regula a dinâmica da conversação e a utilização de recursos de rede.

Os testes mostram também que a banda disponível para a unidade de controle multiponto será normalmente o principal fator limitante para a escalabilidade do sistema.

A abordagem multitarefa para as unidades de controle multiponto não prejudicou sensivelmente o desempenho das unidades de controle multiponto concorrentes nos testes. A abordagem multiprocesso e a abordagem híbrida permitem distribuir as unidades de controle multiponto pela rede, aumentando a escalabilidade do sistema.

O aumento da capacidade de processamento do servidor hospedando a unidade de controle multiponto permite elevar a capacidade do sistema.

As maiores vantagens do sistema desenvolvido são a utilização de tecnologias *web* bastante difundidas, a possibilidade de integração com outros sistemas, a facilidade de personalização da interface homem-máquina e a possibilidade de se distribuir as unidades de controle multiponto pela rede. O sistema pode ser portado para outras plataformas.

O controle de posse da palavra mostrou-se um mecanismo eficiente para restringir o consumo de banda em conferências centralizadas.

Falhas de comunicação com a unidade de controle multiponto e com o moderador da conferência podem torná-la inoperante. Proteger o sistema de conferência contra uma falha da unidade de controle multiponto é uma tarefa complexa e envolveria uma maior isolamento de processos, redundância de unidades de controle multiponto e sincronismo de estados entre elas. O sistema pode ser protegido contra falhas do moderador com a transição para um controle de posse da palavra autônomo no momento em que uma falha for detectada.

Sob o ponto de vista de comunicação, o maior ponto fraco do sistema é, como foi comentada, a ausência de um canal de retorno que ofereça percepção contínua da presença de todos participantes, levando o participante com a posse da palavra continuamente a pedir alguma forma de manifestação dos demais participantes. O uso de vídeo ou um canal de áudio de retorno podem melhorar essa sensação desconfortável, mas elevaria bastante a banda consumida. Outra solução possível seria a mixagem do áudio de todos os participantes sem a posse da palavra e o encaminhamento do áudio resultante somente para o participante com a posse da palavra. Porém, a unidade de controle multiponto passaria a ser dependente de *codec*, seu desempenho seria afetado e essa solução seria inviável para uma conferência com um número grande de participantes. Estudos precisam ser realizados para se descobrir uma forma mais eficiente para se oferecer percepção contínua e um retorno rápido dos demais participantes, com baixo impacto na banda utilizada.

Quando o sistema é utilizado dentro da sua finalidade, isto é, como uma sala de aula virtual, o controle de posse da palavra implementado mostrou-se apropriado para regular o fluxo da conversa.

6.2 Resultados alcançados

Os objetivos do trabalho foram atingidos: a proposta e o desenvolvimento de um sistema de conferência por voz para enriquecer sistemas de educação a distância. A solução apresentada e implementada foi um sistema de conferência centralizada multiponto com controle de posse da palavra.

O uso do sistema associado a educação a distância definiu a abordagem do paradigma da sala de aula virtual e a forma de interatividade através do controle de posse da palavra, entretanto, o sistema pode muito bem ser empregado em outros cenários onde a mesma dinâmica conversacional se aplique, mais especificamente, em qualquer cenário onde a figura do moderador seja necessária.

Dentre os resultados alcançados, destacam-se:

- Uma arquitetura escalável para um sistema de conferência multiponto centralizada (possibilidade de se distribuir os servidores de unidades de controle multiponto pela rede);
- Desenvolvimento de uma unidade de controle multiponto completamente independente de *codec*;
- Desenvolvimento de um protocolo de controle de conferência que realiza controle de sessão e controle de posse da palavra;
- Desenvolvimento do cliente do sistema de conferência utilizando tecnologia *web*;
- Utilização de tecnologia *web* para se criar uma sala virtual de conferência;

6.3 Trabalhos futuros e sugestões

Muitas melhorias podem ser feitas ao sistema, mas sua forma atual já pode ser empregada em algumas situações reais onde um alto grau de proteção das informações não é vital.

A ausência de mecanismos de segurança no sistema, como criptografia do canal de áudio, do canal de controle de conferência e proteção de senhas, é um fator a ser considerado antes de se utilizar o sistema em um ambiente de produção. A criptografia do canal do áudio está sendo implementada.

Possíveis evoluções dos protocolos de controle de sessão e de controle de posse da palavra devem: tentar simplificar o processamento deles na unidade de controle multiponto e na *applet* Java do usuário; buscar uma sincronização mais robusta dos participantes e possuir uma abordagem mais generalizada. A abstração dos tipos de recursos disponíveis na conferência, sejam eles canais de áudio, de vídeo, documentos compartilhados, etc., permite que o controle de posse da palavra seja utilizado irrestritamente, coordenando o acesso concorrente a eles.

O suporte a SIP como protocolo de controle de sessão pode ser incorporado em versões futuras do sistema.

Com relação às funcionalidades do sistema, a utilização de vídeo ou mesmo de um canal de áudio de retorno, permitindo comunicação por voz *full-duplex* em certas situações, são desejados em versões futuras. Compartilhamento de documentos e um mecanismo de votação também são desejados. Passar o *site* de gerenciamento de monousuário para multiusuário ajudaria a distribuir a tarefa de criação e gerenciamento das salas virtuais de conferência.

O uso futuro de IP *multicast* (uma mudança do paradigma de conferência centralizada para a híbrida ou mesmo para a descentralizada) e de mecanismos de qualidade de serviço (QoS) estão nos planos futuros.

6.4 Contribuições

As principais contribuições dessa dissertação foram:

- O levantamento dos conceitos necessários para o desenvolvimento de um sistema de conferência multiponto, resultando no Capítulo 2 deste texto;
- A análise das implicações de cada decisão a ser tomada, contida no Capítulo 3;
- A especificação, projeto e implementação do sistema de conferência multiponto;
- A realização de testes com o sistema desenvolvido;
- Uma avaliação dos efeitos do controle de posse da palavra no consumo de banda e na interatividade entre os participantes de uma conferência multiponto;
- O levantamento de possíveis melhorias no sistema.

A. TABELAS DA BASE DE DADOS DO SISTEMA DE CONFERÊNCIA

“Afirmou-lhe Jesus: Quem beber desta água tornará a ter sede; aquele, porém, que beber da água que eu lhe der nunca mais terá sede; pelo contrário, a água que eu lhe der será nele uma fonte a jorrar para a vida eterna.”

João 4.13-14

As tabelas existentes na base de dados do sistema de conferência são:

- **TabelaSalas:** Essa tabela armazena informações a respeito das salas cadastradas no sistema relativas a: representação da sala virtual de conferência para os participantes; informações de configuração de rede necessárias para o estabelecimento da conferência; definição das políticas de acesso à conferência e de controle de posse da palavra dentro dela; proteção contra eventuais ataques, uso indevido e acessos não autorizados.
- **TabelaParticipantes:** Essa tabela contém informações sobre os usuários cadastrados no sistema, tais como: identificação do usuário; formas de contato; endereços residencial e comercial. Essas informações podem ser utilizadas para melhorar o relacionamento com o usuário e personalização do serviço.
- **TabelaParticipanteCadeiraSala:** Essa tabela informa a quais salas cada usuário está associado e qual o número da sua cadeira dentro de cada uma delas. O número da cadeira não é utilizado na versão atual do sistema, mas pode ser utilizado futuramente para diferenciar algum participante na interface homem-máquina, por exemplo.

Essas tabelas constituem a base de dados do sistema e o relacionamento entre elas está ilustrado na Figura A.1. Todas as suas informações são obtidas a partir do *site* de gerenciamento do sistema, quando as salas e usuários são cadastrados e, posteriormente, quando usuários são associados a salas.

Figura A.1 – Relacionamento entre as três tabelas do sistema.

A tabela *TabelaSalas* armazena as seguintes informações:

- **Número da sala (campo *numeroSala*):** O número da sala identifica unicamente a sala na base de dados. As variáveis de aplicação no servidor *web* são nomeadas de acordo com essa informação, de forma a serem associadas corretamente à sala em questão.
- **Nome da sala (campo *nomeSala*):** Informa o nome da sala virtual de conferência.

- **Assunto da sala (campo *assuntoSala*):** Descreve qual o assunto da conferência a ser realizada na sala.
- **Número de cadeiras da sala (campo *numeroCadeirasSala*):** Informa qual o número máximo de cadeiras virtuais na sala, isto é, sua lotação máxima.
- **Admissão automática de participantes (campo *admitirAutomaticamente*):** Informa se os participantes são admitidos automaticamente na conferência, ou se a admissão deve ser autorizada pelo moderador.
- **Tipo da sala (campo *tipoSala*):** Informa qual o tipo da sala.
- **Interface homem-máquina (campo *interfaceHM*):** Informa como a sala virtual de conferência será representada para o usuário.
- **Ambiente da sala de conferência (campo *ambiente*):** Informa qual o ambiente, geograficamente falando, da sala de conferência.
- **Início da conferência (campo *inicioConferencia*):** Informa qual o horário previsto para o início da conferência. Versões futuras do sistema podem iniciar automaticamente a conferência no horário marcado e enviar convites para os usuários associados à sala, avisando-os da realização da mesma.
- **Fim da conferência (campo *fimConferencia*):** Informa qual o horário previsto para o término da conferência.
- **Mecanismo de controle de posse da palavra (campo *tipoControleRTP*):** O sistema utiliza o mecanismo de controle de posse da palavra assistido, com a presença de um moderador.
- **Moderador da sala (campo *moderador*):** Informa qual participante da conferência é o moderador. Essa informação só é útil se a sala virtual de conferência estiver configurada para utilizar o mecanismo de moderador fixo.
- **Endereço IP do moderador (campo *IPModerador*):** Se o moderador da sala for definido de forma fixa, pode-se cadastrar qual o endereço IP esperado para ser utilizado pelo moderador. O objetivo dessa informação, que pode ser ignorada pelo sistema, é oferecer meios para a validação das mensagens de controle do moderador para se dificultar ataques.

- **Dono da sala (campo *donoSala*):** Informa quem é o dono ou o criador da sala. A versão atual do gerenciador do sistema é monousuário e somente o administrador consegue criar, modificar, apagar, iniciar e terminar salas, mas versões futuras do sistema permitirão que os usuários criem suas próprias salas e sejam inteiramente responsáveis por elas. A informação a respeito do dono da sala visa viabilizar essa funcionalidade.
- **Sala protegida por senha (campo *protegida*):** Informa se a sala é ou não protegida por senha. Essa informação só é utilizada atualmente em salas virtuais de conferência do tipo *temporária*.
- **Senha da sala (campo *senhaSala*):** Informa qual a senha da sala. O sistema não oferece um mecanismo de distribuição de senhas de admissão para as salas, devendo o administrador do sistema ou o dono da sala, em versões futuras, se encarregar dessa tarefa. Essa informação só é utilizada atualmente em salas virtuais de conferência do tipo *temporária*.
- **Utilização de áudio (campo *audio*):** Informa se a conferência realiza comunicação através de áudio. Ao se desabilitar a comunicação por áudio, a *applet* Java do usuário não é carregada. Desabilita-se o carregamento da *applet* durante o desenvolvimento da página *web* da sala virtual de conferência.
- **Codec de áudio (campo *codecAudio*):** Informa qual *codec* de áudio a ser transmitido e recebido pelos participantes da conferência. O *codec* de áudio é uma configuração particular de cada sala e não de cada participante, dessa forma, todos os participantes da conferência utilizam o mesmo *codec* de áudio. Os *codecs* de áudio suportados na versão atual do sistema são: G.711, GSM, G.723.1, G.728 e G.729A.
- **Porta UDP base do usuário (campo *portaBaseUsuario*):** Informa qual a porta base UDP utilizada pela *applet* Java do participante para determinar quais são as portas UDP de recepção e transmissão dos canais de controle de conferência, de RTP e de RTCP. A porta base é definida na configuração da sala virtual de conferência no gerenciador do sistema. A presença de *firewalls* e NATs pode alterar os números das portas para as quais a unidade de controle multiponto deve transmitir os pacotes RTP, RTCP e de controle de conferência, portanto, a

unidade de controle multiponto deve detectar a presença desses elementos antes de iniciar a transmissão de qualquer pacote para o participante.

- **Porta UDP base da unidade de controle multiponto (campo *portaBaseMCU*):** Informa qual a porta base UDP utilizada pela unidade de controle multiponto para determinar quais são as portas UDP de recepção e transmissão dos canais de controle de conferência, de RTP e de RTCP. A porta base é definida na configuração da sala virtual de conferência no gerenciador do sistema.
- **Utilização de vídeo (campo *video*):** Informa se a conferência realiza comunicação através de vídeo. Reservado para uso futuro.
- **Codec de vídeo (campo *codecVideo*):** Informa qual *codec* de vídeo a ser transmitido e recebido pelos participantes da conferência. Reservado para uso futuro.
- **Utilização de texto (campo *chatTexto*):** Informa se a conferência realiza comunicação através de *chat* de texto. A comunicação por *chat* de texto é facultativa, mas, quando presente, aumenta a interatividade da conferência.
- **Conferência local (campo *conferenciaLocal*):** Informa se a conferência será confinada somente à rede local da unidade de controle multiponto. Se a conferência possuir escopo global, participantes com endereços IP quaisquer podem participar da conferência. Se o escopo for local, somente participantes pertencentes à mesma rede da unidade de controle multiponto poderão tomar parte na conferência. Quando a conferência for global e sobre IP *multicast*, deve ser utilizado um endereço IP *multicast* global válido e deve-se utilizar o valor 255 para o campo TTL do cabeçalho IPv4. Essa informação não é utilizada na versão atual do sistema.
- **Endereço do servidor de unidades de controle multiponto (campo *ipMCU*):** Informa o endereço IP e a porta TCP do servidor de unidades de controle multiponto que controla a unidade de controle multiponto.
- **Máscara de rede da unidade de controle multiponto (campo *mascaraRede*):** Associada ao endereço IP da unidade de controle multiponto, pode-se obter o endereço de rede da unidade de controle multiponto, necessário para se

determinar quais participantes pertencem à sua rede e quais pertencem a redes externas. Essa informação não é utilizada na versão atual do sistema.

- **Endereço IP *multicast* da sala de conferência (campo *IPMulticast*):** A versão atual do sistema não oferece suporte a tráfego *multicast*, mas essa informação está disponível para uso futuro. Se a conferência for global, um endereço IP *multicast* global válido deve ser utilizado.
- **Tempo de vida dos pacotes IP da conferência (campo *ttlIPv4*):** Informa qual o tempo de vida (campo TTL do cabeçalho IPv4) (POSTEL, 1981a) a ser utilizado pelos pacotes IP transmitidos tanto pela *applet* Java do participante quanto pela unidade de controle multiponto para restringir a abrangência da conferência. Muito importante para conferências sendo transportadas sobre IP *multicast*. Essa informação não é utilizada na versão atual do sistema.
- **Tipo do serviço dos pacotes IP da conferência (campo *tosIPv4*):** Informa qual o tipo de serviço (campo *Type of Service* – TOS – ou *DiffServ* do cabeçalho IPv4) (POSTEL, 1981a); (BLAKE et al., 1998) e (NICHOLS et al., 1998) a ser utilizado pelos pacotes IP transmitidos tanto pela *applet* Java do participante quanto pela unidade de controle multiponto para tentar se obter priorização dos pacotes e qualidade de serviço. Essa informação não é utilizada na versão atual do sistema.

A tabela *TabelaParticipantes* armazena as seguintes informações:

- **Nome do usuário (campo *nome*):** Informa o nome completo do usuário.
- **Data de nascimento do usuário (campo *dataNascimento*):** Informa a data de nascimento do usuário.
- **Sexo do usuário (campo *sexo*):** Informa o sexo do usuário.
- **Nacionalidade do usuário (campo *nacionalidade*):** Informa a nacionalidade do usuário.

- **Cidade onde o usuário reside (campo *cidade*):** Informa a cidade onde o usuário reside.
- **Estado onde o usuário reside (campo *estado*):** Informa o estado onde o usuário reside.
- **País onde o usuário reside (campo *pais*):** Informa o país onde o usuário reside.
- **E-mail do usuário (campo *email*):** Informa o e-mail do usuário. Essa informação pode ser utilizada para enviar ao usuário horários e senhas de conferências aos quais ele foi associado ou possui acesso.
- **Telefone do usuário (campo *telefone*):** Informa o telefone do usuário. Essa informação pode ser utilizada pelo administrador do sistema ou por pessoas dentro da conferência, caso o usuário esteja enfrentando problemas para estabelecer comunicação.
- **Endereço do usuário (campo *endereco*):** Informa um endereço do usuário para contato.
- **CEP do usuário (campo *cep*):** Informa o CEP do usuário para contato.
- **Empresa onde o usuário trabalha (campo *empresa*):** Informa onde o usuário trabalha.
- **Apelido do usuário (campo *apelido*):** Informa como o usuário será apresentado aos demais participantes na conferência.
- **Suporte ao mecanismo de controle de posse da palavra (campo *podeSerModerador*):** Informa se o usuário pode ser escolhido ou eleito como moderador de uma sala virtual de conferência.
- **Login do usuário (campo *login*):** Informa qual o *login* do usuário para acessar ao sistema de conferência. Identifica de forma única o usuário no sistema. A informação desse campo é a utilizada pela *TabelaSalas* para registrar quem é o moderador e o dono da sala.
- **Senha do usuário (campo *senha*):** Informa a senha de acesso do usuário.

- **Imagem do usuário quando ativo na conferência (campo *imagemAtivo*):** Informa qual a imagem que representará o usuário na interface homem-máquina da sala virtual de conferência quando ele estiver presente e ativo nela.
- **Imagem do usuário quando inativo na conferência (campo *imagemInativo*):** Informa qual a imagem que representará o usuário na interface homem-máquina da sala virtual de conferência quando ele possuir uma cadeira virtual na sala, mas ainda não estiver presente nela.

A tabela *TabelaParticipanteCadeiraSala* armazena as seguintes informações:

- **Login do usuário (campo *login*):** Informação obtida do campo homônimo da *TabelaParticipantes*. Identifica unicamente o participante dentro da sala virtual de conferência.
- **Número da sala (campo *numeroSala*):** Informação obtida do campo homônimo da *TabelaSalas*. Identifica unicamente a qual sala o usuário está associado.
- **Número da cadeira (campo *numeroCadeira*):** Informa qual o número da cadeira virtual do usuário dentro da sala virtual de conferência em questão. Essa informação não é utilizada na versão atual do sistema, mas pode vir a ser utilizada para representar de forma especial um participante na sala virtual de conferência, por exemplo.

Quando o usuário está associado a mais de uma sala, uma outra tupla é armazenada na tabela *TabelaParticipanteCadeiraSala* contendo o *login* do usuário, o número da sala e o número da cadeira.

B. FORMATOS DOS PACOTES DE CONTROLE DE CONFERÊNCIA

“Eu sou o pão da vida. Vossos pais comeram o maná no deserto e morreram. Este é o pão que desceu do céu, para que todo o que dele comer não pereça. Eu sou o pão vivo que desceu do céu; se alguém dele comer, viverá eternamente; e o pão que eu darei pela vida do mundo é a minha carne.”

João 6.48-51

Inicialmente, os protocolos de controle de sessão e de posse da palavra foram implementados sobre o pacote do tipo APP do RTCP (SCHULZRINNE et al., 1996), com o intuito de minimizar o número de portas UDP utilizadas. Com o desenvolver do trabalho, percebeu-se que o decodificador do canal de controle de conferência poderia ser simplificado e mais eficiente se ele fosse separado do canal RTCP e assim foi feito. Entretanto, para reaproveitamento de código, alguns campos do pacote RTCP APP foram mantidos, com modificações. Uma evolução dos protocolos de controle de sessão, de controle de posse da palavra e de *chat* de texto está sendo estudada, baseada na experiência obtida com o desenvolvimento do sistema.

O pacote para pedido de admissão na conferência do protocolo de controle de sessão é apresentado na Figura B.1.

1																																2																																3																															
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1																																																																
V		P		Type=X				PT=204								Length																																																																															
SSRC																																																																																															
User ID																								User Type																																																																							
User IP																																																																																															
UDP Control RX																UDP Control TX																																																																															
UDP RTP Voice RX																UDP RTP Voice TX																																																																															
UDP RTCP Voice RX																UDP RTCP Voice TX																																																																															
UDP RTP Video RX																UDP RTP Video TX																																																																															
UDP RTCP Video RX																UDP RTCP Video TX																																																																															
SDES CNAME																																																																																															

Figura B.1 – Pacote para pedido de entrada na conferência (controle de sessão).

Os campos do pacote de pedido de entrada na conferência são os seguintes:

- **V (*Version* – *Versão*):** 2 *bits*. Campo herdado do pacote RCTP APP (SCHULZRINNE et al., 1996). Especifica a versão do RTP, que é a mesma do RTCP. A versão atual, especificada pela RFC 1889, é dois (10 em binário).
- **P (*Padding* – *Enchimento*):** 1 *bit*. Campo herdado do pacote RTCP APP. Se esse *bit* está marcado, o pacote contém um ou mais *bytes* ao final, que não fazem parte dos dados sendo transportados. O último *byte* do pacote informa quantos *bytes* de enchimento devem ser ignorados. O enchimento é utilizado, por exemplo, para garantir o alinhamento requerido por alguns algoritmos de criptografia com blocos de tamanho fixo ou por algum protocolo das camadas inferiores.
- **Type (*Tipo*):** 5 *bits*. Diferencia qual o tipo de mensagem do protocolo de controle de conferência sendo transportado, se de controle de sessão, de controle de posse da palavra ou se de texto, segundo a Tabela B.1.
- **PT (*Packet type* – *Tipo de pacote*):** 8 *bits*. Campo herdado do RTCP APP. Contém o valor decimal fixo 204.
- **Length (*Comprimento*):** 16 *bits*. Corresponde ao comprimento do pacote em palavras de 32 *bits*, menos um, tornando zero um valor válido. Portanto, um alinhamento de 32 *bits* é obrigatório.
- **SSRC (*Synchronization source identifier* – *Identificador de fonte de sincronismo*):** 32 *bits*. Identifica o SSRC (SCHULZRINNE et al., 1996) do transmissor do pacote de controle. O SSRC é um número aleatório usado para identificar unicamente cada participante em uma sessão RTP. Na verdade, essa não é a única forma de se identificar unicamente o participante dentro da conferência. A outra forma é o SDES CNAME (*Source Description Canonical Name* – Nome canônico de descrição da fonte) do RTCP.
- **User ID (*Identificação do usuário*):** 24 *bits*. Informa qual o número da cadeira virtual do participante dentro da sala virtual de conferência. Corresponde a mais uma forma de identificação do participante.

- **User Type (Tipo de usuário):** 8 *bits*. Informa qual o papel pretendido pelo usuário dentro da conferência, se de moderador (valor 0x01 em hexadecimal) ou de participante comum (valor 0x00 em hexadecimal).
- **UDP Control RX (UDP Controle RX):** 16 *bits*. Informa qual a porta UDP utilizada pela *applet* Java do usuário para a recepção do canal de controle de conferência.
- **UDP Control TX (UDP Controle TX):** 16 *bits*. Informa qual a porta UDP utilizada pela *applet* Java do usuário para a transmissão do canal de controle de conferência.
- **UDP RTP Voice RX (UDP RTP Voz RX):** 16 *bits*. Informa qual a porta UDP utilizada pela *applet* Java do usuário para a recepção dos pacotes RTP de voz.
- **UDP RTP Voice TX (UDP RTP Voz TX):** 16 *bits*. Informa qual a porta UDP utilizada pela *applet* Java do usuário para a transmissão dos pacotes RTP de voz.
- **UDP RTCP Voice RX (UDP RTCP Voz RX):** 16 *bits*. Informa qual a porta UDP utilizada pela *applet* Java do usuário para a recepção dos pacotes RTCP referentes ao canal de voz.
- **UDP RTCP Voice TX (UDP RTCP Voz TX):** 16 *bits*. Informa qual a porta UDP utilizada pela *applet* Java do usuário para a transmissão dos pacotes RTCP referentes ao canal de voz.
- **UDP RTP Video RX (UDP RTP Vídeo RX):** 16 *bits*. Informa qual a porta UDP utilizada pela *applet* Java do usuário para a recepção dos pacotes RTP de vídeo. Esse campo será utilizado quando o sistema suportar o uso de vídeo.
- **UDP RTP Video TX (UDP RTP Vídeo TX):** 16 *bits*. Informa qual a porta UDP utilizada pela *applet* Java do usuário para a transmissão dos pacotes RTP de vídeo. Esse campo será utilizado quando o sistema suportar o uso de vídeo.
- **UDP RTCP Video RX (UDP RTCP Vídeo RX):** 16 *bits*. Informa qual a porta UDP utilizada pela *applet* Java do usuário para a recepção dos pacotes RTCP referentes ao canal de vídeo. Esse campo será utilizado quando o sistema suportar o uso de vídeo.

- **UDP RTCP Video TX (UDP RTCP Vídeo TX):** 16 *bits*. Informa qual a porta UDP utilizada pela *applet* Java do usuário para a transmissão dos pacotes RTCP referentes ao canal de vídeo. Esse campo será utilizado quando o sistema suportar o uso de vídeo.
- **SDES CNAME (*Source description canonical name* – Nome canônico de descrição da fonte):** Variável (até 255 B). Identificador único do participante dentro de uma conferência. Geralmente ele é representado na forma <usuário>@<host>, como “marcel@macadamia.larc.usp.br”, por exemplo.

O pacote de pedido de entrada na conferência difere dos demais pacotes de controle de sessão pelas informações referentes a portas UDP utilizadas e ao endereço IP do usuário. Essas informações são utilizadas quando o usuário está pedindo para entrar na conferência, para auxiliar a unidade de controle multiponto na detecção de NATs/NAPTs na rede.

Tabela B.1 – Tipos de mensagem do protocolo de controle de conferência

Valor binário (valor decimal) do campo <i>Type</i>	Descrição do pacote
00000 (00)	Pedido para entrar na conferência.
00001 (01)	Moderador permite que o usuário entre na conferência.
00010 (02)	Moderador nega a entrada do usuário na conferência.
00011 (03)	A <i>applet</i> do moderador recebeu o pedido para entrar na conferência.
00100 (04)	Participante está abandonando a conferência.
00101 (05)	Moderador está expulsando o participante especificado da conferência.
00110 (06)	Moderador anistia o participante expulso.
00111 (07)	Notificação de problemas de conexão do participante com a unidade de controle multiponto.
01000 (08)	Notificação de restabelecimento de conexão do participante com a unidade de controle multiponto.
01001 (09)	Pacote de sincronismo enviado pelo participante.
01010 (10)	Pacote de controle de posse da palavra.
10100 (20)	Pacote de <i>chat</i> de texto.

O participante transmite periodicamente suas informações de identificação em um pacote de sincronismo, que é repassado pela unidade de controle multiponto aos demais participantes da conferência, de forma que as suas interfaces homem-máquina mostrem quem está presente na conferência.

O pacote do protocolo de controle de sessão é apresentado na Figura B.2.

Figura B.2 – Pacote de controle de sessão.

As informações referentes às portas UDP e ao endereço IP são retiradas do pacote de pedido de entrada na conferência pela unidade de controle multiponto antes de encaminhá-lo aos demais participantes. Essas informações são úteis somente à unidade de controle multiponto. Dessa forma, pacotes menores são transmitidos, economizando-se banda. Esse pacote de controle de sessão é o mesmo utilizado para sinalizar abandono da conferência, expulsão e anistia de participantes.

Os campos *V*, *P*, *Type*, *PT*, *Length*, *SSRC*, *User ID*, *User Type* e *SDES CNAME* são os mesmos do pacote de pedido de entrada na conferência.

O pacote do protocolo de controle de posse da palavra é apresentado na Figura B.3.

Figura B.3 – Pacote do protocolo controle de posse da palavra.

Os campos *V*, *P*, *Type*, *PT*, *Length* e *SSRC* são os mesmos dos pacotes anteriores. Os demais campos do pacote de controle de posse da palavra são os seguintes:

- **PV (*Protocol version* – Versão do protocolo):** 2 *bits*. Indica a versão do protocolo de controle de posse da palavra e conseqüentemente, como os campos devem ser interpretados. A versão atual é 00 em binário.
- **CT (*Control type* – Tipo de controle):** 6 *bits*. Informa o tipo de mensagem de controle sendo transmitida, segundo a Tabela B.2.
- **Reserved (Reservado):** 8 *bits*. Campo reservado para uso futuro.
- **Sequence number (Número de seqüência):** 16 *bits*. Número de seqüência da mensagem sendo transmitida. O valor inicial de cada número de seqüência é aleatório, para dificultar alguns tipos de ataque de texto plano, mas deve estar dentro da faixa $[0, 2^{15}]$, para evitar problemas de estouro precoce do contador de mensagens.
- **Target SSRC (SSRC alvo):** 32 *bits*. Ajuda a identificar de forma única a quem a mensagem se destina. Embora a especificação do RTP (SCHULZRINNE et al., 1996) sugira que um SSRC diferente seja utilizado para cada canal de mídia de uma mesma fonte, o SSRC do canal de áudio, por exemplo, pode ser utilizado como identificador de participantes dentro da conferência, por ser único dentro de uma conferência.
- **Target SDES CNAME (Nome canônico alvo):** Variável. Esse campo utiliza a informação do SDES CNAME do RTCP (SCHULZRINNE et al., 1996) para ajudar a identificar de forma única a quem o pacote se destina. Por herança do pacote RTCP APP, esse campo precisa ser múltiplo de 32 *bits*, de forma que um enchimento de um a três *bytes* pode ser necessário, devendo ser devidamente sinalizado no campo *P*.

Tabela B.2 – Tipos de mensagem de controle de posse da palavra

Valor binário (valor decimal) do campo CT	Descrição da mensagem de controle de posse da palavra
000000 (00)	Participante recebeu a mensagem (ACK do participante).
000100 (04)	Participante requisita a posse da palavra.
001000 (08)	Participante devolve a posse da palavra ao moderador.
001100 (12)	Participante desiste da requisição da posse da palavra.
010100 (20)	Participante aceita ser o novo moderador.
011000 (24)	Participante recusa ser o novo moderador.
011111 (31)	Participante recebeu a mensagem, mas ela não é suportada.
100000 (32)	Moderador recebeu a mensagem (ACK do moderador).
100010 (34)	Moderador desiste da posse da palavra.
100011 (35)	Moderador avisa que deseja de volta a posse da palavra.
100100 (36)	Moderador concede a posse da palavra ao participante especificado.
101000 (40)	Moderador nega explicitamente a posse da palavra ao participante especificado.
101001 (41)	Moderador bloqueia a recepção de áudio do participante especificado.
101010 (42)	Moderador libera o participante especificado a receber áudio novamente.
101100 (44)	Moderador retira explicitamente a posse da palavra do participante especificado.
101101 (45)	Unidade de controle multiponto avisa que o participante não está com a posse da palavra.
111111 (63)	Moderador tenta eleger o participante especificado como novo moderador.

Ainda que haja mensagens explícitas para se notificar a perda de posse da palavra e a negação de posse da palavra, o sistema utiliza predominantemente a forma implícita dessas mensagens, isto é, quando a posse da palavra é concedida a outro participante, implicitamente o participante que a detinha a perde. Da mesma forma, quando há mais de um participante desejando a posse da palavra, os participantes que não a receberam entendem implicitamente que ela lhes fora negada. A perda de posse da palavra implícita só é possível, porque o sistema atualmente só admite um único participante com a posse da palavra. Caso o sistema venha futuramente permitir que mais de um participante fale simultaneamente, para aumentar a interatividade da conferência, será necessário explicitar a perda de posse da palavra.

Futuramente, os campos *Type* e *Control Type* podem ser unificados, ainda que os canais de controle de sessão, de posse da palavra e de *chat* de texto venham a ser separados. Dessa forma, a decodificação do pacote recebido fica simplificada, bastando a verificação do valor de um único campo para saber a finalidade da mensagem.

O pacote do protocolo de *chat* de texto é apresentado na Figura B.4.

Figura B.4 – Pacote do protocolo de *chat* de texto.

Os campos *V*, *P*, *Type*, *PT*, *Length* e *SSRC* são os mesmos dos pacotes anteriores. Os demais campos do pacote de texto são os seguintes:

- **PV (*Protocol version* – Versão do protocolo):** 2 *bits*. Indica a versão do protocolo de *chat* de texto e conseqüentemente, como os campos devem ser interpretados. A versão atual é 00 em binário.
- **ND (*Number of destinations* – Número de destinos):** 4 *bits*. Informa para quantos participantes essa mensagem de texto será transmitida. Esse campo define quantos SSRCs estarão presentes no campo *Target SSRC_N*. O valor 0000 em binário indica que o pacote deve ser encaminhado para todos os participantes da conferência.
- **R (*Reserved* – Reservado):** 2 *bits*. Campo reservado para uso futuro.
- **Sequence number (Número de seqüência):** 12 *bits*. Número de seqüência da mensagem sendo transmitida. O valor inicial de cada número de seqüência é

aleatório, para dificultar alguns tipos de ataque de texto plano, mas deve estar dentro da faixa $[0, 2^{11}]$, para evitar problemas de estouro precoce do contador de mensagens.

- **LSNR (*Last sequence number received* – Último número de seqüência recebido):** 12 *bits*. Número de seqüência da última mensagem recebida. Serve para indicar ao transmissor se sua última mensagem foi recebida corretamente.
- **Last message's SSRC (SSRC da última mensagem):** 32 *bits*. Indica qual o SSRC da última mensagem recebida, para associar a informação do número de seqüência da última mensagem com o originador dela.
- **Target SSRC_N (SSRCs alvos):** De 0 a 15 palavras de 32 *bits*. Dependendo do campo *ND*, pode conter de 0 a 15 SSRCs, indicando a quem a mensagem é destinada. Se não houver nenhum SSRC nesse campo (*ND* com valor 0000 em binário), a mensagem deve ser transmitida a todos os participantes da conferência.
- **Text (Texto):** Variável. Contém o texto a ser transmitido. O comprimento desse campo precisa ser múltiplo de 32 *bits*. Se os cabeçalhos IP, UDP e do protocolo de transporte de texto ocuparem, respectivamente, 20, 8 e de 16 a 76 B (dependendo do número de SSRCs), e considerando a MTU IP como sendo 1.500 B, cada pacote poderia transportar de 1.396 a 1.456 B de texto, sem que ocorra fragmentação do pacote. Com cada caractere ASCII ocupando um *byte*, então, no máximo 1.456 caracteres podem ser transmitidos por pacote, sem compressão.

Os campos que identificam a último pacote de texto recebido servem para permitir um mecanismo de retransmissão de mensagens de texto.

C. DIAGRAMA DE TROCA DE MENSAGENS DE CONTROLE DE CONFERÊNCIA

“Acaso, pode uma mulher esquecer-se do filho que ainda mama, de sorte que não se compadeça do filho do seu ventre? Mas ainda que esta viesse a se esquecer dele, eu, todavia, não me esquecerei de ti.”

Isaías 49.15

Os diagramas de tempo de troca de mensagens de controle de sessão e de controle de posse da palavra entre as *applets* Java da página *web* do participante comum e do moderador e a unidade de controle multiponto são apresentados a seguir. As trocas de mensagens, suas correspondentes ações desencadeadoras e desencadeadas na unidade de controle multiponto, nas *applets* Java e interfaces homem-máquina dos participantes foram projetadas de forma que o usuário seja o mecanismo de retransmissão das mensagens, aliviando o processamento da unidade de controle multiponto e das *applets*, simplificando seu funcionamento e implementação.

Quando um pacote de controle de conferência é enviado ou recebido, ele pode provocar mudanças na interface-homem máquina do participante ao qual o pacote se refere.

Por causa do duplo mecanismo de sincronismo, toda vez que um participante tem sua indicação alterada, ele envia sua nova indicação para o servidor *web*. As únicas exceções ocorrem quando o moderador expulsa um participante da conferência e quando o moderador concede anistia ao participante expulso. Nessas duas situações, o moderador envia para o servidor *web* as novas indicações do participante expulso e anistiado.

Para todos os diagramas a seguir, a unidade de controle multiponto será identificada por *MCU*, o moderador será identificado por *M*, o participante em questão por *P* e os demais participantes da conferência, por *Participantes*. Em alguns dos diagramas, *M* e *P* podem se encontrar dentro do grupo *Participantes*. As mensagens de confirmação de recebimento da unidade de controle multiponto, da *applet* Java do

moderador e do participante serão chamadas de ACK_{MCU} , ACK_M e ACK_P , respectivamente.

C.1 Diagramas de tempo de troca de mensagens de controle de posse da palavra

Os diagramas de tempo de troca de mensagens de controle de posse da palavra são apresentados para definir o funcionamento do mecanismo de controle de posse da palavra.

C.1.1 Participante comum pedindo a posse da palavra

A Figura C.1 ilustra um participante comum pedindo a posse da palavra para o moderador.

Figura C.1 – Participante comum pedindo a posse da palavra.

Estando o participante comum P já admitido na conferência, ele pode requisitar a posse da palavra sempre que sua indicação estiver *normal*, isto é, sempre que ele estiver na conferência sem a posse da palavra (indicação *possePalavra*), sem o seu áudio bloqueado (indicação *semAudio*) pelo moderador e sem problemas de comunicação (indicação *semInformacao*) com a unidade de controle multiponto. Essa restrição decorre do fato de o *menu* de cada participante na sala virtual de conferência apresentar somente as opções compatíveis com a sua indicação atual e seu papel na conferência. Através da sua interface homem-máquina ele requisita a posse da palavra. Há três momentos possíveis para P mudar sua interface homem-máquina para *pedindoPalavra*:

- **No instante em que o pedido é enviado:** Nessa situação, P não tem como saber se M recebeu a sua requisição, porque ela pode ter se perdido entre P e a MCU ou entre a MCU e M . Se a indicação do participante fosse alterada para *pedindoPalavra* e o moderador não a tivesse recebido, a única forma de P reenviar a requisição é enviando uma mensagem de desistência do pedido de posse da palavra, voltando para a indicação *normal* e enviando uma nova requisição.
- **No recebimento do ACK_{MCU} :** Nessa situação, P sabe que a MCU recebeu a sua requisição, mas também não tem como saber se o moderador a recebeu.
- **No recebimento do ACK_M :** Nessa situação, P tem a certeza que M recebeu a sua requisição. O tempo de resposta da ação do participante é o *round-trip time* da camada de aplicação (RTT_{APP}) entre P e M . Isto é, o tempo que leva para a interface homem-máquina de P ser atualizada a partir do instante em que ele requisitou a posse da palavra depende do tempo de processamento e de transmissão da requisição e do ACK_M pela unidade de controle multiponto e pelas *applets* Java de P e de M , mais o atraso inserido pela rede. Se RTT_{APP} for estimado em aproximadamente um segundo para conferências sendo realizadas através da Internet, esse será aproximadamente o tempo que levará para a interface homem-máquina de P ser atualizada. A interface homem-máquina de M e dos demais participantes serão atualizadas antes que a de P . Se ACK_M não for

recebido por P , ou se P enviar uma nova requisição antes do seu recebimento, não haverá problemas, porque as interfaces homem-máquina de M e dos *Participantes* continuará consistente e a *applet* Java de M transmitirá um novo ACK_M .

Portanto, a interface homem-máquina de P é atualizada no recebimento de ACK_M .

C.1.2 Participante comum desistindo de pedir a posse da palavra

A Figura C.2 ilustra um participante comum desistindo do pedido da posse da palavra.

Figura C.2 – Participante comum desistindo de pedir a posse da palavra.

Enquanto ACK_M não for recebido por P , P pode novamente enviar a mensagem de desistência do pedido de posse da palavra, até que sua indicação passe para *normal*.

C.1.3 Participante comum devolvendo a posse da palavra

A Figura C.3 mostra o participante comum P devolvendo a posse da palavra para o moderador M .

Figura C.3 – Participante comum devolvendo a posse da palavra para o moderador.

No instante em que a MCU recebe a devolução da posse da palavra de P , ela pára de encaminhar os pacotes RTP de P e passa a esperar pelos pacotes RTP de M , porque há uma concessão implícita da posse da palavra para M . Quando M recebe a devolução da posse da palavra de P , M muda sua indicação e começa a transmitir seus pacotes RTP de áudio. Se a devolução da posse da palavra for perdida entre a MCU e M , P continuará transmitindo até que ele receba uma ordem expressa da MCU para parar de transmitir, mudando sua indicação para *normal*, ou até que ele reenvie a devolução de posse da palavra e receba ACK_M . No primeiro caso, como M não recebeu a devolução da posse da palavra, ninguém estará transmitindo. Em

último caso, o usuário no papel de moderador perceberá que ninguém está transmitindo e pode tomar a posse da palavra explicitamente.

Quando a troca de mensagens é realizada com sucesso, há um curto período de tempo em que a *MCU* não encaminhará pacotes RTP de ninguém, porque *M* ainda não começou a transmitir, seguido de outro curto período de tempo em que ela recebe pacotes RTP de *P* e de *M*, porque *P* ainda não parou de transmitir. Esse comportamento pode ser observado nos gráficos de banda de recepção e de transmissão da *MCU* nos teste do Capítulo 5.2.3.1.

C.1.4 Moderador concedendo a posse da palavra de um participante para outro

A Figura C.4 mostra o moderador concedendo a posse da palavra de um participante para outro, requisitando-a ou não.

Figura C.4 – Moderador concedendo a posse da palavra de um participante para outro.

O moderador pode conceder a posse da palavra a um participante mesmo que ele não a esteja requisitando no momento. O moderador não pode conceder a posse da palavra para um participante que não esteja dentro da conferência (indicações *foraConferencia*, *expulso* e *pedindoEntrar*), ou com o áudio bloqueado (indicação *semAudio*) ou que esteja com problemas de comunicação com a unidade de controle multiponto (indicação *semInformacao*).

Quando a *MCU* recebe a concessão de posse da palavra para *P*, ela pára de encaminhar os pacotes RTP de áudio do participante que estava com a posse da palavra, *P'*, e passa a esperar pelos pacotes RTP de áudio de *P*.

Se *P'* não receber a concessão de posse da palavra para *P*, ele continuará a transmitir até que a *MCU* ordene explicitamente que ele pare, através de uma mensagem de perda de posse da palavra (pseudo-indicação *semPossePalavra*).

Se o moderador não receber o ACK_P , sua interface homem-máquina continuará indicando *P* sem a posse da palavra, possibilitando ao moderador enviar novamente a concessão de posse da palavra a ele, até que ACK_P seja recebido.

Quando a posse da palavra é concedida para um participante, há uma perda implícita de posse da palavra do participante que a detinha. Então, as interfaces homem-máquina alterarão dois participantes simultaneamente, *P* e *P'*.

Havendo sucesso na troca de mensagens, quando a *MCU* recebe a concessão de posse da palavra para *P*, ela pára de encaminhar os pacotes RTP de áudio de *P'* e passa a esperar os pacotes de *P*.

Por um curto intervalo de tempo, ela não encaminhará os pacotes RTP de nenhum participante. A seguir, por um curto período de tempo, a *MCU* receberá pacotes RTP de áudio de *P* e de *P'*, até que *P'* pare seu transmissor. Esse comportamento também pode ser observado nos gráficos de banda de recepção e de transmissão da *MCU* apresentados no Capítulo 5.2.3.1.

C.1.5 Moderador concedendo a posse da palavra para um participante

A Figura C.5 mostra o moderador com a posse da palavra concedendo-a a um participante comum.

Figura C.5 – Moderador concedendo a posse da palavra para um participante que a esteja requisitando ou não.

Quando a *MCU* recebe a concessão de posse da palavra para *P*, ela pára de encaminhar os pacotes RTP de áudio de *M*, e passa a esperar pelos pacotes RTP de áudio de *P*. Se *M* não receber logo ACK_P , ele continuará a transmitir até que a *MCU* ordene explicitamente que ele pare, através de uma mensagem de perda de posse da palavra (pseudo-indicação *semPossePalavra*).

Se o moderador não receber o ACK_P , sua interface homem-máquina continuará indicando *P* sem a posse da palavra, permitindo que o moderador novamente envie a concessão de posse da palavra a ele, até que ACK_P seja recebido.

As interfaces homem-máquina de todos os *Participantes* devem alterar as indicações de *M* e de *P* quando for recebida a concessão de posse da palavra para *P*.

Analisando o caso quando há sucesso na troca de mensagens: quando a *MCU* recebe a concessão de posse da palavra para *P*, ela pára de encaminhar os pacotes RTP de áudio de *M* e passa a esperar pelos pacotes de *P*. A banda de transmissão de pacotes RTP da *MCU* cai a zero, enquanto a de recepção permanece igual a um canal de áudio. Quando *P* receber a posse da palavra e iniciar seu transmissor, por um curto intervalo de tempo, a *MCU* receberá os pacotes RTP de *M* e de *P*, porque *M* ainda não recebeu o ACK_P e por isso continua a transmitir, a menos que *M* receba nesse intervalo de tempo uma notificação para parar de transmitir. Durante esse período de tempo, a banda de recepção de pacotes RTP da *MCU* dobra e a de transmissão é restabelecida. Esse comportamento pode também ser observado nos gráficos de banda de recepção e de transmissão da *MCU* discutidos no Capítulo 5.2.3.1.

C.1.6 Moderador tomando de volta a posse da palavra

A Figura C.6 mostra o moderador tomando de volta a posse da palavra à força.

Figura C.6 – Moderador tomando de volta a posse da palavra.

Caso P não queira devolver a posse da palavra para M , este pode tomá-la à força, enviando uma mensagem de perda de posse da palavra para P . A perda de posse da palavra carrega implicitamente uma concessão de posse da palavra para M . Se a posse da palavra para M fosse explícita, não seria necessário enviar uma mensagem de perda de posse da palavra para P .

Há três instantes distintos nos quais a interface homem-máquina de M poderia ser atualizada:

- **No envio da perda de posse da palavra:** Se a interface homem máquina de M fosse atualizada nesse instante e M passasse a transmitir seus pacotes RTP de áudio, se a MCU não receber a perda de posse da palavra de P , ela continuará a achar que P está com a posse da palavra, encaminhando seus pacotes RTP de áudio, e irá pedir para M parar de transmitir, acarretando na mudança da indicação de M para *normal*.
- **No recebimento de ACK_{MCU} :** Atualizando a interface homem-máquina de M nesse instante, M tem a certeza que a MCU sabe que ele está com a posse da palavra. Se P não receber a perda de posse da palavra, a MCU acabará transmitindo a ele uma ordem para que ele cesse sua transmissão, mudando sua indicação para *normal*, saindo do estado inconsistente.
- **No recebimento de ACK_P :** Esse é o instante mais inapropriado para se alterar a interface homem-máquina de M , porque se P não transmitir ACK_P , M não conseguiria tomar a posse da palavra de volta.

Portanto, a interface homem-máquina de M é alterada quando M recebe ACK_{MCU} .

Novamente, em caso de sucesso na troca de mensagens, a MCU não encaminhará pacotes RTP de nenhum participante por um curto período de tempo, até que ela passe a receber os pacotes RTP de M . Nessa situação, pode ser que a MCU nem chegue a receber simultaneamente os pacotes RTP de áudio de P e de M , caso P

receba a perda de posse da palavra e pare de transmitir antes que M comece, após o recebimento de ACK_{MCU} .

Quando o moderador toma de volta a posse da palavra de um participante, todas as interfaces homem-máquina devem alterar as indicações de P e de M para *normal* e *possePalavra*, respectivamente.

C.1.7 Moderador pedindo a posse da palavra

A Figura C.7 mostra o moderador pedindo a posse da palavra.

Figura C.7 – Moderador pedindo a posse da palavra.

O moderador não precisaria avisar a ninguém que ele está pedindo a posse da palavra, mas ele pode fazê-lo, para avisar a P que ele deseja tomá-la de volta. Dessa forma, P pode educadamente devolvê-la ou esperar até que M a tome por força.

Esperar pelo ACK_{MCU} para mudar a indicação de M é suficiente, não sendo necessário esperar um eventual ACK_P , mesmo porque se ACK_P não fosse recebido, M não conseguiria alterar sua indicação.

C.1.8 Moderador desistindo do pedido de posse da palavra

Semelhantemente ao participante comum, o moderador também pode desistir de pedir a posse da palavra. A Figura C.8 mostra o moderador desistindo do pedido de posse da palavra.

Figura C.8 – Moderador desistindo do pedido de posse da palavra.

Esperar pelo ACK_{MCU} para mudar a indicação de M é suficiente, não sendo necessário esperar um eventual ACK_P , mesmo porque se ACK_P não fosse recebido, M não conseguiria mais alterar sua indicação.

C.1.9 Moderador bloqueando o recebimento de áudio de um participante

A Figura C.9 mostra o moderador ordenando à unidade de controle multiponto que não encaminhe mais pacotes RTP de áudio para um determinado participante até segunda ordem.

Figura C.9 – Moderador bloqueando o recebimento de áudio de um participante.

O moderador só pode bloquear o áudio de um participante que esteja com as indicações *normal* ou *pedindoPalavra*. Novamente, há três instantes distintos onde a interface homem-máquina de *M* poderia ser alterada:

- **No envio do bloqueio do áudio de *P*:** Se a interface homem-máquina de *M* fosse alterada nesse instante, não há como se garantir que a *MCU* irá parar de encaminhar os pacotes RTP de áudio para *P*, caso o pacote se perca entre *M* e a *MCU*.
- **No recebimento do ACK_{MCU} :** Nesse instante, *M* tem a certeza que a *MCU* não irá mais encaminhar pacotes RTP de áudio para *P*, mas talvez *P* não tenha recebido o bloqueio e fique sem saber o porquê de não estar mais recebendo áudio, podendo achar que há algum problema na rede.
- **No recebimento de ACK_P :** Atualizando a interface homem-máquina de *M* nesse instante garante que a *MCU* e que *P* receberam a mensagem de bloqueio de áudio de *P*.

Portanto, *M* tem sua interface homem-máquina alterada no recebimento de ACK_P .

Quando a *MCU* recebe a mensagem de bloqueio do áudio de *P*, ela pára de encaminhar pacotes RTP de áudio para ele. Para uma sala virtual de conferência, há várias situações em que se pode ser útil bloquear o áudio de um determinado participante por um período de tempo. No caso do paradigma da sala de aula virtual, o professor pode estar explicando algo para um grupo de alunos que o outro grupo não deva saber, a fim de que posteriormente haja um debate entre eles, por exemplo.

C.1.10 Moderador liberando o recebimento de áudio de um participante

A Figura C.10 mostra o moderador ordenando à unidade de controle multiponto que volte a encaminhar pacotes RTP de áudio para o participante com o áudio bloqueado.

Figura C.10 – Moderador liberando o recebimento de áudio de um participante.

Esperar o recebimento de ACK_P para se mudar a indicação de *P* na interface homem-máquina de *M* garante que *P* receberá novamente os pacotes de áudio e que sua interface homem-máquina não ficará inconsistente com relação a isso. Se o ACK_P

fosse perdido e M reenviasse a liberação do áudio de P , P transmitiria novamente ACK_P , mantendo sua indicação inalterada na sua interface homem-máquina.

C.2 Diagramas de tempo de troca de mensagens de controle de sessão

Os diagramas de tempo de troca de mensagens de controle de sessão são apresentados para definir o mecanismo de participação na conferência.

C.2.1 Moderador pedindo para entrar na conferência

A Figura C.11 e a Figura C.12 mostram o pedido para entrar na conferência do moderador sendo aceito e rejeitado pela unidade de controle multiponto.

Figura C.11 – Moderador pedindo para entrar na conferência e sendo aceito pela unidade de controle multiponto.

Quando a página *web* da sala virtual de conferência é carregada, todo participante inicia com a indicação *foraConferencia* e sua *applet* Java transmite automaticamente o pedido para entrar na conferência para a *MCU*. A *MCU* pode aceitar ou não o pedido do moderador para entrar na conferência. Na versão atual do sistema, a *MCU* sempre aceita a entrada do moderador na conferência, mas ela poderia ser alterada de forma a rejeitar o pedido do moderador para entrar na conferência, caso o endereço IP do pacote não seja o endereço IP cadastrado para o moderador na configuração da sala no *site* de gerenciamento.

Quando *M* transmite o pedido para entrar na conferência, ele inicia a transmissão de pacotes RTP de áudio, de forma que a *MCU* possa capturar a porta UDP utilizada pela sua *applet* Java para transmissão e recepção de pacotes RTP de áudio. Esse comportamento é necessário para superar barreiras com NAPT (vide Capítulo 2.4.3).

Ao receber o pedido para entrar na conferência de *M*, a *MCU* adiciona as informações recebidas em sua estrutura de dados de participantes e transmite o ACK_{MCU} , que quando é recebido por *M* provoca a mudança na sua interface homem-máquina para *pedindoEntrar* e a interrupção de pacotes RTP de áudio. Se o ACK_{MCU} não for recebido até um certo tempo determinado, a *applet* Java de *M* irá retransmitir o pedido para entrar na conferência. Isso ocorre um número determinado de vezes²⁵. Se a *MCU* não responder, um aviso na interface homem-máquina de *M* será gerado sobre o ocorrido. Se *M* não for admitido na conferência e não parar de transmitir pacotes RTP de áudio, a *MCU* pede explicitamente para que ele pare de transmitir.

Se a interface homem-máquina do moderador fosse alterada de *foraConferencia* para *pedindoEntrar* no instante que o pedido para entrar na conferência fosse transmitido, o moderador não teria como saber se o seu pedido foi recebido pela *MCU* e ele não teria como pedir novamente para entrar na conferência.

Ao receber a permissão para entrar na conferência, *M* muda sua indicação para *possePalavra*, reiniciando o seu transmissor de pacotes RTP de áudio. O moderador sempre recebe a posse da palavra implicitamente quando é admitido na conferência.

²⁵ A versão atual do sistema transmite um pedido para entrar na conferência a cada quatro segundos, por até cinco vezes.

Figura C.12 – Moderador pedindo para entrar na conferência e sendo rejeitado pela unidade de controle multiponto.

Sempre que um participante estiver com a indicação *foraConferencia*, ele pode pedir para entrar na conferência. O diagrama de tempo do pedido do moderador para entrar na conferência foi projetado de forma que se a requisição do moderador não for recebida pela *MCU* ou se o ACK_{MCU} for perdido, *M* tenha como repetir novamente o processo. Se a permissão para entrar na conferência for perdida, o moderador pode abandonar a conferência, passando da indicação *pedindoEntrar* para a indicação *foraConferencia*.

Se a *MCU* rejeitar o pedido de *M* para entrar na conferência, ela apaga as informações de *M* da sua estrutura de dados e transmite a mensagem contendo a rejeição.

Ao receber a rejeição do seu pedido para entrar na conferência, *M* pára o seu transmissor e muda a sua indicação para *foraConferencia*.

A *MCU* poderia transmitir diretamente a permissão ou a negação para entrar na conferência para *M*, sem transmitir o ACK_{MCU} , porque o resultado final é o mesmo e o intervalo de tempo entre os dois pacotes é muito curto.

Caso a conferência já possua um moderador e algum outro participante tente entrar como moderador (campo *User Type* do pedido para entrar na conferência com valor de moderador), a unidade de controle multiponto encaminha o pedido para entrar na conferência para o moderador atual, já com o campo *User Type* corrigido com valor de participante comum. Ao receber o ACK_M , a *applet* Java do participante que tentou entrar como moderador alterará seu comportamento para funcionar como participante comum.

C.2.2 Participante comum pedindo para entrar na conferência

A Figura C.13 mostra um participante comum pedindo para entrar na conferência.

Figura C.13 – Participante comum pedindo para entrar na conferência.

Quando *P* transmite seu pedido para entrar na conferência, ele inicia a transmissão de seus pacotes RTP de áudio pelos mesmos motivos apresentados no caso de *M*.

Há três instantes distintos nos quais *P* poderia alterar sua indicação na sua interface homem-máquina:

- **No envio do pedido para entrar na conferência:** Se a alteração fosse efetuada nesse instante, P não teria como saber se o seu pedido foi recebido pelo moderador.
- **No recebimento de ACK_{MCU} :** Se a alteração fosse efetuada nesse instante, P também não teria como saber se o seu pedido foi recebido pelo moderador. Entretanto, quando P recebe ACK_{MCU} , ele já pára o seu transmissor de pacotes RTP de áudio.
- **No recebimento de ACK_M :** Nesse instante, P tem a certeza que M recebeu o seu pedido para entrar na conferência. Caso ACK_M se perca no meio do caminho, P consegue facilmente pedir novamente para entrar na conferência. Quando M receber o novo pedido de P para entrar na conferência, M simplesmente retransmitirá ACK_M .

Quando a MCU recebe o pedido de P para entrar na conferência, ela insere as informações a respeito de P recebidas temporariamente na sua estrutura de dados de participantes. Se P for admitido na conferência, suas informações são armazenadas na estrutura de dados de participantes, caso contrário, suas informações são excluídas. Se P for vetado na conferência ou posteriormente expulso, suas informações não são excluídas, para que ele possa ser identificado e tenha seus pacotes bloqueados pela MCU .

C.2.3 Moderador admitindo um participante na conferência

A Figura C.14 mostra o moderador admitindo um participante na conferência.

Figura C.14 – Moderador admitindo um participante na conferência.

A interface homem-máquina de *M* só altera a indicação de *P*, quando *M* recebe ACK_P , porque assim *M* tem a certeza que *P* recebeu a autorização para entrar na conferência. Caso *M* não receba ACK_P , o usuário no papel de moderador reenviará a permissão para *P* entrar na conferência. A *applet* Java de *P*, por sua vez, ao receber a nova autorização para entrar na conferência transmitirá um novo ACK_P .

Se *P* for admitido na conferência, pedir a posse da palavra e receber de *M* uma nova permissão para entrar na conferência, sua *applet* Java retransmite ACK_P e, já que não recebeu o ACK_M do pedido de posse da palavra, sua indicação permanece *normal*.

Se *M* receber um pedido de posse da palavra de *P*, sendo *pedindoEntrar* a indicação de *P* na interface homem-máquina de *M*, a *applet* Java de *M* ignora o pedido, por implicar em uma transição de indicações inválida e espera receber ACK_P .

C.2.4 Moderador rejeitando um participante na conferência

A Figura C.15 mostra o moderador rejeitando um pedido para entrar na conferência.

Figura C.15 – Moderador rejeitando um participante na conferência.

Quando *M* rejeita a entrada de *P* na conferência, ao receber ACK_{MCU} a indicação de *P* na sua interface homem-máquina é alterada. Não se pode esperar por ACK_P para realizar a mudança de indicação, porque se *P* não for admitido na conferência, resolver abandoná-la e ACK_P não for recebido por *M*, a indicação de *P* na interface homem-máquina de *M* não seria alterada, ficando permanentemente como *pedindoEntrar* até o final da conferência.

Quando a *MCU* recebe de *M* a negação do pedido de *P* para entrar na conferência, ela encaminha para *P* a negação do pedido e a seguir apaga as informações referentes a *P* da sua estrutura de dados de participantes.

Se *P* não receber a negação do pedido para entrar na conferência, provavelmente o usuário pedirá novamente, voltando ao ponto inicial.

C.2.5 Moderador expulsando um participante da conferência

A Figura C.16 mostra o moderador expulsando um participante da conferência.

Figura C.16 – Moderador expulsando um participante da conferência.

Quando *M* expulsa *P* da conferência, ele só precisa esperar receber o ACK_{MCU} , semelhantemente ao que ocorre quando *M* não deixa *P* entrar na conferência. A diferença, no entanto, é que a *MCU* não apaga as informações de *P* da sua estrutura de dados de participantes, mas coloca uma indicação de que *P* foi expulso da conferência. Dessa forma, se *P* tentar pedir novamente para entrar na conferência, a *MCU* saberá que ele foi expulso da conferência e não encaminhará seus novos pedidos para entrar na conferência para *M*, a menos que *M* anistie *P* explicitamente.

C.2.6 Moderador expulsando o participante da conferência com a posse da palavra

A Figura C.17 mostra o moderador expulsando o participante da conferência com a posse da palavra.

Figura C.17 – Moderador expulsando um participante que estava com a posse da palavra.

Quando *M* expulsa o participante com a posse da palavra, há uma concessão da posse da palavra implícita para *M*. A *MCU* sempre tem o conhecimento de qual participante está com a posse da palavra, então, quando ela recebe a mensagem de expulsão de *P*, se *P* estiver com a posse da palavra, ela encaminha a mensagem de expulsão de *P* para os *Participantes* e passa a esperar pelos pacotes RTP de áudio de *M*. Os *Participantes*, por sua vez, atualizam suas interfaces homem-máquina alterando a indicação de *P* para *expulso* e a indicação de *M* para *possePalavra*.

Quando *M* recebe *ACK_{MCU}*, ele muda sua indicação para *possePalavra* na sua interface homem-máquina e inicia o seu transmissor, enquanto que *P*, ao receber a mensagem de expulsão, atualiza sua interface homem-máquina para *expulso* e pára o seu transmissor.

C.2.7 Moderador anistiando um participante que foi expulso da conferência

Quando *M* expulsa *P* da conferência, a *MCU* coloca um veto em *P*, não encaminhando mais seus pacotes para *M*, nem encaminhando pacotes para ele.

Figura C.18 – Moderador anistiando um participante que foi expulso da conferência.

A única forma de *P* poder voltar para a conferência é com o reinício da sala virtual de conferência ou recebendo a anistia por parte de *M*. Quando *M* transmite a anistia para *P*, a *MCU* retira o veto de *P* e encaminha a mensagem para *P*. Quando um participante é anistiado, sua indicação passa de *expulso* para *foraConferencia*.

Há três instantes possíveis para mudar a indicação de *P* na interface homem-máquina de *M*:

- **No envio da anistia de *P*:** Se a interface homem-máquina de *M* for alterada nesse instante, *M* não tem como saber que a *MCU* recebeu a anistia e retirou o veto a *P*. Se a *MCU* não receber a mensagem da anistia, *P* continuaria incomunicável com *M* e *M* não teria como reenviar a anistia.
- **No recebimento de ACK_{MCU} :** Se a interface homem-máquina de *M* for alterada nesse instante, *M* não tem como saber se *P* recebeu a anistia. Se para *P* a sua própria indicação é *expulso*, ele não tem como pedir para entrar na conferência. Entretanto, ainda que *P* não receba a mensagem de anistia, em último caso, ele

sairá da sala virtual de conferência e ingressará nela novamente e quando ele o fizer, sua indicação será *foraConferencia*, porque quando *M* o anistiu, o próprio *M* enviou sua nova indicação para o servidor *web*.

- **No recebimento de ACK_P :** Não se deve atualizar a interface homem-máquina de *M*, porque se *P* já tiver abandonado a conferência, a indicação de *P* nunca será alterada para *M*, e *M* não enviará para o servidor *web* a nova indicação de *P*. Dessa forma, se *P* tentar reingressar na sala virtual de conferência, sua indicação ainda será *expulso* e *M* precisaria enviar uma nova mensagem anistiando-o.

Portanto, a indicação da anistia de *P* na interface homem-máquina de *M* é realizada no recebimento de ACK_{MCU} .

C.2.8 Participante abandonando a conferência

A Figura C.19 mostra um participante abandonando a conferência.

Figura C.19 – Participante abandonando a conferência.

A interface homem-máquina de P só é alterada no recebimento do ACK_{MCU} , para garantir que suas informações foram apagadas da estrutura de dados da MCU . Se o ACK_{MCU} for perdido e P reenviar a mensagem de abandono da conferência, a MCU não encontrará a entrada de P em sua estrutura de dados de participantes, mas transmite um ACK_{MCU} a partir das próprias informações contidas no pacote recebido.

Não há motivos para P esperar por ACK_M , pois ele não precisa de uma autorização de M para abandonar a conferência. Se M não tomar conhecimento que P deixou a conferência o máximo que pode acontecer é M tentar conceder a posse da palavra para P e não conseguir. O problema pode ser resolvido com o envio regular de informações de sincronismo por parte da MCU (M perceberá que P não faz mais parte da conferência e atualizará sua interface homem-máquina) ou com M realizando uma sincronização explícita com o servidor *web*.

C.2.9 Participante com a posse da palavra abandonando a conferência

A Figura C.20 mostra o participante com a posse da palavra abandona a conferência.

Figura C.20 – Participante com a posse da palavra abandonando a conferência.

Se P estiver com a posse da palavra e resolver abandonar a conferência, quando a MCU recebe o comunicado de abandono da conferência de P , ela passa a esperar pacotes RTP de áudio do moderador, porque há uma concessão implícita da posse da palavra para M .

Caso o moderador não receba a mensagem a respeito de P , o usuário perceberá que ele não está mais recebendo o áudio de P e pode tomar de volta a posse da palavra. Poderia-se alterar a MCU , fazendo-a explicitar que a posse da palavra está com M , transmitindo para os *Participantes* e para M uma mensagem de concessão de posse da palavra para M . Nesse caso, M teria que interpretar a mensagem recebida de concessão de posse da palavra vinda da MCU como sendo a explicitação do ocorrido. Uma solução mais razoável para explicitar que M está com a posse da palavra seria a MCU transmitindo para todos uma mensagem de sincronismo com essa informação.

C.2.10 Moderador abandonando a conferência

A Figura C.21 mostra o moderador abandonando a conferência.

Figura C.21 – Moderador abandonando a conferência.

Quando M abandona a conferência ela é encerrada, mas a sala virtual não é fechada. Quando a MCU recebe a mensagem de abandono de conferência de M , ela transmite o ACK_{MCU} e encaminha a mensagem de abandono para todos os *Participantes*, que automaticamente abandonam a conferência. Depois de transmitir essas mensagens, a MCU apaga as informações da sua estrutura de dados.

Há dois instantes possíveis para M alterar a sua interface homem-máquina:

- **No envio da mensagem de abandono de conferência:** Se M alterar sua interface homem-máquina nesse instante, não há como garantir que a MCU recebeu sua mensagem de abandono. Se a MCU não recebeu a mensagem de abandono da conferência de M e M voltar a pedir para entrar na conferência, ela precisa entender que M saiu da conferência e está novamente pedindo para entrar na conferência. Dessa forma, ela o admite na conferência, transmite para os *Participantes* em sua estrutura de dados o abandono de M e em seguida limpa sua estrutura de dados, mantendo somente as informações de M .
- **No recebimento do ACK_{MCU} :** Se M esperar o recebimento de ACK_{MCU} para mudar sua indicação e ACK_{MCU} se perde, a MCU já apagou a sua estrutura de dados de participantes. Se a ela receber um novo pedido de abandono de conferência de M , a MCU não encontrará a entrada referente a M na sua estrutura de dados de participantes, mas consegue enviar o ACK_{MCU} a partir das próprias informações contidas no pacote recebido.

Os dois instantes possíveis para se alterar a interface homem-máquina de M possuem mais desvantagens do que vantagens. Escolheu-se esperar pelo recebimento do ACK_{MCU} e tratar na MCU a situação em que ela está com a sua estrutura de dados de participantes vazia, porque se espera que a perda do ACK_{MCU} seja a exceção, não a regra e porque ela assegura melhor a consistência das indicações.

Em último caso, se a MCU não receber a mensagem de abandono de conferência de M e não aceitar o novo pedido de M para entrar na conferência ou apresentar qualquer tipo de problema, há a possibilidade de fechar a sala no *site* de

gerenciamento e iniciá-la novamente, acarretando no encerramento e posterior iniciação da *MCU*.

C.2.11 Moderador tentando eleger um participante como o novo moderador da conferência

A Figura C.22 mostra o moderador tentando eleger um participante da conferência como novo moderador.

Figura C.22 – Moderador tentando eleger um participante como o novo moderador da conferência.

Quando *M* tenta eleger *P* como novo moderador da conferência, ele marca *P* como um candidato a novo moderador. O mesmo faz a *MCU* quando recebe a mensagem perguntando se *P* deseja ser o novo moderador. A *MCU* não encaminha essa mensagem para todos os *Participantes*, somente para *P*. Quando *P* recebe a

mensagem, uma janela é aberta na sua interface homem-máquina perguntando se ele deseja ser o novo moderador. Quando M recebe o ACK_P , aparece uma janela na interface homem-máquina de M avisando que P recebeu a mensagem.

Se M não receber o ACK_P até um determinado tempo, uma janela é aberta na interface homem-máquina de M avisando que P não recebeu a mensagem, ainda que P a tenha recebido. A Figura C.23 ilustra essa situação. Os *Participantes* não são informados da tentativa de eleger P como novo moderador.

Figura C.23 – Moderador tentando eleger um participante como o novo moderador da conferencia, mas não recebe a confirmação de recebimento do participante

Se M não desejar reenviar o convite, M desmarca P como candidato a moderador, mas P continua sendo o candidato a moderador para a MCU , até que uma nova tentativa de eleição de moderador seja feita. Se P aceitou ser o novo moderador e

recebe um novo convite, ele é ignorado. Se P não aceitou o convite e recebe mais uma mensagem, uma nova janela é mostrada convidando-o a tornar-se o novo moderador. Se P ainda não respondeu ao convite, a mesma janela é mantida aberta.

C.2.12 Participante aceitando ser o novo moderador da conferência

A Figura C.24 mostra um participante aceitando ser o novo moderador da sala.

Figura C.24 – Participante aceitando ser o novo moderador da conferência.

A MCU só aceita a mensagem de P aceitando ser o novo moderador, se ela o reconhecer como candidato a novo moderador, isto é, se P recebeu de M um convite para ser o novo moderador. Assim que a MCU recebe mensagem de P aceitando o cargo, ela assume que ele é o novo moderador. Quando P recebe o ACK_{MCU} , sua *applet* Java e sua interface homem-máquina são alteradas de modo a refletir seu novo tipo de usuário. A MCU encaminha para M e para os *Participantes* a mensagem que P aceitou ser o novo moderador. Se o ACK_{MCU} for perdido e P não ficar sabendo que

é o novo moderador, quando ele enviar uma mensagem de controle qualquer como participante comum, a *MCU* transmitiria para ele novamente o ACK_{MCU} .

Se *M* não recebeu a mensagem de *P* aceitando ser o novo moderador e mandar qualquer outra mensagem ainda como moderador, a *MCU* informa-o que *P* aceitou ser o novo moderador. Se *M* receber a mensagem de *P*, uma janela na sua interface homem-máquina informa-o que *P* é o novo moderador. A interface homem-máquina e *applet* Java de *M* são alteradas para comportarem-se como um participante comum.

Pode-se resolver o problema de dois ou mais participantes pensarem ser o moderador da conferência através do envio de mensagens de sincronismo explícito para todos os participantes pela *MCU* informando quem é o verdadeiro moderador da sala.

C.2.13 Participante não aceitando ser o novo moderador da conferência

A Figura C.25 mostra um participante rejeitando ser o novo moderador da sala.

Figura C.25 – Participante não aceitando ser o novo moderador da conferência.

Quando P não aceita ser o novo moderador, sua *applet* Java e interface homem-máquina se desmarcam como candidato a novo moderador da conferência. O mesmo fazem a MCU e o M quando recebem a mensagem informando a recusa. Se M não receber a mensagem de P , provavelmente seu usuário irá refazer o convite para P ser o novo moderador, voltando à situação inicial.

C.2.14 Moderador com problemas de comunicação com a unidade de controle multiponto

Quando a MCU e um participante qualquer ficam um certo tempo sem receber informações um do outro, a interface homem-máquina do participante reflete essa situação alterando a indicação do participante para *semInformacao*, enquanto que a MCU informa aos demais participantes através de um pacote de sincronismo que ela está com problemas para se comunicar com o participante. Quando esse participante é o moderador, a situação é mais grave, porque a MCU não realiza controle de posse da palavra autônomo e sendo assim, todo andamento da conferência é interrompido: ninguém consegue entrar na conferência, pedir a posse da palavra ou realizar qualquer outra ação.

Essa situação decorre da própria arquitetura do sistema. Uma solução, que não foi implementada na versão atual do sistema, seria justamente o controle de posse da palavra e de sessão autônomos em situações críticas, ou então, eleger provisoriamente um novo moderador até que o moderador original tenha o seu sinal restabelecido. Na versão atual do sistema, se M não restabelecer a comunicação com a unidade de controle multiponto, a conferência é encerrada por ela.

Quando o participante fica com a indicação *semInformacao*, ele passa a transmitir periodicamente uma mensagem contendo um “sinal de vida”. Quando a MCU recebe o sinal de vida de M , ela responde um ACK_{MCU} , que quando recebido por M , provoca a mudança da sua indicação para *normal* na sua interface homem-máquina. A MCU

também encaminha o sinal de vida de *M* para os demais *Participantes*, a fim de que eles também atualizem suas interfaces homem-máquina.

A Figura C.26 mostra o moderador restabelecendo a comunicação com a unidade de controle multiponto.

Figura C.26 – Moderador restabelecendo a comunicação com a unidade de controle multiponto.

Se a *MCU* ou o participante recebe qualquer pacote um do outro, havendo problemas de comunicação, eles reiniciam seus *timers* de conexão, mas não necessariamente o outro reinicia o seu *timer*. Por isso, mesmo que a *MCU* não esteja com problemas para receber pacotes de *M*, por exemplo, se ela receber um sinal de vida de *M*, ela responderá com o ACK_{MCU} .

A Figura C.27 mostra o que ocorre quando o moderador não consegue restabelecer a comunicação com a unidade de controle multiponto.

Quando *M* perde a comunicação com a *MCU*, é iniciado o *timer* de perda de conexão. Se a conexão não for restabelecida antes do fim desse *timer*, *M* abandona a conferência. A *MCU* também possui um *timer* de conexão e se não receber um sinal de vida de *M* antes do fim desse *timer*, ela encerra a conferência, enviando para todos uma mensagem de abandono de conferência de *M*.

Figura C.27 – Moderador não conseguindo restabelecer comunicação com a unidade de controle multiponto.

Em seguida, a *MCU* apaga as informações da sua estrutura de dados de participantes, mas não fecha a sala, deixando-a pronta para o início de uma nova conferência.

C.2.15 Participante com problemas de comunicação com a unidade de controle multiponto

A situação onde um participante comum enfrenta problemas de comunicação com a *MCU* só é crítica, se ele estiver com a posse da palavra. O tratamento dessa situação é semelhante ao caso onde o participante com a posse da palavra abandona a conferência: a posse da palavra é passada implicitamente para *M*.

A Figura C.28 mostra um participante com problemas de comunicação com a *MCU* restabelecendo a comunicação com ela. Se *P* restabelecer sua comunicação com a *MCU*, sua indicação passa para *normal* e *P*. A Figura C.29 mostra o que ocorre quando *P* não consegue restabelecer a comunicação com a *MCU*.

Figura C.28 – Participante restabelecendo a comunicação com a unidade de controle multiponto.

Figura C.29 – Participante não conseguindo restabelecer a comunicação com a unidade de controle multiponto.

Se *P* não restabelecer sua comunicação com a *MCU*, ele abandona a conferência e a *MCU*, por sua vez, transmite para todos os demais participantes que *P* abandonou a conferência e apaga as informações de *P* de sua estrutura de dados de participantes.

LISTA DE REFERÊNCIAS

ADAPTATIVE DIGITAL TECHNOLOGIES INC. Conshohocken, Pennsylvania, Estados Unidos. Empresa desenvolvedora de *codecs* e soluções de padrões para DSPs baseadas em padrões abertos. Disponível em: <<http://www.adt-inc.com/>>. Acesso em: 27 nov. 2002.

AGILENT Advisor LAN, versão 15.0.0.1000. Agilent Technology, Inc., 2002. Conjunto de programas. Disponível em: <http://xpi.comms.agilent.com/bv/J1955A_download.asp>. Acesso em: 22 out. 2003.

ALLEN, C.; DIERKS, T. *The TLS Protocol Version 1.0*. RFC 2246, **IETF Network Working Group**. Jan. 1999. Disponível em: <<http://www.ietf.org/rfc/rfc2246.txt>>. Acesso em: 26 nov. 2002.

ANTUNES, P.; GUIMARÃES, N. *Multiuser Interface Design in CSCW Systems*. **BROADCAST Year 2 Deliverable Reports – Subtask C2: Computer Supported Cooperative Working**, 1995. Disponível em: <<http://www.twente.research.ec.org/broadcast/trs/year2-deliv.html>>. Acesso em: 11.08.2003.

ARMSTRONG, S.; FREIER, A.; MARZULLO, K. *Multicast Transport Protocol*. RFC 1301, **IETF Network Working Group**. Fev. 1992. Disponível em: <<http://www.ietf.org/rfc/rfc1301.txt>>. Acesso em: 26 nov. 2002.

BERNERS-LEE, T. et al. *Uniform Resource Identifiers (URI): Generic Syntax*. RFC 2396, **IETF Network Working Group**. Ago. 1998. Disponível em: <<http://www.ietf.org/rfc/rfc2396.txt>>. Acesso em: 12 dez. 2002.

BLAKE, S. et al. *An Architecture for Differentiated Services*. RFC 2475, **IETF Network Working Group**. Dez. 1998. Disponível em:
<<http://www.ietf.org/rfc/rfc2475.txt>>. Acesso em: 12 dez. 2002.

BRADEN, R. (Ed.) et al. *Resource ReSerVation Protocol (RSVP) – Version 1 Functional Specification*. RFC 2205, **IETF Network Working Group**. Set. 1997. Disponível em: <<http://www.ietf.org/rfc/rfc2205.txt>>. Acesso em: 25 nov. 2002.

BRANDY, P. *A technique for investigating on/off patterns of speech*. **Bell Labs Tech Journal**, jan. 44(1), p. 1-22, 1965.

BRAUDES, R.; ZABELE, S. *Requirements for Multicast Protocols*. RFC 1458, **IETF Network Working Group**. Maio 1993. Disponível em:
<<http://www.ietf.org/rfc/rfc1458.txt>>. Acesso em: 26 nov. 2002.

CHURCHILL, E.; SNOWDON, D. *Collaborative virtual environments: An introductory review of issues and systems*. **Virtual Reality**, 3(1):3–15, 1998.

CISCO SYSTEMS, INC. **Quality of Service Networking**. Jun. 1999. Disponível em: <http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/qos.htm>. Acesso em: 29 nov. 2002.

CISCO SYSTEMS, INC. *Cisco 2514 router*. Disponível em:
<http://www.cisco.com/en/US/products/hw/routers/ps233/products_maintenance_guide_chapter09186a008014b47b.html> . Acesso em: 22 out. 2003.

CROWLEY, T.; MILAZZO, P.; BAKER, E.; FORSDICK, H.; TOMLINSON, R.
MMConf: An infrastructure for building shared multimedia applications.
Proceedings CSCW'90, out., p. 637-50, 1990.

CURSOS ON LARC (COL). São Paulo. Ferramenta de ensino a distância do
 Laboratório de Arquitetura e Redes de computadores (LARC). Disponível em:
 <<http://col.larc.usp.br/>>. Acesso em: 22 out. 2003.

DAIGLE, L. (Ed.). *IAB Considerations for UNilateral Self-Address Fixing (UNSAF)*
Across Network Address Translation. RFC 3424, **IETF Network Working Group**.
 Nov. 2002. Disponível em: <<http://www.ietf.org/rfc/rfc3424.txt>>. Acesso em: 22 out.
 2003.

DEERING, S. *Host Extensions for IP Multicasting*. RFC 1112, **IETF Network**
Working Group. Ago. 1989. Disponível em: <<http://www.ietf.org/rfc/rfc1112.txt>>.
 Acesso em: 22 out. 2003.

DOMMEL, H.-P.; GARCIA-LUNA-ACEVES, J. J. *Design Issues for Floor Control*
Protocols. **Proceedings of SPIE Multimedia and Networking**, fev., p 305-16,
 1995.

____. *Floor Control for Multimedia Conferencing and Collaboration*. **Multimedia**
Systems, vol. 5, no. 1, p. 23-38, 1997.

EUROPEAN TELECOMMUNICATIONS STANDARDS INSTITUTE (ETSI).
Digital cellular telecommunications system (Phase 2+) (GSM); Full rate speech;
Transcoding (GSM 06.10 version 7.1.0 Release 1998). Sophia Antipolis, França,
 1998. Padrão europeu ETSI TS 100 961 V7.1.0 (2000-07) da série de
 telecomunicações.

FENNER, W. *Internet Group Management Protocol, Version 3*. RFC 3376, **IETF Network Working Group**. Out. 2002. Disponível em:
<<http://www.ietf.org/rfc/rfc3376.txt>>. Acesso em: 27 nov. 2002.

FIELDING, R. et al. *Hypertext Transfer Protocol – HTTP/1.1*. RFC 2616, **IETF Network Working Group**. Jun. 1999. Disponível em:
<<http://www.ietf.org/rfc/rfc2616.txt>>. Acesso em: 26 nov. 2002.

FREIER, A.; P. KARLTON, P.; KOCHER, P. *The SSL 3.0 Protocol*. **Netscape Communications Corp**, nov. 1996. Disponível em:
<<http://wp.netscape.com/eng/ssl3/draft302.txt>>. Acesso em: 22 out. 2003.

HANDLEY, M. et al. *SIP: Session Initiation Protocol*. RFC 2543, **IETF Network Working Group**. Mar. 1999. Disponível em: <<http://www.ietf.org/rfc/rfc2543.txt>>. Acesso em: 26 nov. 2002.

____. *The Reliable Multicast Design Space for Bulk Data Transfer*. RFC 2887, **IETF Network Working Group**. Ago. 2000. Disponível em:
<<http://www.ietf.org/rfc/rfc2887.txt>>. Acesso em: 26 nov. 2002.

HAYNE. S.; PENDERGAST, M.; GREENBERG, S. *Implementing gesturing with cursors in group support systems*. **Journal of Management Information Systems**, Winter 10(3), p. 43-61, 1993/94.

HOLDREGE, M.; SRISURESH, P. *IP Network Address Translator (NAT) Terminology and Considerations*. RFC 2663, **IETF Network Working Group**. Ago. 1999. Disponível em: <<http://www.ietf.org/rfc/rfc2663.txt>>. Acesso em: 20 out. 2003.

____. *Protocol Complications with the IP Network Address Translator*. RFC 3027, **IETF Network Working Group**. Jan. 2001. Disponível em: <http://www.ietf.org/rfc/rfc3027.txt>. Acesso em: 20 out. 2003.

INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS. **Media Access Control (MAC) Bridges**. Estados Unidos, Jul. 1998. Padrão IEEE 802.1D. O padrão IEEE 802.1p, *Traffic Class Expediting and Dynamic Multicast Filtering*, está contido no padrão IEEE 802.1D. Disponível em: <http://grouper.ieee.org/groups/802/1/index.html>. Acesso em: 26 nov. 2002.

INTERNATIONAL TELECOMMUNICATIONS UNION
TELECOMMUNICATION STANDARDIZATION SECTOR (ITU-T). Genebra, Suíça. Setor de padronização de telecomunicações da ITU. Produz documentos com *status* de recomendações, podendo virar padrões da área de telecomunicações. Disponível em: <http://www.itu.int/ITU-T/>. Acesso em: 26 nov. 2002.

____. **40, 32, 24, 16 kbit/s Adaptive Differential Pulse Code Modulation (ADPCM)**. ITU-T G.726. Genebra, 1990.

____. **5-, 4-, 3- and 2-bits sample embedded adaptive differential pulse code modulation (ADPCM)**. ITU-T G.727. Genebra, 1990.

____. **7 kHz audio-coding within 64 kbit/s**. ITU-T G.722. Genebra, 1988.

____. **A comfort noise payload definition for ITU-T G.711 use in packet-based multimedia communication systems**. Apêndice II, ITU-T G.711. Genebra, 2000.

____. **A digital modem and analogue modem pair for use on the Public Switched Telephone Network (PSTN) at data signalling rates of up to 56 000 bit/s downstream and up to 33 600 bit/s upstream.** ITU-T V.90. Geneva, 1998.

____. **C source code and test vectors for implementation verification of the algorithm of the G.729 silence compression scheme.** Anexo B, ITU-T G.729. Geneva, 1997.

____. **Coding of speech at 16 kbit/s using low-delay code excited linear prediction.** ITU-T G.728. Geneva, 1992.

____. **Coding of speech at 8 kbit/s using Conjugate Structure Algebraic-Code-Excited Linear-Prediction (CS-ACELP).** ITU-T G.729. Geneva, 1996.

____. **Digital network echo cancellers.** ITU-T G.168. Geneva, 2002.

____. **Echo cancellers.** ITU-T G.165. Geneva, 1993.

____. **Information technology – Abstract Syntax Notation One (ASN.1): Specification of basic notation.** ITU-T X.680. Geneva, 2002.

____. **Information technology – ASN.1 encoding rules - Specification of packed encoding rules (PER).** ITU-T X.691. Geneva, 2002.

____. **Methods for subjective determination of transmission quality.** ITU-T P.800. Geneva, 1996.

____. **One-way transmission time.** ITU-T G.114. Geneva, 2000.

____. **Packet-based multimedia communications systems.** ITU-T H.323 (versão 5). Genebra, 2003.

____. **Objective quality measurement of telephone-band (300-3400 Hz) speech codecs.** ITU-T P.861. Genebra, 1998.

____. **Perceptual evaluation of speech quality (PESQ), an objective method for end-to-end speech quality assessment of narrowband telephone networks and speech codecs.** ITU-T P.862. Genebra, 2001.

____. **Pulse Code Modulation (PCM) of voice frequencies.** ITU-T G.711. Genebra, 1988.

____. **Speech coders: Dual rate speech coder for multimedia communications transmitting at 5.3 and 6.3 kbit/s.** ITU-T G.723.1. Genebra, 1996.

____. **Test signals.** Apêndice I, ITU-T P.50. Genebra, 1998.

____. **Visual telephone systems and equipment for local area networks which provide a non guaranteed quality of service.** ITU-T H.323 (versão 1). Genebra, 1996.

INTERNET ASSIGNED NUMBERS AUTHORITY (IANA). Entidade responsável pela administração da Internet. Suas principais tarefas são alocação e definição de endereços IP, associação de portas TCP e UDP a protocolos, definição de parâmetros de protocolos, serviços de nomes de domínios e de sufixos. Disponível em: <<http://www.iana.org/>>. Acesso em: 22 out. 2003.

____. **Application for Multicast Address**. Ago. 2000. Disponível em:
<<http://www.iana.org/cgi-bin/multicast.pl>>. Acesso em: 27 nov. 2002.

____. **Internet Protocol Version 4 Address Space**. Out. 2002. Disponível em:
<<http://www.iana.org/assignments/ipv4-address-space>>. Acesso em: 27 nov. 2002.

INTERNET ENGINEERING TASK FORCE (IETF). Força tarefa internacional aberta, formada por pesquisadores, fabricantes e profissionais da área de redes, comprometidos com a evolução e correto funcionamento da arquitetura da Internet. Disponível em: <<http://www.ietf.org>>. Acesso em: 26 nov. 2002.

INTERNET ENGINEERING TASK FORCE ACTIVE WORKING GROUPS (IETFAWG). Grupos de trabalhos da IETF especializados em áreas específicas, como áreas relacionadas a segurança de redes e a transporte de pacotes. Disponível em: <<http://www.ietf.org/html.charters/wg-dir.html>>. Acesso em: 26 nov. 2002.

KERMODE, R.; VICISANO, L. *Author Guidelines for Reliable Multicast Transport (RMT) Building Blocks and Protocol Instantiation documents*. RFC 3269, **IETF Network Working Group**. Abr. 2002. Disponível em:
<<http://www.ietf.org/rfc/rfc3269.txt>>. Acesso em: 26 nov. 2002.

KIVILUOTO, A. **Speech Coding Standards**. Helsinki, Finlândia. Notas de aula, Tik-111.590 Research Seminar on Digital Media, Spring 2002: Multimedia Communications (3 cr.), Helsinki University of Technology. Disponível em:
<<http://www.tml.hut.fi/Opinnot/Tik-111.590/2002/chapter3.pdf>>. Acesso em: 02 dez. 2002.

LABORATÓRIO DE ARQUITETURA E REDES DE COMPUTADORES (LARC).
São Paulo, Universidade de São Paulo, Escola Politécnica. Disponível em:
<<http://www.larc.usp.br>>. Acesso em: 22 out. 2003.

LUTHI, P. *RTP Payload Format for ITU-T Recommendation G.722.1*. RFC 3047,
IETF Network Working Group. Jan. 2001. Disponível em:
<<http://www.ietf.org/rfc/rfc3047.txt>>. Acesso em: 27 nov. 2002.

MALKIN, G. *Internet User's Glossary*. RFC 1983, **IETF Network Working Group**. Jun. 1996. Disponível em: <<http://www.ietf.org/rfc/rfc1983.txt>>. Acesso em: 20 out. 2003.

MANKIN, A. et al. *IETF Criteria for Evaluating Reliable Multicast Transport and Application Protocols*. RFC 2357, **IETF Network Working Group**. Jun. 1998.
Disponível em: <<http://www.ietf.org/rfc/rfc2357.txt>>. Acesso em: 26 nov. 2002.

MICROSOFT Active Server Pages®, versão 3.0. [S.I.]: Microsoft Corporation, 1999. Disponível em: <<http://msdn.microsoft.com/library/default.asp?url=/nhp/Default.asp?contentid=28000522>> e em <<http://msdn.microsoft.com/library/default.asp?URL=/library/psdk/iisref/aspguide.htm>>. Acesso em: 29 nov. 2002.

MICROSOFT CORPORATION. **HTML and Dynamic HTML**. Disponível em:
<http://msdn.microsoft.com/library/default.asp?url=/workshop/author/dhtml/dhtml_node_entry.asp>. Acesso em: 22 out. 2003.

____. **Windows Script**. Disponível em: <<http://msdn.microsoft.com/library/default.asp?url=/nhp/Default.asp?contentid=28001169>>. Acesso em: 22 out. 2003.

MICROSOFT Internet Explorer®, versão 5.5. [S.I.]: Microsoft Corporation, 2000. Conjunto de programas. Disponível em: <<http://www.microsoft.com/windows/ie/default.asp>>. Acesso em: 02 dez. 2002.

MICROSOFT Internet Information Services®, versão 5.0. [S.I.]: Microsoft Corporation, 2000. Conjunto de programas. Disponível com o Microsoft Windows 2000 Server.

MICROSOFT SQL Server®, versão 2000. [S.I.]: Microsoft Corporation, 2000. Conjunto de programas. Disponível em: <<http://www.microsoft.com/sql/>>. Acesso em: 22 out. 2003.

MICROSOFT Windows® 2000 Server. [S.I.]: Microsoft Corporation, 2000. Conjunto de programas. Um CD-ROM. Disponível em: <<http://www.microsoft.com/windows2000/server/default.asp>>. Acesso em: 02 dez. 2002.

NAI Netasyst WLX, versão 1.0.003. Network Associates Technology, Inc., 2003. Conjunto de programas. Disponível em: <http://www.nai.com/us/products/sniffer/network_performance_management/netasyst_networkanalyzer_lan.htm>. Acesso em: 22 out. 2003.

NETSCAPE COMMUNICATIONS CORPORATION. **Client-Side JavaScript Reference version 1.3**. Disponível em: <<http://devedge.netscape.com/library/manuals/2000/javascript/1.3/reference/ClientReferenceJS13.pdf>>. Acesso em: 22 out. 2003.

____. **HTML Tag Reference**. Disponível em: <<http://devedge.netscape.com/library/manuals/1998/htmlguide/>>. Acesso em: 22 out. 2003.

NICHOLS, K. et al. *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*. RFC 2474, **IETF Network Working Group**. Dez. 1998. Disponível em: <<http://www.ietf.org/rfc/rfc2474.txt>>. Acesso em: 12 dez. 2002.

OPEN H323 PROJECT. **Codec Bandwidth and Latency Calculations**. Jan. 2001. Disponível em: <<http://www.openh323.org/docs/bandwidth.html>>. Acesso em: 29 nov. 2002.

PACKETIZER. *Site na Internet sobre telefonia IP, H.323, ASN.1, SDL, codecs de áudio, SS7, etc.* Disponível em: <<http://www.packetizer.com/>>. Acesso em: 29 nov. 2002.

POSTEL, J. (Ed.). *Internet Protocol – DARPA Internet Program Protocol Specification*. RFC 791, **IETF**. Set. 1981. Disponível em: <<http://www.ietf.org/rfc/rfc791.txt>>. Acesso em: 26 nov. 2002.

____. *Internet Control Message Protocol – DARPA Internet Program Protocol Specification*. RFC 792, **IETF**. Set. 1981. Disponível em: <<http://www.ietf.org/rfc/rfc792.txt>>. Acesso em: 26 nov. 2002.

____. *Transmission Control Protocol – DARPA Internet Program Protocol Specification*. RFC 793, **IETF**. Set. 1981. Disponível em: <<http://www.ietf.org/rfc/rfc793.txt>>. Acesso em: 26 nov. 2002.

____. *User Datagram Protocol*. RFC 768, **IETF**. Ago. 1980. Disponível em: <<http://www.ietf.org/rfc/rfc768.txt>>. Acesso em: 26 nov. 2002.

PROXIM CORP. *ORiNOCO BG-2000 Broadband Gateway*. Disponível em: <<http://www.proxim.com/products/wifi/ap/bg2000/index.html>>. Acesso em: 22 out. 2003.

PSYTECHNICS LIMITED. **PAMS**. Disponível em: <<http://www.psytechnics.com/pages/products/pams.php>>. Acesso em: 07 jan. 2004.

QIU, R.; KUHNS, F.; COX, J. *A Conference Control Protocol for Highly Interactive Video-conferencing*. In: **Proceedings of GLOBECOM 2002**. Taipei, Taiwan, 2002. **Anais eletrônicos**. Disponível em: <<http://www.arl.wustl.edu/Publications/2000-04/globecom02qkc.pdf>>. Acesso em: 20 out. 2003.

RADCOM VOICE OVER IP TECHNOLOGY PROTOCOL REFERENCE. Tel-Aviv, Israel. RADCOM Academy/Protocols.com. Pôster sobre voz sobre IP, RA-PVoIP v.2.0. Disponível em: <<http://www.protocols.com/Archive/posters/posvoip.pdf>>. Acesso em: 10 dez. 2002.

REKHTER, Y. et al. *Address Allocation for Private Internets*. RFC 1918, **IETF Network Working Group**. Fev. 1996. Disponível em: <<http://www.ietf.org/rfc/rfc1918.txt>>. Acesso em: 22 out. 2003.

RESCORLA, E. *HTTP Over TLS*. RFC 2818, **IETF Network Working Group**. Maio 2000. Disponível em: <<http://www.ietf.org/rfc/rfc2818.txt>>. Acesso em: 22 out. 2003.

ROSENBERG, J. et al. *SIP: Session Initiation Protocol*. RFC 3261, **IETF Network Working Group**. Jun. 2002. Disponível em: <<http://www.ietf.org/rfc/rfc3261.txt>>. Acesso em: 25 nov. 2002.

ROSENBERG, J.; SCHULZRINNE, H. *Models for Multi Party Conferencing in SIP*. Internet Draft draft-ietf-sipping-conferencing-models-01.txt, **IETF SIPPING Working Group**. Jul. 2002. Disponível em: <<http://www.ietf.org/internet-drafts/draft-ietf-sipping-conferencing-models-01.txt>>. Acesso em: 26 nov. 2002.
Data de expiração: jan. 2003. Trabalho em andamento.

SCHULZRINNE, H. et al. *RTP: A Transport Protocol for Real-Time Applications*. RFC 1889, **IETF Audio-Video Transport Working Group**. Jan. 1996. Disponível em: <<http://www.ietf.org/rfc/rfc1889.txt>>. Acesso em: 25 nov. 2002.

SCHULZRINNE, H. *RTP Profile for Audio and Video Conferences with Minimal Control*. RFC 1890, **IETF Audio-Video Transport Working Group**. Jan. 1996. Disponível em: <<http://www.ietf.org/rfc/rfc1890.txt>>. Acesso em: 25 nov. 2002.

SEIFERT, R. *Foundations of LAN Switches*. In: SEIFERT, R. **The switch book: the complete guide to LAN switching technology**. Estados Unidos: Ed. John Wiley & Sons, Inc., 2000. p 22-29.

SENIE, D. *Network Address Translator (NAT) – Friendly Application Design Guidelines*. RFC 3235, **IETF Network Working Group**. Jan. 2002. Disponível em: <<http://www.ietf.org/rfc/rfc3235.txt>>. Acesso em: 20 out. 2003.

SMC NETWORKS. *SMC7004ABR Barricade Broadband Router*. Disponível em: <<http://www.smc.com/index.cfm?sec=Products&pg=Product-Details&prod=67&site=c>>. Acesso em: 04 dez. 2003.

SMETANA, G. et al. *A Floor-Controlled Centralized Conference System for Distance Learning*. In: **Proceedings of Web-Based Education 2004 (WBE 2004)**. Innsbrück, Áustria, 2004. Disponível em:

<<http://www.iasted.com/conferences/2004/Innsbruck/wbe.htm>>. Acesso em: 18 dez. 2003.

SUN MICROSYSTEMS. Santa Clara, Califórnia. Estados Unidos. Empresa que desenvolve sistemas operacionais para estações de trabalho e servidores, aplicativos de rede, criadora da tecnologia Java. Disponível em: <<http://www.sun.com>>. Acesso em: 22 out. 2003.

____. **Java Language**. Informações sobre a linguagem Java, Java Virtual Machine, ambientes de desenvolvimento, tutoriais e programas exemplos. Disponível em: <<http://java.sun.com/j2se/>>. Acesso em: 22 out. 2003.

____. **Java Media Framework (JMF) Application Programming Interface (API) Specifications**. Interfaces de programação de aplicação e bibliotecas em linguagem Java para facilitar a implementação de aplicações de rede multimídia de tempo real. Disponível em: <<http://java.sun.com/products/java-media/jmf/>>. Acesso em: 22 out. 2003.

TERAYON COMMUNICATION SYSTEMS. *TeraPro cable modem*. Disponível em: <http://www.terayon.com/tools/static_page/view.html?phase=show&id=1070438557&tool_id=100&cat_id=8.14>. Acesso em: 04 dez. 2003.

VOCAL TECHNOLOGIES, LTD. **Audio compression**. Jan. 2002. Informações sobre *codecs* de áudio e suas principais características. Disponível em: <http://www.vocal.com/data_sheets/audio_compression.html>. Acesso em: 29 nov. 2002.

WORLD WIDE WEB CONSORTIUM (W3C). **HyperText Markup Language (HTML) Home Page**. Disponível em: <<http://www.w3.org/MarkUp/>>. Acesso em: 22 out. 2003.

____. **Extensible Markup Language (XML)**. Disponível em: <<http://www.w3.org/XML/>>. Acesso em: 22 out. 2003.

WHETTEN, B. et al. *Reliable Multicast Transport Building Blocks for One-to-Many Bulk-Data Transfer*. RFC 3048, **IETF Network Working Group**. Jan. 2001. Disponível em: <<http://www.ietf.org/rfc/rfc3048.txt>>. Acesso em: 26 nov. 2002.

ZOPF, R. *Real-time Transport Protocol (RTP) Payload for Comfort Noise (CN)*. RFC 3389, **IETF Network Working Group**. Set. 2002. Disponível em: <<http://www.ietf.org/rfc/rfc3389.txt>>. Acesso em: 26 nov. 2002.