UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

ANÁLISE COMPARATIVA ENTRE *FRAMEWORKS* DE CONFERÊNCIA PARA IMPLANTAÇÃO EM UM AMBIENTE DE UMA OPERADORA DE TELECOMUNICAÇÕES

MÁRCIO RODRIGO BORGES

ORIENTADOR: FLÁVIO ELIAS GOMES DE DEUS

DISSERTAÇÃO DE MESTRADO EM ENGENHARIA ELÉTRICA
PUBLICAÇÃO: PPGENE.DM-047/2008
BRASÍLIA/DF: FEVEREIRO – 2008

UNIVERSIDADE DE BRASÍLIA

FACULDADE DE TECNOLOGIA

DEPARTAMENTO DE ENGENHARIA ELÉTRICA

ANÁLISE COMPARATIVA ENTRE FRAMEWORKS DE CONFERÊNCIA PARA IMPLANTAÇÃO EM UM AMBIENTE DE UMA OPERADORA DE TELECOMUNICAÇÕES

MÁRCIO RODRIGO BORGES

DISSERTAÇÃO SUBMETIDA AO DEPARTAMENTO DE ENGENHARIA ELÉTRICA DA FACULDADE DE TECNOLOGIA DA UNIVERSIDADE DE BRASÍLIA COMO PARTE DOS REQUISÍTOS NECESSÁRIOS PARA A OBTENÇÃO DO GRAU DE MESTRE EM ENGENHARIA ELÉTRICA.

APROVADA POR:

_____

Prof. Flávio Elias Gomes de Deus, Doutor (ENE/FT-UnB)
(Orientador)

_____

Prof. Leonardo Guerra de Rezende Guedes, Doutor (ENE/FT-UnB)
(Examinador Interno)

_____

Prof. Getúlio Antero de Deus Júnior, Doutor (EEEC-UFG)
(Examinador Externo)

BRASÍLIA/DF, 19 DE FEVEREIRO DE 2008

FICHA CATALOGRÁFICA

BORGES, MÁRCIO RODRIGO

Análise comparativa entre frameworks de conferência para implantação em um ambiente de uma operadora de telecomunicações. [Distrito Federal] 2008.
xviii, 134p, 210 x 297 mm (ENE/FT/UnB, Mestre, Engenharia Elétrica, 2008).

Dissertação de Mestrado – Universidade de Brasília. Faculdade de Tecnologia.

Departamento de Engenharia Elétrica.

1. Conferência 2. *Framework*

3. Centralizada 4. Distribuída

I. ENE/FT/UnB II. Título (série)

REFERÊNCIA BIBLIOGRÁFICA

BORGES, M. R. (2008). Comparação entre os frameworks de conferência centralizada e distribuída no ambiente de uma operadora de telecomunicações. Dissertação de Mestrado em Engenharia Elétrica, Publicação PPGENE.DM-047/2008, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 159p.

CESSÃO DE DIREITOS

AUTOR: Márcio Rodrigo Borges.

TÍTULO: Comparação entre os frameworks de conferência centralizada e distribuída no ambiente de uma operadora de telecomunicações.

GRAU: Mestre ANO: 2008

Márcio Rodrigo Borges
SQSW 504 Bloco B Apto 504, Setor Sudoeste.
70.673-502 Brasília – DF – Brasil.

AGRADECIMENTOS

Inicialmente, gostaria de agradecer a minha esposa Laura Maranhão e a minha filha Carolina Borges, que em muitos momentos sofreram com a minha ausência, mas, com muito amor, carinho e compreensão me ajudaram a superar este desafio.

Aos meus pais, Alaor Borges e Maria Helena Sales Borges, que sempre me ensinaram o valor da educação e são exemplos de esforço e dedicação.

A todos os meus colegas de mestrado, que me escolheram como representante da turma, especialmente a André Gruzinski, Angelita Kapp, Fábio Grodzki, Loriza de Andrade, Patrícia Souza e Sebastião Boanerges.

Ao meu orientador Professor Doutor Flávio Elias Gomes de Deus pelo constante incentivo, sempre indicando a direção a ser tomada nos momentos de dúvida, pela sua contribuição, paciência e dedicação na elaboração desta dissertação.

Ao meu co-orientador da UnB Professor Roque Lambert pelas suas excelentes sugestões e contribuições, pela sua amizade e por compartilhar comigo o seu conhecimento e experiência.

Ao meu co-orientador da Brasil Telecom Mauro Fukuda primeiro pela amizade e incentivo, e depois pelo apoio e contribuições para que este objetivo fosse atingido.

Aos meus colegas Alberto Boaventura, Alexandre Castro, Orlando Ruschel e Sebastião Nascimento, pela amizade, pelo apoio e pelo conhecimento que dividiram comigo.

A todos os meus professores do curso de Mestrado.

À Brasil Telecom e à UnB, por esta oportunidade de crescimento pessoal, acadêmico e profissional.

DEDICATÓRIA

Este trabalho é dedicado a minha esposa Laura, minha filha Carolina e ao meu filho ou filha que deve nascer em setembro deste ano.

RESUMO

ANÁLISE COMPARATIVA ENTRE FRAMEWORKS DE CONFERÊNCIA PARA IMPLANTAÇÃO EM UM AMBIENTE DE UMA OPERADORA DE TELECOMUNICAÇÕES.

A evolução das redes de telecomunicações está possibilitando que a comunicação entre pessoas, usando áudio e vídeo simultaneamente, torne-se cada vez mais popular. Desta forma, a demanda por um serviço de videocomunicação com maior qualidade e mais simples de ser usado tem aumentado significativamente. Baseado nisto, os órgãos de padronização começaram a definir a evolução dos atuais sistemas de videoconferência, criando *frameworks* capazes de se integrar as novas redes e de utilizar os novos recursos proporcionados por elas.

Dentro deste contexto, este trabalho introduziu algumas das principais iniciativas dos órgãos de padronização, focando principalmente no *framework* de conferência centralizada e no *framework* de conferência distribuída. Apresentou um estudo comparativo entre os *frameworks* quanto a sua escalabilidade. Realizou uma avaliação financeira, através da criação de cenários e avaliação do valor presente líquido da implementação de cada framework. Com base no resultado destas análises foi apresentada uma proposta de evolução para a Brasil Telecom. Como resultado deste trabalho concluiu-se que, com as premissas utilizadas, em qualquer dos cenários analisados, o *framework* de conferência distribuída apresentou um melhor resultado.

ABSTRACT

COMPARATIVE ANALYSYS AMONG CONFERENCE FRAMEWORKS TO THE IMPLEMENTATION IN AN ENVIRONMENT OF A TELECOMMUNICATIONS OPERATOR.

The telecommunications network evolution is making possible that the communication among people, using audio and video simultaneously, become more and more popular. In this way, the demand for a video communication service, with larger quality and that is simpler to be used, has increased significantly. Based on this, the standards developing organizations have begun to define the evolution of the current videoconferencing systems, creating frameworks capable of been integrated to the new networks and use the new resources offered by them.

Within this context, this work firstly introduced some of the main initiatives of the standards developing organizations, focusing mainly in the centralized conference framework and in the distributed conference framework. Next, it presented a comparative study among the frameworks as for his scalability. After that, it realized a financial evaluation by the creation of sceneries and evaluation of the net present value of the implementation of each framework. Finally, based on the result of these analyses, an evolution proposal was presented to Brasil Telecom. As a result of this work, it was concluded that, with the used premises, in any of the analyzed sceneries, the framework of distributed conference presented a better result.

SUMÁRIO

LISTA DE TABELAS

LISTA DE FIGURAS

LISTA DE NOMENCLATURA E ABREVIAÇÕES

3GPP	*Third Generation Partnership Project*
ACK	*Acknowledge*
AGW	*Access Gateway*
API	*Application Program Interface*
ARJ	*Admission Reject*
ARP	*Address Resolution Protocol*
ARQ	*Admission Request*
AS	*Application Server*
B2BUA	*Back-to-Back User Agent*
BFCP	*Binary Floor Control Protocol*
BGCF	*Breakout Gateway Control Function*
BHCA	*Busy Hour Call Arrivals (or Attempts)*
CAPEX	*Capital Expenditure*
CCP	*Conference control protocol*
CDR	*Call Data Record*
CID	*Conference Identifier*
CIF	*Common Intermediate Format*
CONFIANCE	*CONFerencing IMS-enabled Architecture for Next-generation Communication Experience*
CPU	*Central Processing Unit*
CSCF	*Call Session Control Function*
DCON	*Distributed Conferencing*
DHCP	*Dynamic Host Configuration Protocol*
DNS	*Domain Name System (or Service or Server)*
DTMF	*Dual-Tone MultiFrequency*
ENUM	*Telephone Number Mapping*
ETSI	*European Telecommunications Standards Institute*
FTP	*File Transfer Protocol*
GK	*Gatekeeper*
GMT	*Greenwich Mean Time*
GRJ	*Gatekeeper Reject*

GRQ	*Gatekeeper Request*
GUP	*Generic User Profile*
GW	*Gateway*
HLR	*Home location Subscriber*
HSS	*Home Subscriber Server*
HTML	*Hyper-Text Markup Language*
HTTP	*Hypertext Transfer Protocol*
IANA	*Internet Assigned Numbers Authority*
I-CSCF	*Interrogating* CSCF
ID	*Identifier*
IETF	*Internet Engineering Task Force*
IM	*Instant Message (or Messaging)*
IMS	*IP Multimedia Subsystem*
IP	*Internet Protocol*
IRQ	*Information Request*
IRR	*Information Request Response*
ISUP	*ISDN User Part*
ITU	*International Telecommunications Union*
ITU-T	*ITU - Telecommunication standardization sector*
IVR	*Interactive Voice Response*
IWF	*Interworking Function*
LAN	*Local Area Network*
LCF	*Location Confirmation*
LDAP	*Lightweight Directory Access Protocol*
LRJ	*Location Reject*
LRQ	*Location Request*
MC	*Multipoint Controller*
MCU	*Multipoint Control Unit*
MG	*Media Gateway*
MGC	*Media Gateway Controller*
MGCF	*Media Gateway Control Function*
MP	*Multipoint Processor*
MPEG	*Moving Picture Experts Group*
MRFC	*Multimedia Resource Function Controller*

MRFP	*Multimedia Resource Function Processor*
MTBF	*Mean Time Between Failures*
MTTR	*Mean Time To Recover*
NACK	*Negative Acknowledge*
NASS	*Network Attachment Subsystem*
NGN	*Next Generation Network*
OPEX	*Operational Expenditure*
OSA	*Open Service Access*
P2P	*Peer-to-Peer*
PC	*Personal Computer*
P-CSCF	*Proxy* CSCF
PES	Subsistema de Emulação RTPC/RDSI
QCIF	*Quarter CIF*
QoS	Qualidade de Serviço
RACS	*Resource and Admission Control Subsystem*
RAF	*Repository Access Function*
RAM	*Random Access Memory*
RAS	*Registration, Admission and Status*
RDSI	Rede Digital de Serviços Integrados
RI	Rede Inteligente
RRJ	*Registration Reject*
RRQ	*Registration Request*
RTCP	*Real Time Control Protocol*
RTP	*Real Time Protocol*
RTPC	Rede de Telefonia Pública Comutada
RTSP	*Real Time Streaming Protocol*
S-CSCF	*Serving* CSCF
SCS	*Service Capability Server*
SCTP	*Stream Control Transmission Protocol*
SDP	*Session Description Protocol*
SIP	*Session Initiation Protocol*
SIPPING	*Session Initiation Proposal Investigation*
SLF	*Subscription Locator Function*
SOAP	*Simple Object Access Protocol*

SQCIF	*Sub QCIF*
SS7	Sinalização por Canal Comum No. 7
TCP	*Transport Control Protocol*
TCS	*Terminal Capability Set*
TGW	*Trunking Gateway*
TIR	Taxa Interna de Retorno
TISPAN	*Telecommunication and Internet Services and Protocols for Advanced Networking*
TLS	*Transport Layer Security*
UA	*User Agent*
UDP	*User Datagram Protocol*
UE	*User Equipment*
UPSF	*User Profile Server Function*
URI	*Universal Resource Identifier*
URJ	*Unregister Reject*
URL	*Uniform Resource Locator*
VPL	Valor Presente Líquido
VPN	*Virtual Private Network*
VoIP	*Voice over IP*
WACC	*Weighted Average Cost of Capital*
WAN	*Wide Area Network*
XCON	*Centralized Conferencing*
XML	*eXtensible Markup Language*
XMPP	*eXtensible Messaging and Presence Protocol*

1 – INTRODUÇÃO

A primeira ligação telefônica, realizada em 1876 por Alexander Graham Bell, introduziu a era das redes de voz e revolucionou a comunicação entre os seres humanos. A segunda grande revolução das comunicações globais ocorreu há 50 anos, com o advento da televisão e das redes utilizando cabos. O surgimento da Internet sinalizou um terceiro e crítico ponto de inflexão, com o tráfego de dados juntando-se aos já existentes de áudio e vídeo, elevando assim o nível de sofisticação das infra-estruturas de redes predominantes em todo o mundo.

Os fatos históricos anteriormente citados procuram mostrar momentos de transformação, não somente da tecnologia, mas principalmente, da forma dos seres humanos comunicarem-se.

Com o desenvolvimento da *World Wide Web* nos anos 90 esta comunicação atingiu níveis inimagináveis anos atrás. O explosivo crescimento de usuários da Internet, a desregulamentação dos mercados mundiais, juntamente com uma imensa transformação tecnológica, tem causado grandes mudanças nas redes de telecomunicações.

Uma destas mudanças é o crescimento da demanda por soluções que permitam a comunicação através de áudio e vídeo. Isto pode ser verificado pela observação de dois fenômenos que estão ocorrendo nos serviços de telecomunicações. O primeiro é a popularização do uso de softwares de comunicação, os quais permitem que, através do PC (Computador Pessoal) e de uma câmera *Web*, possa ser facilmente estabelecida uma videocomunicação ponto-a-ponto ou ponto-multiponto. O outro é o crescimento da demanda de grandes e médias empresas por soluções de videoconferência. Estes serviços de videoconferência prestados para empresas, além de apresentar uma qualidade de imagem cada vez maior, também oferecem uma série de serviços agregados como gravação, integração com a *Web*, requisitos de segurança, entre outros.

Atualmente, a Brasil Telecom possui diversos serviços que permitem aos clientes comunicarem-se utilizando recursos de áudio e vídeo: o TV Fone Residencial, o TV Fone Corporativo e o VoIP Fone com vídeo. Além destes, a empresa futuramente irá lançar o serviço de videocomunicação utilizando terminais móveis celulares. Estes serviços são, atualmente, controlados por equipamentos diferentes, além de possuírem diferenças em vários aspectos, tais como a arquitetura que suporta os serviços, nível de qualidade de serviço, protocolos, entre outros.

Para a Brasil Telecom esta situação é bastante desconfortável, tanto pelo ponto de vista de marketing, pois dificulta o aumento da popularização dos serviços, quanto pelo ponto de vista da operação e manutenção da rede que necessita conviver com uma série de equipamentos diferentes realizando funções semelhantes.

Para realizar uma chamada de videocomunicação, são necessários protocolos de controle e sinalização, os quais executam tarefas como: localização de clientes a serem chamados, notificação de chamada, notificação de aceite da chamada, negociação de parâmetros, início da transmissão, finalização de uma transmissão e desconexão, além de prover os serviços adicionais existentes no ambiente de telefonia convencional.

Os primeiros protocolos utilizados para estas tarefas eram proprietários, dificultando a interoperabilidade dos sistemas. Porém, passados mais de 17 anos desde que as primeiras especificações foram lançadas pelo ITU-T (*International Union Telecommunication Standardization Sector*) no início da década de 90, o mundo da videocomunicação é hoje um conjunto de padrões bem definidos.

Até alguns anos atrás, a principal forma de transmissão de imagens com uma qualidade mínima aceitável só era possível através dos equipamentos de videoconferência que seguiam a recomendação H.320 (1999) do ITU-T.

Após esta fase inicial de padronização e com o crescimento da oferta de novos circuitos de dados, foi criado um padrão para a utilização da videoconferência em redes de pacotes, mais especificamente direcionada às redes TCP/IP (*Transmission Control Protocol/ Internet Protocol*) definidas na RFC 793 do IETF *(Internet Engineering Task Force*), que é a especificação H.323 do ITU-T. Esta especificação foi criada para compatibilizar o H.320 para a utilização em redes de pacotes, utilizando o protocolo TCP/IP. Hoje o H.323 é a principal forma de utilização de videoconferência, devido ao uso massivo das redes TCP/IP nas LANs (*Local Area Network*), WANs (*Wide Area Network*) e em toda a Internet.

Com a criação do padrão SIP (*Session Initiation Protocol*), desenvolvido pelo IETF (RFC 3261), surge um conjunto de especificações e protocolos para uso na Internet e redes TCP/IP, planejado especificamente para redes baseadas em comutação de pacotes. Toda sua base é fundamentada junto às especificações para o uso na Internet, sendo assim, diferente das especificações H.323. Estes protocolos não se comunicam diretamente, mas podem co-existir e se comunicarem através de equipamentos que permitem com que dispositivos H.323 possam estabelecer conectividade com dispositivos SIP.

Estes protocolos estabeleceram suas próprias arquiteturas de rede para prestação dos serviços, porém, cada vez mais os clientes exigem simplicidade e maior integração no uso dos serviços. Isto implica em arquiteturas de rede que tenham capacidade de oferecer soluções integradas.

As arquiteturas de redes de telecomunicações estão caminhando em direção a uma estrutura convergente que engloba o tratamento unificado de todas as mídias (voz, dados e vídeo) sobre uma estrutura de transporte única. Esta estrutura é baseada em IP, tanto para acessos fixos como móveis, num ambiente integrado entre os "mundos de telecomunicações e tecnologia da informação".

A esta arquitetura capaz de prover serviços de comunicação, a qualquer cliente, em qualquer lugar, através de qualquer acesso convencionou-se chamar NGN (*Next Generation Network*).

A idéia da arquitetura NGN é definir um conjunto de equipamentos que de forma coerente suportem serviços que utilizam simultaneamente voz, dados e vídeo em uma estrutura de rede única.

Para padronizar esta arquitetura foi criado um grupo de trabalho do ETSI (*European Telecommmunications Standards Institute*) chamado TISPAN (*Telecommunication and Internet Services and Protocols for Advanced Networking*). A arquitetura definida por este grupo de trabalho é chamada TISPAN e está sendo definida como o caminho de evolução das redes das principais operadoras de telecomunicações do mundo.

A arquitetura TISPAN provê uma infra-estrutura para suportar comunicações multimídia pessoa-a-pessoa em tempo real baseadas em IP. Isto inclui a capacidade para integrar múltiplos tipos de serviços como multimídia, voz e dados, em uma única sessão ou chamada. Desta forma, a implantação desta arquitetura possibilita a integração destes serviços, permitindo ao cliente uma videocomunicação independente do tipo de acesso e de equipamento.

Dentro deste contexto é esperado que cada vez mais, a conferência torne-se um serviço sofisticado e abrangente, indo muito além de uma chamada envolvendo vários clientes. Ela deve ser aplicável a qualquer tipo de fluxo de mídia pelo qual os clientes podem querer se comunicar, não somente áudio e vídeo, mas também transferência de mensagens instantâneas, jogos, entre outros; isto é o que hoje é chamado de conferência multimídia. Uma solução de conferência tem que prover os meios para um usuário criar, administrar, terminar, entrar e sair da conferência, além de capacitar a rede com as

habilidades necessárias para entregar as informações sobre estas conferências para as partes envolvidas.

O processo de padronização associado às conferências multimídia sobre IP ainda está em um estágio inicial dentro das diferentes comunidades envolvidas. O IETF é uma comunidade internacional aberta, e interessada na evolução da arquitetura Internet e de seus protocolos. Atualmente os principais grupos de trabalho do IETF envolvidos no esforço de padronização de conferências são o SIPPING (*Session Initiation Proposal Investigation*) e o XCON (*Centralized Conferencing*).

Os esforços destes grupos estão concentrados em desenvolver um *framework* de controle para as conferências. O *framework* de controle de conferência é um conjunto de protocolos que implementam o controle de conferência e a arquitetura dos elementos de rede que fazem parte do mesmo.

Um *framework* precisa procurar o equilíbrio entre ser abrangente o suficiente para tratar a maioria dos cenários práticos e, ao mesmo tempo, não ser muito complexo para que seja amplamente aceito pelos clientes e implementado pelos fabricantes em seus equipamentos.

Como qualquer sistema, um *framework* de controle de conferência deve ser escalável, fácil de ser estendido a outro ponto, genérico, confiável e seguro. Os requisitos de escalabilidade que o *framework* de controle de conferência tem que suportar são grandes, como distribuição geográfica, número de conferências, entre outros. Além disso, ele deve ser modular para que componentes novos possam ser facilmente adicionados ou componentes existentes possam ser trocados.

O grupo de trabalho SIPPING desenvolveu em 2006 um *framework* (RFC 4353) para conferência multiponto utilizando SIP. Este *framework* define um modelo geral de arquitetura, uma terminologia e explica como o SIP é utilizado em uma conferência. O TISPAN adotou a arquitetura definida pelo SIPPING para conferência como parte do padrão TISPAN.

A meta do grupo de trabalho XCON é definir um *framework* de conferência de referência e um modelo de dados para cenários de conferência agnósticos ao protocolo de controle de chamada. O *framework* criado pelo XCON não se restringe ao protocolo SIP permitindo o uso de outros protocolos existentes no mercado, como H.323, Jabber e Q.931.

Porém, tanto o SIPPING como o XCON tratam da padronização de um framework para conferência centralizada, nenhum destes grupos trata da especificação de um *framework* de conferência distribuída. Percebendo esta lacuna na padronização um grupo

de pesquisadores da Universidade de Nápoles criou o DCON (*Distributed Conferencing*) um *framework* de conferência distribuída ou descentralizada baseado no framework desenvolvido pelo XCON com alterações que permitem a descentralização da conferência. A proposta de *framework* DCON foi submetida ao IETF e está sendo analisada pelo XCON através de uma série de documentos colocados em consulta pública.

Neste contexto, o objetivo desta dissertação é mostrar um caminho para uma operadora de telecomunicações, como a Brasil Telecom, evoluir o seu sistema atual de conferências para um sistema compatível com as novas arquiteturas e protocolos de rede que estão sendo definidos pelos órgãos de padronização.

Para atingir este objetivo, inicialmente no capítulo 2 é apresentada uma visão geral dos principais protocolos relacionados com um sistema de conferência e também os principais pontos da arquitetura TISPAN.

A seguir, no capítulo 3, são mostrados mecanismos que permitem o interfuncionamento de H.323 e SIP. Estes mecanismos permitem que clientes que usam protocolos diferentes possam participar da mesma conferência.

No capítulo 4 é introduzido o novo conceito de *framework* de conferência. Primeiro é apresentado o *framework* SIP desenvolvido pelo SIPPING. Em seguida discute-se o *framework* de conferência centralizada criado pelo XCON. Por último é introduzido o *framework* de conferência distribuída DCON.

No capítulo 5 é realizada uma comparação entre os *frameworks* XCON e DCON. As duas arquiteturas serão comparadas quanto a sua escalabilidade e será realizada uma comparação financeira, que levará em conta os investimentos e os custos necessários para a implantação de uma solução de videoconferência na Brasil Telecom. Este estudo irá utilizar uma demanda distribuída geograficamente por toda a área de atuação da Brasil Telecom.

O capítulo 6 apresenta a implementação da arquitetura definida como mais adequada para a Brasil Telecom com base nos resultados do capítulo anterior, bem como o mapeamento dos elementos do *framework* de conferência nos elementos da arquitetura TISPAN.

O Capítulo 7 apresenta as conclusões desta dissertação e sugestões de estudos que possam complementar este trabalho.

2 – PROTOCOLOS E PADRÕES RELACIONADOS COM CONFERÊNCIA E A ARQUITETURA TISPAN

Este capítulo apresentará os pontos mais relevantes dos protocolos, dos padrões e das arquiteturas relacionados com uma conferência, com a intenção de dar uma visão daquilo que atualmente é utilizado e dar sustentação teórica aos demais capítulos. Primeiramente serão apresentados os principais protocolos envolvidos no transporte IP (*Internet Protocol*), os principais padrões de codificação de vídeo e em seguida serão mostradas as características mais relevantes dos protocolos H.323 e SIP, finalizando com a descrição da arquitetura de nova geração TISPAN.

2.1 – *Transmission Control Protocol* (TCP)

O TCP é, sem dúvidas, um dos mais importantes protocolos da família TCP/IP. É um padrão definido na RFC 793 (1981) que fornece um serviço de entrega de pacotes confiável e orientado a conexão. Ser orientado a conexão significa que todos os aplicativos que usam o TCP como protocolo de transporte, antes de iniciar a troca de dados, precisam estabelecer uma conexão. Na conexão são fornecidas, normalmente, informações de validação, as quais identificam o usuário que está tentando estabelecer uma conexão. Um exemplo típico são os aplicativos de FTP (*File Transfer Protocol*).

O TCP tem como características:

- Garantir a entrega de datagramas IP: Esta talvez seja a principal função do TCP, ou seja, garantir que os pacotes sejam entregues sem alterações, sem terem sido corrompidos e na ordem certa.
- Executar a segmentação e reagrupamento de grandes blocos de dados enviados pelos programas e garantir o seqüenciamento adequado e entrega ordenada de dados segmentados: Esta característica refere-se à função de dividir grandes arquivos em pacotes menores e transmitir cada pacote separadamente. Os pacotes podem ser enviados por caminhos diferentes e chegar fora de ordem. O TCP garante que, no destino, os pacotes sejam ordenados corretamente, antes de serem entregues ao programa de destino.
- Verificar a integridade dos dados transmitidos usando cálculos de soma de verificação: O TCP faz verificações para garantir que os dados não foram alterados ou corrompidos durante o transporte entre a origem e o destino.

- Enviar mensagens positivas dependendo do recebimento bem-sucedido dos dados. Ao usar confirmações seletivas, também são enviadas confirmações negativas para os dados que não foram recebidos: No destino, o TCP recebe os pacotes, verifica se estão íntegros e, em caso afirmativo, envia uma mensagem para a origem, confirmando cada pacote que foi recebido corretamente. Caso um pacote não tenha sido recebido ou tenha sido recebido com problemas, o TCP envia uma mensagem ao computador de origem, solicitando uma retransmissão do pacote. Com esse mecanismo, apenas pacotes com problemas terão que ser reenviados, o que reduz o tráfego na rede e agiliza o envio dos pacotes.
- Oferecer um método preferencial de transporte de programas que devem usar transmissão confiável de dados baseada em sessões, como bancos de dados cliente/servidor e programas de correio eletrônico.

2.2 – User Datagram Protocol (UDP)

O UDP é um protocolo e está definido na RFC 768 (1980). O UDP é usado por alguns programas em alternativa ao TCP para o transporte rápido de dados entre hosts TCP/IP.

Porém o UDP não fornece garantia de entrega e nem verificação de dados. De uma maneira simples, o protocolo UDP manda os dados para o destino não se preocupando se eles vão chegar ou se vão chegar sem erros. Pode parecer estranho esta característica do UDP, porém em determinadas situações, o fato de o UDP ser mais rápido (por não fazer verificações e por não estabelecer sessões), recomenda-se o seu uso.

O protocolo UDP fornece um serviço de entrega de pacotes sem conexão com base no melhor esforço, ou seja, o UDP não garante a entrega ou verifica o seqüenciamento para qualquer pacote. Um computador de origem que precise de comunicação confiável deve usar TCP ou um programa que ofereça seus próprios serviços de seqüenciamento e confirmação.

O conceito de porta UDP é idêntico ao conceito de portas TCP, embora tecnicamente, existam diferenças na maneira como as portas são utilizadas em cada protocolo. A idéia é a mesma, se um usuário estiver utilizando vários programas baseados em UDP, ao mesmo tempo, no seu computador, é através do uso de portas, que o sistema operacional sabe a qual programa se destina cada pacote UDP que chega.

O lado servidor de cada programa que usa UDP escuta as mensagens que chegam no seu número de porta conhecido. Todos os números de porta de servidor UDP menores que 1.024 (e alguns números mais altos) são reservados e registrados pela *Internet Assigned Numbers Authority* (IANA, autoridade de números atribuídos da Internet). Cada porta de servidor UDP é identificada por um número de porta reservado ou conhecido.

2.3 - *Stream Control Transmission Protocol* (SCTP)

O SCTP é um protocolo de transporte de dados, estando num nível equivalente ao UDP e ao TCP, que atualmente provêem todas as funções de transporte das principais aplicações da Internet. Suas especificações estão contidas na RFC 2960 (2000).

Assim como o TCP, o SCTP provê um serviço de transporte confiável, assegurando que todos os dados das aplicações serão transportados sem erros. É um protocolo orientado a conexão, significando que um relacionamento é criado entre pontos terminais numa sessão SCTP antes que os dados sejam transmitidos. Este relacionamento é mantido até que toda a transmissão de dados seja concluída com sucesso.

Este protocolo possui determinadas funções que são consideradas críticas para o transporte de sinalização e aplicações que requerem desempenho adicional e confiabilidade. Estas funções são:

- Múltiplos Fluxos (*Multi-Streaming*) - O nome do protocolo é derivado desta função. Ela permite que os dados sejam divididos em fluxos independentes. A perda de uma mensagem afetará a transmissão apenas do fluxo a que ela está associada.
- Múltiplos Endereços (*Multi-Homing*) - Outra característica fundamental é a possibilidade de um ponto terminal ter múltiplos endereços IP. O maior benefício desta propriedade é a possibilidade de se manter uma sessão mesmo com falhas na rede. Em sessões tradicionais, a falha em uma rede local pode isolar o sistema final ou, falhas na rede principal podem causar indisponibilidade temporária até que os protocolos de roteamento contornem o problema.

Na forma atual do protocolo, esta característica é usada apenas para redundância e não para balanceamento de carga.

2.4 - Real-Time Transport Protocol (RTP)

O protocolo RTP (*Real Time Transport Protocol*), definido através da RFC 3550 (2003), é o principal protocolo utilizado pelos terminais, em conjunto com o RTCP (*Real Time Transport Control Protocol*), para o transporte fim-a-fim em tempo real de pacotes de mídia (áudio e vídeo) através de redes de pacotes. Pode fornecer serviços *multicast* (transmissão de um para muitos) ou *unicast* (transmissão de um para um).

O RTP não reserva recursos de rede e nem garante qualidade de serviço para aplicações em tempo real. O transporte dos dados é incrementado através do uso do RTCP que monitora a entrega dos dados e provê funções mínimas de controle e identificação. No caso das redes IP este protocolo utiliza o UDP, que estabelece comunicações sem conexão.

O RTP provê a entrega fim-a-fim de serviços de áudio e vídeo em tempo real. Quando H.323 é usado para transportar dados em redes baseadas sobre IP, o RTP é tipicamente usado para transportar dados via o UDP. O RTP, juntamente com o UDP, provê as funcionalidades de protocolo de transporte. O RTP fornece a identificação dos tipos de carga, a numeração seqüencial, o horário e a monitoração de entrega. O UDP provê os serviços de multiplexação e de verificação de erro.

2.4.1 - Real-Time Transport Control Protocol (RTCP)

O protocolo RTCP, definido também através da RFC 3550, é baseado no envio periódico de pacotes de controle a todos os participantes da conexão (chamada), usando o mesmo mecanismo de distribuição dos pacotes de mídia. Desta forma, com um controle mínimo é feita a transmissão de dados em tempo real usando o protocolo UDP.

O RTCP é o equivalente do RTP que provê serviços de controle. A primeira função do RTCP é permitir o controle da qualidade da distribuição dos dados. Outra função do RTCP é carregar um identificador de nível de transporte para uma fonte RTP, a qual é usada pelos recebedores para sincronizar áudio e vídeo.

2.5 – *Session Description Protocol* (SDP)

O SDP, especificado na RFC 4566 (2006), é o protocolo usado para descrever o anúncio de sessão multimídia, o convite da sessão multimídia e outras formas de iniciar

uma sessão multimídia. Para este estudo, uma sessão multimídia é definida como um conjunto de fluxos de mídia que existem durante certo tempo.

2.6 – Padrões de Codificação de Vídeo

Seguir padrões de codificação das várias mídias é fundamental para que se possa utilizar um sistema de videoconferência aberto. Nas seções a seguir serão mostrados os principais padrões de codificação de vídeo definidos pelos órgãos internacionais de padronização.

2.6.1 – H.261 e MPEG-1

O padrão de codificação de vídeo definido pela recomendação ITU-T H.261 (1993), para utilização em sistemas audiovisuais de faixa estreita, foi desenvolvido em 1990 para a transmissão de sinais digitais de vídeo sobre linhas RDSI (Rede Digital de Serviços Integrados - ITU-T H.320 (1999)). O H.261 opera em taxas múltiplas de 64 kbps, definidas entre 40 kbps e 2 Mbps e suportando quadros de vídeo com resoluções de 352x288, 176x144 ou 88x72 pixels, para 25 quadros por segundo.

O H.261 é o padrão mais simples e com menor taxa de compressão disponível, estando presente em praticamente todos os sistemas de videoconferência profissionais, desde os mais simples aos mais sofisticados. Isso permite, que um equipamento atual com uma série de novos recursos possa se conectar de forma transparente com equipamentos antigos, muitos com mais de 10 anos de uso.

Da mesma forma, o padrão MPEG-1 (*Moving Picture Experts Group*) foi desenvolvido em 1993 com o objetivo de oferecer uma qualidade aceitável de vídeo utilizando taxas de até 1,5 Mbps. Este padrão suporta quadros com varredura progressiva (não entrelaçados) com resolução de 352x240 pixels, para 30 quadros por segundo (sistema NTSC), ou 352x288 pixels, para 25 quadros por segundo (sistemas PAL e SECAM), com qualidade de imagem comparável à oferecida pelas antigas fitas VHS (*Video Home System*).

O MPEG-1 é considerado o formato de maior compatibilidade dentro da família MPEG, sendo reproduzido sem problemas pela grande maioria dos aplicativos disponíveis para computadores pessoais e aparelhos de VCD (*Video Compact Disc*) e DVD (*Digital Video Disc*). É também um elemento desse padrão o MPEG-1 Audio Layer 3, Codec para

compressão de sinais de áudio popularmente conhecido como MP3, que modificou as estruturas da indústria fonográfica mundial a partir do final da década passada, permitindo de forma simples e eficiente o oferecimento e o intercâmbio de músicas através da Internet.

2.6.2 – H.262 ou MPEG-2

Conforme as tecnologias de processamento digital de sinais se tornaram mais poderosas e baratas, dando condições para que equipamentos capazes de decodificar algoritmos complexos fossem acessíveis aos clientes residenciais, permitindo maior qualidade de vídeo, foram desenvolvidos padrões de codificação mais avançados.

Em 1994 foi criado o MPEG2, definido na recomendação ITU-T H.262 (1994) cujo principal objetivo foi a adaptação do MPEG-1 para dar suporte à HDTV (*High Definition TeleVision*), com resolução típica de 1280x720 pixels.

Esse padrão é tipicamente utilizado na codificação de sinais de áudio e vídeo para distribuição *broadcasting* (uma forma de transmissão de dados onde todos os receptores recebem a mesma informação de forma simultânea) exigindo equipamentos mais poderosos, mas alcançando maior eficiência na codificação, ou seja, oferecendo melhor qualidade por quantidade de bits utilizados na transmissão dos sinais.

O MPEG-2 é o padrão utilizado pelos DVDs, assim como nas transmissões diretas via satélite (DTH) (*Direct To Home*) utilizando a banda "Ku" das TVs por assinatura, bem como nas transmissões digitais de TV a cabo.

2.6.3 – H.263

O padrão definido pela recomendação ITU-T H.263 é um codificador de vídeo desenvolvido em 1995 como solução de compressão para baixas taxas de transmissão, inferior a 128kbps em aplicações de videoconferência.

Esse padrão foi desenvolvido como uma evolução do H.261, operando de forma otimizada em taxas inferiores àquelas utilizadas pelo mesmo, considerando também diversos aspectos dos padrões MPEG-1 e MPEG-2, que o tornam um substituto adequado para o primeiro em todas as taxas utilizadas, sobretudo em virtude das suas evoluções H.263v2/H.263+, desenvolvida em 1998, e H.263v3/H.263++, desenvolvida em 2000.

O padrão H.263 foi projetado para utilização em sistemas baseados na recomendação ITU-T H.324, para videotelefonia e videoconferência sobre redes

comutadas a circuitos. Além disso, também é amplamente utilizado nas redes baseadas na recomendação ITU-T H.323, para videoconferência em redes IP e H.320 para videoconferência em redes RDSI.

2.6.4 – H.264 ou MPEG-4

Padrão definido pela recomendação ITU-T H.264 (2003) também conhecido como AVC (*Advanced Video Coding*), que corresponde à Parte 10 do padrão MPEG-4 (2003). Este padrão teve como principal objetivo em seu desenvolvimento a capacidade de oferecer uma boa qualidade de vídeo utilizando taxas 50% inferiores às utilizadas pelos padrões anteriores, como o H.263, o MPEG-2 e o próprio MPEG-4 Parte 2. Isto deveria ser feito sem grandes incrementos de complexidade que tornassem a solução impraticável ou cara demais.

Um segundo objetivo era obter flexibilidade, permitindo que o padrão pudesse ser aplicado a uma grande variedade de aplicações, envolvendo taxas e resoluções de quadro tanto baixas como elevadas, e que operasse sobre diversas redes e sistemas, como videotelefonia comutada a circuitos, redes IP, transmissão de TV digital e armazenamento em DVDs.

Esse padrão tem como característica a elevada compressão de dados, sendo produto de um esforço conjunto entre os grupos VCEG (*Video Coding Experts Group*), patrocinado pelo ITU-T, e o MPEG (*Moving Picture Experts Group*), formando a parceria denominada JVT (*Joint Vídeo Team*), que apresentou sua primeira versão em 2003.

O padrão MPEG-4 absorveu muitas características de seus antecessores MPEG-1 MPEG- 2, incluindo novas funcionalidades como suporte a renderização (converter uma série de símbolos gráficos num arquivo visual) tridimensional, objetos VRML (*Virtual Reality Modelling Language*), suporte para a gerência digital de direitos autorais e interatividade.

Foram também desenvolvidas extensões para suporte à codificação de vídeo com fidelidade superior, denominadas FRExt (*Fidelity Range Extensions*), com maior precisão de amostragem, incluindo a codificação em 10 e 12 bits, e uma melhor resolução de *core*s, além de técnicas avançadas de processamento de sinais.

2.7 – H.323

O padrão H.323 é uma recomendação do ITU-T Grupo de estudo 16 que especifica um sistema e protocolos para comunicação multimídia sobre redes de pacotes. O H.323 permite não somente o estabelecimento e controle para chamada ponto a ponto como também para conferência multiponto.

O padrão H.323 é uma especificação "guarda-chuva" onde vários aspectos são especificados em outras recomendações do ITU-T como:

- H.225.0 (1996) para estabelecimento de conexão e transporte de mídia (RTP), acesso a recursos e tradução de endereços;
- H.245 (1998) para controle de chamada e negociação de capacidades;
- H.332 (1998) para conferências;
- H.235 (1998) para segurança;
- H.246 (1998) para interoperabilidade com a RTPC (Rede de Telefonia Pública Comutada);
- H.450.1 (1998) e H.450.3 (1997) para serviços suplementares como transferência de chamadas.

2.7.1 – Componentes do H.323

A recomendação H.323 define as seguintes entidades:

- Terminal H.323 – São os equipamentos de usuário que permitem comunicações de voz ou vídeo em tempo real com outro terminal H.323, *Gateways* ou MCUs em uma rede.
- MCU/MC/MPs – A *Multipoint Controller Units* (MCU), inclui o *Multipoint Controller* (MC) e um ou mais *Multipoint Processors* (MPs), permite o gerenciamento de conferências multiponto. As regras do MC são fundamentais para a conferência multiponto e geram os comandos para os MPs tratarem os fluxos de multimídia e distribuí-los entre os participantes.
- *Gateways* – equipamentos que permitem a intercomunicação entre as redes de comutação de pacotes, como o IP, e as redes de comutação de circuitos, como a RTPC. Eles provem mapeamento da sinalização bem como facilidades de transcodificação.

- *Gatekeeper* - é um servidor de tradução, localização e admissão, o qual provê tradução de endereços e controle de acesso à rede H.323 para terminais, *gateways* e MCUs, além de outros serviços como gerenciamento de largura de banda, localização de *gateways,* produção de bilhetes, serviços suplementares (como desvio de chamada, captura de chamada, entre outros.) e planos de numeração. Normalmente os *gatekeepers* usam as tecnologias LDAP (*Lightweight Directory Access Protocol*) e DNS (*Domain Name System*) para atingir a funcionalidade requerida.

2.7.2 – Protocolos especificados no padrão H.323

Os protocolos especificados no padrão H.323 serão detalhados na seqüência. Uma típica pilha de protocolos pode ser observada na Figura 2.1

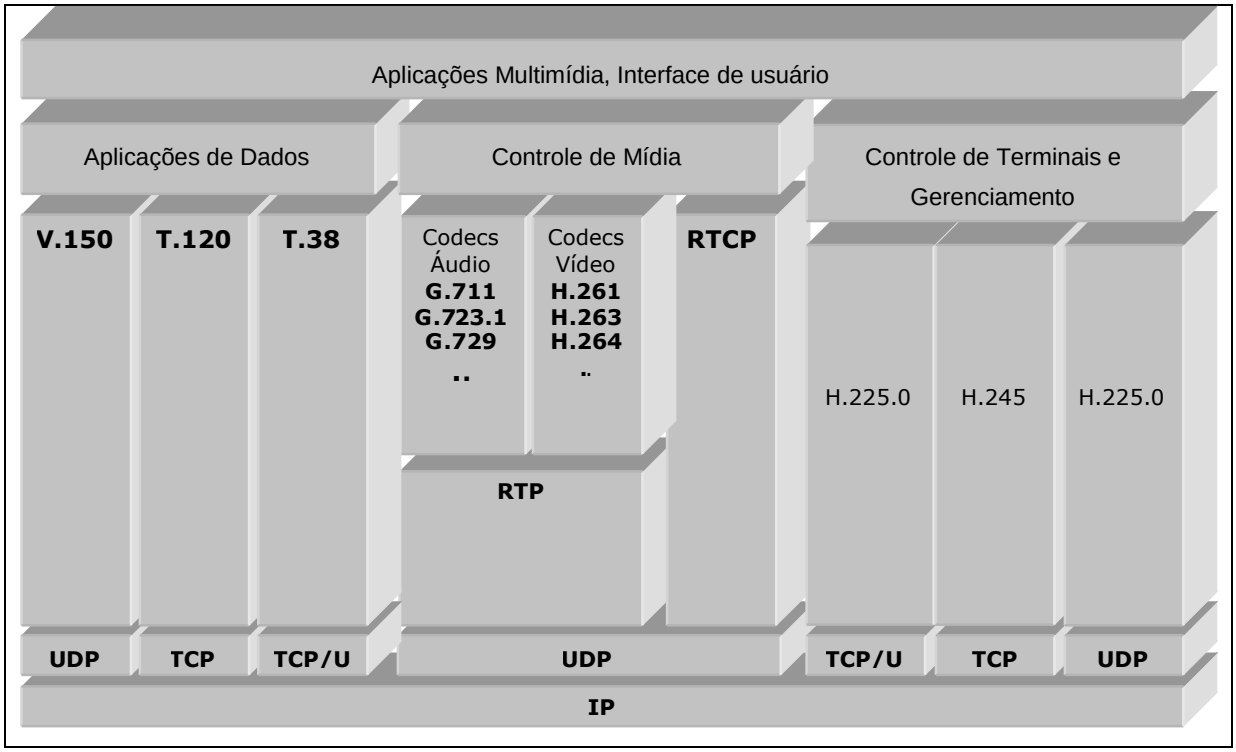


Figura 2.1 – Pilha de protocolos do H.323, adaptado de (Brasil Telecom, 2007).

2.7.2.1 - Codec de Áudio

Um codec de áudio codifica o sinal de áudio captado pelo microfone para a transmissão através do terminal H.323 do usuário A, decodifica o áudio recebido e envia para o alto-falante do terminal H.323 do usuário B. O áudio é o serviço mínimo provido

pelo padrão H.323. Desta forma, os terminais H.323 devem suportar pelo menos o codec de áudio especificado na recomendação G.711 (1998) do ITU-T. Adicionalmente, o terminal pode suportar outros codecs como o G.722 (1998), G.723.1 (1995), G.728 (1992), G.729 (1995).

2.7.2.2 - Codec de Vídeo

Um Codec de vídeo codifica o sinal de vídeo captado por uma câmera para a transmissão através do terminal H.323 do usuário A, decodifica e envia para o display do terminal H.323 do usuário B.

Como o padrão H.323 especifica o suporte a vídeo como opcional o suporte a codecs de vídeo também é opcional. Contudo, um terminal H.323 que irá prestar serviços de vídeo deve suportar pelo menos um dos codecs especificados nas recomendações do ITU-T, como o H.261, H.263 e o H.264.

2.7.2.3 - H.225.0 - Sinalização de chamadas

A sinalização de chamadas é um procedimento básico necessário para iniciar e finalizar uma chamada entre dois pontos. O H.225.0 utiliza um subconjunto do protocolo Q.931 (utilizado pela RDSI para controle de conexão) para este propósito, incorporando-o no formato das suas mensagens.

A sinalização de chamadas H.225.0 é trocada diretamente entre os pontos participantes de uma chamada quando não existe um *gatekeeper.* Quando existe um *gatekeeper*, então as mensagens podem ser roteadas através dele.

Os principais comandos e mensagens do H.225.0 são:

- *Alerting*: Mensagem de alerta para o usuário destino;
- *Call Proceeding*: Requisição de estabelecimento de chamada sendo iniciado;
- *Connect*: Chamada em andamento foi aceita pelo usuário destino;
- *Setup:* Indica que uma entidade de origem deseja iniciar uma conexão com uma entidade destino;
- *Release Complete*: Indica a liberação de uma chamada se o canal de sinalização H.225.0 (Q.931) estiver aberto;

- *Status*: Resposta a uma mensagem de sinalização desconhecida ou a uma mensagem *Status Inquiry*, fornecendo informações do estado da chamada;
- *Status Inquiry*: Requisita informação da chamada.

2.7.2.4 - H.225.0 – RAS (Registration Admission Status)

As mensagens H.225.0 RAS definem a comunicação entre terminais e o *gatekeeper*. O H.225.0 RAS é necessário apenas quando o *gatekeeper* existe. Ao contrário do H.225.0 para sinalização de chamadas e do H.245, o H.225.0 RAS utiliza transmissão não confiável de mensagens.

A comunicação H.225.0 RAS inclui a descoberta de *gatekeepers*, o registro de terminais e a localização de terminais.

Os principais comandos e mensagens do H.225.0 RAS são:

- *Registration Request*: Requisição de um terminal ou *Gateway* para se registrar em um *gatekeeper*;
- *Admission Request*: O terminal requisita o acesso à rede de pacotes ao *gatekeeper*;
- *Bandwidth Request*: O terminal requisita ao *gatekeeper* que seja feita uma alteração na alocação de banda;
- *Disengage Request*: Se esta mensagem for enviada pelo terminal para o *gatekeeper*, indica que o terminal está finalizando a chamada; se ela for enviada pelo *gatekeeper* ao terminal, força a chamada a ser finalizada;
- *InfoRequest Response*: Resposta a uma mensagem IRQ;
- RAS *Timers and Request in Progress*: Valor padrão de tempo de espera para resposta a mensagens RAS e subseqüente reenvio da mensagem se a resposta não é recebida.

2.7.2.5 - H.245 - Controle de mídia

A flexibilidade do H.323 necessita que os terminais de uma comunicação negociem determinadas configurações antes que uma conexão de áudio, vídeo e/ou dados seja estabelecida. O H.245 (1998) troca mensagens e comandos de controle durante a chamada para configurar determinados parâmetros. A implementação do controle H.245 é obrigatória em todos os terminais.

O H.245 fornece as funcionalidades de capacidade de troca, abertura e fechamento de canais lógicos e mensagens de controle de fluxo. Os principais comandos e mensagens do H.245 são:

- *Master-Slave Determination*: Determina qual terminal é o mestre e qual é o escravo;
- *Terminal Capability Set*: Contém informações sobre as capacidades de um terminal para transmitir e receber fluxos multimídia;
- *Open Logical Channel*: Abre um canal lógico para transporte de informações de dados, áudio e vídeo;
- *Close Logical Channel*: Fecha um canal lógico entre dois terminais;
- *Request Mode*: Utilizado por um receptor para requisitar modos particulares de transmissão a um transmissor;
- *Send Terminal Capability Set*: Solicita que um terminal confirme que está recebendo e transmitindo capacidades através do envio de uma ou mais mensagens *Terminal Capability Sets*;
- *End Session Command*: Indica o fim de uma sessão H.245.

2.7.3 – Configuração e finalização de chamadas H.323

A seguir serão descritos os passos envolvidos na criação de uma chamada H.323, o estabelecimento da comunicação e a liberação da chamada. Para este exemplo serão considerados dois terminais H.323 (T1 e T2) conectados a um *gatekeeper*, utilizando sinalização direta das chamadas e encapsulamento RTP para os fluxos de mídia, conforme apresentado pela Figura 2.2.

1. O terminal T1 envia uma mensagem RAS *Admission Request* no canal RAS para registro junto ao *gatekeeper*. Ele requisita o uso de um canal de sinalização direto.
2. O *Gatekeeper* confirma a admissão do terminal T1 enviando uma mensagem *Admission Confirm*. O *gatekeeper* indica nesta mensagem que o terminal T1 pode utilizar a sinalização de chamada direta.
3. O terminal T1 envia uma mensagem de sinalização H.225 para configuração da chamada para o terminal T2, requisitando uma conexão.
4. O terminal T2 responde com uma mensagem H.225 indicando que a chamada está sendo processada.

5. Agora o terminal T2 necessita registrar-se junto ao *gatekeeper*. Ele envia uma mensagem RAS *Admission Request* ao *gatekeeper* no canal RAS.

6. O *gatekeeper* confirma o registro enviando uma mensagem RAS mensagem *Admission Confirm* para o terminal T2.

7. O terminal T2 alerta o terminal T1 do estabelecimento da conexão enviando uma mensagem de alerta H.225.

8. O terminal T2 confirma o estabelecimento da conexão enviando uma mensagem de conexão H.225 ao terminal T1. Nesse momento a chamada está estabelecida.

9. Um canal de controle H.245 é estabelecido entre os terminais T1 e T2. O terminal T1 envia uma mensagem *Terminal Capability Set* para o terminal T2 para troca de parâmetros.

10. O terminal T2 reconhece os parâmetros do terminal T1 enviando uma mensagem H.245 *Terminal Capability Set Ack.*

11. O terminal T2 envia os seus parâmetros para o terminal T1 através de uma mensagem H.245 *Terminal Capability Set*.

12. O terminal T1 reconhece os parâmetros do terminal T2 enviando uma mensagem H.245 *Terminal Capability Set Ack.*

13. O terminal T1 abre um canal de mídia com o terminal T2 enviando uma mensagem H.245 *Open Logical Channel*. O endereço de transporte do canal RTCP é incluído na mensagem.

14. O terminal T2 reconhece o estabelecimento de um canal lógico unidirecional do terminal T1 para o terminal T2 enviando a mensagem H.245 *Open Logical Channel Ack.* Incluídos na mensagem de reconhecimento estão o endereço de transporte RTP alocado no terminal T2 para ser utilizado pelo terminal T1 enviar fluxos de mídia e o endereço RTCP recebido anteriormente do terminal T1.

15. O terminal T2 abre um canal de mídia com o terminal T1 enviando uma mensagem H.245 *Open Logical Channel.* O endereço de transporte do canal RTCP é incluído nesta mensagem.

16. O terminal T1 reconhece o estabelecimento de um canal lógico unidirecional do terminal T2 para o terminal T1 enviando a mensagem H.245 *Open Logical Channel Ack.* Incluídos na mensagem de reconhecimento estão o endereço de transporte RTP alocado no terminal T1 para ser utilizado pelo terminal T2 enviar fluxos de mídia e o endereço RTCP recebido anteriormente do terminal T2.

17. O terminal T1 envia os fluxos de mídia encapsulados no RTP para o terminal T2.

18. O terminal T2 envia os fluxos de mídia encapsulados no RTP para o terminal T1.

19. O terminal T1 envia mensagens de controle RTCP para o terminal T2.

20. O terminal T2 envia mensagens de controle RTCP para o terminal T1.

21. O terminal T2 inicia a fase de liberação da chamada, enviando uma mensagem H.245 *End Session Command* para o terminal T1.

22. O terminal T1 libera a chamada e confirma a liberação enviando uma mensagem H.245 *Close Logical Channel* para o terminal T2.

23. O terminal T2 completa a liberação enviando uma mensagem H.225.0 (Q.931) *Release Complete* para o terminal T1.

24. Os terminais T1 e T2 desligam-se do *Gatekeeper* enviando para este a mensagem RAS *Disengage Request.*

25. O *gatekeeper* confirma o desligamento dos terminais T1 e T2 enviando a mensagem H.225.0 *Disengage Confirm* para os dois terminais.

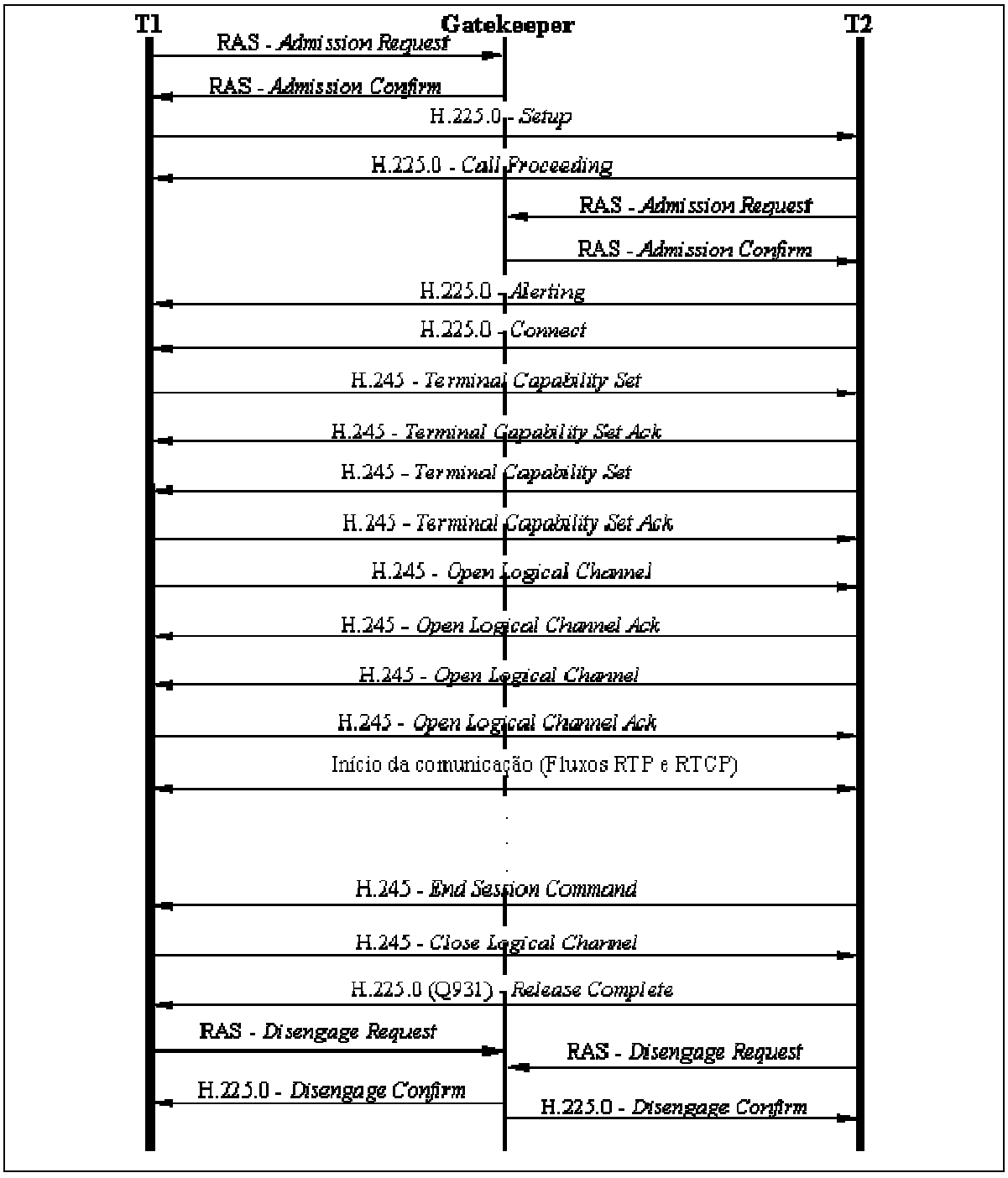


Figura 2.2 – Configuração e Finalização de Chamadas H.323, adaptado de (Baumgarten, 2002).

2.8 – Session Initiation Protocol (SIP)

A recomendação do IETF *Session Initiation Protocol* (SIP), publicada como RFC3261, protocolo de sinalização para iniciar, gerenciar e terminar sessões através de uma rede de pacotes. Estas sessões podem envolver um ou mais participantes. O SIP suporta tanto a comunicação *unicast* como a *multicast*.

O SIP é um protocolo baseado em texto, o que o torna fácil de ler e entender, além disso, é facilmente extensível, podendo ser ampliado para acomodar funcionalidades e serviços como controle de chamadas, presença, mensagens instantâneas, mobilidade e interoperabilidade com os sistemas de telefonia existentes.

2.8.1 – Componentes do SIP

O SIP possui quatro tipos de entidades lógicas que são:

- ***User Agent* (UA)** – é o terminal. UAs iniciam e terminam sessões através de requisições e de respostas. A RFC3261 define o UA como uma aplicação, que contêm ambos o *User Agent client* e o *User Agent server*. Equipamentos que podem ter uma função de UA em uma rede SIP são computadores, *IP-phones*, *telephony gateways*, *call agents*, serviços de resposta automática, entre outros.
- **Servidor *Proxy*** – é uma entidade intermediária que age como um servidor e um cliente com o propósito de fazer requisições em nome de outros clientes. As requisições são tratadas internamente ou repassadas para outros servidores, provavelmente após uma tradução. O *Proxy* interpreta, e, se necessário, reescreve a mensagem antes de re-encaminhar.
- **Servidor de Redirecionamento** – é um servidor que aceita uma requisição SIP, mapeia o endereço SIP da parte chamada do zero (se não é um endereço conhecido) ou endereços mais novos e os retorna para o cliente. Diferentemente do Servidor *Proxy*, o servidor de redirecionamento não passa a requisição para outros servidores.
- **Servidor de Registro** – é um servidor que aceita requisições de registro com o propósito de atualizar a base de dados de localização com a informação de contato do usuário especificado na requisição. Tipicamente, um servidor de registro é uma combinação de um servidor *Proxy* com um servidor de redirecionamento.

O SIP tem um único formato de protocolo para todas as ações, como registro, controle de chamada e presença. O SIP usa o SDP (*Session Description Protocol*) como uma linguagem de descrição de mídia e o RTP/RTCP como o protocolo de transporte em tempo real para a mídia, da mesma forma que o H.323.

O SIP está acima da camada de transporte. Teoricamente, ele é independente do transporte, mas na prática ele usa UDP e TCP, com planos de usar o SCTP (*Stream Control Transmission Protocol*) RFC 2960 no futuro.

O SIP suporta cinco diferentes formas para estabelecer e terminar uma conexão multimídia:

- Localização do usuário: para determinar qual o sistema final vai ser usado para comunicação;
- Funcionalidades de usuário: para determinar qual mídia e quais parâmetros desta mídia devem ser usados;
- Disponibilidade de usuário: para determinar a disponibilidade da parte chamada para participar da comunicação;
- Estabelecimento de chamada: para estabelecer os parâmetros da chamada para ambas as partes (chamado e chamador);
- Manipulação de chamada: para incluir transferências e término da chamada.

O protocolo pode ser usado para iniciar sessões, convidar membros para sessões iniciadas por outros meios ou iniciar uma chamada com vários participantes usando uma MCU.

O SIP suporta de forma transparente mapeamento de nomes e serviços de redirecionamento, permitindo a implementação de serviços da RI (Rede Inteligente) e da RDSI (Rede Digital de Serviços Integrados).

O SIP suporta mobilidade dos clientes através de requisições ao servidor *Proxy* e ao servidor de redirecionamento para saber a localização atual do usuário. O SIP não está vinculado a nenhum protocolo particular de controle de conferência.

2.8.2 – Endereços SIP URL e SIP URI

Os objetos endereçados pelo SIP são clientes em hosts. Estes clientes são identificados por um SIP URL (*Uniform Resource Locator*) RFC 1738 (1994), funcionando da mesma forma que a *mailto* ou a *telnet* URL, ou seja, user@host.

A *user part* é um nome de usuário ou um número de telefone. A *host part* é um domínio ou um endereço IP. Um endereço SIP de um usuário pode ser obtido *out-of-band*, podendo ser aprendido via algum agente de mídia existente, pode ser incluído no cabeçalho

de alguma mensagem ou gravado durante alguma interação anterior. Em muitos casos, o SIP URL de um usuário pode ser suposto a partir de seu endereço de e-mail.

O endereço SIP URL pode designar um indivíduo, a primeira pessoa disponível de um grupo de pessoas ou todo um grupo de pessoas.

O SIP URI (*Universal Resource Identifier*) RFC 2960 (1998) é uma *string* compacta de caracteres para identificar um recurso abstrato ou físico. O URI provê um simples e completo meio para identificar um recurso. Existe muita confusão no relacionamento entre os conceitos de URL e URI. O URI pode ser classificado como um localizador, um nome ou ambos. O URL refere-se a uma parte do URI que identifica recursos via uma representação dos seus primeiros mecanismos de acesso, sua rede/localização.

2.8.3 – Funcionamento do SIP

SIP é um protocolo de requisições e respostas, uma requisição SIP e a apropriada resposta são agrupadas em uma transação SIP. Existem muitos campos que contêm valores idênticos em uma transação SIP para facilitar o mapeamento entre uma requisição e uma resposta. Uma requisição SIP pode ser enviada usando, tanto um protocolo confiável, quanto um não confiável, incluindo UDP e TCP.

A seguir serão apresentados os principais tipos de requisição e de respostas.

2.8.3.1 - Requisições

O protocolo define seis métodos de requisição SIP conforme listado a seguir:

- INVITE para iniciar as sessões. O INVITE indica que o usuário ou o serviço está sendo convidado a participar da sessão.
- ACK para confirmar o estabelecimento da sessão. O ACK confirma que o cliente recebeu uma resposta final a um INVITE. O ACK não gera resposta para nenhum protocolo de transporte.
- OPTIONS para requisitar informações sobre capacidades.
- BYE para terminar uma sessão. O cliente UA usa o BYE para indicar para o servidor que ele deseja liberar uma parte da chamada (*call leg*). Uma requisição BYE é encaminhada pelo servidor como uma requisição INVITE e pode ser emitida tanto pela parte chamada, quanto pela parte chamadora.

- CANCEL para cancelar uma sessão pendente, ou seja, a requisição CANCEL cancela uma requisição pendente.
- REGISTER permite ao cliente associar uma SIP URL permanente a uma SIP URL temporária, refletindo a localização de rede atual. Um cliente usa o REGISTER para vincular o endereço listado no campo de cabeçalho com um servidor SIP para um ou mais URL onde o cliente pode ser encontrado.

2.8.3.2 Respostas

Uma resposta SIP contém um código de *status*. Este código é um número de três dígitos que indica o resultado da requisição. A resposta também contém frase, que fornece uma descrição do resultado da requisição. A frase ajuda o usuário a compreender a resposta.

Os códigos de *status* definidos no SIP têm valores entre 100 e 699. O primeiro dígito do código indica a classe da resposta. A seguir serão apresentadas as classes de resposta do SIP.

- 1xx: Informativo – requisição recebida, continuando a processar a requisição (por exemplo, 180 indica que o telefone do usuário chamado está tocando).
- 2xx: Sucesso - indica que uma requisição foi recebida, compreendida e aceita. O 200 OK e o 202 ACCEPTED são os principais exemplos desta classe.
- 3xx: Redirecionamento – uma ação adicional deve ser tomada para completar a requisição (por exemplo, um servidor *front-end* envia uma resposta 302 para redirecionar o cliente para um servidor).
- 4xx: Falha de Cliente – a requisição contém uma sintaxe errada ou não pode ser efetuada por este servidor (por exemplo, um servidor *home* envia uma resposta, 401 Não Autorizado, se este cliente necessitar fornecer credenciais).
- 5xx: Falha de Servidor – O servidor não tratou uma requisição válida (e.g. um servidor envia uma resposta, 504 *Timeout*, se o tempo no *Gateway* foi esgotado).
- 6xx: Falha Global – A requisição não pôde ser tratada por nenhum servidor.

Requisições SIP podem ser enviadas diretamente de um cliente para um servidor, ou elas podem atravessar um ou mais servidores *Proxy* ao longo do caminho. Os UAs enviam requisições tanto diretamente para o endereço indicado na URI SIP, quanto para

um *Proxy* designado, independentemente do endereço de destino. O endereço de destino atual é levado pela requisição URI. Cada *Proxy* pode encaminhar a requisição baseado nas políticas locais e na informação contida na requisição SIP. O *Proxy* pode reescrever uma requisição URI.

Uma sessão é iniciada com uma requisição de INVITE. Um bem sucedido convite SIP consiste de duas requisições, INVITE seguido por um ACK. A requisição INVITE convida o chamado a juntar-se a uma conferência ou a estabelecer uma conversa entre duas partes. Após o chamado ter concordado em participar da chamada, o chamador confirma que ele recebeu através do envio de uma requisição ACK.

A requisição INVITE tipicamente contém uma descrição de sessão, se a parte chamada desejar aceitar a chamada, ela responde ao convite retornando uma descrição similar listando as mídias que ela deseja usar.

As trocas de informações para um INVITE enviado a um servidor *Proxy* são mostradas na Figura 2.3.

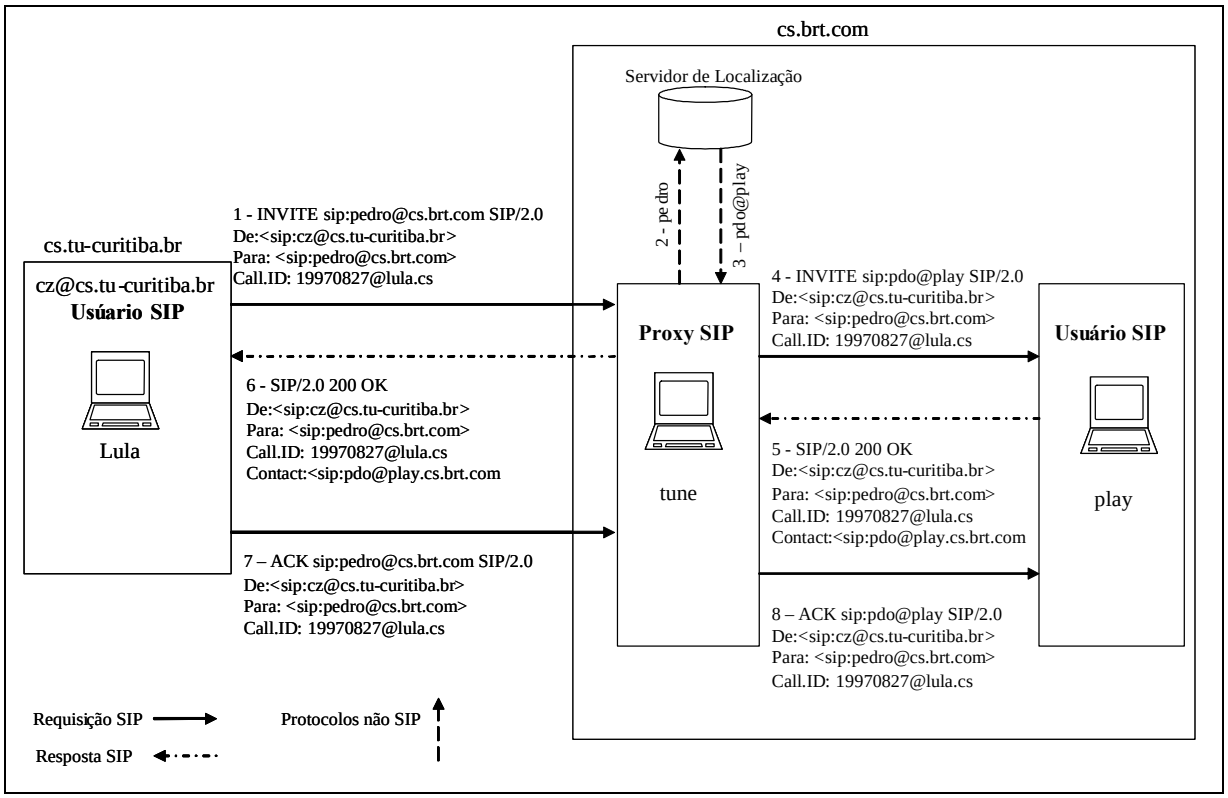


Figura 2.3 – Troca de protocolos para um servidor SIP *Proxy*, adaptado de (Wang, 2002).

Na Figura 2.3, o servidor *Proxy* aceita a requisição INVITE (passo 1), contatando o servidor de localização com todo ou parte do endereço (passo 2) e obtém uma localização

mais precisa (passo 3). O servidor *Proxy* então emite uma requisição INVITE para o endereço retornado pelo servidor de localização (passo 4). O servidor UA alerta o usuário (passo 5) e retorna uma indicação de sucesso para o servidor *Proxy* (passo 6). O servidor *Proxy* retorna o resultado obtido para o usuário chamador original (passo 7). O recebimento desta mensagem é confirmado pelo usuário chamador usando uma requisição ACK.

A Figura 2.4 apresenta a mesma situação utilizando um servidor de redirecionamento.

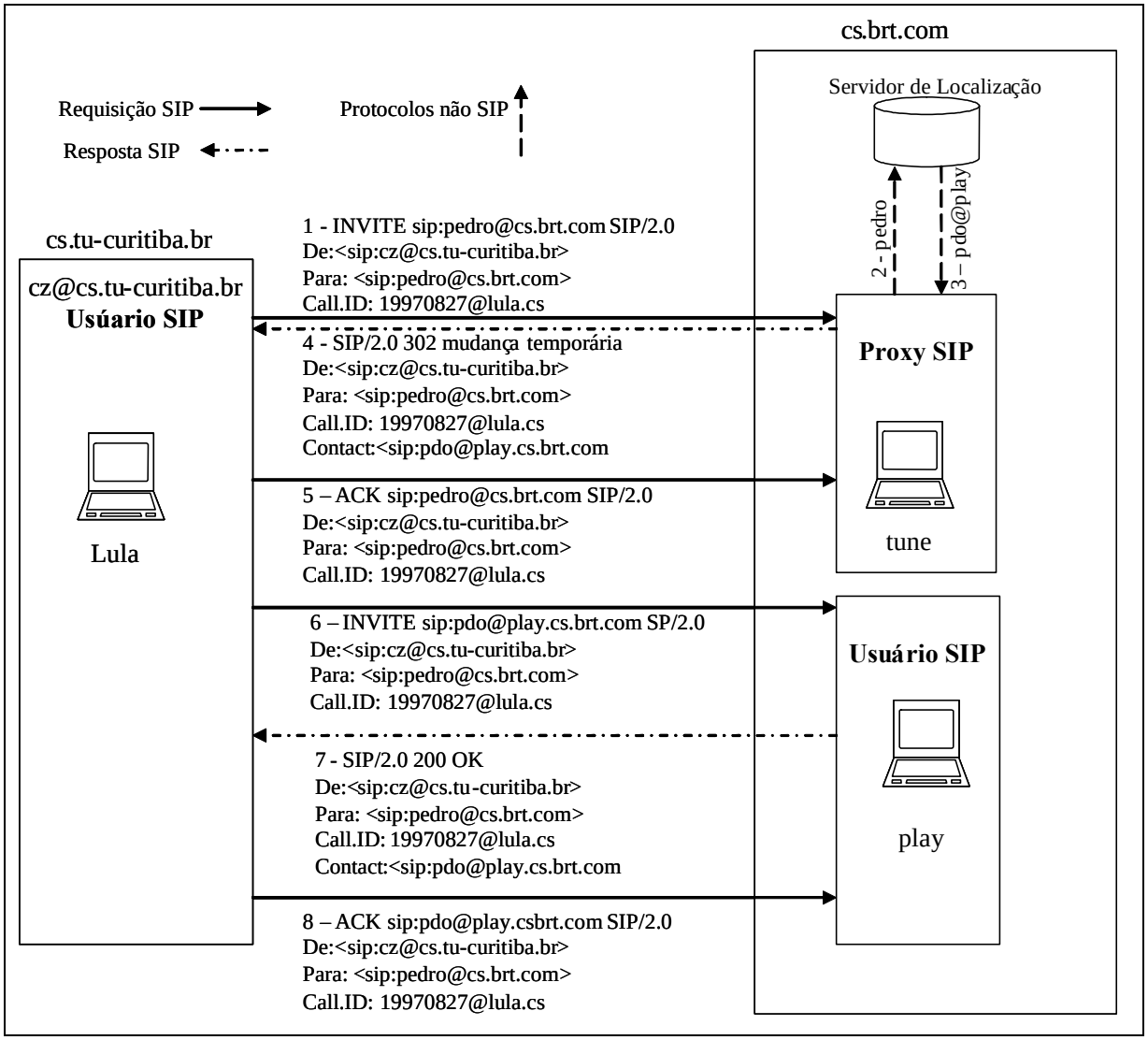


Figura 2.4 – Troca de protocolos para um servidor de Redirecionamento SIP, adaptado de (Wang, 2002).

2.8.4 – Extensões do SIP

Um grande número de extensões e complementações tem sido agregadas a especificação SIP. Isto inclui a adição das seguintes funcionalidades para o SIP, os quais podem ser usados por eventos de notificação, mensagem instantânea e controle de chamada:

- SUBSCRIBE: Permite que o usuário se inscreva em certos eventos. Isto significa que o usuário deve ser informado quando certos eventos ocorrerem.
- NOTIFY: É usado para informar ao usuário um evento no qual ele está inscrito ocorreu.
- MESSAGE: O SIP também pode ser usado pelo serviço de mensagem instantânea. Um usuário envia uma mensagem para outro usuário utilizando uma requisição que inclui o método MESSAGE. Este método carrega o texto no corpo de um pacote SIP.
- INFO: É usado para transferência de informação durante uma sessão, como uma atividade de usuário.
- SERVICE: O método SERVICE pode carregar, como dados, uma mensagem SOAP (*Simple Object Access Protocol*) (2007).
- NEGOTIATE: É usado para negociar vários tipos de parâmetros, como um mecanismo de segurança e algoritmos.
- REFER: Este método permite a quem enviou a requisição instruir a que receber para contatar uma terceira parte usando os detalhes de contato presentes na requisição. A transferência de chamada é uma aplicação que usa o método REFER.

2.9 - TISPAN NGN

O TISPAN (*Telecommunication and Internet Services and Protocols for Advanced Networking*) é um grupo de trabalho criado pelo ETSI (*European Telecommmunications Standards Institute*) para definir como será a evolução da rede fixa de voz comutada e a integração com as redes móveis. Tendo sido adotado pelo ITU-T como padrão para evolução das redes.

A arquitetura TISPAN (ES 282 001) define um conjunto de entidades funcionais que se comunicam através de protocolos e interfaces padronizadas. Ela provê uma infra-estrutura capaz de suportar comunicações multimídia em tempo real baseadas em IP.

Entende-se por multimídia a integração de múltiplos tipos de mídia como áudio, vídeo e dados, em uma única sessão ou chamada.

Desta forma, a implantação da TISPAN possibilitará a integração de serviços de áudio, vídeo e dados, permitindo ao cliente uma videoconferência independente do tipo de acesso e de equipamento.

A arquitetura funcional do TISPAN, definida no documento ES 282 001 está dividida em duas camadas, a de serviço e a de transporte, conforme a Figura 2.5.

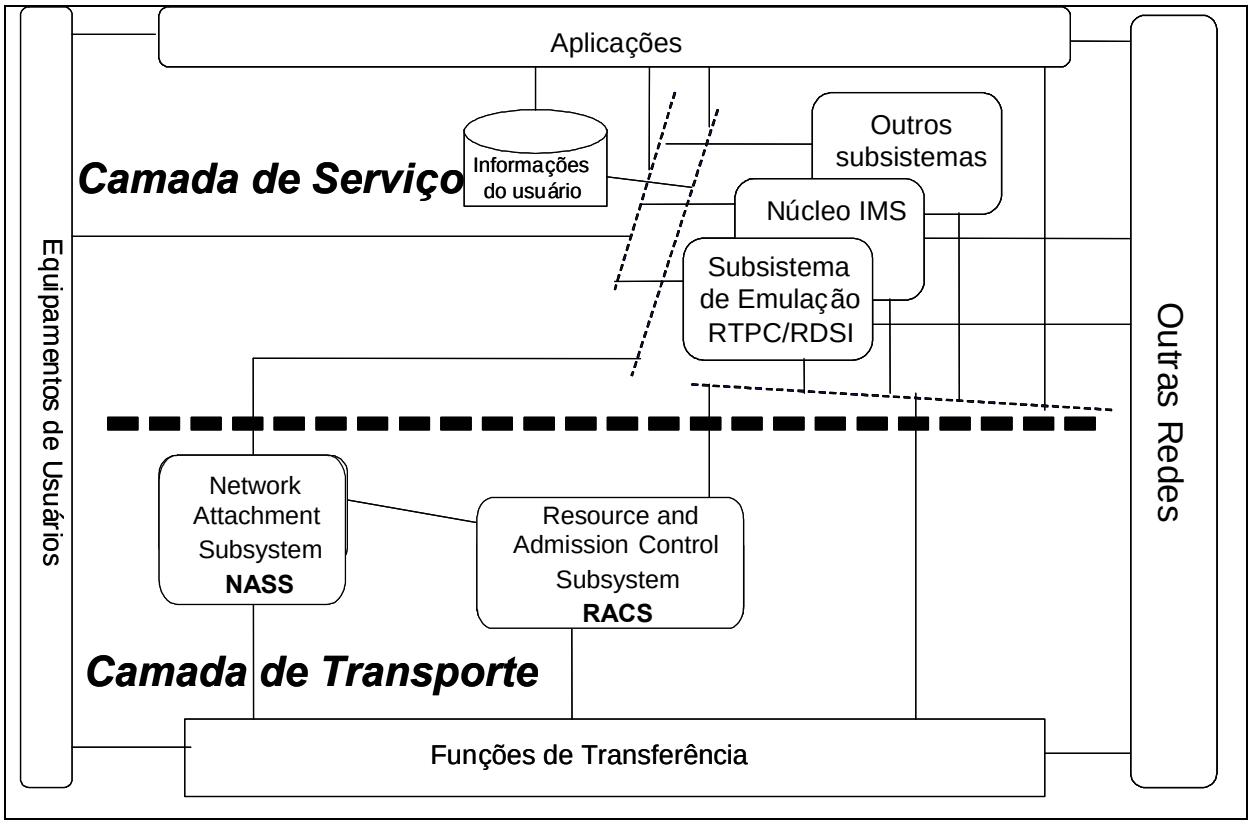


Figura 2.5 – Arquitetura TISPAN, adaptado de (ES 282 001).

A camada de serviços é formada pelos seguintes componentes:

- O núcleo IP *Multimedia Subsystem* (IMS) (ES 282 007).
- O Subsistema de Emulação RTPC/RDSI (ES 282 002).
- Outros subsistemas multimídia (por exemplo, o subsistema de *streaming*, o subsistema de distribuição de conteúdo) e aplicações.
- Componentes comuns (usados por vários subsistemas) como os componentes requeridos por aplicações, funções de cobrança, gerenciamento do perfil do usuário, gerenciamento de segurança, bases de dados de roteamento, entre outros.

Esta arquitetura orientada a subsistemas permite a adição de novos subsistemas no futuro para cobrir novas demandas e novas classes de serviço. Isto também possibilita a importação (e adaptação) de subsistemas definidos por outros órgãos de padronização.

A conectividade IP é provida para o equipamento do usuário da rede de nova geração pela camada de transporte, sob controle do *Network Attachment Subsystem* (NASS) (ES 282 004) e do *Resource and Admission Control Subsystem* (RACS) (ES 282 003). Estes subsistemas escondem a tecnologia de transporte usada no acesso e no núcleo das redes debaixo da camada IP.

O TISPAN suporta o aprovisionamento de serviços multimídia baseados em SIP para terminais de nova geração. Ele também suporta o aprovisionamento de serviços que simulam a RTPC/RDSI.

O núcleo IMS é uma parte do IMS definido no documento TS 23.228, restringindo-se as funcionalidades de controle de sessão.

Para esta dissertação o principal elemento da camada de serviços é o núcleo IMS. A seguir serão apresentados a arquitetura do IMS e seus principais elementos, os quais farão parte da solução proposta.

2.9.1 - Arquitetura IMS

O IMS (IP *Multimedia Subsystem*) originalmente surgiu das iniciativas para padronização de sistemas de comunicações móveis dirigidas pelo 3GPP (*3rd Generation Partnership Project*). O IMS foi adotado pela indústria como sendo o padrão para o sistema de suporte aos serviços multimídia e convergentes relacionados ao acesso.

O IMS tem suas entidades funcionais e elementos definidos com interfaces padrão nas camadas de controle e serviço, indiferente ao tipo de acesso e do serviço prestado, conforme representado na Figura 2.6.

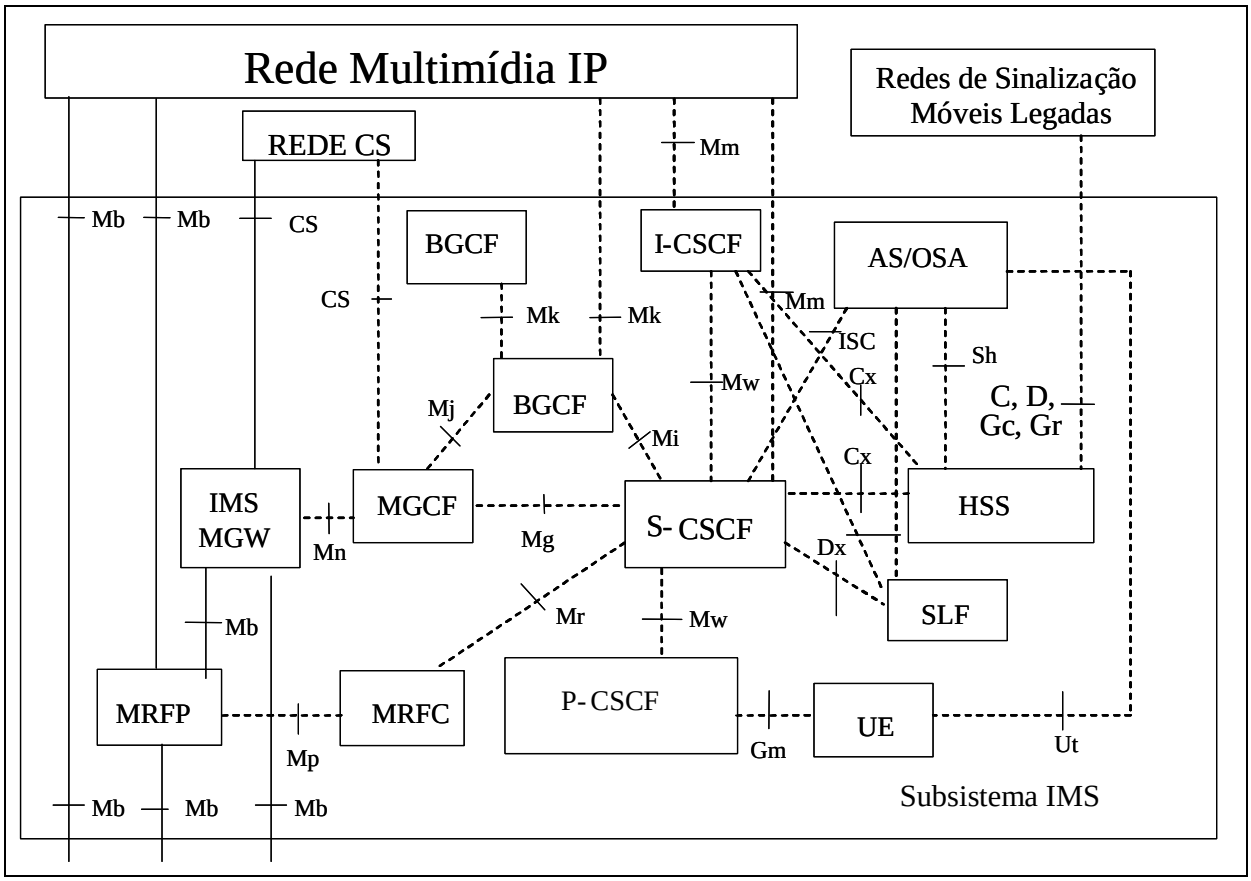


Figura 2.6 – Arquitetura do IMS, adaptado de (TS 23.228).

Os elementos pertencentes ao IMS estão mostrados na Figura 2.6. Para o estabelecimento de sessões multimídia, vários elementos na arquitetura IMS são envolvidos, cujas breves descrições estão a seguir.

2.9.1.1 - CSCF

A *Call Session Control Function* (CSCF) estabelece, monitora, suporta e finaliza as sessões multimídia e gerencia as interações do usuário com o serviço. A CSCF pode atuar como *Proxy* CSCF (P-CSCF), *Serving* CSCF (S-CSCF) ou *Interrogating* CSCF (I-CSCF).

O P-CSCF é o primeiro ponto de contato para o UE (*User Equipment*) com o IMS; o S-CSCF controla o estado das sessões na rede; o I-CSCF é principalmente o ponto de contato dentro da rede da operadora para todas as conexões IMS destinadas a um usuário ou, para clientes em *roaming* que atualmente se encontram dentro da área de serviço da operadora.

2.9.1.2 - P-CSCF

O P-CSCF (*Proxy* – CSCF) é o primeiro ponto de contato do terminal IMS com a rede, no plano de sinalização. Todas as chamadas iniciadas ou terminadas por um terminal IMS passam por um P-CSCF. Ele encaminha as mensagens SIP de registro para um I-CSCF e mensagens SIP de estabelecimento de sessões para um S-CSCF e pode estar localizado na rede do visitante, caso a mesma possua uma rede IMS, ou na própria rede da operadora. A Figura 2.7 apresenta o P-CSCF dentro o núcleo IMS da arquitetura TISPAN.

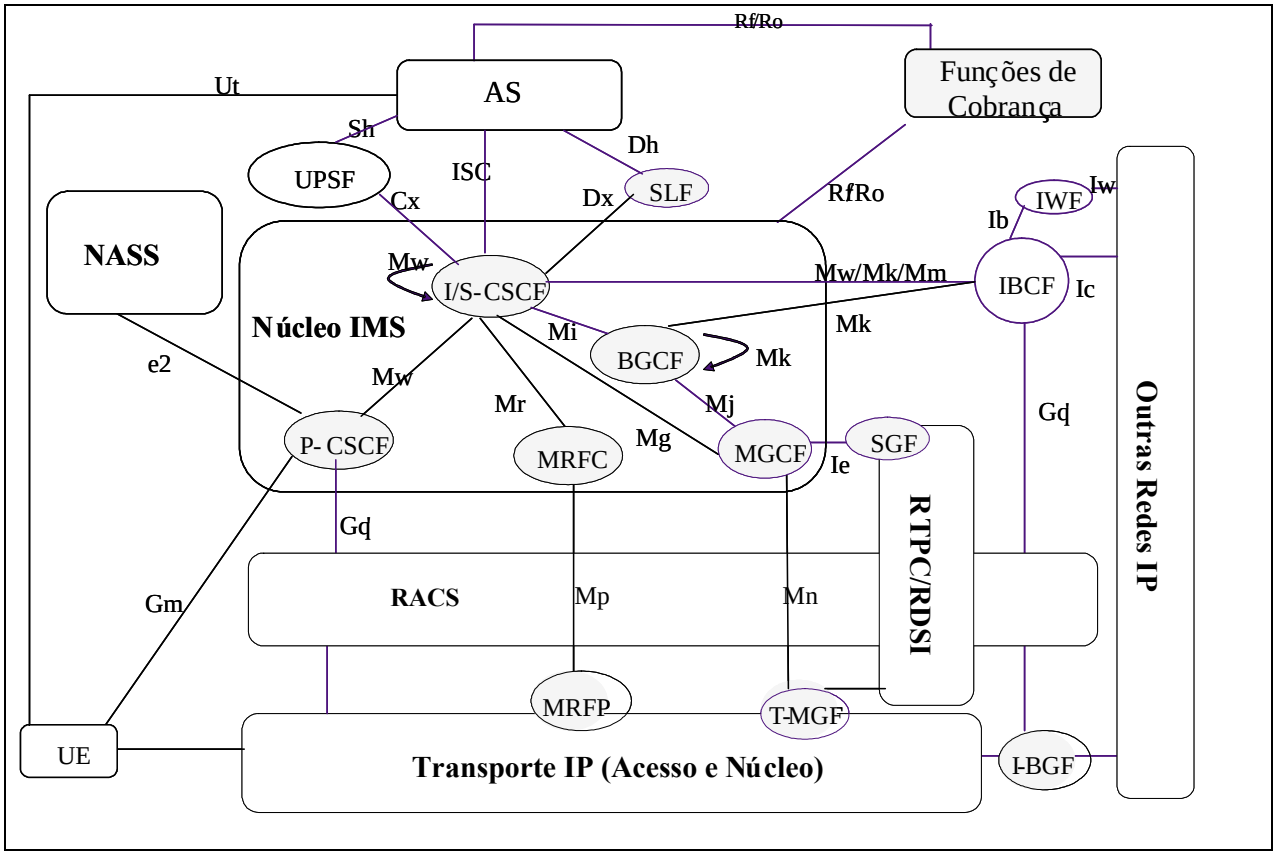


Figura 2.7 – P-CSCF dentro da arquitetura TISPAN, adaptado de (TS 23.002).

2.9.1.3 - S-CSCF

O S-CSCF (*Serving* – CSCF) é o equipamento central do plano de controle. Na arquitetura SIP, o S-CSCF possui as funções de servidor SIP e de servidor de registro SIP. Toda a sinalização originada ou terminada por um terminal IMS passa obrigatoriamente por um S-CSCF e entre as principais funções está a de roteamento de mensagens SIP, inspecionando cada mensagem SIP e determinando para qual elemento (AS - Servidor de

Aplicação, BGCF, I-CSCF, etc.) a mensagem faz referência. Se uma sessão inicia com um número de telefone ao invés de um SIP-URI, o S-CSCF provê os serviços de tradução, consultando ao ENUM (*Telephone Number Mapping*) (RFC 2916, 2000). Outras funções importantes são:

- A responsabilidade por autenticar os clientes que acessam a rede IMS a partir do HSS (*Home Subscriber Server*), efetuando os downloads dos vetores de autenticação deste usuário;
- Auxílio às políticas de estabelecimento de sessões e serviços através do perfil de serviço, proveniente do HSS, para encaminhar as chamadas deste usuário corretamente, para verificar quais tipos de mídia são suportados pelo usuário e para aplicar filtros (*initial filter criteria*), ou políticas, diversos ao usuário;
- Suporte ao *forking* para estabelecimento de múltiplas sessões, entre outras.

2.9.1.4 - I-CSCF

O I-CSCF (*Interrogating* – CSCF) é um p*roxy* SIP localizado na fronteira da rede, que recebe as mensagens SIP de registro de um P-CSCF. Ele é o ponto de contato na rede da operadora para todas as conexões destinadas a um usuário desta rede, ou para um usuário em *roaming* nesta rede. Podem existir múltiplos I-CSCF numa mesma rede. As seguintes funções são desempenhadas pelo I-CSCF:

- Registro: Associação a um S-CSCF para o usuário através do registro SIP;
- Fluxos de associados à sessão e sem associação;
- Roteamento de consulta usando SIP de outra rede para o S-CSCF;
- Obtenção do endereço do S-CSCF através de consulta ao HSS/UPSF (*User Profile Server Function*);
- Redirecionamento de uma consulta SIP ou resposta para o S-CSCF;
- Tarifação e medição dos recursos utilizados: Geração de bilhetes.

Em adição o I-CSCF possui a funcionalidade de criptografar parte das informações nas mensagens SIP que contém conteúdo sensível, como numero dos servidores no domínio, seus nomes no DNS, ou suas capacidades. Esta funcionalidade é referida como THIG (*Topology Hiding Internetork Gateway*).

2.9.1.5 - HSS

O HSS (*Home Subscriber Server*) é o principal repositório de dados para todos os clientes do IMS. No TISPAN o HSS foi designado por outro nome, a saber, UPSF (*User Profile Server Function*). Neste texto o USPF será sempre referenciado como HSS.

O HSS deve ser agnóstico ao tipo de serviço provido ao usuário, a aplicação, a rede, ao equipamento terminal do usuário, a localização geográfica, etc., armazenando os dados que incluem a identidade do usuário, informações de registro, parâmetros de acesso, informações de segurança, informações de localização, e informações relativas a gatilhos de serviços, conforme a especificação TS 23.002. Igualmente, o HSS deve realizar autenticação, autorização, entre outras, conforme previsto no mesmo documento.

No caso de implementação de múltiplos HSS na rede, deve-se utilizar uma base de dados adicional responsável pelo mapeamento dos endereços dos clientes e os respectivos HSS. Este elemento é denominado SLF (*Subscription Locator Function*). Entre suas funcionalidades, o SLF deve mapear as identidades públicas do usuário ao endereço do respectivo HSS que contém as informações do usuário.

O HSS deve ser capaz de integrar informações heterogêneas e permitir que funcionalidades do núcleo da rede sejam oferecidas para as aplicações e domínios de serviço, conseguindo desta forma esconder a heterogeneidade das informações.

O HSS deve ter as seguintes funcionalidades:

- Funcionalidade multimídia IP para prover suporte às funções de controle do IMS. Esta funcionalidade deve ser independente da rede usada para acessar o núcleo IMS;
- O subconjunto de funcionalidades HLR (*Home Location Register*) / AUC (*Authentication Center*) requerido pelo domínio OS;
- O subconjunto de funcionalidades HLR/AUC requeridos pelo domínio CS (*Circuit switching*), caso seja necessário permitir acesso do assinante ao domínio CS ou suportar *roaming* para domínios CS de redes legadas GSM (*Global System For Mobile Communication*) /UMTS (*Universal Mobile Telecommunications System*);
- O HSS deve ser considerado como repositório de dados GUP (*Generic User Profile*) para o núcleo da rede IMS;
- A organização dos dados do assinante deve estar compatível com o especificado no documento TS 23.008;

- Os números, endereços e identificadores, especificados no documento TS 23.003 devem ser armazenados no HSS.

O HSS é responsável por suportar o controle de chamadas e entidades de gerência de sessões de diferentes domínios e subsistemas da operadora.

2.9.1.6 - MRFC/MRFP

Os elementos *Multimedia Resource Function Controller* (MRFC) e *Multimedia Resource Function Processor* (MRFP) são os elementos dentro da arquitetura IMS responsáveis pelo tratamento dos fluxos de mídias e recursos. A utilização de elementos MRFC e MRFP especializados para determinados tipos de serviços ou servidores de aplicações não serão considerados, devido aos custos operacionais envolvidos na manutenção de elementos distintos realizando funções idênticas.

O MRFP prove funções especializadas de processamento de recursos, além das funções disponíveis no *Gateway* de Mídia. Isto inclui recursos para suporte a conferências multimídias, fonte para anúncios multimídia, implementação de funcionalidades de IVR (*Interative Voice Response*) e análises de conteúdo de mídia.

O MRFC, em conjunto com um MRFP, prove um conjunto de recursos no núcleo da rede para o suporte de serviços. O MRFC interpreta a informação que entra proveniente de um servidor de aplicação via um S-CSCF e controla o MRFP de acordo com a mesma. O MRFC, em conjunto com o MRFP, prove *bridges* para conferência, exibição de anúncios, transcodificação de mídia, entre outros.

As funções básicas do elemento MRFC são definidas abaixo:

- Controle de recursos de fluxo de mídias no elemento MRFP;
- Interpretar informações vindas dos servidores de aplicação e elementos S-CSCF e controlar o elemento MRFP de acordo;
- Geração de bilhetes.

As funções básicas do elemento MRFP são definidas abaixo:

- Controle do transporte no ponto de referência Mb, ilustrado na Figura 2.6;
- Mistura fluxos de mídia de entrada (por exemplo, conferência multi-usuário);
- Executa fluxos de mídia para anúncios multimídia;

- Processa fluxos de mídia (por exemplo, transcodificação de áudio);
- Controle de acesso aos recursos de mídia compartilhados.

2.9.1.7 - AS/OSA E SCS/IM-SSF

A arquitetura IMS padronizou a separação da camada de serviço da camada de controle com a definição de três elementos, genericamente chamados de servidores de aplicação (AS). Estes elementos são responsáveis por oferecer serviços multimídia de valor adicionado.

Os AS definidos pelo 3GPP para o IMS, na especificação TS 23.228 são:

- SIP *Application Server*: servidor de aplicações baseado no protocolo SIP e responsável por prover serviços diretamente para o domínio IMS. Não possui interface de programação padronizada e é geralmente utilizado para prover serviços padrões (por exemplo, PoC, IP-Centrex, IM);
- OSA (*Open Service Access*) *Service Capability Server* (SCS): servidor de aplicação (*Gateway*) que provê a capacidade de expor os recursos da rede abaixo (*southbound*) para as aplicações através de um conjunto de APIs padronizadas. Diversos SCSs são definidos, permitindo a integração do mesmo elemento com recursos de controle de chamadas, localização de terminais, envio e recepção de mensagens e integração com serviços *Web*. Diversos protocolos de rede são suportados simultaneamente e é utilizado para prover serviços convergentes;
- CAMEL (*Customized Applications for Mobile Enhanced Logic*) IM-SSF: servidor de aplicação responsável por realizar a interface entre o domínio IMS e serviços tradicionais de rede móvel baseados em plataformas SCP (*Service Control Point*) CAMEL.

Os servidores de aplicação podem residir tanto na rede da operadora quanto em redes de terceiros. Somente o OSA SCS provê recursos padronizados e seguros para autenticação e autorização de aplicações de terceiros no domínio IMS.

De uma maneira geral, o AS é capaz de gerar bilhetes para cada requisição feita pelos elementos de rede, onde o registro mínimo deve conter:

- Os dados básicos da requisição (protocolo, data/hora, duração, endereço IP da origem, tipo de requisição, número chamado, número chamador, entre outros);
- Os SCSs acessados; as aplicações acessadas (identificação, IP do Servidor de Aplicação; dados de desempenho; entre outros).

2.9.1.8 - BGCF

O *Breakout Gateway Control Function* (BGCF) é o elemento de rede da infra-estrutura IMS responsável por selecionar o MGCF (*Media Gateway Control Function*) para interfuncionamento com o domínio RTPC/CS (*Circuit Switching*). BGCF interage primariamente com o S-CSCF, MGCF e o BGCF de outras redes IMS, determinando o melhor roteamento das sessões que saem do IMS para a RTPC.

As funcionalidades básicas do BGCF são:

- Receber a consulta do S-CSCF para selecionar um domínio RTPC/CS apropriado para estabelecimento da sessão.
- Selecionar a rede que interfuncione com o domínio um dado domínio RTPC/CS desejado (e.g. chamada internacional x nacional, móvel x fixa, interconexão x rede própria). Se o interfuncionamento está em outra rede, então o BGCF encaminhará a sinalização SIP para o BGCF desta outra rede. Se o interfuncionamento está numa rede oculta (*network hiding*) pelo I-CSCF, o BGCF deverá encaminhar a sinalização SIP via o I-CSCF (THIG - *Topology Hiding Inter-network Gateway*) até o BGCF da outra rede.
- Selecionar o MGCF na rede em que o interfuncionamento com domínio RTPC/CS irá ocorrer e encaminhar a sinalização SIP para este MGCF.
- Gerar bilhetes.
- Fazer uso da informação recebida de outros protocolos, ou pode fazer uso de informação administrativa, quando fizer a escolha da rede que ocorrerá o interfuncionamento.
- Possuir mecanismos de otimização de roteamento de chamada para a RTPC/CS em função do baixo custo, menor caminho de rede e outros.
- Possuir mecanismos de roteamento de chamada para a RTPC/CS em função do tipo de chamada fixa ou móvel.

- Suportar os endereços baseados em SIP URI (RFC 2396, 1998) e TEL URI (RFC 3966, 2004) para o roteamento de chamadas RTPC/CS.
- Possuir mecanismos de configuração inteligentes a fim de minimizar erros e tempo de adequação ao plano de encaminhamento da rede fixa e móvel.

2.9.1.9 - MGCF

O MGCF (*Media Gateway Control Function*) é o elemento de controle de gateway da arquitetura IMS baseada no 3GPP que tem por objetivo servir de interface entre a rede legada baseada em circuito comutado RTPC e o IMS.

3 – INTERFUNCIONAMENTO ENTRE SIP E H.323

Atualmente mais de 90% dos terminais de clientes que participam de uma videoconferência utilizam como protocolo de sinalização e controle de chamadas o H.323, porém é consenso na indústria que em um curto período de tempo esta situação será revertida e a maioria dos terminais passará a trabalhar com o protocolo SIP.

Desta forma, por um período de tempo é necessário conviver com os dois protocolos na rede, pois não é possível substituir ou impor ao cliente a troca dos terminais que ele já adquiriu para o seu serviço de videoconferência. Portanto, é necessária uma solução para que os terminais baseados em H.323 participem de conferências com terminais baseados em SIP.

Conforme apresentado no capítulo anterior os dois protocolos usam o protocolo RTP para transportar em tempo real tanto o áudio, quanto o vídeo, o que reduz o trabalho de interfuncionamento entre estes protocolos no que se refere à tradução de protocolos de sinalização e à descrição de sessão.

O interfuncionamento entre SIP e H.323 requer suporte transparente de sinalização e descrição de sessão entre os componentes SIP e H.323. O elemento que realiza esta tradução é chamado de SIP-H.323 *Interworking Function* (IWF) definido na RFC 4123 (2005).

A funcionalidade principal do IWF pode ser decomposta em registro do usuário, tradução de endereço, estabelecimento de chamada, e aprovisionamento do serviço. Esta funcionalidade pode ser implementada como parte dos elementos de uma rede VoIP como um *gatekeeper* H.323, um *Proxy* SIP, ou um *Softswitch*, o qual pode englobar um *gatekeeper* e *proxy* SIP. A funcionalidade também pode ser implementada via um *gateway* de sinalização SIP-H.323 externo.

Para endereçar um terminal que usa outro protocolo de sinalização, existem duas formas. Na primeira, o usuário pode explicitamente identificar o protocolo como parte do endereço, inventando alguma forma de URL H.323 (RFC 3508, 2003) como h323:alice@brasiltelecom.com. Se uma URL H.323 é usada por um terminal SIP, ele terá a responsabilidade de encontrar o IWF apropriado.

Alternativamente, um terminal usando um protocolo de sinalização particular, como H.323, vê todos os outros terminais como sendo nativos, e não sabe ou não se importa que um endereço particular seja referente a um terminal de outra rede. Esta alternativa é mais interessante, porém, requer que os registros dos clientes sejam

exportados para outras redes. Dependendo do tipo de informação compartilhado entre os elementos H.323 ou SIP e o IWF, é possível utilizar diferentes arquiteturas para prover uma solução de endereço e um estabelecimento de chamadas transparentes.

Neste capítulo serão descritos os detalhes do interfuncionamento entre SIP e H.323, incluindo a tradução entre H.245 e SDP e apresentados cenários para a implementação desta funcionalidade.

3.1 – Requisitos básicos para a tradução de protocolos

Os requisitos básicos para um interfuncionamento entre SIP e H.323 são sumarizados a seguir:

- Conformidade com o protocolo: O IWF deve usar os componentes do H.323 e do SIP. O IWF deve tratar todas as funcionalidades mandatórias do H.323 e do SIP. Os cenários comuns de chamada devem ser facilmente implementáveis.
- Registro de usuário: O IWF deve usar o registro de usuário nas redes H.323 e SIP para resolver o nome do usuário (Alias ou URL) para um endereço IP. Em outras palavras, ele deve prover um *framework* no qual o usuário pode chamar qualquer endereço sem saber a que rede (H.323 ou SIP) o outro usuário pertence.
- Mapeamento entre H.245 e SDP: O IWF deve ser capaz de mapear todas as mensagens H.245 mandatórias para as apropriadas mensagens SDP e vice-versa, sem que o terminal esteja ciente de que esta transação está ocorrendo. Outras funcionalidades opcionais do H.245 e do SDP devem ser mapeadas para facilitar ao máximo o interfuncionamento entre as duas redes.
- Tráfego direto de dados entre os terminais: Quando possível, o IWF deve rotear o tráfego RTP e RTCP diretamente entre os terminais envolvidos em uma conferência sem passar através do IWF. Isto reduz o atraso dos pacotes de mídia e ajuda a construir IWFs escaláveis.
- Suporte transparente para algoritmos de áudio e vídeo: O IWF deve prover suporte transparente para algoritmos de áudio e vídeo, ou seja, o IWF não deve restringir as capacidades dos terminais de suportar vários algoritmos de áudio e vídeo.
- Mapear a seqüência de chamada: O IWF deve mapear as seqüências de mensagens entre H.323 e SIP de tal maneira que cada decisão importante (aceitar ou rejeitar uma chamada, escolher um algoritmo para um canal lógico, entre outros) seja tomada pelos terminais envolvidos na conferência e não pelo IWF.

Assume-se que a descrição de sessão dada por um terminal SIP se refere às capacidades de transmissão e recepção do terminal SIP. Isto pode não ser verdade para uma aplicação em particular. Se este for o caso, então o terminal SIP espera enviar esta informação no SDP.

A análise do interfuncionamento SIP-H.323 pode ser dividida em estabelecimento de chamada, mapeamento de endereços e encontrar um subconjunto de capacidades descrito pelo H.245 e pelo SDP como conferências, serviços de chamada, segurança e autenticação. Os itens citados acima serão descritos neste capítulo, salvo, segurança e autenticação que não fazem parte do escopo desta dissertação.

3.1.1 Tradução do Estabelecimento de Chamada

A informação necessária para estabelecer uma chamada entre dois terminais pode ser dividida em três partes, o endereço de destino da sinalização, as capacidades de mídia local e remota, e os endereços de transporte de mídia local e remoto no qual o terminal pode receber os pacotes de mídia.

No H.323, esta informação é distribuída em diferentes estágios do estabelecimento da chamada, enquanto o SIP transporta esta informação em uma única mensagem INVITE na sua resposta.

Traduzir uma chamada SIP para uma chamada H.323 é simples. O IWF pega todos os três pedaços de informação na mensagem SIP INVITE e os distribui entre os múltiplos estágios de estabelecimento de uma chamada H.323. Entretanto, na direção contrária, ou seja, do H.323 para o SIP, os diferentes estágios para o estabelecimento da chamada do H.323 devem ser agrupados em uma única mensagem SIP INVITE.

3.1.2 Registro do usuário

A tradução SIP-H.323 tem que resolver o problema de registro do usuário. O registro do usuário envolve mapeamento dos nomes de usuário, números de telefone ou alguma outra forma de identificar os terminais. Permitindo que os clientes sejam alcançados através de identificadores independentes de localização, pois o registro do usuário fornece a mobilidade pessoal. Uma chamada destinada ao

sip:paulo@brasiltelecom.com alcança o usuário Paulo não importando o endereço IP que ele possa estar usando no momento.

No SIP, os servidores *Proxy* e redirecionamento acessam um servidor de localização, normalmente um servidor de registro que recebe as informações de registro do usuário. Um servidor como o brasiltelecom.com mapeará todos os endereços que tiverem o formato sip:juca@brasiltelecom.com para o endereço IP correspondente, independentemente de onde juca esteja logado. No H.323, a mesma funcionalidade é realizada pelo *Gatekeeper* H.323. O IWF deve usar a informação de registro do usuário disponível nas redes H.323 e SIP para traduzir um nome de usuário para um endereço. O IWF pode conter um servidor de registro SIP, um *gatekeeper* H.323 ou nenhum deles, como será discutido na seção a seguir.

3.1.3 Descrição de Sessão

Um IWF também deve mapear as descrições de sessão entre os protocolos de sinalização. Conforme mostrado no capítulo anterior o H.323 usa o H.245 para descrever a sessão. O H.245 pode negociar as capacidades de mídia, provendo controle da conferência, estabelecendo e fechando os canais de mídia. No H.245, capacidades de mídia são descritas como um subconjunto de descritores de funcionalidades, listados em ordem decrescente de preferência.

Um descritor de funcionalidade, também chamado de subconjunto de funcionalidades simultâneas, é um subconjunto de funcionalidades alternativas, onde cada uma contém uma lista de algoritmos, da qual somente um pode ser usado de cada vez. Desta forma um descritor de funcionalidades {[a1;a2][v1;v2][d1]} tem três subconjuntos de funcionalidades alternativas: [a1;a2], [v1;v2], e [d1]. As chaves indicam conjunção, ou seja, {AB} significa A e B, e os colchetes indicam disjunção, ou seja, [A; B] significa A ou B. Assim o descritor de funcionalidade do exemplo acima indica que o terminal pode suportar áudio, vídeo e dados simultaneamente. Áudio pode usar o codec a1 ou a2, vídeo o codec v1 ou v2, e dados o formato d1.

O SIP pode usar vários formatos de descrição de sessão. Como mostrado no capítulo anterior na prática somente o SDP é usado. O SDP lista os tipos de mídia e a codificações suportadas. Diferentemente do H.245, o SDP não pode expressar restrições *cross-media* ou *inter-media*. Assim, o SDP não pode indicar que para um particular tipo de mídia, o outro lado pode somente escolher um subconjunto A ou um subconjunto B de uma

lista de codecs, mas não codecs de ambos os subconjuntos. Da mesma forma, o SDP não pode expressar que certos codecs de áudio podem somente ser usados em conjunto com certos codecs de vídeo.

Então, uma capacidade de mídia SIP pode ser facilmente descrita em H.245, enquanto o contrário é mais complicado. Uma forma de resolver este problema é transportar múltiplas mensagens SDP no corpo de uma requisição SIP INVITE e de sua resposta, usando o tipo de conteúdo multi-partes. Cada mensagem SDP então representa um descritor de funcionalidade do subconjunto de funcionalidades do H.245. Um problema para o uso desta solução é que existem muitos SIP UA (*User Agent*) que não entendem conteúdo multi-partes.

3.1.4 Conferência multiponto

A realização de conferência *ad hoc* entre terminais SIP e H.323 não é possível sem modificação em um ou em ambos os protocolos. A conferência *ad hoc* é aquela na qual os participantes não sabem, antecipadamente, se a chamada será ponto a ponto ou multiponto. Os participantes podem trocar de uma chamada ponto a ponto para uma conferência multiponto ou vive-versa durante a chamada. É possível para os participantes convidarem uma terceira parte para participar da conferência ou ainda a terceira parte pode juntar-se a conferência sem convite.

Os protocolos SIP e H.323, individualmente, podem suportar conferências *ad hoc*. No SIP, a topologia da conferência pode ser malha completa com cada participante tendo relacionamento com todos os outros participantes ou uma conferência centralizada, topologia em estrela, na qual cada participante troca sinalização com um equipamento central de conferências. É possível comutar da conferência em topologia malha para a topologia em estrela.

No H.323, as conferências são gerenciadas por um MC (*Multipoint Controller*) apresentado no capítulo anterior. O MC pode ser parte de um terminal H.323, de um *gateway*, de um *gatekeeper* ou de uma MCU (*Multipoint Control Unit*). As conferências H.323 têm, naturalmente, uma topologia em estrela com todos os participantes tendo um canal de controle H.245 com o MC. O MC é responsável por decidir as capacidades de mídia comuns para a conferência, pelo controle da conferência, e por outras funções da conferência. Todos os participantes devem obedecer às capacidades de mídia definidas pelo MC.

Devido a diferença de topologia das conferências entre o SIP e o H.323, o suporte transparente de uma conferência multiponto não pode ser conseguido sem a modificação dos protocolos.

3.1.5 Serviços de Chamada

Serviços de chamada avançados como desvio e transferência de chamadas são suportados tanto pelo SIP quanto pelo H.323. O H.323 usa o H.450.x para prover estes serviços suplementares. O SIP tem suporte para chamada em espera, transferência assistida por operadora, desvio de chamada, estacionamento de chamada, entre outros, conforme o *Draft: Session initiation protocol service examples* (2006).

3.1.6 Segurança e Qualidade de Serviço

Outros problemas na tradução entre SIP-H.323 incluem segurança e qualidade de serviço (QoS). O SIP e o H.323, individualmente suportam estes itens, porém, a tradução de uma arquitetura aberta como o SIP, onde segurança e QoS são independentes da conexão estabelecida, para o H.323, onde segurança e QoS estão intimamente ligadas com o estabelecimento das chamadas, torna-se muito difícil.

3.2 – Arquitetura para registro do usuário

Nesta seção serão descritas três arquiteturas para registro de usuário e soluções de endereço. Os servidores de registro do usuário são entidades de rede que armazenam informações de registro do usuário. Servidores de registro SIP e *gatekeeper*s H.323 são servidores de registro do usuário. Isto simplifica a localização do usuário independentemente do protocolo de sinalização, no caso do IWF ter acesso direto aos servidores de registro do usuário. O servidor de registro do usuário também encaminha a informação de registro de uma rede, a qual o usuário pertence, para a outra rede.

3.2.1 – IWF Contendo um SIP Proxy e um Servidor de Registro

A primeira arquitetura combina, em um IWF, um servidor de registro SIP e um servidor *proxy*, conforme a Figura 3.1a. Neste enfoque a informação de registro é mantida pelo *gatekeeper* H.323. Sempre que o servidor de registro SIP receber uma requisição SIP REGISTER, ele gerará uma requisição de registro (RRQ) para o *gatekeeper* H.323, traduzindo a SIP URI em um endereço alias H.323.

O H.323 registra o usuário através do procedimento H.225.0. Desde que a informação de registro SIP também esteja disponível através do *gatekeeper* H.323, qualquer entidade H.323 pode resolver o endereço da entidade SIP localizável através do servidor SIP/IWF. Na outra direção, se um SIP UA quer falar com outro usuário, que reside em uma rede H.323, ele envia uma mensagem SIP INVITE para o servidor SIP. O servidor SIP envia uma requisição de localização H.323 *multicasts* (LRQ) para os *gatekeepers* H.323.

O *gatekeeper* no qual o usuário H.323 está registrado responde com o endereço IP do usuário H.323. Uma vez que, o servidor SIP sabe que o endereço pertence a uma rede H.323, ele pode rotear a chamada até o destino. Um inconveniente desta alternativa é que os *gatekeepers* H.323 são sobrecarregados com todos os registros da rede SIP.

Esta alternativa mantém somente aqueles endereços SIP tratados pelos servidores de registro disponíveis para o H.323. Tipicamente, um servidor de registro é responsável por um único domínio (por exemplo, brasiltelecom.com). Assim, cada zona H.323 teria que ter um IWF. Se um usuário H.323 quiser chamar um terminal SIP, primeiramente o terminal H.323 localiza, usando os servidores de nomes de domínios (DNS TXT – Hersent, 2000), o *gatekeeper* apropriado, que usa a informação de registro, disponibilizada pelo IWF, para descobrir que este endereço está localizado atualmente em uma rede SIP.

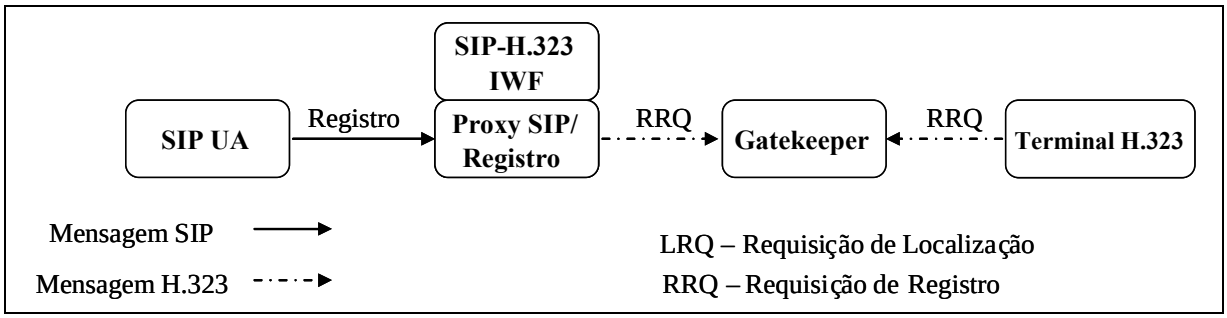


Figura 3.1a –IWF contendo um SIP *Proxy* e um servidor de registro SIP, adaptado de (Kundan, 2006).

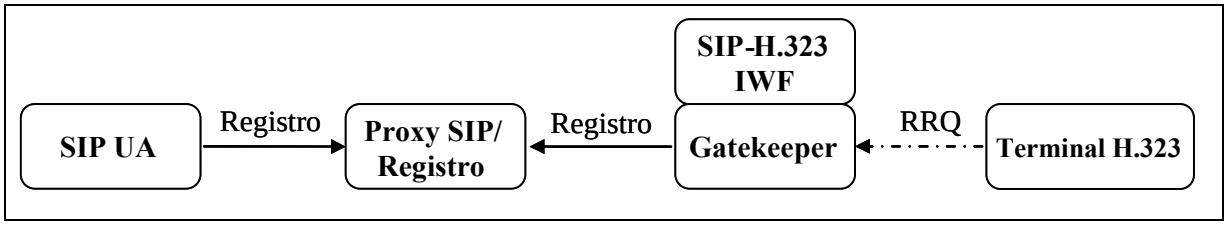


Figura 3.1b – IWF contendo um *Gatekeeper* H.323, adaptado de (Kundan, 2006).

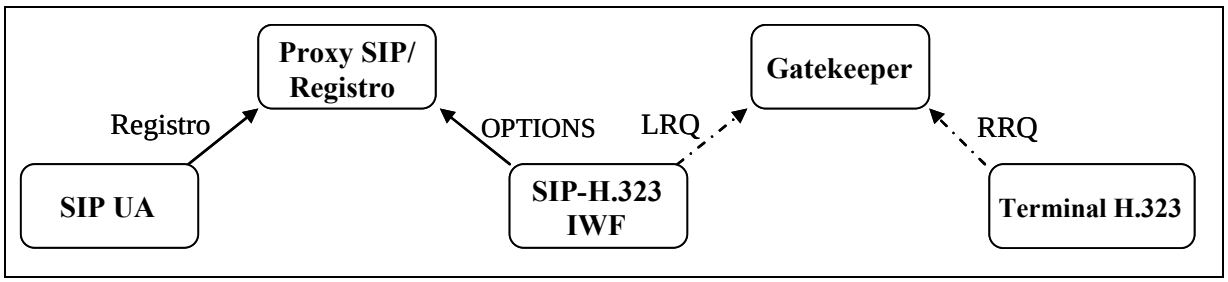


Figura 3.1c –IWF independente de *proxy* ou *gatekeeper*, adaptado de (Kundan, 2006).

3.2.1.1 – Detalhamento da Tradução

Ao receber uma requisição SIP REGISTER, o IWF gera uma requisição H.323 RAS RRQ para o seu *gatekeeper* local. O endereço de sinalização da chamada da mensagem RAS contém o endereço de rede do IWF, o tipo de terminal é definido como "*gateway*" e o terminal Alias é derivado do cabeçalho do SIP *To* ou da REQUEST-URI.

Assim, toda a requisição de resolução de endereço vinda da rede H.323 para um endereço SIP pode ser resolvida por um *gatekeeper* usando uma requisição H.323 RAS. Qualquer requisição vinda da rede SIP para a rede H.323 é enviada para o *gatekeeper* pelo IWF. O *gatekeeper* resolve este endereço usando RAS/H.323.

Durante a inicialização, o IWF registra seu próprio endereço Alias (gw1) com o seu *gatekeeper* local, de modo que qualquer elemento da rede H.323 pode alcançar diretamente os terminais SIP. Para isto, basta conectar o IWF através do endereço Alias e fornecer o endereço do SIP no endereço da extensão remota da mensagem de configuração do H.323.

Na Figura 3.2 é mostrada a inicialização de terminais SIP e H.323, e o IWF quando o mesmo contém o SIP *Proxy* e o servidor de registro. O registro pode ser armazenado em dois *gatekeeper*s independentes da rede H.323.

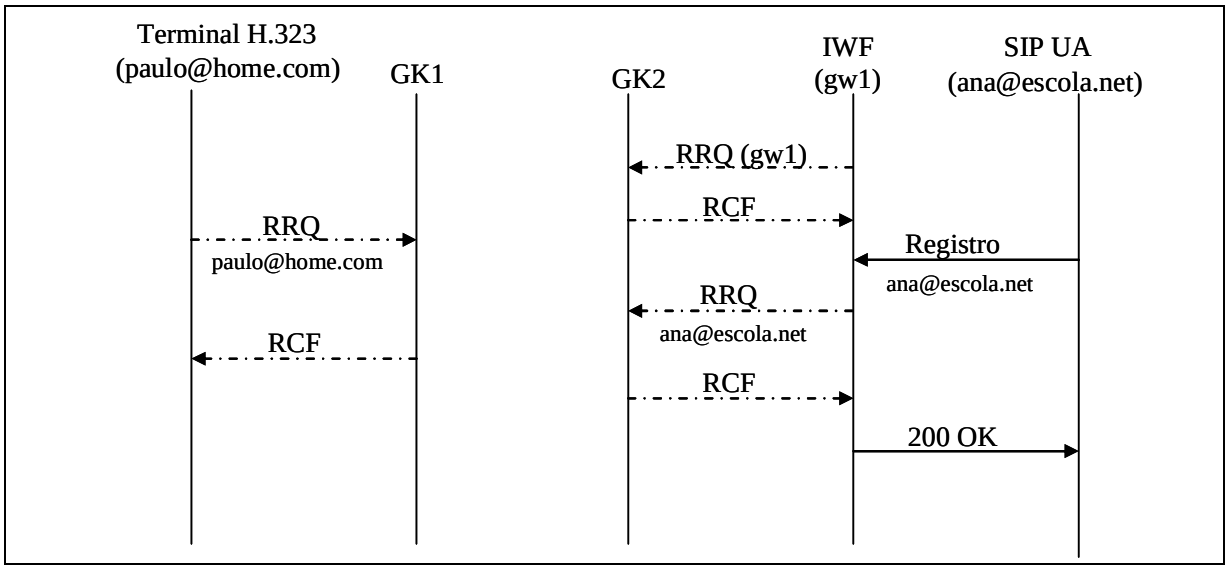


Figura 3.2 – Fluxo de mensagens para uma inicialização correta, adaptado de (Kundan, 2006).

A tradução de endereço do SIP para o H.323 é mostrada na Figura 3.3, enquanto a tradução de endereço do H.323 para o SIP é mostrada na Figura 3.4.

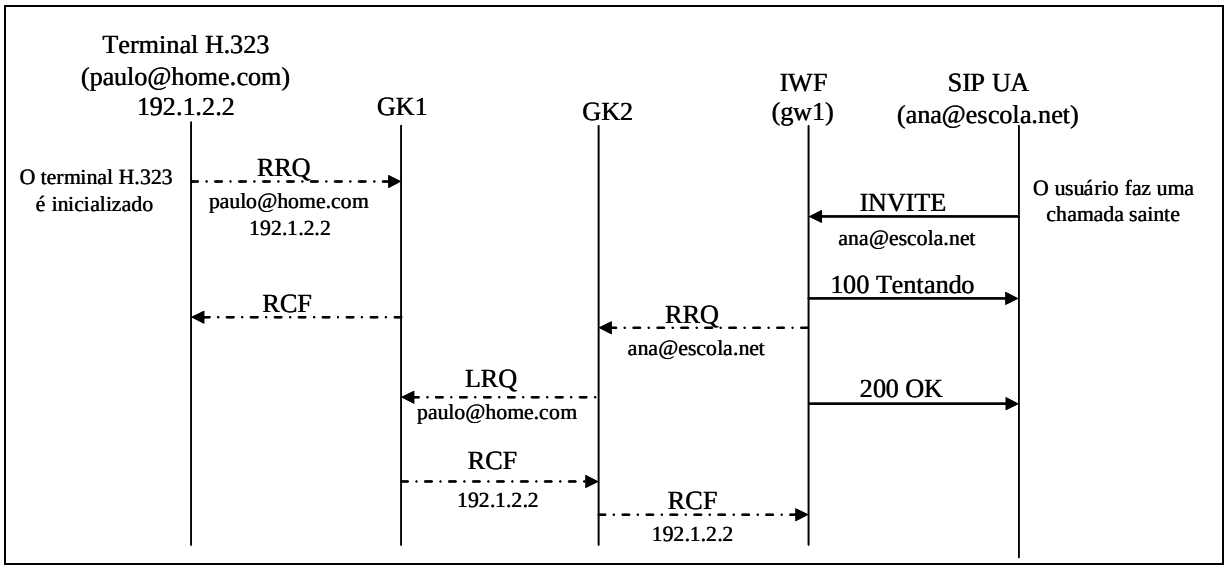


Figura 3.3 – Tradução de endereço do SIP para o H.323, adaptado de (Kundan, 2006).

O esquema apresentado na Figura 3.3 supõe que o IWF tem conhecimento da parte do cliente do protocolo H.323 RAS para que ele possa falar com o *gatekeeper*. Cada SIP UA que se registra com o servidor de registro também aparece na base de dados do *gatekeeper.*

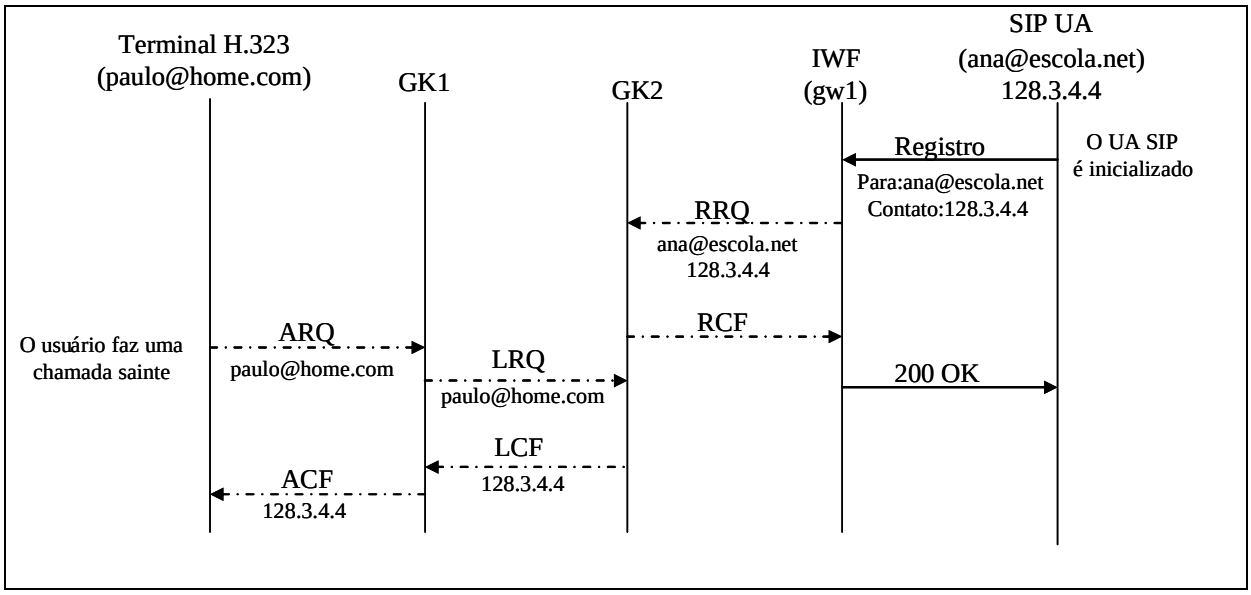


Figura 3.4 – Tradução de endereço do H.323 para o SIP, adaptado de (Kundan, 2006).

3.2.2 – IWF Contendo um Gatekeeper H.323

A arquitetura, mostrada na Figura 3.1b é semelhante a mostrada na Figura 3.1a salvo que o servidor *proxy* SIP mantêm a informação de registro do usuário de ambas as redes. Toda a requisição de registro H.323 recebida pelo *gatekeeper* é enviada para o apropriado servidor de registro SIP, que armazena a informação de registro do usuário de ambas as entidades.

Para o terminal SIP, os terminais H.323 aparecem simplesmente como SIP URLs dentro do mesmo domínio. Se uma entidade H.323 quiser falar com um usuário que reside na rede SIP, ela envia uma requisição de admissão (ARQ) para o *gatekeeper*. O *gatekeeper* envia uma requisição de localização *multicast* (LRQ) para todos os outros *gatekeeper*s.

O servidor GK-IWF captura esta requisição e tenta encontrar se o endereço pertence a um usuário SIP. Isto é realizado pelo envio de uma requisição de opções SIP, que não define nenhum estado de chamada. Se o endereço for válido em uma rede SIP e o usuário estiver disponível para ser chamado, o IWF responde com uma confirmação de localização (LCF), deixando o terminal H.323 sabendo que o endereço é alcançável.

Esta alternativa tem o mesmo inconveniente da alternativa anterior, onde o servidor *proxy* SIP tem que armazenar toda a informação de registro H.323. Entretanto, esta alternativa tem a vantagem que mesmo que alguns *gatekeeper*s H.323 não estejam equipados com o IWF, a resolução de endereço funciona, pois, se um *gatekeeper* não puder resolver um endereço de destino, ele envia uma requisição de localização *multicast* (LRQ)

para os outros *gatekeeper*s na rede. Desde que, pelo menos um *gatekeeper* possua a capacidade de tradução de sinalização SIP-H.323, o usuário SIP pode ser localizado a partir de uma rede H.323.

3.2.2.1 - Detalhamento da Tradução

A tradução de endereço SIP para H.323 é mostrada na Figura 3.5, enquanto a tradução de endereço H.323 para SIP é mostrada na Figura 3.6.

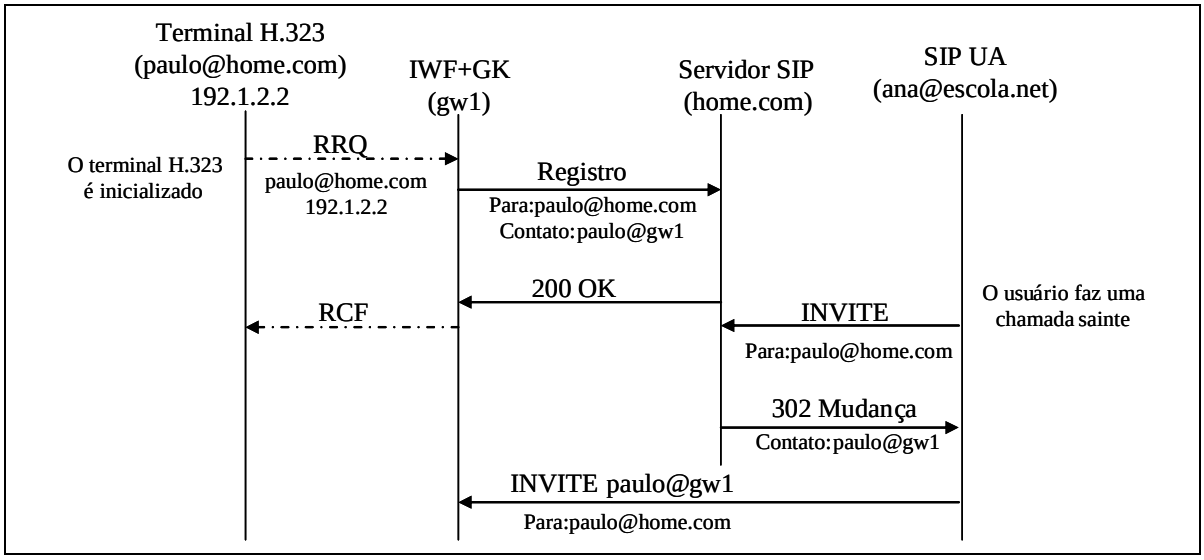


Figura 3.5 – Tradução de endereço do SIP para o H.323, adaptado de (Kundan, 2006).

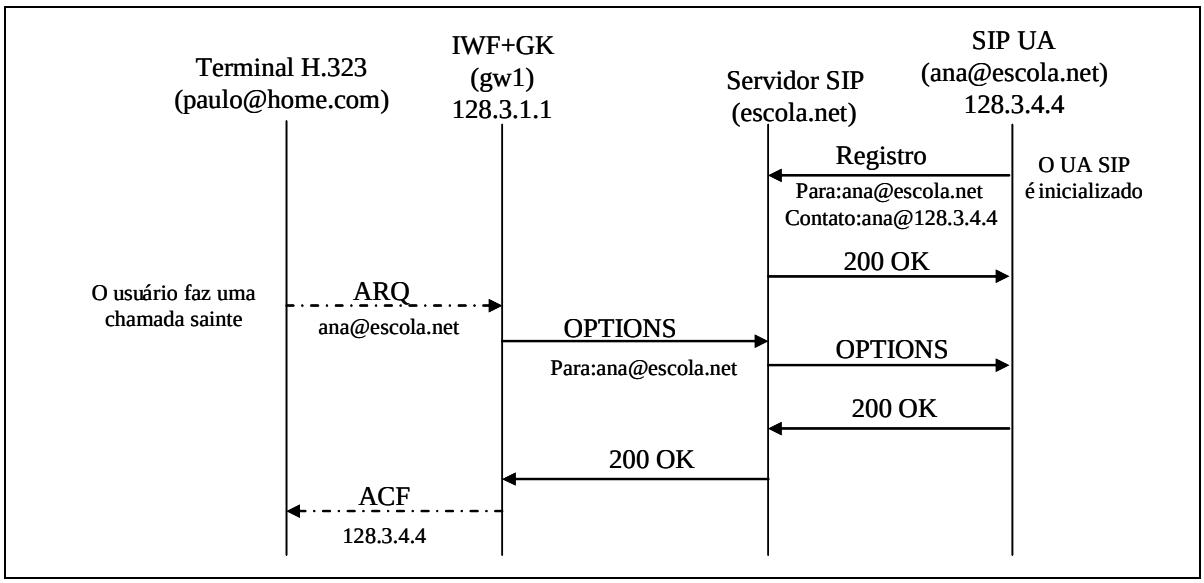


Figura 3.6 – Tradução de endereço do H.323 para o SIP, adaptado de (Kundan, 2006).

3.2.3 – IWF Independente de Proxy ou de Gatekeeper

Na terceira alternativa, mostrada na Figura 3.1c, o IWF não esta inserido em um *gatekeeper* ou *proxy*. O registro do usuário é feito independentemente nas redes SIP e H.323. Entretanto, quando uma chamada alcança o IWF, ele pergunta para a outra rede a localização do usuário. Nesta situação, assume-se que o IWF é capaz de interpretar e responder a uma requisição de localização (LRQ) de uma rede H.323.

O mecanismo de resolução de endereço funciona da seguinte forma. Suponha que o usuário SIP Ana queira falar com o usuário H.323 Paulo. Paulo está registrado com seu próprio *gatekeeper* em uma rede H.323 e o *gatekeeper* conhece o endereço IP do Paulo recebido via RRQ. Quando Ana contata o SIP *proxy* com o nome Paulo, o SIP *proxy* não tem nenhum registro para Paulo, mas está configurado para contatar o IWF caso a parte chamada esteja em uma rede H.323. O IWF, por sua vez, envia uma requisição *multicast* LRQ para todos os *gatekeeper*s perguntando por Paulo. Se não houver nenhuma resposta positiva dos *gatekeeper*s da rede H.323 dentro de um período de tempo, o IWF conclui que o endereço não é válido na rede H.323 e informa uma falha.

Na outra direção, Paulo envia uma requisição ARQ para o seu *gatekeeper*. Desde que este *gatekeeper* não tenha o endereço da Ana mapeado, ele envia uma *multicast* LRQ para os outros *gatekeeper*s da rede perguntando por Ana. Adicionalmente, o IWF está programado para receber a LRQ. O IWF usa uma requisição SIP OPTIONS para saber se Ana está em uma rede SIP e informa o *gatekeeper* se o pedido foi bem sucedido. Então é estabelecida uma chamada H.323 entre Paulo e o IWF e uma chamada SIP entre IWF e a Ana.

3.2.3.1 Detalhamento da Tradução

Quando uma chamada chega ao IWF vinda de uma rede SIP, o IWF envia uma requisição RAS ARQ para a rede H.323. Se o endereço não puder ser resolvido ou se a requisição RAS tiver o seu tempo esgotado, é enviada uma resposta informando a situação para o terminal SIP. Da mesma forma, chamadas da rede H.323 são traduzidas em requisições SIP e enviadas para um servidor *proxy* ou para um terminal.

Esta alternativa funciona bem se as chamadas estiverem identificadas por URLs que indicam o tipo de sinalização, ou seja, se uma requisição H.323 está direcionada para

um SIP URL ou vice-versa. Neste caso, é suficiente que o endereço do IWF esteja pré-configurado ou no *gatekeeper* ou no servidor *proxy*.

Se o endereço de destino não indica o protocolo de sinalização, um servidor SIP *proxy* tem que enviar todas as requisições que entram para o IWF, para o caso do destino estar em uma rede H.323.

Nesta arquitetura, o IWF deve implementar as mensagens de localização (RAS LRQ) e de confirmação de localização LCF. Quando uma chamada é iniciada por uma entidade H.323, o seu *gatekeeper* enviará uma requisição LRQ para os outros *gatekeeper*s. O IWF captura a mensagem LRQ e pode usar um de dois métodos para descobrir se algum terminal SIP está disponível neste endereço.

No primeiro método, o IWF envia uma requisição de REGISTER sem a informação de contato para o domínio identificado na requisição. Se o servidor de registro tem a informação sobre o terminal, ele retorna esta informação no cabeçalho da resposta no campo CONTACT. Então, o IWF traduz esta informação e responde para a rede H.323 com uma mensagem LCF. Se o servidor de registro retorna uma indicação negativa, o IWF responde com uma mensagem localização rejeitada (LRJ) ou permanece em silêncio. Este método é equivalente ao registro de uma terceira parte no SIP e não funciona se o servidor de registro exigir autenticação. O segundo método usa a mensagem SIP OPTIONS, no restante é idêntico ao anterior.

3.2.3.2 Conexão Direta: Sem registro de usuário

O IWF deve suportar conexões H.323 diretas. Desta forma, um usuário SIP (Ana) deve ser capaz de chamar um usuário H.323 (Paulo) através de um IWF (sip323. brasiltelecom.com) endereçando uma chamada para o sip:paulo@sip323.brasiltelecom.com.

Da mesma forma, o usuário H.323 deve poder alcançar um usuário SIP (sip:ana@escola.net) estabelecendo uma conexão Q.931 TCP com o IWF e fornecendo o endereço de destino ou o endereço de extensão remoto na mensagem de estabelecimento Q.931 como sip:usuario1@office.net. A conexão direta não envolve registro de usuário e espera-se que o chamador saiba que o destino é localizável via IWF.

Se um IWF receber uma mensagem de estabelecimento Q.931, ele deve tentar analisar o endereço de destino Q.931. Se o endereço de destino não é do próprio IWF e se

ele é capaz de traduzir para um endereço SIP, então o procedimento descrito na sessão 3.4 é usado no estabelecimento da chamada.

Diferentemente, se o endereço de destino é o do IWF e um endereço de extensão remoto estiver presente na mensagem de estabelecimento Q.931, então o IWF deve usar o endereço de extensão remoto para determinar o endereço SIP. O IWF também pode estar configurado para encaminhar todas as requisições para um SIP *proxy* pré-definido.

3.3 – Tradução de Endereço de Sinalização

Enquanto o registro do usuário exporta sua identidade em uma rede, a tradução de endereço é realizada pelo IWF para traduzir endereços SIP para os endereços H.323 e vice-versa. No SIP, endereços são tipicamente SIP URIs no seguinte formato sip:usuario@computador, onde os nomes de usuário podem ser números de telefone. Entretanto, os terminais SIP também podem suportar outras formas de URI como, "tel:" URIs para números de telefones [43] ou H.323 URLs [39].

Geralmente, se o terminal SIP não conseguiu entender uma URL em particular, ele envia a chamada para seu servidor local na esperança que o servidor consiga traduzi-la.

No H.323, os endereços (ASN.1 Alias *Address*) podem ter diversos formatos, incluindo identificadores não estruturados (H.323-ID), números de telefone que seguem o padrão E.164 (RFC 2916, 2000), URLs de vários tipos, nomes de computadores ou endereços IP, e endereços de e-mail (email-ID). Nomes de clientes locais e nomes de computadores são os mais comuns.

Para garantir a interoperabilidade SIP-H.323, deve haver uma maneira consistente e única de mapear uma SIP URI em um endereço H.323 e vice-versa. Traduzir uma SIP-URI para um endereço Alias H.323 é fácil, deve-se simplesmente copiar o SIP-URI para dentro do H.323-ID. As partes de usuário e de host do SIP-URI são usadas para gerar um identificador do e-mail, "usuario@computador", o qual é armazenado no campo email-ID do endereço Alias. O parâmetro *TRANSPORT*-ID é copiado da parte do computador do SIP-URI, caso ele seja um número. O campo E164 é extraído da parte do endereço SIP do usuário, se este estiver marcado como número de telefone.

Traduzir um endereço Alias H.323 para um endereço SIP é mais difícil, pois as múltiplas representações (E164, URL-ID, *TRANSPORT*-ID) necessitam ser agregadas em um único endereço SIP. No caso mais fácil, o Alias contêm um URL-ID com o SIP-URI, neste caso ele é simplesmente copiado na mensagem SIP. Caso o H.323-ID puder ser

considerado como um endereço SIP válido (“Alice<sip:alice@host>” ou “alice@host”) ele será usado.

Em outra situação, quando o *TRANSPORT*-ID está presente e não aponta o próprio IWF, ele forma as partes do computador e porta do SIP-URI. Finalmente, se o H.323 Alias tem um email-ID, ele é usado no prefixo SIP-URI da forma URI “sip:”.

Note que o endereço traduzido pode não ser necessariamente um endereço válido. No lado H.323, pode ser desejável configurar um *gatekeeper* para rotear todas as chamadas que não são resolvidas dentro da rede H.323 para o para o servidor de interfuncionamento, que tentaria uma tradução para um SIP-URI. Isto permitiria que os terminais H.323 alcançassem qualquer terminal SIP, incluindo aqueles não registrados na outra rede.

Se o servidor de interfuncionamento for configurado para rotear todas as chamadas para um SIP *proxy* padrão, ele enviará os endereços SIP que ele puder formar (a partir do endereço Alias H.323) para o SIP *proxy*. Isto pode ser necessário quando a implementação do servidor de interfuncionamento é separada em duas partes (separadas fisicamente), um terminal H.323 e um SIP UA. O terminal H.323 recebe a chamada, mapeia o endereço H.323 para um endereço SIP e envia uma requisição ao *proxy* SIP.

3.4 – Estabelecimento de Conexão

Uma chamada ponto a ponto da Alice para João necessita de três informações fundamentais, o endereço de destino lógico (A) do João, o endereço de transporte de mídia (T) no qual cada um dos clientes está pronto para receber os pacotes de mídia (RTP/RTCP) e a descrição das capacidades de mídia (M) das partes envolvidas. A seguir são descritas as informações:

- Endereço de destino lógico (A): Este é o endereço SIP para o cabeçalho ou REQUEST-URI, ou o endereço de destino Alias em uma mensagem de estabelecimento Q.931.
- Descrição de mídia (M): No SIP, M é a lista de tipos de dados suportados conforme informado nas linhas de descrição de mídia do SDP (“m=”). No H.245, M é dado pelo subconjunto de funcionalidades de terminais (*Terminal Capability Set* - TCS).
- Endereço de transporte de mídia (T): O endereço de transporte de mídia indica o endereço IP e o número da porta em que os pacotes RTP/RTCP

podem ser recebidos. Esta informação está disponível em “c=” e nas linhas “m=” do SDP e na mensagem canal lógico aberto do H.245.

Alice deve conhecer o A, o T e o M do João e o João precisa saber o T e o M da Alice. A dificuldade de tradução entre o SIP e o H.323 acontece porque o A, o M, e o T estão todos contidos na requisição SIP INVITE e na sua resposta, enquanto o H.323 pode espalhar estas informações entre diversas mensagens.

3.4.1 – Usando o H.323 *FastConnect*

Utilizando o H.323 *FastConnect*, a tradução do protocolo é simplificada porque há um mapeamento de um para um entre as mensagens de estabelecimento de chamadas H.323 e SIP. A mensagem de estabelecimento H.323 com *FastConnect* e a requisição SIP INVITE tem todas as três informações (A, M e T). Quando ocorrer uma chamada, a mensagem H.323 CONNECT com *FastConnect* e a resposta SIP 200, incluindo a descrição de sessão, têm todas as informações necessárias (M e T do destino da chamada).

Os cenários de chamada são apresentados nas Figura 3.7 e Figura 3.8.

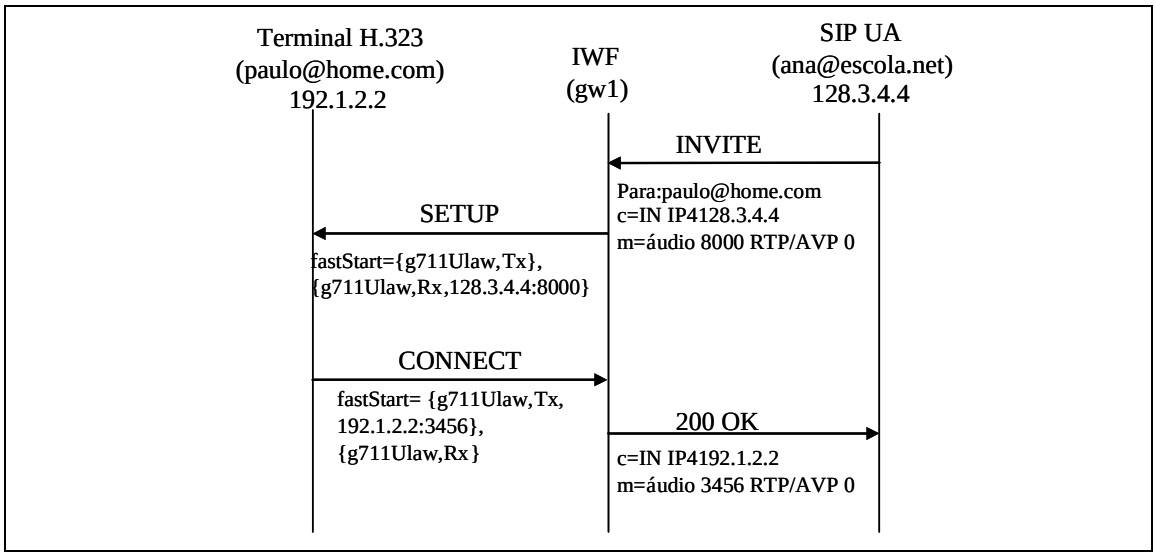


Figura 3.7 – Setup de uma chamada de um SIP UA para um terminal H.323 com FastConnect, adaptado de (Hersent, 2000).

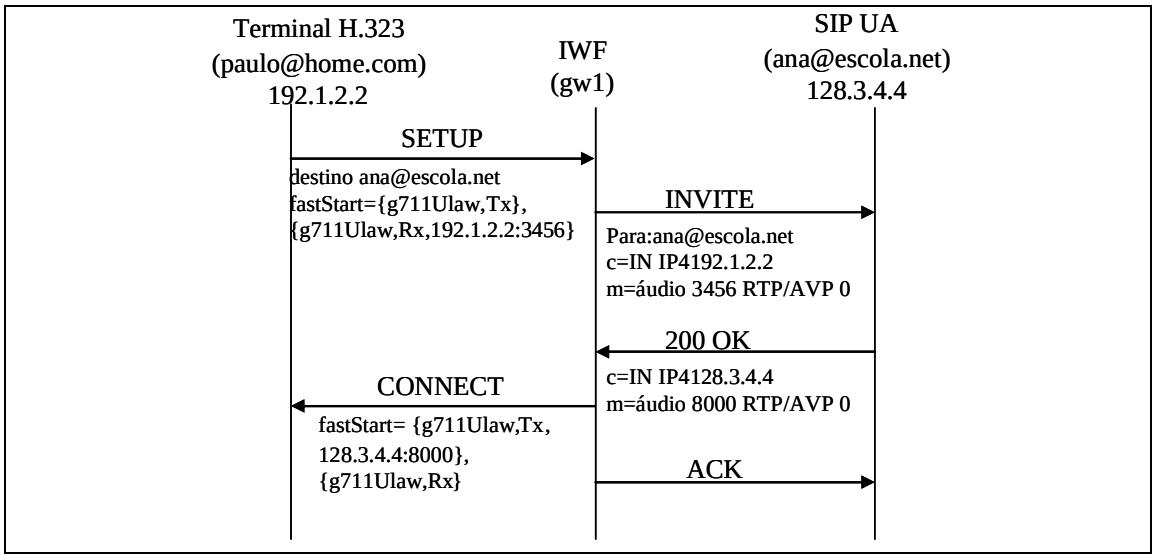
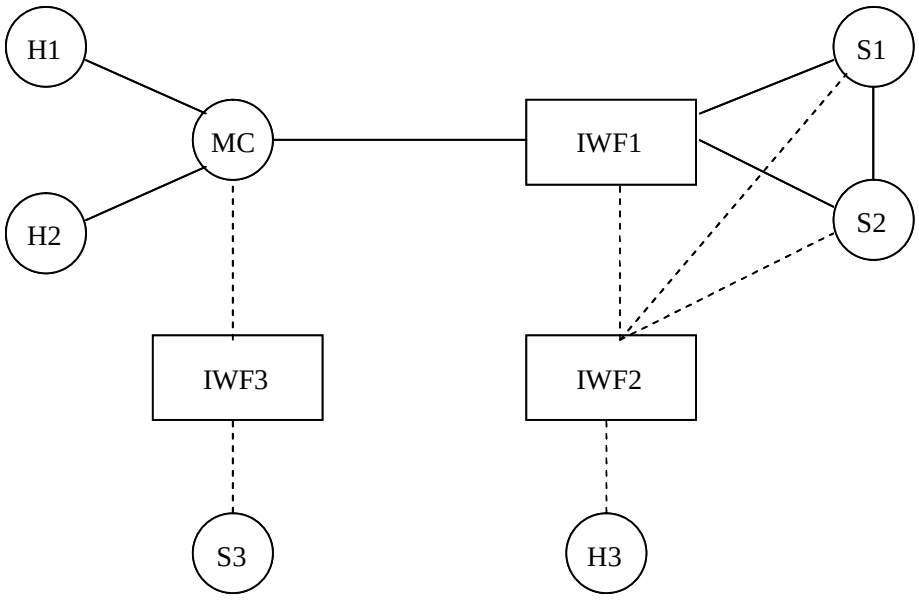


Figura 3.8 – Estabelecimento de uma chamada de um terminal H.323 para um SIP UA com FastConnect, adaptado de (Hersent, 2000).

3.4.2 – Tradução para uma Conferência

Um suporte transparente para uma conferência pode ser alcançado tendo nos terminais um IWF espelho em cada direção. A Figura 3.9 mostra um cenário em que dois terminais H.323 (H1 e H2) e dois SIP UAs (S1 e S2) estão participando de uma conferência.



Hn – terminais H.323 e Sn – terminais SIP

Figura 3.9 – Conferência ad hoc entre terminais SIP e H.323, adaptado de (Hersent, 2000).

Do lado H.323, a IWF1 parece um único terminal H.323. Do lado SIP, a IWF1 age como um único SIP UA.

Este método falha se S1 convida outro usuário H.323, no caso H3, através de uma entidade de interfuncionamento diferente (IWF2). Assim, o participante H2 não consegue saber quando H3 se junta à conferência. Alternativamente, se H1 convida um usuário SIP S3, S2 não saberá da presença de S3.

Uma forma para que os participantes saibam sobre a existência dos outros é contar com os pacotes RTP/RTCP. Isto vai contra a idéia da conferência H.323 onde as mensagens H.245 são usadas para saber da existência de novos participantes.

Este problema pode ser resolvido forçando todos os convites a passar através do IWF. A Figura 3.10 mostra uma conferência gerenciada por um MC onde os terminais H.323 estão diretamente conectados ao MC e os terminais SIP estão conectados através do IWF. Um terminal SIP somente pode convidar outro terminal SIP através do IWF, desta maneira o IWF pode atualizar o estado no MC.

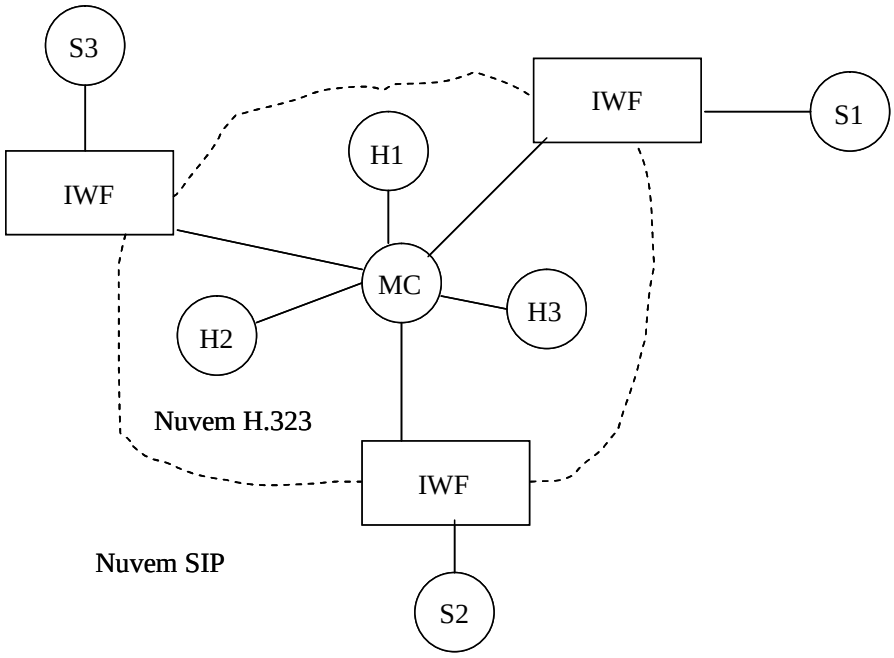


Figura 3.10 – Conferência centrada no H.323, adaptado de (Hersent, 2000).

Em uma arquitetura centrada no SIP, Figura 3.11, o terminal H.323 toma parte na conferência através do IWF.

Normalmente a arquitetura centrada no SIP é a mais recomendada, pois o modelo de conferência SIP é mais genérico, permitido conferências em malha completa com controle distribuído ou conferências centralizadas em MCUs.

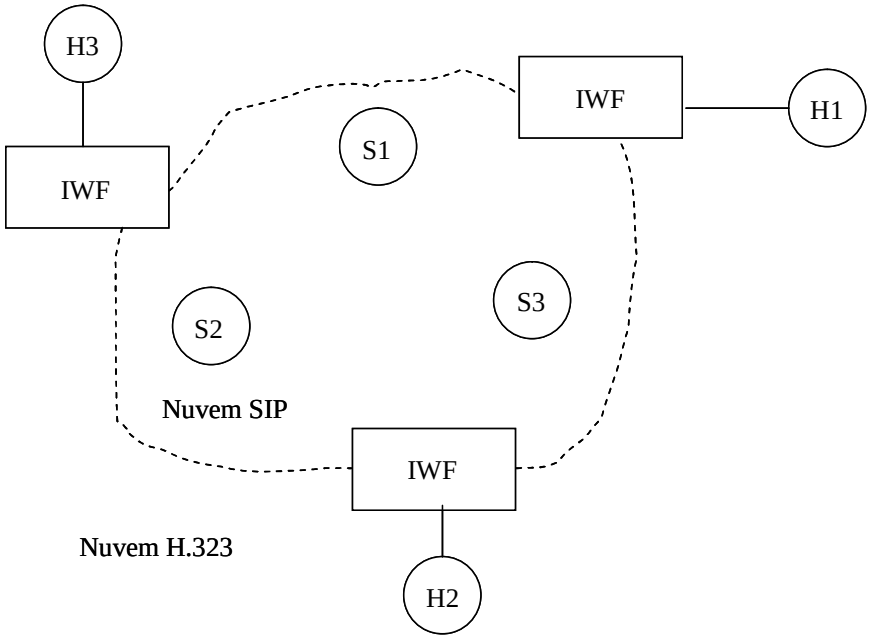


Figura 3.11 – Conferência centrada no SIP, adaptado de (Hersent, 2000).

Em geral, a tradução de serviços é muito simplificada se um operador adota um protocolo de sinalização como principal, com serviços oferecidos somente para este protocolo. Os terminais que usarem outro protocolo estarão restritos a fazerem chamadas através do IWF.

4 – DESCRIÇÃO DOS FRAMEWORKS DE CONFERÊNCIAS

O grupo de trabalho SIPPING do IETF definiu através da RFC 4245 (2005) os principais requisitos para uma conferência baseada em SIP e a partir deste documento o foi criado um *framework* para conferências baseado em SIP conforme definido na RFC 4353 (2006). Este documento gerou uma série de outras RFCs que especificam os protocolos, os cenários, o controle de chamada, entre outros.

O *framework* foi adotado pelo 3GPP e isto pode ser verificado no documento TS 24.147, tornando-se parte da arquitetura IMS e, portanto, o caminho de evolução para as redes de telecomunicações no que se refere à prestação do serviço de conferências. O TISPAN como pode ser observado no documento TS 183.005 também adotou o mesmo *framework* para suas conferências.

Todo este trabalho realizado pelo grupo de redes trata somente as conferências que utilizam SIP, porém existem outros protocolos que podem ser usados como H.323, Q.931, XMPP (*EXtensible Messaging and Presence Protocol* - RFC 3920 (2004), entre outros. Para ampliar a abrangência deste *framework*, outro grupo de trabalho do IETF denominado XCON (*Centralized Conferencing*) está descrevendo um modelo de arquitetura para a evolução dos sistemas de conferência que permita a utilização de vários protocolos e não somente o SIP.

O trabalho do XCON reúne uma grande quantidade de *Drafts*, cujo principal "*A Framework for Centralized Conferencing*" define o *framework* para conferências centralizadas e trata tanto SIP como os demais protocolos de sinalização de chamada.

O *framework* de conferência centralizada ainda não está totalmente definido e padronizado, tendo ainda muitos pontos em aberto, mesmo assim um grupo de pesquisadores da Universidade de Nápoles está questionando o seu desempenho e a sua escalabilidade. Este grupo baseia os seus questionamentos na comparação dos resultados de testes realizados com uma implementação do *framework* de conferência centralizada, com testes realizados com um *framework* para conferência distribuída, criado por eles.

Este *framework* de conferência distribuída, chamado DCON (*Distributed Conferencing*) definido no *Draft* "*A Framework for Distributed Conferencing*" (2007), está sendo desenvolvido utilizando como base o *framework* XCON e propondo novos elementos e novos protocolos para administrar uma conferência distribuída. O resultado do trabalho do grupo DCON foi apresentado e está sendo examinado pelo XCON através da submissão de três *drafts* ao IETF.

A seguir serão descritos o *framework* baseado em SIP por ser o mais definido e base para os demais, e também os dois *framework*s, tanto o centralizado (XCON) quanto o descentralizado (DCON).

4.1 – Terminologia

Nesta seção são apresentados os principais termos que serão utilizados nesta dissertação para descrever tanto o *framework* baseado em SIP como os demais *framework*s, em conformidade com o que está definido nas referências (RFC 4353, 2006) e (*Draft* "*A Framework for Centralized Conferencing*", 2007).

- Conferência: Conferência é um termo muito usado que tem significados diferentes em contextos diferentes. Para estes *frameworks* uma conferência é uma instância de uma comunicação multi-usuário.
- Conferência ativa: O termo conferência ativa se refere a um objeto de conferência que foi criado e ativado pela distribuição de seus identificadores (e.g. identificador de objeto de conferência e identificador de conferência) e do *focus* associado. Uma conferência ativa é criada baseada em um projeto padrão de conferência pré-definido ou uma reserva de conferência específica.
- Conferência cascateada: É um mecanismo para comunicações de grupo no qual um conjunto de conferências estão conectadas tendo seus *focus* interagindo de alguma maneira.
- Conferência cascateada simplex: É um grupo de conferências que estão conectadas, sendo que o UA (*User Agent*) que representa o *focus* de uma conferência é um participante conferência-desavisado em outra conferência.
- Conferência fortemente associada: Uma conferência fortemente associada é uma conferência na qual um único UA, chamado de *focus*, mantém um diálogo com cada participante, ou seja, para a sinalização é uma topologia em estrela. O *focus* faz o papel do gerente centralizado da conferência e é endereçado através de um URI (*Universal Resource Identifier*) da conferência.
- Conferência livremente associada: Uma conferência livremente associada é uma conferência sem relações de sinalização coordenadas entre os participantes. Conferências livremente associadas freqüentemente usam *multicast* para distribuição de convites para a conferência.

- Convite em massa: Uma tentativa de adicionar um grande número de clientes em uma conferência.
- Estado da conferência: O estado da conferência inclui o estado do *focus*, o conjunto de participantes conectados à conferência e o estado dos respectivos diálogos deles.
- Expulsão em massa: Uma tentativa de remover um grande número de clientes de uma conferência.
- Fábrica de conferências: Uma fábrica de conferências é uma entidade lógica que gera um URI(s) único para identificar e representar um *focus*.
- *Focus*: Um *focus* é uma entidade lógica que mantém a interface de sinalização de chamada com cada participante e com o objeto de conferência que representa o estado ativo. Como tal, o *focus* age como um terminal para cada um dos protocolos de sinalização suportados e é responsável por todas as operações primárias da conferência como unir, sair, atualizar a instância de conferência, etc. e para negociação/manutenção de mídia entre um participante da conferência e o *focus*.
- Gráfico de mídia: O gráfico de mídia é a representação lógica do fluxo de mídia para uma conferência.
- Identificador de conferência: Um identificador de conferência é um URI específico que identifica um *focus* de conferência e a instância de conferência associada.
- Identificador de objeto de conferência: Um identificador de objeto de conferência é um URI que identifica, de forma unívoca, um objeto de conferência e é usado por um protocolo de controle de conferência para acessar e modificar a informação de conferência.
- Identificador de usuário de conferência: Um identificador único para um usuário dentro de um sistema de conferência. Um usuário pode ter vários identificadores de usuário de conferência dentro de um sistema de conferência (e.g. para representar papéis diferentes).
- Informação de conferência: A informação de conferência inclui definições de características básicas da conferência, como identificadores de conferência, sinalização, capacidades e tipos de mídia, aplicáveis a uma ampla gama de aplicações de conferência. A informação de conferência também inclui as mídias e dados específicos de aplicações avançadas de conferência, como misturadores de mídia. A informação de conferência é o dado escrito por um objeto de conferência.

- Instância de conferência: Uma instância de conferência se refere a uma implementação interna de uma conferência específica, representada como um conjunto de objetos de conferência lógicos e os identificadores associados.
- Líder da sala: Um líder de sala é um cliente compatível com o protocolo de controle de sala, ou um participante humano ou uma entidade automatizada, que esta autorizado a administrar o acesso a uma sala e pode conceder, negar ou revogar o acesso. O líder de sala não tem que ser um participante da instância de conferência.
- Misturador de mídia: Um misturador de mídia é a entidade lógica com capacidade para combinar contribuições de mídia do mesmo tipo, transcodificar as mídias e distribuir o resultado para um ou mais destinos. Neste contexto, o termo "mídia" significa qualquer tipo de dado sendo entregue pela rede usando os meios de transporte apropriados, como RTP/RTCP ou *Message Session Relay Protocol* definido em (RFC 4975, 2007).
- Objeto de conferência: Um objeto de conferência representa uma conferência em certo estágio (e.g. descrição da criação da conferência, reserva, ativação, etc.) que um sistema de conferência mantém com o objetivo de descrever as capacidades de sistema e prover acesso para os serviços disponível para cada objeto independentemente. O esquema de objeto de conferência está baseado na informação de conferência.
- Papel: Um papel provê o contexto para o conjunto de operações de conferência que um participante pode executar. Um papel básico (e.g. o participante da conferência padrão) sempre existirá, proporcionando ao usuário um conjunto básico de operações da conferência básico. Baseado em um sistema de autenticação e autorização específico, um usuário pode assumir papéis alternados, como moderador da conferência, permitindo acesso a um conjunto mais amplo de operações da conferência.
- Participante: O elemento de software que conecta um usuário ou máquina a uma conferência. Ele implementa, no mínimo, um UA SIP, mas também pode implementar mecanismos não-SIP (baseados em protocolos diferentes do SIP) para funcionalidades adicionais.

- Participante anônimo: Um participante anônimo é aquele que os outros participantes sabem que ele existe pelo serviço de notificação de conferência, mas a identidade não é divulgada.
- Participante conferência-desavisado: Um participante conferência-desavisado é um participante de uma conferência que não está consciente de que está em uma conferência. Para o participante é uma chamada ponto-a-ponto.
- Participante conferência-atento: Um participante conferência-atento é um participante em uma conferência que aprendeu, por meios automatizados, que está em uma conferência. Um participante conferência-atento pode usar o serviço de notificação de conferência ou mecanismos não-SIP para obter funcionalidades adicionais.
- Políticas de conferência: Políticas de conferência se referem a um conjunto de direitos, permissões e limitações que pertencem a operações que são executadas em certo objeto de conferência.
- Projeto de conferência: Um projeto de conferência é um objeto de conferência estático, pré-definido, construído dentro de um sistema de conferências, o qual descreve uma conferência típica com parâmetros que o sistema suporta. Um projeto de conferência é a base para criação de objetos de conferência dinâmicos. Um sistema pode ter vários projetos. Cada projeto contém valores iniciais e o conjunto de valores nos quais os elementos do objeto podem excursionar, em conformidade com os esquemas de dados da conferência.
- Protocolo de controle de conferência (*Conference control protocol* - CCP): Um protocolo de controle de conferência provê a interface para manipulação de dados e recuperação de estado para os dados da conferência, representados pelo objeto de conferência.
- Protocolo de sinalização de chamada: O protocolo de sinalização de chamada é usado entre um participante e um *focus*. Neste contexto, o termo "chamada" significa um canal ou uma sessão usados para fluxos de mídia.
- Reserva de conferência: Uma reserva de conferência é um objeto de conferência que é criado de um sistema padrão ou de um projeto de conferência selecionado pelo cliente.
- Sala: O conceito de sala utilizado nestes *frameworks* é referente a um conjunto de dados ou recursos associados com uma instância de conferência, para o qual um

participante de conferência ou grupo de participantes, tem acesso temporário concedido.

- Servidor de conferência: Um servidor de conferência é um servidor físico que contém, no mínimo, o *focus*. Também pode incluir um servidor de política de conferência e misturadores.
- Serviço de notificação da conferência: Um serviço de notificação da conferência é uma função lógica provida pelo *focus*. O *focus* pode agir como um servidor de notificação, aceitando subscrições ao estado da conferência e notificando os subscritores sobre mudanças para aquele estado.
- Servidor de política de conferência: Um servidor de política de conferência é uma função lógica que pode armazenar e manipular a política de conferência. Esta função lógica não é especificamente SIP e pode não existir fisicamente. Ela se refere ao componente que conecta um protocolo à política de conferência.
- *Sidebar*: Um *sidebar* é uma instância de conferência separada que só existe dentro do contexto de uma instância de conferência "mãe". O objetivo de um *sidebar* é poder prover mídias adicionais ou alternadas somente para participantes específicos.
- Sistema de conferência: O sistema de conferência se refere a uma solução de conferência baseada no modelo de dados apresentado por este *framework* e construído usando os protocolos definidos por este *framework*.
- Sussurro: Um sussurro envolve uma única entrada de mídia de um participante específico dentro de uma instância de conferência específica, usando um *sidebar* já criado. Um exemplo de um sussurro seria um anúncio injetado somente para o líder da conferência ou para um novo participante que se une a conferência.
- URI da conferência: Um URI, normalmente um SIP URI, identifica o *focus* de uma conferência.

4.2 – *Framework* SIP

Conforme apresentado no capítulo 3 o SIP suporta o início, a modificação e terminação das sessões de mídia entre UAs (*User Agent*). Estas sessões são realizadas através de diálogos SIP que representam um relacionamento SIP entre um par de UAs.

Como os diálogos são sempre entre pares de UAs, o uso do SIP em comunicações ponto a ponto (como um telefonema), é óbvio. Porém, sessões de comunicações com participantes múltiplos são mais complicadas.

O SIP pode suportar muitos modelos de comunicações multiponto. Um deles, chamado conferências livremente associadas, utiliza grupos de mídia *multicast*. No modelo livremente associado, não há nenhuma relação de sinalização entre os participantes na conferência. Não há nenhum ponto central de controle ou servidor de conferência. A participação é gradualmente instruída por informações de controle passadas como parte da conferência, uma das formas é usando o RTCP. As conferências livremente associadas são facilmente suportadas pelo SIP usando endereços *multicast* dentro de suas descrições de sessão.

Em outro modelo, chamado conferência multiponto completamente distribuída, cada participante mantém uma relação de sinalização com os outros participantes, usando SIP. Novamente, não há nenhum ponto central de controle. O controle é completamente distribuído entre os participantes. Nesta dissertação este tipo de conferência não será tratado porque exige que pelo menos um dos equipamentos de cliente, que participam da conferência, tenha capacidade de misturar os fluxos de mídia. A maioria dos equipamentos de clientes não possui esta capacidade. Além disso, nesta conferência o cliente responsável por misturar as mídias irá receber os fluxos de todos os demais participantes, exigindo um acesso com uma largura de faixa capaz de suportar todo esse tráfego.

Em um terceiro modelo chamado conferência fortemente associada, há um ponto central de controle. Cada participante se conecta a este ponto central. Ele provê uma variedade de funções de conferência e pode executar a função de misturar as mídias. As conferências fortemente associadas não são tratadas diretamente pela RFC 3261, embora uma participação básica seja possível sem qualquer apoio de protocolo adicional.

A seguir será apresentado o *framework* para uma conferência SIP fortemente associada, simplesmente referida deste ponto em diante como "conferência". Este *framework* apresenta um modelo de arquitetura geral para estas conferências, além de apresentar as formas que o próprio SIP é envolvido na conferência. O objetivo do *framework* é satisfazer os requerimentos para conferência definidos na RFC 4245 (2005).

4.2.1 – Elementos do *Framework*

A lista a seguir apresenta os principais elementos do *framework*:

- *Focus*: É o centro da conferência. É nele que são conectados todos os participantes da conferência através de um diálogo SIP. O *focus* é o responsável por assegurar que os diálogos estão conectando um grupo de participantes, cujo acesso a conferência foi permitido conforme definição da política. O *focus* também usa o SIP para manipular as sessões de mídia, com o objetivo de ter certeza que cada usuário obtenha todas as mídias necessárias para participar da conferência. Para fazer isto o *focus* utiliza os misturadores.
- Servidor de Política de Conferência: É um componente lógico do sistema. Ele representa a interface entre os clientes e a política de conferência que governa a operação da conferência. Os clientes se comunicam com o servidor de política de conferência usando um mecanismo não-SIP.
- Misturadores: É responsável por combinar os fluxos de mídia que compõem a conferência e gerar um ou mais fluxos que serão distribuídos para os participantes ou para outros misturadores. O processo de combinar a mídia é específico para cada tipo de mídia e é definido pelo *focus* de acordo com as regras descritas na política de mídia. Um misturador sempre é controlado por um *focus*.
- Serviço de Notificação da Conferência: O *focus* pode prover um serviço de notificação da conferência. Neste papel, ele age como um servidor de notificação como definido na RFC 3265 (2002). Ele aceita solicitações de clientes para o URI da conferência e gera notificações para eles com o estado das mudanças da conferência.
- Participantes: Um participante em uma conferência é qualquer UA SIP que tem um diálogo com o *focus*. Este UA SIP pode ser uma aplicação em um computador, um telefone SIP ou um gateway da rede de telefonia. Além destes, outro *focus* também pode ser um participante. Uma conferência que tem um participante que é *focus* de outra conferência é chamada de conferência em cascata.
- Política de Conferência: Contém as regras que guiam a operação do *focus*. As regras podem ser simples, como uma lista de acesso que define um conjunto de participantes que podem participar de uma conferência. Também podem ser complexas, especificando regras de participação

baseadas em hora do dia, condicionadas a presença de outros participantes. É importante entender que não há nenhuma restrição no tipo de regra que pode estar contida em uma política de conferência.

4.2.2 – Visão Geral da Arquitetura

O elemento central de uma conferência SIP é o *focus*. O *focus* mantém um relacionamento, através de sinalização SIP, com cada participante da conferência. O resultado é uma topologia em estrela, como apresentado na Figura 4.1.

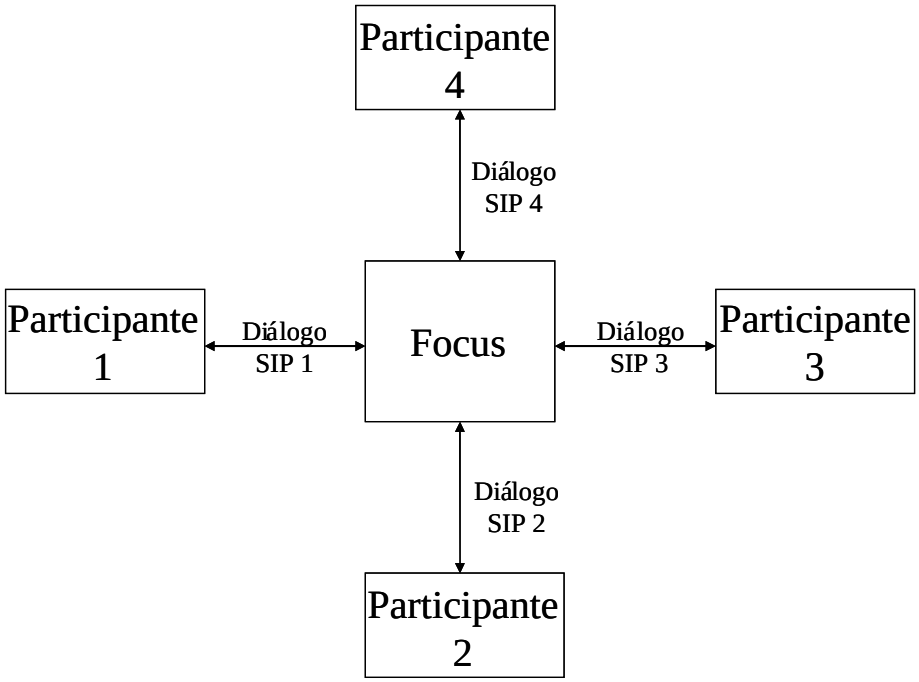


Figura 4.1 – Arquitetura da conferência SIP, adaptado de (RFC 4353, 2006).

O *focus* é responsável por garantir que os fluxos de mídia que formam a conferência estão disponíveis aos participantes da conferência. Isto é possível através do uso de um ou mais misturadores de mídia, onde cada um deles combina vários fluxos de mídia para produzir um ou mais fluxos de mídia. O *focus* usa as definições da política de conferência para mídia para determinar a configuração mais apropriada para os misturadores.

O *focus* tem acesso à política de conferência, uma instância que existe para cada conferência. Efetivamente, a política de conferência pode ser pensada como um banco de dados que descreve de que forma a conferência deve operar. É responsabilidade do *focus*

forçar estas políticas. O *focus* necessita ter acesso ao banco de dados e também precisa saber quando alguma coisa mudou. Tais mudanças podem resultar em sinalização SIP (por exemplo, a exclusão de um usuário da conferência usando BYE) e as mudanças que afetam o estado de conferência exigirão o envio de uma notificação para os participantes usando o serviço de notificação da conferência.

A conferência é representada por um URI que identifica o *focus*. Cada conferência tem um *focus* único com um URI único que o identifica. As requisições para um URI da conferência são roteadas para o *focus* daquela conferência específica.

Clientes normalmente se integram a conferência enviando um INVITE ao URI da conferência. Desde que a política de conferência permita, o INVITE é aceito pelo *focus* e o usuário é admitido na conferência. Os clientes podem sair da conferência enviando um BYE, como é feito em uma chamada comum.

De maneira similar, o *focus* pode terminar um diálogo com um participante. Quando isto ocorrer, a política de conferência deve mudar para indicar que o participante já não faz parte da conferência. O *focus* também pode iniciar um INVITE para trazer um participante para a conferência.

O conceito de participante conferência-desavisado é importante neste *framework*. Um participante conferência-desavisado nem mesmo sabe que o UA com o qual está se comunicando vem a ser um *focus*. Até onde ele sabe, o UA é como qualquer outro UA. O *focus*, logicamente, sabe que é um *focus* e executa as tarefas necessárias para a conferência funcionar.

Os participantes conferência-desavisados têm acesso a várias funcionalidades da conferência. Eles podem entrar e sair das conferências SIP e obtêm acesso a funcionalidades mais avançadas através de *stimulus signaling*, descrito no *Draft A Framework for Application Interaction in the SIP* (2005). Porém, se os participantes desejarem explicitar aspectos de controle de conferência usando protocolos de sinalização funcionais, somente poderão fazer isso os participantes conferência-atento.

Um participante conferência-atento tem acesso a funcionalidades avançadas através de interfaces de protocolo adicionais, que podem incluir acesso à política de conferência através de mecanismos não-SIP específicos. Um modelo para esta interação é apresentado na Figura 4.2. O participante pode interagir com o *focus* usando extensões, como REFER para acessar funções de controle de chamada mais sofisticadas (RFC 4579, 2006).

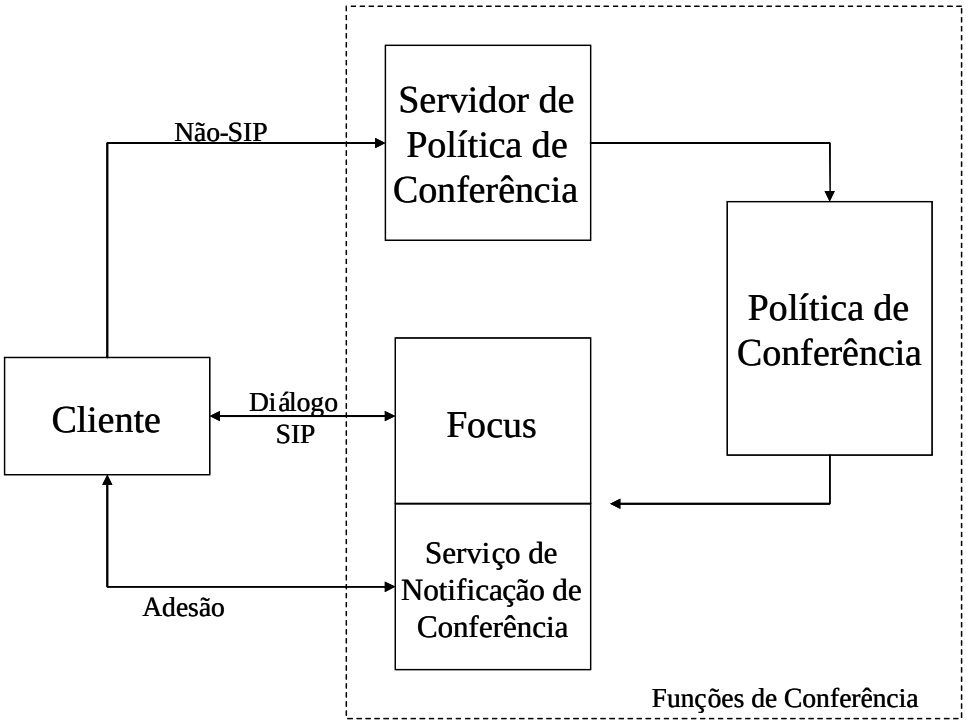


Figura 4.2 – Modelo de interação, adaptado de (RFC 4353, 2006).

O participante conferência-atento pode enviar um SUBSCRIBE ao URI da conferência e ser conectado ao serviço de notificação da conferência provido pelo *focus*. Através deste mecanismo, pode aprender sobre mudanças dos participantes e saber qual o efetivo estado dos diálogos e das mídias.

O participante pode se comunicar com o servidor de política de conferência usando algum tipo de mecanismo não-SIP através do qual ele pode alterar a política de conferência. O servidor de políticas de conferência não precisa estar disponível em uma conferência em particular, embora sempre exista uma política de conferência para a mesma.

As interfaces entre o *focus* e a política de conferência, e entre o servidor de política de conferência e a política de conferência são não-SIP. No caso de conferências baseadas em SIP, eles representam papéis lógicos em uma conferência, ao invés de representar elementos físicos. A separação destas funções é utilizada para esclarecer o entendimento e os requerimentos. Esta abordagem provê as implementações SIP individuais, a flexibilidade para compor um sistema de conferência escalável e robusto sem necessitar o desenvolvimento completo destas interfaces.

É fundamental para este *framework* que uma conferência seja identificada de forma unívoca por um URI, e que este URI identifique o *focus* que é responsável pela

conferência. O URI da conferência é único, ou seja, não existem duas conferências com o mesmo URI. Um URI da conferência é sempre um SIP ou SIP*Security* URI (SIP TLS - *Transport Layer Security*).

O URI da conferência é uma caixa preta para qualquer participante. Não há como saber com certeza se o URI identifica um *focus*, ou um usuário, ou ainda, uma interface de um *gateway* da rede de telefonia pública comutada. Isto está alinhado com a filosofia geral de uso do URI (RFC 3986, 2005). Porém, a informação contextual que cerca o URI (por exemplo, parâmetros de cabeçalho do SIP) pode indicar que o URI representa uma conferência.

Quando uma requisição SIP é enviada para o URI da conferência, a requisição é roteada para o *focus*, e somente para o *focus*. O elemento ou sistema que criou o URI da conferência é o responsável por garantir esta propriedade.

O URI da conferência pode representar uma conferência permanente (que se repete com alguma periodicidade definida pelo cliente) ou grupo de interesse, como "sip:discussão-sobre-futebol@exemplo.com". O *focus* identificado por este URI sempre existiria e a conferência sempre seria administrada por algum participante que estivesse fazendo parte da conferência naquele momento. Outros URIs de conferência podem representar conferências efêmeras, como uma conferência *ad hoc*.

O URI da conferência pode ser enviado em um e-mail ou em uma mensagem instantânea. O URI da conferência também pode ser obtido em uma página *Web* ou através de algum mecanismo não-SIP.

Para determinar que um URI representa um *focus* podem ser usadas técnicas padronizadas. Especificamente, a RFC 3840 (2004) provê o "*isfocus*" que é uma etiqueta para indicar que o UA está agindo como *focus* neste diálogo. Também são usados outros parâmetros desta RFC para indicar que um *focus* suporta o serviço de notificação de conferência. Isto é feito declarando o suporte ao método SUBSCRIBE e aos pacotes pertinentes, nos parâmetros de preferências do chamador associados com o URI da conferência.

Outras funções em uma conferência podem ser representadas por URIs. Se a política de conferência estiver exposta através de uma aplicação *Web*, ela é identificada por um URI HTTP. Se ela é acessada usando um protocolo explícito, o URI terá sido definido por aquele protocolo.

4.2.3 – Operações Comuns

Os clientes podem interagir com uma conferência de várias formas. Eles podem entrar, sair, definir políticas, aprovar participantes, e assim por diante. Nesta seção serão mostradas as operações mais significativas da conferência, mostrando resumidamente como elas acontecem. Exemplos mais detalhados dos mecanismos SIP podem ser encontrados na RFC 4579 (2006). A lista com as principais operações comuns:

- Criar uma conferência;
- Adicionar participantes;
- Remover participantes;
- Terminar a conferência;
- Obter informações dos participantes;
- Adicionar e remover mídia;
- Anúncios e gravações;

4.2.4 – Realização Física

Nesta seção, serão apresentadas várias instâncias físicas dos componentes para mostrar como estas funções básicas podem ser combinadas para resolver uma variedade de problemas.

4.2.4.1 – Servidor Centralizado

Na realização mais simplista do *framework* SIP, há um único servidor físico na rede que implementa o *focus*, o servidor de políticas de conferência e os misturadores. Esta é clássica solução "*one box*", é apresentada pela Figura 4.3.

Esta implementação, apesar de ser a mais comum, pode não ser a mais adequada para uma operadora de telecomunicações, porque, normalmente, a operadora distribui geograficamente os seus misturadores para evitar que a mídia percorra grandes distâncias dentro da rede. Esta solução "*one box*" torna esta estratégia economicamente mais onerosa, pois, ao invés do focus estar em um ponto centralizado e controlar vários misturadores, tem-se vários focus controlando apenas um misturador.

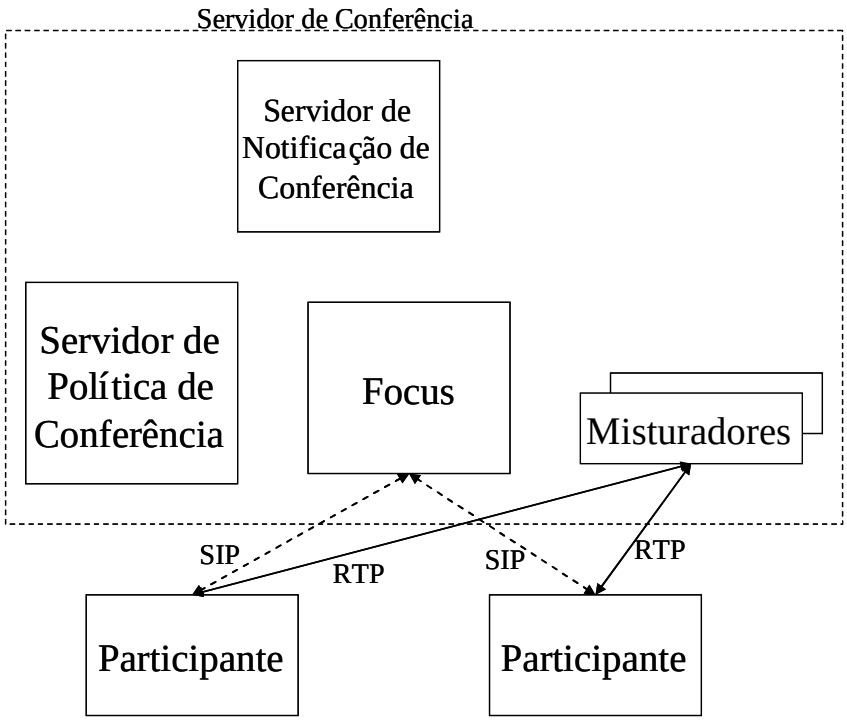


Figura 4.3 – Conferência em um único servidor, adaptado de (RFC 4353, 2006).

4.2.4.2 – Servidor de Terminais

Outro modelo importante é aquele em que uma conferência *ad hoc* é misturada localmente. Neste cenário, dois clientes (A e B) estão em uma chamada ponto a ponto. Um dos participantes (A) decide colocar na conferência um terceiro participante, C. Para fazer isto, A começa a agir como um *focus*. O diálogo existente com B se torna o primeiro diálogo com o *focus*. Então, é enviado um re-INVITE para B mudando seu URI de contato para um novo URI que identifica o *focus*. Essencialmente, A se transforma de um simples usuário (UA) para um *focus* mais um UA, e neste processo de transformação o URI também muda. Então, o *focus* faz um INVITE para C. Quando C aceitar, A irá misturar as suas mídias junto com as de B e C, e redistribuirá os resultados. A Figura 4.4 mostra um diagrama desta transição.

Este modelo funciona somente para conferências de pequeno porte e exige que os equipamentos de cliente tenham capacidade de misturar mídia. Isto aumenta muito o custo do equipamento, e exige que o cliente, que está fazendo o papel de misturador, tenha uma faixa de acesso capaz de suportar o tráfego de todos os fluxos de mídia enviados pelos outros participantes.

Na maioria dos casos, este modelo é usado por empresas em seus sistemas de conferências corporativas. Em serviços de videoconferência prestados por operadoras de telecomunicações este modelo não é estimulado, porque a operadora não tem o controle da conferência, desta forma, não consegue oferecer os recursos mais sofisticados, como agendamento, *chat*, gravação, entre outros.

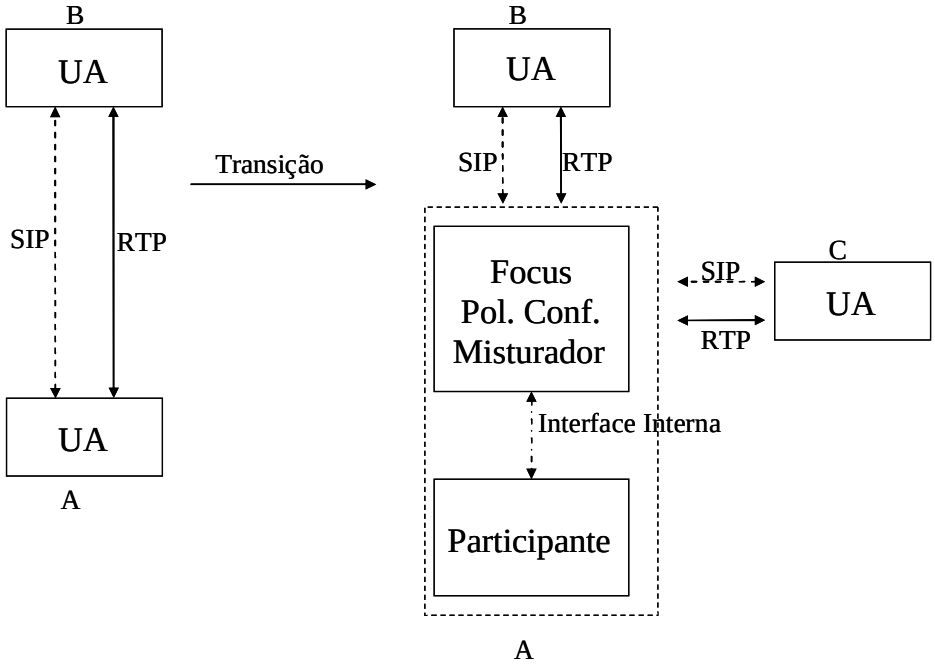


Figura 4.4 – Diagrama de transição, adaptado de (RFC 4353, 2006).

É importante notar que as interfaces externas neste modelo, entre A e B, e entre B e C, são exatamente as mesmas que seriam usadas em um modelo de servidor centralizado. O usuário A também poderia implementar uma política de conferência e um serviço de notificação de conferência, permitindo aos participantes ter acesso a eles. Porque o *focus* é o co-residente com um participante não significa que qualquer aspecto do comportamento e das interfaces externas irá mudar.

4.2.4.3 – Servidor de Mídia

No modelo representado na Figura 4.5, cada conferência envolve dois servidores centralizados.

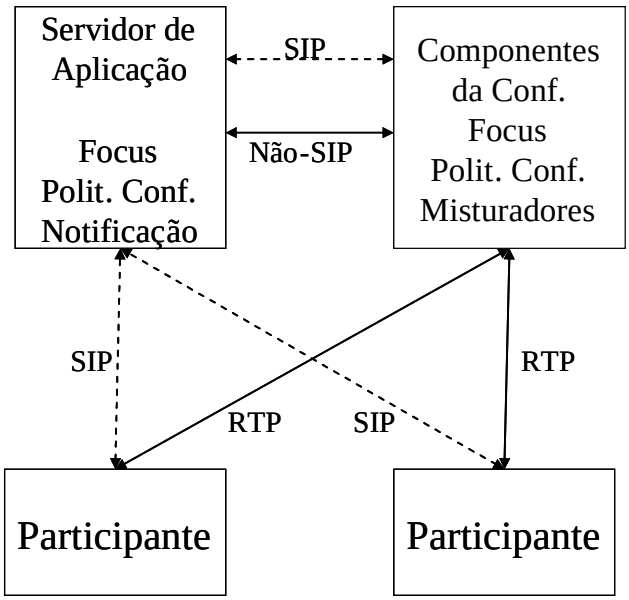


Figura 4.5 – Conferência com dois servidores centralizados, adaptado de (RFC 4353, 2006).

Um destes servidores, chamado “servidor de aplicação” possui e administra os participantes e as políticas de mídia, além de manter um diálogo com cada participante. Desta forma ele representa o *focus* visto por todos os participantes da conferência.

Entretanto, este servidor não provê suporte de mídia. Para executar a função de misturador de mídia, é utilizado um segundo servidor, chamado misturador. Este servidor inclui um *focus* e implementa uma política de conferência, mas não tem nenhum serviço de notificação de conferência. Sua política de conferência diz que ele deve aceitar todos os convites de *focus* de alto nível. O *focus* no servidor de aplicação usa controle de chamada de terceiros para conectar os fluxos de mídia de cada usuário ao servidor de mistura, quando for necessário. Se o *focus* no servidor de aplicação recebe um comando de controle de política de conferência de um cliente, ele delega isso ao servidor de mídia, e faz o mesmo para um comando de controle de política de mídia.

Este modelo permite que o servidor de mistura seja usado como um recurso para uma variedade de aplicações de conferência diferentes. Isto acontece porque ele é somente um “escravo” do servidor de nível mais alto fazendo tudo o que lhe é solicitado.

4.2.4.4 – Misturadores distribuídos

Mesmo em uma conferência onde os misturadores estão distribuídos, ainda existe um servidor centralizado que implementa o *focus*, o servidor de política de conferência e o servidor de política de mídia. Porém, não há nenhum misturador centralizado. Entretanto, há misturadores em cada terminal, junto com um servidor de política de conferência. O *focus* distribui as mídias usando controle de chamada de terceiro (RFC 3725, 2004) para mover um fluxo de mídia de cada participante para o outro participante. Como resultado, se houver *n* participantes em uma conferência, haverá um único diálogo entre cada participante e o *focus*, mas a descrição de sessão associada com aquele diálogo será construída para permitir a distribuição de mídia entre os participantes. A Figura 4.6 apresenta a conferência com misturadores de mídia distribuídos.

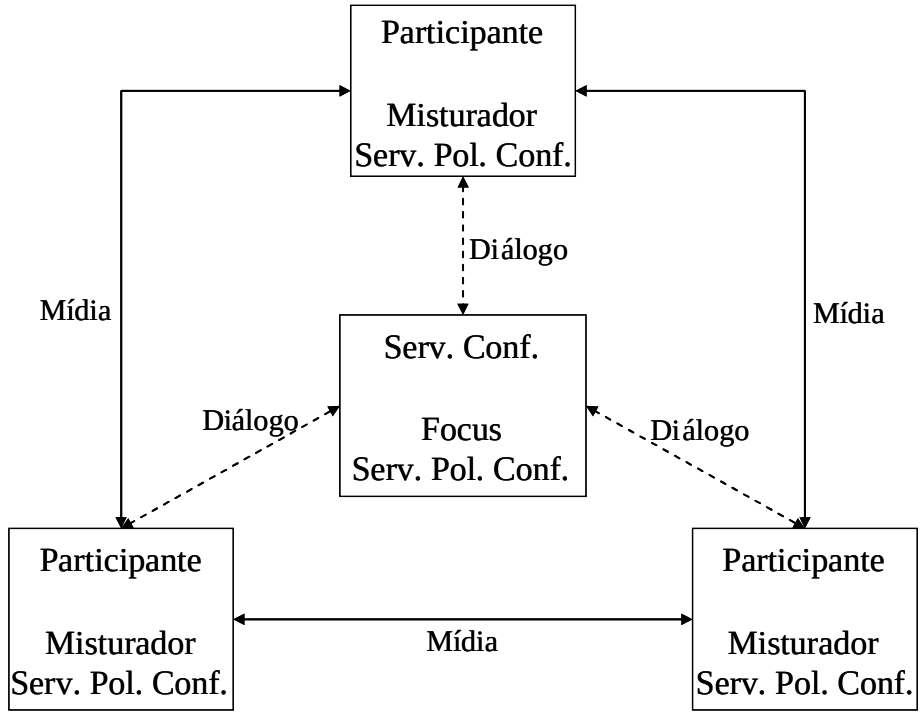


Figura 4.7 – Conferência com misturadores de mídia distribuídos, adaptado de (RFC 4353, 2006).

A distribuição da mídia para cada participante misturar pode ser feita de várias formas. Em um modelo *multi-unicast*, cada participante envia uma cópia de suas mídias para os outros participantes. Neste caso, a descrição de sessão administra *n*-1 fluxos de mídia.

Em um modelo de *multicast*, cada participante se une a um grupo *multicast* comum e cada participante envia uma única cópia de seu fluxo de mídia àquele grupo. A infra-estrutura de *multicast* distribui as mídias de forma que cada participante receba uma cópia.

Em um modelo de *multicast* de fonte única, cada participante envia seus fluxos de mídia a um ponto central usando *unicast*. O ponto central redistribui as mídias para todos os participantes usando *multicast*.

O *focus* é responsável por selecionar uma modalidade de distribuição de mídia, e por controlar qualquer modelo híbrido que seja necessário, dependendo das capacidades dos clientes de misturar as mídias.

Quando um novo participante se une ou é adicionado, o *focus* executará o controle de chamada de terceiros necessário, para distribuir as mídias do novo participante para todos os outros participantes, e vice-versa.

O servidor de conferência central também expõe uma interface para a política de conferência. Obviamente, o servidor de conferência central não pode implementar diretamente nenhuma das operações de mídia ou políticas. Ele delega a implementação a cada participante. Assim, se um participante decide trocar o modo de conferência global de "ativado por voz" para "presença contínua", ele irá se comunicar com o servidor de política de conferência central. Por sua vez, o servidor de política de conferência comunicaria aos servidores de política de conferência que são co-residente com cada participante, usando algum mecanismo não-SIP e instruiria para que eles usassem "presença contínua".

Este modelo requer funcionalidades adicionais em UAs que podem ou não estar presentes. Logo, os participantes devem ser capazes de anunciar estas capacidades ao *focus*.

4.2.4.5 – Misturadores cascateados

Em conferências em que o número de participantes é maior do que o número de fluxos de mídia que um único misturador pode tratar simultaneamente, é necessário o uso de misturadores cascateados. Nesta arquitetura, há um *focus* centralizado, mas a função de misturador é implementada por vários misturadores, espalhados ao longo da rede. Cada participante é conectado a um único misturador. O *focus* usa algum tipo de protocolo de controle (não definido pelo *framework* SIP) para conectar os misturadores, de forma que

todos os participantes podem ver/ouvir um ao outro. Esta arquitetura é representada na Figura 4.7.

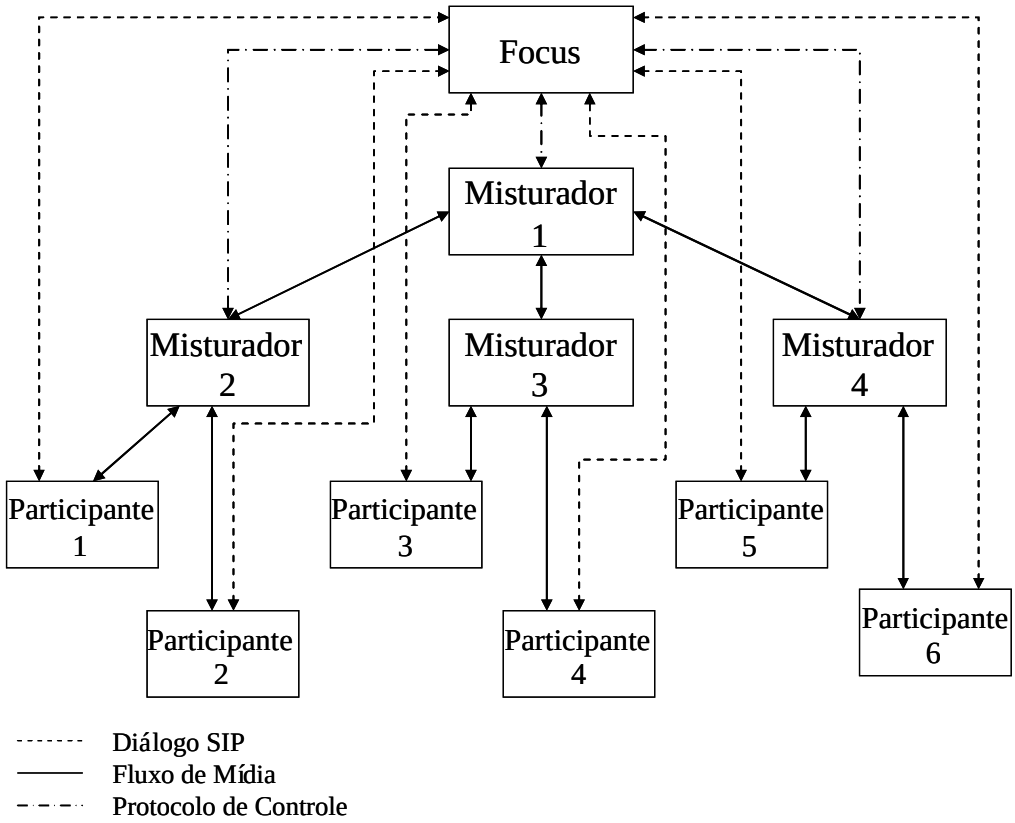


Figura 4.7 – Conferência com misturadores cascateados, adaptado de (RFC 4353, 2006).

4.3 – *Framework* de Conferência Centralizada

Esta seção descreve o *framework* para conferência centralizada criado pelo grupo de trabalho do ETSI chamado XCON. Este *framework* permite que clientes usando vários protocolos de sinalização de chamada, como SIP, H.323, XMPP, Q.931 ou ISUP, participem de uma mesma conferência centralizada.

Este *framework* define entidades lógicas e nomeia convenções dentro de um modelo de dados de conferência. Ele também esboça um conjunto de protocolos de conferência, que são complementares aos protocolos de sinalização de chamada, para tornar possível a construção de aplicações avançadas de conferência.

De acordo com as definições do XCON, este *framework* é compatível com o *framework* de conferências SIP apresentado na seção 4.2.

4.3.1 Visão Geral

Uma conferência centralizada é uma associação de terminais, que são chamados de participantes de conferência, com o *focus* da conferência. Esta relação é exatamente igual a que ocorre no *framework* SIP, e da mesma forma a topologia da conferência, no que se refere à sinalização de chamada, é uma estrela.

Além das funcionalidades básicas de conferência, o *framework* centralizado pode oferecer funcionalidades mais sofisticas como aplicações dedicadas para conferências, conferências reservadas recorrentes, serviços de presença e de mensagem instantânea, entre outros.

O sistema de conferência centralizado é construído ao redor de um conceito fundamental de objeto de conferência. Um objeto de conferência provê a representação de dados de uma conferência durante cada uma das várias fases de uma conferência (por exemplo, criação, reserva, ativação, encerramento). Um objeto de conferência é acessado através dos elementos funcionais lógicos usando os vários protocolos identificados na Figura 4.8.

Os elementos funcionais definidos para um sistema de conferência descrito pelo *framework* são o servidor de controle de conferência, o servidor de controle de sala, os *focus* e o serviço de notificação. Um protocolo de controle de conferência (CCP) provê a interface entre a conferência, os clientes que controlam a mídia e o servidor de controle de conferência. Um protocolo de controle de sala (por exemplo, BFCP (*Binary Floor Control Protocol*) (RFC 4582, 2006) que será apresentado mais adiante) provê a interface entre um cliente de controle de sala e o servidor de controle de sala.

Um protocolo de sinalização de chamada (por exemplo, SIP, H.323, XMPP) provê a interface entre um cliente de sinalização de chamada e um *focus*. Um protocolo de notificação (por exemplo, SIP *Notifiy* (RFC 3265, 2002)) provê a interface entre o cliente de conferência e o serviço de notificação.

Um sistema de conferência pode suportar um subconjunto das funções de conferência descritas no sistema de conferência mostrado na Figura 4.8. Porém, há alguns componentes essenciais que são usados tipicamente através de outras funções avançadas, como o serviço de notificação.

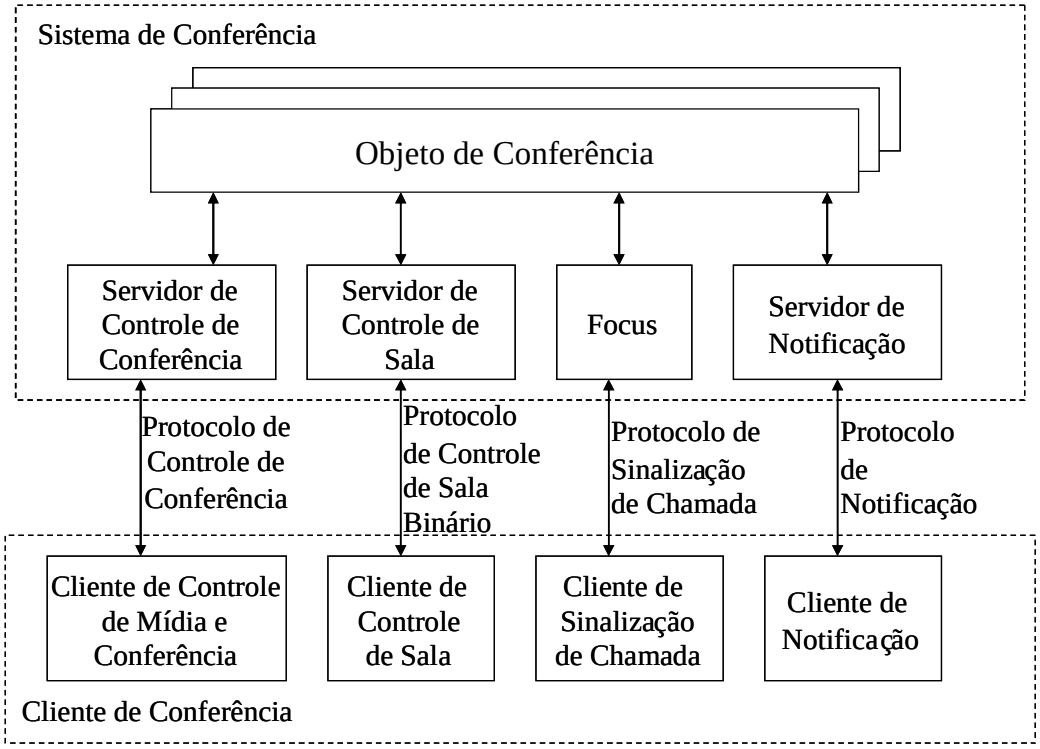


Figura 4.8 - Decomposição Lógica do Sistema de Conferência, adaptado de (*Draft* "*A Framework for Centralized Conferencing*", 2007).

O gráfico de mídia de uma conferência pode ser centralizado, descentralizado ou qualquer combinação de ambos e potencialmente difere por tipo de mídia. No caso centralizado, as sessões de mídia são estabelecidas entre um misturador de mídia controlado pelo *focus* e cada um dos participantes. No caso descentralizado, o gráfico de mídia é um *multicast* ou uma malha *multi-unicast* entre os participantes. Conseqüentemente, o processamento de mídia pode ser controlado somente pelo *focus* ou pelos participantes. O *framework* centralizado utiliza o modelo de mídia centralizado.

4.3.2 Dados de Conferência Centralizados

Os dados de conferência centralizados são logicamente representados pelo objeto de conferência. Um modelo de objeto de conferência "tipo de informação da conferência" é apresentado na Figura 4.9.

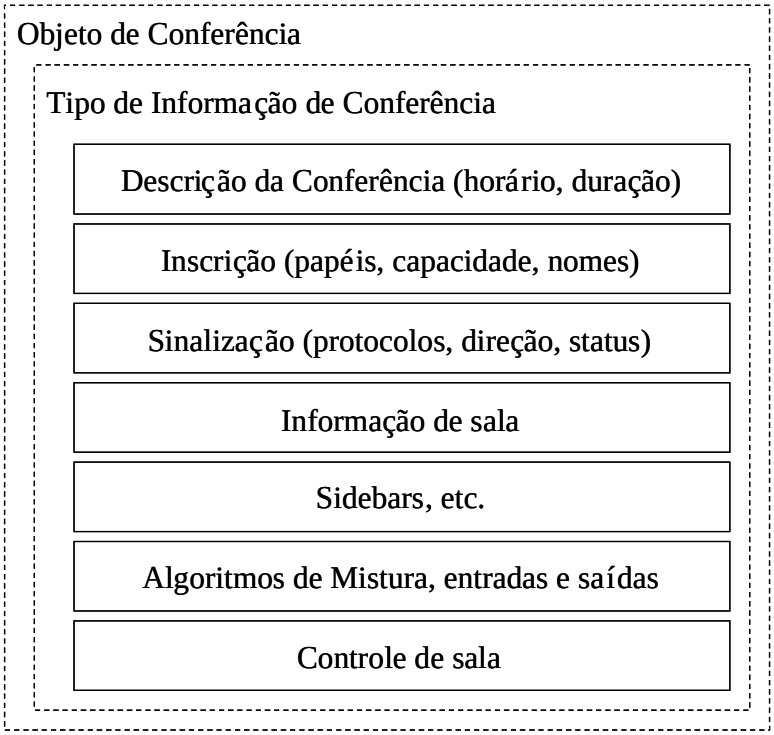


Figura 4.9 - Objeto de Conferência adaptado de (*Draft* "*A Framework for Centralized Conferencing*", 2007).

Em um sistema baseado no *framework* de conferência centralizada, o mesmo tipo de objeto de conferência é usado para representar uma conferência durante suas diferentes fases. Este objeto pode estar expressando as capacidades do sistema de conferência, reservando recursos de conferência ou refletindo o estado das conferências em andamento. O esquema XML (*EXtensible Markup Language*) exato do objeto de conferência, inclusive a organização da informação de conferência pode ser encontrado no *Draft* "*A Common Conference Information Data Model for Centralized Conferencing*" (2007).

4.3.3 - Informação de Conferência

Há um conjunto principal de dados de informação de conferência que são utilizados em qualquer conferência, independente da natureza da mídia da conferência (por exemplo, os algoritmos de mistura executados, o controle de sala avançado aplicado). Este conjunto de dados de informação de conferência contém as definições que representam as capacidades do objeto de conferência, funções, sinalização de chamada e *status* de mídia pertinentes para as diferentes fases do ciclo de vida da conferência. Este conjunto pode ser

representado usando o tipo de conferência definido no pacote de evento de conferência SIP (RFC 4575, 2006).

Para suportar manipulações de mídia mais complexas e funcionalidades de conferência mais sofisticadas, a informação de conferência, como definido *Draft* "*A Common Conference Information Data Model for Centralized Conferencing*" (2007), que trata do modelo de dados, contêm dados adicionais além dos definidos na RFC 4575 (2006). A informação definida no modelo de dados provê detalhes específicos de mistura de mídia, controles de sala disponíveis e outros dados necessários para suportar funcionalidades de conferência mais avançadas. Esta informação permite a clientes autorizados manipular o comportamento do misturador através do *focus*, com a distribuição da mídia resultante para todos ou para participantes individualmente. Desta forma, um cliente pode mudar seu próprio estado e o estado de outros participantes na conferência.

4.3.4 - Políticas de Conferência

As políticas de conferência, conforme já definido anteriormente, se referem a um conjunto de direitos, permissões e limitações das operações que são executadas em certo objeto de conferência.

O conjunto de direitos descreve os privilégios de acesso de leitura/escrita para o objeto de conferência. Este acesso normalmente será concedido e definido para dar acesso de leitura somente, ou de leitura e escrita a clientes que desempenham certos papéis na conferência. A administração deste acesso requer que o sistema de conferência tenha acesso à informação de política básica para tomar as decisões, mas necessariamente não requer uma representação explícita no modelo de política.

4.3.5 – Construção de Conferência Centralizada e Identificadores

Esta seção provê detalhes dos identificadores associados com a construção do *framework* de conferência centralizado e os identificadores necessários para endereçar e administrar os clientes associados com o sistema de conferência.

4.3.5.1 - Identificador de Conferência

Como já informado o identificador de conferência (conferência ID) é um URI específico do protocolo de sinalização de chamada que identifica um *focus* de conferência e sua instância de conferência associada. Uma fábrica de conferência é um método para gerar uma conferência com um ID único, identificar e endereçar um *focus* de conferência, usando uma interface de sinalização de chamada.

4.3.5.2 - Objeto de Conferência

Um objeto de conferência provê a representação lógica de uma instância de conferência em certa fase durante o período em que ela está ativa. Cada objeto de conferência é endereçável de maneira independente pela interface do protocolo de controle de conferência.

A Figura 4.10 ilustra as relações entre o identificador de conferência, o *focus* e o ID do objeto dentro do contexto de uma instância de conferência lógica, com o objeto correspondente a uma conferência ativa.

Um objeto de conferência representando uma conferência ativa pode ter múltiplos identificadores. Existe um mapeamento um para um entre um objeto de conferência ativo e um *focus* de conferência.

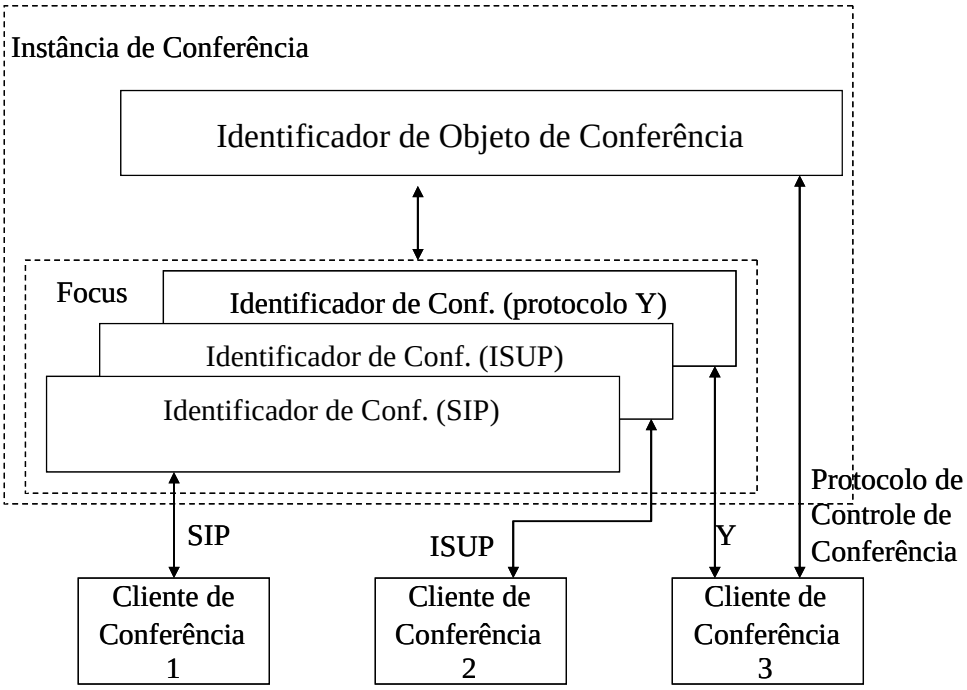


Figura 4.10 - Relações do identificador para uma conferência ativa, adaptado de (*Draft "A Framework for Centralized Conferencing*", 2007).

4.3.5.3 - Identificador de Usuário de Conferência

O identificador de usuário é usado em associação com o identificador de objeto de conferência para identificar de maneira unívoca um usuário dentro do escopo do sistema de conferência. Também há uma exigência de identificar clientes do sistema de conferência que podem não estar participando de uma instância de conferência.

O identificador de usuário de conferência é necessário em requisições do protocolo de controle de conferência para determinar quem esteja fazendo a solicitação, de forma que políticas apropriadas possam ser aplicadas ao pedido.

Uma forma comum de distribuir o identificador de usuário é através de mecanismos que atuam fora da banda durante configuração do cliente de conferência, assim o mecanismo está fora do escopo do *framework* de conferência centralizada e dos protocolos. Porém, um sistema de conferência também deve ser capaz de alocar e distribuir um identificador de usuário durante a primeira interação de sinalização com o sistema de conferência, como um pedido inicial para projetos ou acrescentando um usuário novo a uma conferência existente que usa o protocolo de controle de conferência. Quando um usuário se une a uma conferência que usa um protocolo de sinalização específico, como SIP, deve ser nomeado para ele um identificador de usuário de conferência.

O identificador de usuário de conferência é logicamente conectado com os outros identificadores de usuário associados ao cliente de conferência para outras interfaces de protocolo, como um usuário SIP autenticado.

4.3.6 – Realização do Sistema de Conferência

Implementações baseadas no *framework* centralizado podem variar de sistemas que suportam conferências *ad hoc*, somente com ambiente padrão, para sistemas sofisticados com a habilidade para programar conferências recorrentes, com características distintas, sendo integrado com ferramentas de reserva de recursos e provendo informações instantâneas de conferência em quaisquer das fases do ciclo de vida da conferência.

Considerando que um objeto de conferência é a representação lógica de uma instância de conferência em certa fase, o *framework* de conferência centralizada não designa o uso atual do objeto de conferência, mas define o conceito de árvore de clonagem geral, que será apresentado a seguir, e os mecanismos necessários para sua realização.

A política global em termos de permissões e limitações não faz parte do *framework*. As políticas aplicáveis ao objeto de conferência como um todo em termos de acesso de leitura/escrita requerem que o sistema de conferência tenha acesso a informação de política básica para tomar as decisões. Neste trabalho as políticas são mostradas associadas logicamente com os objetos de conferência para enfatizar o requisito de funcionalidade de política necessário para a realização do *framework*.

4.3.6.1 Árvore de Clonagem

O conceito definido nesta seção é somente uma representação lógica de como isto se reflete através dos mecanismos de conferência centralizados: os URIs e os protocolos. A implementação de um sistema pode diferir do modelo aqui apresentado. A intenção é apresentar o papel dos elementos lógicos provendo uma interface para os dados, baseado em um sistema de conferência e ações dos clientes da conferência, e descrever as implicações resultantes disto nos protocolos.

Qualquer objeto de conferência é criado clonando explicitamente um objeto existente ou sendo implicitamente clonado de um projeto de conferência padrão. Um projeto de conferência é um objeto de conferência estático usado para descrever uma conferência típica suportada pelo sistema. Cada sistema pode manter múltiplos projetos,

normalmente cada um descreve um tipo de conferência diferente que usa o formato de informação de conferência.

A operação de clonagem precisa especificar se a ligação entre o “pai” e o “filho” precisa ser mantida no sistema ou não. Se não existe nenhuma ligação entre o eles, os objetos ficam independentes e o “filho” não é impactado por qualquer operação no “pai”, nem a qualquer limitação do objeto “pai”.

Quando o objeto novo é criado, ele pode ser endereçado por um URI de objeto de conferência único designado pelo sistema. O objeto recentemente criado contém todos os dados que existem no objeto “pai”. O “filho” pode ampliar os dados nele contidos, dentro dos tipos de esquema suportados pelo pai e também pode restringir o acesso de leitura/escrita a seus objetos. Porém, a menos que o objeto seja independente, ele não pode modificar as restrições de acesso impostas pelo objeto “pai”.

Qualquer parte dos dados do objeto “filho” pode ser acessada e modificada independentemente, sem afetar os dados do “pai”.

A menos que o objeto seja independente, o “pai” pode obrigar políticas diferentes marcando certos elementos de dados como “pai executável”. Os valores destes elementos de dados não podem ser mudados acessando diretamente o “filho”, nem podem ser ampliados somente no objeto “filho”.

A Figura 4.11 ilustra um exemplo de uma conferência (Pai B) que é criada independente de seu “pai” (Pai A). Pai B cria dois objetos “filhos”, Filho 1 e Filho 2. Quaisquer dos elementos de dados de Pai B podem ser modificados e dependendo do elemento, as mudanças serão refletidas em Filho 1 e Filho 2, considerando que mudanças em Pai A não tem impacto nos elementos de dados de Pai B.

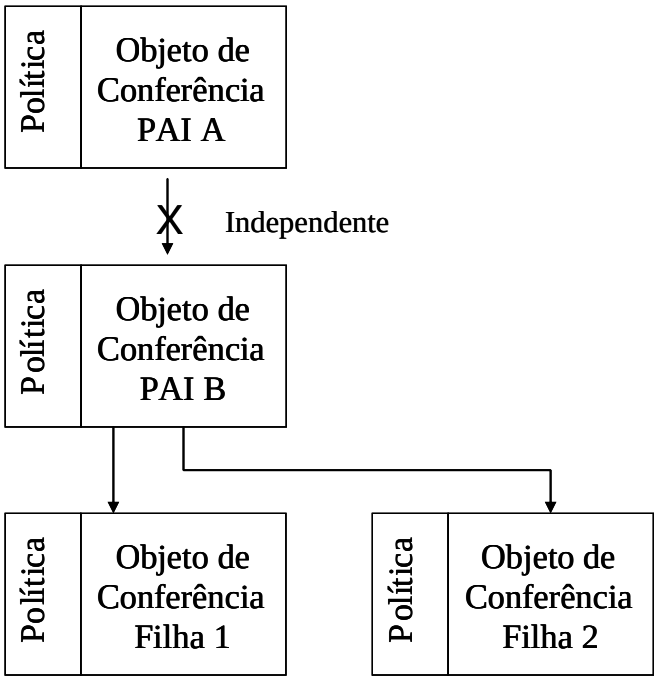


Figura 4.11 - A árvore de clonagem adaptado de (*Draft* "*A Framework for Centralized Conferencing*", 2007).

4.4 – *Framework* de Conferência Distribuída

O *framework* de conferência distribuída ou descentralizada usa a mesma terminologia adotada pelos *frameworks* para conferência SIP e conferência centralizada do XCON e expande esta terminologia no *Draft* "*A Framework for Distributed Conferencing*", (2007). de acordo com a sua necessidade. Os termos adicionais são mostrados a seguir e são definidos para uso específico dentro do ambiente de conferência distribuída:

- Descoberta de *Focus*: este termo representa à capacidade de descobrir a presença de novos *focus* em um *framework* de conferência distribuída.
- Propagação de Informação: este termo se refere à propagação de informação relacionada à conferência entre os *focus* distribuídos.
- Distribuição de Protocolo: este termo representa a capacidade de remeter/distribuir as mensagens de um protocolo que nativamente é centralizado de forma adequada em um ambiente distribuído.
- DCON *Focus*: este termo se refere a uma entidade específica que habilita a comunicação de um sistema de conferência centralizada com o mundo externo. Um

DCON *focus* permite a construção de um sistema de conferência distribuída como um conjunto de componentes de conferência centralizada.

- Nuvem de conferência: este termo se refere a um par específico composto de um *focus* centralizado (XCON) e seu *focus* distribuído associado (DCON).
- Troca de rótulo: A troca dos rótulos nomeados para um recurso específico é utilizada para evitar conflitos no envio de rótulos nomeados relativos ao mesmo recurso, através de várias comunicações ponto a ponto.

4.4.1 – Visão Geral

Para poder construir uma conferência distribuída em cima do *framework* de conferência centralizada, é necessário introduzir duas funções principais:

- Um nível de coordenação entre os *focus* de conferência;
- Uma forma efetiva de distribuir a informação do estado da conferência.

O primeiro ponto é necessário para administrar uma conferência distribuída ao longo de todo seu ciclo de vida. Desta forma, uma vez que um usuário decide criar uma nova conferência, o correspondente *focus* da conferência tem que distribuir a informação de conferência a todos os outros *focus*, de uma forma que permita a outros potenciais participantes obter os dados necessários e participar da conferência.

Todas as operações necessárias dentro de uma única nuvem de conferência são administradas pelos protocolos e interfaces definidas pelo XCON. Conseqüentemente, cada nuvem continua a operar em uma topologia em estrela no que se refere à sinalização de chamada. As várias estrelas estão conectadas por uma topologia superior baseada em malha que provê a comunicação entre os *focus*.

Conforme mostrado na Figura 4.12, a topologia global do cenário de conferência distribuída tem uma camada sobreposta de *focus*, onde cada um administra a ilha de conferência centralizada que se encontra na camada inferior. Nesta dissertação a ilha de conferência centralizada engloba um focus XCON e todos os clientes que se conectam a ele para criar ou participar de uma conferência.

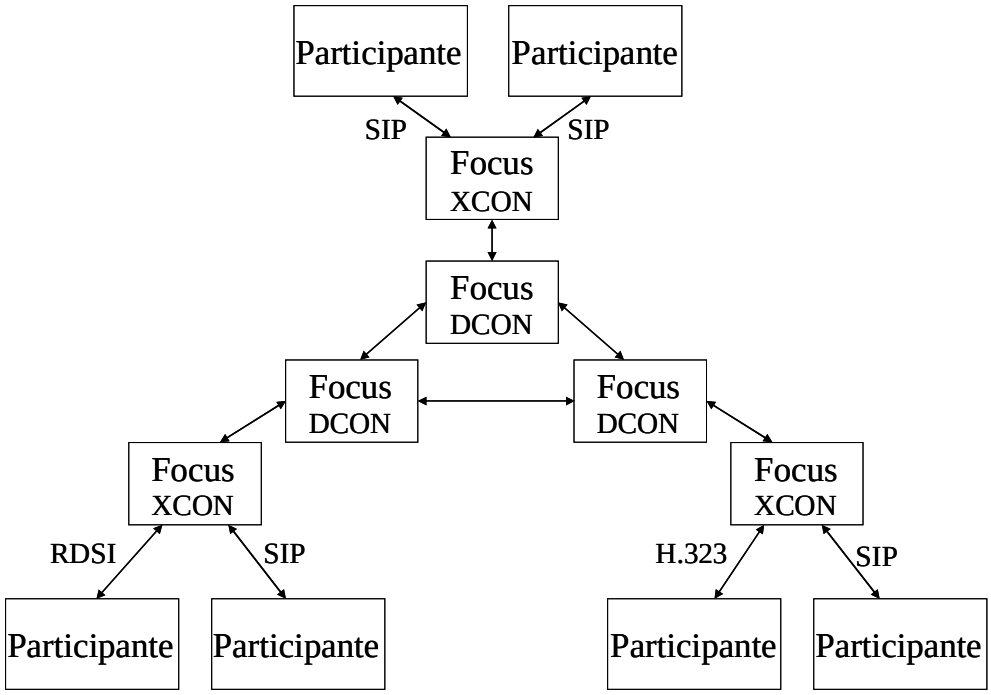


Figura 4.12 - Arquitetura DCON, adaptado de (*Draft* "*A Framework for Distributed Conferencing*", 2007).

Uma forma efetiva de distribuir a informação do estado da conferência é necessária ao trocar da topologia centralizada para a distribuída. Sempre que uma nova conferência é criada (ou uma conferência ativa muda seu estado) este evento tem que ser comunicado a todos os participantes interessados.

Devido à natureza intrínseca do framework de conferência distribuída (que na verdade amplia o de conferência centralizada pela introdução de uma camada superior de *focus*), o atual fluxo de informação sempre irá prever a interação entre *focus* de conferência para a troca de informação de conferência e notificações de mudança de estado. O mesmo obviamente também se aplica aos protocolos centralizados envolvidos definidos no *framework* XCON. Um mecanismo teve que ser definido para permitir o envio de mensagens centralizadas pela rede DCON.

O mecanismo em questão tem que ser completamente compatível com a operação existente nas nuvens XCON, as quais têm que manter seus participantes locais totalmente desavisados da potencial natureza distribuída da conferência.

A divulgação do estado da conferência pode acontecer de vários modos. Uma forma é que cada *focus* pode inundar a malha de comunicação entre *focus* com a informação recebida, garantindo que aqueles potenciais participantes que pertencem a diferentes ilhas irão receber a informação. Neste caso, as entidades *focus* são "*stateful*", ou

seja, cada um deles armazena a informação sobre as sessões atuais e remete esta informação a todas as entidades pares para garantir que elas estão atualizadas em relação às sessões de conferência disponíveis.

Por outro lado, um repositório distribuído poderia ser usado para armazenar a informação de conferência. Os *focus* acessariam tal repositório para publicar (a criação de uma nova conferência, ou a notificação de uma mudança no estado de uma conferência ativa) e obter informação sobre conferências ativas (e.g. quando um novo participante quer acessar a lista de sessões de conferência atuais ou agendadas que ele poderia estar interessado em participar). Neste último caso, os *focus* são "*stateless*".

Finalmente, uma solução ponto a ponto pode ser utilizada com a finalidade de divulgar a informação de estado de conferência.

4.4.2 - Arquitetura do *Framework* de Conferência Distribuída

Nesta seção primeiramente será descrita a arquitetura do *framework* de conferência distribuída, realçando as entidades envolvidas e as relações entre elas. Após serão detalhados alguns casos de uso que ajudam a entender a interação em um ambiente descentralizado.

Do ponto de vista da arquitetura, a Figura 4.13, mostra como várias ilhas de XCON podem interagir para trocar mensagens de sincronização entre cada par de sistemas de conferência. Tais mensagens são necessárias para que a informação da conferência circule entre todas as entidades envolvidas. Torna-se necessário um protocolo dedicado para levar a comunicação entre cada par. Considerando que a tarefa deste protocolo é sincronizar o XCON como o par DCON, ele será chamado XDSP (XCON-DCON *Synchronization Protocol*).

A coordenação entre ilhas pode ser realizada de diversas maneiras, uma delas é utilizando SIP/SIMPLE (*Session Initiation Protocol for Instant Messaging and Presence Leveraging Extensions*), outra é utilizando XMPP. Neste trabalho será adotado o uso da interação baseada em IM (*Instant Messaging*). Mais precisamente, será utilizado o módulo de servidor-para-servidor (S2S) baseado no protocolo XMPP para satisfazer as exigências impostas pela arquitetura distribuída.

Finalmente, os fluxos de mídia irão passar diretamente entre as nuvens XCON uma vez uma conferência distribuída tenha sido estabelecida.

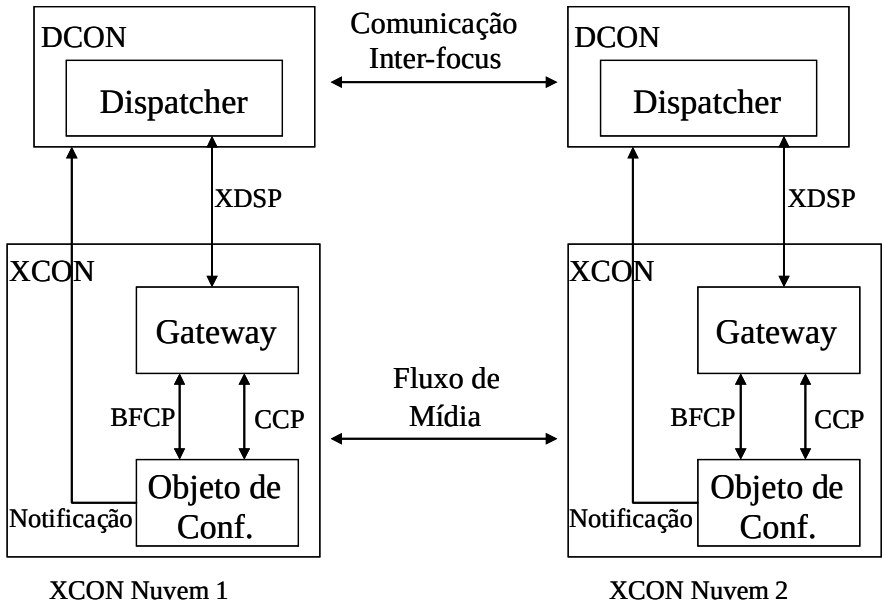


Figura 4.13 - Framework para conferência distribuída adaptado de (*Draft* "*A Framework for Distributed Conferencing*", 2007).

A seguir serão descritos os passos necessários a organização de um ambiente de conferência distribuída. Os pontos enfatizados a seguir ajudarão a esclarecer como é efetivamente estabelecida e gerenciada uma conferência distribuída.

4.4.2.1 - Criação e gerenciamento da camada sobreposta

A criação de uma camada sobreposta permite a efetiva operação do *framework* de conferência distribuída. Esta camada é formada pela interconexão de todas as nuvens de conferência. A camada sobreposta pode ser construída através da interligação de todos os *focus* (onde cada *focus* é o centro de uma de conferência centralizada) por uma topologia em malha.

Quando a camada sobreposta é criada deve ser prevista uma forma apropriada de gerenciamento desta estrutura. Isto deve incluir, entre outros, a atualização dinâmica da informação de topologia quando ocorrerem eventos relevantes.

4.4.2.2 - Descoberta de focus

Deve ser definido um mecanismo apropriado para a descoberta de *focus*. Dada a natureza sensível de compartilhar informação, deve ser adotado um mecanismo de

autenticação apropriado. O gatilho do processo de descoberta pode estar relacionado ao conceito de “presença”, neste caso, pode ser utilizada uma mensagem instantânea (IM).

Alternativamente, uma lógica centralizada, com repositório fisicamente distribuído (e.g. UDDI (*Universal Description, Discovery, and Integration*)) pode ser empregada como se fosse um único ponto de referência para a descoberta de entidades. Uma solução ponto a ponto também pode ser considerada para o mesmo propósito.

4.4.2.3 - Configuração automática

Eventos como a inclusão de uma nova nuvem sob a camada sobreposta de conferência distribuída, necessitam que alguns passos de configuração sejam executados de uma forma automatizada. Isto requer que todas as notícias sejam trocadas adequadamente através da camada sobreposta e, se necessário, às nuvens centralizadas também devem ser notificadas.

4.4.2.4 - Compartilhamento de informação

O principal ponto da operação de um *framework* de conferência distribuída reside na possibilidade de trocar informação entre todas as entidades envolvidas. O processo de compartilhamento de informação deve ser feito com a maior eficácia possível. Uma das formas de fazer isso é limitando a informação que é enviada para fora de uma única nuvem de conferência centralizada, aos dados que são estritamente necessários, para garantir que o estado global da camada sobreposta é consistente e não redundante.

O compartilhamento adequado da informação pode ser obtido através do uso de mecanismos de pedido/resposta, ou pela adoção de mensagens de notificação assíncronas. Normalmente deverá ser utilizada uma combinação dos métodos mencionados.

4.4.2.5 - Atualização dinâmica

Todas as nuvens que participam da conferência distribuída devem manter os pares atualizados em relação aos eventos significativos que ocorrerem no âmbito da sua área de atuação. Isto pode ser feito utilizando um método de pedido/resposta, ou pela adoção de mensagens de notificação assíncronas. Assim como para o item anterior é recomendado o uso combinado de ambos os métodos.

4.4.2.6 - Gerenciamento de conferência distribuída

Mecanismos apropriados para permitir o acesso de clientes a conferências criadas remotamente devem ser providos pelo *framework*. Tais mecanismos devem habilitar a administração transparente, tanto das instâncias de conferência criadas localmente como das criadas remotamente. Uma solução ponto a ponto pode ser utilizada para implementar este requisito.

4.4.2.7 - Roteamento e distribuição de protocolos centralizados

O *focus* deve remeter qualquer mensagem de protocolo centralizado para o seu par na camada sobreposta sempre que a mensagem é dirigida a um receptor que não pertence ao sistema centralizado local. As mensagens nativas de protocolos centralizados incluem qualquer protocolo definido e especificado pelo *framework* do XCON (e.g. administração de controle de conferência e controle de sala) como também a propagação de mensagens DTMF (*Dual Tone Multiple Frequency*).

Um exemplo são as mensagens BFCP (RFC 4582, 2006) que o servidor de controle de sala local necessita enviar a um usuário que está participando remotamente da conferência (porque ele não pertence a esta nuvem de XCON).

4.4.2.8 - Misturador distribuído

Assim que duas ou mais ilhas de conferência centralizada são conectadas para prover para um cenário de conferência distribuída, surge a necessidade de misturar fluxos de mídia gerados pelos participantes de conferência. Este assunto não será tratado neste trabalho, pois ainda não é tratado pelos documentos existentes do *framework* que focam na distribuição da informação de controle e na sinalização da conferência, não tratando da administração de mídia.

4.4.3 – Exemplos da operação do framework DCON

Nesta seção serão mostrados alguns modelos da operação do *framework* para conferência distribuída.

4.4.3.1 - Criando uma nova conferência distribuída

A Figura 4.14 procura mostrar como uma conferência distribuída pode ser criada e administrada em um ambiente distribuído.

Um participante entra em contato com o seu *focus* para pedir a criação de uma nova instância de conferência. A instância de conferência é criada de acordo com o procedimento definido pelo *framework* de conferência centralizado, após a criação o *focus* tem que publicar a informação da conferência através da notificação ao seu correspondente *focus* DCON. Isto é necessário para que os outros *focus* remotos possam ser atualizados sobre as sessões de conferência disponíveis.

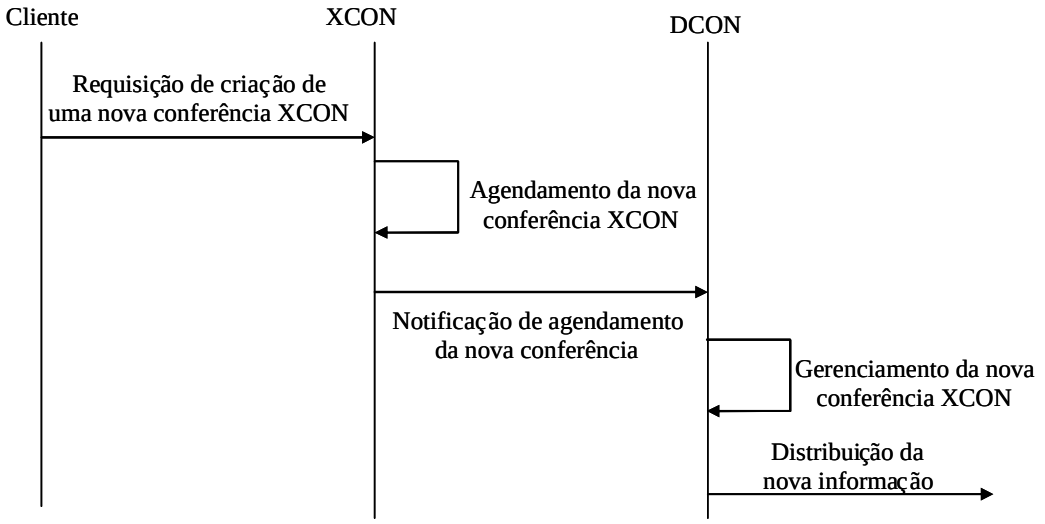


Figura 4.14 - Criando uma nova conferência adaptado de (*Draft* "*A Framework for Distributed Conferencing*", 2007).

4.4.3.2 - Obtendo informação sobre conferências disponíveis

A Figura 4.15 ilustra como obter a informação sobre conferências disponíveis, sejam elas centralizadas ou distribuídas.

Um participante contata o seu *focus* para pedir informações sobre conferências disponíveis. Após receber a requisição do participante o *focus* XCON tem que remeter o pedido ao seu correspondente *focus* DCON. A entidade *focus* distribuída é capaz de prover esta informação, que incluirá a lista de conferências centralizadas (local) e distribuídas (remoto).

Desta forma, o participante poderá continuar contatando o *focus* XCON para adquirir todas as informações que ele precise, tanto para conferências centralizadas quanto para distribuídas.

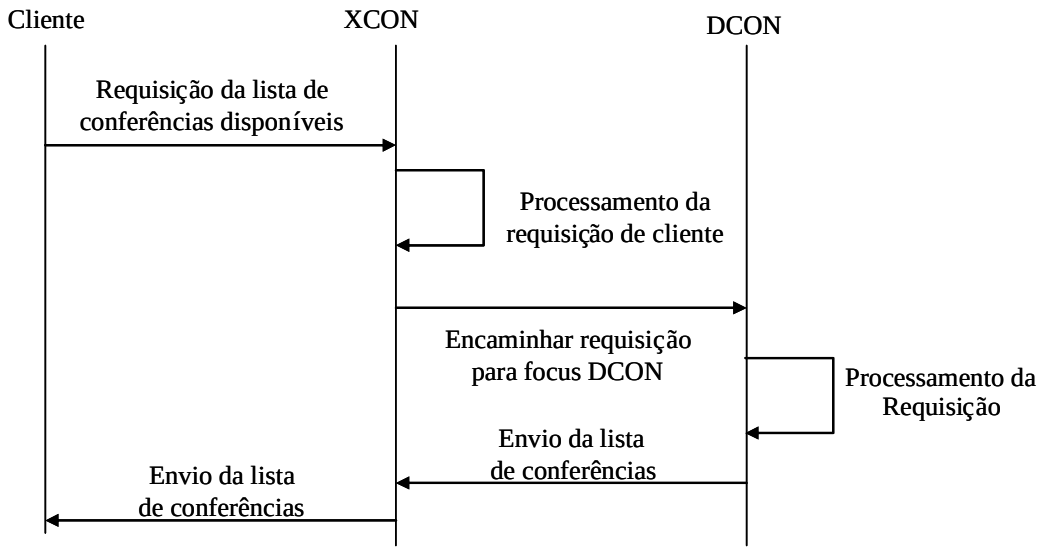


Figura 4.15 - Obtendo informações sobre conferências disponíveis adaptado de (*Draft* "*A Framework for Distributed Conferencing*", 2007).

4.4.3.3 - Distribuindo protocolos XCON em uma conferência DCON

A Figura 4.16 demonstra como protocolos XCON de natureza centralizada podem ser corretamente utilizados em um ambiente distribuído. Este mecanismo permite que os clientes que participam de conferências distribuídas não precisem conhecer os endereços de transporte necessários para se comunicar com *focus* remotos, e possam continuar recorrendo aos endereços do *focus* local para acessar o *focus* remoto de maneira transparente.

Para entender quem deverá ser o atual receptor de uma mensagem, todas as mensagens são interceptadas por uma entidade lógica chamada de *gateway*. Esta entidade pertence ao *focus* XCON. O *gateway* entenderá se uma mensagem é dirigida a uma

entidade local (e.g. um usuário que pertence ao *focus* XCON ou ao servidor de controle de sala local) ou para uma entidade remota que pertence a outro *focus* (e.g. um usuário participando remotamente ou um servidor de controle de sala remoto).

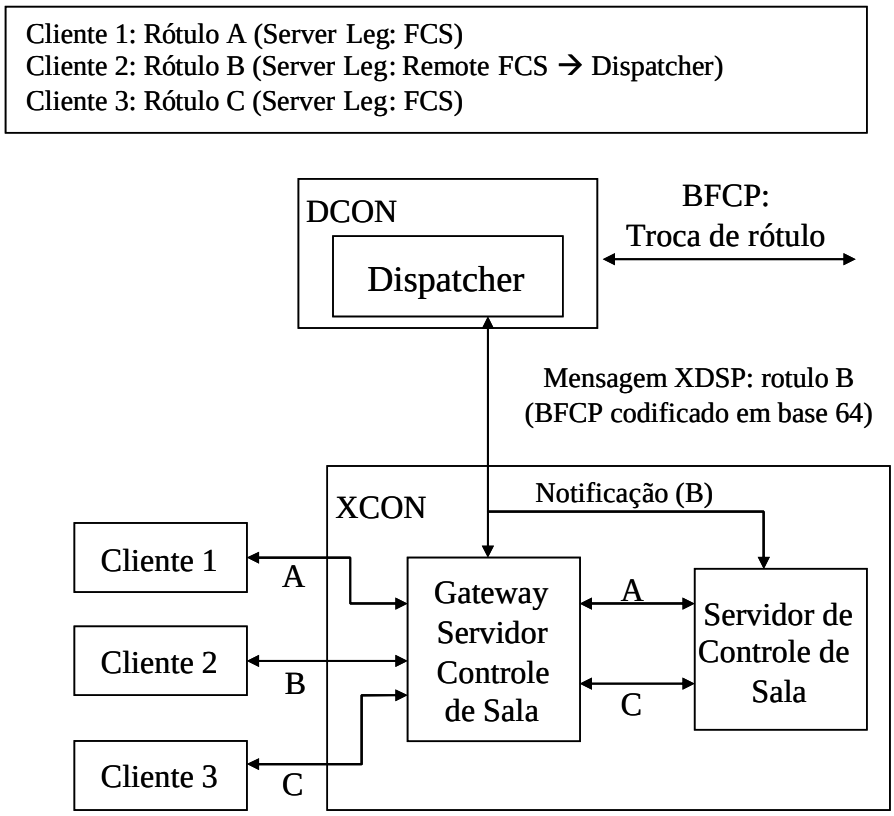


Figura 4.16 - Tratamento de protocolos centralizados adaptado de (*Draft* "*A Framework for Distributed Conferencing*", 2007).

5 – COMPARAÇÃO ENTRE OS FRAMEWORKS DE CONFERÊNCIA CENTRALIZADA E DISTRIBUÍDA

Neste capítulo será realizada uma comparação entre o *framework* de conferência centralizada e o *framework* de conferência distribuída. O objetivo desta comparação é definir qual a melhor arquitetura para evolução do serviço de videoconferência da Brasil Telecom.

Para balizar esta escolha será apresentada uma análise de escalabilidade realizada pelo grupo de estudos da Universidade de Nápoles comparando os dois *frameworks*, apresentada no trabalho "*Improving the scalability of an IMS-compliant conferencing framework through presence and event notification*" apresentado no IPTComm 2007 em Nova York.

Além da análise de escalabilidade, será apresentada uma avaliação financeira da implementação dos dois *frameworks* na rede da Brasil Telecom com base em uma demanda definida, considerando as peculiaridades da rede da Brasil Telecom como distâncias, custos de operação, interesse de tráfego e demanda de clientes.

O *framework,* que apresentar os melhores resultados na avaliação realizada neste capítulo, é utilizado no capítulo 6 para sugerir uma possibilidade de evolução para a rede da Brasil Telecom.

5.1 - Análise de Escalabilidade

Um dos principais pontos a ser avaliado na escolha de uma solução técnica para implantação de um serviço em uma operadora de telecomunicações é a escalabilidade. A solução deve permitir que mesmo começando com um pequeno número de clientes, ela possa ser expandida para um número dezenas ou centenas de vezes maior. Isto é necessário, porque o produto, na maioria das vezes, é lançado no mercado em uma região definida ou com um número limitado de acessos a fim de evitar que, caso não haja uma boa aceitação do produto, o investimento inicial não tenha sido muito grande.

Desta forma, é fundamental que a solução escolhida possibilite que o serviço tenha uma ampliação do número de clientes, simplesmente através do acréscimo de capacidade dos equipamentos e eventualmente do crescimento no número de equipamentos, mas sem alterar a arquitetura do serviço.

5.1.1 - Considerações preliminares

O objetivo da seção 5.1 é comparar uma plataforma baseada no *framework* de conferência centralizada e um ambiente baseado no *framework* de conferência distribuída e identificar qual deles tem uma melhor escalabilidade.

Os testes de desempenho focaram dois aspectos:

- O número de clientes que o sistema pode administrar e;
- A carga de CPU e consumo de recursos de hardware com certa quantidade de clientes no sistema.

Estes aspectos foram escolhidos para que fosse possível identificar qual dos frameworks consegue evoluir para um número maior de clientes usando o mesmo hardware.

Em ambos os casos foi utilizada a ferramenta SIPp, uma ferramenta de teste de desempenho aberta para o protocolo SIP que gera tráfego de acordo com um cenário XML totalmente customizável. Enquanto a ferramenta inclui alguns arquivos de modelo básicos para os cenários de chamada mais comuns, foram criados cenários próprios para administrar o re-INVITE de mensagens enviadas de volta pelo servidor CONFIANCE (*CONFerencing IMS-enabled Architecture for Next-generation Communication Experience*), junto com as respostas subseqüentes que constituem o modo de confirmação que caracteriza a adesão a uma conferência.

Este re-INVITE e sua renegociação conseqüente, sempre acontece quando um cliente SIP se unir a uma conferência, os dados BFCP necessários para o cliente (endereço de transporte do servidor de controle de sala e os identificadores relacionados) são encapsulados dentro o re-INVITE no corpo do SDP como especificado na RFC 4583 (2006).

Outra característica útil da ferramenta SIPp é a possibilidade de enviar tráfego de mídia (áudio e vídeo) através do RTP/pcap.

Usando a ferramenta SIPp, foram testados os ambientes centralizados e descentralizados, conforme será apresentado nas seções 5.1.2 e 5.1.3, respectivamente.

5.1.2 Cenário do *Framework* de Conferência Centralizada

A Figura 5.1 ilustra a configuração do cenário de teste para conferência centralizada. O console do SIPp é usado para controlar remotamente e coordenar um único teste, enviando comandos para o servidor originador de chamadas (SIPp *stresser*).

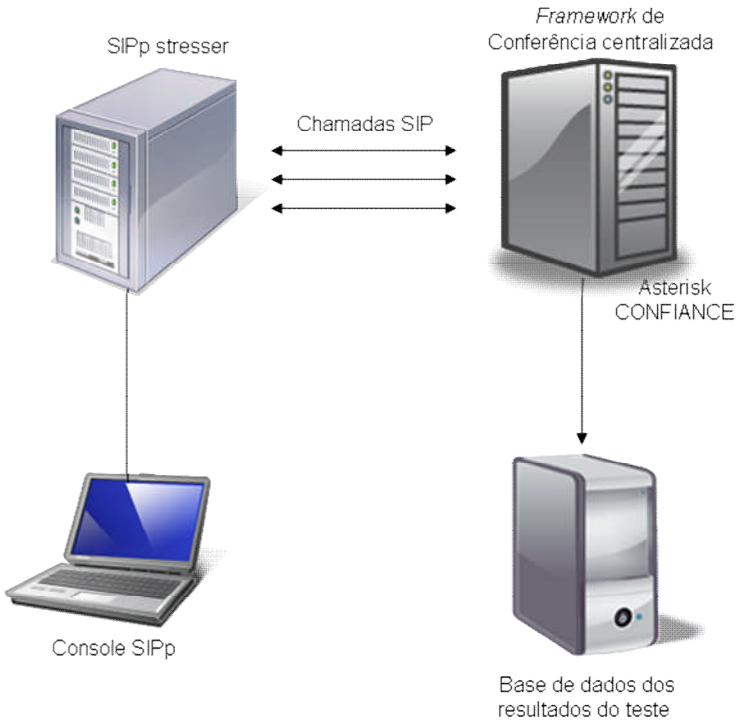


Figura 5.1 – Configuração do cenário de teste para o *framework* de conferência centralizada, adaptado de (IPTComm, 2007).

O SIPp *stresser* cria e envia requisições de chamada ao servidor CONFIANCE baseado em Asterisk seguindo as indicações do console SIPp, emulando um perfil de chamadas real.

Durante o teste, a base de dados de acessos é continuamente atualizada com informações sobre o *status* do servidor CONFIANCE.

Todas as máquinas usadas no teste (excluindo o console da ferramenta SIPp) operavam com sistema operacional Linux Fedora *Core* 6, equipadas com um *kernel* 2.6.15. Elas tinham uma CPU Intel XEON de 3,2 GHz e 2 GB de RAM (*Random Access Memory*).

A largura da faixa não era um fator limitante para a avaliação do desempenho, pois foi usada rede *gigabit ethernet* dedicada.

A avaliação está baseada na realização de um grande número de testes para cada cenário. O objetivo foi evitar que a análise fique baseada em um pequeno conjunto de dados que podem não representar a realidade. Para cada cenário, será apresentado somente um resultado que é o caso mais representativo daquele cenário.

Nos testes que serão apresentados, quando o objetivo era avaliar o número de clientes que poderiam acessar o sistema, não foi utilizada a função "SIPp *pcap replay*". Isto garantiu que cada cliente gerou somente tráfego de sinalização, sem enviar qualquer pacote RTP para o *focus*, embora recebesse os pacotes RTP resultantes da operação de mistura do próprio *focus*. Neste caso, o *focus* enviou apenas silêncio, ou seja, RTP vazio, pois ele não tinha nenhuma mídia para misturar. Desta forma, foi possível reduzir o número de operações que o *focus* tinha que executar como transcodificação e potenciais descartes ou mistura de pacotes de acordo com o *status* do fluxo de mídia no servidor de controle de sala.

Por outro lado, quando foi envolvido tráfego RTP no trabalho de análise, o foco passou a ser o consumo de recurso. Nesta visão o limitante foi a utilização da CPU, e não outros parâmetros de hardware como, memória RAM disponível. Então o estudo considerou a ocupação da CPU como o indicador de desempenho fundamental.

Ao considerar a avaliação de desempenho da CPU, foi utilizada a funcionalidade de *pcap replay* para que cada usuário envie SIP e tráfego RTP, pois a transcodificação de mídia e a funcionalidade BFCP demandavam ciclos de processamento e recursos.

A Figura 5.2 mostra que, tendo somente uma conferência ativa e 300 clientes que se uniram a ela, a carga da CPU do *focus* que administra aquela conferência é de aproximadamente 99,42%.

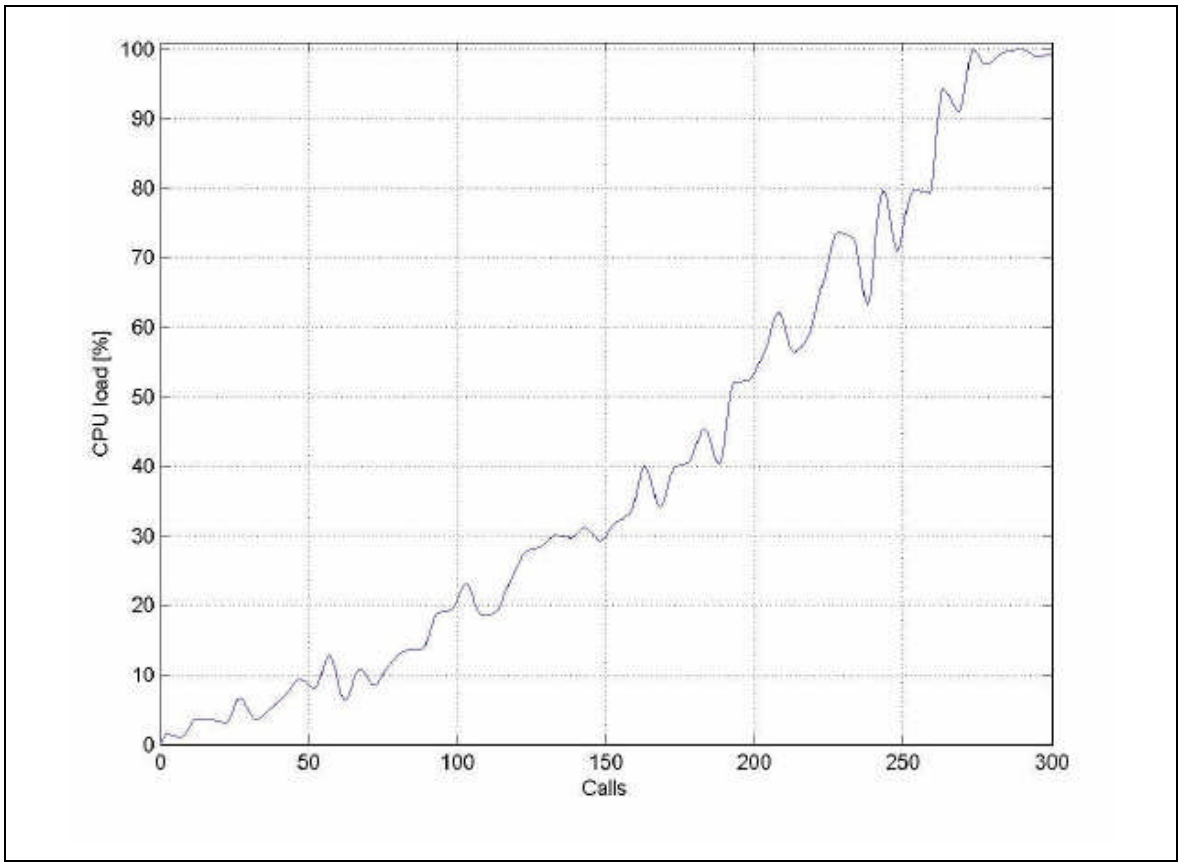


Figura 5.2 – Utilização de CPU no cenário centralizado (IPTComm, 2007).

Este resultado (300 clientes como o valor de pico para o cenário centralizado na presença de fluxos de mídia) será usado como um parâmetro de comparação em um cenário de *framework* de conferência distribuída.

5.1.3 Cenário do *Framework* de Conferência Distribuída

A Figura 5.3 ilustra a configuração do teste no caso do cenário de *framework* de conferência distribuída com somente duas ilhas de conferência interconectadas.

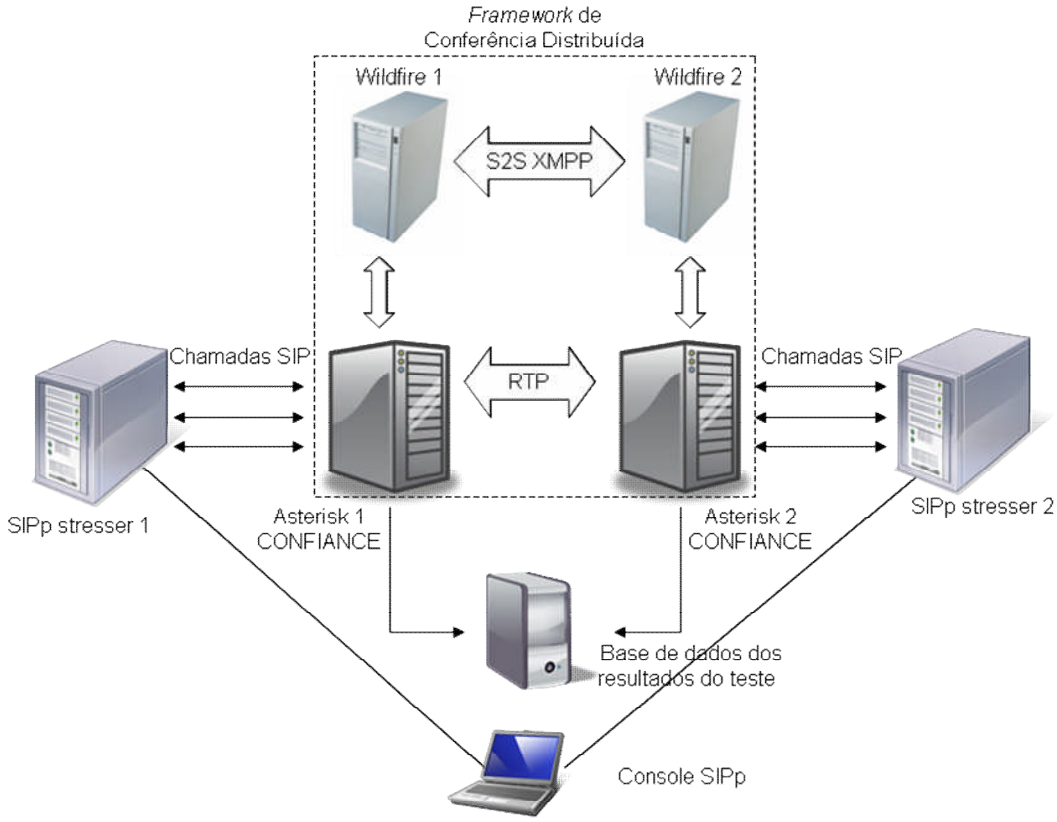


Figura 5.3 – Configuração do cenário de teste para o framework de conferência distribuída, adaptado de (IPTComm, 2007).

Com relação ao caso centralizado, foi adicionado o componente de *Wild-fire,* um servidor de mensagens instantâneas de fonte aberta bastante popular, que é dedicado especificamente para divulgar a informação e despachar o protocolo.

Também pode ser notado que o console SIPp é usado para administrar ambas as entidades SIPp *stresser.*

A sinalização e o controle dos *focus* são administrados através de protocolos de despacho e sincronização entre *focus*, suas multimídias (áudio e vídeo) são misturadas nos *focus* remotos, e então enviadas ao *focus* principal como se elas viessem de um único usuário. A mesma coisa acontece para as mídias que vão do *focus* principal para os focos remotos.

O *focus* principal mistura as mídias que vêm de seus clientes locais e de todos os *focus* remotos envolvidos na conferência. Baseado no fato que é necessário somente um tronco de RTP entre cada *focus* remoto e o *focus* principal, o número de participantes cresce linearmente com o número de ilhas DCON. Cada *focus* remoto se conecta com o *focus* principal através de um canal no barramento compartilhado, desta forma, um canal a

menos estará disponível para os clientes locais, tanto do *focus* remoto quanto do *focus* principal.

A Figura 5.4 resume as considerações acima, representando o crescimento linear no número de clientes suportados pelos quatro cenários considerados.

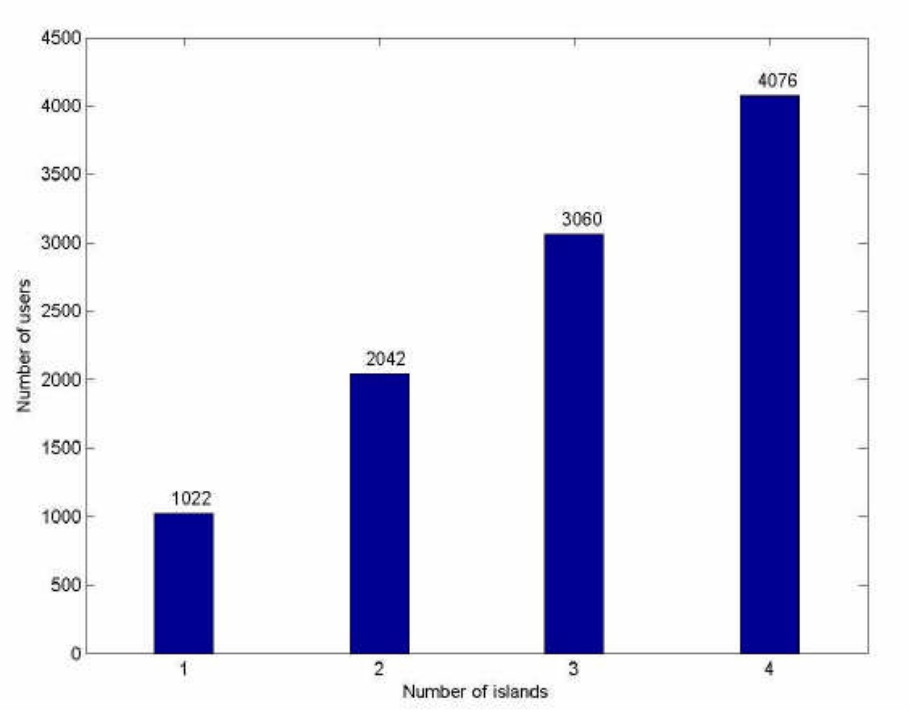


Figura 5.4 – Número de clientes suportados nos 4 cenários analisados (IPTComm, 2007).

Foram considerados para avaliação do nível de CPU os seguintes cenários:

1) Topologia com duas ilhas com 150 clientes locais e 150 clientes remotos;
2) Topologia com três ilhas com:
    (a) 100 clientes locais e 200 remotos igualmente distribuídos entre os dois *focus* remotos;
    (b) 150 clientes locais e 150 remotos igualmente distribuídos entre os dois *focus* remotos.
3) Topologia com quatro ilhas com:
    (a) 75 clientes locais e 225 remotos igualmente distribuídos entre os três *focus* remotos;
    (b) 150 clientes locais e 150 remotos igualmente distribuídos entre os três *focus* remotos.

No primeiro cenário com 150 clientes no focus principal e 150 clientes no focus remoto, a carga de CPU do *focus* principal foi de aproximadamente 30,04%, enquanto a do *focus* remoto era aproximadamente 20,19%, conforme a Figura 5.5.

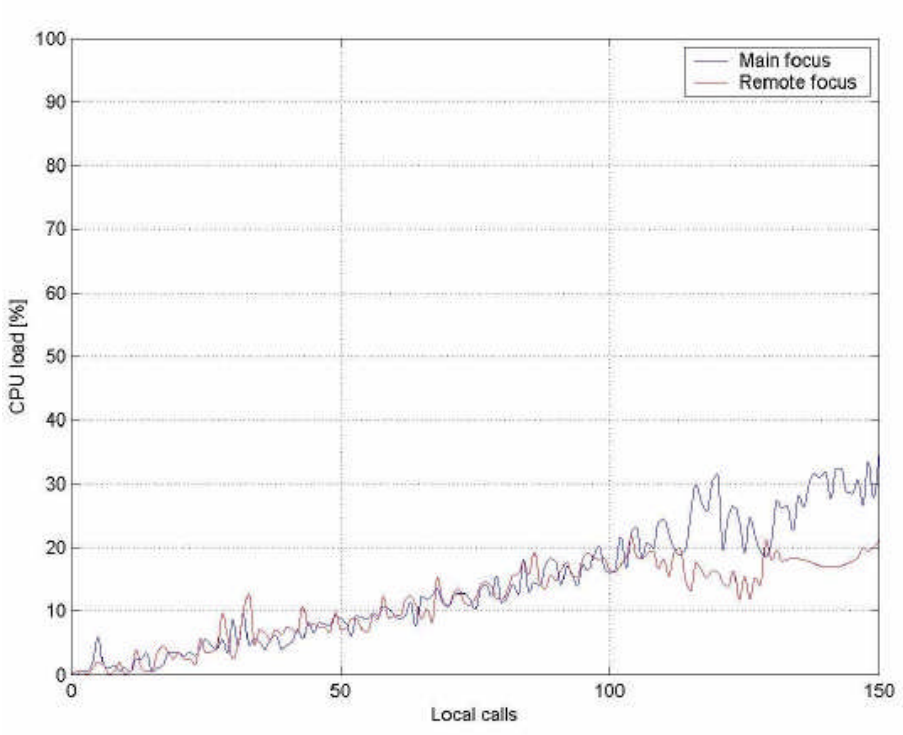


Figura 5.5 – Utilização de CPU no cenário distribuído com 2 ilhas (IPTComm, 2007).

No cenário 2(a) composto por três ilhas, uma contendo o *focus* principal e as outras duas *focus* remotos, com 300 clientes igualmente distribuídos entre as ilhas, o nível de utilização de CPU do *focus* principal era de aproximadamente 20% e em ambos os *focus* remotos a carga ficou em aproximadamente 18%. Isto é apresentado na Figura 5.6.

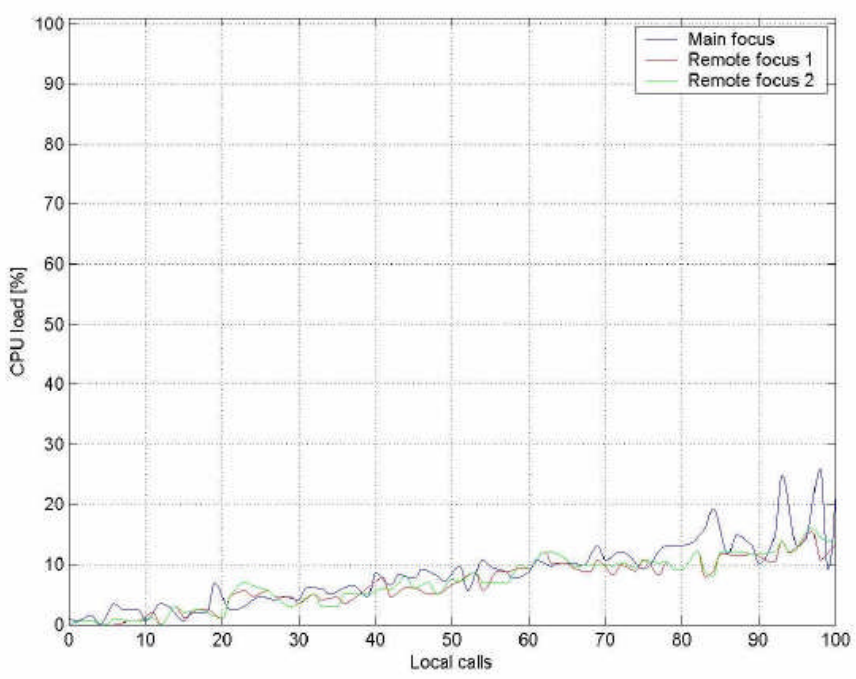


Figura 5.6 - Utilização de CPU no cenário distribuído com 3 ilhas – 2a (IPTComm, 2007).

No caso 2(b), com 150 clientes no *focus* principal e 150 clientes igualmente distribuídos entre os dois *focus* remotos, a CPU do *focus* principal chegou a 31,2%, enquanto a CPU dos *focus* remotos estavam praticamente sem carga (nível de utilização da CPU aproximadamente 12%).

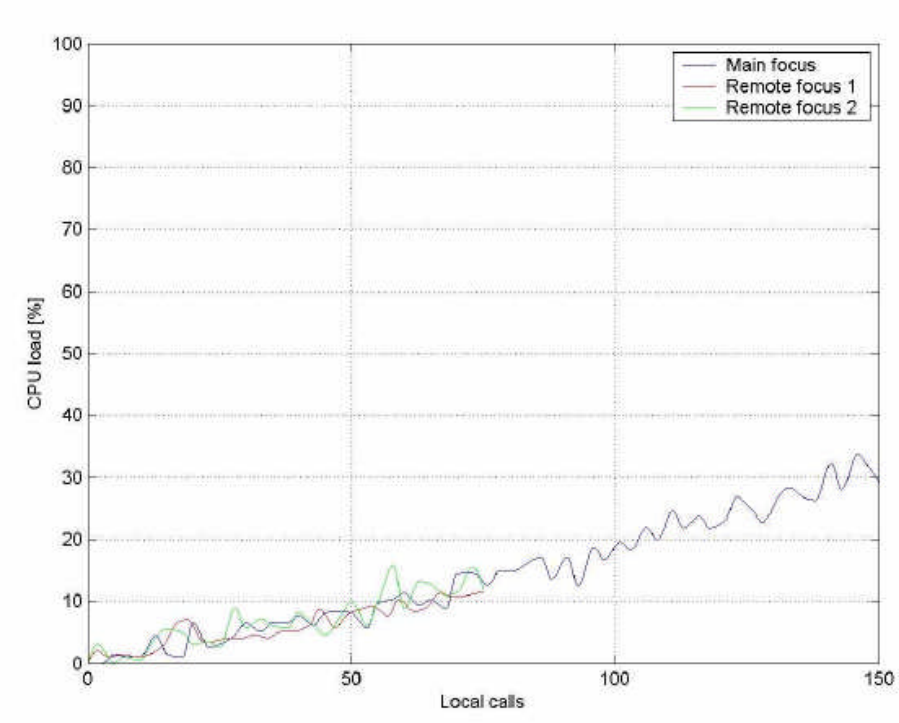


Figura 5.7 - Utilização de CPU no cenário distribuído com 3 ilhas – 2b (IPTComm, 2007).

No cenário 3(a), composto por quatro ilhas, uma contendo o *focus* principal e as outras três *focus* remotos, com 300 clientes igualmente distribuídos entre elas, o consumo de CPU do *focus* principal foi de 12,66% e 12% nos *focus* remotos, conforme representado na Figura 5.8.

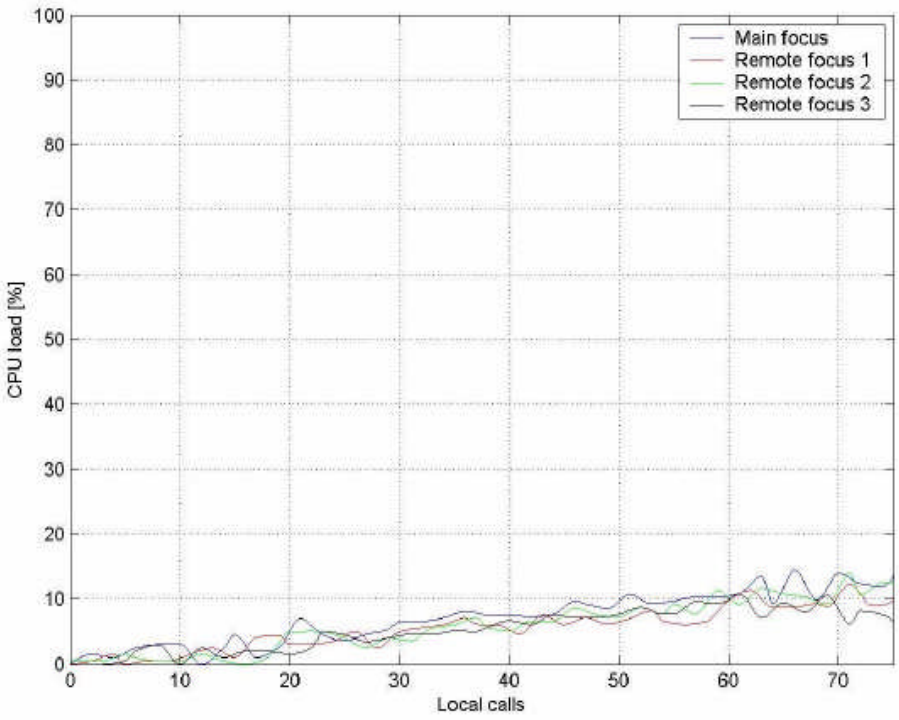


Figura 5.8 - Utilização de CPU no cenário distribuído com 4 ilhas – 3a (IPTComm, 2007).

No caso 3(b), com 150 clientes no *focus* principal e 150 clientes igualmente distribuídos entre os três *focus* remotos, a utilização de CPU do *focus* principal foi de 32,4% e 7,8% nos *focus* remotos. Este resultado é apresentado na Figura 5.9.

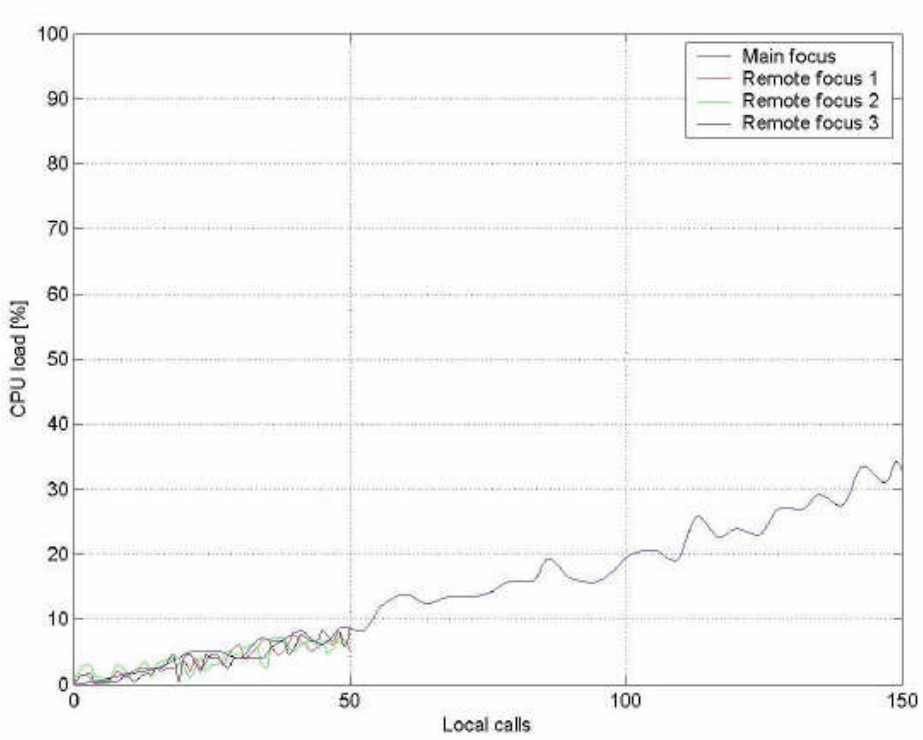


Figura 5.9 - Utilização de CPU no cenário distribuído com 4 ilhas – 3b (IPTComm, 2007).

5.1.4 Análise comparativa

Nesta seção, serão analisados os resultados apresentados na seção 5.1.3 e resumidos na Tabela 5.1, mostrando como a migração de um cenário centralizado para um cenário descentralizado melhora o desempenho em termos de escalabilidade.

Tabela 5.1 – Comparação entre os cenários adaptado de (IPTComm,2007).

Número de ilhas	Número de usuários locais	Número de usuários remotos	Carga da CPU do Focus principal	Carga da CPU do Focus remoto 1	Carga da CPU do Focus remoto 2	Carga da CPU do Focus remoto 3
1	300	-	99,40%	-	-	-
2	150	150	30,04%	20,19%	-	-
3	100	200 (100/100)	20%	18%	18%	-
3	150	150 (75/75)	31,05%	12%	12%	-
4	75	225 (75/75/75)	12,66%	12%	12%	12%
4	150	150 (50/50/50)	32,40%	7,80%	7,80%	7,80%

Deve ser observado que os testes mostraram uma grande melhoria em termos de desempenho de CPU. No cenário centralizado a carga de CPU estava próxima de 100% enquanto no cenário descentralizado foi reduzida para aproximadamente 30%, no caso de

duas ilhas, 20% no caso de três ilhas e aproximadamente 12% no caso de quatro ilhas. Além disso, notou-se que a soma da carga de CPU de todos os *focus* envolvidos nos cinco cenários também era inferior que a carga da plataforma centralizada.

Finalmente, analisando os testes apresentados no caso 1, caso 2(b) e caso 3(b), pode ser observado como a distribuição dos clientes remotos atrás de diferentes *focus* remotos causa uma pequena diminuição no desempenho do *focus* principal. Isto parece razoável quando se leva em conta que o *focus* principal tem de divulgar os eventos de conferência para todos os *focus* ativos através dos canais servidor-para-servidor, o que acaba se tornando um potencial limitador para o sistema inteiro.

5.2 – Análise de Cenários

A recomendação de qual *framework* é mais adequado para ser implantado na rede da Brasil Telecom é baseada em uma série de fatores entre os quais o desempenho e a escalabilidade avaliados na seção 5.1, e o valor do investimento, os custos operacionais e as características da operadora (distribuição de clientes, área de atuação, interesse de tráfego) que são discutidos nesta seção. Assim, nesta seção será feita uma análise econômico-financeira dos dois *frameworks* de conferência (Centralizada e Distribuída) e considerando três diferentes topologias para cada *framework.* Esta análise utilizou o método de Valor Presente Líquido (VPL) para verificar qual cenário, entre os propostos, apresenta melhor resultado econômico-financeiro.

5.2.1 – Metodologia

Para avaliar qual o *framework* mais adequado do ponto de vista econômico-financeiro será utilizada uma metodologia de análise de fluxo de caixa.

Para poder realizar este estudo foi criada uma demanda de clientes de videoconferência. Para este estudo foi definido como cliente o equipamento de usuário capaz de participar de uma conferência, portanto uma empresa com 20 equipamentos terminais de videoconferência ou 20 PCs que possuam software que permite participar de uma videoconferência é considerada como 20 clientes, variando somente a faixa necessária para a conexão com o misturador.

Esta demanda foi criada da seguinte forma: multiplicou-se o número atual de clientes que utilizam o serviço de videoconferência da Brasil Telecom, obtido do relatório

fornecido pela Diretoria de Receita da empresa, por um fator de correção arbitrário. Este procedimento foi necessário para evitar a divulgação de dados confidenciais da empresa.

O relatório apresentava o número de clientes por município e a faixa de acesso contratada. Como a quantidade de municípios com clientes era maior que 200 e a maior parte destes municípios possuíam 1 ou 2 clientes, foi adotada uma simplificação, ou seja, diminuir o tamanho da matriz de tráfego utilizada no estudo.

Estes clientes foram agrupados em 19 regiões dentro da área de concessão da Brasil Telecom. Estas regiões estão divididas da seguinte forma:

- 9 regiões que representam os clientes localizados nas capitais dos estados da região de concessão da Brasil Telecom.
- 9 regiões que englobam os clientes localizados nas cidades do interior dos estados da região de concessão da Brasil Telecom.
- Uma região que engloba os clientes do Distrito Federal.

Os clientes de cada região foram divididos em 4 intervalos de acordo com a faixa de acesso contratada:

- (A) de 0 a 256kbps;
- (B) de 256kbps a 512kbps;
- (C) de 512kbps a 1Mbps;
- (D) acima de 1Mbps.

O número de clientes por região e divididos nos intervalos de faixa são apresentados na tabela 5.2. Devido ao fato da informação sobre demanda de clientes para o serviço de videoconferência da Brasil Telecom ser considerada estratégica, os valores foram normalizados para evitar a divulgação de informações sigilosas.

Tabela 5.2 – Demanda para o serviço de videoconferência da Brasil Telecom.

Regiões	Banda							
	(A) até 256kbps		(B) entre 256 e 512kbps		(C) entre 512 kbps e 1Mbps		(D) acima de 1Mbps	
	SIP	H.323	SIP	H.323	SIP	H.323	SIP	H.323
Brasília	800	100	40	100	30	10	20	0
Campo Grande	194	24	10	24	7	2	5	0
MS	213	27	11	27	8	3	5	0
Cuiabá	136	17	7	17	5	2	3	0
MT	272	34	14	34	10	3	7	0
Curitiba	896	112	45	112	34	11	22	0
PR	1087	136	54	136	41	14	27	0
Florianópolis	435	54	22	54	16	5	11	0
SC	815	102	41	102	31	10	20	0
Goiânia	467	58	23	58	18	6	12	0
GO	376	47	19	47	14	5	9	0
Palmas	37	5	2	5	1	0	1	0
TO	90	11	4	11	3	1	2	0
Porto Alegre	1264	158	63	158	47	16	32	0
RS	926	116	46	116	35	12	23	0
Porto Velho	82	10	4	10	3	1	2	0
RO	120	15	6	15	4	1	3	0
Rio Branco	55	7	3	7	2	1	1	0
AC	22	3	1	3	1	0	1	0
Total	8286	1036	414	1036	311	104	207	0

Para realizar o estudo não é suficiente saber o número de clientes por área, é necessário saber com quem estes clientes querem se comunicar, portanto foi criada uma matriz de interesse de tráfego percentual, apresentada no apêndice A.1, entre todas as regiões, incluindo o interesse de tráfego para fora da região da Brasil Telecom. Neste estudo, como simplificação, foi adotado que este interesse de tráfego para fora da região da Brasil Telecom seria concentrado em São Paulo.

A seguir foi criada uma matriz de que mostra a faixa de transmissão gerada pelos clientes entre as regiões. Para criar esta matriz admitiu-se que durante o período de maior movimento, 25% dos clientes estariam utilizando o serviço de videoconferência. Desse modo, para definir qual a faixa proveniente de Brasília em direção a Campo Grande, foi somado o número de clientes de Brasília SIP e H.323 que utilizam até 256 kbps e multiplicado por 192 kbps (velocidade média dos clientes deste grupo). O mesmo procedimento foi realizado para os grupos de clientes entre 256 e 512 kbps (multiplicando por 384), entre 512 e 1024 kbps (multiplicando por 768) e para o grupo cuja faixa é superior a 1024 kbps (multiplicando por 1500). O resultado destas operações foi somado e

multiplicado por 0,25 (25%) e pelo valor percentual do interesse de tráfego de Brasília para Campo Grande, fornecido pela matriz de interesse de tráfego.

Para que seja disponibilizada esta faixa de transmissão é necessário um investimento que depende da distância entre as regiões. Para simplificar os cálculos de custos e tarifas, que dependem da distância, as operadoras de telecomunicações utilizam o conceito de "degrau". Degrau é um intervalo, onde a variação da distância não altera o custo ou a tarifa do serviço que está sendo prestado. A Tabela 5.3 apresenta os nove degraus utilizados neste trabalho e os seus intervalos.

Tabela 5.3 – Padrão de distâncias.

D0 - Local
D1 - para distâncias até 50 km
D2 - para distâncias superiores a 50 km e até 100 km
D3 - para distâncias superiores a 100 km e até 200 km
D4 - para distâncias superiores a 200 km e até 300 km
D5 - para distâncias superiores a 300 km e até 500 km
D6 - para distâncias superiores a 500 km e até 700 km
D7 - para distâncias superiores a 700 km e até 1000 km
D8 - para distâncias superiores a 1000 km

Com base nas distâncias geodésicas entre as regiões e nos degraus definidos foi criada uma matriz de distâncias apresentada no apêndice A.2.

Para cada intervalo de distâncias foi determinado um valor anual de Opex (*Operational Expenditure*) e o Capex (*Capital Expenditure*) para transportar 2 Mbps, utilizando os custos médios adotados pela Brasil Telecom, conforme a Tabela 5.4.

Tabela 5.4 – Capex e Opex em R$ em função da distância.

Distância	OPEX	CAPEX
D0	441,3	526,2
D1	600,4	526,2
D2	822,6	734,9
D3	1042,9	1152,5
D4	1125,9	1570,0
D5	1169,0	2405,1
D6	1173,5	3240,2
D7	1175,1	4492,8
D8	1175,8	4701,6

Para determinar o investimento em transmissão basta dividir o valor da faixa de transmissão entre duas áreas, apresentada no apêndice A.3 para o cenário 2A, por 2 Mbps e multiplicar pelo valor correspondente da coluna Capex considerando o intervalo que melhor representa a distância entre a origem e o destino. Porém, esta distância depende da localização do misturador. Assim, caso seja colocado um misturador em Campo Grande, o fluxo de vídeo entre Porto Velho e Rio Branco deverá ir a Campo Grande para ser misturado e retornar para suas origens. Caso o misturador que atenda Porto Velho e Rio Branco esteja em Brasília, os fluxos de vídeo devem vir a Brasília para que sejam misturados e retornar as suas origens. Portanto a distância que o fluxo de vídeo irá percorrer dependerá da localização dos misturadores (matriz de distâncias apresentada no apêndice A.4), e desta forma, os custos de Opex e Capex também dependem da localização dos misturadores. As matrizes de Capex e Opex para o cenário 2A são apresentadas nos apêndices A.5 e A.6 respectivamente.

Para que fosse verificada qual a influência dos custos de transmissão e dos custos de equipamentos misturadores e de controle, foram criadas três topologias A, B e C, que se diferenciam entre si pela quantidade e localização dos misturadores e dos controladores.

A topologia A tem 2 controladores e os misturadores estão divididos em 5 localidades, esta alternativa corresponde à atual topologia da rede de videoconferência da Brasil Telecom. A topologia B tem 5 controladores e os misturadores estão divididos em 7 localidades, esta alternativa foi proposta para avaliar se uma maior distribuição dos elementos pode diminuir os custos da rede. A topologia C, por sua vez, tem 2 controladores e os misturadores estão divididos em 2 localidades, esta alternativa foi proposta para avaliar se uma maior concentração de equipamentos poderia diminuir os custos da rede.

A Tabela 5.5 apresenta as topologias A, B e C definindo a localização dos misturadores e controladores.

Tabela 5.5 – Alternativas de topologia.

	Controladores	Misturadores
Topologia A	Brasília, Curitiba	Brasília, Campo Grande, Curitiba, Florianópolis, Porto Alegre
Topologia B	Brasília, Campo Grande, Curitiba, Florianópolis, Porto Alegre	Brasília, Campo Grande, Cuiabá, Curitiba, Florianópolis, Goiânia, Porto Alegre
Topologia C	Brasília, Curitiba	Brasília, Curitiba

A topologias A, B e C foram utilizadas na avaliação dos dois *frameworks*. Quando aplicadas no *framework* centralizado geraram os cenários denominados 1A, 1B e 1C, quando aplicadas no *framework* distribuído geraram os cenários chamados de 2A, 2B e 2C. A Tabela 5.6 apresenta os seis cenários utilizados na avaliação econômica.

Tabela 5.6 – Cenários da avaliação econômica.

	Framework de Conferência	Controladores	Misturadores
Cenário 1A	Centralizada	Brasília, Curitiba	Brasília, Campo Grande, Curitiba, Florianópolis, Porto Alegre
Cenário 1B	Centralizada	Brasília, Campo Grande, Curitiba, Florianópolis, Porto Alegre	Brasília, Campo Grande, Cuíaba, Curitiba, Florianópolis, Goiânia, Porto Alegre
Cenário 1C	Centralizada	Brasília, Curitiba	Brasília, Curitiba
Cenário 2A	Distribuída	Brasília, Curitiba	Brasília, Campo Grande, Curitiba, Florianópolis, Porto Alegre
Cenário 2B	Distribuída	Brasília, Campo Grande, Curitiba, Florianópolis, Porto Alegre	Brasília, Campo Grande, Cuíaba, Curitiba, Florianópolis, Goiânia, Porto Alegre
Cenário 2C	Distribuída	Brasília, Curitiba	Brasília, Curitiba

Para os equipamentos, misturadores e controladores, foram adotados valores de Capex e Opex baseados nas seguintes premissas:

- Misturador para 80 fluxos simultâneos: Capex = R$ 315.000 e Opex = a 10% do valor do Capex por ano (valores médios das últimas aquisições da Brasil Telecom).
- Controladores: Capex = R$ 149,3 por cliente e Opex = a 10% do valor do Capex por ano (valores médios das últimas aquisições da Brasil Telecom).

Assumindo que a demanda, apresentada anteriormente, irá gerar uma receita de R$ 3.000.000,00 por ano, foi feita uma avaliação financeira para determinar qual dentre estes seis cenários apresenta a melhor relação entre o investimento e receita.

Nesta análise financeira foi utilizada uma ferramenta clássica de avaliação de investimentos baseada em fluxo de caixa descontado, a análise de Valor Presente Líquido (VPL) (Monteiro, 2003). Este método será descrito na próxima seção.

5.2.2 – Método do VPL

Para entender o método VPL, é importante entender o conceito de fluxo de caixa. Denomina-se fluxo de caixa ao conjunto de entradas e saídas de dinheiro ou equivalente a dinheiro, ao longo do tempo, para um indivíduo ou empresa. As entradas correspondem aos recebimentos e as saídas correspondem aos pagamentos ou desembolsos.

Graficamente o fluxo de caixa é representado através do Diagrama de Fluxo de Caixa (DFC), conforme as seguintes convenções: no eixo horizontal é marcada a escala de tempo, subdividida em sub-períodos (meses, anos, dias, etc); o ponto 0 é a data inicial ou data zero, a partir da qual, todas as demais se encontrarão relacionadas; as quantias são representadas por segmentos verticais, que na medida do possível devem ser proporcionais aos respectivos valores; entradas de caixa correspondem a segmentos traçados acima do eixo horizontal e saídas de caixa correspondem a segmentos traçados abaixo.

A Figura 5.10 apresenta um DFC típico onde os fluxos FC1, FC3 e FCn correspondem a entradas de caixa e FC0 e FC2 correspondem a saídas de caixa.

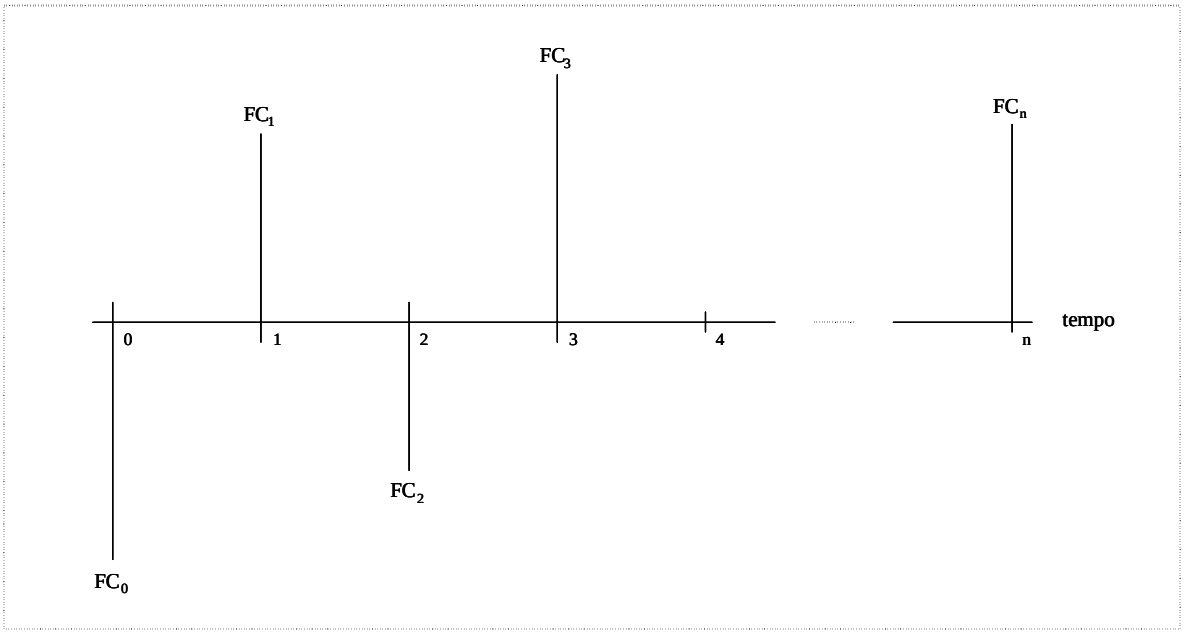


Figura 5.10 – Diagrama de Fluxo de Caixa (DFC) adaptado de (Zentgraf, 2002).

Apesar de simples, o conceito de fluxo de caixa é extremamente relevante em finanças, pois a grande maioria dos problemas de matemática financeira recai na resolução de alguns poucos diagramas predefinidos.

É importante ser considerado na montagem de um fluxo de caixa o cuidado com despesas ou receitas que não representem efetivas saídas ou entradas de caixa, tais como despesas de depreciação, provisões, reversões e outros, ou seja, não confundir lucro com fluxo de caixa.

Será apresentado um exemplo bastante ilustrativo de Zentgraf (2002) para melhor explicar a utilização do fluxo de caixa e definir alguns conceitos adicionais.

Exemplo: Uma empresa planeja adquirir uma máquina que irá proporcionar redução em seus custos de produção (custos hoje estimados em $500,00/ano passarão a $400,00/ano). Monte o DFC para a proposta sabendo que a nova máquina custará $1.500,00, possui cinco anos de vida útil (sem valor residual) e que a alíquota de IR (Imposto de Renda) para a empresa é de 30,00%.

Solução: A grosso modo, o resultado (ou lucro) de uma empresa será o valor das receitas por ela obtida diminuído das despesas que incorreu. A cada ano as empresas são obrigadas a apurar seus resultados com base nesta definição. Caso as receitas superem as despesas, haverá lucro e a empresa pagará imposto; caso contrário haverá prejuízo, que poderá ser compensado com lucros futuros, observados os limites estabelecidos na legislação.

Cálculo da Depreciação: A aquisição de uma máquina utilizada em processo produtivo é uma despesa que a empresa incorrerá, e como tal deverá ser deduzida da base de cálculo do IR. O lançamento de todo o custo da aquisição como despesa logo no primeiro ano, entretanto, estará inadequado, pois o equipamento servirá à empresa por cinco anos. Note ainda que caso assim fosse feito, estaria-se diminuindo em excesso a base de cálculo do IR no primeiro ano, o que certamente a Receita Federal não deseja. Sendo assim, contábil e fiscalmente correto será o lançamento a cada ano de uma fração deste investimento, denominada despesa de depreciação. No exemplo, a máquina não possui valor residual (valor de revenda ao fim da vida útil) e dura cinco anos; a despesa de depreciação será portanto, de $300,00/ano (=$1.500,00/5). Observe que esta é uma despesa que não irá representar uma saída de caixa já que todos os pagamentos a ela relacionados foram efetuados por ocasião da compra da máquina.

Cálculo do Fluxo de Caixa Incremental: Conforme os dados listados no Demonstrativo de Resultados do Exercício (DRE) da Tabela 5.7, onde a coluna “Sem”

apresenta os resultados atuais da empresa em análise, a coluna “Com” os resultados caso o equipamento seja adquirido, e a coluna “Delta-Caixa” as variações de fluxo de caixa relevantes à análise desta aquisição (equivale à coluna “Com” subtraída da coluna “Sem”). Observe:

- Como o enunciado não especifica alteração nas receitas caso o equipamento seja adquirido, assume-se que serão fixas e iguais a $2.000,00/ano;
- A redução dos custos, por permitir à empresa um menor desembolso, aparece na variação positiva (entrada de caixa) na coluna “Delta-Caixa”;
- A depreciação não entra na última coluna, pois não representa saída de caixa; também não devem ser incluídos na última coluna os resultados provenientes das linhas de cálculo utilizadas na DRE (linhas LAIR e Lucro Líquido);
- O LAIR (Lucro Antes do Imposto de Renda, correspondente à base de cálculo do IR) será reduzido caso a máquina seja adquirida; a empresa, portanto, pagará menos imposto e conseqüentemente a variação de caixa será positiva. Cabe observar que o valor obtido ($60,00) é a resultante de dois efeitos opostos: o primeiro, referente à redução dos custos, contribuirá para um aumento da carga tributária em $30,00 (=$100,00x30,00%) e o segundo, referente à dedutibilidade da despesa de depreciação do LAIR, contribuirá para a redução da carga tributária (benefício fiscal) em $90,00 (=$300,00x30,00%);
- A diferença entre o lucro líquido e o fluxo de caixa fica por conta da depreciação, que entra no cálculo do lucro líquido, mas não pode ser considerada no cálculo do fluxo de caixa líquido.

Tabela 5.7 – VPL por cenário analisado

DRE	Sem ($)	Com ($)	Delta-Caixa ($)
Receitas	2.000,00	2.000,00	0
(-) Custos	-500	-400	100
(-) Depreciação	0	-300	0
(=) LAIR	1.500,00	1.300,00	
(-) IR	-450	-390	60
(=) Lucro Líquido	1.050,00	910	
(+) Depreciação	0	300	0
Fluxo de Caixa Líquido	**1.050,00**	**1.210,00**	**160**

Traçado do DFC: Dado o investimento inicial de $1.500,00, as entradas de caixa líquidas de $160,00/ano e o prazo de cinco anos para o projeto, tem-se na Figura 5.11 o DFC resultante.

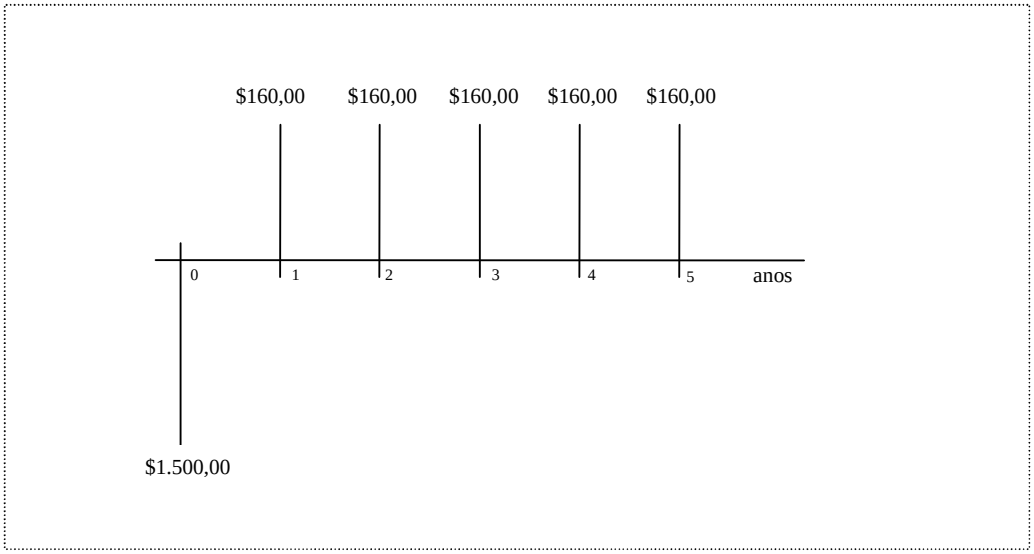


Figura 5.11 – Diagrama de Fluxo de Caixa do Exemplo.

Segundo Monteiro (2003), o valor presente líquido (VPL) ou método do valor atual é uma forma matemático-financeira de se determinar o valor presente de pagamentos futuros, descontados a uma taxa de juros apropriada, menos o custo do investimento inicial. Basicamente, é o calculo de quanto os futuros pagamentos somados a um custo inicial estaria valendo atualmente. Deve ser considerado o conceito de valor do dinheiro no tempo, ou seja, R$ 1 milhão hoje, não valeria R$ 1 milhão daqui a um ano, devido ao custo de oportunidade de se colocar, tal montante de dinheiro na poupança ou em outra aplicação para render juros.

Este método é usado para a análise do orçamento de capitais - planejamento de investimentos a longo prazo. Usando o método VPL um projeto de investimento potencial deve ser empreendido se o valor presente de todas as entradas de caixa menos o valor presente de todas as saídas de caixa (que iguala o valor presente líquido) for maior que zero. Se o VPL for igual a zero, o investimento é indiferente, pois o valor presente das entradas é igual ao valor presente das saídas de caixa; se o VPL for menor do que zero, significa que o investimento não é economicamente atrativo, já que o valor presente das entradas de caixa é menor do que o valor presente das saídas de caixa.

Para cálculo do valor presente das entradas e saídas de caixa é utilizado o custo ponderado de capital (WACC - *Weighted Average Cost of Capital*) como taxa de desconto. As vantagens principais do método VPL são:

- Ao contrário da taxa média de retorno contábil, o método VPL usa fluxos de caixa ao invés de lucros líquidos, incluindo a depreciação como fonte de recursos. Esta característica torna a abordagem do VPL consistente com a teoria financeira moderna;
- O VPL, ao contrário da taxa média de retorno e do *payback* simples, reconhece o valor do dinheiro no tempo;
- Ao aceitar projetos com VPL positivos, a empresa também aumentará o seu valor (visando a maximização da riqueza dos acionistas) e não correrá o risco de aceitar um projeto com retorno negativo, num projeto onde existam múltiplas taxas de retorno;
- Na comparação entre dois projetos de investimentos, o método do VPL permite que seja encontrada uma taxa de desconto ajustada ao risco de cada projeto, eliminando o problema de comparação entre projetos de perfis de risco diferenciados;
- Na escolha entre dois projetos de investimentos mutuamente excludentes (ou independentes), nos quais distintas taxas de desconto podem inverter a ordem de preferência entre projetos, o método do VPL é sempre o mais adequado, pois evita que decisões erradas sejam tomadas com base na TIR (Taxa Interna de Retorno), que é uma taxa de desconto que iguala o valor presente dos fluxos de caixa futuros ao investimento inicial, individual dos projetos.

A fórmula do VPL das receitas líquidas é dada por (Monteiro, 2003):

$$VPL = \sum_{t=1}^{T} \frac{C_t}{(1+r)^t} - \mathrm{I} \qquad (5.1)$$

onde:

r = taxa de desconto;

Ct = é o fluxo de caixa líquido para o período t;

I = investimento inicial;

T = número de períodos do projeto.

Um ponto crítico da abordagem do VPL está na decisão de qual taxa de desconto utilizar. As taxas de desconto são influenciadas pelo nível de risco e duração do projeto, e tendem a subir acompanhando taxas de juros e inflação. Assim, o VPL apresentado sem o ajuste de risco, com base na premissa de que os valores de fluxo de caixa estimados são absolutamente precisos, podem levar à aceitação de um projeto que deveria ser rejeitado ou vice-versa. Nesta dissertação foi adotado que a taxa de desconto será igual ao WACC utilizado pela Brasil Telecom definido pela Diretoria de Análise de Investimentos e corresponde a 11,5%.

5.2.3 – Resultados

Aplicando a demanda anteriormente apresentada nos seis cenários previamente definidos, utilizando os custos de Opex e Capex, são obtidos os seguintes valores em R$ apresentados na Tabela 5.8.

Tabela 5.8 – Capex e Opex de transmissão e equipamentos por cenário analisado.

	Capex Transmissão	Opex Transmissão	Capex Equipamentos	Opex Equipamentos
Cenário 1A	R$ 1.868.512	R$ 601.009	R$ 6.615.000	R$ 819.000
Cenário 1B	R$ 1.864.754	R$ 595.639	R$ 6.930.000	R$ 913.500
Cenário 1C	R$ 1.924.672	R$ 616.304	R$ 6.300.000	R$ 693.000
Cenário 2A	R$ 850.955	R$ 449.134	R$ 6.865.900	R$ 844.090
Cenário 2B	R$ 758.469	R$ 403.282	R$ 7.192.847	R$ 939.785
Cenário 2C	R$ 1.389.171	R$ 565.524	R$ 6.538.952	R$ 716.895

Os valores de *Ct* obtidos para cada ano, considerando 0 o ano de implantação e 5 o último ano do estudo, são apresentados na Tabela 5.9:

Tabela 5.9 - Fluxo de caixa para os cenários analisados (em R$).

	C(0)	C(1)	C(2)	C(3)	C(4)	C(5)
Cenário 1A	8.483.512	2.156.870	2.156.870	2.156.870	2.156.870	2.156.870
Cenário 1B	8.794.754	2.088.904	2.088.904	2.088.904	2.088.904	2.088.904
Cenário 1C	8.224.672	2.249.974	2.249.974	2.249.974	2.249.974	2.249.974
Cenário 2A	7.716.855	2.231.523	2.231.523	2.231.523	2.231.523	2.231.523
Cenário 2B	7.951.316	2.197.623	2.197.623	2.197.623	2.197.623	2.197.623
Cenário 2C	7.928.123	2.256.693	2.256.693	2.256.693	2.256.693	2.256.693

Considerando que o período de estudo é de 5 anos, aplicando os valores da Tabela 5.9 na fórmula do VPL (5.1), obtemos os resultados apresentados na Tabela 5.10:

Tabela 5.10 – VPL por cenário analisado.

	VPL
Cenário 1A	- R$ 611.202
Cenário 1B	- R$ 1.170.508
Cenário 1C	- R$ 12.543
Cenário 2A	R$ 427.930
Cenário 2B	R$ 69.738
Cenário 2C	R$ 308.530

Este estudo mostra que, para as premissas e parâmetros adotados, através da utilização da metodologia apresentada o cenário que apresenta o maior VPL é o 2A.

Porém, durante a avaliação econômica notou-se que o custo do misturador é uma das partes que mais influência no resultado do VPL. Desta forma, um custo maior ou menor do misturador poderia alterar o cenário que apresenta o maior VPL.

Com base em diversas tomadas de preço realizadas pela Brasil Telecom nos últimos anos, notou-se que o custo das MCUs tem variado muito pouco, o que varia significativamente são as funcionalidades e a capacidade do equipamento de suportar certo número de fluxos de mídia simultâneos.

Neste estudo, o custo utilizado para o equipamento misturador corresponde ao valor de uma MCU com capacidade de tratar, em média, 80 fluxos simultâneos. Este valor foi utilizado porque ainda não existem misturadores disponíveis no mercado e portanto, ainda não tem preço definido.

Quando os misturadores forem lançados no mercado o custo pode ser maior ou menor que o considerado por este estudo. Para avaliar o impacto desta variação de custo foi realizado um teste de sensibilidade para o custo do misturador. Neste teste o valor do misturador foi congelado no valor adotado para 80 fluxos e variou-se o número de fluxos que o misturador pode tratar simultaneamente. Quando a variação no número de fluxos é para um valor maior do que 80 significa que o misturador terá um custo inferior ao adotado inicialmente, por outro lado quando a variação é par um valor menor do que 80 significa que o custo do misturador é maior que a referência utilizada.

A Figura 5.12 mostra o resultado desta variação no número de fluxos tratados por cada misturador no valor do VPL dos 6 cenários.

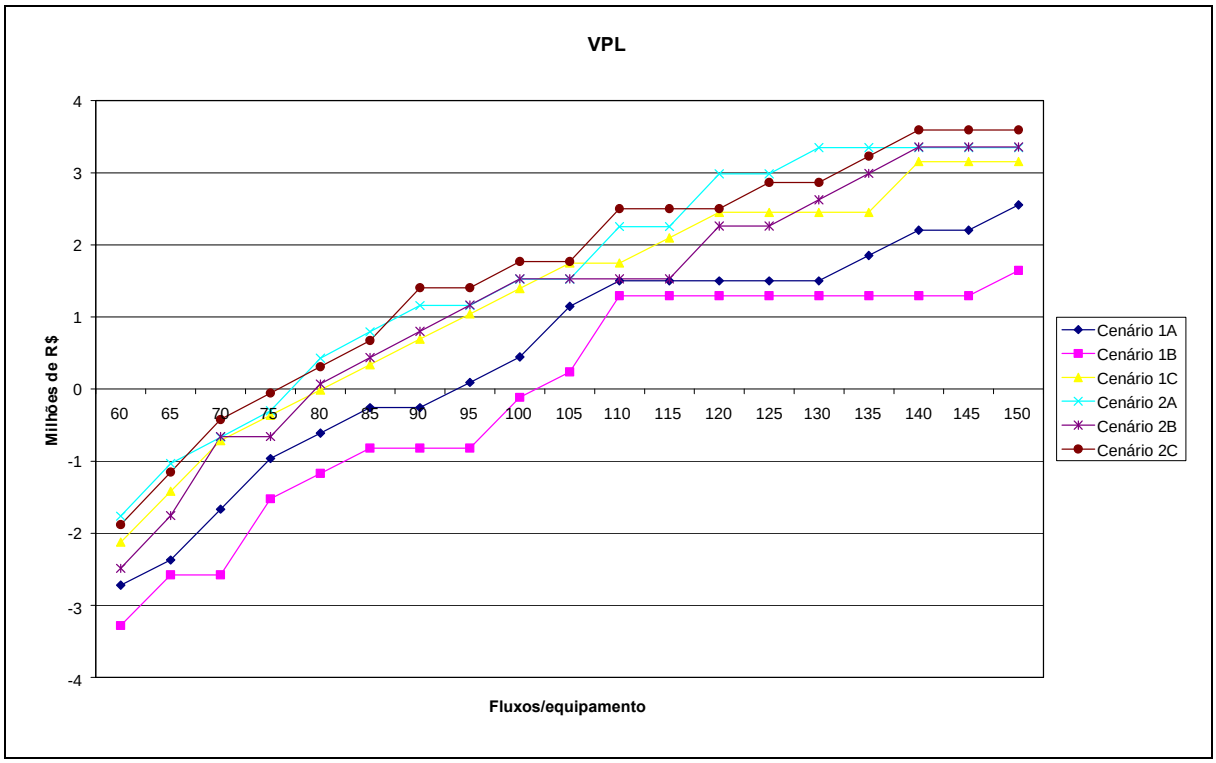


Figura 5.12 – Variação do número de fluxos simultâneos tratados pelo misturador.

Na Figura 5.12 pode ser observado que o valor de VPL mais alto alterna entre o cenário 2A e o cenário 2C, onde ambos utilizam o *framework* distribuído. Além disso, pode ser constatado que nenhum dos cenários de *framework* centralizado (1A, 1B e 1C) tem um VPL mais alto que todos os cenários que usam a *framework* distribuído (2A, 2B e 2C), ou seja, para qualquer um dos valores do intervalo analisado o *framework* distribuído é mais vantajoso do ponto de vista financeiro, segundo a metodologia utilizada.

Porém, esta alternância entre os cenários 2A e 2C dificulta a decisão sobre qual cenário seria o mais adequado do ponto de vista financeiro, pois no primeiro cenário (2A) os misturadores estão distribuídos em 5 localidades e no segundo cenário (2C) os misturadores estão concentrados em apenas 2 localidades.

Para tentar obter mais dados que possam ajudar na convergência para um único cenário, foi analisada a variação do outro parâmetro que tem um peso significativo no estudo, o custo de transmissão.

O custo de transmissão pode ter influência na comparação entre os cenários 2A e 2C, pois no primeiro, como os misturadores estão em 5 localidades, a distância que os fluxos de mídia tem que percorrer até os misturadores é menor do que no cenário 2C, onde os misturadores estão em apenas 2 localidades.

Para verificar a influência do custo da transmissão, primeiramente foram refeitas as curvas para o valor de VPL variando o número de fluxos simultâneos no misturador, considerando um decréscimo de 10% no custo de transmissão. O resultado pode ser observado na Figura 5.13.

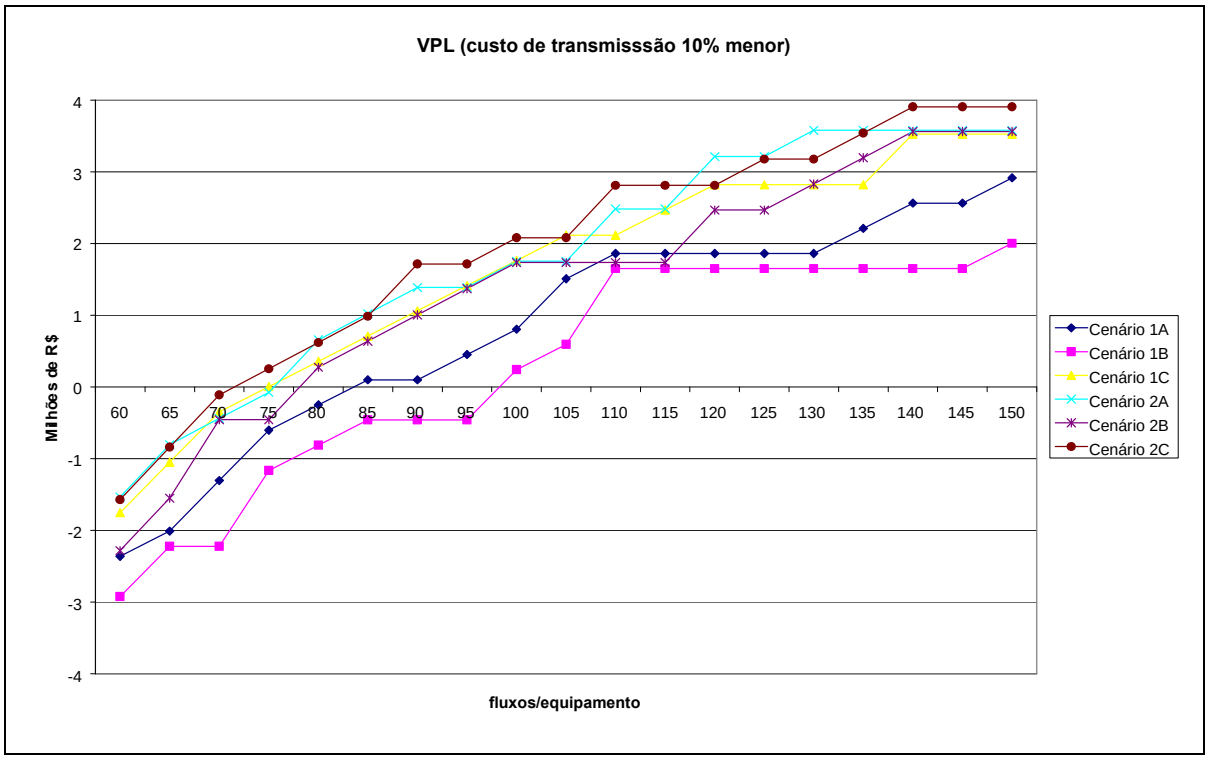


Figura 5.13 – Decréscimo de 10% nos custos de transmissão.

Após foram refeitas as curvas para o valor de VPL variando o número de fluxos simultâneos no misturador, considerando um acréscimo de 10% no custo de transmissão. O resultado pode ser observado na Figura 5.14.

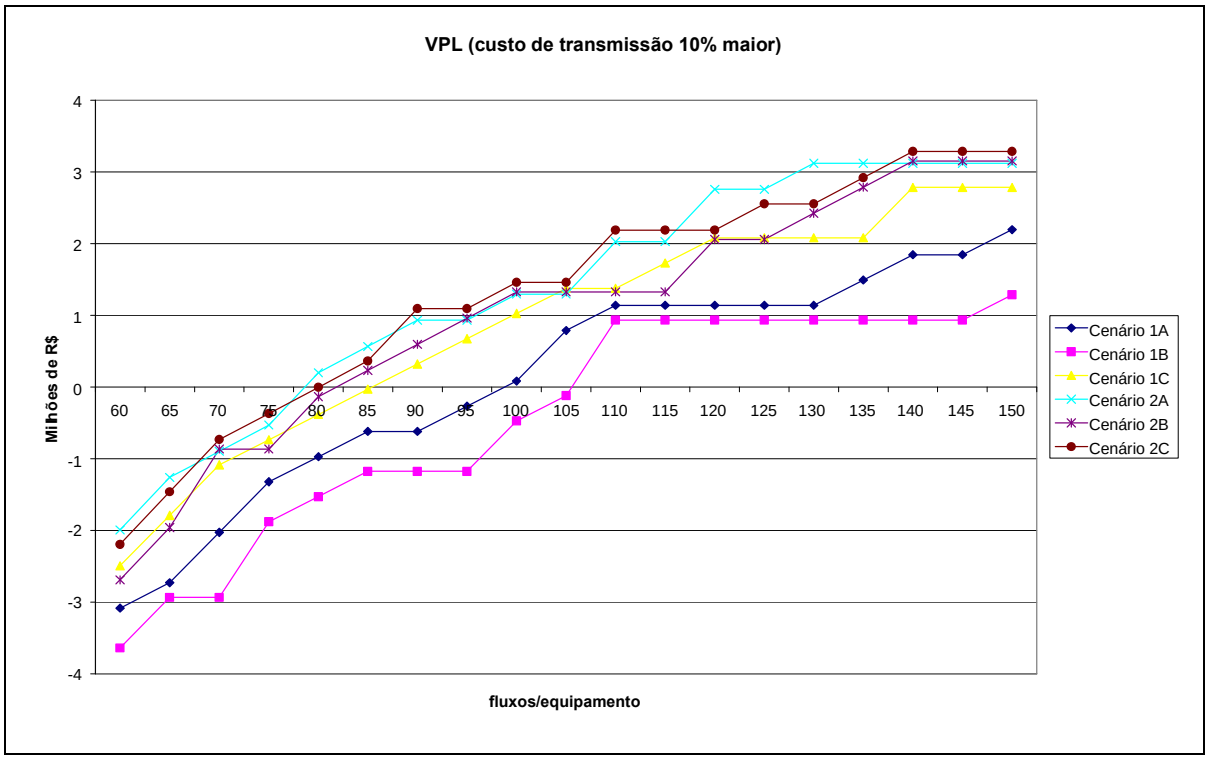


Figura 5.14 – Acréscimo de 10% nos custos de transmissão.

Os gráficos das Figuras 5.13 e 5.14 mostram que mesmo alterando os custos de transmissão para valores menores ou maiores, o resultado praticamente não se altera, ou seja, para a maioria dos pontos o resultado mostrou que o cenário que apresenta o maior VPL continua sendo o mesmo do gráfico da Figura 5.12.

O valor adotado para o número de fluxos simultâneos neste estudo foi de 80 fluxos por equipamento, observando as três curvas o resultado para este ponto, mesmo com a variação do custo de transmissão não se alterou com relação a qual cenário apresenta o maior VPL. Em qualquer uma das curvas o cenário 2A que utiliza o *framework* distribuído apresenta o maior valor de VPL.

6 – DESCRIÇÃO DA SOLUÇÃO PROPOSTA PARA A BRASIL TELECOM

Atualmente na Brasil Telecom, os serviços de conferência de áudio, de vídeo e *Web* estão reunidos em um produto chamado "Multiconferências". Estas diferentes formas de conferência foram integradas para permitir ao cliente flexibilidade para participar da conferência através de um telefone fixo ou celular (somente áudio) ou através de terminais específicos para videoconferência. Esta solução permite ao cliente o agendamento das suas conferências através de interface *Web* ou através do *call center* da empresa.

Qualquer terminal de qualquer operadora, fixa ou móvel, pode participar da audioconferência, porém, para participar da videoconferência o cliente tem que contratar um acesso a VPN (*Virtual Private Network*) da Brasil Telecom (produto denominado "Vetor"). Caso não tenha este acesso, o cliente somente poderá participar da conferência gerando uma chamada RDSI para a plataforma. Caso o cliente não tenha o acesso da Brasil Telecom ou uma conexão RDSI, ele não poderá participar da videoconferência. Desta forma, clientes que possuam equipamentos IP (dedicados ou softwares clientes em PCs) que não estejam na VPN de acesso ao serviço ou que tenham softwares clientes em seus celulares não podem acessar o serviço. Além disso, atualmente os terminais homologados pela Brasil Telecom para acessarem o serviço de videoconferência são baseados apenas em H.323 e não existe nenhum elemento na arquitetura da rede para fazer o interfuncionamento entre o H.323 e o SIP.

Pode-se notar que o serviço, principalmente no que se refere às formas de acesso e aos protocolos de controle, começa a ficar defasado em relação às exigências do mercado de telecomunicações, onde, o uso do SIP tem aumentado enquanto o uso do H.323 tem diminuído. Outro ponto é a introdução de tecnologias de telefonia móvel de terceira geração que permitem serviços de dados com maior velocidade, o que deve tornar o uso do aparelho celular como terminal de videoconferência cada vez mais comum.

Desta forma torna-se necessária uma evolução da arquitetura de rede que suporta o serviço de videoconferência para atender as novas exigências do mercado. Assim, neste capítulo será apresentada uma proposta para evolução do serviço de videoconferências existente na Brasil Telecom.

6.1 – Proposta de Solução

A arquitetura da rede da Brasil Telecom conforme definido no Caderno de Diretrizes de Tecnologia e Arquitetura (Brasil Telecom, 2007) irá evoluir para o padrão definido pelo TISPAN. Conforme apresentado no capítulo 2, a arquitetura TISPAN utiliza o SIP como protocolo de comunicação entre os elementos de controle e os equipamentos de usuário. Portanto, a nova solução de conferência tem como requisito básico o suporte ao SIP.

Atualmente a totalidade dos clientes de videoconferência da Brasil Telecom utiliza equipamentos baseados em H.323. Alguns destes equipamentos podem suportar uma atualização de software para trabalhar com SIP, sendo que a maioria deles teriam que ser substituídos. A Brasil Telecom não pode exigir dos clientes a substituição dos equipamentos, e a solução de videoconferência proposta deverá continuar suportando H.323, até que todos os clientes tenham decidido trocar seus equipamentos.

O capítulo 4 mostrou que a visão dos órgãos de padronização (IETF, 3GPP, ETSI) da evolução da videoconferência passa pela introdução do conceito de *framework* de conferência. Este *framework* pode ser totalmente baseado em SIP ou ser agnóstico ao protocolo de controle. Caso a solução sugerida fosse a utilização de um *framework* SIP seria necessária a utilização de outros mecanismos para que os clientes H.323 pudessem usufruir do serviço de videoconferência.

O capítulo 3 mostrou como pode ser realizado o interfuncionamento entre o SIP e o H.323 através do uso do IWF. Porém, qualquer uma das possibilidades de interfuncionamento apresentadas permite somente a utilização das funcionalidades mais básicas de uma videoconferência. Conforme descrito no início deste capítulo, o diferencial do serviço de conferências da Brasil Telecom está justamente na grande quantidade de funcionalidades disponíveis para os clientes. Desta forma a utilização do *framework* SIP representaria um retrocesso para a maioria dos clientes que são H.323.

A outra alternativa seria utilizar um dos dois *frameworks* apresentados no capitulo 4 que são agnósticos ao protocolo de controle. Tanto o *framework* de conferência distribuída quanto o *framework* de conferência centralizada podem trabalhar com SIP e H.323 simultaneamente sem a perda de funcionalidades.

A utilização de um ou de outro framework não é uma decisão simples e depende da distribuição geográfica dos clientes, do tamanho da rede (atrasos), da quantidade de

clientes (escalabilidade), dos custos dos equipamentos envolvidos, dos custos de transporte dos fluxos de mídia.

No capítulo 5 foram avaliados alguns destes itens. Através de testes de escalabilidade e de uma avaliação financeira utilizando o conceito de VPL foram comparados os dois *frameworks.* O resultado mostrou que, para as condições de contorno definidas, o framework de conferência distribuída pode ser uma solução mais adequada.

Na próxima seção será mostrada uma sugestão de implementação do *framework* de conferência distribuída em uma rede que tenha adotada a arquitetura TISPAN.

6.2 – Elementos da Solução

Os elementos funcionais do *framework* de conferência distribuída têm que ser mapeados dentro dos elementos funcionais da arquitetura TISPAN, principalmente nos elementos do núcleo IMS. A referência TS 24.147 auxilia a desenvolver este mapeamento.

Uma alternativa de implementação do *framework* de conferência na Brasil Telecom pode utilizar o mapeamento das seguintes funções:

- Participante da conferência: Deve ser implementado no equipamento de usuário (UE).
- *Focus*, servidor de controle de sala, serviço de notificação de conferência, servidor de política de conferência e servidores de política de mídia: São implementados dentro de um SIP AS (*Application Server*).
- Controle dos fluxos de mídia: É realizado pelo MRFC (*Media Resource Function Control*).
- Misturador de mídia: É uma função incorporada pelo MRFP (*Media Resource Function Processing*).

Com base na proposta de mapeamento apresentada acima, nota-se que o UE deve suportar SIP, CCP e BFCP para que o participante da sala ou o líder da sala possam desempenhar suas funções corretamente. Todas as mensagens que envolvem o UE (em qualquer direção) devem passar pelo P-CSCF (*Proxy-Call Session Control Function*) que, conforme apresentado no capítulo 2 (seção 2.10.2.1), representa o ponto de acesso ao núcleo IMS.

Todas as mensagens SIP enviadas por, ou destinadas a um UE atravessam um S-CSCF (*Serving-Call Session Control Function*) devidamente alocado. O S-CSCF

inspeciona cada mensagem e determina o correto AS para o qual ela deve ser enviada para continuar o processo.

O MRFC controla os fluxos de mídia que vão para o MRFP usando as informações recebidas do AS e do S-CSCF.

Desta forma todas as entidades lógicas definidas pelo *framework* de conferência distribuída foram mapeadas dentro de elementos da arquitetura TISPAN. A Figura 2.6 apresentou os componentes da arquitetura IMS, a Figura 6.1 apresenta os elementos da arquitetura IMS/TISPAN, envolvidos na prestação do serviço de videoconferência.

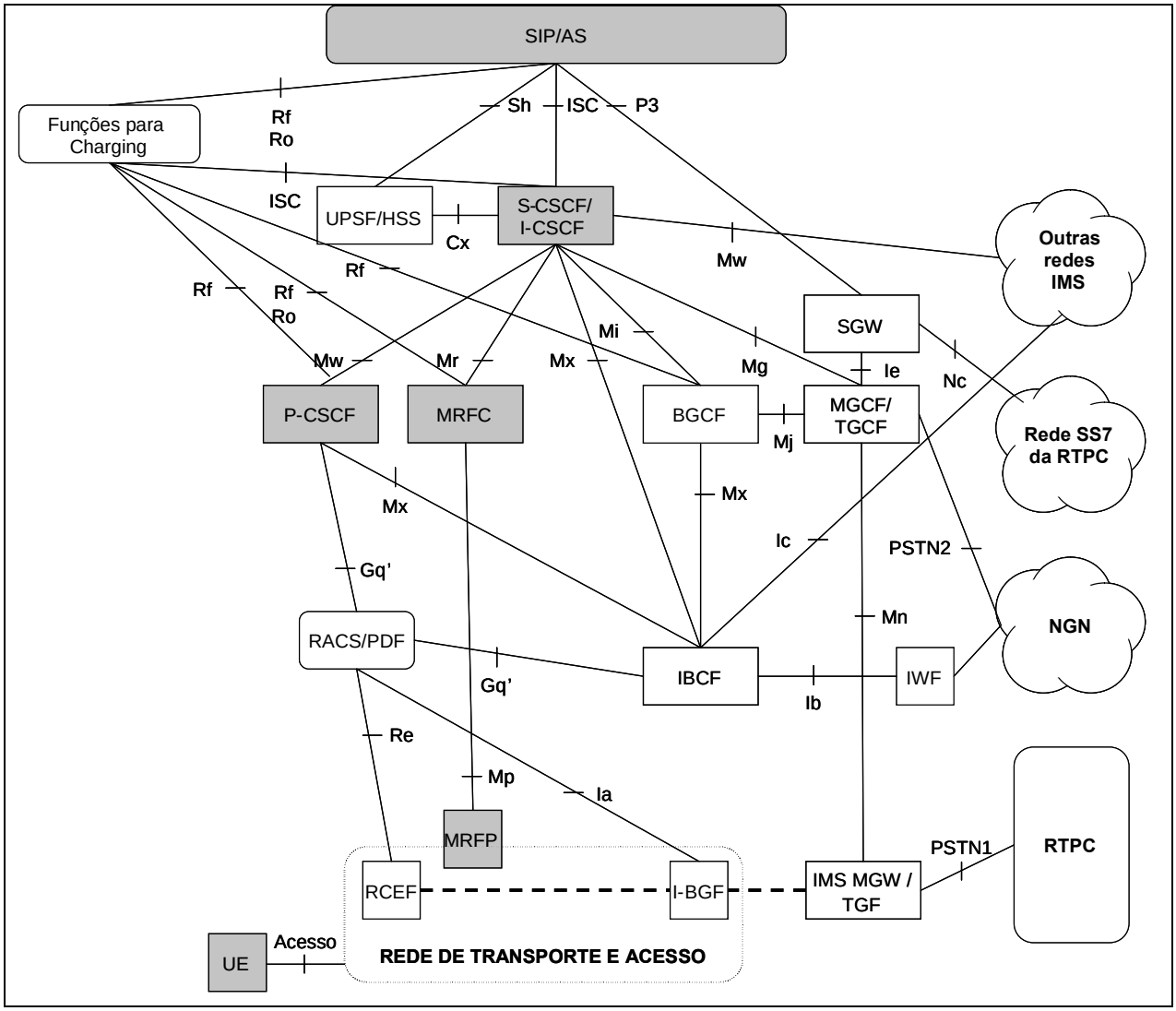


Figura 6.1 – Mapeamento das funções do *framework* nos elementos da arquitetura TISPAN adaptado de (Brasil Telecom, 2007).

As caixas mais escuras representam os elementos da arquitetura TISPAN que serão utilizados diretamente para prestação do serviço de videoconferência.

O equipamento de usuário (UE), mostrado na Figura 6.1, pode ser tanto um terminal móvel, quanto uma sala de videoconferência, ou ainda, qualquer outro dispositivo capaz de receber/gerar vídeo dentro dos padrões definidos pelo *framework* de conferência distribuída, desde que possa fazer uso das redes de acesso de faixa larga fixa ou móvel de uma operadora de telecomunicações.

De acordo com a alternativa de cenário sugerida (2A) no capítulo 5, solução mais adequada dentro das condições de contorno estabelecidas, as funções de *focus* seriam executadas em duas localidades, no caso Curitiba e Brasília. De acordo com o mapeamento proposto anteriormente, as funções de *focus* seriam desempenhadas pelo SIP AS, portanto para atender a alternativa 2A deveriam ser instalados 2 SIP AS, um em Brasília e outro em Curitiba.

Na alternativa 2A os misturadores estão divididos em distribuídos em cinco localidades, Brasília, Campo Grande, Curitiba, Florianópolis e Porto Alegre. Segundo o mapeamento sugerido, as funções de misturador são desempenhadas por dois equipamentos: o MRFC que executa as funções de controle de fluxos e o MRFP que faz o efetivo tratamento da mídia. Porém, nos equipamentos disponíveis atualmente no mercado o MRFP e o MRFC estão concentrados em um único equipamento, portanto deveriam ser colocados equipamentos MRFC/MRFP nas cinco localidades do cenário sugerido (2A).

A Figura 6.2 apresenta uma proposta de topologia lógica da rede, apresentando a hierarquia de controle entre os elementos de acordo com o mapeamento sugerido, e seguindo a distribuição geográfica na rede apresentada no cenário 2A.

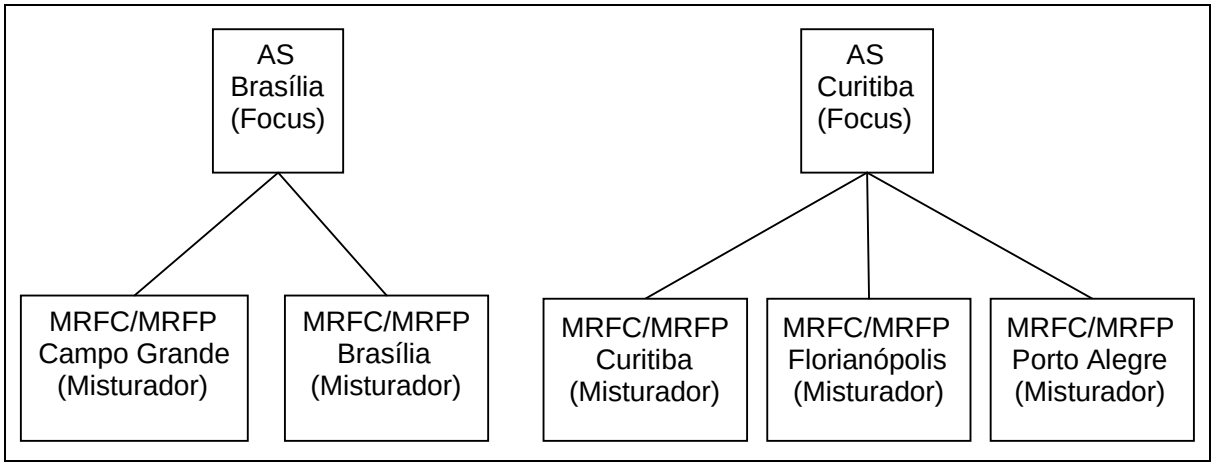


Figura 6.2 – Proposta de topologia de *focus* e misturadores para a Brasil Telecom.

Esta arquitetura proposta não é imutável, ela pode ser alterada tanto na topologia, com a inclusão/exclusão de localidades, seja para controle ou para tratamento da mídia, quanto entre os tipos de *framework*.

Com a evolução dos equipamentos ofertados pelos fabricantes, será possível separar as funções de MRFC e MRFP, o que permitirá que as funções de controle de fluxos possam ser concentradas em um número menor de pontos, enquanto as funções de tratamento de mídia possam ser espalhadas em um maior número de localidades. Esta separação de funções permitirá que os custos dos misturadores diminuam.

Misturadores com custo mais baixo irão permitir um aumento do número de localidades com estes equipamentos, diminuindo o custo de transporte da mídia do usuário até o elemento misturador.

O estudo financeiro realizado no capítulo 5 mostrou que para as condições estabelecidas, o *framework* de conferência distribuída apresenta um VPL maior que o framework de conferência centralizada. Porém, este mesmo estudo mostrou que a alternativa com maior VPL dependia diretamente do custo do misturador, portanto uma alteração neste custo pode alterar o resultado do estudo, mesmo com a manutenção de todas as demais condições de contorno.

7 - CONCLUSÃO

Os sistemas de videocomunicação possibilitam a comunicação entre grupos de pessoas independentemente de suas localizações geográficas, através de áudio e vídeo simultaneamente. Os novos sistemas de conferência permitem que se trabalhe de forma cooperativa e se compartilhe informações e materiais de trabalho sem a necessidade de locomoção geográfica.

A videoconferência não é uma idéia nova, nem original, está disponível desde os anos sessenta, na forma de sistemas de alto custo em salas de conferência especialmente equipadas, com objetivo de prover comunicação entre pessoas dispersas geograficamente e ocupadas o suficiente para não poderem realizar encontros pessoais freqüentemente.

A evolução das redes das empresas de telecomunicações para a arquitetura TISPAN irá potencializar o uso de videocomunicação, irá tornar a videoconferência um serviço popular através do uso de computadores pessoais, aparelhos celulares, permitindo maior flexibilidade nas formas de acesso e no preço do serviço.

Mas para tornar o ambiente descrito acima uma realidade, é necessário o uso de um *framework* de conferências padronizado, que possa aproveitar todos os avanços que a nova rede de telecomunicações permitirá.

Com o objetivo de mostrar um caminho para esta evolução, no capítulo 4 foram apresentados três diferentes *frameworks* que estão sendo padronizados no IETF e devem ser adotados pelas operadoras de telecomunicações como evolução para os atuais sistemas de videoconferência.

Uma operadora de telecomunicações irá implementar um destes *frameworks*, e a escolha de qual o mais adequado não é simples, depende de muitas variáveis e pode utilizar vários critérios de avaliação. Para exemplificar algumas destas variáveis e sugerir alguns critérios de avaliação, no capítulo 5 foi realizada uma comparação entre os dois *frameworks* mais abrangentes. Foram avaliados o *framework* de conferência centralizada e o de conferência distribuída.

A análise da escalabilidade mostrou como a distribuição de informação e/ou componentes pode ajudar melhorar o desempenho global de um sistema de conferência. Utilizando uma aproximação de engenharia, primeiramente foi avaliado o nível de desempenho de uma referência centralizada e então avaliada a melhoria de desempenho que pode ser alcançada ao distribuir a informação e o gerenciamento da funcionalidade. A

análise também ajudou a identificar potenciais limitadores de desempenho na implementação de um *framework* DCON.

Por sua vez, a análise financeira mostrou que o custo dos equipamentos para misturar as mídias, pode influenciar muito na avaliação de qual o cenário com o maior valor presente líquido (VPL). Foram traçadas curvas para cada um dos seis cenários estudados tendo em um eixo o VPL e no outro o número de clientes/equipamento de mistura de mídia, considerando que o custo por cliente diminui a medida que o número de clientes aumenta.

Foi mostrado na seção 5.2.2 que o cenário com maior VPL depende do ponto da curva que está sendo analisado. Como foi definida previamente a capacidade de tratamento de clientes simultâneos dos equipamentos com base nos dados fornecidos pelos fabricantes, para este valor a curva demonstrou que a alternativa com maior VPL era o cenário 2A baseado no *framework* de conferência distribuída.

Dentro dos limites do estudo, tendo com base estas duas análises a sugestão para a Brasil Telecom seria a implantação de um *framework* de conferência distribuída baseado no cenário 2A. Uma possibilidade de desenvolvimento desta alternativa foi apresentada no capítulo 6, sugerindo um mapeamento dos elementos do *framework* escolhido nos elementos da arquitetura TISPAN. Neste mesmo capítulo também foi mostrada a distribuição geográfica dos equipamentos de controle e de mistura de mídia que poderia ser implementada na Brasil Telecom de acordo com a topologia do cenário 2A.

O *framework* de conferência distribuída permite que o *focus* de uma operadora de telecomunicações controle uma conferência, na qual os fluxos de mídia dos clientes são tratados por misturadores que podem ser dela ou de outras operadoras. Isto só é possível porque como foi mostrado no capítulo 4 o framework DCON permite a comunicação entre *focus* através do protocolo XMPP. Atualmente todos os participantes de uma conferência têm que se conectar a uma mesma MCU, isto limita o uso do serviço a clientes de uma mesma operadora ou a conexões via RDSI a velocidades bem mais baixas. Para que isso possa acontecer serão necessários acordos técnicos e comerciais entre as operadoras.

Esta dissertação limitou o seu escopo a alguns aspectos do estudo de evolução de um serviço de videocomunicação. Foram abordados os aspectos referentes somente a serviços de videoconferência ponto-multiponto e não serviços de videocomunicação ponto-a-ponto. Foram mostrados os *frameworks*, as diferenças entre eles e seus pontos em comum e sua integração com o com a visão de evolução da rede da Brasil Telecom. Também foram analisados os aspectos de escalabilidade dos *frameworks* e a influência dos

custos de equipamentos e de transporte de fluxos, além da distribuição geográfica dos elementos.

Não foram tratados os aspectos referentes aos equipamentos de usuário e as modificações que necessárias nos mesmos para poder suportar toda a gama de novas funcionalidades que o *framework* irá permitir que sejam criadas. Não foram detalhados os novos protocolos como o BFCP e o CCP que fazem parte dos *frameworks*. Também não foram descritos em detalhes os novos serviços e seu funcionamento, assim como os servidores de aplicação que serão necessários para o seu correto funcionamento, nem a interação destes servidores com os elementos de controle, no que se refere a funções mais sofisticadas do que uma videoconferência convencional.

Outro ponto importante é que os documentos que descrevem os *frameworks* de conferência tanto a centralizada, quanto a distribuída, são drafts do IETF e ainda podem ser modificados até que se tornem RFCs. Existem vários pontos destes documentos que precisam ser melhorados e complementados por futuros trabalhos dos grupos de padronização. Entre estes trabalhos podem ser citados: melhorar a descrição do modelo de dados, criar um documento descrevendo o CCP, detalhar os itens de segurança, especificar o protocolo entre os misturadores e os controladores da conferência.

Mesmo com todos os pontos que ainda precisam ser definidos, as operadoras de telecomunicações, que já iniciaram a evolução de suas redes, precisam migrar os seus serviços de videocomunicação para a NGN. Esta dissertação mostrou que existe um caminho de evolução parcialmente definido e que caberá as operadoras definirem o momento mais conveniente para migrar os seus clientes para este novo ambiente. O principal fator que irá motivar esta migração é a capacidade da nova rede de permitir a um número muito maior de clientes o acesso aos serviços de videocomunicação, não somente através de videoconferência, mais também através da videofonia ponto a ponto.

Os estudos referentes aos *frameworks* de videoconferência estão em fase inicial, pois, como já mencionado ainda há muitos pontos em aberto na padronização. Assim sendo, existe muito trabalho a ser realizado. A lista a seguir apresenta algumas sugestões de trabalhos futuros que podem complementar este estudo e colaborar com o desenvolvimento dos esforços dos órgãos de padronização que estão tratando dos *frameworks* de conferência:

- Introduzir no estudo o tráfego de audioconferência, de mensagem instantânea, de troca de arquivos, de exibição de apresentações e de trabalho colaborativo;

- Descrever os protocolos CCP, BFCP, o uso do XMPP para a comunicação entre os *focus*;
- Introduzir no estudo a videocomunicação ponto-a-ponto, e verificar o impacto da mesma nos elementos de controle;
- Avaliar o funcionamento do *framework* de conferência distribuído quando a conferência tem clientes de duas ou mais operadoras e os *focus* das mesmas precisam se comunicar;
- Simular os cenários apresentados em uma ferramenta para verificar qual o impacto da distância no controle da conferência e na mistura da mídia no que se refere a parâmetros como atraso, *jitter*, entre outros;
- Comparar o desempenho do *framework* de conferência distribuída com o desempenho da conferência totalmente distribuída baseada em SIP, onde tanto o controle como a mistura de mídia são executados nos terminais de clientes;
- Descrever os protocolos e softwares envolvidos na comunicação com os terminais de cliente (UE), tratando não somente da troca de fluxos de vídeo, mas também das funcionalidades adicionais como trabalho colaborativo, compartilhamento de arquivos, mensagem instantânea, mecanismos de presença, entre outras;
- Complementar o estudo financeiro considerando a separação das funções de controle de fluxos de mídia e mistura de fluxos de mídia em dois equipamentos;
- Descrever como é criada e como funciona o gerenciamento da camada de *focus* sobreposta do *framework* de conferência distribuída.

REFERÊNCIAS BIBLIOGRÁFICAS

Baumgarten de Oliveira, Emerson. Sistematização de Procedimentos para Projeto e Implementação de Sistemas Voip em Redes Lan/Wan Utilizando a Recomendação ITU-T H.323. Dissertação apresentada ao Programa de Mestrado em Engenharia Elétrica, da Faculdade de Engenharia da Pontifícia Universidade Católica do Rio Grande do Sul em Agosto de 2002.

Brasil Telecom: Caderno de Diretrizes de Tecnologia e Arquitetura 2008 – 2010, 2007.

ETSI ES 282 001: Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Functional Architecture Release 1, 08/2005.

_____ ES 282 002: Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); PSTN/ISDN Emulation Subsystem (PES); Functional Architecture, 03/2006.

_____ ES 282 003: Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Resource and Admission Control Sub-system (RACS).

_____ ES 282 004: Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Network Attachment Sub-System (NASS).

_____ ES 282 007: Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); IP Multimedia Subsystem (IMS), 06/2006.

_____ TS 23.002: 3rd Generation Partnership Project (3GPP); Network Architecture.

_____ TS 23.008: 3rd Generation Partnership Project (3GPP); Organization of subscriber data.

_____ TS 23.228: 3rd Generation Partnership Project (3GPP); IP Multimedia Subsystem (IMS); Stage 2.

_____ TS 24.147: 3rd Generation Partnership Project (3GPP); Conferencing using the IP Multimedia *Core* Network subsystem.

_____ TS 183.005: Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); RTPC/ISDN simulation services: Conference (CONF); protocol specification.

Hersent, O.; Gurle, D.; Petit, J.-P.; IP telephony. Reading, Massachusetts: Addison Wesley, 2000.

IETF Draft: A Common Conference Information Data Model for Centralized Conferencing (XCON), 04/2007.

_____ Draft: A Framework for Application Interaction in the Session Initiation Protocol (SIP), 02/2005.

_____ Draft: A Framework for Centralized Conferencing, 08/2007.

_____ Draft: A Framework for Distributed Conferencing, 07/2007.

_____ Draft: Session initiation protocol service examples, 03/2006.

_____ RFC 768: User Datagram Protocol, 08/1980.

_____ RFC 793: Transmission Control Protocol, 09/1981.

_____ RFC 1738: Uniform resource locators (URL), 12/1994.

_____ RFC 2396: Uniform Resource Identifiers (URI), 08/1998.

_____ RFC 2916: E. 164 number and DNS, 09/2000.

_____ RFC 2960: Stream Control Transmission Protocol, 10/2000.

_____ RFC 3261: SIP: session initiation protocol, 06/2002.

_____ RFC 3265: Session Initiation Protocol (SIP)-Specific Event Notification, 06/2002.

_____ RFC 3508: H.323 uniform resource locator (URL) scheme registration, 04/2003.

_____ RFC 3550: RTP: a transport protocol for real-time applications, 07/2003.

_____ RFC 3725: Best Current Practices for Third Party Call Control (3pcc) in the Session Initiation Protocol (SIP), 04/2004.

_____ RFC 3840: Indicating User Agent Capabilities in the Session Initiation Protocol (SIP), 08/2004.

_____ RFC 3920: Extensible Messaging and Presence Protocol (XMPP): Core 10/2004.

_____ RFC 3966: The tel URI for telephone numbers, 12/2004.

_____ RFC 3986: Uniform Resource Identifier (URI): Generic Syntax, 01/2005.

_____ RFC 4123: Session Initiation Protocol (SIP)-H.323 Interworking Requirements, 07/2005.

_____ RFC 4245: High-Level Requirements for Tightly Coupled SIP Conferencing, 11/2005.

_____ RFC 4353: A *Framework* for Conferencing with the Session Initiation Protocol (SIP), 02/2006.

_____ RFC 4566: SDP: Session Description Protocol, 07/2006.

_____ RFC 4575: A Session Initiation Protocol (SIP) Event Package for Conference State, 08/2006.

_____ RFC 4579: Session Initiation Protocol (SIP) Call Control - Conferencing for User Agents 08/2006.

_____ RFC 4582: The Binary Floor Control Protocol (BFCP), 11/2006.

_____ RFC 4583: Session Description Protocol (SDP) Format for Binary Floor Control Protocol (BFCP) Streams, 11/2006.

_____ RFC 4975: The Message Session Relay Protocol (MSRP), 09/2007.

International Conference on Next Generation Teletraffic and Wired/Wireless Advanced Networking, 2007, St. Petersburg, Russia. A. Buono, S. Loreto, L. Miniero, and S. P. Romano. Design and implementation of an open source IMS enabled conferencing architecture. 09/2007.

IPTComm 2007 Telecommunications in the Internet Age, New York. A. Buono, S. Loreto, L. Miniero, and S. P. Romano. Improving the scalability of an IMS-compliant conferencing framework through presence and event notification. p. 19-28, 07/2007.

ISO/IEC JTC 1 Recommendation MPEG1: Coding of moving pictures and associated audio for digital storage media at up to about 1.5 Mbit/s – Part 2: Video, 11/1993.

_____ Recommendation MPEG 2: Generic coding of moving pictures and associated audio information – Part 2: Video, 11/1994.

_____ Recommendation MPEG 4: Advanced Video Coding for Generic Audiovisual Services, 05/2003.

ITU-T Recommendation G.711: Pulse Code Modulation (PCM) of Voice Frequencies, 1998.

_____ Recommendation G.722: 7 kHz Audio-coding within 64 kbit/s, 1998.

_____ Recommendation G.723.1: Dual Rate Speech codec for multimedia telecommunications transmitting at 6.4 and 5.3 kbit/s, 1995.

_____ Recommendation G.728: Speech Coding at 16 kbit/s, 1992.

_____ Recommendation G.729: Speech codec for multimedia telecommunications transmitting at 8/13 kbit/s, 1995.

_____ Recommendation H.225.0: Media stream packetization and synchronization on non-guaranteed quality of service LANs, 11/1996.

_____ Recommendation H.235: Security and encryption for H-series (H.323 and other H.245-based) multimedia terminals, 02/1998.

_____ Recommendation H.245: Control protocol for multimedia communication, 02/1998.

_____ Recommendation H.246: Interworking of H-series multimedia terminals with H-series multimedia terminals and voice/voiceband terminals on GSTN and ISDN, 02/1998.

_____ Recommendation H.261 v1: Video codec for audiovisual services at px64 kbits/s, 03/1993.

_____ Recommendation H.262: Generic coding of moving pictures and associated audio information – Part 2: Video, 11/1994.

_____ Recommendation H.263 v3: Video coding for low bit rate communication, 11/2000.

_____ Recommendation H.264: Advanced Video Coding for Generic Audiovisual Services, 05/2003.

_____ Recommendation H.320: Narrow-band visual telephone systems and terminal equipment, 05/1999.

_____ Recommendation H.323: Packet based multimedia communication systems, 06/2006.

_____ Recommendation H.332: H.323 extended for loosely coupled conferences, 09/1998.

_____ Recommendation H.450.1: Generic functional protocol for the support of supplementary services in H.323, 02/ 1998.

_____ Recommendation H.450.3: Call diversion supplementary service for H.323, 09/1997.

_____ Recommendation Q.931: ISDN user-network interface layer 3 specification for basic call control.

Kundan Narendra Singh, "Reliable, Scalable and Interoperable Internet Telephony", Doctors's Thesis Columbia University, 2006.

Monteiro, Regina C. Contribuições da Abordagem de Avaliação de Opções Reais em Ambientes Econômicos de Grande Volatilidade – Uma Ênfase no Cenário Latino-Americano. São Paulo: Dissertação de Mestrado submetida à FEAC/USP, 2003.

Wang, Ligang. Modelling And Verification Of Interworking Between SIP And H.323 Thesis in The Department of Computer Science, 04/ 2002.

World Wide *Web* Consortium Recommendation SOAP v 1.2 part 0: Primer (Second Edition), 04/2007.

Zentgraf, Roberto. Matemática Financeira Objetiva. 3. ed. Editoração Ed. E ZTG Ed, 2002.

APÊNDICE

A.1 – Matriz de interesse de tráfego

De/Para	Brasília	Campo Grande	MS	Cuiabá	MT	Curitiba	PR	Florianópolis	SC	Goiânia	GO	Palmas	TO	Porto Alegre	RS	Porto Velho	RO	Rio Branco	AC
Brasília	25%	8%	5%	10%	8%	10%	7%	10%	10%	10%	10%	10%	10%	9%	6%	10%	10%	10%	10%
Campo Grande	3%	20%	20%	2%	3%	1%	2%	2%	3%	3%	3%	2%	2%	3%	2%	5%	5%	3%	4%
MS	2%	12%	15%	2%	2%	2%	2%	2%	2%	2%	3%	2%	2%	2%	2%	2%	2%	2%	3%
Cuiabá	3%	2%	3%	20%	15%	1%	1%	1%	1%	1%	2%	2%	2%	1%	2%	5%	5%	3%	4%
MT	2%	2%	3%	10%	15%	2%	3%	2%	3%	2%	2%	2%	3%	2%	2%	2%	2%	2%	3%
Curitiba	6%	7%	8%	7%	8%	21%	18%	8%	9%	8%	7%	7%	7%	7%	6%	4%	3%	4%	5%
PR	4%	5%	6%	8%	5%	10%	15%	9%	6%	5%	5%	5%	4%	4%	5%	0%	0%	0%	0%
Florianópolis	3%	4%	4%	4%	4%	3%	4%	15%	15%	4%	4%	4%	4%	3%	4%	2%	0%	2%	0%
SC	5%	5%	5%	3%	7%	4%	6%	10%	15%	5%	3%	3%	0%	3%	8%	0%	0%	0%	0%
Goiânia	4%	4%	4%	4%	4%	3%	4%	4%	4%	20%	20%	10%	8%	4%	4%	5%	4%	5%	4%
GO	4%	3%	4%	3%	3%	3%	3%	3%	3%	10%	15%	3%	4%	2%	4%	3%	3%	3%	3%
Palmas	2%	1%	1%	1%	0%	0%	0%	2%	0%	3%	2%	20%	25%	1%	1%	0%	0%	2%	0%
TO	0%	1%	0%	1%	1%	1%	1%	0%	0%	0%	0%	10%	10%	0%	0%	0%	0%	0%	0%
Porto Alegre	5%	8%	7%	7%	6%	9%	8%	7%	9%	7%	6%	7%	6%	20%	20%	5%	3%	4%	2%
RS	3%	2%	2%	3%	3%	3%	4%	3%	5%	3%	2%	3%	3%	10%	10%	0%	0%	0%	0%
Porto Velho	2%	1%	2%	1%	1%	1%	1%	2%	0%	2%	0%	0%	0%	2%	2%	20%	30%	5%	4%
RO	0%	0%	0%	0%	0%	1%	0%	0%	0%	0%	0%	0%	0%	0%	0%	18%	13%	5%	2%
Rio Branco	2%	1%	1%	1%	0%	0%	1%	0%	0%	0%	0%	0%	0%	2%	2%	3%	3%	25%	30%
AC	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	1%	1%	15%	15%
Fora da Região 2	25%	15%	10%	15%	15%	25%	20%	20%	15%	15%	15%	10%	10%	25%	20%	15%	15%	10%	10%
Total	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%

A.2 – Matriz de distâncias.

De/Para	Brasília	Campo Grande	MS	Cuiabá	MT	Curitiba	PR	Florianópolis	SC	Goiânia	GO	Palmas	TO	Porto Alegre	RS	Porto Velho	RO	Rio Branco	AC
Brasília	D0	D7	D7	D7	D7	D8	D8	D8	D8	D3	D3	D6	D6	D8	D8	D8	D8	D8	D8
Campo Grande	D7	D0	D2	D6	D6	D7	D7	D8	D8	D7	D7	D8	D8	D8	D8	D8	D8	D8	D8
MS	D7	D2	D0	D6	D6	D7	D7	D8	D8	D7	D7	D8	D8	D8	D8	D8	D8	D8	D8
Cuiabá	D7	D6	D6	D0	D2	D8	D8	D8	D8	D7	D7	D8	D8	D8	D8	D8	D8	D8	D8
MT	D7	D6	D6	D2	D0	D8	D8	D8	D8	D7	D7	D8	D8	D8	D8	D8	D8	D8	D8
Curitiba	D8	D7	D7	D8	D8	D0	D2	D4	D4	D7	D7	D8	D8	D6	D6	D8	D8	D8	D8
PR	D8	D7	D7	D8	D8	D2	D0	D4	D4	D7	D7	D8	D8	D6	D6	D8	D8	D8	D8
Florianópolis	D8	D8	D8	D8	D8	D4	D4	D0	D2	D8	D8	D8	D8	D5	D5	D8	D8	D8	D8
SC	D8	D8	D8	D8	D8	D4	D4	D2	D0	D8	D8	D8	D8	D5	D5	D8	D8	D8	D8
Goiânia	D3	D7	D7	D7	D7	D7	D7	D8	D8	D0	D2	D7	D7	D8	D8	D8	D8	D8	D8
GO	D3	D7	D7	D7	D7	D7	D7	D8	D8	D2	D0	D7	D7	D8	D8	D8	D8	D8	D8
Palmas	D6	D8	D8	D8	D8	D8	D8	D8	D8	D7	D7	D0	D2	D8	D8	D8	D8	D8	D8
TO	D6	D8	D8	D8	D8	D8	D8	D8	D8	D7	D7	D2	D0	D8	D8	D8	D8	D8	D8
Porto Alegre	D8	D8	D8	D8	D8	D6	D6	D5	D5	D8	D8	D8	D8	D0	D2	D8	D8	D8	D8
RS	D8	D8	D8	D8	D8	D6	D6	D5	D5	D8	D8	D8	D8	D2	D0	D8	D8	D8	D8
Porto Velho	D8	D8	D8	D8	D8	D8	D8	D8	D8	D8	D8	D8	D8	D8	D8	D0	D2	D5	D5
RO	D8	D8	D8	D8	D8	D8	D8	D8	D8	D8	D8	D8	D8	D8	D8	D2	D0	D5	D5
Rio Branco	D8	D8	D8	D8	D8	D8	D8	D8	D8	D8	D8	D8	D8	D8	D8	D5	D5	D0	D2
AC	D8	D8	D8	D8	D8	D8	D8	D8	D8	D8	D8	D8	D8	D8	D8	D5	D5	D2	D0
Fora da Região 2	D7	D7	D7	D8	D8	D5	D5	D5	D5	D7	D7	D8	D8	D7	D7	D8	D8	D8	D8
Total																			

A.3 – Matriz de banda necessária para o cenário 2A em Mbps.

De/Para	Brasília	Campo Grande	MS	Cuiabá	MT	Curitiba	PR	Florianópolis	SC	Goiânia	GO	Palmas	TO	Porto Alegre	RS	Porto Velho	RO	Rio Branco
Brasília	18,0	1,4	1,0	1,2	2,0	8,0	6,8	3,9	7,3	4,2	3,4	0,3	0,8	10,2	5,0	0,7	1,1	0,5
Campo Grande	2,2	3,5	3,8	0,2	0,7	1,2	1,7	0,6	2,2	1,3	1,0	0,1	0,2	3,4	1,7	0,4	0,5	0,1
MS	1,4	2,1	2,9	0,2	0,5	1,3	1,9	0,7	1,5	0,8	1,0	0,1	0,2	1,9	1,7	0,1	0,2	0,1
Cuiabá	2,2	0,3	0,6	2,4	3,7	0,8	1,2	0,4	0,9	0,5	0,7	0,1	0,2	1,2	1,7	0,4	0,5	0,1
MT	1,3	0,4	0,6	1,2	3,7	1,6	2,4	0,9	1,9	1,0	0,8	0,1	0,2	2,5	1,7	0,2	0,3	0,1
Curitiba	4,3	1,3	1,6	0,9	1,9	16,9	17,6	2,9	6,2	3,2	2,4	0,2	0,6	8,1	5,0	0,3	0,3	0,2
PR	2,9	0,9	1,1	1,0	1,2	8,0	14,6	3,6	4,4	2,1	1,7	0,2	0,3	4,5	4,2	0,0	0,0	0,0
Florianópolis	2,1	0,6	0,8	0,4	0,9	2,6	3,9	5,9	11,0	1,5	1,3	0,1	0,3	3,9	3,3	0,1	0,0	0,1
SC	3,9	0,9	1,0	0,4	1,8	3,2	5,9	3,9	11,0	2,1	1,0	0,1	0,0	3,4	6,7	0,0	0,0	0,0
Goiânia	2,9	0,7	0,8	0,5	1,0	2,8	4,2	1,5	3,2	8,4	6,7	0,3	0,6	4,2	3,3	0,4	0,4	0,2
GO	2,9	0,5	0,7	0,4	0,8	2,2	3,4	1,2	2,2	4,2	5,1	0,1	0,3	2,3	3,3	0,2	0,4	0,1
Palmas	1,4	0,2	0,2	0,1	0,1	0,0	0,3	0,8	0,0	1,3	0,7	0,7	2,0	1,1	0,8	0,0	0,0	0,1
TO	0,0	0,1	0,0	0,1	0,2	0,5	0,8	0,0	0,0	0,0	0,0	0,3	0,8	0,0	0,0	0,0	0,0	0,0
Porto Alegre	3,6	1,4	1,3	0,9	1,5	7,6	7,8	2,7	6,6	2,9	2,0	0,2	0,5	22,7	16,6	0,4	0,3	0,2
RS	2,2	0,3	0,4	0,4	0,7	2,4	3,9	1,2	3,7	1,3	0,7	0,1	0,2	11,3	8,3	0,0	0,0	0,0
Porto Velho	1,4	0,1	0,4	0,1	0,2	0,5	0,7	0,8	0,0	0,8	0,0	0,0	0,0	2,3	1,7	1,5	3,2	0,2
RO	0,0	0,0	0,0	0,0	0,0	0,7	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	1,3	1,4	0,2
Rio Branco	1,4	0,2	0,2	0,1	0,0	0,0	1,0	0,0	0,0	0,2	0,2	0,0	0,0	2,3	1,7	0,2	0,3	1,2
AC	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,1	0,1	0,7
Fora da Região 2	18,0	2,6	1,9	1,8	3,7	20,1	19,5	7,8	11,0	6,3	5,1	0,3	0,8	28,4	16,6	1,1	1,6	0,5
Total	71,9	17,5	19,2	12,2	24,5	80,5	97,7	38,9	73,0	41,9	33,7	3,3	8,0	113,8	83,1	7,3	10,7	4,9

A.4 – Matriz de distâncias para o cenário 2A.

De/Para	Brasília	Campo Grande	MS	Cuiabá	MT	Curitiba	PR	Florianópolis	SC	Goiânia	GO	Palmas	TO	Porto Alegre	RS	Porto Velho	RO	Rio Branco
Brasília	D0	D0	D2	D6	D6	D0	D2	D0	D2	D3	D3	D6	D6	D0	D2	D8	D8	D8
Campo Grande	D0	D0	D2	D6	D6	D0	D2	D0	D2	D3	D3	D6	D6	D0	D2	D8	D8	D8
MS	D0	D0	D2	D6	D6	D0	D2	D0	D2	D3	D3	D6	D6	D0	D2	D8	D8	D8
Cuiabá	D0	D0	D2	D6	D6	D0	D2	D0	D2	D3	D3	D6	D6	D0	D2	D8	D8	D8
MT	D0	D0	D2	D6	D6	D0	D2	D0	D2	D3	D3	D6	D6	D0	D2	D8	D8	D8
Curitiba	D0	D0	D2	D6	D6	D0	D2	D0	D2	D3	D3	D6	D6	D0	D2	D8	D8	D8
PR	D0	D0	D2	D6	D6	D0	D2	D0	D2	D3	D3	D6	D6	D0	D2	D8	D8	D8
Florianópolis	D0	D0	D2	D6	D6	D0	D2	D0	D2	D3	D3	D6	D6	D0	D2	D8	D8	D8
SC	D0	D0	D2	D6	D6	D0	D2	D0	D2	D3	D3	D6	D6	D0	D2	D8	D8	D8
Goiânia	D0	D0	D2	D6	D6	D0	D2	D0	D2	D3	D3	D6	D6	D0	D2	D8	D8	D8
GO	D0	D0	D2	D6	D6	D0	D2	D0	D2	D3	D3	D6	D6	D0	D2	D8	D8	D8
Palmas	D0	D0	D2	D6	D6	D0	D2	D0	D2	D3	D3	D6	D6	D0	D2	D8	D8	D8
TO	D0	D0	D2	D6	D6	D0	D2	D0	D2	D3	D3	D6	D6	D0	D2	D8	D8	D8
Porto Alegre	D0	D0	D2	D6	D6	D0	D2	D0	D2	D3	D3	D6	D6	D0	D2	D8	D8	D8
RS	D0	D0	D2	D6	D6	D0	D2	D0	D2	D3	D3	D6	D6	D0	D2	D8	D8	D8
Porto Velho	D0	D0	D2	D6	D6	D0	D2	D0	D2	D3	D3	D6	D6	D0	D2	D8	D8	D8
RO	D0	D0	D2	D6	D6	D0	D2	D0	D2	D3	D3	D6	D6	D0	D2	D8	D8	D8
Rio Branco	D0	D0	D2	D6	D6	D0	D2	D0	D2	D3	D3	D6	D6	D0	D2	D8	D8	D8
AC	D0	D0	D2	D6	D6	D0	D2	D0	D2	D3	D3	D6	D6	D0	D2	D8	D8	D8
Fora da Região 2	D0	D0	D2	D6	D6	D0	D2	D0	D2	D3	D3	D6	D6	D0	D7	D8	D8	D8
Total																		

A.5 – Matriz de Capex de transmissão para o cenário 2A em R$.

De/Para	Brasília	Campo Grande	MS	Cuiabá	MT	Curitiba	PR	Florianópolis	SC	Goiânia	GO	Palmas	TO	Porto Alegre	RS	Porto Velho	RO	Rio Branco
Brasília	4735	526	735	3240	3240	2631	2940	1052	2940	3457	2305	3240	3240	3157	2205	4702	4702	4702
Campo Grande	1052	1052	1470	3240	3240	526	735	526	1470	1152	1152	3240	3240	1052	735	4702	4702	4702
MS	526	1052	1470	3240	3240	526	735	526	735	1152	1152	3240	3240	526	735	4702	4702	4702
Cuiabá	1052	526	735	6480	6480	526	735	526	735	1152	1152	3240	3240	526	735	4702	4702	4702
MT	526	526	735	3240	6480	526	1470	526	735	1152	1152	3240	3240	1052	735	4702	4702	4702
Curitiba	1578	526	735	3240	3240	4735	6614	1052	2940	2305	2305	3240	3240	2631	2205	4702	4702	4702
PR	1052	526	735	3240	3240	2631	5879	1052	2205	2305	1152	3240	3240	1578	2205	0	0	0
Florianópolis	1052	526	735	3240	3240	1052	1470	1578	4410	1152	1152	3240	3240	1052	1470	4702	0	4702
SC	1052	526	735	3240	3240	1052	2205	1052	4410	2305	1152	3240	0	1052	2940	0	0	0
Goiânia	1052	526	735	3240	3240	1052	2205	526	1470	5762	4610	3240	3240	1578	1470	4702	4702	4702
GO	1052	526	735	3240	3240	1052	1470	526	1470	3457	3457	3240	3240	1052	1470	4702	4702	4702
Palmas	526	526	735	3240	3240	0	735	526	0	1152	1152	3240	6480	526	735	0	0	4702
TO	0	526	0	3240	3240	526	735	0	0	0	0	3240	3240	0	0	0	0	0
Porto Alegre	1052	526	735	3240	3240	2105	2940	1052	2940	2305	2305	3240	3240	6314	6614	4702	4702	4702
RS	1052	526	735	3240	3240	1052	1470	526	1470	1152	1152	3240	3240	3157	3675	0	0	0
Porto Velho	526	526	735	3240	3240	526	735	526	0	1152	0	0	0	1052	735	4702	9403	4702
RO	0	0	0	0	0	526	0	0	0	0	0	0	0	0	0	4702	4702	4702
Rio Branco	526	526	735	3240	0	0	735	0	0	1152	1152	0	0	1052	735	4702	4702	4702
AC	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	4702	4702	4702
Fora da Região 2	4735	1052	735	3240	6480	5788	7349	2105	4410	4610	3457	3240	3240	7892	40436	4702	4702	4702
Total	23151	11049	13964	61564	64804	26834	41156	13680	32337	36879	29964	51843	51843	35253	69833	70524	70524	75226

A.6 – Matriz de Opex de transmissão para o cenário 2A em R$.

De/Para	Brasília	Campo Grande	MS	Cuiabá	MT	Curitiba	PR	Florianópolis	SC	Goiânia	GO	Palmas	TO	Porto Alegre	RS	Porto Velho	RO	Rio Branco
Brasília	3972	441	823	1173	1173	2207	3291	883	3291	3129	2086	1173	1173	2648	2468	1176	1176	1176
Campo Grande	883	883	1645	1173	1173	441	823	441	1645	1043	1043	1173	1173	883	823	1176	1176	1176
MS	441	883	1645	1173	1173	441	823	441	823	1043	1043	1173	1173	441	823	1176	1176	1176
Cuiabá	883	441	823	2347	2347	441	823	441	823	1043	1043	1173	1173	441	823	1176	1176	1176
MT	441	441	823	1173	2347	441	1645	441	823	1043	1043	1173	1173	883	823	1176	1176	1176
Curitiba	1324	441	823	1173	1173	3972	7404	883	3291	2086	2086	1173	1173	2207	2468	1176	1176	1176
PR	883	441	823	1173	1173	2207	6581	883	2468	2086	1043	1173	1173	1324	2468	0	0	0
Florianópolis	883	441	823	1173	1173	883	1645	1324	4936	1043	1043	1173	1173	883	1645	1176	0	1176
SC	883	441	823	1173	1173	883	2468	883	4936	2086	1043	1173	0	883	3291	0	0	0
Goiânia	883	441	823	1173	1173	883	2468	441	1645	5214	4172	1173	1173	1324	1645	1176	1176	1176
GO	883	441	823	1173	1173	883	1645	441	1645	3129	3129	1173	1173	883	1645	1176	1176	1176
Palmas	441	441	823	1173	1173	0	823	441	0	1043	1043	1173	2347	441	823	0	0	1176
TO	0	441	0	1173	1173	441	823	0	0	0	0	1173	1173	0	0	0	0	0
Porto Alegre	883	441	823	1173	1173	1765	3291	883	3291	2086	2086	1173	1173	5296	7404	1176	1176	1176
RS	883	441	823	1173	1173	883	1645	441	1645	1043	1043	1173	1173	2648	4113	0	0	0
Porto Velho	441	441	823	1173	1173	441	823	441	0	1043	0	0	0	883	823	1176	2352	1176
RO	0	0	0	0	0	441	0	0	0	0	0	0	0	0	0	1176	1176	1176
Rio Branco	441	441	823	1173	0	0	823	0	0	1043	1043	0	0	883	823	1176	1176	1176
AC	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1176	1176	1176
Fora da Região 2	3972	883	823	1173	2347	4854	8226	1765	4936	4172	3129	1173	1173	6620	10576	1176	1176	1176
Total	19418	9267	15630	22296	23469	22507	46067	11474	36196	33372	27115	18775	18775	29568	43481	17637	17637	18812