Rodrigo Santana

Uma Arquitetura Experimental de Serviços Integrados para prover QoS em Aplicações de Vídeo Conferência

Florianópolis - SC

2004

UNIVERSIDADE FEDERAL DE SANTA CATARINA
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

Rodrigo Santana

Uma Arquitetura Experimental de Serviços Integrados para prover QoS em Aplicações de Vídeo Conferência

Dissertação submetida à Universidade Federal de Santa Catarina como parte dos requisitos para obtenção do grau de mestre em ciência da computação.

Prof. Dr. Carlos Becker Westphall
Orientador

Florianópolis, Dezembro de 2004.

Uma Arquitetura Experimental de Serviços Integrados, para prover QoS em Aplicações de Vídeo Conferência

Rodrigo Santana

Esta dissertação foi julgada adequada para a obtenção do Título de mestre em Ciência da Computação, Área de concentração Sistemas de Computação e aprovada na sua forma final pelo programa de Pós-Graduação em Ciência da Computação.

_____

Prof. Dr. Raul S. Wazlawick

Coordenador do Curso de Pós-Graduação em Ciência da Computação

_____

Prof. Dr. Carlos Becker Westphall

Orientador

Banca Examinadora:

_____	_____
Prof. Dr. Carlos Becker Westphal Presidente	Prof. Dr. Rômulo Silva de Oliveira
_____	_____
Prof. Dr. Mário Antonio Ribeiro Dantas	Prof Dr. Alexandre Moraes Ramos

Dedicatória

Para minha esposa, Raquel;

Minha filha Maria Fernanda;

Meu pai, Vitório;

Minha mãe, Lani;

Meus irmãos e

Meus amigos.

Agradecimentos

Primeiramente agradeço a Deus, o Grande Arquiteto do Universo que me deu forças e luz para a realização deste trabalho;

Ao professor Dr. Carlos Becker Westphall, pelo incentivo, apoio e orientação;

Ao professor Dr. Roberto Willrich, pelas correções e orientações nos experimentos;

Aos demais membros da banca;

A todos os amigos da Unisul, de ontem, de hoje e de sempre, em especial ao Daniel Cadorin e Dickson Guedes que me ajudaram muito;

A todos os amigos do NPD da UFSC e do projeto IQoM, em especial ao Fernando Cerutti;

E um agradecimento especial, ao amigo, e mestre Edson Melo pelo apoio, incentivo e companheirismo, que me foram muito importantes para realização deste trabalho.

Resumo

Este trabalho apresenta uma arquitetura experimental de serviços integrados para prover QoS em aplicações de vídeo conferência.

Para validar sua funcionalidade foram executados estudos teóricos sobre qualidade de serviço em redes IP, principalmente o modelo de serviços integrados e toda a problemática envolvida em medições de QoS. Foram também executados diversos experimentos com o objetivo de avaliar a eficácia do modelo de serviços integrados para prover QoS em aplicações de vídeo conferência. Os experimentos avaliaram o comportamento do tráfego de vídeo conferência em redes com e sem congestionamento e com e sem qualidade de serviço.

Em todos os experimentos, foram realizadas medições associadas ao atraso, à variação do atraso e a perda de pacotes.

Os resultados obtidos comprovam a eficácia dos mecanismos de priorização de tráfego do modelo de serviços integrados, deixando bem claro que aplicações como as de vídeo conferência, precisam de mecanismos de priorização de tráfego para que possam funcionar perfeitamente.

Abstract

This work presents an experimental framework of the integrated service framework to provide QoS in video conference applications.

For validating its functionality, theoretical studies were made about quality of service on IP networks, especially the integrated service model and the whole set of problems involved in QoS measurements. Several experiments were carried out with the purpose of evaluating the effectiveness of the integrated service model to provide QoS in video conference applications. The experiments evaluated the behavior of the video conference traffic on networks with and without congestioning, and with and without quality of service.

In the experiments, measurements were made, associated with delay, jitter and lost packet.

The results achieved prove the effectiveness of the traffic priorization mechanisms of the integrated service model, making it very clear that applications such as video conference need traffic priorization mechanisms in order to be able to work perfectly.

ÍNDICE

Lista de Figuras

Lista de Tabelas

Lista de Abreviaturas

ATM	Asynchronous Transfer Mode
BE	Best Effort
CAR	Committed Access Rate
CIR	Commited Information Rate
CQ	Custom Queuing
DiffServ	Differentiated Services
DS	Differentiated Service
DSCP	Differentiated Services
EF	Expedited Forwarding
FF	Fixed Filter
FIFO	First In First Out
FTP	File Transfer Protocol
IETF	Internet Engineering Task Force
IntServ	Integrated Services
IP	Internet Protocol
IPPM	Ip Performance Metric
LAN	Local Área Network
MPLS	Multiprotocol Label Switching
NTP	Network Time Protocol
PHB	Per Hop Behaviour
Phop	Previous Hop
PPP	Point to Point Protocol
PQ	Priority Queuing
PQ	Priority Queuing
QOS	Quality of Service
RED	Random Early Detection
RESV	Reservation
RSVP	Resource Reservation Setup Protocol
RTCP	Sender Reports Receiver Reports
RTT	Round Trip Time

SE	Shared Explicit
SLA	Service Level Agreement
SNMP	Simple Network Manage Protocol
TCP	Transmission Control Protocol
TOS	Type of Service
UDP	User Datagram Protocol
VBR	Variable Bit Rate
VoIP	Voice over IP
WAN	Wide Área Network
WF	Wild Card Filter
WFQ	Weighted Fair Queuing
WFQ	Weighted Fair Queuing
WRED	Weighted Random Early Detection

1. INTRODUÇÃO

A comunicação de dados através das redes IP, esta se tornando cada vez mais comum nas empresas e instituições, e ganhando novas funcionalidades, como comunicação multimídia, além da pura e simples transmissão de dados. A comunicação multimídia é um serviço de telecomunicações de interesse coletivo com legislação específica, possibilitando a oferta de transmissão, emissão e recepção de informações multimídia, utilizando qualquer meio de transmissão, incluindo redes de dados de baixa velocidade [ANA 2004].

Aplicações multimídia como vídeo conferência e voz sobre IP, têm exigências rígidas quanto ao atraso [MEL 2001], necessitando serem tratadas de forma diferenciada. As redes IP oferecem serviços de melhor esforço "*best-effort*", onde os pacotes competem igualmente pelos recursos da rede, tornando-se muito difícil garantir que os pacotes chegarão ao destino, não se conseguindo um gerenciamento dos parâmetros de atraso, variação do atraso e perda de pacotes [ABE 2001]. Para tratar este tipo de tráfego de forma diferenciada é necessário torná-lo prioritário em uma transmissão, para isso é necessário deixar de lado a forma tradicional de transmissão por melhor esforço e aplicar técnicas de qualidade de serviço (QoS), que tornam possível a transmissão deste tráfego de forma prioritária. Segundo [MEL 2001], a necessidade de se aplicar qualidade de serviço é evidente, principalmente quando possuímos restrições da capacidade de largura de banda das redes WAN *(Wide Area Network)*.

O gerenciamento de QoS é considerado tão importante quanto a sua implementação. Não basta implementar uma política de QoS sem ter uma análise através de medições de sua eficácia na rede. Existem muitas formas de se implementar QoS em redes IP, as mais conhecidas são a arquitetura de serviços diferenciados e a arquitetura de serviços integrados. Hoje muitos estudos são feitos sobre a arquitetura de serviços integrados como exemplo [FON 99], [KUO 2003], [SCH 2000] e [BRA 99], mas a arquitetura é pouco usada por ser bastante complexa e requerer muitos recursos dos roteadores. Quando comparamos as redes IP com a ATM o grande ponto fraco do IP é o QoS, este fato serve como motivação para o estudo de QoS em redes IP. A razão para estudar especificamente o modelo de serviços integrados, é o fato do modelo permitir que a

aplicação defina os seus requisitos de QoS à rede, permitir serviços garantidos e de carga controlada, além de ser um modelo orientado ao fluxo.

Neste trabalho foi estudado e analisado através de experimentação prática, a implementação real, através de roteadores Cisco, da arquitetura de serviços integrados (IntServ) para prover QoS, em aplicações de vídeo conferência. Foi implementado um ambiente de testes para os experimentos onde se adquiriu conhecimento e experiência prática na configuração desta arquitetura. O ambiente serviu principalmente para avaliação das métricas de QoS, tais como atraso, variação do atraso, perda de pacotes e realizar os experimentos de vídeo conferência.

1.1 Trabalhos correlatos e o estado da arte

Inúmeras pesquisas comprovam a eficácia da utilização de métodos de QoS para contribuir no desempenho de aplicações de rede. Neste capítulo são apresentados alguns trabalhos correlatos e é feita uma relação com o estado da arte em QoS.

Em [LEE 2004] o autor fala que a gerência de mobilidade e de qualidade serviço serão importantes para o desenvolvimento das redes sem fio. O autor propõe uma arquitetura que suporte ambos, qualidade de serviço e gerência de mobilidade. Para o provimento de QoS é habilitado o QoS fim-a-fim que é garantido pelo uso do protocolo de reserva de recursos (RSVP). Também é utilizada uma técnica de reserva de recursos passiva para reduzir a influência de uma estação móvel para o atraso da reserva de recursos. Uma análise de performance foi feita para justificar a arquitetura proposta.

Em [LEO 2004] o autor propõe um policiamento para controle de admissão de chamadas (CAC) para sistemas de celular suportando voz e serviços de dados e provendo uma alta prioridade para as chamadas. É proposto um modelo 3D para provimento de QoS em sistema de redes móvel.

Em [GHE 2004] o autor fala sobre gerencia de serviços, critérios e métricas associados a classe de serviços, acordos de nível de serviço e qualidade de serviços em redes IP. Faz uma avaliação da nova geração de sistemas/plataformas de gerencia de serviços e QoS.

Em [PAS 2004] O autor mostra os resultados de prover QoS em redes heterogêneas e o futuro da internet com redes sem fio utilizando a estrutura de redes MPLS e modelo

de serviços integrados. O autor também destaca a importância do roteamento, segurança e o resultado do gerenciamento de tráfego fim-a-fim.

Em [BER 2003] é relatado a problemática das transmissões de vídeo e da clara necessidade de uso de qualidade de serviço. Ele fala sobre especificação de base de dados de vídeo. Define uma infra-estrutura informal para a orientação de usuários, a especificação e aplicabilidade de QoS. Também aponta a unificação de idéias para precedente trabalho, provendo maior fundamentação formal e expressando muitos aspectos de QoS de uma maneira fácil e conveniente para o entendimento.

Em [GOZ 2003], o autor fala da terminologia de qualidade de serviço em redes IP. O autor provê uma visão mais comum da terminologia relatada para qualidade de serviços em redes IP. São abordadas as definições de QoS e comparadas. Também é relatado em detalhes a terminologia utilizada nas duas arquiteturas mais importantes de QoS em redes IP, IntServ e DiffServ.

Em [LEV 2000], é tratado o controle de congestionamento em aplicações de vídeo conferência multiponto. O autor propõe uma estratégia para o controle de congestionamento para vídeo conferência multiponto, esta estratégia tem um controle sobre parâmetros que podemos configurar para fazer uma troca entre uma baixa qualidade de serviço e a considerada ideal. A estratégia implica algumas aritméticas e operações simples, que podem ser executadas rapidamente para o controle de congestionamento em tempo real.

Em [FAY 2002], o autor fala da validação de métricas para testar a efetividade de mecanismos de qualidade de serviço para sistemas fim-a-fim como distribuição de áudio e vídeo.

Em [BAR 98] o autor fala do desenvolvimento e implementação de uma arquitetura de qualidade de serviço em RSVP para serviços integrados. Esta arquitetura representa um aumento funcional para a pilha do protocolo TCP/IP. O artigo também descreve a implementação desta arquitetura na plataforma IBM AIX, e relata os experimentos feitos neste ambiente.

Em [KUO 2003], os autores fazem uma introdução sobre o protocolo de reserva de recursos e relatam uma falha de flexibilidade dos recursos do protocolo RSVP. É feito uma proposta para uma extensão do protocolo RSVP chamado de *Dynamic RSVP protocol* onde é possível prover diferentes reservas de recursos, necessária para

diferentes nós receptores. No DRSVP existem dois módulos de decisão para onde as requisições são passadas, chamados de *admission control* e *policy control*. Neste artigo dois aspectos diferem do modelo RSVP definido no RFC 2205, um é que os recursos necessários no DSRVP são recursos variados e não um valor específico, e outro é que cada roteador no caminho da reserva pode ajustar os recursos reservados dinamicamente.

Em [MEL 2001] foi desenvolvido uma análise baseada em medições da efetividade da utilização de QoS usando a arquitetura de serviços diferenciados. Neste trabalho foi comprovado através de experimentações práticas a eficiência da arquitetura de serviços diferenciados no provimento de políticas de qualidade de serviço.

Em [FON 99] são feitas comparações entre resultados sobre FIFO, WFQ e RSVP em aplicações de vídeo em tempo real. Foi constatado que o RSVP em situações de congestionamento da rede tem resultados muito bons em relação a perda de pacotes, mas quanto ao atraso dos pacotes não teve o comportamento desejável.

Em [MES 99] foi estudado um modelo analítico para a avaliação de desempenho de aplicações de vídeo sobre demanda em ambientes ATM, com a utilização do protocolo RSVP, este trabalho teve um resultado bem positivo permitindo prever como o sistema reagirá à variações em sua configuração.

Em [LUN 2001] foi desenvolvido um estudo para o desenvolvimento de aplicações com a capacidade de modificar seu comportamento conforme o desempenho oferecido pela rede. O trabalho apresentou uma camada de adaptação de QoS, esta monitoração deu-se através da análise dos pacotes RTCP *Sender Reports Receiver Reports*, pois permitem monitorar a qualidade da distribuição dos dados.

1.2 Comparação do modelo estudado com o estado da arte

Observou-se nas pesquisas realizadas uma tendência forte para o desenvolvimento de soluções complementares para QoS, além de inúmeras experimentações sobre o modelo de serviços integrados. Este trabalho também apresenta um estudo experimental sobre o modelo de serviços integrados com forte referência ao que vem sendo desenvolvido por pesquisadores de renome internacional. Os trabalhos correlatos analisados apontam para o entendimento de que o modelo de serviços integrados é eficaz, porém exige um grande esforço de implementação. Este foi um dos resultados

conclusivos deste trabalho, em conformidade com os resultados obtidos por outros trabalhos correlatos.

1.3 Objetivos do trabalho

1.3.1 Objetivo geral

Fazer uma análise experimental da implementação de serviços integrados em redes IP, avaliando a eficiência da arquitetura através de experimentos de laboratório.

1.3.2 Objetivos específicos

- *Implementar um ambiente de QoS, utilizando a arquitetura de serviços integrados;*
- *Verificar através dos experimentos de medição, o atraso, a variação do atraso e perda de pacotes em redes congestionadas;*
- *Verificar a capacidade do protocolo RSVP em isolar tráfego em redes congestionadas;*
- *Verificar o comportamento de uma aplicação de vídeo conferência em uma rede IP com QoS habilitado e não habilitado.*

1.4 Organização do trabalho

O trabalho esta dividido em três partes: Conceitos, Experimentos e Resultados. Estas três partes foram divididas em nove capítulos descritos a seguir:

Capítulo 2: Qualidade de serviços – Neste capitulo são apresentados os conceitos sobre QoS, os mecanismos de controle de tráfego e a real necessidade do uso de QoS. Também são apresentadas as formas de medição em redes IP, e toda a problemática envolvida nas medições de QoS.

Capítulo 3: Engenharia de tráfego e QoS: Neste capítulo é apresentado os mecanismos de policiamento de tráfego, controle de congestionamento, a arquitetura do modelo de serviços integrados e protocolo de reserva de recursos RSVP.

Capítulo 4: Vídeo Conferência e QOS: Neste capítulo, são apresentados os conceitos de vídeo conferência, os tipos de vídeo conferência e o padrão H323.

Capítulo 5: Resultados Experimentais: Neste capítulo serão descritos com detalhes todos os experimentos realizados em laboratório, e os resultados dos referidos experimentos.

Capítulo 6: Conclusões: Neste capítulo são apresentadas as conclusões finais e recomendações para trabalhos futuros.

2. QUALIDADE DE SERVIÇO

2.1 O que é qualidade de serviço (QoS)

Com o enorme crescimento e popularidade da internet, devido a sua grande capacidade de interconectar redes distintas, a tendência natural foi a convergência para o protocolo IP. Segundo [MEL 2001], uma frase tornou-se popular: "*IP over everything*", ou tudo sobre IP. Devido ao fato da internet trabalhar através de melhor esforço sem garantia de qualidade, tornaram-se necessários estudos para descobrir formas de se garantir qualidade e confiabilidade nas transmissões IP, pois ao se comparar com o ATM o problema do IP é não possuir QoS. Segundo [MEL 2001] o valor agregado que as redes IP provêem para aplicações de áudio e vídeo é enorme e habilitam novas dimensões:

- *Incluir ligações WEB ou envio de slides e arquivos durante uma transmissão;*
- *Comunicação nos dois sentidos permitindo que receptores possam interagir com provedores.*

As aplicações que necessitam de interação como voz e vídeo conferência não dependem apenas da largura de banda mas devem ter as perdas de pacotes e o atraso bem controlados. Perdas de pacotes muito altas, inviabilizam totalmente a execução de aplicações com estas características. Como a convergência é uma realidade, praticamente tudo roda sobre o protocolo IP, a diminuição e o controle do atraso, da variação do atraso e da perda de pacotes se torna primordial.

Não existe uma definição específica do que é QoS. No âmbito de redes, QoS é a capacidade de uma rede para poder garantir continuidade de transmissão em tecnologias como IP, frame-relay, ATM e ethernet. Em [CIS 2002a], QoS é habilidade de uma rede para prover melhor serviço para um determinado tráfego.

Para [SAN 99], quando utiliza-se QoS, pode-se oferecer maior garantia e segurança nas aplicações para a internet, pois aplicações avançadas como voz sobre IP e vídeo conferência possuem prioridade sobre outras aplicações que continuam utilizando melhor esforço.

Com o forte crescimento das redes e com a grande diversidade de aplicações que nela rodam, as aplicações tem mostrado diferentes necessidades de QoS. São apresentados cada vez mais os estudos sobre mecanismos de controle de tráfego.

Existem muitos mecanismos de controle de tráfego como serviços integrados/RSVP, serviços diferenciados, MPLS, 802.1p, entre outros [ABE 2001], [CAD 2003]. Os mecanismos de controle de tráfego estão divididos em mecanismos por conversação e mecanismos por agregação. No mecanismo de controle de tráfego por conversação os controles são feitos por fluxos separados. Neste contexto é incluído todo o tráfego entre uma instância de uma aplicação e o host [MEL 2001]. Os serviços integrados são um bom exemplo de controle de tráfego por conversação.

No mecanismo de controle de tráfego por agregação o tráfego é agrupado em um conjunto de tráfego de múltiplas conversações e classificado para o mesmo fluxo e controlado de forma agregada [MEL 2001]. Um bom exemplo de controle de tráfego por agregação é o modelo 802.1p e serviços diferenciados [CAD 2003].

Neste capítulo referenciaremos todos estes mecanismos dando uma ênfase maior em serviços integrados que é o tema deste trabalho.

2.2 802.1p

O 802.1p é uma proposta padrão de um mecanismo de controle de tráfego que foi desenvolvido para prover QoS basicamente nas estruturas de rede local [CAD 2003].

O 802.1p *priority queueing*, define um campo no cabeçalho dos pacotes 802, que possuem 8 níveis de prioridade, através de um rótulo de 3 bits que é transmitido no frame ethernet [CAD 2003]. Quando uma aplicação requer uma determinada priorização dentro da rede local, podemos exemplificar o caso de telefones IP, o telefone faz a marcação da precedência e o frame ethernet segue para o switch de acesso que naturalmente precisa suportar o protocolo 802.1p [SIL 2000]. A priorização é explicitamente definida na marcação do campo, esta priorização não deriva do endereço MAC de origem nem de destino [DUA 2002]. É necessário, também que seja implementado filas separadas, com políticas bem definidas para os quadros de prioridade diferentes [DUA 2002].

2.3 802.1q

O 802.1q é uma proposta de padrão de arquitetura que possibilita a criação de redes virtuais, também conhecidas como *virtual LAN* ou simplesmente VLAN, que são separadas logicamente, mas compartilham a mesma estrutura física [MOL 2004].

As redes virtuais são conjuntos de objetos que se comunicam independentemente da localização física, como se fossem uma mesma rede lógica ou estivessem no mesmo domínio de broadcast [MOL 2004]. O padrão IEEE 802.1Q, define a operação de VLANs na camada 2, permitindo a definição, operação e administração de redes virtuais. O IEEE 802.1Q foi desenvolvido para endereçar o problema de como dividir as redes grandes em partes menores, deste modo o tráfego broadcast e multicast, não necessitariam mais largura de banda [MET 2004].

2.4 ATM

A tecnologia ATM *Asynchronous transfer mode* ou modo de transferência assíncrona, é baseada na transmissão de pequenas unidades de informação com tamanho fixo e de formato padronizado, chamado de células [SOA 95]. Estas células são transmitidas através de uma conexão através de circuitos virtuais, onde o encaminhamento é baseado em informações contidas dentro do cabeçalho do pacote [SOA 95]. Esta células são parecidas com os pacotes, mas em tamanho menor e também possuem sempre o mesmo valor. O ATM trabalha com comutação de pacotes e não com comutação de circuitos, onde a tecnologia ATM pode ser aplicável tanto em redes de longa distancia WAN como em redes locais LAN.

Uma das premissas básicas no desenvolvimento das redes ATM foi a garantia de qualidade de serviço para o transporte integrado de dados, voz e vídeo [CAR 2004].

O ATM trabalha com priorização de tráfego com base nas classes de serviço, que por sua vez são associados a uma conexão ATM [CAR 2004].

As principais características da rede ATM é:

- *Não possui controle de erros no campo de dados e fica então sob responsabilidade das camadas superiores este controle;*
- *Opera no modo orientado a conexão, segundo um modelo de circuitos virtuais;*
- *Pode fazer transporte de qualquer tipo de dado, seja ele inclusive voz e vídeo;*
- *As células tem tamanho fixo e reduzido.*

O ATM trabalha num modelo divido em camadas ou níveis:

- *Nível AAL – ATM Adpatation layer;*
- *Nível ATM – Canais e caminhos virtuais;*
- *Nível Física [MOR 2004].*

2.5 MPLS

MPLS (*Multiprotocol Label Switching*), é um protocolo de roteamento que usa pacotes rotulados, cada rótulo representa um índice na tabela de roteamento do próximo roteador [ASS 2002]. Quando um roteador recebe um pacote ele faz um busca na sua tabela de roteamento, baseado no endereço IP ele decide para onde enviar o pacote, esta busca em alguns casos pode levar bastante tempo, o MPLS vem para mudar isso usando um rótulo de tamanho fixo, o MPLS também é conhecido como técnica de encaminhamento baseada em rótulos (*Label Switching*) [KAM 99]. Os pacotes que tem o mesmo rótulo e mesma classe de serviço são tratados igualmente. Ele é chamado de multi protocolo porque pode trabalhar com qualquer protocolo da camada 3.

Os pacotes são enviados de um roteador para outro através de um protocolo de rede sem conexão, cada roteador analisa o pacote e toma decisões independentes sobre para onde enviar o pacote.

O MPLS está dividido em dois componentes, componente de controle e componente de encaminhamento [DIA 2001]. No componente de encaminhamento, é onde os pacotes são enviados de uma entrada para uma saída, é utilizada uma tabela de encaminhamento mantida pelo componente de controle e a informação mantida no próprio pacote. O componente de controle constrói e mantém a tabela de encaminhamento [DIA 2001].

2.6 Serviços Diferenciados

A arquitetura de serviços diferenciados foi projetada para oferecer classes de serviços agregados, onde os fluxos são agrupados e tratados pela rede de acordo com a classe de serviço que se encontram [ABE 2001]. Seu funcionamento baseia-se em marcar no cabeçalho do pacote IP, o campo TOS (*Type of Service*) isto para o IPV4, agora chamado campo DS.

A figura 2.1 representa o uso do campo DS. Os primeiros bits de 0 à 5 representam o DSCP (Differentiated Service code point) e os outros bits são reservados.

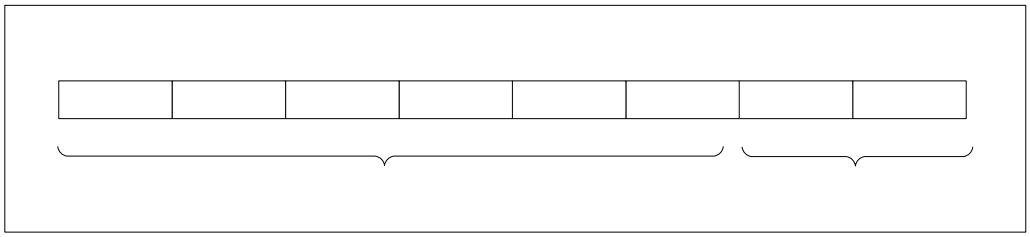

Figura 2.1 – Representação do campo DS

Serviços diferenciados definem o conceito de domínio DS, que é um conjunto de nós DS que aplicam um conjunto comum de políticas sobre o tráfego [MEL 2001].
Todo o tráfego que chega em uma rede DiffServ é primeiro classificado, depois passa por um filtro com o objetivo de molda-lo de acordo com a política associada aquela classificação [ABE 2001]. Na arquitetura existem os roteadores de borda que classificam o fluxo que chega e os roteadores internos que aplicam um tratamento agregado por nó aos pacotes. Os pacotes são sujeitos a tratamento específico, chamado comportamento agregado por nó (PHB – "Per-Hop-Behavior"), que dependerá do valor do campo DS [ABE 2001].

Na figura 2.2 é representado o domínio DS.

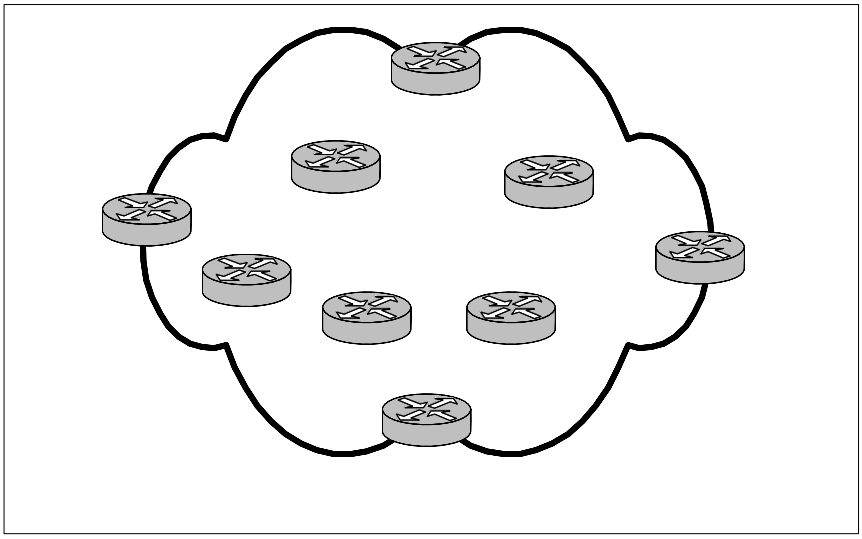

Figura 2.2 – Representação de Domínio DS

Os PHBs foram padronizados em PHB EF (*Expedited Forwarding*) e PHB AF (*Assured Forwarding*).

O PHB EF, também representa os serviços premium ou de canal dedicado, onde é usado para tráfego que exige baixa perda, baixo atraso e baixa variação do atraso [MEL 2001]. Estes requisitos são garantidos assegurando que este grupo tenha pouco enfileiramento [MEL 2001].

O PHB AF, faz entrega de pacotes IP, com uma largura de banda assegurada e quatro classes de transmissão, mas não faz garantias quanto ao atraso [MEL 2001].

2.7 Serviços Integrados

A estrutura de serviços integrados foi desenvolvida para possibilitar o provimento de QoS fim a fim, podendo assim prover qualidade de serviços total entre dois pontos [BRA 94].

Recentemente experimentos demonstraram a capacidade de protocolos de comutação de pacotes, suportar serviços integrados, para transporte de áudio e vídeo em tempo real [WRO 2000]. No modelo de serviços integrados, cada aplicação que necessite de recursos de QoS, deve informar as condições necessárias para que isto aconteça, desta forma a requisição da qualidade de serviço é feita pela aplicação. Para este modelo, torna-se necessário o uso de um protocolo de reserva de recursos chamado de RSVP, para que seja possível a requisição e reserva de um determinado caminho para a aplicação, seja isto num ambiente ponto a ponto ou multicast [SCH 2000]. O funcionamento do RSVP se baseia no envio de duas mensagens, uma chamada de mensagem *path* que tem como função percorrer o caminho ponto a ponto para verificar se o ambiente tem suporte ao serviço e uma mensagem chamada de mensagens *resv*, que faz o caminho inverso confirmando o estabelecimento da sessão.

2.8 Métricas de QoS

A análise de tráfego nos permite a identificação de anomalias na rede, no que diz respeito a questões de segurança e arquitetura da rede. Através da análise de tráfego é possível a identificação de possíveis tentativas de invasão, ou de até mesmo falhas no desenho da arquitetura de uma rede [NUP 2004]. Muitas redes apresentam problemas

em sua infra-estrutura, como a falta de controle de erros e atrasos, altas taxas de congestionamento, a falta de priorização das aplicações de missão crítica dentre inúmeros outros problemas. Em virtude disto a necessidade de se gerenciar o tráfego e fazer medições em redes IP se torna extremamente necessário. Com a análise de tráfego é permitido se identificar problemas e anomalias nas redes aumentando a segurança e a disponibilidade de uma conexão IP. As medições estão basicamente divididas de duas formas. As medições passivas e ativas. A medição passiva faz a coleta das informações dos pacotes que trafegam na rede, sem que para isso seja necessário fazer qualquer tipo de interferência no tráfego. Na medição ativa o principio é diferente, são pacotes de testes que são inseridos na rede, para que se possa analisar o seu desempenho. Cada uma destas formas tem o seu valor, e são usadas dependendo do objetivo e da métrica adotada.

As métricas de performance IP (*IPPM – IP Performance Metrics)*, como meta cobrem com um arco o esforço de concluir uma situação em que usuários e provedores de internet tem transportado serviços cuidadosamente vindo do entendimento de desempenho e confiabilidade dos componentes da internet que eles usam ou provêem [PAX 98]. Realizar estas métricas de desempenho e confiabilidade para estes caminhos completos precisam ser melhor desenvolvidos [PAX 98].

Reuniões do grupo de trabalho do IETF tem definido alguns destes critérios que devem obedecer os seguintes itens [PAX 98]:

- *As métricas devem ser concretas e bem definidas;*
- *As métricas não devem exibir tendências para implementações IP com tecnologia idênticas;*
- *As métricas devem exibir entendido e em linhas justas para as redes IP implementadas com tecnologias não idênticas;*
- *As métricas devem ser usuais para usuários e provedores no entendimento de que desempenho eles ensaiam ou provem;*
- *As métricas devem evitar induzir metas de desempenho artificial.*

Existe na prática uma dificuldade muito grande de definir as métricas e medições de redes IP [PAX 98]. Cada métrica deverá ser definida em termos de unidades padrão de medição. O sistema internacional de métricas é usado com os seguintes pontos especialmente notados [PAX 98]:

- *Quando uma unidade é expressa simplesmente em metros (como distância ou tamanho) ou em segundos (para duração,) unidades relacionadas apropriadamente em um mil ou mili-segundos de unidades aceitáveis são aceitáveis. Deste modo distâncias expressas em Kilo-metros e duração expressa em milisegundos ou microsegundos são reconhecidas, mas não centímetros (devido ao prefixo que não é um termo em mil-segundos ou mili-segundos).*
- *Quando a unidade é expressa numa combinação de unidades, apropriadamente relacionadas a unidades baseadas em mil-segundos ou mili-segundos de unidades aceitáveis são aceitáveis. Deste modo Kilometros por segundo são aceitos, mas metros por mili-segundos não.*
- *A unidade de informação é o bit.*
- *Quando prefixos de métricas são usados com bits ou com combinações incluindo bits, estes prefixos terão seus sentidos de métrica relacionadas para 1000, e não o significado convencional de armazenamento de computador de 1024. Em algum RFC de que define de que unidades incluem bits, esta convenção será seguida e repetida.*
- *Quando um tempo é dado, isto será expresso em UTC.*

Nota-se então que estes pontos aplicam-se para ser especificados por métricas e não, para formato de pacotes onde os *octetos* serão provavelmente usados em preferência ou adição aos bits [PAX 98]. Finalmente nota-se que algumas métricas podem ser definidas em termos de outras métricas, tais métricas são chamadas de métricas simples [PAX 98].

2.9 Metodologia de medição

Para um dado conjunto de métricas bem definidas um número distinto de métodos de medição pode existir. A seguir é listado uma lista parcial:

- *Medições diretas de métricas de desempenho usam teste inocular de tráfego. Como exemplo: Medição de atraso round-trip de pacotes IP de um dado tamanho sobre uma dada rota em um dado momento;*
- *Projeção de uma métrica vinda de medições de baixo nível;*
- *Estimativa de uma métrica constituinte vinda de um conjunto de mais medições agregadas;*

- *Estimativa de uma determinada métrica em um tempo vindo de um conjunto de métricas relacionadas em outros tempos.*

Uma metodologia para uma métrica deve ter a propriedade que é reconstituição: Se a metodologia é usada múltiplas vezes embaixo de condições equivalentes, isto deve resultar em medições consistentes.

2.10 Atraso

É o tempo onde um pacote é passado do emissor, através da rede, para o receptor, o tempo que o pacote leva da origem ao destino.

Quanto maior o atraso, maiores são os problemas causados para que os protocolos de transporte funcionem bem, como o TCP. As aplicações de áudio e vídeo exigem o controle dos níveis máximos de atraso [KAM 99]. Caso o atraso seja muito grande ele prejudica a conversação através da rede, tornando difícil a interatividade necessária para certas aplicações. Os principais responsáveis pelo atraso são o atraso de transmissão de codificação e de empacotamento [BRU 2002].

2.10.1 Atraso de Transmissão

É o tempo após a placa de rede ter transmitido até chegar na placa de rede destino. Vários fatores, como o atraso no meio físico, processamento em cada roteador ou Switch e fila de espera nos roteadores e switchs.

2.10.2 Atraso de Codificação e Decodificação

Os sinais como voz e vídeo normalmente são codificados num padrão do tipo PCM (G.711 em 64 Kbps) para voz ou H.261 para vídeo.

Esta codificação gasta um tempo de processamento da máquina. Alguns protocolos gastam menos como o G.711, que ocupa menos de 1 ms porém requerem 64 Kbps. Outros protocolos como G.729 requerem 25 ms de codificação, mas ocupam apenas 8 Kbps de banda.

2.10.3 Atraso de Empacotamento e Desempacotamento

Após codificado o dado deve ser empacotado na pilha do modelo de referencia OSI para ser transmitido na rede, isto gera um certo atraso. Este atraso de empacotamento e seu desempacotamento no destino devem ser considerados.

2.11 Variação do atraso

Também conhecido como *jitter*, é a variação do atraso fim à fim. Mesmo com níveis de atraso dentro dos limites, variações altas no atraso podem ter efeitos negativos na qualidade dos serviços oferecidos pela rede [KAM 99].
O gerenciamento do atraso não é suficiente para se garantir qualidade na transmissão, pois as redes não conseguem garantir uma entrega constante de pacotes ao destino. Desta forma os pacotes chegam de forma variável, causando uma variação do atraso ou *jitter*. [BRU 2002]

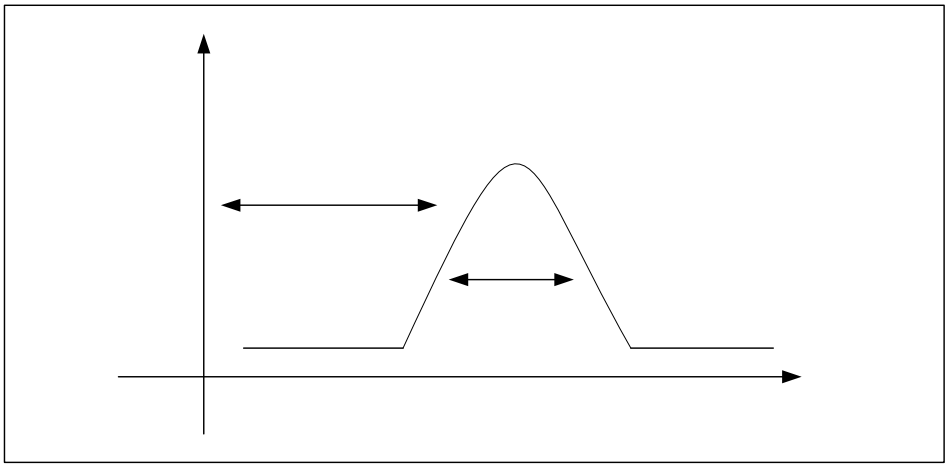

Figura 2.3 – Representação da variação do atraso

A aplicação no destino deve criar um *buffer*, cujo tamanho vai depender do *jitter*, gerando mais atraso na conversação. Este *buffer* serve como uma reserva para manter a taxa de entrega constante no interlocutor.

	Telefone	Download	TV	Vídeo Conferência
Latência	Sensível	Insensível	Insensível	Sensível
Jitter	Sensível	Insensível	Sensível	Sensível
Largura de banda	Baixa	Depende	Alta	Alta

Tabela 2.1 - Pacotes críticos para aplicações multimídia

2.12 Efeitos de tamanho de fila

Uma declaração mais precisa pode ser feita sobre os mecanismos de descartes de desvio inicial . A capacidade de transmissão e o tamanho da fila são relacionados. Se a largura de banda de uma transmissão é de 1 Mbps e a taxa de chegada de um pacote é 1,5 Mbps, por exemplo, a fila crescerá a uma taxa de 0,5 Mbps (ou 64 Kbps). Se o tamanho da fila é Q bytes, a velocidade de transmissão é T bits por segundo, e a taxa de chegada dos pacotes é A bits por segundo o descarte dos pacotes ocorrerá depois (8 * Q) / (A / T) segundos. Neste estado cada pacote da fila é atrasado por (8*Q) / T segundos [MEL 2001]. Incrementando o tamanho da fila com uma fração de redução da transmissão de largura de banda proporcional aos pacotes descartados desde que estouro passageiro do trafego. Isto também incrementa a variável de tempo de transmissão de pacotes, de qualquer modo que a rotação dos tempos de retransmissão TCP. Este aumento da variação RTT causa respostas TCP mais lentas para disponibilidade dinâmica de recursos da rede [MEL 2001].

2.13 Medir QoS

Uma ordem de interesse obvio é como se deve medir QoS em uma rede. Para que seja analisado se os requisitos de QoS estão sendo atendidos, a necessidade de se realizar medições de QoS é essencialmente importante [NUP 2004]. Uma de muitas razões aparentes de se medir QoS é para prover faturamento de serviços para tráfegos que recebem um tratamento diferenciado em uma rede comparado com o trafego tradicional tarifado como melhor esforço [FER 99]. Outra importante razão é o fato de uma organização que prove o serviço deve ser competente de ordem de capacidade

neste *backbone,* que irá entender a disparidade entre melhor esforço e tráfego de QoS [FER 99].

Desta forma pode-se adotar algumas técnicas de medição de QoS, para que se possam executar atividades de coleta, armazenamento, visualização e análise da rede [NUP 2004].

Como já dito anteriormente existem dois métodos de medição as medições ativas e passivas, também conhecidas respectivamente como intrusiva e não intrusiva.

2.13.1 Medições Ativas

As medições ativas também conhecidas como medições intrusivas consistem na injeção de pacotes na rede e a posterior coleta destes pacotes para uma análise da situação da rede [FER 99]. O comando *ping* ou ICMP é um exemplo bem simples deste método de medição. Pelo envio seqüencial de pacotes *ping* em intervalos regulares, uma estação de medição pode medir parâmetros tais como alcançabilidade, a transmissão RTT para uma localização remota e a expectativa de perda de pacotes. Por fazer um número de suposições secundárias com referência a maneiras de enfileiramento dentro dos *Switches*, combinados com medições de perda de pacotes e variação do atraso imposto, pode-se fazer algumas suposições sobre a largura de banda disponível entre dois pontos e seu nível de congestionamento. Medir com efetividade uma estrutura de QoS deve ocupar uma transação típica de carga de rede e medir este desempenho abaixo de condições controladas. Pode-se fazer isso pelo uso de gatilhos remotamente de gerador de dados [MEL 2001]. A metodologia de requisição é medir com efetividade taxa de dados sustentados, a taxa de retransmissão, a estabilidade de estimativas de RTT e sobre o tempo das transações. O problema é que mecanismos de QoS são visíveis somente quando partes da rede estão por baixo da contenção de recursos, e a introdução de medições intrusivas num sistema promover condições de sobre carga. Ocasionalmente suficiente isto é uma re-expressão do principio físico de bem entendimento: Dentro de uma quantidade sistema físico, existe um limite absoluto para a precisão de medições simultâneas de posição e cinética de um elétron [MEL 2001].

2.13.2 Medições Passivas

As medições passivas também conhecidas como medições não intrusivas, medem a rede pela observação da taxa de processamento de pacotes até o sistema fim e fazem algumas deduções do estado da rede, por meio disto deduzem a efetividade do QoS com base nestas execuções [FER 99] [MEL 2001].

Em geral, esta pratica requisita conhecimento intimo das aplicações que geram o fluxo de trafego inicialmente observadas, onde as ferramentas de medição podem distinguir entre o comportamento de aplicações remotas e moderação deste comportamento remoto pelo estado imposto da rede. O simples monitoramento de um site arbitrariamente de dados valores não produz muitas informações de valor e podem resultar em interpretações imprecisas dos resultados. Por esta razão o monitoramento *single-ended* como medição básica de desempenho de uma rede e pela conclusão, performance de QoS não é recomendado como um caminho efetivo para o problema [MEL 2001].

De qualquer modo pode-se esperar .para olhar mais adiante a preparação de ferramentas de monitoração baseadas em *host* que olham a maneira dos fluxos TCP e o tempo dos pacotes com o fluxo. Interpretações cuidadosas de partida dos pacotes enviados com obtenção de pacotes pode oferecer alguma indicação como enfileiramento induzido o caminho da rede num sistema remoto. Esta interpretação também pode prover uma indicação aproximada da capacidade de dados, embora a advertência aqui é que a interpretação possa ser finalizada cuidadosamente e os resultados devem ser relatados com considerável atenção [FER 99] [MEL 2001].

2.14 Resumo do capítulo

Neste capítulo, foram observados de forma geral, as técnicas de QoS existentes e os modelos de QoS fim a fim. Foram também apresentados os requisitos básicos para as redes suportarem QoS e analisadas as técnicas de medição em redes IP, principalmente a problemática relacionada com as medições de QoS. Foram também analisados alguns conceitos relacionados às métricas em redes IP.

3. ENGENHARIA DE TRÁFEGO E QOS

Quando se aplica QoS em redes IP, é permitido ao usuário escolher os métodos para enfileiramento e encaminhamento de pacotes e também a possibilidade de ajustes para estes parâmetros. Desta forma este capítulo descreve os principais métodos utilizados em redes IP.

3.1 Policiamento de tráfego

É um mecanismo disponível para controlar o tráfego de saída de uma interface para taxas especificas que esta interface possa suportar. Desta forma pode-se controlar o volume de tráfego que é enviado para a rede e a taxa de envio [FLA 2001].

Pode ser importante para identificar fluxos de tráfego que entram na rede, e que possam permitir separar o tráfego em fluxos individuais e molda-los de forma diferente.

O uso das técnicas de policiamento e modelagem de tráfego existem para que se possa evitar o congestionamento de circuitos de dados [FLA 2001].

Existem predominantemente dois modelos de policiamento de tráfego que são descritos com bastante profundidade em [FER 99], [FLA 2001] e [VEG 2001]. São eles o balde furado e o balde de tokens.

3.1.1 Balde furado

O balde furado é o conceito chave para nos dar um entendimento da teoria de enfileiramento [FLA 2001]. Uma fila pode ser comparada a um balde que recebe uma enxurrada de água. O balde tem um furo embaixo. A velocidade que esta água entra no balde, não influência na sua saída, que permanece constante, dependendo da largura do furo. Quando o balde ficar cheio, a água que entrar escorrerá pelos lados e será perdida [MEL 2001], [FLA 2001], fazendo uma analogia isto é o mesmo que o descarte de pacotes. Ao invés de usarmos água usaremos pacotes da rede, onde cada host conectado à uma interface que contém um balde furado [FLA 2001]. Se o pacote chegar e a fila estiver cheia ele será descartado [FLA 2001].

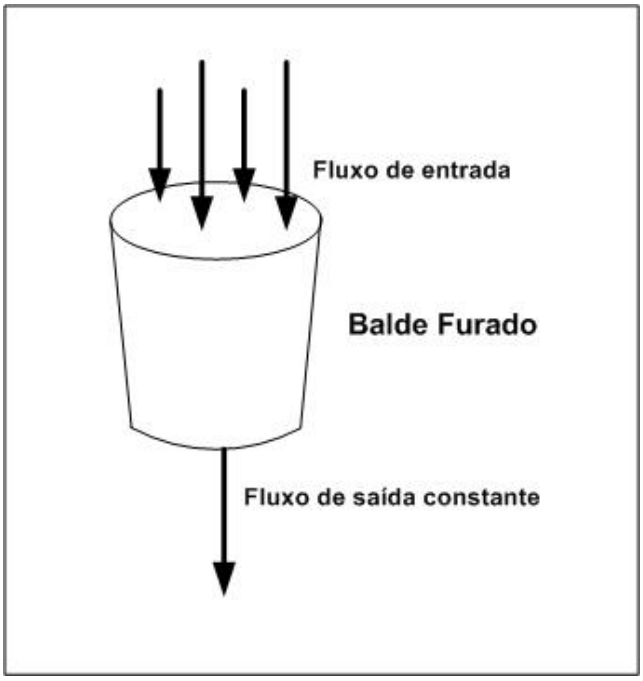

Figura 3.1 – Representação do modelo de balde furado

Quando a fila fica cheia os próximos pacotes à chegar são descartados, esta carência que faz que as filas não sejam infinitas [VEG 2001]. Eles podem somente segurar um conjunto de informações. Os administradores de redes normalmente podem configurar os tamanhos das filas em seus roteadores, mas o padrão é utilizar os tamanhos definidos pelo fabricante [FLA 2001].

Pacotes são colocados em fila na ordem que são recebidos e quando uma fila fica cheia são descartados [FLA 2001]. Na terminologia de filas este descarte se chama *Tail Drop*, ou descarte do último [MEL 2001] [FLA 2001]. Estes pacotes nunca entrarão na fila e serão descartados pelo roteador [FLA 2001]. O fato de pacotes serem descartados não indica que existe algum problema na rede [FLA 2001].

Alguns mecanismos de QoS, tais como *Random Early Detection* (RED) e *Weighted Random Early Detection* (WRED), fazem uso destes princípios para controlar o nível de congestionamento da rede [FLA 2001].

O mecanismo de *Tail Drop* pode impactar na resposta dos usuários. Pacotes descartados requerem meios de retransmissão [FLA 2001]. Com mais e mais aplicações sendo executadas através do protocolo TCP/IP, *Tail Drop* pode introduzir um fenômeno conhecido como *Global synchronization.*

3.1.2 Balde de tokens

No balde furado existe um fluxo de saída constante independente do tipo de tráfego. E, alguns casos é necessário que o fluxo de saída seja aumentado quando se recebe rajadas maiores de tráfego. Para complementar isto existe o balde de tokens que retém os tokens que são gerados por um *clock* na faixa de um token a cada *x* segundos [MEL 2001] é representado na figura 3.2. Diferente do balde furado o balde de tokens não permite nenhum mínimo descarte vindo do fundo [MEL 2001] [FLA 2001]. O que vai dentro do balde deve vir do topo. Com o passar do tempo os *tokens* são armazenados no balde pela rede [FLA 2001]. O algoritmo do balde de *tokens* joga os *tokens* fora quando o balde fica cheio, mas nunca faz o descarte de pacotes. Pelo fato deste algoritmo permitir rajadas em pequenos intervalos, o tráfego tende a ser mais regular se for colocado um balde furado após o balde de *tokens* [FLA 2001] [VEG 2001].

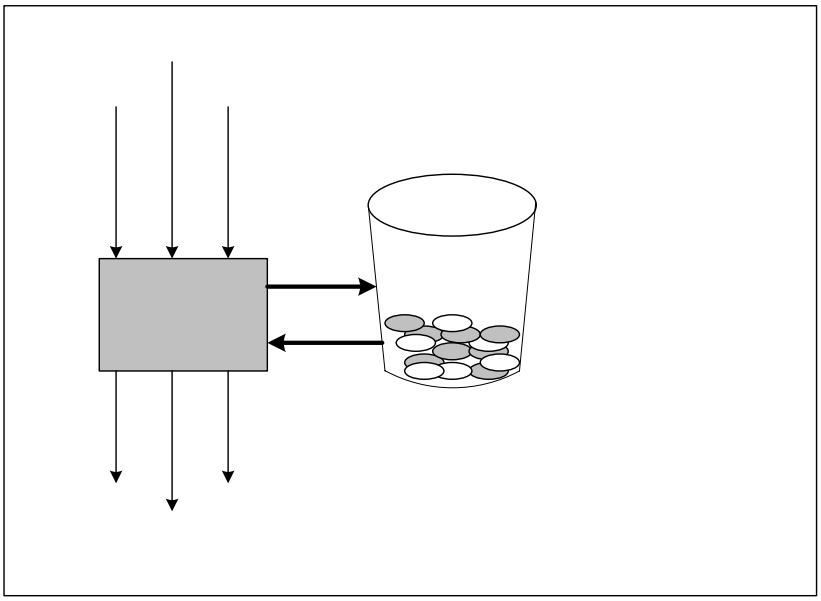

Figura 3.2 – Representação do modelo de balde de tokens

3.2 Controle de congestionamento

O controle de congestionamento é um termo que circunda as disciplinas de enfileiramento, que são usadas para gerenciar situações onde a demanda de largura de banda de certas aplicações na rede excedem a largura de banda total que pode ser

provida pela rede [FLA 2001]. Dentro do contexto de engenharia de redes, o enfileiramento é a ação de armazenar pacotes ou células, para um posterior processamento [FER 99]. O roteador é formado por processos de entrada, que remontam os pacotes do jeito como foram recebidos, pelos processos de encaminhamento, que identificam qual será o destino do pacote e por fim os processos de saída que são responsáveis pela transmissão dos pacotes para o próximo nó da rede. O conjunto de todos estes processos representa o funcionamento básico de um roteador, onde as filas existem para segurar e ordenar pacotes antes que estes recursos sejam encaminhados para as portas de saída [MEL 2001] [FLA 2001]. Se não existe congestionamento num roteador logicamente os pacotes terão um encaminhamento imediato [FLA 2001].

A seguir com mais detalhes são estudados algumas técnicas de enfileiramento:

- *First In First Out – **FIFO***
- *Priority Queuing – **PQ***
- *Custom Queuing - **CQ***
- *Weighted Fair Queuing - **WFQ***

Algumas destas técnicas de enfileiramento são aplicadas quando o tráfego existente na interface de um roteador excede a largura de banda de saída de uma porta e necessita ser priorizada [FLA 2001] [VEG 2001]. O administrador de redes deve conhecer os fluxos de dados que trafegam pela rede e como fazer a política de priorização deste tráfego [FLA 2001].

3.2.1 Enfileiramento First In First Out – FIFO

O enfileiramento FIFO, f*irst in first out* é considerado como um método básico bastante simples. Provê *store-and-forward*, armazenamento e encaminhamento [FLA 2001]. O primeiro pacote ao entrar na interface é o primeiro a sair [MEL 2001] [FLA 2001]. O mecanismo é colocado como um balde furado simples, que guia todo o tráfego para a interface de saída [FLA 2001].

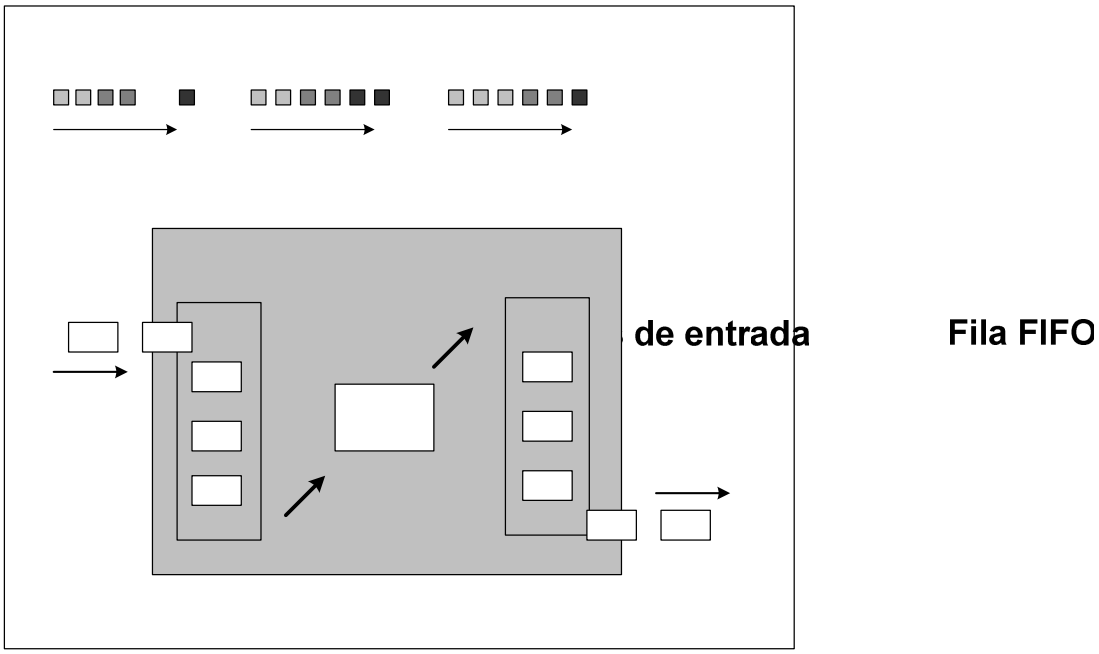

Figura 3.3 – Representa o Enfileiramento FIFO

O maior propósito da fila FIFO é guiar pacotes que chegam para uma interface. O FIFO possui muitas deficiências, tais como: Não tomar decisão sobre prioridade do pacote, a ordem de chegada é que determina a largura de banda que será obtida e não provê proteção contra aplicações ou fontes de tráfego com comportamento prejudicial [MEL 2001] [FLA 2001].

3.2.2 Priority Queuing – PQ

Priority Queuing (PQ) é uma forma poderosa e rigorosa de controle de congestionamento [FLA 2001]. PQ permite ao administrador de redes definir 4 filas de tráfego da rede [FLA 2001]. Estas filas são classificadas como prioridade alta, média, normal e alta. O roteador faz o processamento da fila baseado nestas prioridades [FLA 2001]. Se existem pacotes na fila com prioridade alta, esta fila irá processar até esvaziar, independente do estado das outras filas. Uma vez uma fila com prioridade alta é esvaziada, o roteador move a fila média e despacha um único pacote. Imediatamente o roteador despacha a fila alta para garantir o esvaziamento. Isto vai para a fila alta, fila média, normal e então a baixa [FLA 2001] [VEG 2001]. Todas as três, alta, média, e normal devem ser completamente esvaziadas, antes de um único pacote ser despachado

para a fila baixa. A cada momento o roteador despacha um pacote checado na fila alta [FLA 2001].

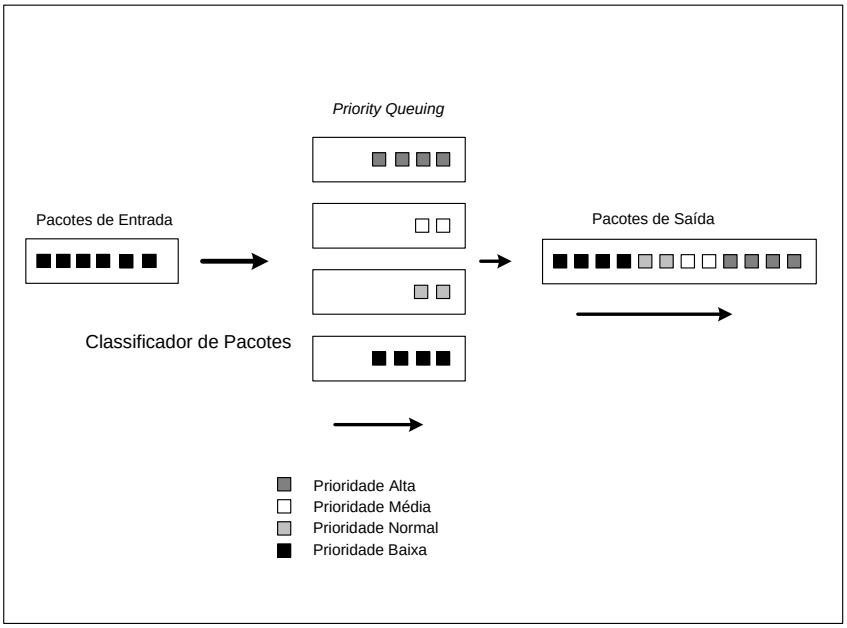

Figura 3.4 – Modelo *Priority Queuing*

Priority Queuing concede aos administradores de rede extraordinário controle sobre o tráfego da rede [FLA 2001]. Porém isto também permite aos administradores de rede poder suficiente para alterar a alteração de trafego de prioridade baixa para ser transmitidos a todos. Quando o tráfego de uma fila de prioridade baixa não é ocupado desde que exista muito tráfego em filas de prioridade alta, uma condição chamada *queue starvation* é citado para ter de ocorrer.

A função *Queue Starvation* é uma cilada do *Priority Queuing*, e é habilitado para enfraquecer completamente o tráfego de prioridade baixa, é algo que deve ser considerado cuidadosamente antes de projetar as estratégias de PQ [MEL 2001] [FLA 2001].

Tipicamente, PQ é usado quando aplicações sensíveis ao atraso encontram problemas na rede [FLA 2001]. PQ pode ser uma excelente ferramenta para protocolos tais como *serial tunneling* (STUN), *data link swit* (DLSW), ou *remote source bridging* (RSRB) [FLA 2001]. Deve-se ter um cuidado enorme antes de fixar um plano de priorização de tráfego. Como exemplo um administrador de redes configura um trafego http como tendo prioridade em uma rede onde o tráfego web é muito grande, isto é

provável que os outros protocolos nunca alcançarão serviços constantes, pois existe uma fila priorizando tráfego Web. Todas as outras filas encherão e descartarão pacotes quando alcançarem sua capacidade [FLA 2001]. O PQ, pode classificar tráfego de rede usando as características mostradas abaixo:

Pacotes que não são classificados pelo PQ são automaticamente colocados numa fila de prioridade normal [FLA 2001].

- *Protocolo de rede tipo IP, IPX, etc...;*
- *Tamanho de pacotes em bytes;*
- *Interfaces onde os pacotes chegam;*
- *O pacote é como um fragmento IP;*
- *Qualquer que possa ser descrito em uma lista de acesso normal ou extendida.*

Em *priority Queuing*, a fila padrão é a fila normal, de qualquer modo isto pode ser movido para qualquer fila [MEL 2001].

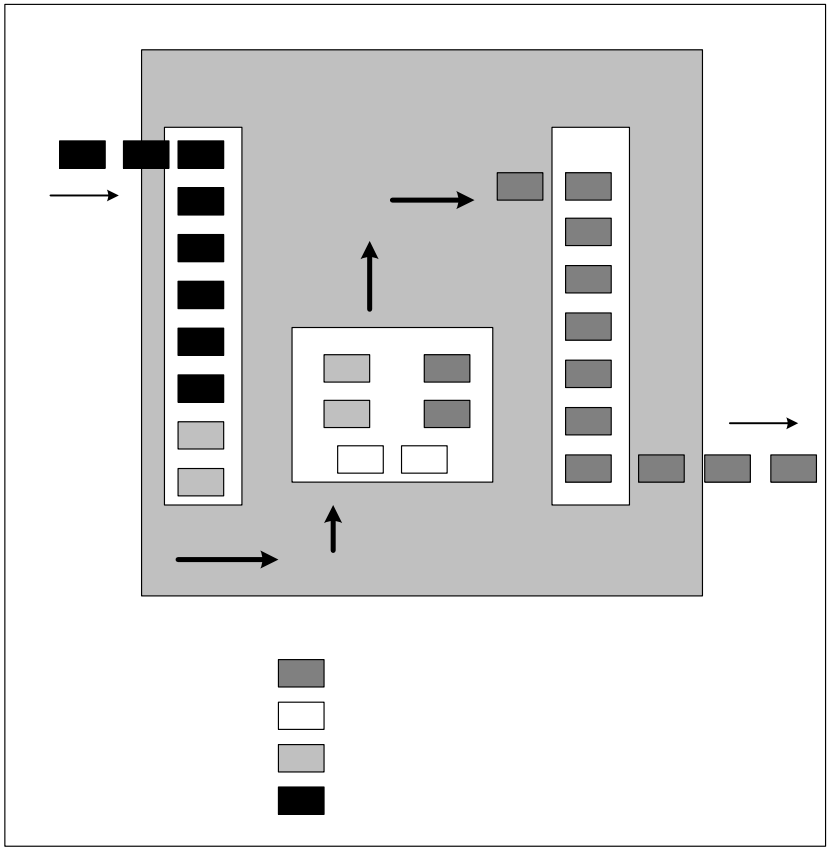

Figura 3.5 – Comportamento do modelo *Priority Queuing*

3.2.3 Custom Queuing - CQ

Supera o rigor do *priority queuing* (PQ), onde um administrador de rede pode escolher implementar em seu lugar uma *custom queuing* (CQ) [FLA 2001]. CQ permite ao administrador de redes priorizar o trafego em que afete a aparência de diminuir o desejo de filas prioritárias como visto em PQ [FLA 2001].

CQ permite a criação de 16 filas de categoria de tráfego, cada uma é descarregada em forma de circulo.

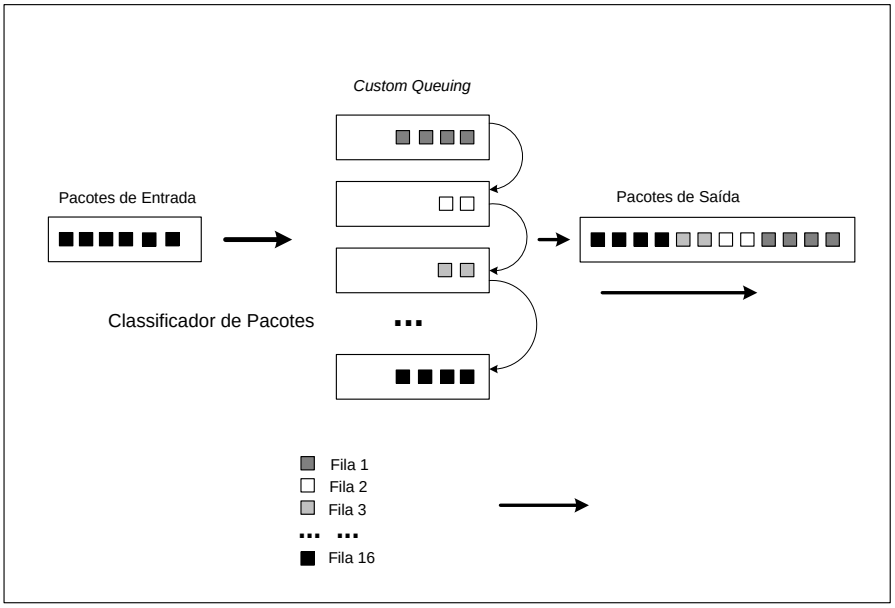

Figura 3.6 – Filas *custom queuing*

Quando a priorização vem disputar com CQ é um montante de dados que é servido para cada fila durante um ciclo [FLA 2001].

É importante notar que, enquanto uma vontade de fila é verdadeira, a forma *custom queuing* não é possível, isto é possível para marcar um conjunto de ciclo em qualquer fila alta que não pegar a banda que eles precisam de maneira conveniente [FLA 2001]. Quando isto ocorre, a aplicação com dados em parte pequena a fila pode estourar o tempo.

Enquanto isto não é verdade, aparência é similar e o sentido que a aplicação será incapaz de propriamente funcionar [FLA 2001].

3.2.4 Weighted Fair Queuing - WFQ

O método *fair queuing* é uma outra forma de controle de congestionamento. *Fair Queuing*, geralmente refere-se para *Weighted Fair Queuing*, isto é uma estratégia de enfileiramento padrão para as interfaces com pouca velocidade [MEL 2001]. WFQ é um método automático provendo amostras de alocação de banda para todo o tráfego da rede. WFQ distribui aleatoriamente o tráfego na rede em fluxos que criam uma conversação na rede pelo uso de uma combinação de parâmetros [MEL 2001].

Como exemplo, conversações individuais TCP/IP são identificadas usando os seguintes parâmetros:

- *Protocolo IP;*
- *Endereço IP de origem;*
- *Endereço IP de destino;*
- *Porta de origem;*
- *Porta de destino;*
- *Campo do tipo de serviço.*

Outros protocolos ou tecnologias usam parâmetros que são apropriados para estas características [FLA 2001]. Por rastreamento de vários fluxos, o roteador pode determinar que fluxos são intensos na banda, tais como FTP, e outros, que estão mais sensíveis ao atraso, tais como telnet ou FTP [FLA 2001]. O roteador prioriza estes fluxos e garante que fluxos de volume alto são levados para o fim da fila, e os de volume baixo sensíveis ao atraso tenham prioridade sobre outras conversações [FLA 2001].

Existem 256 filas disponíveis por padrão quando o WFQ é habilitado [FLA 2001]. O fator forte do WFQ entra em ação quando os pacotes tem diferentes níveis de precedência. Existem oito níveis de precedência com o valor mais alto proporcionando a prioridade maior [FLA 2001] [VEG 2001].

Eles são os seguintes:

- *Precedência de controle de rede (7);*
- *Precedência de controle internet (6);*
- *Precedência critica (5);*
- *Precedência de aumento relâmpago de velocidade (4);*

- *Precedência relâmpago (3);*
- *Precedência imediata (2);*
- *Precedência prioritária (1);*
- *Precedência de rotina (0).*

Quando projeta-se uma rede com WFQ, algumas limitações e considerações devem ser respeitadas [MEL 2001].

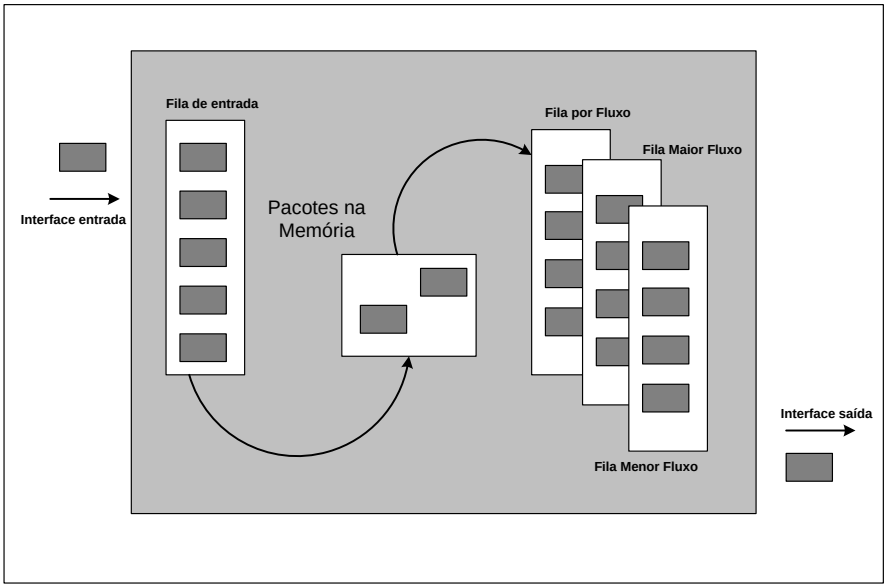

Figura 3.7 – Modelo *Weighted Fair Queuing* - WFQ

São mostradas algumas das características do WFQ, para ter em mente para distribuí-lo numa rede em produção [FLA 2001]:

- *Tráfego SNA e DLSW+ não podem ser quebrado em fluxos separados devido a maneira que sessões TCP/IP são estabelecidas dentro do fluxo. Devido ao fato de conversações compartilharem uma única sessão TCP/IP parece haver um único fluxo mesmo que existam múltiplas conversações dentro do fluxo..*
- *Isto não é recomendado usar WFQ para sessões SNA usando encapsulamento IP dentro DLSW+ bem como APPN.*

Quando o bit de precedência IP dentro do byte TOS em disputa, ajuste WFQ pelo processamento de maiores pacotes vindos de filas de fluxos precedência alta do que os de precedência baixa [FLA 2001].

Além do mais pacotes estão de saída pelo balde furado. A seqüência em que as filas estão em serviço pelo vestígio do mesmo WFQ, mas o conjunto de informações processadas vinda de cada fila agora da fila do que da fila [FLA 2001].

O fator peso é inversamente proporcional a precedência do pacote [VEG 2001]. Por esta razão conversações WFQ com peso baixo será provido com melhor serviço que fluxos com peso alto [VEG 2001].

3.3 Controle de admissão

Fisicamente links limitando velocidade por *clocking*, taxa de dados especificas em um circuito ou usando o balde tokens alavanca o trafego que entra [FLA 2001]. A implementação do balde de tokens pode ser uma implementação isolada ou *stand alone* ou parte da arquitetura de serviços integrados [FER 99]. Como uma alternativa não usar o enfileiramento *FIFO* como uma tentativa para a prioridade que certos tipos de trafego transmitem na interface do roteador, existem outros métodos como o controle de admissão que são usadas para controlar qual o trafego real é transmitido dentro de uma rede ou a taxa em que é admitido. Em suma o controle de admissão faz a distinção em que tipo de trafego pode ser admitido na rede em primeiro lugar [FER 99].

3.4 Arquitetura de Serviços Integrados

A estrutura de serviços integrados foi desenvolvida para prover um conjunto de extensão para o tráfego de melhor esforço, esta estrutura foi desenvolvida para prover um manuseio para certos tipos de tráfego e para prover mecanismos de controle de tráfego para as aplicações [FER 99] [BRA 97].

A concepção da arquitetura de serviços integrados inicia com o entendimento de que a infra-estrutura da internet não precisa ser modificada para que possa vir a suportar aplicações com diferentes requisitos de controle de atraso e variação do atraso, como áudio e vídeo em tempo real [FER 99].

A filosofia do modelo é baseada em fluxos, onde é necessário que os roteadores reservem recursos para garantir QoS para os fluxos dos usuários [ABE 2001]. Um fluxo de dados com QoS é um conjunto de pacotes que terá um tratamento especial ou prioritário.

Os fluxos são definidos por sessões que são identificados por uma especificação genérica, contento o endereço IP, o protocolo de transporte, a porta destino, e a lista de emissores para aquela sessão [ABE 2001].

A arquitetura de serviços integrados é baseada na reserva de recurso, por isso sempre antes de ser feita uma transmissão é necessário saber se a rede suporta a transmissão com QoS, para isto existem os protocolos de sinalização como o RSVP (*Resource Reservation Setup Protocol*), que se encarregam de analisar as condições da rede.

3.5 Exigências de QoS

O modelo de serviços integrados preocupa-se muito com o tempo de distribuição do tráfego, onde o atraso por pacotes é o tema central de determinação de comprometimentos de QoS [FER 99].

Aplicações de tempo real geralmente podem ser definidas como um fluxo de dados que é empacotado na origem e transportado pela rede até o seu destino onde é desempacotado por aplicações de recebimento. Conforme os dados são transmitidos, certamente a latência é introduzida em cada ponto do caminho [FER 99] [ABE 2001].

A quantidade de variação de latência introduzida é uma soma acumulativa de tempos de transmissão e tempo de espera na fila (onde estes tempos de espera podem ser altamente variados). A variação da latência também conhecida como *jitter* é o sinal de tempo real e é o que deve ser amenizado pela transmissão [FER 99] [MEL 2001]. O receptor compensa este *jitter* pelo armazenamento temporário de dados para o período de tempo (como atraso compensado) antes de enviar um fluxo de dados, em uma tentativa de negar os efeitos do *jitter* introduzido pela rede [FER 99]. O truque é calcular o atraso compensado que seja curto demais para o nível corrente de *jitter* efetivamente tornando o sinal de tempo real sem valor [FER 99].

O cenário ideal é ter um mecanismo que possa dinamicamente calcular e ajustar o atraso compensado em resposta a flutuação das médias de *jitter* induzidos [FER 99] [MEL 2001]. Uma aplicação que consiga ajustar o atraso compensado é chamada de aplicação de transmissão adaptável. O traço predominante de uma aplicação de tempo real, é que ela não espera a chegada atrasada dos pacotes quando transmitidos no

emissor também conhecido como *Sender*, ela simplesmente impõem um atraso compensado antes do processamento [FER 99].

A arquitetura de serviços integrados propõem duas classes de serviços, os serviços garantidos e os serviços de carga controlada.

3.5.1 Serviços garantidos

A classe de serviços garantidos é especificada pela RFC 2212 e prove uma infra-estrutura para a distribuição de tráfego para aplicações que requerem uma garantia de banda. As classes de serviços garantidos fornecem limites rígidos, prováveis matematicamente em termos de atraso de enfileiramento, onde os pacotes estarão condicionados dentro dos roteadores [SHE 97]. Os serviços garantidos somente computam o atraso de enfileiramento dentro do caminho de tráfego fim a fim [FER 99].

A estrutura dos serviços garantidos matematicamente afirma que o atraso de enfileiramento é uma função de dois fatores – primeiramente a espessura do *Token Bucket* (b) e o padrão do dado (m) que a aplicação requisita [FER 99]. É requerida uma taxa de transmissão garantida para os seus pacotes [SHE 97]. O modelo não garante o controle do atraso mínimo, e não controla ou minimiza a variação do atraso, ele somente controla o atraso de enfileiramento máximo [FER 99] [SHE 97].

A garantia do serviço é invocada por um emissor ou *Sender* que especifica o parâmetro de fluxo de trafego (*TSpec*) e subsequentemente o receptor requisita a garantia de nível de serviço (*RSpec*) [FER 99]. A classe de serviços garantidos também usa o parâmetro *Token_Bucket_Tspec* com o *TSpec* [FER 99]. O *RSpec* que é a especificação de reserva consiste de um padrão de dados (r) e de um *Slake term* (s), quando (r) for obrigado a ampliar ou a equalizar o *Token_Bucket* padrão (r) [FER 99].

O padrão (r) é mensurado em bytes de datagramas IP por segundo e tem um valor médio entre 1 byte por segundo e 40 terabytes por segundo [FER 99]. O *Slake-term* é mensurado em microsegundos [FER 99]. O *RSpec* padrão pode ser maior que o *TSpec* padrão, por causa do padrão superior que foi assumido para reduzir o atraso de enfileiramento o *Slake-term* representa a diferença entre o atraso desejado e o atraso obtido.[FER 99].

Por causa do calculo fim a fim e *Hop-by-Hop* de dois termos de erro (c e d), todos os nós num caminho de tráfego devem implementar serviços garantidos [FER 99]. O

primeiro termo de erro (c) prove uma crescente representação de atraso. O termo de erro (c) é mensurado em bytes [FER 99]. O segundo termo de erro (d) é um padrão independente, por representação de elementos do atraso imposto pelo tempo que foi esperado para a transmissão [FER 99]. O termo de erro (d) é mensurado em unidades de 1 microsegundos, o crescimento do calculo fim a fim destes termos de erro representam um afastamento de fluxo de um *Fluid model* [FER 99]

Dois tipos de policiamento de tráfego estão associados com os serviços garantidos: Policiamento simples e reformados [FER 99]. O policiamento simples é feito nas bordas de uma rede e o reformado é feito nos nós intermediários de uma rede [FER 99]. Policiamento simples está comparando o tráfego dentro de um fluxo oposto por uma conformidade *TSpec* [FER 99]. O policiamento reformado consiste de um esforço para restaurar o fluxo de tráfego característicos conforme o *TSpec* [FER 99].

Este modelo é ideal para aplicações que requerem limites de atraso rígidos, como aplicações de vídeo conferência.

3.5.2 Serviços de carga controlada

Os serviços de carga controlada tentam prover comportamento de tráfego fim a fim que aproximadamente se igualam ao modelo tradicional de melhor esforço [FER 99]. Deste modo um pouco melhor que o trafego de melhor esforço [FER 99].

O comportamento fim a fim provido para uma aplicação por uma série de elementos de rede prove serviço de carga controlada, que aproxima o visível comportamento para aplicações receberem serviço de melhor esforço de uma série de elementos de rede [WRO 97b].

O serviço de carga controlada pretende suportar uma boa parte de classes de aplicações que já estão desenvolvidas para serem usadas na internet hoje, mas que estão altamente sensíveis as sobrecargas da rede [WRO 97b]. Como exemplo uma sessão que requer uma classe de serviço de carga controlada receberá um QoS muito próximo daquele que um fluxo poderia receber de uma rede não sobrecarregada. O serviço de carga controlada não fornece garantias quantitativas acerca do desempenho [FER 99] [WRO 97b].

Este tipo de serviço é bom para aplicações de tempo real adaptativas, estas aplicações funcionam razoavelmente bem quando a rede não esta sobrecarregada, mas se degradam rapidamente quando a rede esta congestionada.

3.6 Protocolo para reserva de recursos (RSVP)

A arquitetura de serviços integrados provê uma estrutura para que as aplicações possam vir a escolher entre múltiplos níveis de serviços controlados de entrega de seus fluxos de trafego. Existem dois requerimentos básicos para suportar esta estrutura [FER 99]. O primeiro requerimento é para que os nós no caminho do tráfego suportem os mecanismos de controle de QoS, os serviços garantidos e serviços de carga controlada. O segundo requerimento, é um mecanismo onde as aplicações podem comunicar seus requerimentos de QoS para os nós ao longo do caminho. Possibilita também que nós de rede comuniquem entre si os requisitos de QoS, que devem ser providos para os fluxos de tráfego particular [FER 99]. Isto tudo pode ser provido de várias maneiras, uma delas é pela chamada RSVP.

RSVP (*Resource Reservation Setup Protocol*) é um protocolo de sinalização de controle de rede que possibilita aplicações obterem diferentes níveis de qualidade de serviço para seus fluxos de dados [CIS 2002b]. Este protocolo foi desenvolvido para trabalhar no modelo de serviços integrados. Tal como uma capacidade de identificar que diferentes aplicações tem diferentes requerimentos de rede [CIS 2002b]. O protocolo RSVP é usado por um host para requisitar qualidade de serviço de uma rede, por aplicações de fluxo de dados [BRA 97]. Além disso o RSVP é usado pelos roteadores para distribuir requisitos de qualidade de serviço para todos os nós ao longo do caminho dos fluxos e estabelecer e manter para prover os serviços requeridos [BRA 97].

É muito importante destacar que o RSVP não é um protocolo de roteamento [CIS 2002b]. RSVP trabalha em conjunto com protocolos de roteamento, e colocam a equivalência com as listas de acesso dinâmicas ao longo das rotas calculadas pelos protocolos de roteamento [CIS 2002b]. Deste modo implementações de RSVP não existem para requerer migração para um novo protocolo de roteamento [CIS 2002b].

O RSVP negocia a reserva de recursos em um único sentido de cada vez, desta forma utilizando um fluxo de dados *simplex*. O protocolo trata distintamente receptores e transmissores, operando juntamente com a camada de transporte.

Pesquisadores da University of Southern Califórnia (USN), da Information Sciences Institute (ISI) e da Xerox's Palo Alto Research Center (PARC), pensaram inicialmente o modelo RSVP [CIS 2002b]. O Internet Engineering Task Force (IETF), especificou uma versão aberta do protocolo RSVP mostrada no RFC 2205 [BRA 97], baseada na versão da USN e Parc [CIS 2002b]. Na figura 3.8 podemos analisar o modelo RSVP.

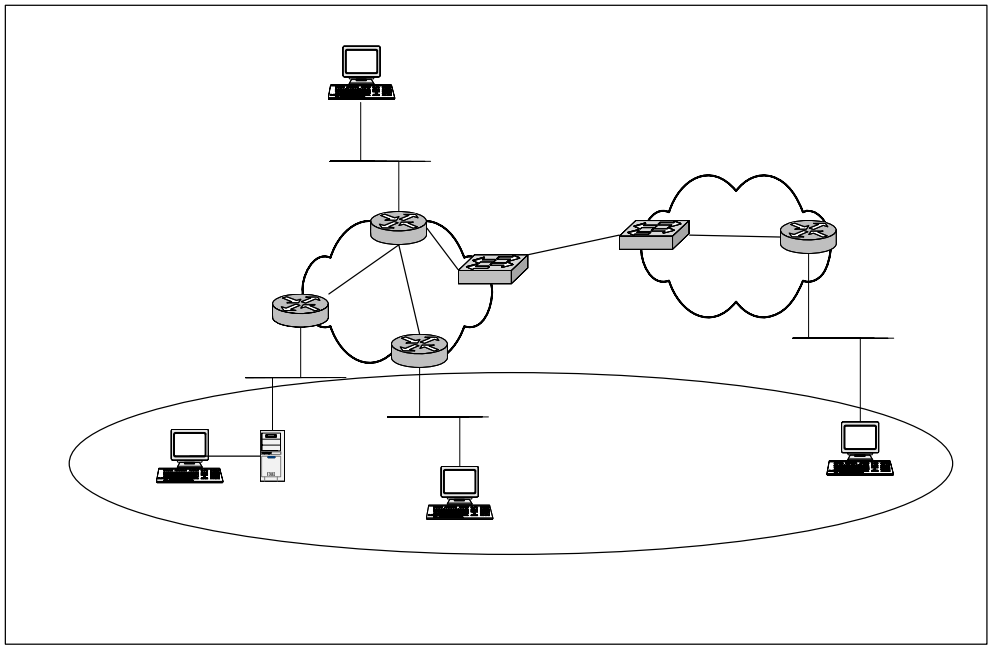

Figura 3.8 – Ambiente RSVP

O RSVP trabalha tanto no Ipv4 quanto no Ipv6, ocupando o lugar do protocolo de transporte [BRA 97]. De qualquer modo o RSVP não transporta dados de aplicações, mas é propriamente como o protocolo de controle da internet [BRA 97]. Ele não faz transporte de dados e atua no mesmo nível de outros protocolos como o ICMP (*Internet Control Message Protocol*), o IGMP (*Internet Group Management Protocol*) ou em alguns protocolos de roteamento como mostrado na figura 3.9 [SCH 2000] [BRA 97].

Emissores RSVP

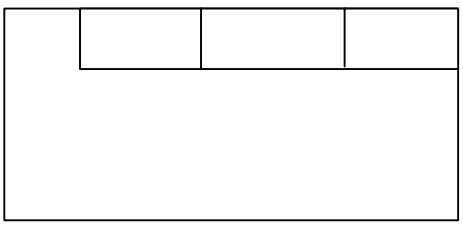

Figura 3.9 – Camada de atuação do RSVP

O gerenciamento ocorre no inicio da comunicação sendo reiniciado de tempos em tempos [BRA 97]. Cabe ao receptor a responsabilidade em fazer a requisição de QoS. RSVP requisita o receptor para responsabilizar-se pela requisição de serviços de QoS em vez do emissor [FER 99]. Imaginemos a situação onde computadores concordam em estabelecer uma sessão que tenha grandes fluxos de dados. A máquina que deve receber os dados usa mensagens de reserva para contatar cada roteador na rota reserva, até o originador dos dados e nele estabelecer a reserva de banda.

A grande vantagem é deixar essa tarefa a cargo do receptor, pois permite aos roteadores perceberem quando múltiplos receptores estão solicitando o mesmo fluxo de dados, combinando-os em transmissões multicast.

A implementação do RSVP será tipicamente executada em background, não encaminhando dados no caminho como mostra a figura 3.10 [BRA 97]

O protocolo RSVP foi desenvolvido tanto para o tráfego unicast quanto para o trafego multicast.

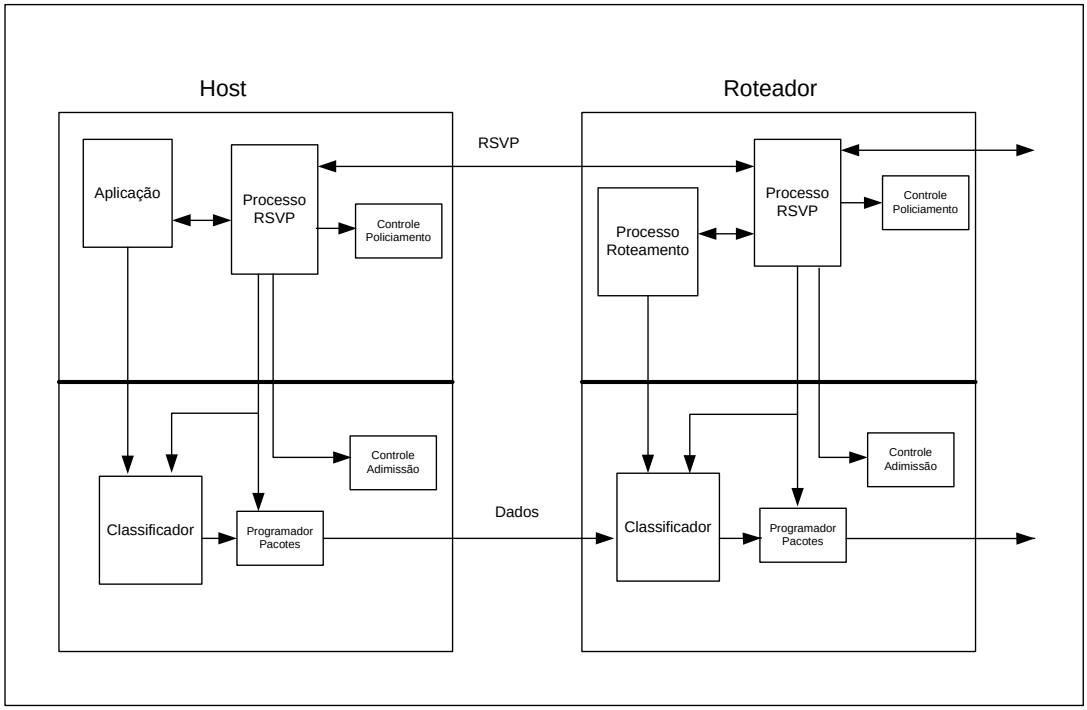

Figura 3.10 – RSVP dentro de hosts e roteadores

3.6.1 Fluxos de Dados

RSVP define uma sessão para ser um fluxo de dados com uma destinação particular e protocolo da camada de transporte [BRA 97]. O fluxo de dados é uma seqüência de datagramas que tem a mesma origem, destino e qualidade de serviço [CIS 2002b]. Requisições de QoS comunicam sem interrupção um fluxo específico.

Uma sessão RSVP é definido por três pontos principais (Endereço Destino - DestAdress, ID do protocolo - ProtocolID e Porta Destino - DSTPort) [BRA 97].

O DestAdress é o endereço destino dos pacotes de dados, que podem ser endereços multicast ou unicast, o ProtocolID é o ID do protocolo IP e o parâmetro DSTPort é o número da porta destino, que pode ser uma porta UDP ou TCP.

O protocolo RSVP define também que sessão é todo o enlace da comunicação por onde se relacionam as camadas de transporte de todos os participantes da comunicação, podendo ser unicast ou multicast [SCH 2000].

Cada sessão é tratada independentemente. Na figura 3.11 ilustra-se os pacotes de fluxo de dados em uma sessão RSVP simples [BRA 97].

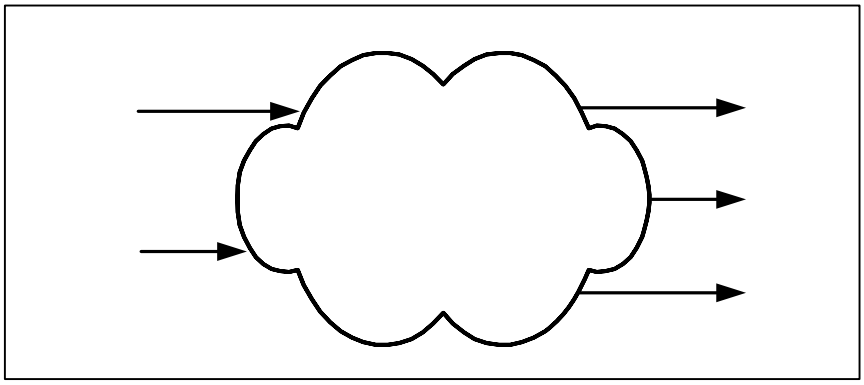

Figura 3.11 – Sessão de distribuição Multicast

A seta indica o fluxo de dados dos emissores S1 e S2 e os receptores R1, R2 e R3. A nuvem representa a malha de distribuição criada pelo roteamento multicast.

3.6.2 Estilos de reserva

Uma requisição de reserva (Resv) contém um conjunto de opções que são chamadas de estilo de reserva [FER 99].

O RSVP suporta duas classes de reserva: reservas distintas e reservas compartilhadas.

Reservas distintas instala um fluxo para cada um emissor em cada uma sessão [CIS 2002b] [BRA 97]. Reservas compartilhadas são usadas por um conjunto de emissores que não estão interferindo um com o outro. A tabela 3.1 mostra tipos de reserva RSVP distintas e compartilhadas.

Seleção do Emissor	Reservas	
	Distintas	Compartilhadas
Explicit	Fixed-filter FF	Shared-explicit SE
WildCard	Não definido	WildCard-filter WF

Tabela 3.1 – Estilos e atributos de reserva

3.6.3 Mensagens RSVP

Como o modelo RSVP é baseado na reserva de recursos, antes de se estabelecer uma conexão, como por exemplo uma transmissão de vídeo conferência, um conjunto de mensagens ou objetos RSVP, são obrigatoriamente trocadas entre a aplicação e os elementos da rede. Isto permitirá a requisição de qualidade de serviço para uma determinada sessão [BRA 97].

A mensagem RSVP possui um campo *message type* no seu cabeçalho que indica a função da mensagem [FER 99] [BRA 97]. Após a sessão ser definida mensagens de controle RSVP serão trocadas [SCH 2000]. Apesar dos sete tipos existentes de mensagem RSVP, dois são considerados fundamentais [FER 99] [SCH 2000]:

As mensagens *Resv* e mensagens *Path*, que provêem as operações básicas do RSVP.

Como já mencionado anteriormente, um emissor também conhecido como *Sender* RSVP, transmite as mensagens *Path* ao longo do caminho do trafego, provido pelo

protocolo de roteamento [FER 99]. Estas mensagens *Path* armazenam informações do caminho, em cada nó do trafego que inclui no mínimo o endereço IP de cada *previous Hop* (Phop) no caminho do trafego. O endereço IP do *Phop* é usado para determinar o caminho que subsequentemente encaminhará as mensagens *Resv* [FER 99].

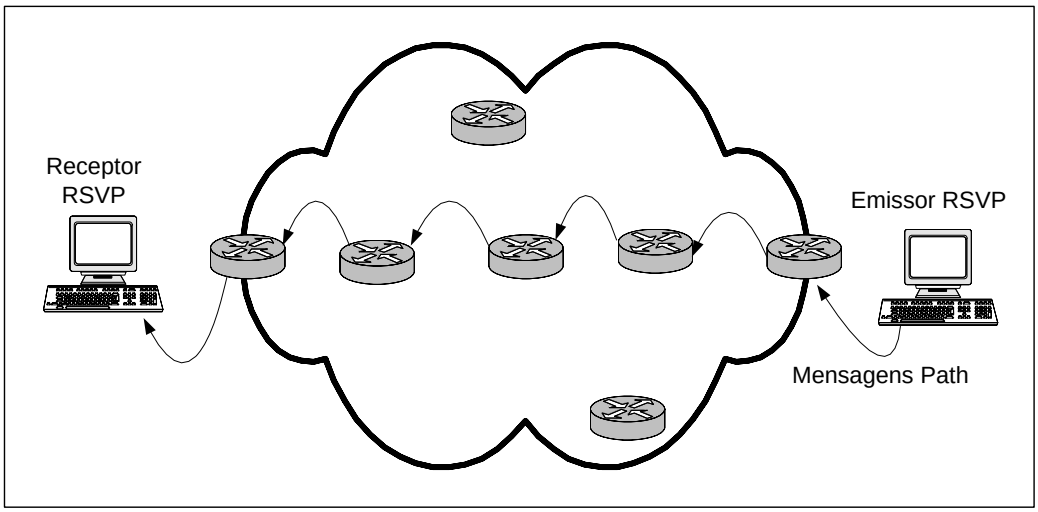

Figura 3.12 – Fluxo de uma mensagem Path

As mensagens *Resv* são geradas pelo receptor e é transportada atrás em direção ao emissor criando e mantendo estado de reserva em cada nó ao longo do caminho de trafego [FER 99].

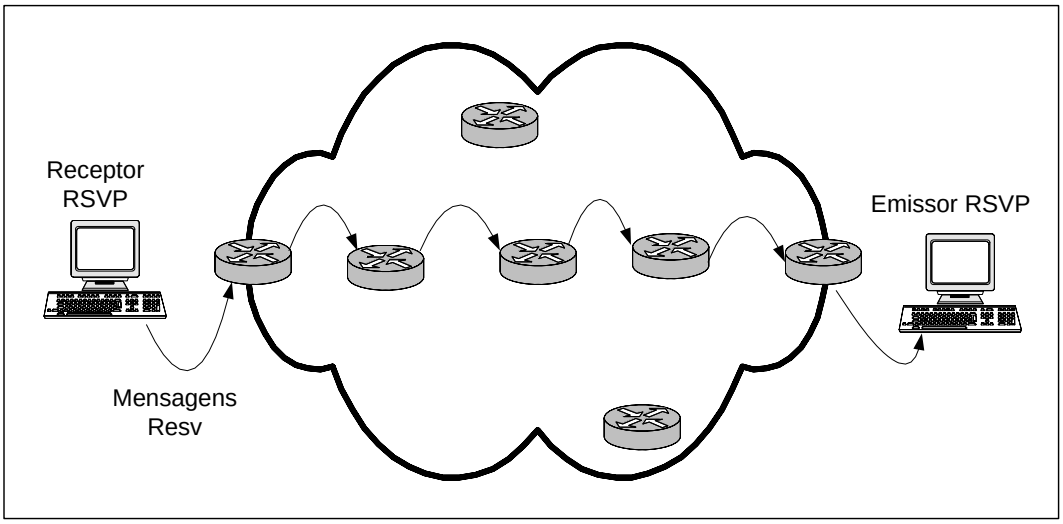

Figura 3.13 – Fluxo de trafego das mensagens Resv

A figura 3.13 mostra o modelo RSVP dentro de um roteador de núcleo. Cada fluxo de dados que chega sem interrupção de um *Previous Hop* corresponde a uma interface de entrada e parte sem interrupção para uma ou mais interfaces de saída. A mesma interface pode agir em ambos, em regras de saída e entrada para diferentes fluxos de dados em uma mesma sessão [BRA 97]. Múltiplos *Previous Hops* e *Next Hops* podem ser alcançados sem interrupção uma determinada interface física. Como exemplo a figura inclui que D e D' estão conectados para (D), com um broadcast LAN [BRA 97].

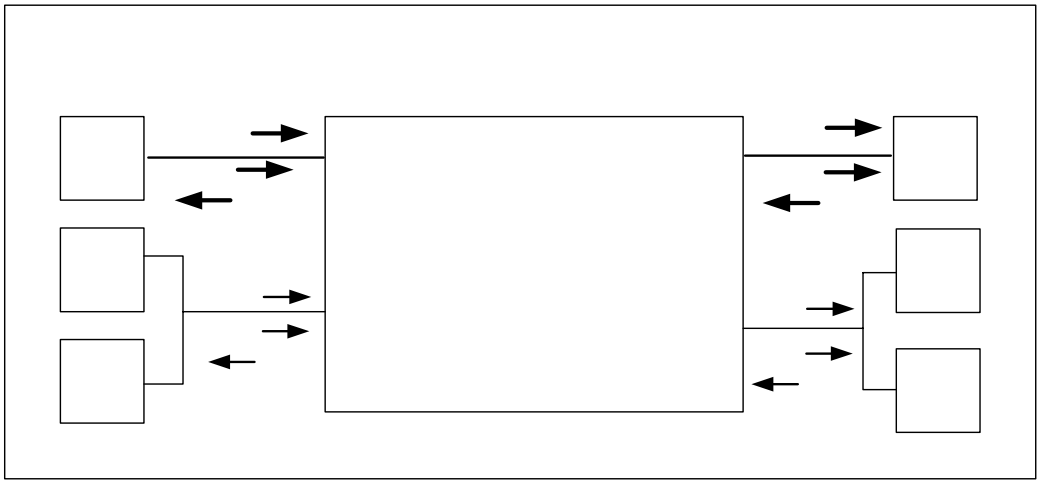

Figura 3.14 - Roteador usando RSVP

3.6.3.1 Mensagens Path

Uma mensagem *Path* possui informações adicionais para o endereço *Phop*, que caracteriza o trafego do emissor. Estas informações adicionais são elementos chamados S*ender Template*, *Tspec*, e *Adspec* [FER 99].

Uma mensagem *Path* é enviada por um emissor *Sender* e é propagada pelo caminho da rede, seja esta transmissão *Uniscat* ou *Multicast*, seguindo uma rota informada até os receptores ou *Receivers* [SCH 2000]. Qualquer elemento no caminho dos dados ao receber uma mensagem *Path* criará um estado chamado *Path State* e estas mensagens armazenam todos os caminhos ao qual percorreram [SCH 2000].

A mensagem *Path* é requisitada para atingir um S*ender Template* ou um emissor modelo, que descreve o formato do pacote de dados e do trafego de dados que o emissor irá originar [FER 99] [BRA 97]. O *Sender Template* chama informações contidas num *Filter Spec*, que identifica o emissor do fluxo de outros fluxos presentes e pode ser usado para selecionar estes emissores de pacotes em qualquer sessão RSVP de qualquer

link [FER 99] [BRA 97]. A mensagem *Path* é requisitada para conter um *SenderTspec* que caracteriza o fluxo de trafego que o emissor irá gerar [FER 99] [BRA 97].

O *Sender Template* tem que cobrar a mesma força expressiva e formatar como os *Filter Spec* aparecem nas mensagens *Resv* [BRA 97]. Por esta razão um *Sender Template* pode especificar somente o endereço IP do emissor e opcionalmente a porta TCP/UDP do emissor, e aceitar o ID do protocolo especificado para esta sessão [BRA 97].

Mensagens path podem conter fragmentos adicionais contendo um *Adspec* [FER 99] [SCH 2000]. Quando um *Adspec* recebe uma mensagem path pelo nó, isto é passado para o processo de controle de trafego local, que atualiza o *Adspec* com informações dos recurso e os passa atrás para o processo RSVP ser encaminhado para o próximo *Hop*, então a versão atualizada é encaminhada dentro da mensagem *Path* no caminho oposto, também conhecido como *DownStream* [FER 99] [BRA 97] [SCH 2000].

O *Adspec* contém informações requisitadas pelos receptores que permitem escolher um serviço de controle de QoS e determinar os parâmetros de reserva apropriados [FER 99].

O *Adspec* permite o receptor determinar se o nó tem suporte ao RSVP ou quer um serviço de controle de QoS específico [FER 99]. O Adspec prove informações padrão ou informações de serviço específico sobre cada roteador no caminho da transmissão, para que se possa caracterizar parâmetros para a classe de serviços garantidos [FER 99] [SCH 2000].

Informações podem ser geradas ou modificadas dentro da rede e usadas pelos receptores para fazer decisão de reserva [FER 99]. A informação pode incluir recursos específicos disponíveis, estimar atraso e largura de banda e vários parâmetros usados por serviços de controle de QoS específicos [FER 99]. A informação é carregada dentro do objeto *Adspec* e coletada para vários nós, como caminhos substitutos em direção dos receptores [FER 99].

A informação do *Adspec* representa um sumário acumulativo que é computado e atualizado o tempo todo [FER 99] [BRA 97]. O emissor RSVP também gera um objeto *Adspec* inicial que caracteriza as capacidades de controle deste QoS [FER 99]. Esta forma deve inicializar o ponto inicial para a acumulação de propriedades de caminho

[FER 99]. O *Adspec* é adicionado para uma mensagem *Path* criada e transmitida pelo emissor [FER 99].

Como mencionado anteriormente a informação no *Adspec* é dividida em fragmentos; cada fragmento é associado com um serviço de controle específico. Isto permite ao *Adspec* alcançar informações sobre múltiplos serviços e permite a adição de novas classes de serviço no futuro, fora modificações para os mecanismos de transporte usados por eles [FER 99]. O tamanho do *Adspec* depende do número e do tamanho dos fragmentos *Per-Service* individuais incluídos, tanto a presença de parâmetros fora do padrão [FER 99]. Em cada nó o *Adspec* é passado de processo RSVP para o modulo de controle de trafego. O processo de controle de trafego atualiza o *Adspec* por identificar o serviço específico dentro do *Adspec* e chama cada processo para atualizar esta porção identificada de *Adspec* como necessário [FER 99]. Se o processo de controle de trafego descobrir um serviço de QoS especificado dentro do *Adspec* que não é suportado pelo nó, uma flag é marcada reportando este ao receptor [FER 99].

3.6.3.2 Mensagens formato Resv

A mensagem Resv contém informações sobre o estilo de reserva. A atribuição do objeto *Flowspec* e o *FilterSpec* que identifica qual é o emissor [FER 99]. O par de *FlowSpec* e *Filter Spec* é originado como *Flow Descriptor* [FER 99]. A mensagem *Resv* que é enviada por um receptor possui um descritor de fluxo que define e aceita o QoS daquela mensagem *Path* [BRA 97] [SCH 2000]. O *FlowSpec* é usado para marcar parâmetros dentro de um processo de programação de pacotes de um nó, e o *Filter Spec* é usado para marcar parâmetros num processo classificador de pacotes [FER 99]. Dados que não estão igualando qualquer tipo de *Filter Spec* é tratado como trafego de melhor esforço [FER 99] [BRA 97].

Mensagens *Resv* são enviadas periodicamente para manter o estado de reserva ao longo de um caminho de trafego particular [FER 99]. Isto se refere ao *Soft State*, porque o estado de reserva é mantido pelo uso da renovação periódica destas mensagens [FER 99].

Vários bits de informações devem ser comunicadas entre o receptor e o nó intermediário para atribuir chamada de serviço de controle de QoS [FER 99] [BRA 97]. Dentre os tipos de dados que são necessários para serem comunicados entre aplicações e nós, é a informação gerada por cada receptor que descreve o desejo de serviço de

controle de QoS, uma descrição do fluxo de trafego para qual a reserva de recurso devia aplicar (*Receiver Tspec*), e os parâmetros necessários requeridos para chamar o serviço de QoS (*Receiver Respec).* Esta informação esta contida dentro do *FlowSpec* (especificação de fluxo) objeto mensageiro dentro da mensagem *Resv* [FER 99]. A informação contida dentro do objeto *FlowSpec* pode ser modificada pelo nó intermediário no caminho do trafego por fundir a reserva e outros fatores [FER 99].

Uma mensagem *Resv* é requisitada para alcançar um emissor *TSpec*, que define quais as características de trafego do fluxo de dados que o emissor irá gerar. Este *Tspec* é usado pelo controle de tráfego para efetuar um excesso de reserva e possibilitar desnecessariamente falhas no controle de admissão [BRA 97].

O formato do *FlowSpec* é diferente dependendo de que o emissor esta requisitando carga controlada ou serviço garantido. Quando um receptor requisita serviço de carga controlada, somente um *TSpec* esta contido dentro do *FlowSpec*, quando requisita-se serviços garantidos, ambos um *TSpec* e um *RSpec* estão contidos dentro do objeto *FlowSpec* [FER 99].

Na versão 1 do RSVP, todos os receptores em particular uma sessão RSVP estão requisitados para escolher qualquer serviço de controle de QoS [FER 99] [BRA 97].

3.6.3.3 Mensagens Adicionais

Ao lado das mensagens *Resv* e *Path*, existem outros tipos de mensagens RSVP e erros de reserva (*Patherr e Resverr*) caminho de reserva (*PathTear e ResvTear*) e confirmação para um requisito de reserva (*Resvconf*) [FER 99].

As mensagens *Patherr* e *Resverr* simplesmente são enviadas no caminho original também conhecido como *Upstream* para o emissor que criou o erro e não modificou o estado de caminho dentro do nó sem interrupção que eles passam [FER 99]. Uma mensagem *Patherr* indica um erro de processamento de mensagens *Path* enviadas através do emissor [FER 99] [BRA 97]. Mensagens *Resverr* indicam um erro de processamento de mensagens *Resv* e são enviadas para o receptor [FER 99].

Mensagens *Teardown* removem caminho ou estado de reserva de nós como logo eles estão recebidos [FER 99]. Uma mensagem *Resvconf* indica cada nó no caminho de transito que recebe uma mensagem *Resv* contendo um objeto de confirmação de reserva [FER 99] [BRA 97]. Quando um receptor quer obter uma confirmação para requisitar uma determinada reserva, pode incluir uma confirmação de requisição ou *Resc confirm*

objeto dentro da mensagem *Resv* [FER 99]. Uma requisição de reserva com um grande *Flowspec* para qualquer lugar, normalmente resulta numa mensagem *Resverr* ou *Resvconf* iniciando a geração e envio atrás do receptor [FER 99]. Deste modo a mensagem *Resvconf* confirma a reserva fim a fim [FER 99] [BRA 97].

3.7 Resumo do Capítulo

Neste capítulo, são apresentados os principais métodos existentes de enfileiramento e policiamento de tráfego. Também, são definidos os conceitos relacionados à arquitetura do modelo de serviços integrados, é discutido em detalhes as duas classes de serviços que são os serviços garantidos e os serviços de carga controlada. São apresentados os conceitos referentes ao protocolo de reserva de recursos, o RSVP, e sobre as mensagens Path e Resv e das demais mensagens adicionais.

4. VÍDEO CONFERÊNCIA E QOS

Como já foi visto anteriormente neste trabalho, a evolução das redes de computadores, nos traz um novo cenário, onde a viabilidade para o desenvolvimento de aplicações avançadas como vídeo conferência, é uma realidade. A vídeo conferência é uma forma de comunicação que permite uma interatividade total entre as partes, que podem ser pessoas ou grupo de pessoas. Através dos recursos que as tecnologias de vídeo conferência nos oferecem, pode-se realizar reuniões, palestras, aulas e discussões com grupos de pessoas que podem estar dispostas remotamente, independentemente da localização geográfica. A vídeo conferência de forma básica consiste na transmissão de vídeo e voz, entre pontos separados fisicamente.

Existe uma variedade de soluções de vídeo conferência, cada uma com requisitos específicos quanto às necessidades de comunicação e qualidade de serviços. Neste trabalho estudaremos os modelos e protocolos de vídeo conferência para rede IP, também conhecidas como vídeo conferência por pacotes.

Os modelos de vídeo conferência são divididos em: modelo centralizado, modelo descentralizado e híbrido [LEO 2001a].

4.1 Modelos de comunicação para vídeo conferência

4.1.1 Modelo Centralizado

Este modelo se baseia-se na comunicação ponto à ponto, também conhecida como comunicação unicast, onde a comunicação se dá entre dois pontos, uma origem e um destino. Para que uma comunicação se estabeleça neste modelo, utilizando-se mais de dois pontos, é necessário a utilização de um MCU – *Multipoint Control Unit*, que tem a função de fazer o controle da comunicação multiponto. Desta forma as conexões são efetuadas ao MCU, que tem a função de fazer o gerenciamento da sessão de vídeo conferência através do protocolo H.245, que faz parte do padrão H.323 [LEO 2001a].

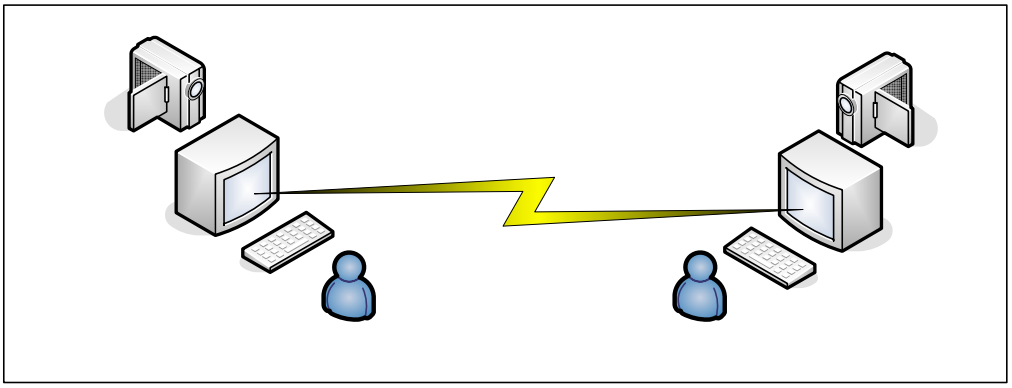

Figura 4.1 – Transmissão simples de vídeo conferência - Unicast

Como mostrado na figura acima uma conexão simples de uma sessão de vídeo conferência entre dois pontos distantes, como já citado esta conexão é conhecida com Unicast.

No desenho 4.2, visualizamos uma conexão de vídeo conferência entre vários pontos, utilizando um MCU para o gerenciamento das sessões.

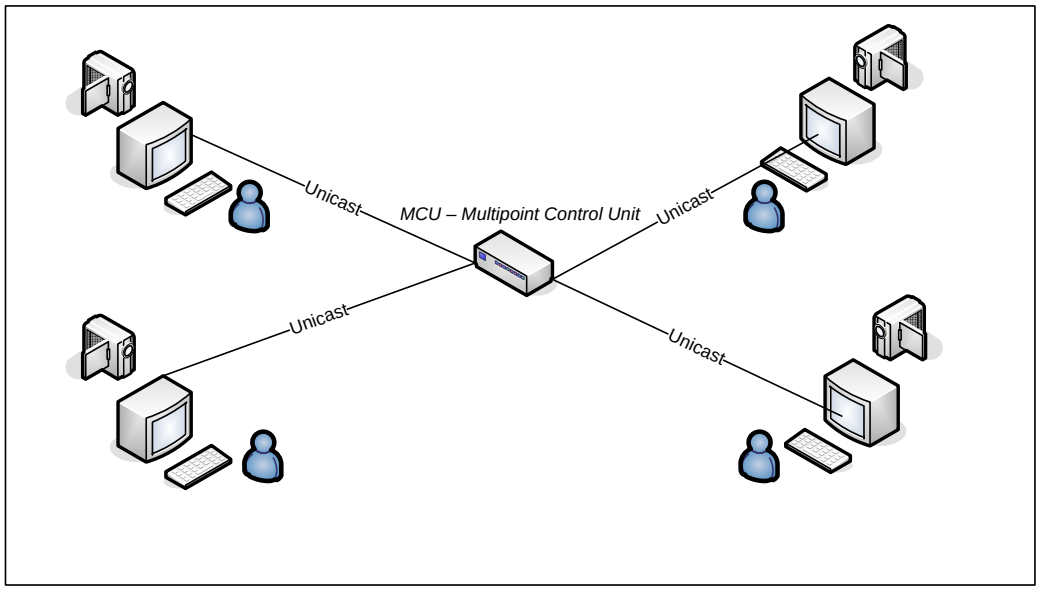

Figura 4.2 – Transmissão através de MCU

Pode-se destacar vantagens e desvantagens sobre este modelo.

Vantagens:

- *Economia de recurso das estações, pois o gerenciamento é feito pelo MCU;*

- *Não requisita estrutura especial de rede, pois as conexões entre os equipamentos são ponto a ponto. [LEO 2001 a]*

Desvantagens:

- *A MCU normalmente custa caro;*
- *Gera mais tráfego na rede. [LEO 2001 a]*

4.1.2 Modelo Descentralizado

No modelo descentralizado as características de controle são as mesmas do modelo centralizado, mas o controle do fluxo é feito de forma diferente [LEO 2001 a]. O controlador multiponto é responsável em fazer o controle de três ou mais participantes durante uma sessão. No modelo centralizado o MCU fica responsável pelo processamento do fluxo, já no modelo descentralizado os fluxos são enviados por todos fim a fim. O controlador de multiponto é muito importante neste modelo, pois é ele que é responsável pela interligação dos pontos, e é colocado como um dos pontos. Os próprios participantes ou pontos ficam responsáveis pela mesclagem de áudio e vídeo [LEO 2001 a]. Este trafego pode ser feito por multicast, ou até mesmo através de vários fluxos unicast. Na figura 4.3 pode-se observar melhor as características deste modelo.

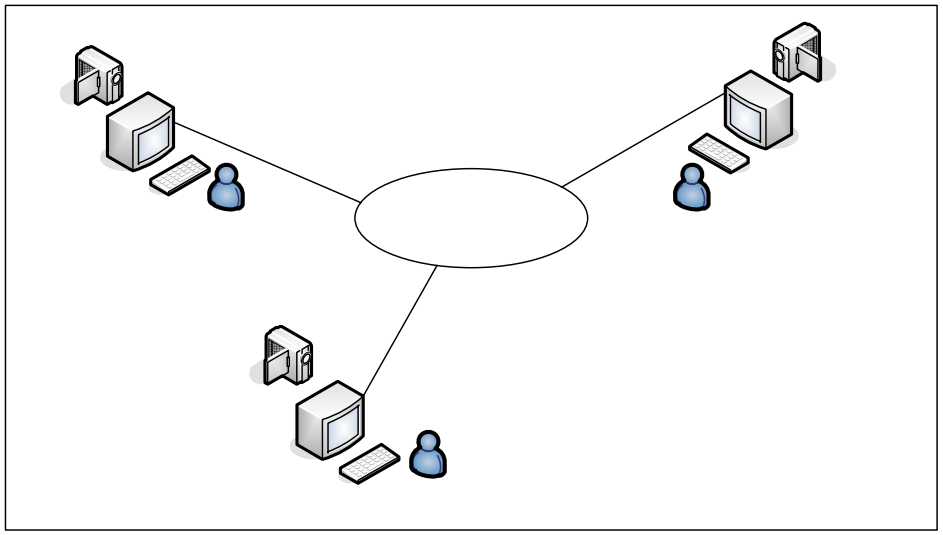

Figura 4.3 – Modelo de vídeo conferência descentralizado

Como vantagens pode-se destacar:

- *Não existe a necessidade de um MCU;*
- *Permite um processamento individualizado de cada participante;*

- *Permite o uso de tráfego multicast, economizando recursos de rede. [LEO 2001a].*

As desvantagens:

- *O controlador de multiponto é obrigado a estar ativo durante toda a transmissão;*
- *Como o controle do fluxo é feito por cada participante, uma maquina com pouca capacidade de processamento, pode ser prejudicada. [LEO 2001a]*

4.1.3 Modelo Híbrido

No modelo hibrido existe uma mesclagem do que há de melhor dos dois modelos apresentados anteriormente. O modelo hibrido pode funcionar numa rede multicast, fazer a distribuição do fluxo como no modelo descentralizado, possuir um servidor, por exemplo, para fazer o controle de documentos compartilhados [LEO 2001a].

O modelo híbrido prove o armazenamento centralizado para as sessões sem a necessidade de controlar a cada instante a aplicação dos participantes de uma sessão de vídeo conferência [LEO 2001a].

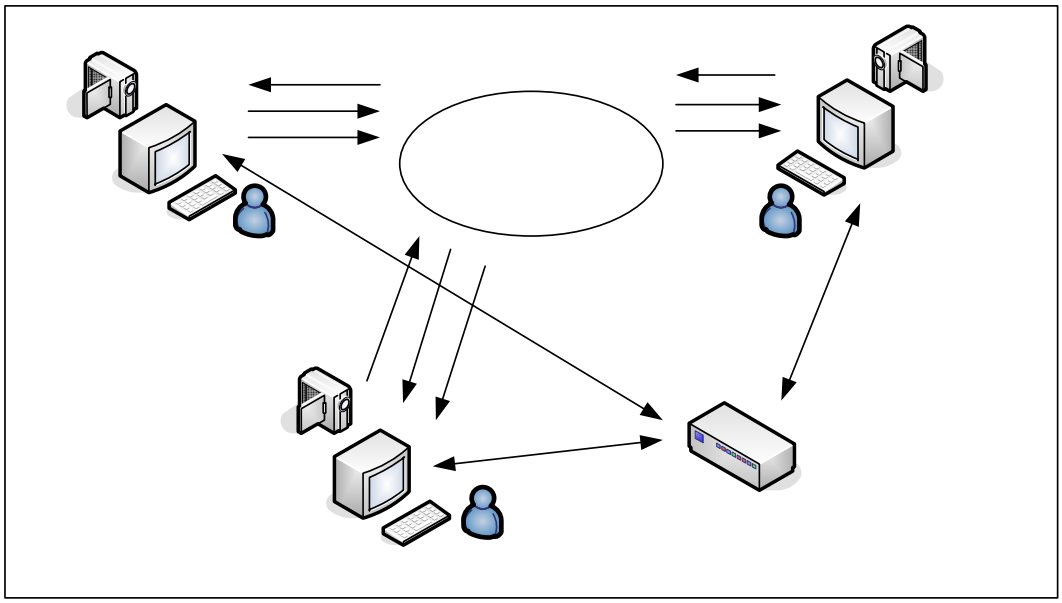

Figura 4.4 – Modelo de vídeo conferência descentralizado

4.2 Padrão H323

O padrão H323 é uma tecnologia de base com o objetivo de especificar sistemas multimídia em redes IP [LEO 2001b]. O padrão especifica o uso de áudio, vídeo e dados nas comunicações multimídia, com uma variedade de formas de comunicação, envolvendo apenas áudio, como telefonia IP, e áudio e vídeo, como sistemas de vídeo conferência [LEO 2001b]. O padrão H323 é o utilizado, pelas ferramentas de vídeo conferência utilizadas neste trabalho.

O padrão especifica quatro tipos de componentes:

- *Terminais – São computadores utilizados na rede, ou até mesmo telefones IP, e estes terminais devem suportar, no mínimo áudio;*
- *Gateway – São objetos que provêem a interoperabilidade do padrão H323 com outros padrões existentes de comunicação multimídia;*
- *Gatekeepers – É o ponto central de todas as chamadas, fazendo o controle das chamadas e o gerenciamento da largura de banda;*
- *MCU – São objetos que permitem a interconexão de três ou mais participantes [LEO 2001b].*

O padrão utiliza funcionalidades de chamadas de sinalização e controle, que são [QUI 2003]:

- *H.323 – Sistema de comunicação multimídia baseada em pacotes;*
- *H.225 – Protocolo de controle de chamada;*
- *H.235 – Segurança;*
- *H.245 – Protocolo de controle de mídia;*
- *Q.931- Sinalização de assinante digital;*
- *H.450.1- Protocolo de funções genéricas [QUI 2003].*

4.3 Resumo do Capítulo

Neste capítulo, foram apresentados os conceitos sobre vídeo conferência, os modelos e tipos existentes. Também é discutido sobre o padrão H323 que especifica as comunicações multimídia no protocolo IP.

5. RESULTADOS EXPERIMENTAIS

Com o objetivo de avaliar a arquitetura de serviços integrados para prover QoS em aplicações de vídeo conferência, vários experimentos foram realizados e divididos basicamente em 2 etapas.

Na primeira etapa foi realizada uma análise quantitativa que avaliou, em um ambiente real, composto por roteadores Cisco, a necessidade de usar técnicas de qualidade de serviço, comprovando que em redes congestionadas quando não se possui controle sobre o atraso, variação do atraso e perda de pacotes a qualidade de transmissão fica comprometida.

Na segunda etapa foi simulado um tráfego real de vídeo conferência com fluxos de áudio e vídeo entre duas redes locais interconectadas por um canal de 1 Mbps. Nesta etapa foram aplicadas as configurações de RSVP necessárias para a priorização dos pacotes.

5.1 Etapa 1

Nesta etapa, o objetivo principal foi avaliar a vazão e o tempo de resposta fim a fim em redes com congestionamento e sem congestionamento. Para a execução das análises realizadas nesta etapa de experimentos, foi montada uma estrutura de rede conforme a figura 5.1. A arquitetura montada é composta por dois roteadores Cisco 2511, quatro estações de trabalho, onde duas trocavam tráfego para congestionar o canal e as outras duas trocavam tráfego para realizar as medições, com uma conexão WAN entre os roteadores de 1 Mbps.

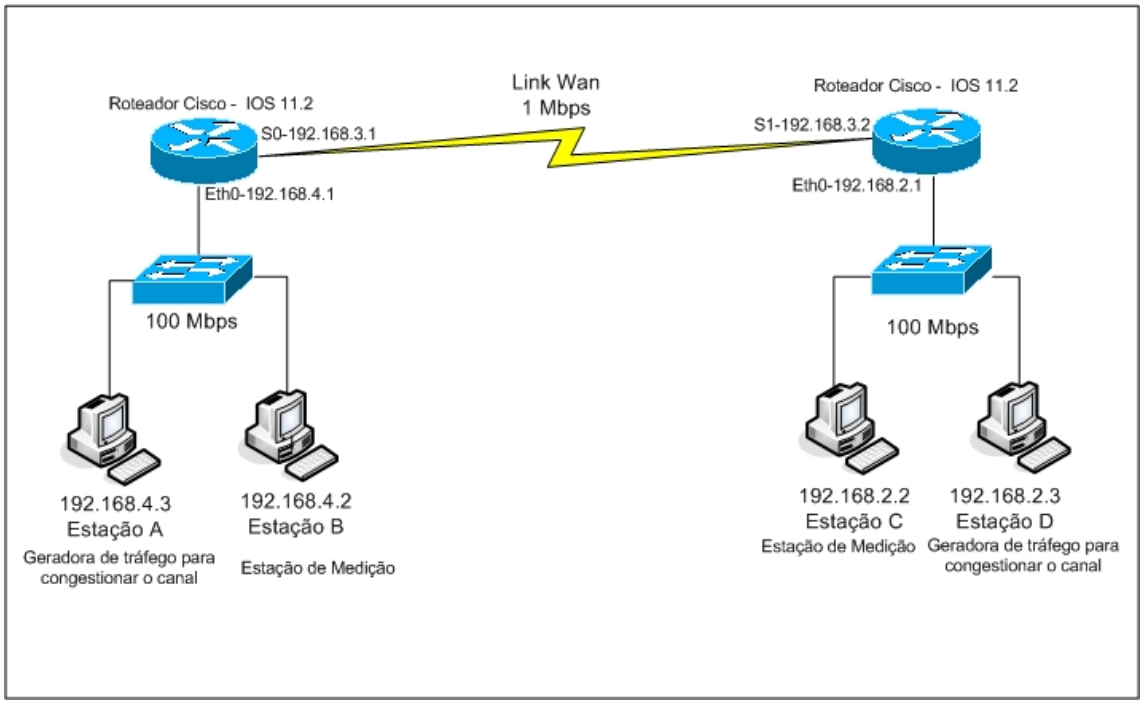

Figura 5.1 – Arquitetura da Etapa 1 dos experimentos

Como ilustrado na figura 5.1, as estações A e B estão conectadas entre si através de um switch Fast-ethernet, assim como as estações C e D também conectadas entre si através de um switch Fast-ethernet. As duas redes locais se conectam através de um canal WAN de 1 Mbps. As estações A, B e D possuíam sistema operacional Windows XP e a estação C, sistema operacional Windows 2000. Todas as estações possuem 1 placa de rede Fast-ethernet de 100 Mbps.

Foi utilizada a ferramenta Qcheck [IXI 2004] para medir a vazão da rede com os protocolos TCP e UDP e o tempo de resposta fim a fim, com a ida e a volta dos pacotes da origem ao destino, usando o protocolo TCP e UDP. A ferramenta Qcheck [IXI 2004] estava instalada na máquina B e C, e as duas eram responsáveis pela troca de pacotes e a realização das medições. Portanto as medições foram realizadas entre as estações B e C. Na seqüência com o mesmo ambiente, foi utilizado o software PCATTCP [DIV 2003] e MGEN [NAV 2004] para congestionar o canal. Com o PCATTCP [DIV 2003] foram gerados fluxos TCP que utilizaram 85 % do canal, com o MGEN [NAV 2004] foram gerados fluxos UDP que utilizaram 15 % do canal. Estes fluxos TCP e UDP foram utilizados para congestionar o canal, pois se entende que melhor representa a situação real de uma rede congestionada. Desta forma com o canal congestionado os

experimentos com o Qcheck foram refeitos para analisar os resultados agora com o estado de uma rede congestionada.

5.1.1 Resultados da etapa 1

A primeira avaliação feita na etapa 1 dos experimentos foi a vazão TCP em uma rede sem congestionamento, para isso foi utilizada a ferramenta Qcheck [IXI 2004].

Na figura 5.2 é apresentado como exemplo, o log gerado pela ferramenta, onde podemos constatar que o resultado da vazão da rede com o protocolo TCP atingiu 951,702 Kbps, sendo totalmente compatível com o ambiente montado.

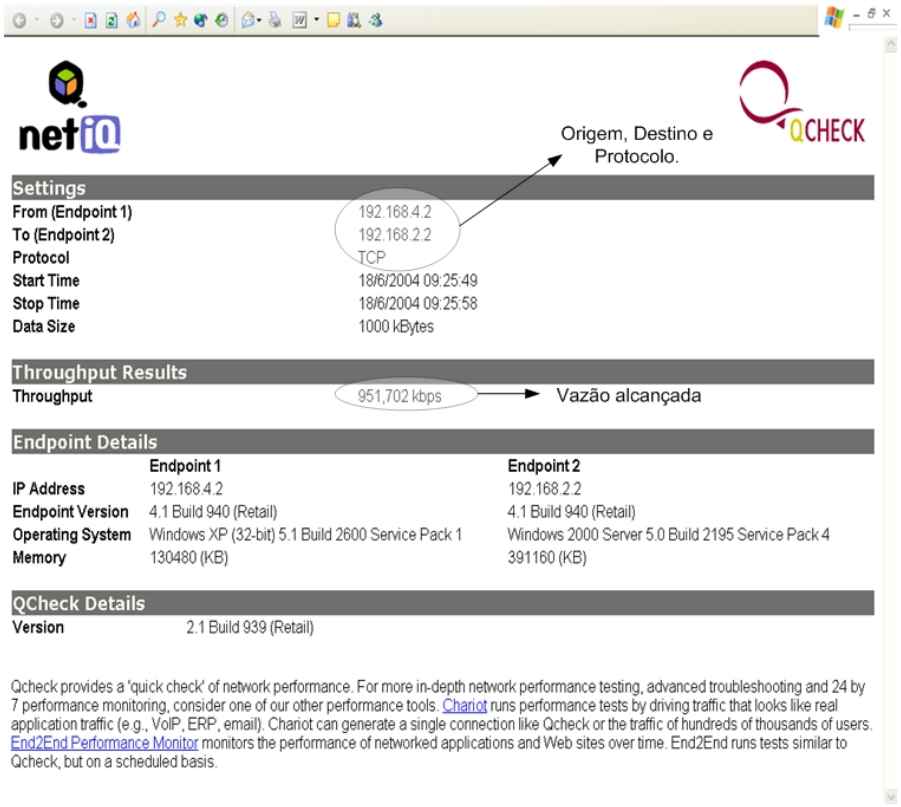

Figura 5.2 – Log da ferramenta Qcheck

Na seqüência foi gerado um tráfego em background com objetivo de congestionar o canal, e avaliar o comportamento em uma rede congestionada. Neste momento pode-se observar que a vazão em um estado de rede congestionada alcançou 499 Kbps, tendo uma diferença significativa ao comparado com a rede sem congestionamento.

Para uma comparação um pouco mais detalhada, foi executado o teste de vazão do protocolo UDP, desta vez num estado de rede sem congestionamento. Obteve-se uma vazão 909,919 Kbps. Na seqüência como realizado anteriormente com o protocolo TCP, foi gerado tráfego em background para congestionar o canal e realizar a análise da vazão UDP num estado de rede com congestionamento. Foi observado que a vazão usando o protocolo UDP numa rede com congestionamento, foi de 155,192 Kbps, desta forma é fácil concluir que as aplicações multimídia, como a vídeo conferência que normalmente usam o protocolo UDP, e tem fluxos que consomem de 256 Kbps a 512 Kbps de banda, possuem problemas sérios em rodar em redes com congestionamento.

Uma nova avaliação foi efetuada com a ferramenta Qcheck, avaliando desta vez o tempo de resposta com o protocolo TCP, no estado da rede sem congestionamento. Neste experimento pode-se constatar que o tempo médio de resposta é de 13 ms, quando utilizado o protocolo TCP.

Na seqüência como já feito anteriormente foi gerado tráfego em background para congestionar o canal, e analisar os tempos de resposta com o protocolo TCP e rede congestionada. Foi observado que o tempo de resposta médio aumentou consideravelmente para 321 ms.

A mesma análise de tempo de resposta foi feita analisando o protocolo UDP. O tempo de resposta com o protocolo UDP numa rede sem congestionamento, também demonstrando um tempo médio de 13 ms, a exemplo da análise com o protocolo TCP.

Na seqüência, foi gerado tráfego em background para congestionar o canal, e analisar o tempo de resposta com o protocolo UDP em redes com congestionamento. Pode-se observar um tempo de resposta médio de 378 ms.

Na tabela 5.1 pode-se observar uma síntese e uma comparação quantitativa em todos os estágios do experimento com a ferramenta QCHECK.

Tipo de experimento	Tráfego	Estado da rede
Vazão TCP	951,702 Kbps	Sem congestionamento
Vazão TCP	499 Kbps	Com congestionamento
Vazão UDP	909,910 Kbps	Sem congestionamento
Vazão UDP	155,192 Kbps	Com congestionamento
Atraso Médio TCP	13 ms	Sem congestionamento
Atraso Médio TCP	321 ms	Com congestionamento
Atraso Médio UDP	13 ms	Sem congestionamento
Atraso Médio UDP	378 ms	Com congestionamento

Tabela 5.1 – Resultado dos experimentos com Qcheck

5.2 Etapa 2

Na etapa 2, o objetivo era realizar medições mais apuradas que pudessem expressar melhor as transmissões de vídeo conferência. Foram realizadas sessões reais de vídeo conferência ponto a ponto para conhecer as características do tráfego de vídeo conferência. Para isso foi utilizado o equipamento de vídeo conferência ViewStation FX do fabricante Polycom [POL 2004]. Foram realizadas sessões de vídeo conferência IP com o equipamento [POL 2004] nas velocidades de 128 Kbps, 256 Kbps e 384 Kbps. Percebeu-se que na velocidade 384 Kbps, a qualidade de vídeo se mostrou superior às demais. Devido a este fato, tanto a sessão realizada com o equipamento de vídeo conferência como as simulações foram realizadas com um tráfego de 384 Kbps. O equipamento utilizado, assim como a maioria dos produtos de mercado para vídeo conferência, utiliza o padrão H.323, que tem como característica utilizar um fluxo de áudio e outro fluxo de vídeo.

Através do software de gerência do equipamento e o auxilio de uma ferramenta de *Sniffer* [ASS 2004], observou-se que as transmissões possuíam fluxos de áudio no protocolo G.722 e fluxos de vídeo no protocolo H.263. O tamanho dos pacotes de áudio ficou na média de 280 bytes e os de vídeo na média de 1024 bytes. As figuras 5.3 e 5.4 mostram o diagnóstico da sessão de vídeo conferência realizada.

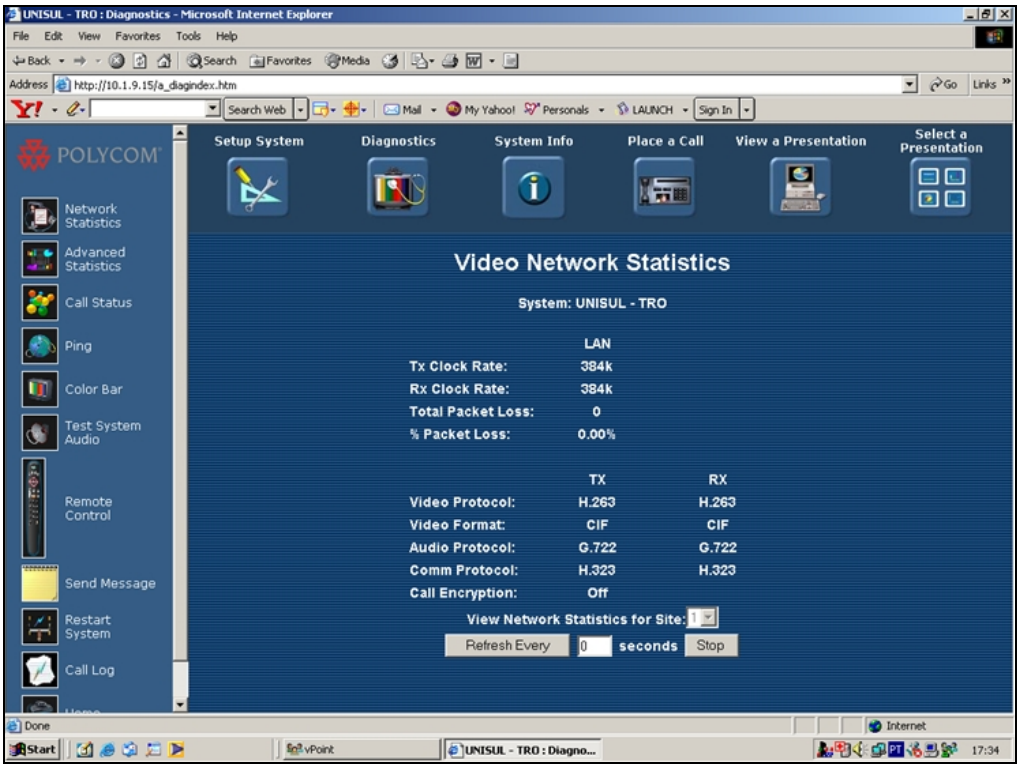

Figura 5.3 – Estatísticas de rede da vídeo conferência

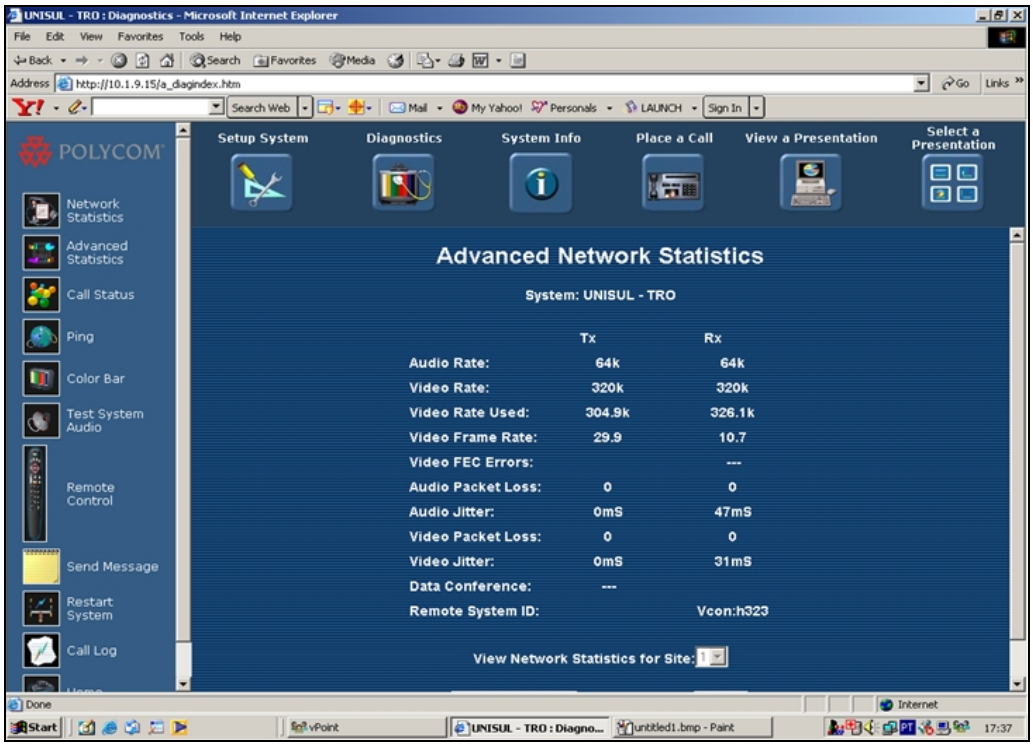

Figura 5.4 – Estatísticas avançadas de rede da vídeo conferência

Após conhecer as características do tráfego de vídeo conferência, foi realizada uma medição com a ferramenta MGEN [NAV 2004], foram utilizadas como base as características a seguir:

Porta Origem	Porta Destino	Tipo de Fluxo	Banda	Tamanho dos pacotes
5001	5010	Vídeo	320 Kbps	1024 bytes
5002	5011	Áudio	64 Kbps	280 bytes

Tabela 5.2 – Características das medições com MGEN

Os valores expressos na tabela acima, representam os resultados das características de tráfego de vídeo conferencia.

Para a realização desta medição foi utilizado o laboratório mostrado na figura 5.5.

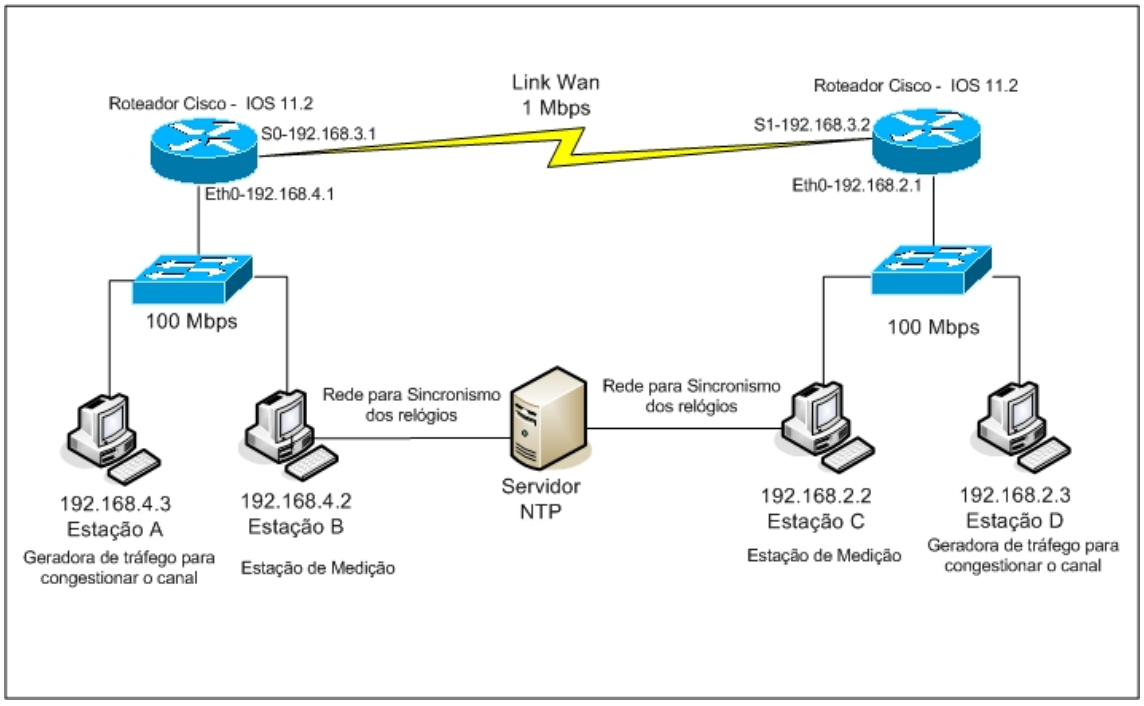

Figura 5.5 – Arquitetura do primeiro ambiente da segunda etapa de experimento

O ambiente é composto por dois roteadores Cisco 1760, com IOS versão 12.3, conectados entre si através de um canal WAN de 1 Mbps. Desta forma o ambiente fica disposto com duas redes locais interligadas através destes roteadores. A primeira rede esta composta de duas estações de trabalho. A Estação A responsável em gerar tráfego

para congestionar o canal e a estação B responsável pela realização das medições com a ferramenta MGEN. A segunda rede esta composta de duas estações de trabalho. A estação C responsável em fazer as medições em conjunto com a estação B e a estação D responsável pelo tráfego de congestionamento do canal com a estação A. Ambas as estações de trabalho possuem sistema operacional Windows. Como as medições são realizadas em um sentido, *one way*, o sincronismo dos relógios das estações responsáveis pelas medições é primordial. Para isso existe uma rede paralela de sincronismo com um servidor de NTP exclusivo para o serviço.

O resultado obtido com a ferramenta MGEN não foi satisfatório, existindo em alguns casos situações onde o atraso dos pacotes era negativo. Desta forma concluiu-se que o sincronismo dos relógios e a precisão da ferramenta de medição eram fatores críticos de sucesso. Para continuação dos experimentos foi selecionada uma nova ferramenta de medição, chamada Rude & Crude [LAN 2002]. A razão da escolha da ferramenta foi o fato de possibilitar a geração do arquivo de log sem decodificação imediata dos dados, deixando esta decodificação para o momento de análise dos dados, isto reduz o processamento e influência na precisão.

Os experimentos foram refeitos, desta vez com a ferramenta Rude & Crude, utilizando o mesmo ambiente descrito na figura 5.5, porém com as estações B e C, rodando em sistema operacional Linux. Os resultados obtidos foram compatíveis com os encontrados com a ferramenta MGEN, reforçando o fato de que o sincronismo dos relógios é um fator crítico para a realização de medições em um único sentido. Desta forma buscou-se preparar um ambiente de medições onde a máquina que enviasse o pacote fosse a mesma a recebê-lo, como descrito na figura 5.6.

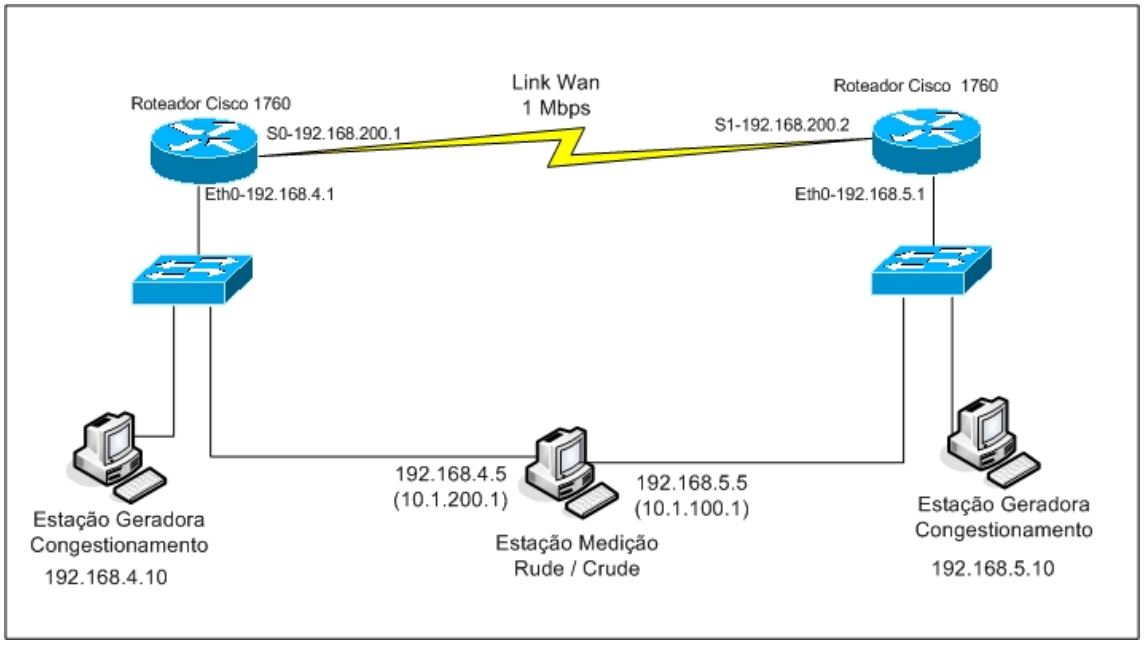

Figura 5.6 – Arquitetura do segundo ambiente da etapa dois de experimentos

O ambiente é composto por dois roteadores Cisco 1760, com IOS versão 12.3, interconectados através de um canal WAN de 1 Mbps. Para que o sincronismo dos relógios não fosse um fator problemático na estrutura, fez-se necessário que a estação que envia e recebe os pacotes de medição fosse a mesma. Desta maneira o sincronismo dos relógios não seria necessário. Como a estação que envia é a mesma que recebe os pacotes, as métricas de roteamento indicam que o pacote deve ser enviado diretamente para a outra interface de rede, criando ai uma situação inconveniente para a medição. Para resolver este problema fez-se necessário um método que permitisse que os pacotes enviados através da interface de origem, fossem encaminhados pelo roteador através do canal de 1Mbps para o outro roteador, onde então fossem encaminhados para a interface de rede de destino e que pudessem também retornar desta interface e seguir o mesmo caminho até a origem. Este método foi implementado através do serviço de NAT (*Network Address Translation*) configurando os roteadores para traduzir o endereço local como 192.168.4.5 num endereço pertencente a outra rede IP 10.1.200.1, e 192.169.5.5 em 10.1.100.1, e também aplicando rotas estáticas para o encaminhamento do pacote seguir corretamente para o *gateway* respectivo. Na tabela 5.3 pode-se observar a configuração de NAT realizada no roteador da rede 192.168.4.0, e na tabela 5.3 pode-se observar a configuração de NAT do roteador da rede 192.168.5.0.

```
!
ip nat inside source static 192.168.4.5 10.1.200.1
ip classless
ip route 0.0.0.0 0.0.0.0 Serial1/0
ip route 10.1.100.0 255.255.255.0 Serial1/0
no ip http server
ip rsvp reservation 192.168.4.5 192.168.5.5 UDP 5010 5001 192.168.4.5 FastEthernet0/0 FF RATE 420 10
ip rsvp reservation 192.168.4.5 192.168.5.5 UDP 5011 5002 192.168.4.5 FastEthernet0/0 FF RATE 84 10
!
```

Tabela 5.3 – Configuração de NAT do roteador da rede 192.168.4.0

```
!
ip nat inside source static 192.168.5.5 10.1.100.1
ip classless
ip route 0.0.0.0 0.0.0.0 Serial1/0
ip route 10.1.200.0 255.255.255.0 Serial1/0
no ip http server
ip rsvp sender 192.168.4.5 192.168.5.5 UDP 5010 5001 192.168.5.5 FastEthernet0/0 420 10
ip rsvp sender 192.168.4.5 192.168.5.5 UDP 5011 5002 192.168.5.5 FastEthernet0/0 84 10
!
```

Tabela 5.4 – Configuração de NAT do roteador da rede 192.168.5.0

O ambiente também foi composto por outras duas estações de trabalho que tinham como objetivo a troca de tráfego para congestionar o canal. Os experimentos foram realizados com as seguintes características:

Porta Origem	Porta Destino	Tipo de Fluxo	Banda	Pacotes	Reserva
5001	5010	Vídeo	320 Kbps	1024 bytes	420 Kbps
5002	5011	Áudio	64 Kbps	280 bytes	84 Kbps

Tabela 5.5 – Características das medições com Rude & Crude

Foram realizadas três tipos de medição com o Rude & Crude [LAN 2002], todas as medições avaliaram o atraso, a variação do atraso e a perda de pacotes. No primeiro experimento a rede estava sem congestionamento, no segundo a rede estava congestionada, e no terceiro a rede estava congestionada, porém com políticas de QoS aplicadas. Os experimentos desta vez tiveram os resultados condizentes com a realidade. O resultados serão apresentado no capítulo 5.2.2.

5.2.1 Política de RSVP aplicada

A definição das políticas de QoS inclui a identificação e conhecimento de perfis de fluxo de tráfego e a alocação de largura de banda necessária para cada tipo de perfil. No modelo de serviços integrados como já visto anteriormente, existem dois tipos de classes de serviço, os serviços garantidos e os serviços de carga controlada. A versão do IOS utilizado permitia tanto a configuração dos serviços de carga controlada quanto os serviços garantidos. Com os fluxos utilizados, simulando transmissões de vídeo conferência, os limites são rígidos em termos de atraso de enfileiramento e requerem uma taxa de transmissão garantida. Desta forma nos experimentos realizados optou-se em utilizar os serviços garantidos por se adaptar melhor aos requisitos dos fluxos de tráfego utilizados nos experimentos. O RSVP permite aos sistemas finais requisitar garantias de QoS para a rede, sendo que a necessidade da rede de reservar recursos difere muito do tipo de fluxo de tráfego. O RSVP trabalha em conjunto com o *weighted fair queueinf* (WFQ) ou com o *random early detection* (RED), este conjunto de parâmetros de reserva com enfileiramento de pacotes, usa dois conceitos chave: Fluxos fim a fim com o RSVP e conversações de roteador para roteador com o WFQ. Por padrão em roteadores cisco, o RSVP vem desabilitado, e é necessário que o IOS, suporte os comandos RSVP.

Para habilitar o RSVP em uma interface IP, é necessário utilizar o seguinte comando:

Comando	Propósito
Ip rsvp bandwidth [interface-kbps] [single-flow-kbps]	Habilitar o RSVP para uma determinada interface IP

Tabela 5.6 – Comandos RSVP

Por padrão a largura de banda máxima é 75 % de uma interface.

Nos experimentos realizados como as aplicações não possuíam as características do protocolo RSVP, não conseguindo desta forma enviar as mensagens PATH pode-se configurar o roteador para comporta-se como o responsável pelo envio das mensagens PATH. Para configurar um roteador como emissor das mensagens PATH, o chamado *sender* utiliza-se o seguinte comando:

Comando	Propósito
ip rsvp sender session-ip-address sender-ip-address [tcp | udp | ip-protocol] session-dport sender-sport previous-hop-ip-address previous-hop-interface bandwidth burst-size	Habilitar o roteador como emissor, *sender* para processar as mensagens RSVP PATH.

Tabela 5.7 – Comandos RSVP

Para configurar o roteador receptor para processar as mensagens RSVP RESV deve-se usar o seguinte comando:

Comando	Propósito
ip rsvp reservation session-ip-address sender-ip-address [tcp | udp | ip-protocol] session-dport sender-sport next-hop-ip-address next-hop-interface {ff | se | wf} {rate | load} bandwidth burst-size	Habilitar o roteador como receptor, responsável pelo processamento das mensagens RSVP RESV.

Tabela 5.8 – Comandos RSVP

Para os experimentos realizados foi configurado então os serviços garantidos com uma reserva de 512 Kbps. Esta reserva foi feita considerando um acréscimo de aproximadamente 30 % para o cabeçalho IP, como pode-se observar:

Fluxo Vídeo = 320 Kbps + 30 % = 420 Kbps
Fluxo Áudio = 64 Kbps + 30 % = 84 Kbps

Total = 504 Kbps, arredondando para 512 Kbps de reserva.

De um lado temos o *sender* que atua como emissor das mensagens RSVP PATH, e de outro o *reservation* que atua como recpetor e gerador das mensagens RSVP RESV, na interface do roteador é aplicada uma reserva para uma determinada largura de banda. Foi necessário também a configuração das filas WFQ. Foi utilizado o comando ***fair-***

queue 64 16 2, onde o 64 representa o estado de inicio do descarte de pacotes, o 16 o número de filas dinâmicas simultâneas e 2 a quantidade de filas reservadas.

Na figura 5.7 pode-se observar a forma de configuração RSVP adotada nos experimentos.

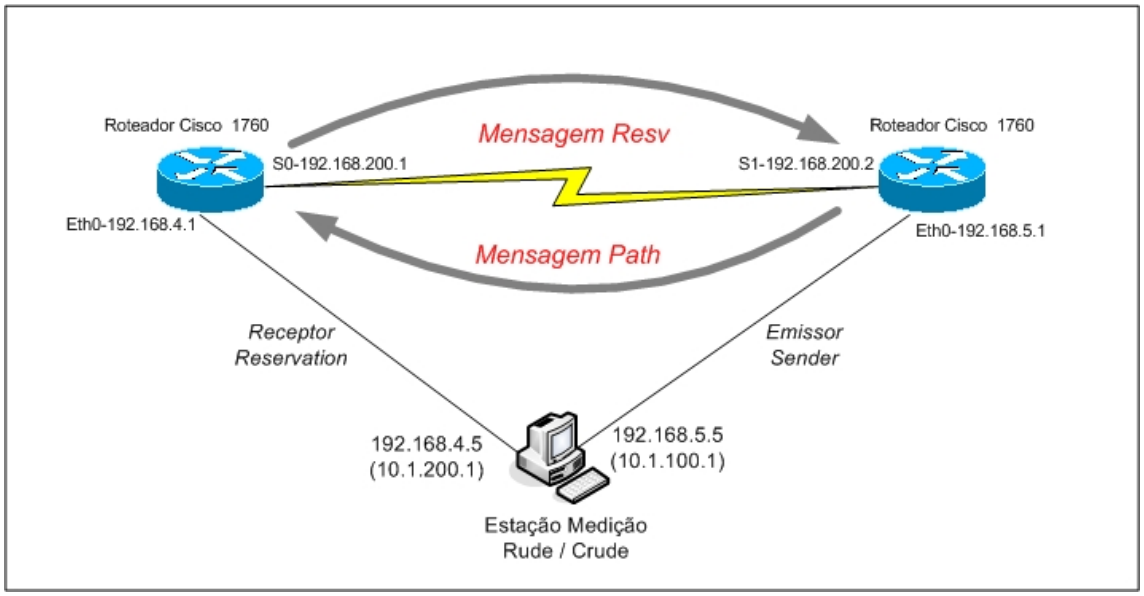

Figura 5.7 – Arquitetura RSVP aplicada

Na tabela 5.9 pode-se observar as configurações de RSVP adotadas no roteador da rede 192.168.5.0. Este roteador teve o papel de *sender*, onde foram feitas as reservas considerando os dois fluxos.

```
!
interface FastEthernet0/0
 ip address 192.168.5.1 255.255.255.0
 ip nat inside
 speed auto
 ip rsvp bandwidth 512
!
interface Serial1/0
 ip address 192.168.200.2 255.255.255.252
 ip nat outside
 fair-queue 64 256 16
 clockrate 1000000
```

```
 ip rsvp bandwidth 512
!
ip nat inside source static 192.168.5.5 10.1.100.1
ip classless
ip route 0.0.0.0 0.0.0.0 Serial1/0
ip route 10.1.200.0 255.255.255.0 Serial1/0
no ip http server
ip rsvp sender 192.168.4.5 192.168.5.5 UDP 5010 5001 192.168.5.5 FastEthernet0/0 420 10
ip rsvp sender 192.168.4.5 192.168.5.5 UDP 5011 5002 192.168.5.5 FastEthernet0/0 84 10
!
```

Tabela 5.9 – Configuração de RSVP do roteador *SENDER*

O roteador da rede 192.168.4.0 teve o papel de *reservation*, na tabela 5.10 são apresentadas as configurações efetuadas neste roteador.

```
!
interface FastEthernet0/0
 ip address 192.168.4.1
 ip nat inside
 speed auto
 ip rsvp bandwidth 512
!
interface Serial1/0
 bandwidth 2000
 ip address 192.168.200.1 255.255.255.252
 ip nat outside
 fair-queue 64 256 16
 ip rsvp bandwidth 512
!
!
ip nat inside source static 192.168.4.5 10.1.200.1
ip classless
ip route 0.0.0.0 0.0.0.0 Serial1/0
ip route 10.1.100.0 255.255.255.0 Serial1/0
no ip http server
ip rsvp reservation 192.168.4.5 192.168.5.5 UDP 5010 5001 192.168.4.5 FastEthernet0/0 FF RATE 420 10
ip rsvp reservation 192.168.4.5 192.168.5.5 UDP 5011 5002 192.168.4.5 FastEthernet0/0 FF RATE 84 10
!
```

Tabela 5.10 – Configuração de RSVP do roteador *RESERVATION*

5.2.2 Resultados Obtidos

Neste capítulo serão descritos os resultados dos experimentos realizados com a ferramenta Rude & Crude. Nos experimentos da etapa dois, foi avaliado o atraso, a variação do atraso e a perda de pacotes. Os experimentos simularam tráfego de vídeo

conferência, num estado de rede sem congestionamento, com congestionamento e com congestionado e QoS. Foram gerados fluxos de vídeo num total de 320 Kbps com pacotes de 1024 bytes e fluxos de áudio num total de 64 Kbps com pacotes de 280 bytes, totalizando 384 Kbps de tráfego. Os fluxos foram gerados da interface 10.1.100.1 para a interface 10.1.200.1.

Na tabela 5.11 podemos observar os resultados obtidos:

Estado da Rede		**Atraso**		**Variação Atraso**		**Perda Pacotes**	
		Vídeo	**Áudio**	**Vídeo**	**Áudio**	**Vídeo**	**Áudio**
Rede Limpa	Média (ms)	10,168630	4,937678	0,145568	3,329492	0 %	0%
	Máximo (ms)	58,910131	42,180061				
	Mínimo (ms)	10,010004	3,199816				
	Desvio Padrão	0,749314	2,761350				
Congestionada	Média (ms)	390,693493	386,923974	11,021923	11,094743	10,4%	11,8%
	Máximo (ms)	424,230099	428,829978				
	Mínimo (ms)	29,850006	27,869940				
	Desvio Padrão	15,149485	15,118863				
Congestionada com QoS	Média (ms)	24,336527	16,945831	3,112280	6,471557	0%	0%
	Máximo (ms)	31,080008	29,719830				
	Mínimo (ms)	18,399954	3,910065				
	Desvio Padrão	2,899266	5,343965				

Tabela 5.11 – Resultado dos experimentos com Rude & Crude

Pode-se observar que num estado de rede com congestionamento, os fluxos enviados tiveram um atraso e uma variação de atraso bastante altos. Quando se compara estes resultados com os obtidos num estado de congestionada, mas com mecanismo de QoS, percebe-se claramente, que o atraso e a variação ficam muito próximos a de um estado de rede sem congestionamento, concluindo-se que o uso de QoS, realmente é necessário em situações onde a rede apresenta um estado de congestionamento muito alto. Sem o uso de QoS, com toda a certeza uma aplicação de vídeo conferência não funcionaria de forma eficaz, em uma rede congestionada e sem QoS.

Nas próximas tabelas são apresentadas algumas informações sobre o estado dos roteadores, nesta etapa do experimento.

A tabela 5.12 informações do roteador *sender* sobre o estado da reserva.

```
ROUTER-06#sh ip rsvp reservation
To          From        Pro DPort Sport Next Hop      I/F      Fi Serv BPS
192.168.4.5 192.168.5.5 UDP 5010  5001  192.168.4.5   Fa0/0    FF RATE 420K
192.168.4.5 192.168.5.5 UDP 5011  5002  192.168.4.5   Fa0/0    FF RATE 84K
ROUTER-06#sh ip rsvp sender
To          From        Pro DPort Sport Prev Hop      I/F      BPS
192.168.4.5 192.168.5.5 UDP 5010  5001  192.168.200.2 Se1/0    420K
192.168.4.5 192.168.5.5 UDP 5011  5002  192.168.200.2 Se1/0    84K
ROUTER-06#sh ip rsvp request
To          From        Pro DPort Sport Next Hop      I/F      Fi Serv BPS
192.168.4.5 192.168.5.5 UDP 5010  5001  192.168.200.2 Se1/0    FF RATE 420K
192.168.4.5 192.168.5.5 UDP 5011  5002  192.168.200.2 Se1/0    FF RATE 84K
```

Tabela 5.12 – Roteador *Sender*

Na tabela 5.13 pode-se observar as configurações de RSVP aplicadas no roteador *Sender*.

```
ROUTER-06#sh ip rsvp installed
RSVP: FastEthernet0/0
BPS   To          From        Protoc DPort  Sport
420K  192.168.4.5 192.168.5.5 UDP    5010   5001
84K   192.168.4.5 192.168.5.5 UDP    5011   5002
```

Tabela 5.13 – Configuração de RSVP do roteador *Sender*

Na tabela 5.14 pode-se observar os parâmetros de RSVP do roteador *Reservation*.

```
ROUTER-05#sh ip rsvp neighbor
 0.0.0.0         Unknown
 192.168.4.5     Unknown
 192.168.200.1   RSVP
ROUTER-05#sh ip rsvp
RSVP: enabled (on 2 interface(s))
Rate Limiting: disabled
  Max msgs per interval: 4
  Interval length (msec): 20
  Max queue size: 500
  Max msgs per second: 200

Refresh Reduction: disabled
  ACK delay (msec): 250
  Initial retransmit delay (msec): 1000
  Local epoch: 0x4E7FB4
  Message IDs: in use 0, total allocated 0, total freed 0

Neighbors: 3
  RSVP encap: 1 UDP encap: 0 RSVP and UDP encap: 0

Local policy:
COPS:

Generic policy settings:
    Default policy: Accept all
    Preemption:     Disabled
```

Tabela 5.14 – Configurações de RSVP do roteador *Reservation*

Desta maneira pode-se concluir que a política de QoS, aliada a disciplina de enfileiramento WFQ, foram bastante eficazes, conseguindo controlar o atraso e a variação de atraso num estado de rede congestionada.

5.3 Resumo do Capitulo

Neste capítulo, foram relatados os experimentos realizados e seus resultados. Na primeira etapa ficou comprovada a necessidade de utilização de técnicas de QoS para priorização de tráfego. Na etapa 2 foi verificado como o sincronismo dos relógios afeta a precisão de medições unilaterais e também a eficácia do protocolo RSVP de reserva de recursos para configuração de QoS para priorização de tráfego.

6. CONCLUSÕES

6.1 Conclusões gerais

Neste trabalho foi elaborada uma pesquisa bibliográfica, que se baseou principalmente em artigos publicados por instituições de renome como a IEEE, RFCs, documentação de fabricantes e em alguns livros. No decorrer do trabalho conceitos sobre qualidade de serviços e vídeo conferência foram apresentados, e também a justificativa que norteou o desenvolvimento deste trabalho.

O modelo de serviços integrados (IntServ) foi apresentado, como uma das alternativas de provimento de qualidade de serviço em redes IP, principalmente para aplicações multimídia, como o caso de vídeo conferência.

Foram realizados vários experimentos em diversos estados de rede, que tiveram como objetivo principal avaliar a eficácia do modelo de serviços integrados para prover qualidade de serviço em redes IP. Os experimentos e resultados conclusivos foram divididos em duas etapas, e estão descritos com detalhes no capítulo 5 deste trabalho.

Os resultados atingidos por este trabalho comprovam a necessidade do uso de técnicas de qualidade de serviço em redes IP, e que é praticamente impossível garantir que aplicações multimídia, como vídeo conferencia, funcionem de forma correta, sem que estas aplicações tenham prioridade sobre as demais aplicações que estejam rodando em uma rede IP. Os resultados apresentados no capítulo 5 comprovam que o modelo de serviços integrados é eficaz no provimento de QoS, porém desperta a atenção de que não existe uma receita pronta de como prover QoS no modelo de serviços integrados e que exige um grande esforço de implementação. Para cada tipo de necessidade e situação, deve haver uma análise de qual arquitetura deve ser a ideal e de como deve ser implementada.

Também conclui-se com este trabalho, que nada adianta o aumento não racional de largura de banda nas redes como forma à garantir qualidade e melhor desempenho as aplicações. Torna-se cada vez mais importante o gerenciamento do tráfego e da largura de banda, de forma a priorizar as aplicações mais sensíveis ao atraso e variação de atraso, evitando desta forma a contratação desnecessária de largura de banda, com isto reduzindo os custos operacionais das redes.

6.2 Principais contribuições

O modelo de serviços integrados, foi apresentado como uma solução para prover QoS em redes IP. Esta é uma área onde existe a necessidade de mais estudos experimentais. Nos experimentos foi possível comprovar na prática a real necessidade do uso de QoS em aplicações multimídia, como vídeo conferência. Foi observado que fluxos de vídeo conferência em redes congestionadas, possuem um atraso, uma variação do atraso e perda de pacotes bastante grande, acarretando o mau funcionamento de aplicações de vídeo conferência. Um fator problemático na realização dos experimentos foi o sincronismo dos relógios. Quando utiliza-se ferramentas de medição unilaterais, o sincronismo do relógio afeta em muito os resultados dos experimentos. Concluindo com isso que o protocolo NTP de sincronismo não é muito eficaz, e que a única forma de obter sucesso em medições unilaterais, é o uso de sincronismo com GPS. Pode-se concluir também que o modelo de serviços integrados possui problemas de escalabilidade no núcleo da rede. Os roteadores de núcleo precisarão lidar com a manutenção de estados, sinalização, policiamento e controle de filas de espera, num grande número de reservas.

6.3 Trabalhos futuros

No desenvolvimento deste trabalho foi constatado que existem pontos, aos quais ainda não existem trabalhos muito aprofundados. Não existe uma receita para aplicação de técnicas de qualidade de serviço, é necessário uma análise com base num escopo de proposta de serviços. Diante disso seria de grande valia, um estudo comparativo entre os dois modelos de qualidade de serviços, serviços diferenciados e serviços integrados, propondo a implantação de um modelo misto, utilizando o que cada modelo tem de melhor e vantagem. Observou-se também a grande deficiência de ferramentas para medição e gerência de QoS. Um estudo que aprofundá-se a problemática de medições de QoS, e de gerência poderia contribuir muito para o desenvolvimento dos referidos modelos.

REFERÊNCIAS

[ABE 2001] ABELÉM, Antonio Jorge G. et al. **QoS Fim a Fim através da Combinação entre serviços integrados e Serviços Diferenciados**. Florianópolis, UFSC, 2001.

[ALM 99a] ALMES, G.; KALIDINDI, S.; ZEKAUSKAS, M. **RFC 2679 - A One-way Delay Metric for IPPM**. Network Working Group Request for Comments - IETF. New York: 1999. Disponível em < www.ietf.org/rfc/rfc2679.txt > Acesso em: 20 Jan. 2004.

[ALM 99b] ALMES, G.; KALIDINDI, S.; ZEKAUSKAS, M. **RFC 2680 - A One-way Packet Loss Metric for IPPM.** Network Working Group Request for Comments - IETF. New York: 1999. Disponível em:< www.ietf.org/rfc/rfc2680.txt > Acesso em: 21 Jan. 2004.

[ALM 99c] ALMES, G.; KALIDINDi, S.; ZEKAUSKAS, M. **RFC 2681 - A Round-trip Delay Metric for IPPM**. Network Working Group Request for Comments – IETF. New York. 1999. Disponível em: < www.ietf.org/rfc/rfc2681.txt > Acesso em 22 Jan. 2004.

[ANA 2004] ANATEL. Comunicação Multimídia. ANATEL. Brasília. Disponível em: <http://www.anatel.gov.br/Comunicacao_Multimidia/default.asp?CodArea=33&CodPrinc=1> Acesso em 10 Jan 2004.

[ASS 2002] ASSIS, Martin Seefelder. **MPLS**. UFRJ. Rio de Janeiro: 2002. Disponível em: < http://www.gta.ufrj.br/grad/01_2/mpls/mpls.htm > Acesso em: 17 Jan. 2004.

[ASS 2004] ASSUNÇÃO, Marcos Flávio Araújo. Sniffers. Site. **Revista Eletrônica Invasão**, 2004. Disponível em: < http://www.invasao.com.br/coluna-marcos-17.htm > Acesso em: 05 Nov. 2004.

[BAR 98] BARZILAI, Tsipora; KANDLUR, Dilip. Design and implementation of an RSVP-Based Quality of Service Architecture for an Integrated Services Internet. **IEEE Journal on Selectec areas in communications,** v.16, n.1, p. 397-413, Abr. 1998.

[BRA 94] BRADEN, R.; CLARK, D.; SHERENKER, S. **RFC 1633 - Integrated Services in the Internet Architecture**: an Overview. Network Working Group Request for Comments – IETF. Cambridge: 1994.
Disponível em: <http://www.ietf.org/rfc/rfc1633.txt>
Acesso em: 10 Jan 2004.

[BRA 97] BRADEN, R. et al. **RFC 2205 - Resource Reservation Protocol RSVP**. Network Working Group Request for Comments - IETF. Los Angeles: 1997. Disponível em: < http://www.ietf.org/rfc/rfc2205.txt >
Acesso em 19 Jan. 2004.

[BRA 99] BRADEN, Bob. **RSVP and Integrated Services.** University of Southern California. California: 1999.
Disponível em: < http://portal.etsi.org/stq/old_workshop/RSVP.pdf >
Acesso em: 01 Fev. 2004.

[BER 2000] BERNET, Yoram. The complementary roles of RSVP and differentiated services in the full-service QoS Network. **IEEE Communication Magazine,** v.1, n.1, p. 154-162, Fev. 2002.

[BER 2003] BERTINO, Elisa et al. Quality of Service Specification in vídeo databases. **IEEE Computer Society**, Lyon, v.1, n. 1, p. 71-81, Dez. 2003.

[BOK 2004] BOKUN, Igor et al. The MECCANO Internet Multimedia Conferencing Architecture. 2004.
Disponível em: <http://www.ice.cs.ucl.ac.uk/multimedia/projects/meccano/architecture/meccano-architecture.html > Acesso em: 15 Jun. 2004.

[BRU 2002] BRUN, Altamir; VOGT, Eide Marta Gonçalves; MENDES, Alessandra da Silveira. **QoS – Qualidade de Serviço em TCP/IP**. PUCPR. Curitiba:2002.
Disponível em: <http://www.ppgia.pucpr.br/~jamhour/Download/pub/ArtigosPos/Monografia.PDF>
Acesso em: 15 Fev. 2004.

[CAD 2003] CADORIN, Daniel. **Ferramenta para monitoramento de redes IP com Serviços Diferenciados utilizando SNMP**, Florianópolis: UFSC, 2003. 77 p. Dissertação (Mestrado) – Programa de Pós-Graduação em Ciência da Computação, Universidade Federal de Santa Catarina, Florianópolis, 2003.

[CAR 2004] CARVALHO, Tereza Cristina Melo de Brito. **Tecnologias Convergentes**. USP. São Paulo: 2004.
Disponível em:<http://www.redes.usp.br/conteudo%5Cdocumentos/artigo0102.pdf >
Acesso em: 02 Jul. 2004.

[CHA 2003] CHAPPELL, Laura; FARKAS, Dan. **Diagnosticando Redes Cisco Internetwork Troubleshooting**. São Paulo: Cisco Press, 2003, 1ª Ed.

[CIS 2002a] CISCO SYSTEM INC. Introduction: Quality of Service Overview. Cisco System, 2002.
Disponível em: <http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/qos_c/qcintro.htm>
Acesso em: 10 Jan. 2004.

[CIS 2002b] CISCO SYSTEM INC. **Resource Reservation Protocol**. Cisco System. 2002.
Disponível em: <http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/rsvp.htm>
Acesso em 20 Jan. 2004.

[CIS 2002c] CISCO SYSTEM INC. **Quality of Service Solutions**. Cisco System, 2002.
Disponível em : < http://www.cisco.com>
Acesso em 11 Jan. 2004.

[COM 98] COMER, Douglas E. **Interligação em Redes com TCP/IP**. Rio de Janeiro: Campus, 1998, 2 ª Ed.

[COM 99] COMER, Douglas E.; STEVENS David L. **Interligação em rede com TCP/IP**: Volume II, Projeto, implementação e detalhes internos**.** Rio de Janeiro: Campus, 1999, 3ª Ed.

[DIA 2001] DIAS, Roberto Alexandre. Serviços **Diferenciados Baseados na tecnologia MPLS em Redes Heterogêneas**. Centro Federal de Educação Tecnológica de Santa Catarina. Florianópolis: 2001.
Disponível em: < http://www.nersd.org/~beto/artigos/sbmidia2001.pdf >
Acesso em 17 Jan. 2004.

[DIV 2003] DIVINI, Thomas F. Test TCP (TTCP) Benchmarking Tool for Measuring TCP and UDP Performance. PCAUSA. Georgia: 2003.
Disponível em:< http://www.pcausa.com/Utilities/pcattcp.htm >
Acesso em: 21 Mai. 2004.

[DUA 2002] DUARTE, Otto Carlos Muniz Bandeira; BICUDO, Marcos Dias Dutra. **IEEE 8021.p – QoS na camada MAC.** UFRJ. Rio de Janeiro: 2002.
Disponível em:< http://www.gta.ufrj.br/grad/02_2/802.1p/ >
Acesso em: 01 Jul. 2004.

[DUR 2004] Hector A. Duran et al. Adaptive Resource Management in Middleware: A Survey. **IEEE Distributed systems online**, vol.5, n.7, Jul. 2004.

[FAY 2002] FAYAZ, Shaikh et al. **End** to End testing of IP QoS mechanisms. **IEEE Communication Magazine,** 50 th Anniversary Commemorative, p. 116-127, Mai. 2002.

[FER 99] FERGUSON, Paul; HUSTON, Geoff. **Quality of Service:** Delivering QoS on the Internet and in Corporate Networks. New York: Wiley Computer Publishing, 1999.

[FLA 2001] FLANAGAM, Michael E. **Administering Cisco QoS in IP Networks**. Rockland: Syngress Publishing Inc, 2001.

[FON 99] FONSECA, Fernanda; CARAPINHA, Jorge. **QoS em Rede IP.** Portugal Telecom. Portugal: 1999.
Disponível em:< http://www.fccn.pt/crc1999/FINAIS/artigo30/ARTIGO30.HTM > Acesso em: 25 Jan. 2004.

[GHE 2004] Ghetie, Joseph. Internet Network and service management. **The Ninth IEEE Symposium on computers and communications (ISCC'2004)**, Jun. 2004.

[GOZ 2003] GOZDECKI, Januz; JAJSZCZYK, Andrzej; STANKIEWICZ. Quality of Service Terminology in IP Networks. **IEEE Communications Magazine**, v.1, n.1, p. 153-159, Mar. 2003.

[IXI 2004] IXIA. **Qcheck Aplications.** IXIA. Calabasas: 2004.
Disponível em: <http://www.ixiacom.com/products/performance_applications/pa_display.php?skey=pa_q_check >
Acesso em: 20 Abr. 2004.

[KAM 2000] KAMIENSKI, Carlos Alberto; SADOK, Djamel. **Engenharia de Tráfego em uma Rede de Serviços Diferenciados**. Universidade Federal de Pernanbuco. Recife: 2000.
Disponível em:< http://www.cin.ufpe.br/~cak/publications/sbrc2000.pdf >
Acesso em: 17 Jan. 2004.

[KAM 99] KAMIENSKI, Carlos Alberto. **Qualidade de Serviço na Internet**. Universidade Federal de Pernanbuco. Recife: 1999.
Disponível em:< http://www.cin.ufpe.br/~cak/publications/kamienski-qos-eine-99.pdf >
Acesso em: 17 Jan. 2004.

[KUO 2003] KUO, Geng; KO, Po chang. Dynamic RSVP Protocol. **IEEE Communication Magazine,** v.1, n.1, p. 130-135, Mai. 2003.

[LAN 2002] LAINE, Juha et al. Introduction to Rude & Crude. **Project Source Forge**, v. 0,7, Set. 2002. Disponível em: < http://rude.sourceforge.net/ > Acesso em: 05 Nov. 2004

[LEE 2004] LEE, Guanling et al. Architecture for Mobility and QoS Support in All-IP Wireless Networks. **IEEE Journal**, 2004.

[LEO 2001a] LEOLPODINO, Graciela Machado; MOREIRA, Edson dos Santos. **Modelos de comunicação para vídeo conferência**. USP. São Paulo: 2001.

[LEO 2001b] LEOPOLDINO, Graciela Machado; MEDEIROS, Rosa Cristina Martins de Medeiros. **H323: Um padrão para sistemas de comunicação multimídia baseado em pacotyes**. RNP – Rede Nacional de ensino e pesquisa. Rio de Janeiro: 2001. Disponível em: < http://www.rnp.br/newsgen/0111/h323.html > Acesso 15 Jul. 2004.

[LEO 2004] Leong, Chi Wa et al. Call Admission Control for Integrated On/Off Voice and Best-Effort Data Services in Mobile Cellular Communications. **IEEE Transactions on communications**, 2004.

[LEU 2000] LEUNG, Yiu-Wing. Congestion Control for Multipoint Videoconferencing. **IEEE Transactions on circuits and systems for video technology,** v. 10, n.5, p. 715-724, Ago. 2000.

[LIM 2002] LIMA, Michele Mara de Araújo Espíndola; FONSECA, Nelson Luis Saldanha da. **Controle de Trafego Internet**. UNICAMP. Campinas: 2002. Disponível em:< http://ftp.inf.pucpcaldas.br/CDs/SBRC2002/Minicursos/cap4.pdf > Acesso em: 18 Jan. 2004.

[LUN 2001] LUNARDI, Sediane Carmem. **Uma Camada de Suporte à Qualidade de Serviço para Aplicações Multimídia na Internet**. Porto Alegre: PUCRS, 2001. 95 p. Dissertação (Mestrado) – Programa de Pós-Graduação em Ciência da Computação, Faculdade de Informática, Pontifícia Universidade Católica do Rio Grande do Sul, Porto Alegre, 2001. Disponível em: < http://www.pucrs.br/inf/pos/dissertacoes/arquivos/sediane.pdf > Acesso em: 25 Jan. 2004.

[MAH 99a] MAHDAVI, J.; PAXSON, V. **RFC 2498 - IPPM Metrics for Measuring Connectivity**. Network Working Group Request for Comments. Network Working Group Request for Comments - IETF. Pittsburgh: 1999. Disponível em: < www.ietf.org/rfc/rfc2498.txt > Acesso em: 21 Jan. 2004.

[MAH 99b] MAHDAVI, J; PAXSON, V. **RFC 2678 - IPPM Metrics for Measuring Connectivity**. Network Working Group Request for Comments – IETF. Pittsburg: 1999. Disponível em: < www.ietf.org/rfc/rfc2678.txt > Acesso em 21 Jan. 2004.

[MEL 2001] MELO, Edson Lopes. **Qualidade de Serviço em Redes IP com DiffServ: Avaliação através de Medições.** Florianópolis: UFSC, 2001. 113 p. Dissertação (Mestrado) – Programa de Pós-Graduação em Ciência da Computação, Universidade Federal de Santa Catarina, Florianópolis, 2001.

[MES 99] MESQUITA, Thienne. Modelagem e Análise de Desempenho do Serviço Vídeo-sob-Demanda em Reeds de Alta Velocidade Utilizando o Protocolo RSVP sobre Redes ATM. UFSCAR. São Carlos: 1999.
Disponível em:< http://www.dc.ufscar.br/posgrad/discentes/diss96.htm >
Acesso em 25 Jan. 2004.

[MET 2004] METRO ACCESS NETWORKS. **IEEE 8021.q**. XLINX. 2004.
Disponível em:
<http://www.xilinx.com/esp/networks_telecom/optical/net_tech/ieee8021q.htm >
Acesso em: 02 Jul. 2004.

[MIC 99] MICROSOFT CORPORATION: **Quality of Service Technical White Paper.** Microsoft Corporation, 1999.
Disponível em:
<http://www.microsoft.com/windows2000/techinfo/howitworks/communications/trafficmgmt/qosover.asp > Acesso em: 15 Jan 2004.

[MIL 96] MILLS, D. RFC 2030 - Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI. Network Working Group Request for Comments – IETF. Newark: 1996. Disponível em: < http://www.ietf.org/rfc/rfc2030.txt?number=2030 >
Acesso em: 20 Mai. 2004.

[MOL 2004] MOLINARI, Marcelo M. **Redes Virtuais:** Tecnologias e Status da Padronização. 3Com. Brasil: 2004.
Disponível em: < http://www.prodepa.psi.br/marcelo/Home%20Page/Docs-Redes/vlan_pad.PDF > Acesso em: 01 Jul. 2004.

[MOR 2004] MOREIRA, André. **Asynchronous Transfer Mode.** ISEP. 2004.
Disponível em:< http://www.dei.isep.ipp.pt/~andre/documentos/atm.html >
Acesso em: 02 Jul. 2004.

[MRT 2004] MRTG. Multi Router Traffic Grapher. MRTG. 2004.
Disponível em:< http://mrtg.hdl.com/mrtg.html > Acesso em: 21 Mai. 2004.

[NAV 2004] NAVAL RESEARCH LABORATORY. The Multi-Generator (MGEN) Toolset. NRL. 2004. Disponível em: < http://manimac.itd.nrl.navy.mil/MGEN/ > Acesso em: 21 Mai. 2004.

[NUP 2004] NUPERC. Grupo de Trabalho em Qualidade de Serviço. UNIFACS. Salvador: 2004.
Disponível em:< http://www.nuperc.unifacs.br/gtqos2/netflow.htm > Acesso em: 02 Jul. 2004.

[PAQ 2003] PAQUET, Catherine; TEARE, Diane. **Construindo Redes Cisco Escaláveis**. São Paulo: Cisco Press, 2003, 1ª Ed.

[PAS 2004] Pascal, Lorenz. IP-Oriented QoS in Next Generation Networks: Application to Wireless Networks. **The Ninth IEEE Symposium on computers and communications (ISCC'2004)**, Jun. 2004.

[PAX 98] PAXSON, V. et al. **RFC 2330 - Framework for IP Performance Metrics**. Network Working Group Request for Comments - IETF. Pittsburgh: 1998.
Disponível em: < www.ietf.org/rfc/rfc2330.txt > Acesso em: 20 Jan. 2004.

[POL 2004] POLYCOM COMPANY INC. **Products & Services ViewStation FX.** Polycom Compnay: 2004.
Disponível em: <http://www.polycom.com/products_services/1,1443,pw-35-4364,00.html > Acesso em: 05 Nov. 2004.

[QUI 2003] QUICKNET TECHNOLOGIES. **Open H323 Project.** Quicknet. 2003.
Disponível em: < http://www.openh323.org/ > Acesso em: 21 Mai. 2004.

[RNP 2004] RNP. **Serviço NTP.** RNP. Rio de Janeiro: 2004.
Disponível em: < http://www.rnp.br/ntp/ > Acesso em: 20 Abr. 2004.

[SAN 99] SANTOS, Ana Paula Silva. **Qualidade de Serviço na Internet.** RNP. Rio de Janeiro: 1999, Volume 3, Número 6.
Disponível em:<http://www.rnp.br/newsgen/9911/qos.html> Acesso em 10 Jan. 2004.

[SCH 2000] SCHMIDT, Ana Luísa Pereira. O Protocolo RSVP e o Desempenho de Aplicações Multimídia. RNP. Rio de Janeiro: 2000.
Disponível em:< http://www.rnp.br/newsgen/0005/rsvp.html#ng-rsvp >
Acesso em: 20 Jan. 2004.

[SHE 97] SHENKER, S.; PARTRIDGE, C.; GUERIM, R. **RFC 2212 - Specification of Guaranteed Quality of Service**. Network Working Group Request for Comments - IETF. Palo Alto: 1997.
Disponível em:< http://www.ietf.org/rfc/rfc2212.txt > Acesso 19 Jan. 2004.

[SIL 2000] SILVA, Adailton. Qualidade de Serviço em VoIP - Parte 2. RNP. Rio de Janeiro: 2000. Disponível em: < http://www.rnp.br/newsgen/0009/qos_voip2.html#ng-5 > Acesso em: 16 Jun. 2004.

[SOA 95] SOARES, Luiz Fernando G.; LEMOS, Guido; COLCHER, Sérgio. **Redes de Compuatadores: Das LANs, MANs e WANs às redes ATM**. Rio de Janeiro: Campus, 1995, 6ª Ed.

[TAN 97] TANENBAUM, Andrew S. **Redes de Computadores**. Rio de Janeiro: Campus, 1997. 5ª Ed.

[VEG 2001] VEGESNA, Srinivas. **Ip Quality of Service**. Portland: Cisco Press, 2001.

[VID 2004] VIDE. Videoconferencing Cookbook. Vide. 2004.
Disponível em:< http://www.videnet.gatech.edu/cookbook/ > Acesso em: 21 Mai. 2004.

[WHI 97] WHITE, Paul P. RSVP and Integrated Services in the Internet: A Tutorial. **IEEE Communication Magazine,** v.1, n.1, p. 100-106, Mai. 1997.

[WRO 2000] WROCLAWSKI, John. **Integrated Services**. Network Working Group Request for Comments - IETF. 2000.
Disponível em:< http://www.ietf.org/html.charters/intserv-charter.html > Acesso em: 18 Jan. 2004.

[WRO 97a] WROCLAWSKI, John. **RFC 2210 - The use of RSVP with IETF Integrated Services**. Network Working Group Request for Comments - IETF. Cambridge: 1997. Disponível em: <http://www.ietf.org/rfc/rfc2210.txt> Acesso em 19 Jan. 2004.

[WRO 97b] WROCLAWSKI, John. **RFC 2211 - Specification of the Controlled-Load Network Element Service**. Network Working Group Request for Comments - IETF. Cambridge: 1997. Disponível em:< http://www.ietf.org/rfc/rfc2211.txt >
Acesso em 18 Jan. 2004.

[ZHA 93] ZHANG, Lixia et al. RSVP: A new resource reservation protocol. **IEEE Network**, v.1 n.1, p. 8-10, Set. 1993.