Universidade Federal de Santa Catarina
Programa de Pós-Graduação em Ciência da Computação

Edison Tadeu Lopes Melo

Qualidade de Serviço em Redes IP com DiffServ: Avaliação através de Medições

Dissertação submetida à Universidade Federal de Santa Catarina como parte dos requisitos para a obtenção do grau de Mestre em Ciência da Computação

Prof. Dr. Carlos Becker Westphall
Orientador

Florianópolis, Maio de 2001.

Edison Tadeu Lopes Melo

Qualidade de Serviço em Redes IP com DiffServ: Avaliação através de Medições

Florianópolis
2001

Qualidade de Serviço em Redes IP com DiffServ: Avaliação através de Medições

Edison Tadeu Lopes Melo

Esta Dissertação foi julgada adequada para 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. Carlos Becker Westphall
Orientador

Prof. Dr. Fernando Alvaro Ostuni Gauthier
Coordenador do Curso de Pós-Graduação em Ciências da Computação

Banca Examinadora:

Prof. Dr. Carlos Becker Westphall
Presidente

Prof. Dr. Jean-Marie Farines

Prof. Dr. Roberto Willrich

Msc. Elvis Melo Vieira

Resumo

Esse trabalho apresenta uma avaliação sobre a implementação de Qualidade de Serviço (QoS) em redes IP através de medições. Foram testados os padrões DiffServ em diferentes plataformas. A avaliação constituiu-se de duas fases: Na primeira fase, realizou-se uma análise global sobre o ambiente DiffServ e verificou-se a capacidade de isolamento de tráfego e garantia de largura de banda por classe de serviços. Ainda nessa etapa realizou-se monitoração nos nós DiffServ para verificar o comportamento dos mecanismos de classificação e descarte de pacotes. Na segunda fase, a medição de QoS foi empregada para estudar o impacto do tráfego melhor esforço, TCP e UDP, com diferentes tamanhos de pacotes, sobre o desempenho da classe de serviços de tráfego expresso (EF).

Para todos os experimentos, utilizou-se um tráfego de *background* para saturar o canal de comunicação. Na classe EF foram realizadas medidas associadas ao atraso, à variação do atraso e à taxa de perda de pacotes. Os resultados foram conclusivos quanto a garantia de QoS quando a classe de serviços EF é configurada para suporte a tráfego com taxa constante de bits (CBR). Os resultados demonstraram, entretanto, existir situações onde mecanismos de garantia de QoS são afetados pela presença de tráfego *background* intenso na rede. Finalmente, efetuou-se transmissão de áudio e vídeo para relacionar o desempenho dessas aplicações nos ambientes de testes. Essas transmissões comprovaram a efetividade dos mecanismos de priorização de tráfego de DiffServ e das políticas de configuração adotadas.

Abstract

This work presents an evaluation, about a Quality of Service implement on IP Networks, through measurements. It was tested the DiffServ Standard on different platforms. The evaluation has two phases: On the first phase, it was made a global analysis about the DiffServ environment, in which was verified the capacity of traffic isolation and guarantee of bandwidth per service class. Further in this phase, monitoring was done on the DiffServ nodes to verify the behavior of the classification mechanisms and packet discards. On the second phase, the QoS measurements was used to study the impact of the best effort traffic - TCP and UDP with different sizes of packets – on the performance of service class of Expedited Forwarding (EF).

For all the measurement experiments, it was used background traffic to saturate the communication channel. In the EF class, it was made measurements concerned with the delay, variation of the delay (jitter) and the packet loss rate. The results were conclusive considering the QoS guarantee when the service class EF was configured to support one CBR traffic. However, the results demonstrated the existence of situations where the mechanisms of QoS guarantee are affected by the presence of intensive background traffic on the network. Finally, it was made audio and video transmission to compare the performance of these applications in the test environments. These transmissions validated the effectiveness of the traffic prioritization of DiffServ and the configuration policies adopted.

Dedicatória

Para minha esposa, Edilce;

Minha filha, Natália;

Meu pai, Tubalcaim;

Minha mãe, Hiolita;

Minha irmã e irmãos; e

Meus amigos.

Agradecimentos

A Edilce e Natália pelo amor, dedicação e companheirismo que foram muito importantes para a realização deste trabalho.

A minha família, pelo apoio e incentivo em todas as horas.

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

Aos demais membros da banca:

Professor Jean-Marie Farines, pelos muitos trabalhos realizados, pelas oportunidades, pelo convívio, amizade e exemplo;

Professor Roberto Willrich, pelas sugestões; e

Elvis Melo Vieira, pelas discussões, sugestões e amizade.

A todos amigos do NPD, de ontem, de hoje e de sempre e, em especial, ao Márcio, Fernando, João Batista, Nicolau, Izabel, Kathia Jucá, André, Adriano, Jussara e Gerson.

Aos amigos da RMAV-FLN, em especial, a Solange, Walter e Pedro. A todos os meus amigos e a Deus.

ÍNDICE

Lista de Figuras

Lista de tabelas

Lista de abreviaturas

AF	Assured Forwarding
ATM	Asynchronous Transfer Mode
BA	Behaviour Aggregate
BE	Best-Effort
bg	*background*
CAR	Committed Access Rate
CBR	Constant Bit Rate
CIR	Committed Information Rate
Diffserv	Differentiated Services
DS	Differentiated Services
DSCP	Differentiated Services Code-Point
e2e	End to End
EF	Expedited Forwarding
ERP	Enterprise Resource Planning
FIFO	First In First Out
IETF	Internet Engineering Task Force
Intserv	Integrated Services
IP	Internet Protocol
IPDV	Instantaneous Packet Delay Variation
IPPM	IP Performance Working Group
LAN	Local Area Network
PPP	Point-to-Point Protocol
MF	Multi-field
NTP	Network Time Protocol
PHB	Per-Hop Behaviour
PQ	Priority Queuing
QoS	Quality of Service
RTT	Round Trip Time
RSVP	Resource ReSerVation Protocol
SLA	Service Level Agreement

SCFQ	Self Clocked Fair Queuing
TCP	Transmission Control Protocol
TOS	Type of Service
UBR	Unspecified Bit Rate
UDP	User Datagram Protocol
VBR	Variable Bit Rate
VoIP	Voice over IP
VPC	Virtual Path Connection
WAN	Wide Area Network
WFQ	Weighted Fair Queuing

1 INTRODUÇÃO

1.1 Considerações iniciais

A medida em que as redes ganham novas funcionalidades, tornam-se ativos empresariais estratégicos e centros de operações das empresas. Aplicações de missão crítica, tais como as de Planejamento de Recursos Empresariais – ERP (*Enterprise Resource Planning),* compartilham largura de banda com o tráfego convencional (transferência de arquivos, acesso a páginas WWW) e outras aplicações. As redes, entretanto, convergem para uma infra-estrutura única compartilhada, capaz de suportar também áudio e vídeo e, neste cenário, tipos diferentes de tráfego devem ser tratados de modo diferenciado. Algumas aplicações, como as de áudio, têm exigências rígidas quanto ao atraso fim-a-fim, mas podem tolerar perdas mínimas de pacotes, enquanto outras como transferência de arquivos são sensíveis a este último aspecto, mas as exigências quanto ao atraso são pouco severas [53].

As aplicações de missão crítica dão suporte às principais operações das empresas e não podem tolerar atrasos causados por aplicações multimídia. Estas possuem altos requisitos de largura de banda e, potencialmente, podem absorver todos os recursos de rede disponíveis. Em uma instituição financeira, por exemplo, aplicações de missão crítica são aquelas ligadas diretamente ao negócio, como as de suporte às operações de saque, emissão de extrato, consulta a saldo e outras desta natureza. Já a empresa que decide implantar uma aplicação de voz sobre IP (VoIP) em sua rede corporativa pode necessitar priorizar o tráfego gerado por essa aplicação em relação as demais, sem entretanto afetá-las significativamente.

A necessidade de Qualidade de Serviço (QoS) é evidente quando se busca utilizar eficientemente canais de comunicação de redes de longa distância WAN – (*Wide Area Network*), os quais muitas vezes apresentam baixa taxa de transferência e/ou alto custo mensal. Em redes corporativas espalhadas por diversas localizações geográficas conectadas por uma WAN, pode ser imperativo dar maior prioridade ao tráfego de voz e de missão crítica que a outros tipos de tráfego.

Uma das maneiras de se conseguir QoS (*Quality of Service*) é o encaminhamento de pacotes, de forma diferenciada, através do agrupamento destes em categorias de tráfego chamadas classes. Uma classe pode conter um único fluxo[1,2] ou a agregação de múltiplas instâncias de um fluxo [15]. Tratamento diferenciado nos pacotes pode ser empregado para criar serviços. Um serviço está associado às necessidades das aplicações como largura de banda, atraso, variação do atraso ou *jitter* e taxa de perda de pacotes. Conceitualmente, a *largura de banda* define a capacidade de transmissão de dados de um canal de comunicação, enquanto o *atraso* é o tempo decorrido entre o envio de uma mensagem e sua recepção no nó destino. Em redes de pacotes, a *variação do atraso* é uma distorção nos tempos de chegada entre pacotes comparados aos tempos originais de transmissão, enquanto que a *taxa de perda de pacotes* representa o percentual de pacotes que foram transmitidos, mas não chegaram ao destino em um determinado período de tempo.

Pesquisas feitas pelo ATM Fórum[4] e IETF[3] [27] apresentam diversas soluções para prover QoS em redes de computadores: o padrão ATM (*Asynchronous Transfer Mode*) [4], o protocolo de reserva de recursos, RSVP (Resource ReSerVation Protocol) [45], principal componente da arquitetura IntServ de serviços integrados [28] e a arquitetura DiffServ de serviços diferenciados [22] [9] são soluções interoperáveis e complementares que buscam resolver este problema.

O suporte de QoS requer medição de desempenho para aferir se os níveis de qualidade especificados foram alcançados. Quando um provedor Internet ou uma corporação fornece serviços baseados em QoS para seus usuários, diferentes níveis de medições podem ser realizados:

- na aplicação para adaptação aos níveis de QoS esperados;
- pelos usuários para verificar o serviço fornecido pela rede; e
- pelo provedor para monitorar e validar os serviços.

---

[1] Em QoS, fluxo pode ser definido como um conjunto de pacotes que, ao atravessarem um elemento da rede, são cobertos pelos mesmos requisitos de controle de QoS.

[2] Conjunto de pacotes com o mesmo endereço fonte e destino. Endereço pode ser IP (IP, porta TCP), (IP, porta UDP), Mac Address, etc.

[3] Internet Engineering Task Force é uma confederação livre de voluntários da indústria de redes e da academia com objetivo de estabelecer protocolos padrões para a Internet.

O problema da medição de desempenho é abordado pelo grupo de trabalho *IP Performance Working Group* [30] do IETF. A medição depende da disponibilidade de métricas, ferramentas e métodos padronizados para quantificar o desempenho.

Neste trabalho serão investigados aspectos relacionados à implementação e análise da arquitetura de Serviços Diferenciados (DiffServ) [22] para prover QoS em redes de longa distância. Ambientes de testes serão montados e utilizados para ganhar experiência com DiffServ e com as ferramentas de medição, a fim de investigar o funcionamento e a efetividade dos mecanismos de priorização e a possibilidade de utilização desta arquitetura em um ambiente de produção.

1.2 Objetivos do trabalho

1.2.1 Objetivo geral

Avaliar, através de medições e experimentação com aplicações de voz e multimídia, a entrega de pacotes em redes IP utilizando a arquitetura de Serviços Diferenciados para implementação de qualidade de serviço (QoS).

1.2.2 Objetivos específicos

- Verificar através da avaliação experimental se existe um comportamento dinâmico nos níveis de tráfego com e sem priorização de QoS;
- verificar a capacidade de isolamento de tráfego e alocação de largura de banda entre diversas classes de serviços do padrão DiffServ;
- verificar o efeito do tráfego melhor esforço, ou ausência desse, sobre o atraso, variação do atraso e taxa de perda de pacotes nos fluxos de tráfego priorizados;
- verificar a relação entre a gerência de qualidade de serviços e a gerência de segurança em redes;
- demonstrar a viabilidade da implantação de mecanismos de QoS em uma rede WAN, usando DiffServ como forma de melhoria do nível de serviço apresentado para as aplicações; e
- verificar o comportamento de aplicações de voz e "*video streaming*" na rede com QoS habilitado e não habilitado na presença e na ausência de tráfego em *background*.

Para o cumprimento desses objetivos, foram montados dois ambientes de testes, constituídos por redes de longa distância, onde foram realizados um conjunto de experimentos para avaliar o grau de efetividade dos mecanismos da arquitetura DiffServ na priorização do tráfego gerado pelas aplicações diferenciadas que compartilham a largura de banda com tráfego melhor esforço.

1.3 Necessidade de QoS

Logo no surgimento do IETF [27], uma frase se tornou popular: "*IP over everything*" ou IP sobre tudo ou qualquer coisa. Esta frase caracterizava a capacidade do protocolo IP de operar praticamente sobre qualquer meio de transmissão e comunicar-se através de qualquer plataforma de sistema. Com o alto crescimento da Internet nos últimos anos, o surgimento de um grande número de novas aplicações, a convergência de outras redes, telefone, rádio e televisão tendo a Internet como meio de comunicação, *"Everything Over IP"* ou tudo sobre IP é certamente a frase adequada para os dias atuais.

1.3.1 O protocolo IP e a Internet

Este crescimento acentuado na utilização da rede, mencionado anteriormente, tem um custo. O tráfego aumentou, assim como o número de usuários e aplicações. Entretanto, o aumento crescente da largura de banda para o transporte de dados não é, em muitos casos, suficiente para acomodar este aumento de demandas. O tráfego na Internet e nas Intranets corporativas não só aumentou, como também mudou suas características. Aplicações novas têm exigências de novos serviços, e como resultado, a Internet precisa mudar também.

O protocolo IP possibilitou uma rede global com uma variedade infinita de sistemas e meios de transmissão. Troca de e-mails e navegação na WEB fazem parte do dia a dia das pessoas a título de trabalho, estudo e lazer. Outras redes como a de telefonia, de rádio e de televisão também estão convergindo para IP aproveitado-se de sua grande abrangência e flexibilidade. Com estas novas redes aparecem novas aplicações e novos usuários. Não há nenhum sinal que o crescimento fenomenal da Internet irá diminuir tão cedo [53].

1.3.2 Roteamento IP

Uma razão para sucesso do IP é sua simplicidade. O princípio fundamental de projeto do IP é derivado do "argumento fim-a-fim" (*end-to-end*) que põe a inteligência nas extremidades da rede (no nó fonte e no nó destino) deixando os nós intermediários, no núcleo da rede, com pouca inteligência. Por exemplo, os roteadores IP, ao longo da rede, necessitam somente conferir o endereço destino do pacote IP contra uma tabela de roteamento para determinar o próximo nó (*next hop)* para um pacote IP. Se a fila para o próximo nó for longa, o pacote pode ser atrasado. Se a fila estiver cheia ou indisponível, é permitido ao roteador IP descartar o pacote. O resultado é que o IP provê um serviço do tipo "melhor esforço" que está sujeito a atrasos imprevisíveis e perdas de dados.

1.3.3 Exigências das aplicações

Redes existem para apoiar aplicações. Como resultado, aplicações impulsionam e motivam avanços na rede. Diferentes aplicações possuem exigências operacionais diferentes que exigem serviços de rede diferentes. O aumento de tráfego na rede requer aumento da capacidade de largura de banda, mas como já foi dito, aplicações como telefonia sobre IP têm outras exigências e o simples aumento de largura de banda pode não ser a única solução ou pode ser somente parte da solução. Neste sentido, algumas aplicações requerem que as redes IP ganhem um pouco mais de inteligência.

Tipo de taxa	Descrição
Fluxo constante	Entrega previsível a uma taxa de bits relativamente constante – CBR (*Constant Bit Rate*). Fluxos de áudio e vídeo geralmente são considerados CBR porque eles têm limites superiores quantificáveis, embora suas taxas flutuem freqüentemente.
Rajada	Entrega imprevisível de "blocos" de dados a uma taxa de bits variável, VBR (*Variable Bit Rate*). Aplicações como transferência de arquivos que movimentam grandes volumes de dados podem aumentar a taxa de bits de modo a usar toda a largura de banda disponível (nenhum limite superior).

Tabela 1-1 - Formas de caracterizar taxas de bits de aplicações em termos de previsibilidade relativa

Em [53] define-se que aplicações de rede podem ser caracterizadas em termos de quão previsíveis são suas taxas de dados (Tabela 1-1) e quão tolerantes são aos atrasos de entrega de dados (Tabela 1-2). Geralmente, aplicações com tráfego nos dois sentidos são mais sensíveis a atrasos que as de tráfego em um único sentido.

Tolerância a atrasos	Tipo de Entrega	Descrição
Alta	Assíncrono	Nenhuma restrição quanto ao tempo de entrega.
	Síncrono	Dados sensíveis ao tempo, porém flexível.
	Interativo	Os atrasos podem ser visíveis a usuários / aplicações, mas não afetam a usabilidade ou funcionalidade prejudicialmente.
	Isócrono	Sensível ao tempo de modo a afetar a usabilidade prejudicialmente.
Baixa	Missão Crítica	Atrasos na entrega de dados de missão-crítica incapacitam a funcionalidade e podem ter conseqüências desastrosas em alguns casos.

Tabela 1-2 - Formas de caracterizar a sensibilidade de aplicações a atrasos de entrega de dados

1.3.4 Convergência para IP

Para redes de dados, a convergência para IP é um fato incontestável. Muitas tecnologias de informação e aplicações comerciais já migraram para IP e outras estão em mudança. Em termos de exigência de rede, a maioria das aplicações possui baixa prioridade e baixo requisito de largura de banda e alta tolerância a atrasos, mas outras têm rígidas exigências operacionais.

As redes de rádio e televisão já estão convergindo para a tecnologia IP [53], mas ainda há um longo caminho a percorrer. Primeiramente, é necessário aumentar a largura de banda, e isso já está acontecendo. O modelo de difusão em *broadcast* (de um para todos) atual é um ponto de partida para o modelo IP *multicast*, (de um para muitos). Os serviços de difusão *broadcast* atingem milhões de clientes simultaneamente e o modelo *unicast* (de um para um) na Internet nunca poderia atingir estes níveis.

Conseqüentemente, o desenvolvimento de *multicast* é necessário para habilitar a convergência de redes de televisão e rádio para IP.

O valor agregado que as redes IP podem prover para aplicações de áudio e vídeo é elevado, pois habilitam novas dimensões ao conteúdo da multimídia, tais como:

- inclusão de ligações WEB ou, simultaneamente, envio de *slides* e arquivos ou outro conteúdo durante a transmissão para enriquecer a entrega;
- comunicação nos dois sentidos, permitindo aos receptores de conteúdo interagir com provedores e, como *multicast* permite aos receptores falarem entre si na forma de muitos-para-muitos, as redes IP abrem a porta a uma nova geração de aplicações com novas possibilidades, tais como:
    - grupos de discussão;
    - ensino a distância com interatividade;
    - jogos e espetáculos; e
    - pesquisas instantâneas.

As redes IP fornecem o potencial para audiências globais, de forma econômica, e focadas em determinados nichos. Mas antes que este potencial todo possa estar disponível, há outras exigências de serviços de rede para satisfazer além de *multicast*.

Para aplicações interativas em tempo real como telefonia sobre IP, os requisitos de tempo são mais significativos que os de largura de banda, onde os requisitos são modestos, entre 8 Kbps e 14 Kbps por fluxo [53], dependendo da qualidade desejada. Duas pessoas conversando, tem evidências imediatas sobre a qualidade ou falta de qualidade em uma chamada. Perdas e atrasos são notados e atrapalham. Atrasos na entrega fim-a-fim, superiores a 500ms podem inviabilizar a chamada. Atrasos no roteamento e perdas de pacotes em redes de trânsito congestionadas, pela natureza imprevisível do tráfego em rajadas, resultam em tempos de ida e volta inadequados em redes IP e que limitam severamente a utilização de serviços de telefonia sobre IP.

O incremento na largura de banda melhora o serviço IP resolvendo o problema do atraso. Entretanto, somente isto não é suficiente para satisfazer os requisitos de aplicações como a de telefonia.

1.3.5 Largura de banda

Aumento de largura de banda é inevitável principalmente devido aos aspectos abordados nos itens 1.3.3 e 1.3.4 e a solução mais simples para controlar os períodos de pico decorrentes de tráfego em rajada é o super dimensionamento da rede, para que esta possa prover excesso de largura de banda, antecipando-se a esses períodos. Porém isto não é economicamente viável, pelo menos com a tecnologia e infra-estrutura atual. Desde que as taxas de picos de dados e as regiões de rede nas quais eles podem acontecer raramente são possíveis de predizer, esta não é uma alternativa realista [53].

O serviço do tipo melhor esforço não pode prover sempre um serviço confiável e de boa qualidade. Até mesmo em uma rede IP relativamente descarregada, a demora na entrega pode variar o suficiente para afetar aplicações que tenham restrições de tempo.

Para prover garantias de serviço, dentro de um nível de confiança quantificável, os serviços IP devem ser complementados. E isto requer acrescentar alguma funcionalidade à rede para que esta possa diferenciar o tráfego e habilitar níveis de serviço diferentes para os usuários e aplicações diferentes. *Em outras palavras, redes IP precisam de administração de largura de banda ativa.*

1.4 Organização do trabalho

Inicialmente são examinadas definições e conceitos relacionadas à qualidade de serviço em redes de computadores bem como a sua necessidade. Ao longo do trabalho são apresentadas fundamentações teóricas e os resultados de uma avaliação experimental efetuada através da medição de alguns parâmetros utilizados para verificação dos níveis de desempenho da rede e de fluxos individuais.

Os 10 capítulos desta dissertação, de forma resumida, apresentam os seguintes conteúdos:

Capítulo 1: Introdução - Neste capítulo são apresentados os objetivos do trabalho e a sua justificativa em termos de necessidades de QoS, que é discutida num contexto de convergência de diversas formas de comunicação existentes em redes dedicadas, tal como na rede de voz, para um ambiente compartilhado sobre redes IP. Ainda neste capítulo, apresenta-se a forma de organização do trabalho.

Capítulo 2: Definições e Conceitos Relacionados a QoS - Neste capítulo são apresentadas resumidamente, definições e conceitos relacionados a Qualidade de Serviço em redes de computadores, escopo deste trabalho. Também fazem parte deste capítulo uma introdução sobre os mecanismos de QoS existentes, como estes estão sendo utilizados e uma visão geral do que QoS pode prover.

Capítulo 3: Mecanismos para Controle de Tráfego em Redes IP - Neste capítulo são descritos os dois principais mecanismos para controle de tráfego e provimento de QoS em redes IP, quais sejam, a arquitetura de Serviços Diferenciados (DiffServ) e a de Serviços Integrados (IntServ). Ao final é feita uma comparação entre ambas.

Capítulo 4: Mecanismos de Enfileiramento e Policiamento do Tráfego - Mecanismos de priorização de tráfego como os implementados em DiffServ são suportados pelas camadas subjacentes da rede através de disciplinas de enfileiramento e pelos métodos de policiamento ou formatação de tráfego. Neste capítulo é dada uma visão geral sobre as principais disciplinas de enfileiramento e métodos de policiamento de tráfego atualmente em uso nas redes.

Capítulo 5: Métricas de QoS e Sua Medição - Este capítulo aborda questões conceituais e práticas relacionadas à medição em redes IP. Neste estudo a medição de QoS é considerada um caso particular de medição IP, porém fica demonstrado que existem certas dificuldades, notadamente associadas à precisão das medições.

Capítulo 6: Descrição dos Experimentos – Neste capítulo são descritos os experimentos e o método de medição utilizado, incluindo a descrição das ferramentas, parâmetros de classificação e policiamento do tráfego, entre outros.

Capítulo 7: Resultados e Análise – Fase I - Neste capítulo são apresentados os resultados experimentais na utilização de DiffServ para prover QoS em redes IP. Os resultados da fase I dizem respeito à avaliação da efetividade dos mecanismos de isolamento de tráfego e à alocação da largura de banda para fluxos nas classes de tráfego EF, AF e BE. Neste capítulo também são efetuadas coletas de informações nos

roteadores com DS habilitado, permitindo ter-se uma visão do comportamento da rede em termos de descarte, marcação e coloração de pacotes.

Capítulo 8: Resultados e Análise – Fase II – Este capítulo descreve os resultados dos experimentos realizados na fase II do trabalho. São utilizados dois ambientes, um com nós DS IBM e outro com nós DS CISCO, para avaliação dos parâmetros de atraso, variação do atraso e taxa de perdas quando se utiliza a classe de serviços EF para prover QoS na rede.

Capítulo 9: Conclusões - Neste capítulo são apresentadas as conclusões finais do trabalho, as principais contribuições e as perspectivas de trabalhos futuros nesta área.

Capítulo 10: Referências – A bibliografia utilizada e as referências bibliográficas são apresentadas neste capítulo.

Anexo I – Configuração DS ambiente IBM **–** Neste anexo são mostradas as configurações realizadas nos roteadores que compõem o ambiente DS IBM. São detalhados também o significado e valores que podem ser assumidos pelos diversos parâmetros.

Anexo II – Configuração DS no ambiente CISCO - Neste anexo são mostradas as configurações realizadas nos roteadores que compõem o ambiente DS CISCO. São detalhados também o significado e valores que podem ser assumidos pelos diversos parâmetros.

Anexo III – Ferramentas de geração e medição do tráfego – Neste anexo as diversas ferramentas de geração e medição de tráfego utilizadas são descritas. São mostrados também os *scripts* e parâmetros utilizados.

2 DEFINIÇÕES E CONCEITOS RELACIONADOS A QOS

2.1 Considerações iniciais

No capítulo anterior verificou-se que a convergência para IP é uma realidade, e que em conseqüência disto, a Internet precisa mudar para acomodar as demandas das novas aplicações. Verificou-se também que a ampliação da largura de banda é necessária, mas não suficiente; é necessário que esta seja administrada.

Até o momento, o IP tem fornecido serviço de "melhor esforço" onde os recursos da rede são divididos de forma igualitária. A adição de QoS na rede representa uma mudança significativa pois possibilita o tratamento diferenciado de serviços. Entretanto, modifica o princípio fundamental da simplicidade que fez o sucesso da Internet.

Por outro lado, novos serviços sobre IP estão sendo criados, gerando novas oportunidades e incentivando o suporte a QoS, que é essencial em aplicações de comunicação em tempo real envolvendo áudio e vídeo. Neste capítulo, QoS em redes IP será melhor contextualizado e definido. Uma relação mais completa sobre conceitos, termos e definições associadas a QoS pode ser encontrada em [54].

2.2 O que é qualidade de serviço (QoS)

Não existe uma única expressão para definir qualidade de serviço. Num passado ainda recente, QoS (*Quality of Service*) tinha conotações mais específicas para algumas tecnologias de rede, tal como ATM, mas o termo é agora mais amplamente usado. Fala-se de QoS nos sistemas de armazenamento em disco, nos sistemas operacionais, além de outros. Para a área de redes, refere-se à habilidade que uma rede tem de prover melhor serviço para um determinado tráfego em tecnologias como: IP, Frame-Relay, ATM, Ethernet com o padrão IEEE 802.1 e outras [15].

Em [53], a Qualidade de Serviço é definida como a capacidade da rede prover serviço de encaminhamento de dados de forma consistente e previsível. Em outras palavras, é a capacidade de satisfação das necessidades das aplicações dos usuários. Em [23], qualidade de serviço é definida como a habilidade de um elemento da rede, seja uma aplicação, *host*, roteador, ou outro dispositivo, ter algum nível de garantia que seu tráfego e exigências de serviço podem ser satisfeitas.

Para Ben Teitelbaum [56] QoS é um termo que freqüentemente possui duplo significado: refere-se ao desempenho de uma rede em relação as necessidades de uma aplicação e ao conjunto de tecnologias que permitem a rede satisfazer estas garantias de desempenho.

No contexto deste trabalho Qualidade de Serviço é entendida como a capacidade da rede, através dos mecanismos de reserva de largura de banda e priorização de tráfego, em fornecer garantias de que determinados fluxos de tráfego irão ter tratamento diferenciado.

2.3 Qualidade de serviço em redes IP

Habilitar QoS requer a cooperação de todos os níveis da rede, desde o topo até a base, bem como de todos os elementos da rede de fim-a-fim. Qualquer garantia de QoS será no máximo tão boa quanto o elo mais fraco na "cadeia" entre origem e destino [50].

Para QoS, disponibilidade de largura de banda é o ponto fundamental [53]. Mecanismos de QoS administram a largura de banda de acordo com as exigências da aplicação e parâmetros de configuração e administração da rede e, desta forma, não podem prover garantias nos casos onde compartilhamento estiver envolvido. Conseqüentemente, QoS com um nível de serviço garantido requer alocação de recursos a fluxos de dados individuais. A largura de banda alocada a uma aplicação em uma "reserva de recurso" não estará disponível para uso em aplicações do tipo "melhor-esforço".

Considerando que largura de banda é um recurso finito, a prioridade dos projetistas de QoS tem sido assegurar que o tráfego de melhor esforço não pereça após as reservas serem efetivadas [53]. Habilitar QoS para aplicações de alta prioridade não deve impossibilitar o uso das aplicações de baixa prioridade. No pior caso, estas últimas, devem continuar funcionando mesmo tendo um serviço mais lento.

Essencialmente existem dois mecanismos básicos disponíveis para prover QoS em redes IP:

- ***Reserva de Recursos***: os recursos da rede são divididos de acordo com os requisitos de QoS da aplicação, e sujeitos à política de administração de largura de banda. O RSVP (*Resource ReSerVation Protocol*), por exemplo, fornece os mecanismos para implementação de serviços integrados (IntServ) [10] baseado na reserva de recursos.

- ***Priorização***: o tráfego da rede é classificado e os recursos de rede são divididos de acordo com critérios de políticas de administração de largura de banda. Para habilitar QoS os mecanismos de classificação dão tratamento preferencial a aplicações identificadas como tendo requisitos mais exigentes. A arquitetura de Serviços Diferenciados [DiffServ] [9], [22] provê este tipo de serviço.

Estes dois grupos de protocolos de QoS e algoritmos não são mutuamente exclusivos. Ao contrário, eles são complementares. Ou seja, eles são projetados para uso em conjunto, de forma a acomodar diferentes exigências operacionais em diferentes contextos de redes.

2.4 Modelos de qualidade de serviço fim-a-fim

Um modelo de serviço, também chamado nível de serviço, descreve um conjunto de capacidades de QoS fim-a-fim. QoS fim-a-fim é a habilidade da rede em prover o serviço requerido por um tráfego específico de uma extremidade a outra da rede [12].

2.4.1 Serviço de melhor esforço

Este serviço também é conhecido como sem QoS e, provê simplesmente a conectividade básica sem garantias. A Internet de hoje é um bom exemplo de serviço de melhor esforço. Embora o serviço de melhor esforço não ofereça QoS, ele proporciona um ponto de referência quanto à rigidez da especificação e, apesar de não oferecer garantias, é adequado para uma grande gama de aplicações de rede, tais como, correio eletrônico e transferência de arquivos, pois estas adaptam-se facilmente às condições da rede.

2.4.2 Serviço diferenciado

Nessa abordagem uma porção do tráfego é tratada de forma privilegiada sobre o restante. É oferecida manipulação mais rápida, mais largura de banda na média e menor

taxa de perda. Esta é uma preferência estatística, não uma garantia rígida. Com métodos adequados, incluindo a utilização de determinadas políticas nas extremidades da rede, a arquitetura de serviços diferenciados pode prover um tratamento adequado para uma boa gama de aplicações, incluindo aquelas de missão crítica, as que necessitam de baixo atraso, aplicações de voz sobre pacotes, e outras. Na maioria das vezes, serviços diferenciados estão associados com a classificação do tráfego. O tráfego é agrupado em um pequeno número de classes e cada classe recebe uma Qualidade de Serviço na rede.

O grupo de trabalho *Differentiated Services* (DiffServ) do IETF está trabalhando na especificação e definição de um padrão para os serviços de rede sob o nome genérico de Serviços Diferenciados. Este esforço está focado em grande parte no uso do campo TOS (Tipo de Serviço) do cabeçalho do IPv4, agora chamado campo DS (*Differentiated Service*), como um mecanismo de sinalização de QoS. A Figura 2-1 ilustra o uso deste campo. Os bits de 0 a 5 representam o DSCP (*Differentiated Service Code Point*), os bits 6 e 7 não são utilizados.

Figura 2-1 - Campo DS do cabeçalho do IPv4

Na seção 3.3 a arquitetura de serviços diferenciados é descrita em detalhes.

2.4.3 Serviço integrado

Serviço integrado é um modelo de serviço múltiplo que pode acomodar múltiplos requisitos de QoS. Neste modelo a aplicação solicita um tipo específico de serviço da rede antes de enviar os dados. A solicitação é feita através de uma sinalização explicita; a aplicação informa à rede seu perfil de tráfego e requisita um tipo específico de serviço capaz de satisfazer suas exigências de largura de banda e atraso. É esperado da aplicação que os dados sejam enviados somente após receber confirmação da rede e que estes estejam dentro do perfil de tráfego descrito.

Tipicamente, serviços integrados estão associados com o nível de classificação do tráfego e, muitas vezes, refere-se ao nível de fluxo individual, ou seja, determinados fluxos devem ter recursos de rede reservados para alcançarem suas exigências.

O grupo de trabalho *Integrated Services* (IntServ) [28] do IETF desenvolveu padrões e definições específicas para o serviços definidos sob o termo genérico de Serviços Integrados. Este esforço tentou prover uma arquitetura consistente para especificar fluxos na Internet com exigências variadas. Os serviços primários em uso são o Serviço de Carga Controlada e o Serviço Garantido. O RSVP foi desenvolvido como um mecanismo de sinalização de QoS para prover serviços baseados nestes tipos de fluxo. Na seção 3.2 serviços integrados serão descritos em detalhes.

2.5 Requisitos essenciais em redes com QoS

Em [50] define-se um conjunto de requisitos considerados essenciais para redes que implementam mecanismos de QoS. Estes incluem a minimização do atraso fim-a-fim e da variação do atraso (*jitter*), a minimização da taxa de perda de pacotes e o provimento de vazão de dados e largura de banda consistente conforme detalhado nas sessões que seguem:

2.5.1 Atraso fim-a-fim

É o tempo entre o envio de uma mensagem por um nó e a recepção desta mensagem pelo nó destino. Este atraso ocorre no caminho de transmissão ou em um dispositivo no caminho de transmissão. Em um roteador, o atraso é o montante de tempo entre a recepção do pacote e a sua transmissão. Este tempo é também referido como atraso de propagação.

2.5.2 Variação do atraso (*jitter*)

Em redes de pacotes, *jitter* é uma distorção ocorrida nos tempos de chegada entre pacotes comparados aos tempos originais de transmissão entre pacotes. É uma distorção que acontece, por exemplo, quando fluxos de voz ou vídeo são transmitidos em uma rede e os pacotes não chegam no seu destino dentro da ordem sucessiva ou em uma determinada cadência. Ou seja, eles variam em termos de tempo de atraso. Esta

distorção é particularmente prejudicial ao tráfego multimídia, fazendo com que o sinal de áudio ou vídeo tenham uma qualidade distorcida ou fragmentada na recepção.

2.5.3 Perda de pacotes

A perda de pacotes representa o número de pacotes que foram transmitidos na rede, mas não alcançaram seu destino em um determinado período de tempo. Para ilustrar, tem-se que a média mensal de perda de pacotes total na rede deve ser menor que 1% [54].

2.5.4 Largura de banda e vazão

Largura de banda é uma medida de capacidade de transmissão de dados, normalmente expressa em kilobits por segundo (Kbps) ou megabits por segundo (Mbps). A *largura de banda* indica a capacidade máxima de transmissão teórica de uma conexão. Entretanto, na medida em que a taxa de transmissão utilizada se aproxima da *largura de banda* teórica máxima, fatores negativos como atraso na transmissão das informações podem causar deterioração na qualidade. *A largura de banda* de uma rede pode ser vista como um tubo que transfere dados. Quanto maior o diâmetro do tubo, mais dados podem ser enviados através dele simultaneamente.

A *vazão* é o montante de tráfego de dados movidos de um nó da rede para outro em um determinado período de tempo. A vazão também é expressa em Kbps ou Mbps.

2.6 Considerações finais sobre este capítulo

Neste capítulo foi definido QoS em redes de pacotes de uma forma geral. Foram introduzidos os modelos de qualidade de serviço fim-a-fim para redes IP, bem como os requisitos necessários às redes que oferecem QoS. No próximo capítulo serão examinadas com mais detalhes e comparadas a arquitetura DiffServ e a Arquitetura IntServ.

3 MECANISMOS PARA CONTROLE DE TRÁFEGO EM REDES IP

Subjacentes a qualquer mecanismo de controle de tráfego existem um conjunto de filas e algoritmos para sua manutenção, bem como mecanismos de policiamento ou formatação do tráfego. No capítulo 04 - são examinados alguns desses algoritmos e os dois principais métodos utilizados para policiamento do tráfego.

Neste capítulo são examinadas as duas principais arquiteturas para controle de tráfego em redes IP:

- a arquitetura de Serviços Integrados (IntServ); e
- a arquitetura de Serviços Diferenciados - (DiffServ).

Cada um desses mecanismos é apropriado a circunstâncias e mídias específicas como descrito nas seções que seguem.

3.1 Tipos de mecanismos para controle de tráfego

Os mecanismos de controle de tráfego podem ser categorizados em mecanismos por conversação e em mecanismos por agregação [35].

3.1.1 Mecanismos para controle de tráfego por conversação

Mecanismos para controle de tráfego por conversação são mecanismos que controlam cada conversação como um fluxo separado. Neste contexto, uma conversação inclui todo o tráfego entre uma instância de uma aplicação específica em um *host,* e uma outra instância de uma aplicação par em outro *host.* No caso de tráfego IP, o endereço IP fonte e destino, porta e protocolo identificam de forma única a conversação. Tradicionalmente, mecanismos IntServ são fornecidos por conversação[28], [35].

Quando o tráfego é controlado por conversação, os recursos são alocados também por conversação, sob a perspectiva da aplicação. Isto significa que ao tráfego da aplicação é garantido recurso completamente independente do efeito do tráfego de outras conversações similares da rede. Estes mecanismos tendem a melhorar a qualidade de serviço experimentado pela aplicação, mas impõem maior carga ao equipamento de rede que deve manter o estado independente e aplicar processamento independente para cada

conversação. No núcleo de grandes redes, onde é possível ocorrer milhares de conversações simultaneamente, essa modalidade de controle pode não ser prática.

3.1.2 Mecanismos para controle de tráfego por agregação

Nos mecanismos de controle de tráfego agregado, um conjunto do tráfego de múltiplas conversações é classificado para o mesmo fluxo e é controlado de forma agregada. Diffserv e IEEE 802.1p são exemplos de mecanismos de controle de tráfego agregado, respectivamente, nas camadas 3 e camada 2 do modelo de referência OSI. Em ambos os mecanismos, pacotes correspondentes a conversações múltiplas são marcados com as mesmas marcas DSCP (*Differentiated Services Code Point)* ou IEEE 802.1p [35].

Quando o tráfego é controlado de forma agregada, a carga de processamento e manutenção de estado nos dispositivos do núcleo de uma grande rede é reduzida significativamente. Por outro lado, a qualidade de serviço percebida na conversação de uma aplicação não é independente do efeito do tráfego de outras conversações que foram agregadas no mesmo fluxo. Como resultado, no controle de tráfego agregado, a qualidade do serviço percebida por uma aplicação pode não ser muito consistente [35]. Alocação de recursos em excesso para uma classe de tráfego agregado pode reduzir este efeito. Entretanto, esta abordagem tende a reduzir a eficiência de utilização dos recursos da rede.

3.2 Serviços integrados

Os Serviços Integrados (*Integrated Services* ou IntServ) [10] [28], propostos pelo IETF *(Internet Engineering Task Force),* foram projetados para prover um conjunto de extensões ao modelo de entrega de tráfego de melhor esforço atualmente utilizado nas redes com tecnologia IP em geral, incluindo a Internet [10]. Em essência, eles foram projetados para dar tratamento especial para certos tipos de tráfego e prover um mecanismo para que as aplicações possam escolher entre múltiplos níveis de serviços de entrega para seu tráfego. IntServ é baseado na reserva de recursos, ou seja, antes que os dados sejam transmitidos, as aplicações devem primeiro configurar caminhos e reservar recursos. O RSVP [23] é um protocolo de sinalização para esse fim.

O modelo de Serviços Integrados como já citado em 2.4.3 propõe duas classes de serviço em adição ao Serviço Melhor Esforço:

- **Serviço Garantido** (***Guaranteed Service***) [49]: fornece limites rígidos, matematicamente prováveis em termos de atrasos de enfileiramento, aos quais os pacotes estarão condicionados nos roteadores. Ele garante tanto o atraso quanto a taxa de bits. Basicamente, uma sessão requisitando Serviço Garantido está requerendo que os bits em seus pacotes tenham uma taxa de transmissão garantida. Deve-se notar que este serviço não tenta minimizar a variação de atraso, mas controlar o atraso máximo de enfileiramento. Para este tipo de serviço, todos os nós intermediários devem implementar os serviços garantidos. Este serviço pode ser útil para aplicações requerendo limites de atraso fixos, tais como as de áudio e vídeo em tempo-real.

- **Serviço de Carga Controlada** (***Controlled Load Service***) [57]: uma sessão requerendo tal serviço receberá uma QoS muito próxima daquela que um fluxo poderia receber de uma rede não sobrecarregada. Em outras palavras, a sessão pode assumir que uma "percentagem muito alta" de seus pacotes passará com sucesso através do roteador sem ser cortada e com um atraso de enfileiramento muito próximo a zero. O Serviço de Carga Controlada não fornece garantias quantitativas acerca do desempenho – ele não especifica o que constitui uma "percentagem muito alta" de pacotes, nem que qualidade de serviço aproximada será fornecida por um elemento de rede não sobrecarregado. Este tipo de serviço é dirigido para aplicações em tempo-real adaptativas como as que estão sendo desenvolvidas atualmente na Internet. Estas aplicações funcionam razoavelmente bem quando a rede não está sobrecarregada, mas elas se degradam rapidamente quando a rede fica congestionada.

No modelo IntServ os roteadores devem ser capazes de reservar recursos a fim de fornecer QoS especial para fluxos de pacotes específicos do usuário. Neste caso, o estado específico dos fluxos deve ser mantido pelos roteadores. Este modelo é implementado por quatro componentes (Figura 3-1):

- **protocolo de sinalização:** aplicações necessitando de Serviço Garantido ou Serviço de Carga Controlada devem configurar um caminho e reservar recursos antes da transmissão de seus dados. Para isto elas devem usar um protocolo de sinalização como o RSVP, por exemplo.

- **rotina de controle de admissão:** decide se um pedido de alocação de recursos pode ser garantido. Ela implementa o algoritmo de decisão que um roteador ou *host* usa para determinar se um novo fluxo pode ter sua QoS garantida sem afetar fluxos anteriormente garantidos.

- **classificador:** quando um roteador recebe um pacote, o classificador executa uma classificação Multi-Campo (MF – *Multi-Field*) e coloca o pacote em uma fila específica em função do resultado da classificação. A classificação MF é o processo de classificar pacotes, baseado no conteúdo dos seus campos tais como: endereço fonte, endereço destino, byte TOS[4] (*Type of Service*) e identificador do protocolo[5]. Cada pacote que chega deve ser mapeado em alguma classe; todos os pacotes na mesma classe obtêm o mesmo tratamento do escalonador. Uma classe pode corresponder a uma grande categoria de fluxos. Por exemplo, todos os fluxos de vídeo, ou, todos os fluxos atribuíveis a uma organização particular. Por outro lado, uma classe pode manter apenas um único fluxo. Uma classe é uma abstração que pode ser local a um roteador particular. O mesmo pacote pode ser classificado de várias formas por diferentes roteadores ao longo do caminho. Por exemplo, roteadores de *backbone* podem escolher o mapeamento de muitos fluxos em poucas classes agregadas, enquanto que roteadores periféricos, onde existe menos agregação, podem usar uma classe separada para cada fluxo.

---

[4] Campo de 8 bits do cabeçalho do datagrama IP: 3 bits mais significativos indicam a natureza e prioridade do datagrama; TOS (4 bits) especifica o tipo de serviço: minimiza atraso, maximiza vazão, maximiza confiabilidade, minimiza custos monetários, serviço normal; e o bit menos significativo é reservado. Geralmente este campo é ignorado pelos roteadores.

[5] Especifica qual protocolo de alto nível foi usado para criar a mensagem que está sendo transportada na área de dados do datagrama.

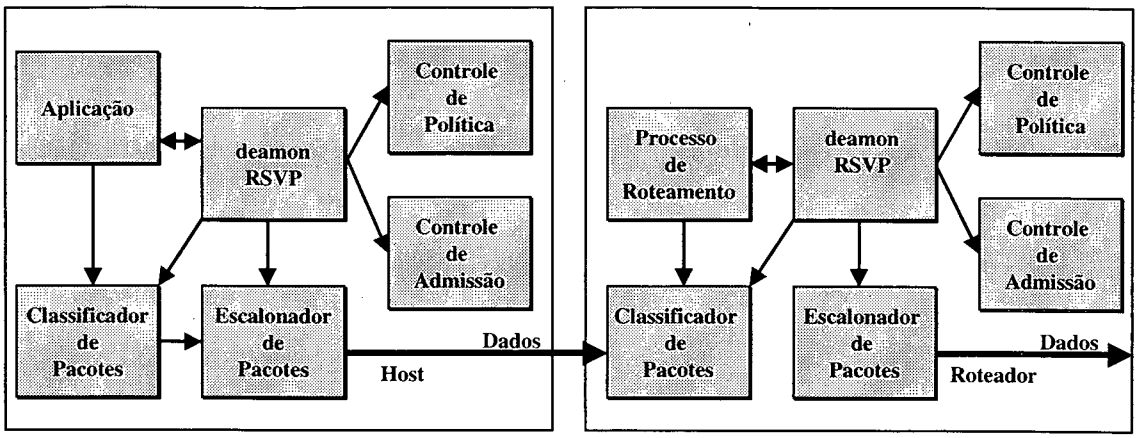


Figura 3-1- RSVP nos *hosts* e roteadores

- **escalonador de pacotes:** após a classificação, o escalonador seleciona para transmissão o pacote de modo a satisfazer os requisitos de QoS. O escalonador de pacotes gerencia a retransmissão dos diferentes pacotes usando um conjunto de filas, tal como definido na seção 4.1, e outros mecanismos tais como temporizadores.

Na Internet atual, a retransmissão IP é completamente igualitária: todos os pacotes recebem a mesma qualidade de serviço e os pacotes são retransmitidos usando uma fila First In First Out (ver seção 4.1.1). Para IntServ, um roteador deve implementar uma QoS apropriada para cada fluxo de dados, de acordo com o modelo de serviço. A função do roteador que cria diferentes qualidades de serviço é chamada de controle de tráfego. Controle de tráfego é implementado pelos componentes escalonador de pacote, classificador e controle de admissão, mastrados na Figura 3-1.

3.3 Serviços diferenciados

3.3.1 Visão geral

A arquitetura de Serviços Diferenciados (Differentiated Services, DiffServ ou DS) [9] posiciona-se entre os extremos do melhor esforço (BE - sem priorização) e Serviços Integrados [10], [50] com reserva de recursos e grande sobrecarga de sinalização. Na arquitetura DiffServ não existe alocação explícita de recursos e não é feita sinalização, tendo em vista que a prioridade do pacote é transmitida no cabeçalho IP, permitindo desta forma maior escalabilidade e baixa sobrecarga de sinalização.

O diagrama da Figura 3-2 mostra onde os componentes-chave de uma rede DiffServ são empregados. Diffserv define o conceito de domínio DS, que é um conjunto contíguo de nós DS que aplicam um conjunto comum de políticas sobre o tráfego que atravessa o domínio. Um domínio DS tem nós de borda e nós de interior [9] e [33]. Os nós DS de borda são responsáveis pela classificação e condicionamento do tráfego que entra no domínio DS.

Para cada fluxo de tráfego entrando no domínio pelos nós de borda, a política de QoS define qual terá um serviço diferenciado, como este deverá ser marcado nos nós de borda e como será tratado pelos nós interiores. Estes, por sua vez, examinam a marcação dos pacotes e atuam de acordo com as políticas definidas ou seu perfil de tráfego.

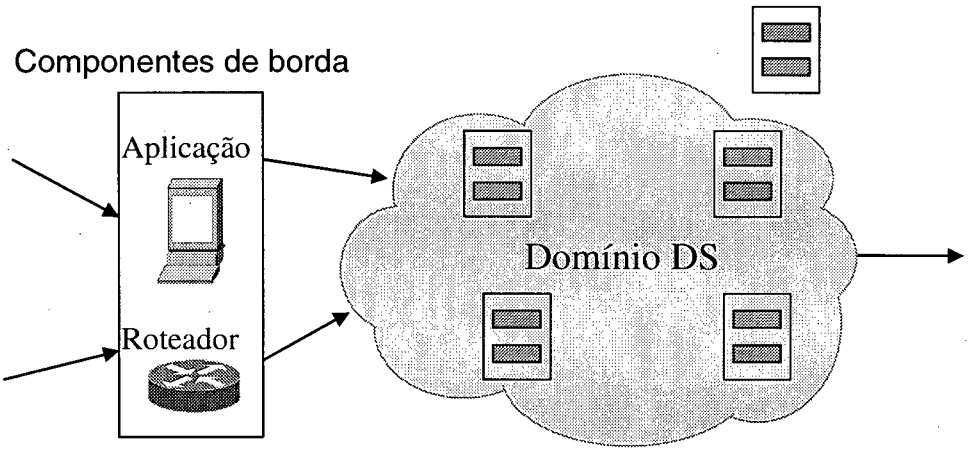


Figura 3-2 – Serviços diferenciados – visão geral

3.3.1.1 Classificação e condicionamento do tráfego

A arquitetura DiffServ define dois importantes componentes nos nós DS conforme mostra a Figura 3-3: os componentes de classificação e de condicionamento de tráfego. Estas funções são mais complexas em nós DS de borda que em nós de interior, mas ambos os nós têm um classificador.

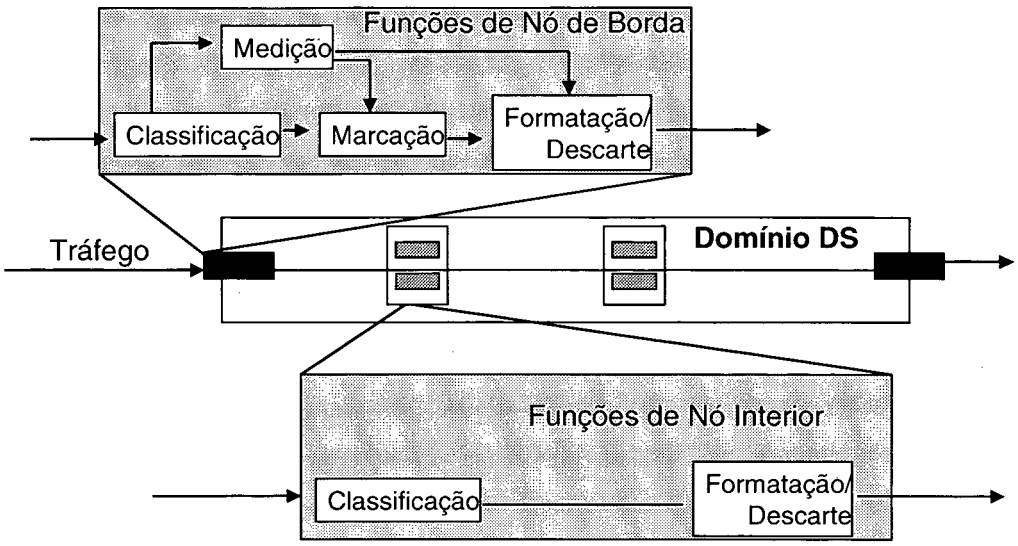


Figura 3-3 – Roteador que implementa arquitetura DiffServ

Existem dois tipos de classificadores: um que classifica o fluxo baseado apenas na classificação DS e outro que verifica múltiplos campos no cabeçalho IP. Estes classificadores são conhecidos como classificador de comportamento agregado (BA – *behaviour agregate*) e classificador multi-campo (MF – *multifield classifier*), respectivamente. A marca de classificação DS é conhecida como *DS codepoint* ou DSCP.

Em nós DiffServ o ***classificador*** [33] é o componente que divide o fluxo de entrada em um conjunto de fluxos de saída por meio de filtros de tráfego baseados no conteúdo do cabeçalho do pacote e/ou em diferentes atributos do pacote que podem ser implicitamente derivados.

De acordo com a chegada do pacote o ***medidor*** verifica se o pacote está de acordo com um perfil de tráfego pré-definido. Dependendo da conformidade várias ações podem ser executadas, através dos *elementos de ações*. Três tipos de ações, e a combinação delas, podem ser executadas: *Marcação, formatação e descarte*.

Escalonamento é o processo de decidir no momento da transmissão qual fila entre o conjunto de candidatas deve ser servida, dependendo de alguma propriedade da fila e/ou do pacote. Geralmente ele é empregado no caso de contenção de recursos na saída. A ação de ***Formatação*** ou policiamento modifica o tráfego de entrada para forçar um determinado perfil de saída.

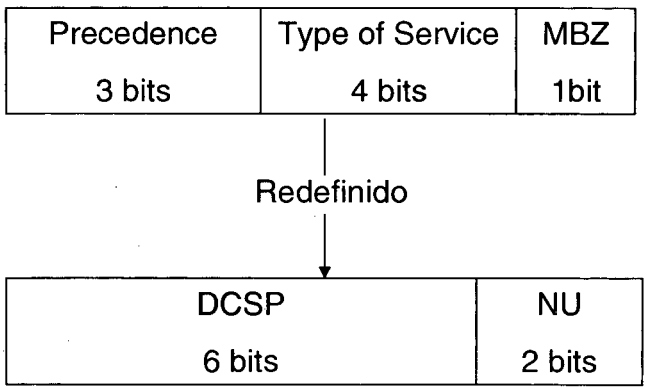
Uma ***fila***, por sua vez, é uma área de memória necessária para executar escalonamento e/ou formatação.

Condicionadores *de tráfego* são empregados em um determinado estágio do caminho dos dados para forçar uma determinada política. Eles podem ser implementados através da combinação de um ou mais componentes de DiffServ definidos anteriormente (classificadores, medidores, elementos de ação e filas) ou, alternativamente, através da combinação de condicionadores de tráfego existentes. Marcação é um exemplo de condicionamento de tráfego.

3.3.2 Encaminhamento de tráfego - PHBs

Como foi citado, nos nós de borda, o fluxo de tráfego é classificado e marcado. Os campos DSCP (*DiffServ Code Point*) [5] são mapeados para os PHBs (*Per Hop Behaviors*) [43] definidos na arquitetura DiffServ. Os PHBs [22], [26], [31] definem o comportamento de encaminhamento de um pacote em um nó DiffServ.

PHBs são identificados através de um *label* de 6 bits, do campo TOS (*Type Of Service*) do cabeçalho do pacote IPv4 e o campo *Class* do cabeçalho do pacote IPv6 agora chamados de *Differentiated Services Code Point* (DSCP) conforme mostra a Figura 3-4,



[42] que é colocado no campo Diffserv do cabeçalho do pacote IP.

Figura 3-4 – Campo TOS versus Byte DS

Os seis bits do campo DS são usados para selecionar o PHB que o pacote terá em cada nó. Este campo é tratado como um índice em uma tabela usada para selecionar o mecanismo de manipulação de pacotes implementado em cada dispositivo. Este campo

é definido como um campo não estruturado para facilitar a definição de futuros PHBs. Outros comportamentos podem especificar que, para determinados pacotes, serão dadas certas prioridades relativas a outros, em termos de vazão média (*throughput)* ou de preferência para descarte, mas sem ênfase particular em atrasos. PHBs são implementados utilizando mecanismos de enfileiramento.

PHBs são comportamentos individuais aplicados em cada roteador, por isso isoladamente não garantem QoS fim-a-fim [35]. Entretanto, a interligação de roteadores com os mesmos PHBs e a limitação da taxa em que os pacotes são enviados para um PHB, possibilita o uso de PHBs para construir QoS de fim-a-fim. Por exemplo, a concatenação de EF PHBs ao longo de uma rota preestabelecida, com um cuidadoso controle de admissão, pode prover um serviço similar ao de uma linha dedicada, que é satisfatório para voz interativa. Uma outra concatenação de PHBs pode ser utilizada para transmissão de vídeo armazenado, e assim por diante.

O PHB *default* serve para o tráfego BE (*best effort*) melhor esforço. Ele assegura compatibilidade com o encaminhamento melhor esforço padrão em todos os roteadores e é documentado no RFC1812 [5], [33]. PHBs de tráfegos com DSCP mais alto devem ter encaminhamento preferencial sobre aqueles com valor mais baixo. Por exemplo, o PHB 111000 deve ter prioridade mais alta que 000000.

3.3.3 PHBs padrões

Dois importantes PHBs foram padronizados: o PHB EF (*Expedited Forwarding)* que é documentado no RFC2598 [31] e o PHB AF (*Assured Forwarding)* documentado no RFC2597 *[26].*

O PHB EF, também referido como serviço premium ou de canal dedicado, pode ser usado para tráfego com requisitos de baixa perda, baixo atraso, baixo *jitter* (variação de atraso) e garantia de largura de banda. Estes requisitos são alcançados assegurando-se que os agregados de tráfego encontram nenhum ou pouco enfileiramento.

As implementações devem prover meios de limitar o dano que o tráfego EF pode infligir sobre o outro tráfego. Os dispositivos de borda do domínio DS devem policiar o

tráfego EF para assegurar a taxa de bits definida. Pacotes em excesso devem ser descartados.

O PHB AF tem por objetivo fornecer entrega de pacotes IP, com largura de banda assegurada, em quatro classes de transmissão, mas não oferece garantias quanto ao atraso. Cada classe tem três precedências de descartes (*Drop Precedence*), as quais são utilizadas para determinar a importância do pacote. Assim, um nó congestionado dá preferência para serem descartados, entre os pacotes de uma mesma classe, aqueles com maiores valores de precedência de descarte.

Os três primeiros bits do DSCP identificam a classe de transmissão, 001, 010, 011 e 100 e os três últimos bits definem a precedência de descarte – 010 para a precedência mais baixa (ou seja, ultimo a ser descartado), 100 para precedência média e 110 para a mais alta precedência de descarte (ou seja, primeiro a ser descartado). Na Tabela 3-1, Tabela 3-2 e Tabela 3-3 são apresentados os DSCP recomendados para as classes de tráfego AF, BE e EF.

Precedência de descarte	Classe AF1		Classe AF2		Classe AF3		Classe AF4	
	Binário	Decimal	Binário	Decimal	Binário	Decimal	Binário	Decimal
Baixa	001010	10	010010	18	011010	26	100010	34
Média	001100	12	010100	20	011100	28	100100	36
Alta	001110	14	010110	22	011110	30	100110	38

Tabela 3-1 – PHB AF – RFC2597 – quatro classes de tráfego independentes

Precedência de descarte	Classe BE	
	Binário	Decimal
N/A	000000	0

Tabela 3-2 – PHB Default – Tráfego melhor esforço

Precedência de descarte	Classe EF	
	Binário	Decimal
N/A	101110	46

Tabela 3-3 – PHB EF – RFC2598 – Tráfego *premium*

A marcação da precedência de descartes para tráfegos AF pode seguir dois enfoques: marcador com taxa simples [24] e marcador com taxa dupla [25]. Ambos usam um regulador do tipo duplo balde furado (*Dual Leaky Bucket*), sendo que no marcador

simples, os dois baldes são preenchidos na mesma taxa e no marcador com taxa dupla, os baldes são preenchidos com duas taxas diferentes. Ambos os enfoques medem o tráfego e marcam o pacote, dependendo se o fluxo excede a taxa acordada ou contratada CIR (*Committed Information Rate*). Um pacote é marcado como *verde*, *amarelo* ou *vermelho* dependendo em quanto o CIR foi excedido. Um pacote *verde* tem a menor prioridade de descarte, enquanto que um pacote *vermelho*, a mais alta. O principal objetivo é fornecer a marcação para algum mecanismo de descarte baseado na precedência de descartes, tal como o mecanismo RED (*random early detect*) [23] e [33].

3.3.4 Serviços em um domínio DS

Na arquitetura DiffServ ***serviço*** está associado à QoS do ponto de vista da aplicação, permitindo especificar as necessidades destas em termos de largura de banda, atraso, *jitter* e taxa de perdas, e pode ser quantitativo ou qualitativo. No primeiro caso o *serviço* é especificado através de um conjunto de métricas e valores de referência correspondentes, enquanto que no segundo caso somente uma definição de alto nível é fornecida. Em ambos os casos a implementação de QoS está baseada em uma determinada combinação dos componentes de DiffServ acima mencionados. Isto faz a arquitetura de DiffServ muito flexível.

Quanto aos serviços oferecidos por um domínio aderente a DS, devemos notar:

- serviços DS são todos para tráfego unidirecional apenas; e
- serviços DS são para tráfegos agregados, não fluxos individuais. Em [9] um Serviço é definido como o tratamento global de um subconjunto do tráfego do cliente dentro de um domínio aderente a DS ou fim-a-fim. O tráfego na rede geralmente atravessa uma concatenação de redes que podem incluir *hosts*, redes residenciais e de escritório, redes corporativas/campus e várias redes de longa distância. Redes residenciais e de escritório são normalmente clientes de redes de campus ou corporativas, que são por sua vez clientes de redes de longa distância. Note-se que existem várias fronteiras, cliente-provedor, em que o conceito de serviço se aplica.

Os clientes podem marcar os campos DS dos pacotes para indicar o serviço desejado, ou estes campos podem ser marcados pelo roteador de borda que liga o cliente à rede,

baseado na classificação MF. No ponto de ingresso da rede, os pacotes são classificados, policiados e, possivelmente, atrasados para torná-los aderentes a algum perfil de tráfego pré-definido. As regras de classificação, policiamento e atrasos usadas nos roteadores de ingresso da rede são derivadas a partir de um Acordo de Nível de Serviço (SLA – *Service Level Agreement*) [52]. O montante de espaço de bufferização necessário para estas operações também é derivado dos SLAs.

Um exemplo simples de perfil de tráfego poderia ser: medir o fluxo de pacotes do endereço IP a.b.c.d e se sua taxa ficar abaixo de 200 Kbps, marque o byte DS com o valor X, senão marque o byte DS com o valor Y. Se a taxa exceder a 600 Kbps, corte os bytes excedentes. Os perfis são configurados pelo operador de acordo com os SLAs. A maneira pela qual os perfis são fornecidos (configuração manual ou sinalização) está fora do escopo do padrão DiffServ.

3.3.5 Políticas de QoS em DiffServ

Uma política relaciona um perfil de tráfego com ações para serem efetuadas neste perfil [52] e [33]. O perfil de tráfego determina quais os requisitos (como endereços fonte e destino, portas fonte e destino, protocolo e DSCP) sob os quais um fluxo de tráfego é identificado. Uma vez classificado um pacote (identificado o seu perfil de tráfego) é aplicada à ação correspondente ao perfil identificado de acordo com sua política.

3.4 Comparação DiffServ versus IntServ

A arquitetura Serviços Integrados/RSVP representa uma mudança fundamental na arquitetura atual da Internet, que é fundamentada no conceito de que todas as informações de estado relacionadas aos fluxos deveriam estar nos sistemas finais. Neste sentido, existem alguns problemas com a arquitetura Serviços Integrados [23], [50], [58]:

- o montante de informações de estado aumenta proporcionalmente ao número de fluxos. Isto causa uma sobrecarga de armazenamento e processamento nos roteadores. Portanto esta arquitetura é pouco escalável;
- os requisitos nos roteadores são altos: todos os roteadores devem implementar RSVP, controle de admissão, classificação MF e escalonamento de pacotes;

- para Serviço Garantido, toda a rede deve suportar IntServ. Uma instalação gradativa de Serviço de Carga Controlada é possível; e
- IntServ/RSVP não são satisfatoriamente aplicáveis em aplicações do tipo navegadores WWW, onde a duração de um fluxo típico é apenas de poucos pacotes. A sobrecarga causada pela sinalização RSVP poderia facilmente deteriorar o desempenho da rede sendo percebida pela aplicação.

Por outro lado na arquitetura DiffServ, destacam-se as seguintes características:

- existência de apenas um número limitado de classes de serviço indicadas no campo DS. Desde que o serviço é alocado na granularidade de uma classe, o conjunto de informações de estado é proporcional apenas ao número de classes e não proporcional ao número de fluxos. Serviços Diferenciados é, portanto, mais escalável;
- as operações de classificação, marcação, policiamento e retardo são necessárias somente nas fronteiras das redes e dependendo das políticas definidas, os fluxos de tráfego com requisitos similares são agregados. Assim, os roteadores intermediários necessitam apenas implementar a classificação Comportamento Agregado (BA – *Behavior Aggregate*), que é uma classificação baseada apenas no byte DS. Portanto, DiffServ é mais fácil de implementar e usar; e
- no modelo Serviços Diferenciados, um Serviço Assegurado pode ser fornecido por um sistema que suporta parcialmente os Serviços Diferenciados. Os Roteadores que não suportam DiffServ simplesmente ignoram os campos DS dos pacotes e fornecem serviço assegurado ou serviço de melhor esforço. Como os pacotes de serviço assegurado têm menos probabilidade de serem descartados em roteadores compatíveis com DS, o desempenho total do tráfego de Serviço Assegurado será melhor que o tráfego Melhor Esforço.

As facilidades apontadas na comparação entre os dois modelos de provimento de QoS analisados motivaram a escolha pela implementação DiffServ. Percebeu-se que estas facilidades apontadas em termos de implementação, escalabilidade e, principalmente, o fato de não ser necessário modificar as aplicações, visto que a classificação, marcação e priorização dos fluxos de tráfego podem ser feitas nos roteadores de borda, viabilizariam a implantação imediata do serviço em ambientes de produção.

3.5 Considerações finais sobre este capítulo

Neste capítulo foi efetuada uma revisão conceitual sobre os dois principais mecanismos de controle de tráfego definidos para uso em redes IP. As arquiteturas DiffServ e IntServ foram examinadas em detalhes permitindo, desta forma, perceber as dificuldades e aplicabilidade de ambas.

Neste capítulo também foi justificada a escolha do DiffServ para a realização dos experimentos e foi também destacada a importância dos mecanismos de enfileiramento e formatação de tráfego utilizados em DiffServ e que serão examinados no próximo capítulo.

4 MECANISMOS DE ENFILEIRAMENTO E POLICIAMENTO DO TRÁFEGO

No contexto de QoS em redes IP e, em particular na arquitetura DiffServ, é permitido ao usuário a escolha das disciplinas de enfileiramento e encaminhamento de pacotes, bem como ajustar os parâmetros de configuração dos métodos de policiamento do tráfego. Por esta razão, neste capítulo descreve-se os principais algoritmos e métodos utilizados em redes IP para essa finalidade.

4.1 Mecanismos de enfileiramento

Um modo que os elementos de rede possuem para controlar um transbordamento de pacotes na entrada de uma interface é usar um algoritmo de enfileiramento para ordenar este tráfego e, então, determinar algum método de priorizar seu encaminhamento através de uma interface de saída. No contexto de engenharia de redes, *enfileiramento* é a ação de armazenar pacotes ou células em um local onde eles permaneçam até serem processados [23]. Tipicamente, o enfileiramento ocorre dentro de roteadores quando os pacotes são recebidos pelo processador de interface do dispositivo (fila de entrada), e ocorre também antes da transmissão dos pacotes para uma outra interface (fila de saída) do mesmo dispositivo.

Um roteador básico é composto por: um conjunto de processos de *entrada*, que remontam os pacotes na forma como foram recebidos, verificando a integridade de sua estrutura básica; um ou mais processos de *encaminhamento*, que determinam a interface destino do pacote; e processos de *saída*, que estruturam e transmitem os pacotes para o próximo nó da rede. A união dos processos de entrada, de encaminhamento e de saída compreendem o processo de gerenciamento de filas de pacotes como mostra a Figura 4-1.

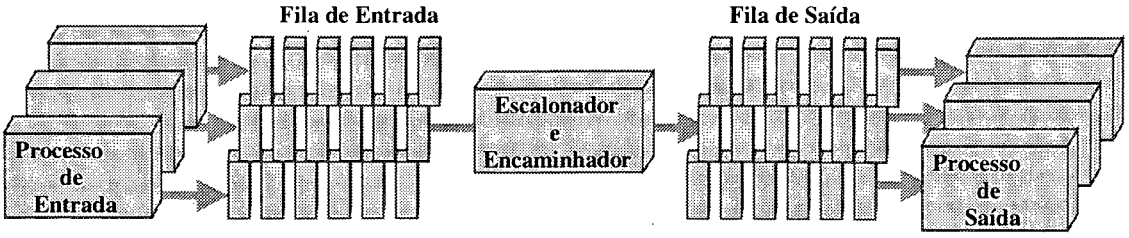


Figura 4-1- Diagrama de blocos de enfileiramento e escalonamento em um roteador

É importante entender o papel que as estratégias de enfileiramento desempenham no provimento de *serviços diferenciados.* As redes não orientadas à conexão, onde as redes IP são as principais representantes, operam segundo o paradigma *store-and-forward*[6] e todos os pontos finais estão distantes uns dos outros mais do que um *hop.* Portanto, deve-se entender a complexidade do enfileiramento de tráfego, o efeito que o enfileiramento tem no sistema de roteamento e aplicações e porque mecanismos de gerenciamento de filas adequados são cruciais para QoS [23].

O gerenciamento de filas depende basicamente do algoritmo de enfileiramento dos pacotes e do tamanho máximo da fila [23]. A escolha do algoritmo e o tamanho máximo da fila podem, a primeira vista, ser relativamente simples, porém esta escolha pode ser extremamente difícil em função do padrão de comportamento do tráfego na rede ser aparentemente randômico. Se um tamanho elevado é imposto à fila, introduz-se um atraso e *jitter* no RTT (*Round-Trip-Time*), que pode interromper aplicações e protocolos de transporte fim-a-fim. Por outro lado se a fila é muito pequena, pode-se enfrentar o problema de tentar enviar dados para a rede de forma mais rápida do que ela pode aceitar, resultando em excesso de perda de pacotes.

Em tráfego de fluxo confiável, como quando se utiliza o protocolo TCP, tais pacotes descartados devem ser identificados e retransmitidos [23]. Em fluxos de tempo-real não confiável, como quando se utiliza o protocolo UDP, tais como áudio e vídeo, os pacotes perdidos acabam por representar uma degradação do sinal. A seguir são descritas algumas técnicas tratar o enfileiramento nas interfaces de saídas, pois estas são as estratégias predominantes para tráfego do tipo *store-and-forward* e enfileiramentos relacionados a QoS. Cada um dos algoritmos foi projetado para resolver problemas específicos de tráfego na rede e tem um efeito particular no desempenho desta, conforme descrito nos itens 4.1.1 a 4.1.4.

4.1.1 Enfileiramento First In, First Out (FIFO)

O enfileiramento *first in, first out* (FIFO) – primeiro que entra, primeiro que sai - provê capacidade básica de *store-and-forward,* armazenamento e encaminhamento. Em sua

[6] No paradigma *store-and-forward* os pacotes são armazenados no roteador e em seguida transmitidos.

Biblioteca Universitária
UFSC
0-343.039-9

forma mais simples ele envolve o armazenamento de pacotes quando a rede está congestionada e o envio deles na ordem de chegada quando a rede não estiver mais congestionada.

FIFO é em muitos casos o algoritmo de enfileiramento padrão, porém ele possui muitas deficiências:

- ele não toma nenhuma decisão sobre prioridade do pacote;
- a ordem de chegada determina a largura de banda que será obtida, a prioridade e a alocação de *buffers*; e
- não provê proteção contra aplicações ou fontes de tráfego com comportamento prejudicial [23].

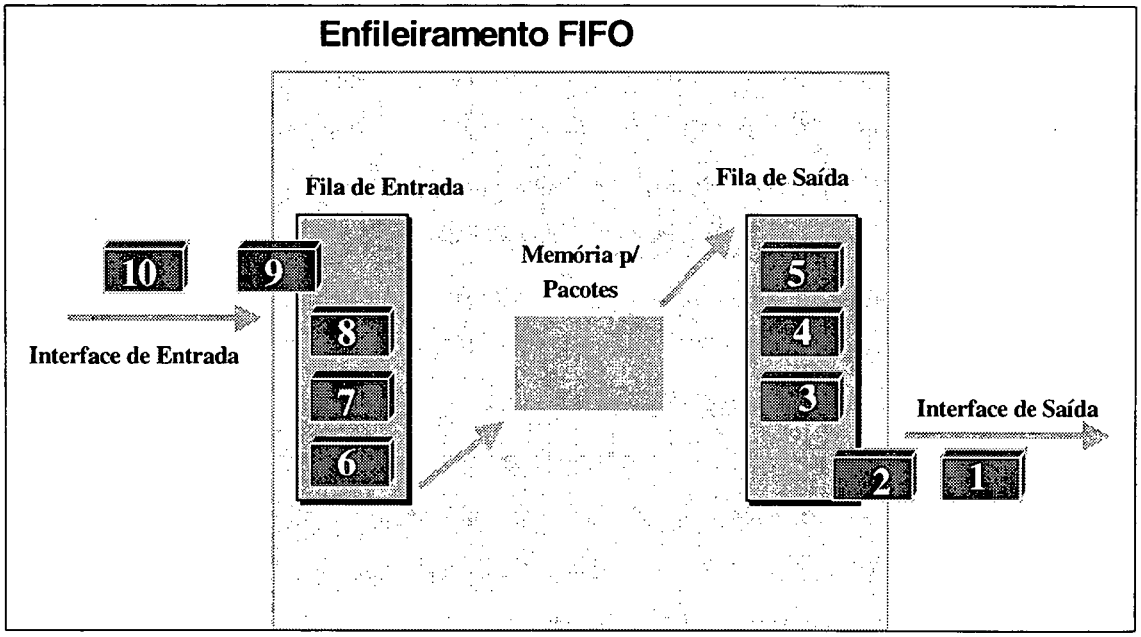


Figura 4-2- Enfileiramento FIFO – *first in, first out*

Fontes em "rajadas" podem causar atrasos altos na entrega do tráfego de aplicações sensíveis ao tempo e nas mensagens de sinalização e controle da rede. O enfileiramento FIFO pode ser considerado como um primeiro passo no controle de tráfego, porém a maioria das redes atualmente precisa de algoritmos mais sofisticados. A Figura 4-2 mostra que, na medida em que os pacotes entram na fila da interface de entrada, eles são colocados na fila de saída da interface apropriada na mesma ordem que foram recebidos.

4.1.1.1 Vantagens e Desvantagens

Quando a rede opera com suficiente nível de capacidade de transmissão e comutação, as filas são necessárias somente para assegurar que tráfegos em rajada de curta duração não causem descarte de pacotes. Em tais ambientes, enfileiramento FIFO é altamente eficiente, pois, na medida em que o tamanho da fila permanece pequeno, a média de retardo de pacotes na fila é uma fração insignificante do tempo de transmissão fim-a-fim. Entretanto, quando a carga da rede aumenta, o tráfego em rajada causa significativo atraso de enfileiramento em relação ao tempo de transmissão total e, quando a fila está totalmente cheia, todos os pacotes subseqüentes são descartados. Quando a fila opera deste modo por longos períodos, o serviço, inevitavelmente, degenera [23].

4.1.2 Enfileiramento por Prioridade - *Priority Queuing – (PQ)*

O mecanismo de enfileiramento por prioridade foi projetado para dar prioridade rígida ao tráfego importante [17]. Este mecanismo é baseado no conceito que certos tipos de tráfego podem ser identificados e colocados à frente da fila de saída e desta forma transmitidos na frente de outros tráfegos.

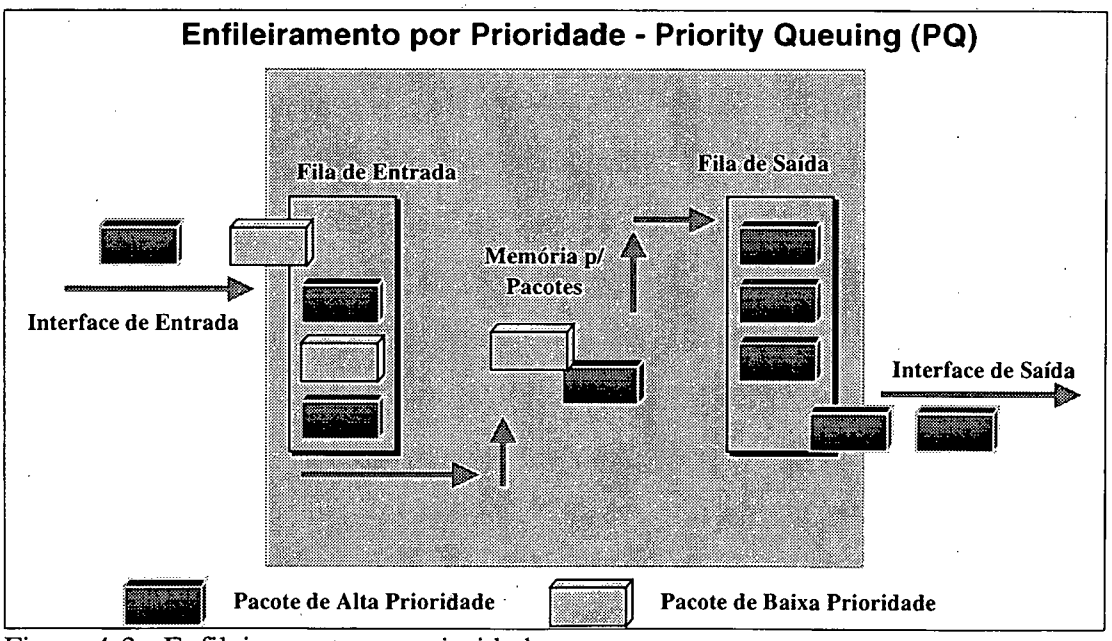


Figura 4-3 - Enfileiramento por prioridade

Este mecanismo de enfileiramento pode ter um efeito adverso no desempenho de encaminhamento dos pacotes por causa da reordenação destes na fila de saída e também, porque o roteador tem de analisar em detalhes cada pacote para saber como ele

deve ser enfileirado, sobrecarregando, desta forma, o processador. Em ligações de baixa velocidade, o roteador tem mais tempo para examinar e manipular os pacotes. Entretanto, na medida em que a velocidade do canal de comunicação aumenta, o impacto no desempenho torna-se mais visível. A Figura 4-3 mostra como os pacotes são recebidos na interface de entrada e reordenados, baseados em critérios definidos pelo usuário, quando colocados na fila de saída. Os pacotes de alta prioridade são colocados na fila de saída antes dos pacotes de prioridade normal.

4.1.2.1 Vantagens e Desvantagens

Diversos níveis de prioridade são possíveis, tais como: alto, médio, normal e baixo. Cada um dos níveis exerce uma preferência na fila de saída. Também a forma como o tráfego pode ser classificado na fila de saída é bastante flexível. Por exemplo, o tráfego IPX pode ser enfileirado antes do IP, o IP antes do SNA e assim por diante. Serviços específicos dentro de uma família de protocolos podem ser classificados da seguinte maneira: o tráfego TCP pode ser priorizado em relação ao UDP; telnet (porta TCP 23) pode ser priorizado em relação ao FTP (portas TCP 20 e 21), e assim por diante.

Embora bastante flexível em relação aos protocolos, este mecanismo de enfileiramento apresenta vulnerabilidades [23]. Se o volume de tráfego de alta prioridade for usualmente alto, o tráfego normal esperando para entrar na fila pode ser descartado por causa de insuficiência de espaço de armazenamento (*buffer*).

Outra consideração é o impacto adverso que a latência induzida pode causar à aplicação quando o tráfego esperar em uma fila por extensos períodos. Às vezes é difícil calcular como o enfileiramento não-FIFO pode injetar latência adicional no RTT fim-a-fim. No pior caso, algumas aplicações podem não funcionar corretamente por causa da latência adicional ou talvez porque protocolos de roteamento mais sensíveis ao tempo sofreram *time-out* por não receberem confirmação dentro de um período predeterminado.

Este mecanismo simples de enfileiramento não possui escalabilidade de modo a fornecer bom desempenho em ligação de maior velocidade [23].

4.1.3 Enfileiramento Baseado em Classes (CBQ)

O mecanismo de enfileiramento CBQ (*Class-Based Queuing)* ou CQ *(Custom Queuing)* foi projetado para permitir que várias aplicações, com especificações de largura de banda mínimas ou exigências de latência controlada, compartilharem a rede [17]. Este mecanismo é uma variação do enfileiramento por prioridades, onde várias filas de saída podem ser definidas. Pode-se também definir a preferência em que cada fila será servida e a quantidade de tráfego enfileirado que deve ser escoada de cada fila em cada passagem na rotação do serviço neste método de enfileiramento [23].

Utilizando-se CBQ é possível prover largura de banda garantida em um ponto potencial de congestionamento, assegurando ao tráfego especificado uma porção fixa da largura de banda disponível e deixando a banda remanescente para o restante do tráfego. CBQ manipula o tráfego assinalando um montante do espaço da fila para cada classe de pacotes e depois servindo a fila na modalidade *round-robin*[7].

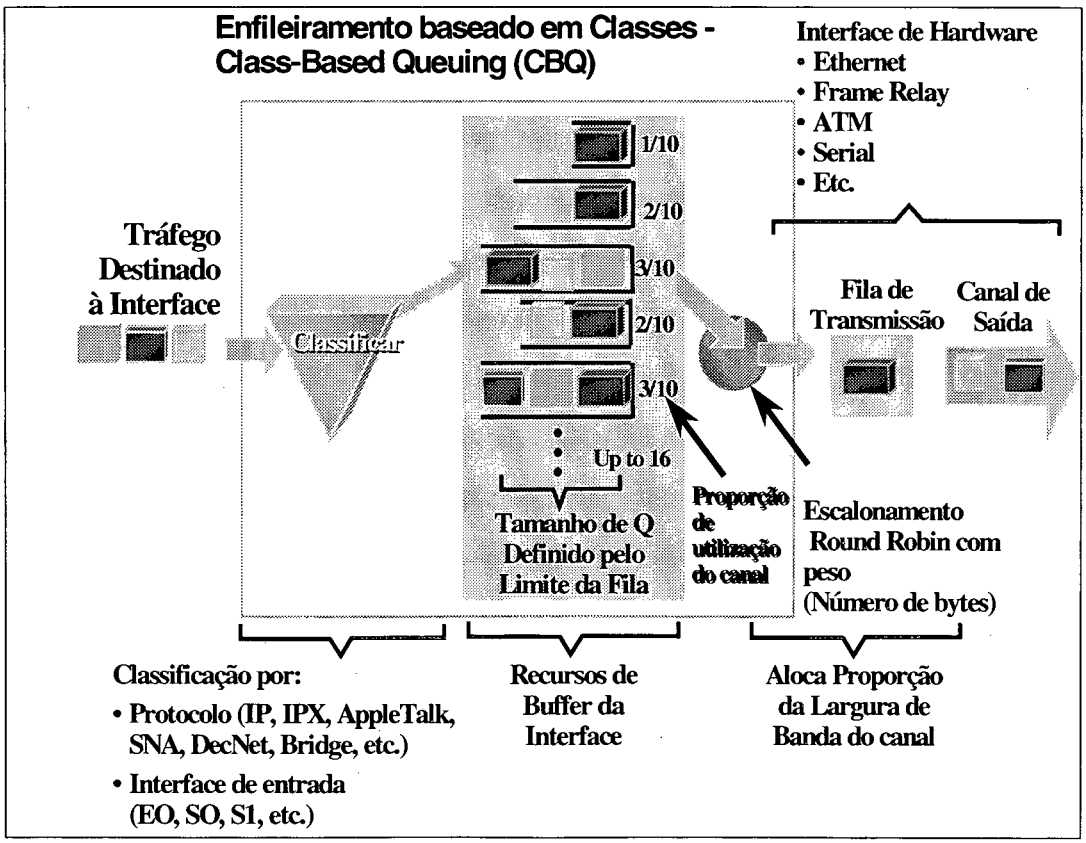


Figura 4-4 - Enfileiramento baseado em classes - CBQ

No exemplo da Figura 4-4 foram criados 3 *buffers*: alto, médio e baixo. O roteador pode ser configurado para servir 200 bytes na fila de alta prioridade, 150 bytes na fila de prioridade média e 100 bytes na fila de baixa prioridade em cada rotação. Após o tráfego em cada fila ser processado, os pacotes continuam a ser servidos até que o contador exceda o limite configurado ou a fila esteja vazia. Desta forma o tráfego que foi categorizado e classificado para ser enfileirado em diversas filas tem boas chances de ser transmitido sem que uma latência significativa seja induzida, permitindo ao sistema evitar escassez de *buffer*.

4.1.3.1 Vantagens e Desvantagens

O mecanismo de priorização baseado em classes geralmente é tido como um método de alocação de porções dedicadas de largura de banda para tipos específicos de tráfego. Mas, na realidade, ele provê um mecanismo onde o modelo absoluto de serviço para a fila de alta prioridade e total falta de recursos para as outras filas do modelo PQ (*priority queuing*) é substituído por um modelo mais eqüitativo com um aumento de recursos para a fila de mais alta prioridade e uma diminuição relativa para as filas de mais baixa prioridade. A questão fundamental colocada é que a falta absoluta de recursos é de longe pior que a redução de recursos [23].

CBQ tem sido considerado um método razoável para implementação de tecnologias que fornecem compartilhamento de canais de comunicação para classes de serviços - CoS *(Class of Service)* - e um método eficiente para gerenciamento de recursos de filas. Entretanto, apresenta falha na questão de escalabilidade por causa da sobrecarga computacional na reordenação de pacotes e gerenciamento intensivo de filas em canais de alta velocidade. Portanto, embora CBQ forneça mecanismos básicos para prover diferenciação de classes de serviços, ele é apropriado somente para canais de baixa velocidade, o que limita sua utilização.

4.1.4 Enfileiramento - WFQ (*Weighted Fair Queuing*)

O mecanismo de enfileiramento WFQ procura algoritmicamente prover comportamento previsível na entrega de pacotes e assegurar que os fluxos não tenham falta total de *buffers* [23]. Este mecanismo dá aos fluxos de baixo volume de tráfego tratamento

[7] Um algoritmo que serve cada fila em uma seqüência pré-definida.

preferencial e permite aos fluxos de alto volume utilizarem o restante da capacidade de enfileiramento. Ele pode ser utilizado para situações nas quais é desejável prover tempo de resposta consistente a usuários pesados e leves de modo semelhante, sem ter que adicionar largura de banda excessiva.

Este mecanismo executa duas tarefas simultaneamente:

- escalona o tráfego interativo na frente da fila para reduzir o tempo de resposta; e
- compartilha de forma imparcial a largura de banda restante entre fluxos com alto consumo de largura de banda [23].

Adicionalmente, WFQ assegura que as filas não sofram por falta de largura de banda, e que o tráfego receba um serviço previsível. Fluxos com baixo volume de tráfego, os quais incluem a maioria do tráfego, recebem serviço preferencial, de forma que sua carga seja transmitida inteira em uma porção de tempo. Fluxos com alto volume de tráfego compartilham o restante da capacidade proporcionalmente entre eles como mostrado na Figura 4-5.

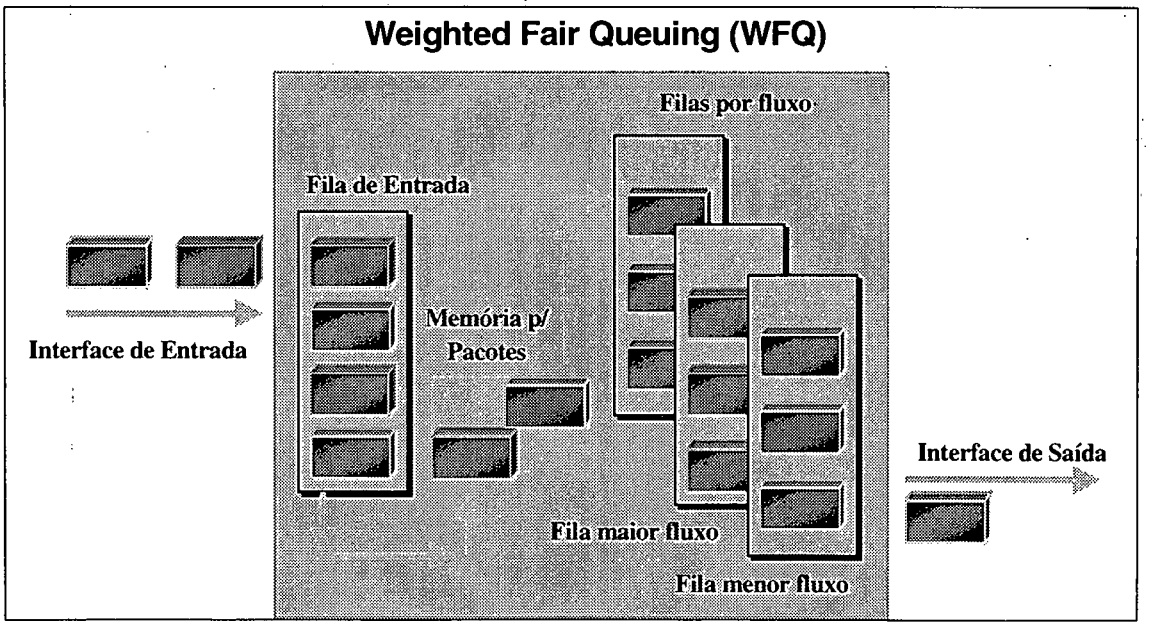


Figura 4-5 – Enfileiramento - *Weighted Fair Queuing (WFQ).*

O método WFQ foi projetado para minimizar esforço de configuração e adaptar-se automaticamente às mudanças nas condições de tráfego de rede. É um mecanismo eficiente na medida em que pode utilizar toda a largura de banda disponível para transmitir o tráfego de baixa prioridade se não existir tráfego de mais alta prioridade.

4.1.4.1 Vantagens e Desvantagens

WFQ possui algumas das características dos mecanismos de enfileiramento por prioridade (PQ) e enfileiramento baseado em classes (CBQ) e apresenta, pelos mesmos motivos, problemas de escalabilidade. Um outro problema está na falta de granularidade no controle do mecanismo utilizado para favorecer alguns fluxos sobre os outros. Por padrão, WFQ protege fluxos de baixo volume de tráfego de outros no esforço de prover equidade para todos. A utilização de pesos é atrativa do ponto de vista de justiça. Contudo, não são fornecidos formas de avaliar ou ajustar estes parâmetros para alterar o comportamento, pois o método de preferir alguns fluxos sobre outros é estaticamente definido na implementação específica de cada fabricante [23].

4.2 Policiamento do tráfego

O policiamento de tráfego fornece um mecanismo para controlar o montante e o volume de tráfego que é enviado para a rede e a taxa em que este está sendo enviado. Ele pode também ser necessário para identificar fluxos de tráfego no ponto de ingresso (ponto em que o tráfego entra na rede) com uma granularidade que permita ao método utilizado separar o tráfego em fluxos individuais e moldá-los diferentemente.

Dois métodos predominantes para policiamento de tráfego na redes de pacotes são descritos em [23] e [33]: o método do balde furado (*leaky bucket*) e o método do balde de tokens (*token bucket*).

4.2.1 O método do balde furado

A idéia principal deste algoritmo tem como base um balde com um pequeno furo embaixo, conforme Figura 4-6. A velocidade com que a água entra no balde não tem influência no fluxo de saída, que fica em uma taxa constante, e quando o balde estiver cheio, a água que entrar nele irá escorrer pelos lados e será perdida. Porém ao invés de água utiliza-se pacotes Figura 4-7. Cada *host* é conectado à rede por uma interface que contém um balde furado (fila interna finita). Se um pacote chegar e a fila estiver cheia, ele será descartado.

O *host* pode inserir um pacote a cada pulso de relógio na rede, transformando um fluxo de pacotes irregular dos processos de usuário dentro do *host* em um fluxo de pacotes regular para a rede, suavizando rajadas e reduzindo muito as chances de ocorrência de

um congestionamento. Quando os pacotes são todos do mesmo tamanho (por exemplo, células ATM), esse algoritmo pode ser usado da forma descrita acima. Se forem utilizados pacotes de tamanho variável, a melhor opção é permitir um número fixo de bytes por pulso, em vez de apenas um pacote.

O tamanho do balde e a taxa de transmissão geralmente são configuráveis pelo usuário e medidos em bytes.

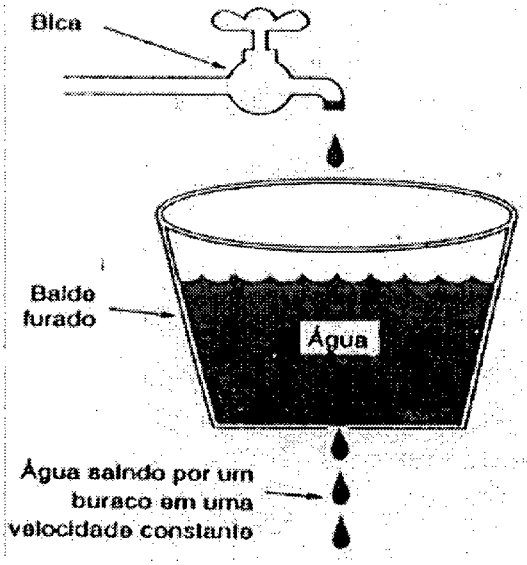


Figura 4-6 – Método balde furado (a)

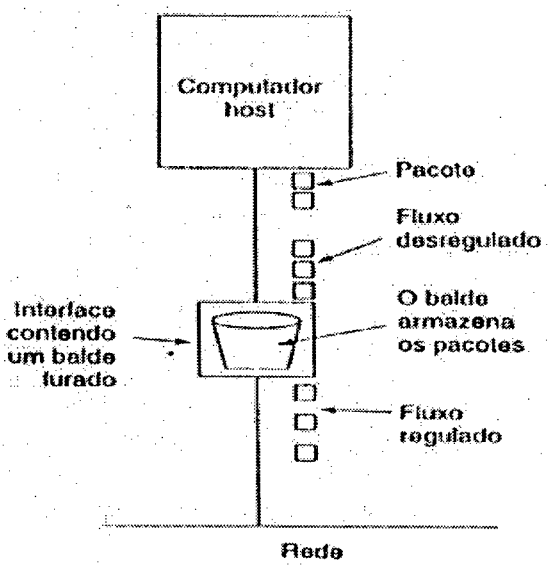


Figura 4-7 – Método balde furado (b)

4.2.2 O método do balde de tokens

O algoritmo do balde furado força um padrão de saída constante, independentemente da irregularidade do tráfego. Em muitas aplicações é melhor permitir que a saída aumente um pouco sua velocidade quando chegarem rajadas maiores. Para esses casos existe o algoritmo do balde de *tokens*, onde o balde retém *tokens*, gerados por um *clock* na faixa de um *token* a cada ΔT segundos.

Na Figura 4-8 vemos um balde com três *tokens*, com cinco pacotes aguardando para serem transmitidos. Para que um pacote seja transmitido, ele deve capturar e destruir um *token*. Na Figura 4-9, vemos que três dos cinco pacotes percorreram todo o caminho, mas os outros dois estão emperrados, aguardando que dois outros *tokens* sejam gerados.

O algoritmo do balde de *tokens* joga *tokens* fora quando o balde enche, mas nunca descarta pacotes. Pelo fato de o balde de *tokens* permitir rajadas em pequenos intervalos

de tempo, o tráfego pela rede será mais regular se for colocado um balde furado após o balde de *tokens*.

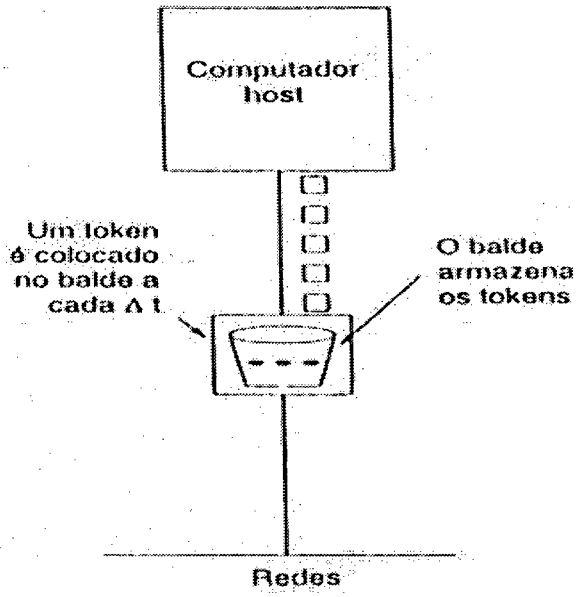


Figura 4-8 – Método balde de tokens (a)

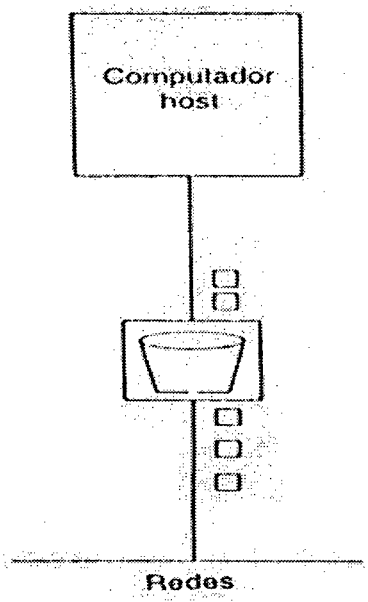


Figura 4-9 – Método balde de tokens (b)

4.3 Considerações finais sobre este capítulo

Neste capítulo foram examinados os principais métodos de enfileiramento e policiamento de tráfego. Como se pode perceber ao longo da leitura, este é um tópico bastante importante e complexo. Importante no sentido de que em algum momento o administrador da rede deverá optar por um ou mais métodos para prover QoS na rede e complexo no sentido de que não existe uma única opção possível para cada situação. De qualquer forma, sempre é possível iniciar pelos parâmetros padrões do fabricante e depois executar algum tipo de medição e análise comparativa, e então definir o método ou métodos mais adequados a cada situação. No próximo capítulo a questão de medição de QoS e as métricas associadas serão examinadas.

5 MÉTRICAS DE QOS E SUA MEDIÇÃO

Existem diversas maneiras de implementar QoS em uma rede [13]. Uma questão crítica, no entanto, é medir a efetividade da implementação de QoS escolhida no ambiente específico. Este capítulo provê uma visão geral de algumas técnicas e potenciais abordagens para medir QoS na rede e define o conjunto de métricas utilizadas para esse fim.

5.1 Considerações iniciais

As principais questões na medição de QoS na rede são determinar qual *agente* irá executar a medição e o que este *agente* irá medir. Um *agente* é uma aplicação que pode ser usada para monitorar ou medir um componente da rede [23]. Um fator relevante na determinação das medidas que estão disponíveis para o *agente* é o nível de acesso que ele possui para os vários componentes da rede, como *hosts* e roteadores. Outra questão é determinar quais medidas podem ser obtidas diretamente destes componentes e quais medidas devem ser derivadas destes pontos primários de dados.

Um usuário de uma rede com suporte a QoS pode estar motivado a medir:

- a diferença nos níveis de serviços entre transações com QoS habilitado e transações com QoS não habilitado;
- o nível de variação de uma transação em particular e derivar uma métrica de constância no ambiente de QoS. Ou seja, determinar se o desempenho da transação se mantém constante independente da carga existente na rede; e
- a capacidade de a rede consumir os recursos até o seu nível máximo de reserva e determinar a eficácia do esquema de reserva no caso de ambientes de QoS baseados na reserva de recursos.

Existem duas motivações principais das para a medição no ambiente de rede considerando QoS, quais sejam: primeiro, determinar quão bem pode-se entregar serviços que correspondem às necessidades particulares de um usuário. De fato, isto é a medição do nível de consistência entre o ambiente que oferece QoS e as necessidades do usuário; e segundo, o usuário pode estar interessado em medir o sucesso ou falha do provedor de rede em satisfazer os parâmetros de QoS acordados. Portanto, o usuário

está motivado a executar medições que correspondam às métricas de um ambiente com QoS em particular.

Um usuário de uma rede remota pode também estar interessado em medir a transitoriedade de um ambiente de QoS, de modo a verificar se os níveis de QoS de uma transação são mantidos quando esta atravessa a rede de diversos provedores e se os mecanismos de QoS utilizados em cada rede são compatíveis.

O administrador da rede também está interessado em medir parâmetros do ambiente com QoS, mas por razões diferentes do usuário. O administrador está interessado em medir:

- o nível de recursos alocados para o ambiente com QoS e seu impacto sobre a alocação de recursos no ambiente sem QoS; e
- o desempenho que o ambiente com QoS está entregando ao usuário, para assegurar que os níveis de serviços estão dentro dos parâmetros acordados.

Os usuários estão limitados a medir os efeitos da arquitetura de QoS através da medição de dados de desempenho do sistema final que gerou a transação na rede e não podem ver diretamente o comportamento dos dispositivos internos da rede. A medição no sistema final pode ser efetuada medindo o comportamento de uma transação em particular ou instalando *probes* ou sondas na rede e medindo o tempo de resposta nestes *probes*. Para medição remota da rede, o *agente*, um administrador remoto ou usuário remoto, geralmente é limitado a estas técnicas de medição no sistema final, ou medição de transações ou medição através de *probes*.

Na prática, não existe um único meio de medir QoS e nem um único resultado para uma métrica de QoS. Por isto, o conhecimento da rede que está sendo medida e seu perfil de comportamento em condições normais tornam-se fundamentais na análise dos resultados.

5.2 Medição de redes IP

A medição de desempenho de um ambiente de rede com QoS pode ser considerada como um caso especial de medição de desempenho no ambiente de rede IP (*Internet*

Protocol), e a utilização da experiência e estudos existentes nesta área são apropriados. Ferramentas de medição devem ser baseadas no nível de entendimento da arquitetura que está sendo medida para serem consideradas como ferramentas efetivas. O grupo de trabalho IPPM (*IP Provider Metric*) [30] do IETF procura estabelecer padrões de medição de desempenho em redes IP tanto sob a perspectiva do usuário quanto do administrador de rede.

De forma simplificada, um ambiente Internet pode ser visto como uma coleção de comutadores de pacotes de dados interconectados. Em cada comutador quando um pacote é recebido seu cabeçalho é examinado e encaminhado para transmissão. Se o comutador puder encaminhar o pacote, este é mapeado imediatamente para transmissão na interface de saída apropriada. Se a interface já estiver transmitindo um pacote, este é enfileirado para posterior transmissão. Se o tamanho da fila exceder o tamanho máximo, o pacote pode ser descartado imediatamente, ou pode ser descartado após um tempo de espera para transmissão na fila. Enfileiramento contínuo e descarte de pacotes no comutador ocorrem quando a taxa de chegada de pacotes excede a capacidade do meio de transmissão incluindo a capacidade da interface.

5.3 O efeito do tamanho da fila

A capacidade de transmissão e o tamanho da fila estão relacionados. Se a largura de banda de transmissão é de 1 Mbps e a taxa de chegada de pacotes é de 1.5 Mbps, por exemplo, a fila irá crescer a uma taxa de 0,5 Mbps. Se o tamanho da fila é de Q bytes, a velocidade de transmissão é de T bits por segundo, e a taxa de chegada é de A bits por segundo, o descarte de pacotes ocorre após (8*Q) / (A-T) segundos. Neste caso, cada pacote é retardado por (8 * Q)/T segundos [23]. Aumentando o comprimento de fila em uma fração da largura de banda de transmissão diminui-se a probabilidade de perda de pacotes por causa de aumentos eventuais do tráfego. Isto também aumenta a variação do tempo de transmissão dos pacotes e reduz a sensibilidade dos cronômetros de retransmissão de pacotes do TCP. Este incremento na variância do RTT (*Round Trip Time*) faz com que o TCP responda mais lentamente à disponibilidade dinâmica de recursos da rede. Desta forma, embora filas nos comutadores sejam um bom mecanismo, um espaço muito grande para filas no comutador tem um impacto adverso no tempo de resposta fim-a-fim.

5.4 O atraso

Em redes IP, considerando que cada interface de um nó é um sistema de enfileiramento, o atraso está diretamente relacionado com o tamanho e a taxa de serviço da fila (ou largura de banda) de cada interface [23], visto que o atraso devido ao tempo de propagação do canal é constante. Uma fila grande pode evitar o descarte de pacotes, mas pode provocar mais demora em seu encaminhamento. Por outro lado, uma fila com alta taxa de serviço, exige *hardware* de maior desempenho (processador, *buffer*, memória e canais de comunicação).

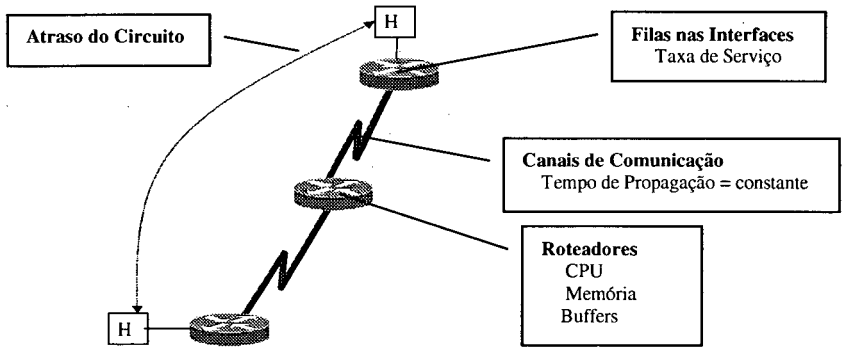


Figura 5-1 - Pontos que colaboram com o atraso fim-a-fim

Outra forma de minimizar o atraso sobre determinados fluxos de tráfego, além de aumentar a taxa de serviço, é priorizá-los sobre os demais, tal como ocorre em Serviços Diferenciados [9] [50]. Desta forma, certos fluxos sofreriam menor atraso pela rede, pois teriam seus pacotes, prioridade de envio nas filas sobre os demais, numa tentativa de manter uma largura de banda assegurada para estes fluxos.

5.5 Como medir QoS

Uma das razões para se medir o tráfego com QoS é poder cobrar ou contabilizar de maneira diferenciada o tráfego que recebe tratamento diferenciado na rede em comparação com o tráfego de melhor esforço. Uma outra razão importante é o fato de que uma organização que provê o serviço deve estar ciente da capacidade de seu *backbone*, assim ela quer verificar a diferença entre o tráfego designado para QoS e o de melhor esforço. Em [23] são definidos dois métodos básicos para medir o tráfego com QoS em uma rede: intrusivo ou ativo e não intrusivo ou passivo.

5.5.1 Medição não intrusiva

O método de medição não intrusiva mede o comportamento da rede através da observação da taxa de chegada de pacotes em um sistema final [23]. Deduções sobre o estado da rede e, portanto, sobre a efetividade de QoS são feitas com base nestas observações. Em geral, esta prática requer conhecimento detalhado da aplicação que está gerando o fluxo de dados que está sendo observado. Assim, a ferramenta para medição pode distinguir entre o comportamento da aplicação remota e a moderação deste comportamento imposta pelo estado da rede.

Simplesmente monitorar um dos lados de uma troca de dados arbitrária não acrescenta muita informação de valor e pode resultar em diversas interpretações dos resultados. Por esta razão, monitoração em um único lado como base para medição de desempenho da rede e, por inferência, desempenho de QoS não é recomendado como uma abordagem efetiva para o problema. Entretanto, existem ferramentas de monitoração baseadas em *hosts* que analisam o comportamento do fluxo TCP e a temporização dos pacotes dentro do fluxo. Uma interpretação cuidadosa comparando pacotes enviados com pacotes recebidos pode oferecer alguma indicação sobre a extensão da distorção, se houver enfileiramento dentro do caminho da rede para o sistema remoto. Esta interpretação também pode prover uma indicação aproximada da capacidade de dados disponível no caminho. Uma ferramenta que pode ser utilizada para medição através do comportamento dos fluxos TCP é DBS (*Distributed Benchmark System*) [37]. De qualquer forma, esta técnica apresenta dificuldades para a avaliação dos resultados.

5.5.2 Medição intrusiva

Medição intrusiva refere-se à injeção controlada de pacotes na rede e a subseqüente coleta destes pacotes. A troca de pacotes PING[8] – (*ICMP echo request* e *ICMP echo reply*) é um bom exemplo deste método de medição. Enviando seqüências de pacotes através deste comando em intervalos regulares, a estação de medição pode medir parâmetros tais como: alcançabilidade, tempo de resposta RTT (*Round Trip Time)* de transmissão para uma estação remota e expectativa de perda de pacotes no caminho de ida e volta.

A execução de um determinado número de medições considerando o comportamento da fila dentro dos comutadores/roteadores, combinando estas medidas com a medida de perda de pacotes e o *jitter* imposto, pode-se fazer algumas inferências sobre a largura de banda disponível entre dois pontos e o nível de congestionamento. Tais medições não são, entretanto, medidas da eficácia do ambiente com QoS. Para medir a efetividade de uma estrutura de QoS, deve-se utilizar uma transação de dados típica da carga da rede e medir seu desempenho em condições controladas. Pode-se fazer isto utilizando-se ferramentas de geração e medição de tráfego como o MGEN [39] e o Netperf [32].

O método requer que seja medida a eficácia da taxa contínua, a taxa de retransmissão, a estabilidade do RTT estimado e o tempo global da transação [23]. Com a introdução da medição de QoS na rede, a comparação do nível de degradação destas métricas de uma rede sem carga para uma rede plenamente carregada deve representar uma métrica de efetividade de QoS da rede.

O problema, em relação a esse aspecto, é que os mecanismos de QoS são visíveis somente quando partes da rede estão com contenção de recursos e a introdução de mecanismos de medição intrusiva no sistema acarretará aumento na condição de sobrecarga. Na prática, tentar observar o estado dinâmico de uma rede perturba este estado, e há um limite na precisão das medidas [23].
Quanto mais detalhada a informação a ser obtida, maior será o tráfego inserido, e portanto, maior o erro na medição [23]. A Figura 5-2 mostra como seria o fluxo de pacotes de tráfego de medição e o fluxo sendo medido quando se utiliza um método de medição intrusiva.
Neste trabalho, em condições de carga controlada na rede, foi utilizado um método intrusivo para medir:

- a vazão;
- o atraso fim-afim;
- a variação do atraso; e
- a taxa de perda de pacotes.

[8] A aplicação ping , é baseada no ICMP e mede o tempo decorrido entre o envio de um pacote e seu retorno à estação de medição.

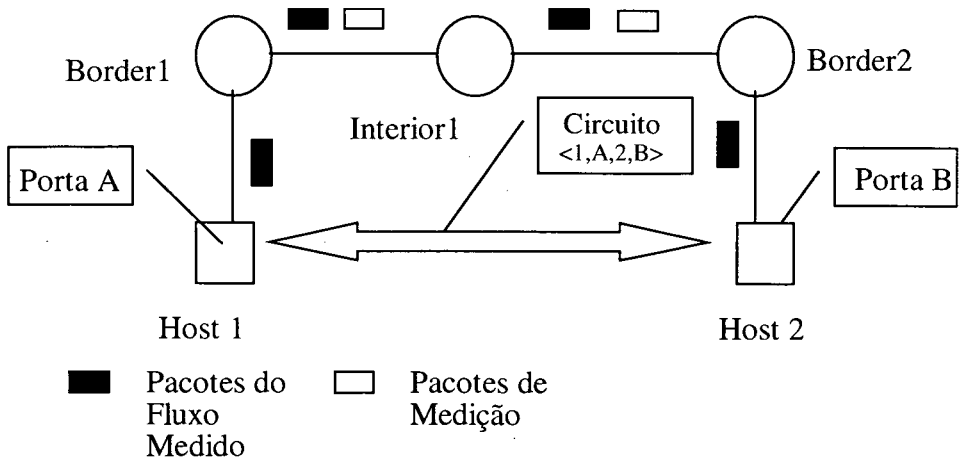


Figura 5-2 - Medição intrusiva em um circuito

Neste caso, o problema do erro na medição descrita por Ferguson em [23] não é caracterizado, pois este método é na realidade uma variação do método de medição intrusiva, sendo todo o tráfego utilizado para a medição e a rede trabalhando em condições controladas, ou seja, a quantidade de tráfego imposta à rede é controlada. Desta forma, a condição utilizada em um determinado experimento pode ser reproduzida em outro.

Utilizando-se de ferramentas apropriadas este método consiste na transmissão de fluxos de tráfego de uma ou mais estações e a sua recepção na estação remota. Na estação remota o tráfego é analisado e obtêm-se as informações sobre o comportamento da rede e dos fluxos individuais.

5.6 Métricas

As métricas para avaliação de DiffServ foram divididas em três grupos:

- as que descrevem o comportamento do DiffServ de um modo geral;
- as relativas à marcação AF; e
- as relativas ao comportamento da classe EF.

5.6.1 Métricas relativas a DiffServ de forma geral

São as métricas que descrevem o comportamento das classes de serviços EF, AF e BE em cada interface de rede. Através deste conjunto de métricas, pode-se obter

informações sobre o desempenho de cada classe e desta em relação às outras. Em resumo, pode-se citar as seguintes métricas:

- número de pacotes descartados por classe de serviço;
- número de *buffers* alocados por classe de serviço;
- número de pacotes enviados por classe de serviço; e
- número de pacotes que excederam a quantidade de *buffers* ou perfil de tráfego definido para uma classe de serviço.

5.6.2 Métricas relativas a marcação AF

Devido a existência de um marcador de pacotes para os fluxo na classe AF [24], [25], DiffServ apresenta adicionalmente métricas específicas para as filas AF não aplicáveis as outras duas classes:

- número de pacotes marcados com Verde;
- número de pacotes marcados com Amarelo;
- número de pacotes marcados com Vermelho; e
- número de pacotes alterados de Verde para Amarelo.

5.6.3 Métricas relativas a classe EF

Foram selecionadas três métricas para a caracterizar o comportamento da classe de tráfego EF e verificar a adequação desta classe às aplicações que possuem demandas estritas de QoS:

- atraso do pacote fim-a-fim em um sentido;
- variação do atraso ou IPDV–iitter – *Instantaneous Packet Delay Variation*; e
- taxa de perda de pacotes.

Para garantir medições consistentes e reprodutíveis, adotou-se para estas métricas as definições do grupo de trabalho IPPM do IETF.

Para o IPPM a noção de *"wire time"* é fundamental. Esta noção assume que o dispositivo de medição tem um posto de observação no canal IP. O pacote chega em um *"wire time"* particular quando o primeiro bit aparece no ponto de observação e o pacote parte do canal em um *wire time* particular quando o último bit do pacote passar pelo ponto de observação. Em [3] também é definida a noção de *"host time"*. Quando a medição é feita por software, este registra o *"timestamp"* imediatamente antes de enviar

o pacote de teste e o receptor registra o "*timestamp*" imediatamente após a recepção do pacote. A diferença entre os dois tempos é o atraso fim-a-fim em um sentido.

5.6.3.1 Atraso fim-a-fim

O atraso fim-a-fim (*One-way Delay)* é definido formalmente no RFC 2679 [3]. Esta métrica é medida do *"wire time" ou "host-time"* do pacote chegando no canal de comunicação observado pelo emissor para o *"wire time" ou "host time"* do último *bit* do pacote observado pelo receptor. A diferença entre estes dois valores é o atraso fim-a-fim. Neste trabalho, as medições foram realizadas por software. Portanto os valores do atraso são calculados utilizando-se a noção de "*host time*".

5.6.3.2 Variação do atraso ou IPDV-Jitter

A variação do atraso ou IPDV-Jitter *(Instantaneous Packet Delay Variation)* é formalmente definida pelo grupo de trabalho do IPPM através do Draft (*Instantaneous Packet Delay Variation Metric for IPPM)* [21]. Ele é baseado na medição do *atraso* fim-a-fim e é definido para pares consecutivos de pacotes. A medição de um único IPDV requer dois pacotes. Supondo que D_i seja o atraso do i-ésimo pacote, então o IPDV do par de pacotes é definido com $D_i - D_{(i-1)}$. De acordo com a literatura corrente, o valor do IPDV-jitter é computado de acordo com a seguinte fórmula:

IPDV-jitter = | IPDV | = módulo do IPDV

Neste trabalho, os termos variação do atraso, *jitter* e IPDV-jitter são utilizados com o mesmo significado.

5.6.3.3 Taxa de perda de pacotes

A taxa de perda de pacotes em um sentido (*One-Way Packet Loss*) é calculada no lado do receptor como a razão entre a quantidade de pacotes perdidos e a quantidade de pacotes transmitidos, em cada intervalo de tempo considerado [2]. A perda de pacotes se dá em função do descarte que estes sofrem nas filas dos roteadores quando estas se tornam cheias e não permitem mais a admissão e o armazenamento de pacotes para posterior envio. Protocolos como TCP se recuperam desta situação através da detecção e reenvio dos pacotes porventura perdidos. Já o protocolo UDP, normalmente utilizado para transmissão de áudio e vídeo, não retransmite pacotes e, portanto estas perdas não são recuperadas.

A taxa percentual de perdas de pacotes é calculada da seguinte forma:

```
Taxa de perdas = (Número de pacotes perdidos / Número total de pacotes recebidos) * 100
```

5.7 Considerações finais sobre este capítulo

Este capítulo abordou a problemática relacionada à medição de QoS. A discussão permitiu concluir que a medição, sempre que possível, deve considerar a hipótese de se utilizar uma carga controlada de tráfego, pois esta abordagem permite uma maior precisão e um melhor conhecimento da capacidade da rede e do comportamento dos mecanismos de priorização. Neste capítulo buscou-se também uma definição precisa sobre as métricas utilizadas nos experimentos que serão definidos no próximo capítulo.

6 DESCRIÇÃO DOS EXPERIMENTOS

De modo a avaliar a arquitetura de serviços diferenciados para prover qualidade de serviço em redes IP, um conjunto de experimentos foi realizado. Estes experimentos foram divididos em duas fases.

A fase I teve como meta uma avaliação global de serviços diferenciados e para tal foi utilizado um ambiente composto por roteadores IBM 2210 e 2216, pois esta implementação separa bem as classes de serviços AF, EF e BE, facilitando desta forma a avaliação geral pretendida. Na fase II, os objetivos se voltaram para uma análise mais específica de 3 (três) parâmetros fundamentais em QoS e aplicáveis a classe EF da arquitetura DiffServ: o *atraso*, a *variação do atraso* e a *taxa de perda de pacotes*. Estas duas fases serão descritas a seguir.

6.1 Experimentos – Fase I - Análise geral de DiffServ

Nesta fase, o objetivo principal foi analisar de forma geral a utilização de Serviços Diferenciados para implementar QoS em uma rede IP de longa distância. Para realizar esta análise, em um ambiente composto por roteadores IBM 2210 e 2216, foram estudados e medidos os seguintes parâmetros:

- vazão;
- atraso;
- largura de banda; e
- descarte e marcação de pacotes observados nos nós DS.

Os experimentos realizados nesta avaliação incluíram:

- a implementação de um domínio DS e a definição de um conjunto de políticas de condicionamento de tráfego segundo este padrão;
- a comparação das políticas definidas com comportamento observado do tráfego introduzido na rede, verificando se foi obtido o comportamento esperado;
- a comparação do comportamento dos fluxos de tráfego no ambiente com QoS e sem QoS;
- a avaliação da Arquitetura DS através dos indicadores fornecidos pelos nós DiffServ;

- a execução de testes de isolamento de tráfego (estes testes visam verificar a capacidade da implementação DiffServ de isolar as diferentes classes de tráfego, uu seja, verificar se fluxos de alta prioridade são protegidos do tráfego de melhor esforço intensivo na rede e verificar se o comportamento de uma classe fica dentro dos parâmetros de QoS definidos sobre diferentes condições de tráfego); e
- a execução de testes de gerenciamento da largura de banda (estes visam verificar a capacidade de um fluxo TCP de obter mais largura de banda que o valor definido na configuração de DS no caso de ausência de congestionamento).

6.1.1 Ambiente DS para realização dos experimentos

Para possibilitar as medições de QoS em uma rede do tipo WAN, foi montado um domínio DiffServ conforme ilustrado na Figura 6-1. Este domínio é composto por 3 roteadores, 2 sistemas servidores e 3 sistemas clientes, e a conexão entre os roteadores é feita através de enlaces PPP em dois canais WAN de 64 Kbps. O roteador border1 conecta a rede local dos clientes na WAN, enquanto que o roteador border2 conecta a rede local dos servidores.

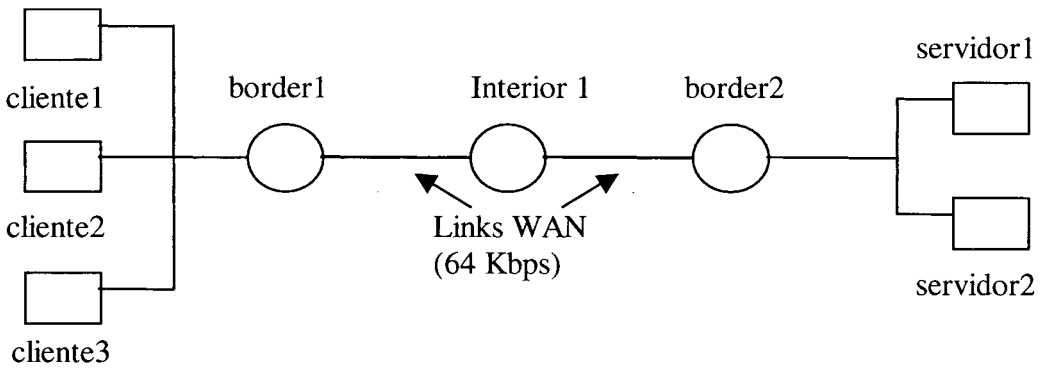


Figura 6-1 – Domínio DiffServ – fase I

Foram utilizados roteadores IBM 2210 que, na versão 3.4 do sistema operacional, implementam DiffServ para interfaces PPP e Frame-Relay. Os servidores e clientes utilizaram computadores Intel Pentium II com sistema operacional Windows NT 4.0. Como rede local, utilizou-se duas ELANs (redes locais emuladas sobre ATM) [48] a 25 Mbps, uma para a rede local dos servidores e outra para a rede local dos clientes.

6.1.2 Políticas de QoS definidas

A definição das políticas de QoS, segundo [22] e [33] inclui:

- a identificação dos perfis de fluxos de tráfego existentes e sua forma de agregação;
- a associação dos tipos de serviços (EF, AF ou BE) aos perfis; e
- a alocação da largura de banda para cada perfil.

Na configuração da rede mostrada na Figura 6-1 foram utilizados os fluxos de tráfegos ilustrados na Figura 6-2.

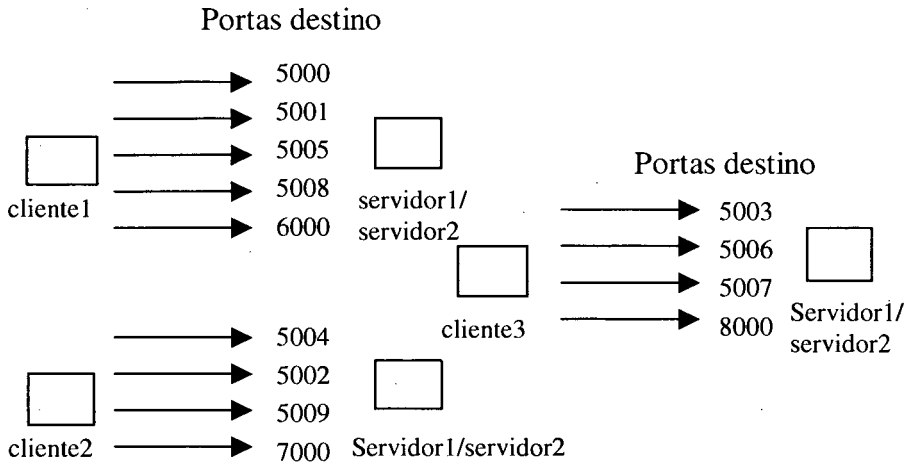


Figura 6-2 – Fluxos de tráfegos

A Figura 6-2 ilustra que cada um dos clientes estabelece conexões com *servidor1* e *servidor2*. Entretanto, estas conexões não são simultâneas, ou seja, assim que a conexão com o *servidor1* é encerrada e sua medição é efetuada, uma conexão com mesmo número de porta destino é estabelecida com *servidor2*. Esta técnica permite manter iguais as condições de tráfego na rede ao longo da medição. A manutenção desta condição é importante para não distorcer os resultados das medições.

Resumidamente, tem-se 5 fluxos de tráfegos gerados pelo *cliente1*, 4 fluxos pelo *cliente2* e 4 fluxos pelo *cliente3*. Todos estes fluxos são TCP e as portas destinos nos servidores são numeradas como na Figura 6-2. As portas fontes nos clientes podem variar em cada conexão, tendo em vista que são alocadas dinamicamente e não podem ser determinadas com exatidão. Desta forma, pode-se montar as políticas definidas na Tabela 6-1 resumindo os parâmetros de cada uma. A classificação MF nos roteadores

de borda é feita com base no endereço da porta destino do servidor. O endereço IP do cliente fonte e do servidor destino não são detalhados na tabela.

Endereço fonte	Portas fonte	Endereço destino	Portas destino	Tipo de fluxo	Largura de banda definida
192.168.1.2	N/A	192.168.4.2	5000	EF	19%
192.168.1.0	N/A	192.168.4.0	5001-5003	AF	24%
192.168.1.0	N/A	192.168.4.0	5004-5006	AF	15%
192.168.1.0	N/A	192.168.4.0	5007-5009	AF	9%
192.168.1.0	N/A	192.168.4.0	6000,700,8000	BE	10%

Tabela 6-1- Políticas de DiffServ definidas

6.1.3 Topologia da rede

Conforme mostrado na Figura 6-1, os roteadores *border1*, *interior1* e *border2* foram interligados através de um canal PPP de baixa velocidade (64 Kbps). Esse canal constituiu-se em um ponto de gargalo, tendo em vista que a geração e recepção do tráfego são realizadas por computadores ligados a rede através de interfaces ATM_LANE de 25 Mbps. Essa configuração provoca uma situação de saturação dos canais de 64 Kbps e, conseqüentemente, a atuação dos mecanismos de reserva priorização de DiffServ.

6.1.4 Geração e medição do tráfego

A geração de tráfego foi realizada através do software WSTTCP (uma implementação para Windows/NT do programa TTCP [38]). Os fluxos de tráfego foram realizados sempre em condições de rede congestionada, pois o objetivo era verificar a efetividade dos mecanismos de QoS que só atuam com a rede nestas condições. Para obtenção dos resultados foram realizadas diversas seqüências de medições utilizando-se de fluxos simples para a classe EF e de fluxos agregados para as classes AF e BE. Na Tabela 6-2 e Tabela 6-3 são descritos os parâmetros utilizados nas medições realizadas, respectivamente, com DS habilitado e DS desabilitado nos roteadores. Estas tabelas descrevem, resumidamente, cada fluxo gerado pelo programa WSTTCP. Em cada entrada das tabelas são descritos:

- a quantidade de fluxos gerados;
- a largura de banda definida;
- o tamanho de cada pacote; e
- o número de pacotes enviados pelos clientes aos servidores.

Para experimentos com DS não habilitado, (Tabela 6-3) a largura de banda não é definida, ou seja, todos os fluxos são tratados igualitariamente (melhor esforço).

Tráfego	Quantidade de fluxos	Banda reservada (% de 64 Kbps)	Tamanho dos pacotes (bytes)	Número de pacotes
Fluxo EF	1	19	128, 256 e 512	2048
Fluxo AF-1	3	24	128, 256 e 512	2048
Fluxo AF-2	3	15	128, 256 e 512	2048
Fluxo AF-3	3	9	128, 256 e 512	2048
Fluxo BE	3	10	128, 256 e 512	2048

Tabela 6-2 – Medições realizadas com DS habilitado

Tráfego	Quantidade de fluxos	Largura de banda (% de 64 Kbps)	Tamanho dos pacotes	Número de pacotes
Fluxo EF	1	-	128, 256 e 512	2048
Fluxo AF-1	3	-	128, 256 e 512	2048
Fluxo AF-2	3	-	128, 256 e 512	2048
Fluxo AF-3	3	-	128, 256 e 512	2048
Fluxo BE	3	-	128, 256 e 512	2048

Tabela 6-3 - Medições realizadas com DS não habilitado

6.2 Experimentos – Fase II

Na fase II o objetivo foi analisar o desempenho da classe de serviços EF (*Expedited Forwarding*) para suporte a aplicações sensíveis ao *atraso*, *variação do atraso* e *perdas*. Para efetivação desse objetivo dois ambientes para realização de experimentos foram utilizados. O primeiro foi montado com roteadores IBM com uma topologia descrita na seção 6.2.3 e o segundo, cuja topologia está descrita na seção 6.2.6, com roteadores CISCO.

A utilização dos dois ambientes não teve como objetivo estabelecer comparativos de desempenho entre ambos e sim conhecer aspectos funcionais das duas implementações sem, no entanto, tentar traçar comparativos sobre as duas arquiteturas de roteadores ou sobre os dois ambientes montados. Desta forma, esta análise possibilita avaliar estas implementações de DiffServ sob diferentes perspectivas e sua adequação às aplicações de tempo real como voz e vídeo. A seleção das duas plataformas também foi motivada

pela necessidade de implementar QoS nas redes que fazem parte de nosso contexto de trabalho na redeUFSC[9] e RMAV-FLN[10].

6.2.1 Ambiente DS com roteadores IBM

O propósito geral deste ambiente é avaliar o tráfego EF para suporte a aplicações com requisitos rígidos de QoS, como aplicações de voz ou telefonia sobre IP em uma rede WAN de baixa velocidade (64 Kbps). Enquanto DS foi projetado para fluxos unidirecionais, o tráfego de voz, especialmente em telefonia, é tipicamente bidirecional e, desta forma, o ambiente de testes deve ser configurado adequadamente para suportar esta característica. Por outro lado, a geração do tráfego e as medições devem ser, preferencialmente, em ambos os sentidos.

6.2.2 Fundamentos da implementação DS nos roteadores IBM

Nos roteadores IBM a garantia de largura de banda é forçada através de esquemas de alocações de memória, em que o montante alocado para uma classe de tráfego é proporcional a sua capacidade de compartilhamento do canal. O tráfego EF de entrada é controlado por um mecanismo de policiamento do tipo balde furado – (*leaky bucket*) (ver seção 4.2.1) chamado "*two-parameter leaky bucket policer*", cujo tamanho de rajada "*burst size*" é configurável. Os pacotes EF são classificados e marcados. No ponto de saída do roteador de borda, o tráfego EF está sujeito a enfileiramento. O algoritmo de escalonamento é um tipo de "*Weight Fair Queuing*" chamado *SCFQ* "*Self-Clocked Fair Queuing*" [33]. O tamanho da fila e seu peso (que por *default* tem valor de 90%) podem ser configurados. SCFQ é habilitado na interface de saída do roteador IBM2210 (interface PPP) como mostra a Figura 6-3.

6.2.3 Topologia do ambiente IBM

O ambiente utilizado (Figura 6-3) é constituído por 4 redes locais interligadas por uma rede WAN *multi-hop*. As redes locais 192.168.100.0/24 e 192.168.101.0/24, através das estações BE1 e BE2, são utilizadas para geração de tráfego bidirecional do tipo *melhor esforço*. Este tráfego não será controlado e nem medido quanto ao desempenho, pois é

[9] redeUFSC é nome da infra-estrutura de rede que dá suporte às comunicações LAN e WAN na UFSC – Universidade Federal de Santa Catarina.
[10] RMAV-FLN é um projeto de pesquisa e desenvolvimento em redes de alta velocidade e aplicações multimídia interativa, financiado pela RNP (Rede Nacional de Pesquisa).

um tráfego de *background* utilizado somente para provocar congestionamento nos canais PPP de 64 Kbps.

Os blocos funcionais Diffserv (Classificação, Marcação, Medição e Escalonamento) são habilitados nos nós DS, *border1* e *border2*. No nó *interior1* não é necessária a função de marcação, e a função de classificação é feita de forma simplificada com base no DSCP assinalado em *border1* e *border2*. *No* Anexo I – Configuração DS ambiente IBM são mostradas com detalhes as configurações realizadas nos roteadores IBM.

As redes 192.168.1.0/24 e 192.168.4.0/24, através das estações EF1 e EF2, são utilizadas para geração do *tráfego priorizado* EF. Como o interesse do experimento é verificar a adequação desta classe de serviço para garantia de QoS para tráfego de voz, tanto o tráfego EF quanto o tráfego BE serão bidirecionais. As estações VoIP1 e VoIP2 são utilizadas para o estabelecimento de chamadas de voz sobre IP.

A rede 200.135.0.0/24, que aparece na Figura 6-3, externa ao ambiente, permite o gerenciamento da rede sem gerar tráfego no canal de medição e também permite a sincronização dos relógios das estações de medição em um servidor de NTP no mesmo domínio de *broadcast.*

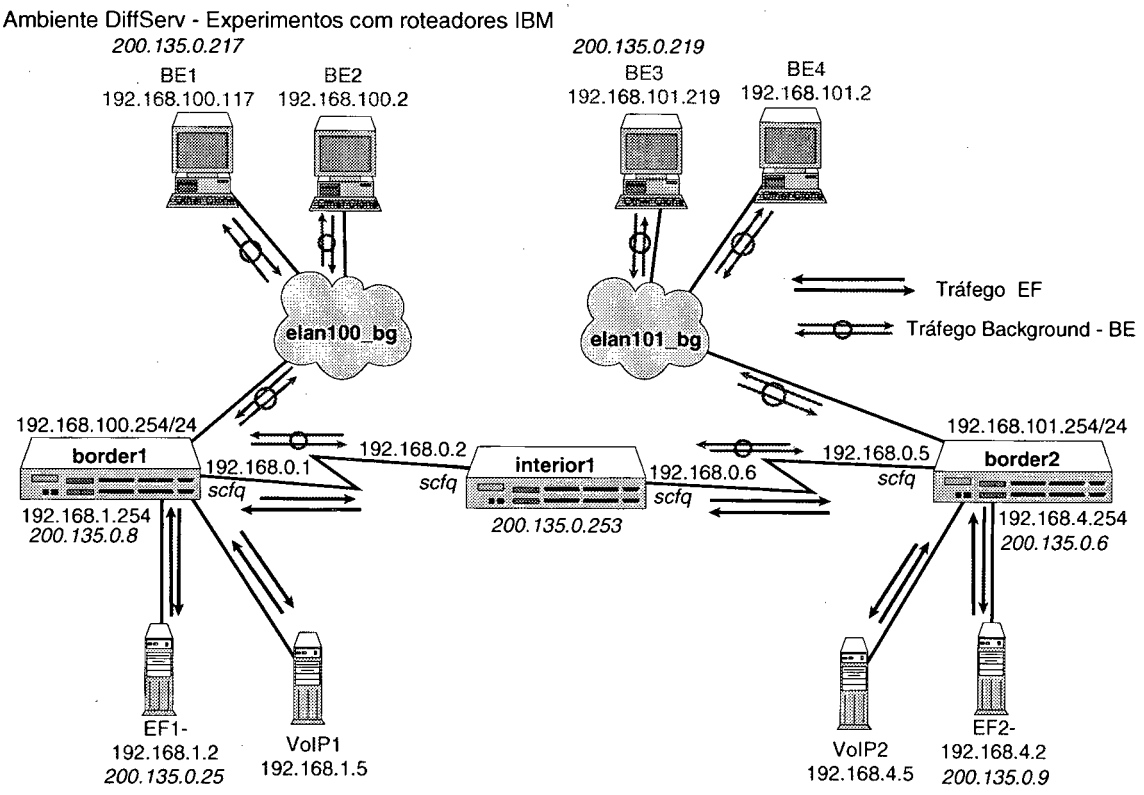


Figura 6-3 – Ambiente DS com roteadores IBM e conexões PPP

6.2.4 Ambiente DS com roteadores CISCO

O propósito geral deste ambiente é avaliar o tráfego EF para suporte a aplicações com requisitos rígidos QoS, como aplicações vídeo e voz sobre IP em redes WAN de média e alta velocidade.

6.2.5 Fundamentos da implementação DS nos roteadores CISCO

Nos roteadores CISCO, o suporte a DS é obtido através de um mecanismo chamado CAR (*Committed Access Rate*) [18], que implementa diversas funções como descritas a seguir, em conjunto com algoritmos de priorização de pacotes utilizados nas interfaces em caso de congestionamento.

De forma geral, pode-se descrever CAR como responsável pelas seguintes funções:

- ***classificação multi-campo (MF) dos pacotes***: A classificação MF é aplicada ao tráfego na direção de entrada no roteador de ingresso. As classes de tráfego podem ser definidas através de listas de controle de acesso estendidas (ACL). Nos experimentos realizados neste trabalho, esta classificação foi feita segundo os endereços IP fonte e destino, protocolo de transporte em uso (TCP/UDP) e pelas portas dos protocolos;
- ***marcação ou re-marcação dos pacotes***: Através da marcação, feita no roteador, mesmo o tráfego gerado por uma aplicação que não implementa DS pode ser marcado com uma dada precedência. A re-marcação é fundamental quando um roteador está localizado no limite entre dois domínios Diffserv e o valor atual de precedência do pacote necessita ser substituído por um valor diferente. Por esta razão, a remarcação habilita a interoperabilidade entre diferentes domínios DS; e
- ***policiamento***: O limiar superior da taxa de bits é definido e associado a uma classe de tráfego. Semelhante a marcação, policiamento é uma função do roteador de borda. O policiamento pode ser utilizado para assegurar acordos de níveis de serviços (SLAs), como por exemplo, para limitar para uma classe de tráfego uma taxa de bits especificada. Policiamento é importante para assegurar alocação justa de recursos. A implementação de policiamento requer a utilização da medição de tráfego. No ambiente CISCO a medição e o policiamento são implementados através de um mecanismo do tipo balde de *tokens* (ver seção 4.2.2). O tráfego EF utilizando WFQ (*Weighted Fair*

Queuing) (ver seção 4.1.4), está sujeito a policiamento no roteador de ingresso para assegurar que a taxa de partida configurada é superior a taxa de chegada e que o *atraso de fila* introduzido pelo sistema de enfileiramento é minimizado. Por outro lado, o enfileiramento PQ (*Priority Queue*), (ver seção 4.1.2), assegura que somente a fração limitada do tráfego é injetada na fila de alta prioridade, prevenindo, desta forma, que o restante do tráfego não seja prejudicado em excesso.

Para uma determinada interface, o mecanismo CAR pode ser empregado para o tráfego de entrada e saída, e para interfaces físicas ou lógicas. No Anexo II – Configuração DS no ambiente CISCO, é mostrada a sintaxe geral do comando que implementa o mecanismo CAR bem como os outros parâmetros de configuração DS para os roteadores CISCO.

6.2.6 Topologia do ambiente CISCO

No ambiente CISCO (Figura 6-4) tem-se um ambiente de redes de alta velocidade. A rede é baseada em conexões PVCs ATM cuja largura de banda foi definida em 2 Mbps. Os blocos funcionais DS (classificação, marcação, medição e escalonamento) são habilitados somente no primeiro nó DS (roteador CISCO 7507) em função de restrições apresentadas pelo outro equipamento. No Anexo II – Configuração DS no ambiente CISCO são mostradas em detalhes as configurações referentes a DS realizadas no ambiente CISCO.

O ambiente é constituído por quatro redes locais interligadas por uma rede WAN. As redes 192.168.11.0/24 e 192.168.14.0/24 são utilizadas para geração do tráfego EF através das estações EF1 e EF2. As redes 192.168.150.0/24 e 192.168.151.0/24 são utilizadas para geração do tráfego melhor esforço em *background*, através das estações BE1 e BE2. A estação "vídeo server" é utilizada para transmissão de vídeo e a estação "vídeo visualização" para a visualização e captura de estatísticas de desempenho da rede.

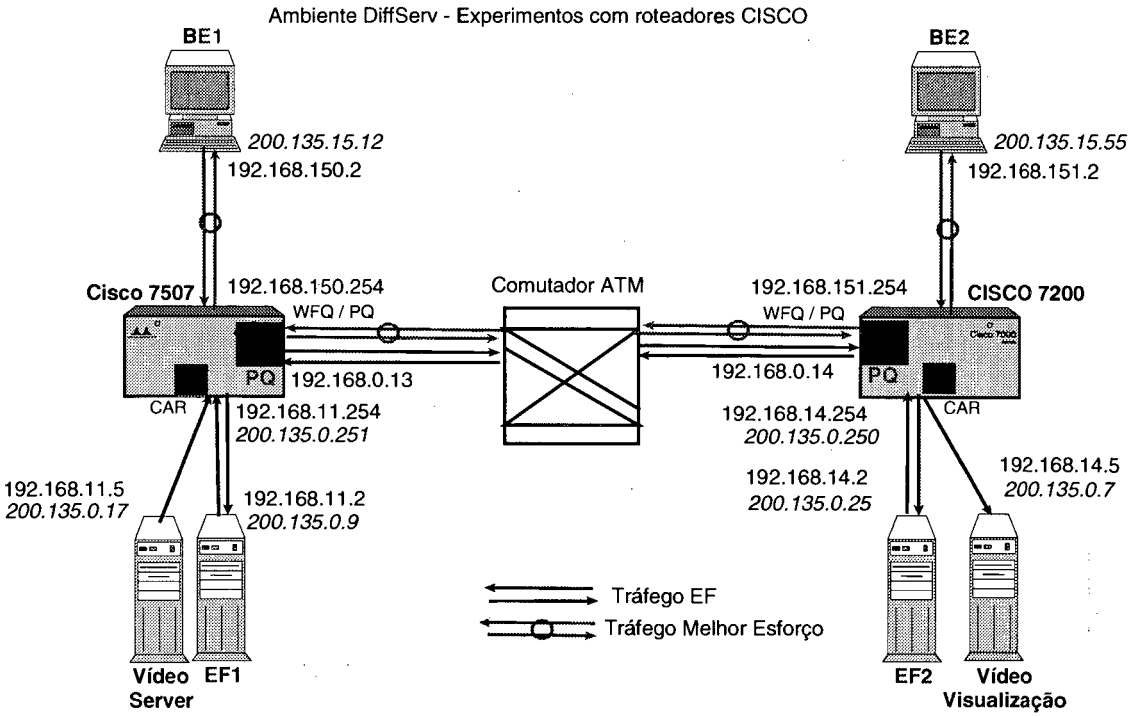


Figura 6-4 – Ambiente DS com roteadores CISCO e conexões ATM

6.2.7 Objetivos dos experimentos

Em ambos os ambientes os objetivos principais dos experimentos são basicamente os mesmos e serão detalhados nas seções que seguem.

6.2.7.1 Análise quantitativa

- Avaliar a influência do tráfego melhor esforço sobre os parâmetros de atraso, variação do atraso e taxa de perda de pacotes do tráfego EF;
- Estudar a influência da agregação de tráfego EF no desempenho fim-a-fim quando comparado a um tráfego EF isolado; e
- Avaliar a adequação da classe de tráfego EF aos requisitos do tráfego de aplicações de áudio e vídeo.

6.2.7.2 Análise qualitativa

- No ambiente IBM, de baixa velocidade, realizar chamadas de voz (VoIP) e analisar a qualidade desta em condições de rede congestionada e não congestionada, com DS habilitado e com DS não habilitado; e
- No ambiente CISCO realizar a transferência de fluxos de áudio e vídeo e analisar a qualidade dessas aplicações em condições de rede congestionada e não congestionada com DS habilitado e DS não habilitado.

6.2.8 Método utilizado nas medições

Em linhas gerais o método utilizado para a realização das medições consiste na:

- determinação do perfil da rede em condições normais;
- avaliação do RTT com DS habilitado e DS não habilitado;
- definição das métricas para avaliação do atraso, variação do atraso e taxa de perda de pacotes;
- escolha das ferramentas para geração e medição do tráfego;
- definição das políticas de classificação e marcação dos pacotes;
- sincronização dos relógios nas estações de medição;
- execução das medições; e
- sumarização e análise dos resultados.

Cada um destes tópicos será detalhado a seguir.

6.2.8.1 Determinação do perfil da rede

Esta etapa no processo de análise experimental de serviços diferenciados visa monitorar o desempenho da rede em condições normais de tráfego com DS não habilitado. Dados de vazão, TCP e UDP, bem como, RTT (*Round Trip Time*) são coletados com objetivo de determinar o perfil de funcionamento normal da rede.

- **RTT**

A avaliação do RTT permite verificar se as conexões estão totalmente livres de perdas e que o RTT apresenta valores constantes. Nestes testes, o RTT entre os sistemas finais EF1 e EF2 é medido com pacotes de 84 Bytes (64 de carga e 20 do cabeçalho IP), pois é o valor padrão nos sistemas Linux utilizados nas medições.

- **Vazão TCP**

O perfil da rede quanto ao tráfego TCP do tipo melhor esforço foi determinado através da medição da vazão e do número de transações TCP por segundo. O tráfego foi gerado e medido utilizando-se a ferramenta Netperf [32], descrita no item 13.2.

No ambiente IBM a vazão de um fluxo TCP do tipo melhor esforço foi medida de modo a estimar o desempenho máximo obtido no conjunto de canais PPP que interligam os sistemas de medição. A vazão máxima teórica para esse canal PPP é de 63,65 Kbps, conforme estimativa efetuada através das seguintes expressões:

PacotesPorSegundo = VelocidadeDoCanal / (TamanhoMaximoDoPacote * BitsPorByte) Vazão = (TamanhoMaximoDoPacote – CabeçalhoPPP) * PacotesPorSegundo * BitsPorByte / 1000
Onde: - BitsPorByte = Número de bits por byte = 8; - PacotesPorSegundo = número máximo de pacotes transmitidos por segundo; - VelocidadeDoCanal = Taxa de bits nominal do canal em bits por segundo; - TamanhoMaximoDoPacote = Tamanho padrão do pacote TCP utilizado pelo software Netperf nas medições em bytes; e - CabeçalhoPPP = Tamanho em bytes do cabeçalho do frame PPP = 8.

Tabela 6-4 – Cálculo da vazão teórica máxima em um canal PPP

Pelas expressões acima se obtêm a seguinte vazão máxima para o canal PPP.

PacotesPorSegundo = 64000 / (1500*8) = 5,33;

Vazão máxima teórica = (1500-8)*5,33*8/1000 = 63,65 Kbps.

No ambiente CISCO a vazão foi medida para estimar o desempenho máximo obtido no PVC ATM que interliga os sistemas de medição. A vazão máxima teórica para esse canal ATM, após a retirada da sobrecarga do cabeçalho da célula, pode ser estimada através das seguintes expressões:

Vazão = CelulasPorPacote * (TamanhoDaCelula – CabecalhoCelula) * BitsPorByte * PacotesPorSegundo; CelulasPorPacote = (TamanhoMaximoDoPacote / (TamanhoDaCelula –CabecalhoCelula); PacotesPorSegundo = VelocidadeDoCanal / (TamanhoMaximoDoPacote + (CelulasPorPacote*CabecalhoCelula)) * BitsPorByte);
Onde: - BitsPorByte = Número de bit por byte = 8; - PacotesPorSegundo = número máximo de pacotes transmitidos por segundo; - CelulasPorPacote = Número de células ATM por pacote; - VelocidadeDoCanal = Taxa de bits nominal do canal em bits por segundo; - TamanhoMaximoDoPacote = Tamanho padrão do pacote TCP utilizados pelo software Netperf nas medições em bytes; e - CabeçalhoCelula = Tamanho em bytes do cabeçalho da célula ATM = 5.

Tabela 6-5 - Cálculo da vazão teórica máxima em um PVC ATM

Pelas expressões acima se obtêm a seguinte vazão máxima para o PVC ATM:

CelulasPorPacote = (1500 / (53-5) = 32;

PacotesPorSegundo = 2.000.000 / ((1500 + (32*5)) * 8) = 150;

Vazão teórica máxima = 32 * (53 – 5) * 8 * 150 = 1.843 Mbps.

- **Vazão UDP**

A vazão máxima de um canal pode também ser obtida utilizando-se um ou mais fluxos UDP. Através da ferramenta *MGEN,* descrita em 13.1, foram gerados fluxos UDP bidirecionais com frame de 1500 bytes (1472 bytes de carga + 28 bytes de cabeçalho) com taxa de pacotes por segundo suficiente para consumir toda a capacidade dos canais de comunicação. A Tabela 6-6 mostra para os ambientes IBM e CISCO os parâmetros utilizados para configurar a ferramenta de geração do tráfego para obtenção da vazão UDP.

Ambiente	Velocidade do Canal	Tamanho do pacote em bytes	Taxa de pacotes por segundo	Vazão Máxima possível
IBM	64 Kbps	1500	6	72 Kbps
CISCO	2000 Kbps	1500	166	1992 Kbps

Tabela 6-6 – Taxa de pacotes por segundo e vazão máxima gerada

6.2.8.2 Avaliação do RTT

Antes de passar efetivamente à medição dos parâmetros selecionados, através da aplicação PING, foi verificado o comportamento do tráfego *ICMP Echo Request* e *ICMP Echo Reply,* classificado como tráfego EF e também como tráfego BE na presença de um tráfego melhor esforço UDP intenso em *background.*

Para o ambiente IBM o tráfego melhor esforço em *background* foi gerado com o MGEN a uma taxa 64 Kbps, ou oito pacotes de 1000 bytes por segundo, em ambos os sentidos.

Para o ambiente CISCO a taxa foi de aproximadamente 2000 Kbps, ou 250 pacotes de 1000 bytes por segundo.

Nesta avaliação são efetuadas as seguintes medições sobre o tráfego ICMP com DS habilitado e com DS não habilitado:

- tempo de ida e volta (RTT) dos pacotes ICMP com e sem tráfego UDP *background*; e
- taxa de perda de pacotes ICMP com e sem tráfego UDP *background.*

6.2.8.3 Métricas de QoS utilizadas

Foram medidas as métricas definidas no item 5.6.3, ou seja:

- o *atraso*;
- a *variação do atraso* (IPDV-jitter); e

- a *taxa de perda* de pacotes.

6.2.8.4 Ferramentas para geração e medição do tráfego

Os componentes de software (mgen, drec, e mcalc) da família MGEN [39] foram utilizados, respectivamente, para geração, recepção e processamento (obtenção dos valores de medição) dos dados do tráfego EF. Esta ferramenta utiliza a noção de "*host time*" conforme descrito na seção 5.6.3 para efetuar a medição do atraso em um sentido. Para o tráfego em *background*, utilizado para congestionamento da rede, foram utilizados os módulos (mgen, drec) no caso do tráfego UDP e o Netperf para o tráfego TCP. No Anexo III – Ferramentas de geração e medição do tráfego pode-se encontrar uma descrição detalhada das ferramentas, os parâmetros configurados, bem como cópia dos *scripts* utilizados nas medições.

6.2.8.5 Sincronização dos relógios

A medição do atraso fim-a-fim em um sentido exige que os relógios das estações de medição, geradora e receptora do tráfego, estejam sincronizados dentro de uma determinada precisão. Neste caso, as duas estações tiveram seus relógios sincronizados através do NTP (*Network Time Protocol*) com uma precisão superior a 10 ms que é suficiente para esta aplicação. Esta precisão no ajuste dos relógios das estações de medição foi obtida através da sincronização de ambas as estações a cada minuto, com base em um único servidor de NTP posicionado em um segmento de rede ethernet específico e compartilhado também pelas estações de medição.

6.2.8.6 Tempo e número de repetições das medições

Para garantir que os experimentos realizados possam ser repetidos e que os resultados serão semelhantes aos obtidos nestes experimentos, todas as medições tiveram a duração de 5 (cinco) minutos e foram repetidas 10 vezes. O número de 10 medições foi considerado suficiente em virtude da baixa variação observada nos resultados entre as medições, haja visto ser um ambiente dedicado.

6.2.8.7 Classificação, marcação e encaminhamento dos pacotes

No ambiente IBM, a classificação e marcação dos pacotes foram feitas nos roteadores de borda (*border1* e *border2*). O tráfego EF foi classificado em função do endereço fonte e destino (classificação MF) e foi marcado com o DSCP xF8 para receber tratamento prioritário nas interfaces de saída de *border1* e border2. No nó *interior1* o

tráfego EF que foi marcado com o DSCP xF8 sofre uma classificação de comportamento agregado, classificação BA e também recebe tratamento diferenciado e prioritário nas interfaces de saída através do algoritmo SCFQ. O restante do tráfego recebe o tratamento padrão da rede com melhor esforço.

No ambiente CISCO a marcação e classificação dos pacotes foram feitas somente em um dos roteadores o CISCO 7507. Na interface de entrada foi feita a classificação MF com base no endereço IP origem e destino da rede. Os pacotes classificados como tendo origem na rede 192.168.11.0/24 e destino na rede 192.168.14.0/24 foram marcados com DSCP 46. Na interface de saída estes sofrem uma classificação de comportamento agregado (BA) e são encaminhados para o canal de transmissão através do algoritmo Priority Queue (seção 4.1.2) definido nessa interface para essa classe de tráfego.

6.2.8.8 Geração e medição do tráfego expresso - EF

Cada um dos experimentos envolveu a utilização de 2 (duas) estações com sistema operacional Linux Red Hat 7.0. O tráfego EF gerado era constituído de fluxos UDP a uma taxa constante (CBR). O canal de comunicação é *full-duplex* e a estação que transmite, ao mesmo tempo recebe o fluxo de bits da outra estação, tendo desta forma o comportamento de uma aplicação com tráfego bidirecional. Em função das capacidades diferentes dos canais de comunicação nos dois ambientes existem algumas considerações:

- **Ambiente IBM**

A largura de banda reservada para o tráfego EF foi de 40 Kbps nos experimentos com 5 fluxos EF e 24 Kbps nos experimentos com 1 e 3 fluxos EF. A taxa de transmissão utilizada foi de 13 pacotes de 68 bytes por segundo que equivale a 7,072 Kbps para cada fluxo transmitido. Este valor foi utilizado por estar próximo dos valores dos fluxos de voz em rede de pacotes e em função da própria limitação da largura de banda total do canal.

Um fluxo de voz na rede ocupa entre 8 e 14 Kbps dependendo da compactação utilizada, e cada pacote tem no mínimo 50 bytes (20 bytes do cabeçalho IP, 8 bytes do cabeçalho UDP, 12 bytes de cabeçalho RTP e 10 bytes do frame de voz) [36], [19]. Como mais de um frame pode ser colocado em um pacote por vez considerou-se um pacote médio de 68 bytes (40 bytes de carga e 28 de cabeçalho).

- **Ambiente CISCO**

A largura de banda reservada para o tráfego EF foi de 344 Kbps. Esta quantidade foi escolhida por ter a capacidade de suportar um fluxo de vídeo codificado no padrão *Real Server* da ordem de 230 Kbps. O tráfego EF foi gerado com pacotes de 68 bytes, incluindo a sobrecarga IP e UDP com a taxa de 450 pps, equivalente a uma taxa de bits de 244,8 Kbps. Essa taxa de pacotes foi escolhida após constatar-se que, acima desse valor, a taxa de perda de pacotes subia acima de 0,01 por cento com um fluxo EF apenas. Essa taxa de perdas provavelmente ocorreu por deficiência da ferramenta de medição em capturar, na estação de recepção, todos os pacotes transmitidos.

6.2.8.9 Geração do tráfego melhor esforço - BE

Duas estações Linux Red Hat 7.0 foram utilizadas para geração do tráfego BE em *background*, utilizado para congestionar o canal de comunicação. Este tráfego gerado e transmitido pode ser TCP ou UDP a uma vazão constante de 64 Kbps e 2000 Kbps, respectivamente, no ambiente IBM e no ambiente CISCO, variando-se o tamanho do pacote e taxa de pacotes por segundo. A Tabela 6-7 e Tabela 6-8 mostram os parâmetros do tráfego de *background* associados ao ambiente IBM e a Tabela 6-9 e Tabela 6-10 os parâmetros associados ao ambiente CISCO.

Tamanho da carga (bytes)	Tamanho do cabeçalho (bytes)	Tamanho do pacote (bytes)	Taxa de transmissão (pps)	Vazão (Kbps)
996	28	1024	7	57,34
484	28	512	15	61,44
228	28	256	31	63,49
100	28	128	62	63,49
36	28	64	125	64,00
0	0	0	0	0

Tabela 6-7 – Vazão do tráfego UDP em *background – ambiente IBM*

Pode-se notar que existe uma diferença na vazão entre as duas tabelas. Na tabela referente ao tráfego UDP, que é um protocolo sem confirmação, essa é a vazão que chega na interface de entrada no sistema de transmissão, sendo que o tráfego excedente é descartando.

Na tabela referente ao tráfego TCP o valor da vazão é obtido através da medição do número de transações TCP por segundo que o *Netperf* consegue efetuar dependendo do

tamanho do pacote. O valor da vazão TCP é reduzido na medida em que se reduz o tamanho do pacote em virtude da confirmação de cada transação.

Tamanho da carga (bytes)	Tamanho do cabeçalho (bytes)	Tamanho do pacote (bytes)	Taxa de transmissão (pps)	Vazão (Kbps)
992	32	1024	1,60	26,21
480	32	512	2,89	23,67
224	32	256	5,29	21,67
96	32	128	6,60	13,51
32	32	64	10,06	10,31
0	0	0	0	0

Tabela 6-8 – Vazão do tráfego TCP em *background – ambiente IBM*

Tamanho da carga (bytes)	Tamanho do cabeçalho (bytes)	Tamanho do pacote (bytes)	Taxa de transmissão (pps)	Vazão (Kbps)
1472	28	1500	166	1992,00
996	28	1024	244	1998,85
484	28	512	488	1998,85
228	28	256	976	1998,85
100	28	128	1953	1999,87
36	28	64	3906	1999,87
0	0	0	0	0

Tabela 6-9 – Vazão do tráfego UDP em *background* – ambiente CISCO

Tamanho da carga (bytes)	Tamanho do cabeçalho (bytes)	Tamanho do pacote (bytes)	Transações por segundo	Vazão (Kbps)
1448	52	1500	80,20	962,44
972	52	1024	115,10	942,90
460	52	512	214,47	878,47
204	52	256	340,92	698,19
76	52	128	411,75	421,63
12	52	64	494,71	253,29
0	0	0	0	0

Tabela 6-10 – Vazão do tráfego TCP em *background* – ambiente CISCO

6.2.8.10 Sumarização dos resultados

Ao final de cada medição foi gerado na estação receptora um arquivo contendo dados que permitem extrair as seguintes informações:

- atraso;
- variação do atraso; e

- taxa de perdas.

Através da aplicação *mcalc*[39] estas informações foram obtidas, em seguida tabuladas e sumarizadas para geração dos gráficos apresentados e analisados ao longo do trabalho.

6.3 Considerações finais sobre este capítulo

Ao longo deste capítulo, procurou-se descrever o ambiente de experimentação, as ferramentas utilizadas nas medições, as capacidades nominais dos ambientes e os parâmetros de configuração DS. O método de medição utilizado foi descrito de forma que os experimentos possam ser repetidos e também para que estes resultados possam ser utilizados para a continuidade de pesquisas e experimentos nesta área.

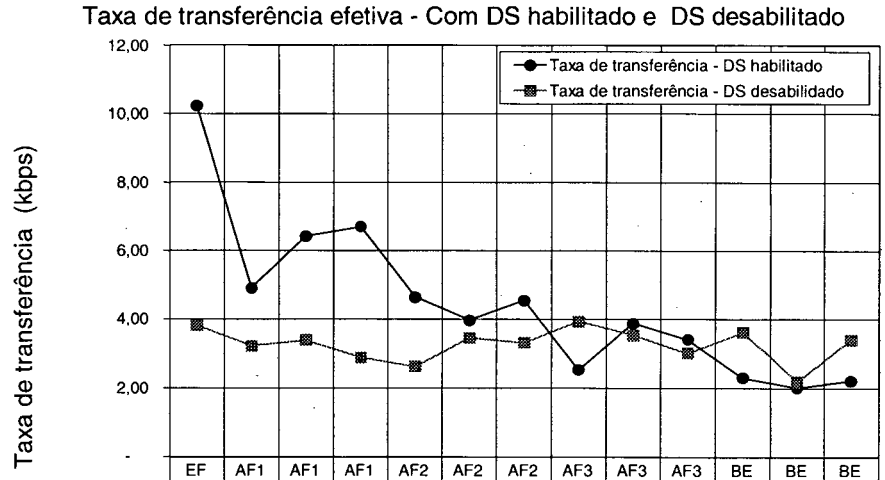
Nos próximos dois capítulos serão apresentados os resultados dos experimentos realizados para que, depois de analisados, possam contribuir para a formulação das conclusões deste trabalho.

7 RESULTADOS E ANÁLISE – FASE I

Na fase I, utilizando-se de um ambiente DS com roteadores IBM, definiu-se como meta principal avaliar DS de forma geral através da medição dos parâmetros vazão, atraso e da obtenção nos nós DS de informações sobre descarte e marcação de pacotes. Nesta etapa do trabalho foi avaliado o comportamento das classes de serviço BE, EF e AF.

7.1 Avaliação da vazão

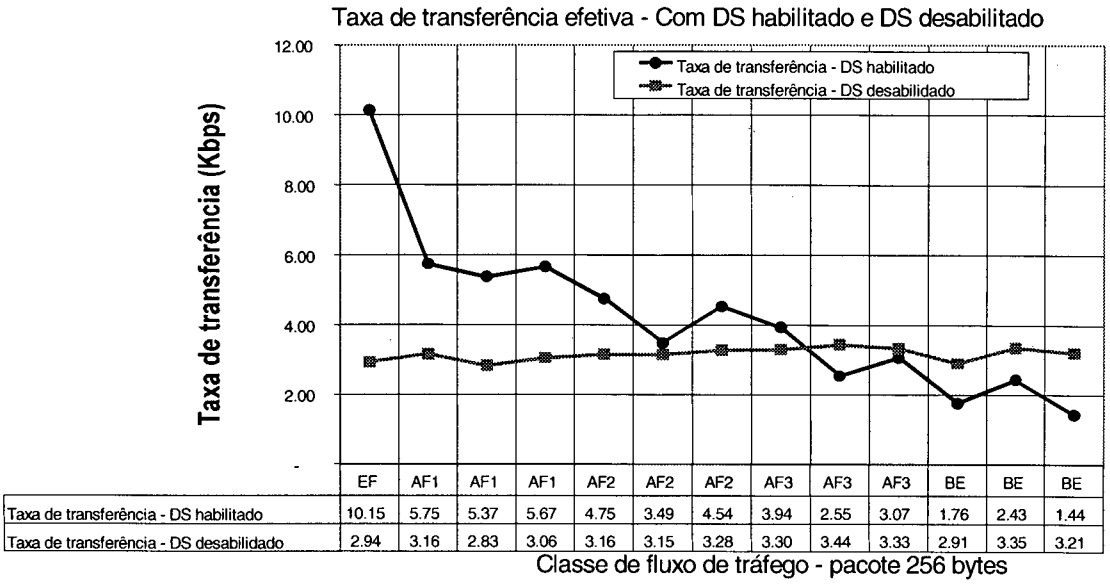
Os gráficos apresentados na Figura 7-1, Figura 7-2 e Figura 7-3 mostram a vazão medida por fluxo transmitido na situação de rede com DS habilitado e com DS não habilitado. Nota-se que, independentemente do tamanho do pacote, as curvas são aproximadas. No caso dos fluxos agregados das 3 classes AF (AF1, AF2, AF3) a vazão média em Kbps é proporcional à largura de banda reservada (Tabela 6-2) o que comprova a capacidade de isolamento de tráfego e gerenciamento da largura de banda pela implementação DS. As curvas que representam as medições dos mesmos fluxos de tráfego sem habilitar DS tendem a obter vazão semelhante (entre 2 e 4 Kpbs).



	EF	AF1	AF1	AF1	AF2	AF2	AF2	AF3	AF3	AF3	BE	BE	BE
Taxa de transferência - DS habilitado	10,25	4,91	6,43	6,71	4,64	3,97	4,55	2,53	3,88	3,41	2,30	2,02	2,21
Taxa de transferência - DS desabilidado	3,82	3,23	3,39	2,89	2,62	3,46	3,32	3,94	3,53	3,01	3,62	2,20	3,40

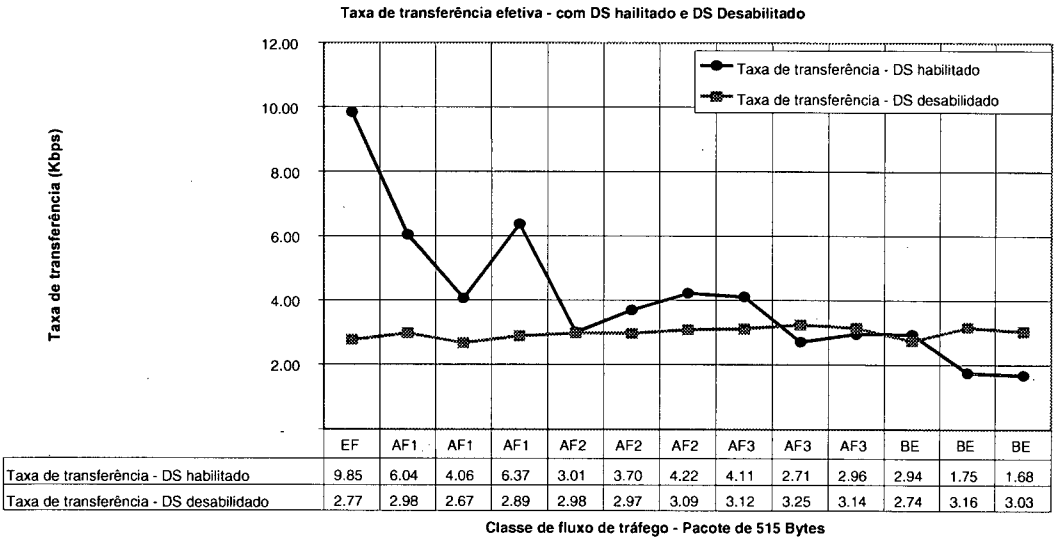
Classe de fluxo de tráfego - pacotes 128 bytes

Figura 7-1 – Vazão por fluxo de tráfego – pacote 128 bytes



	EF	AF1	AF1	AF1	AF2	AF2	AF2	AF3	AF3	AF3	BE	BE	BE
Taxa de transferência - DS habilitado	10.15	5.75	5.37	5.67	4.75	3.49	4.54	3.94	2.55	3.07	1.76	2.43	1.44
Taxa de transferência - DS desabilidado	2.94	3.16	2.83	3.06	3.16	3.15	3.28	3.30	3.44	3.33	2.91	3.35	3.21

Figura 7-2 – Vazão por fluxo de tráfego – pacote 256 bytes



	EF	AF1	AF1	AF1	AF2	AF2	AF2	AF3	AF3	AF3	BE	BE	BE
Taxa de transferência - DS habilitado	9.85	6.04	4.06	6.37	3.01	3.70	4.22	4.11	2.71	2.96	2.94	1.75	1.68
Taxa de transferência - DS desabilidado	2.77	2.98	2.67	2.89	2.98	2.97	3.09	3.12	3.25	3.14	2.74	3.16	3.03

Figura 7-3 – Vazão por fluxo de tráfego – pacote 512 bytes

7.2 Largura de banda definida versus vazão efetiva

Os gráficos apresentados na Figura 7-4, Figura 7-5 e Figura 7-6, mostram com DS habilitado, uma significativa semelhança de comportamento. Esta semelhança indica a efetividade da formatação do tráfego em relação às políticas definidas, pois de forma geral, a vazão medida para as classes AF é superior à largura de banda definida, tendo em vista que estas podem alocar *buffers* compartilhados, reservados para este fim na implementação do roteador utilizado, e que pelo padrão DS podem obter largura de banda superior a definida.

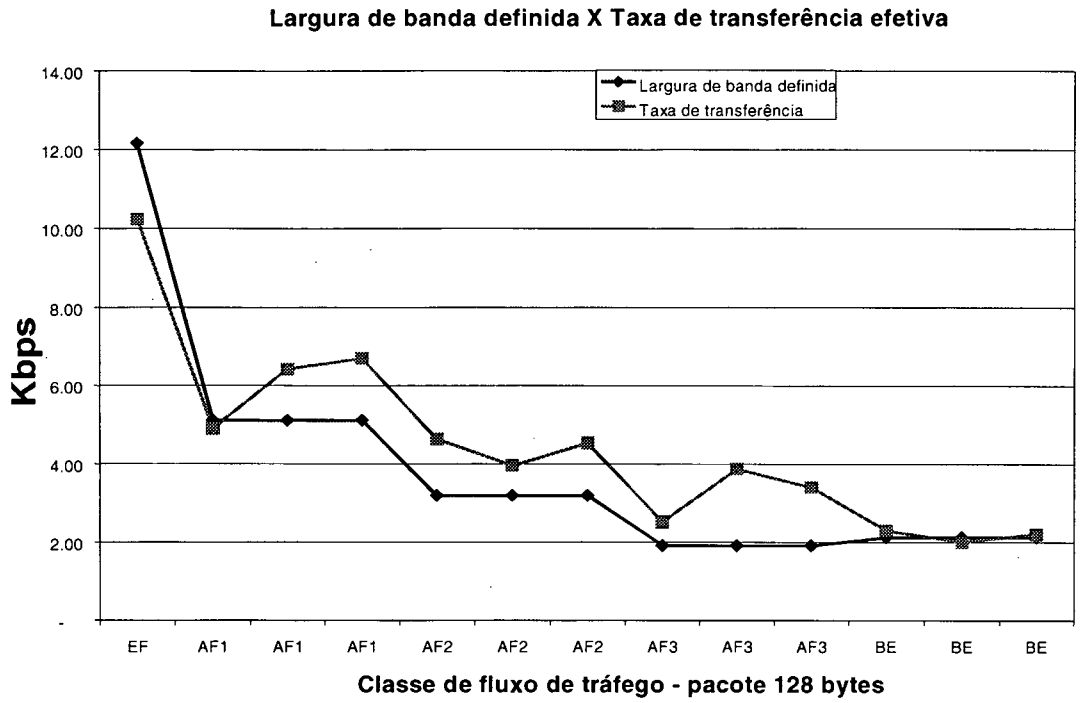


Figura 7-4 – Vazão medida vs. largura de banda definida - pacote 128 *bytes*

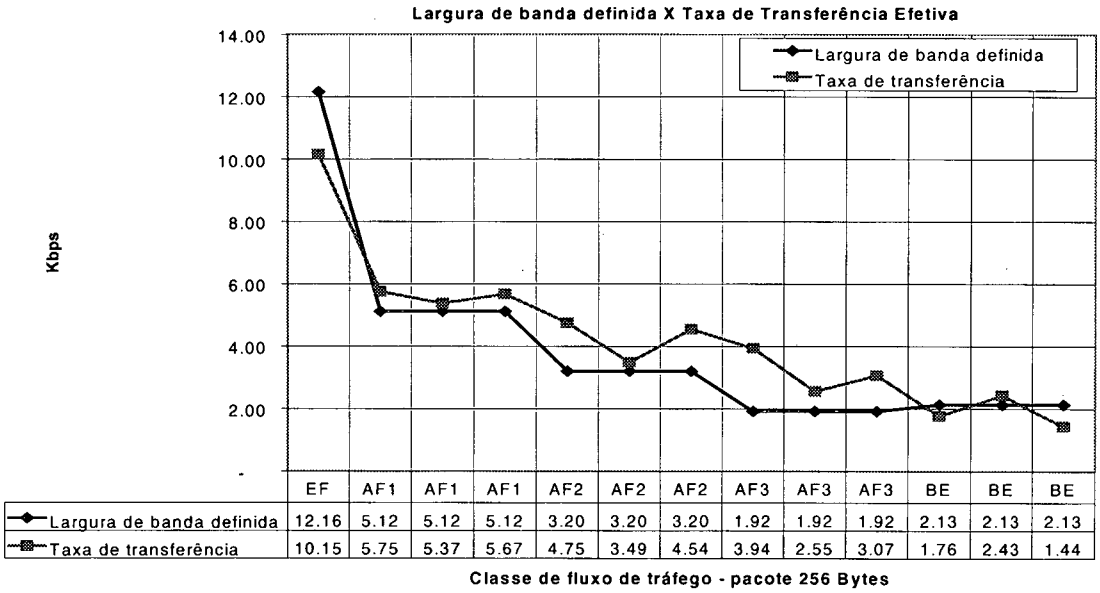
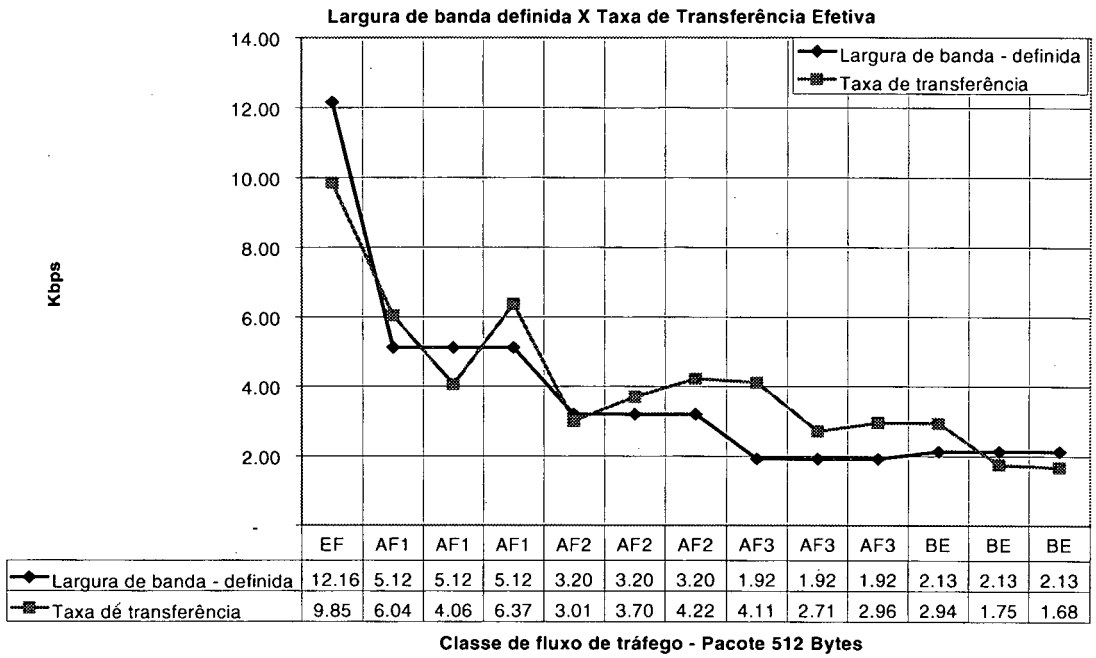


Figura 7-5 – Vazão medida vs. largura de banda definida – pacote 256 bytes

Os fluxos agregados de cada uma das classes AF (AF1, AF2 E AF3) conseguem obter uma utilização da largura de banda superior, entre 10% e 80%, à definida nas respectivas políticas. Embora a largura de banda seja assegurada para os fluxos agregados, o comportamento individual de cada fluxo é bastante variado. De fato, a

largura de banda assegurada da classe é dividida entre os fluxos, recomendando-se assim, poucos fluxos por classe.



	EF	AF1	AF1	AF1	AF2	AF2	AF2	AF3	AF3	AF3	BE	BE	BE
Largura de banda - definida	12.16	5.12	5.12	5.12	3.20	3.20	3.20	1.92	1.92	1.92	2.13	2.13	2.13
Taxa de transferência	9.85	6.04	4.06	6.37	3.01	3.70	4.22	4.11	2.71	2.96	2.94	1.75	1.68

Figura 7-6 – Vazão medida vs. largura de banda definida – pacote 512 bytes

Nos resultados para o fluxo de tráfego BE, verifica-se que a taxa de transferência efetiva foi ligeiramente inferior (entre 2% e 12%) à largura de banda definida, demonstrando sob a ótica deste indicador um comportamento inadequado que merece investigação futura.

7.3 Visão geral sobre o comportamento da rede

Os gráficos mostrados da Figura 7-7 até a Figura 7-10 permitem uma visão geral sobre o comportamento de DS na rede. No experimento da Figura 7-7 foram transferidos fluxos TCP com pacotes de tamanhos de 128, 256 e 512 bytes em todas as classes de serviço e obtidos o tempo para a transferência de 2048 pacotes. Pode-se observar o comportamento do tráfego EF, onde o tempo de transferência é diretamente proporcional ao tamanho do pacote, indicando a natureza de tráfego CBR (*Constant Bit Rate*) desta classe conforme prevê a arquitetura DiffServ [9], [31] e [50]. O comportamento das curvas apresentadas na Figura 7-8 mostra que a vazão total da rede é maior com DS habilitado do que com DS não habilitado. O ganho neste caso é da ordem de 25% e é praticamente constante.

A Figura 7-9 mostra a utilização da largura de banda definida para cada uma das classes (EF, AF-1, AF-2, AF-3 e BE) bem como a vazão medida. Pode-se notar, em todas as classes, com exceção da classe EF, que a vazão medida foi superior à largura de banda definida. De acordo com o padrão, a classe EF descarta pacotes que excedem a largura de banda alocada e as classes AF podem utilizar largura de banda compartilhada e não utilizada pelas outras classes AF [33].

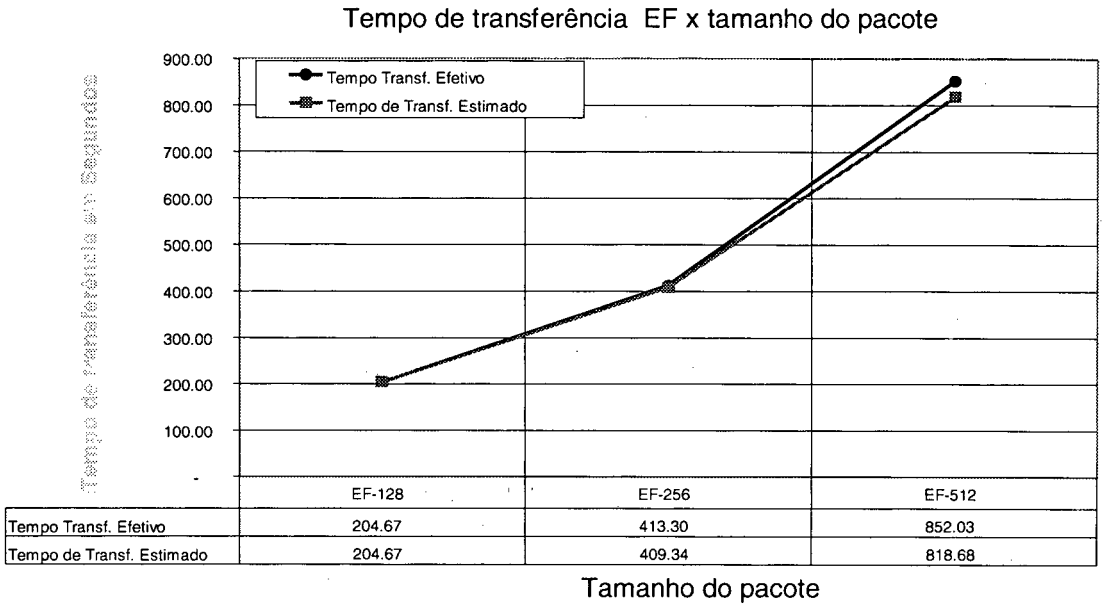


Figura 7-7 –Tempo de transferência vs. tamanho do pacote (bytes) na classe EF

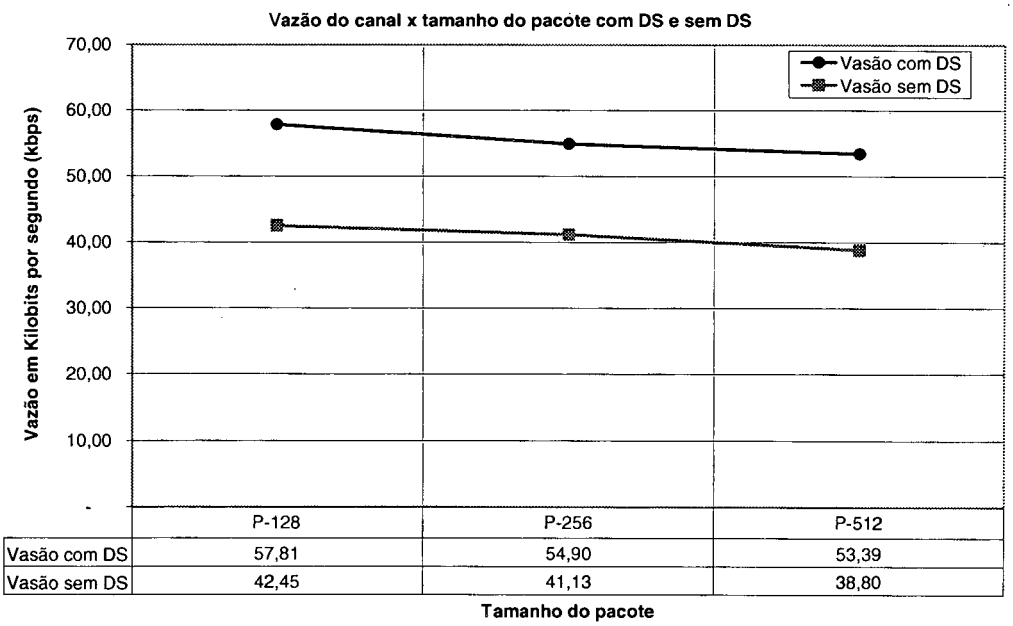
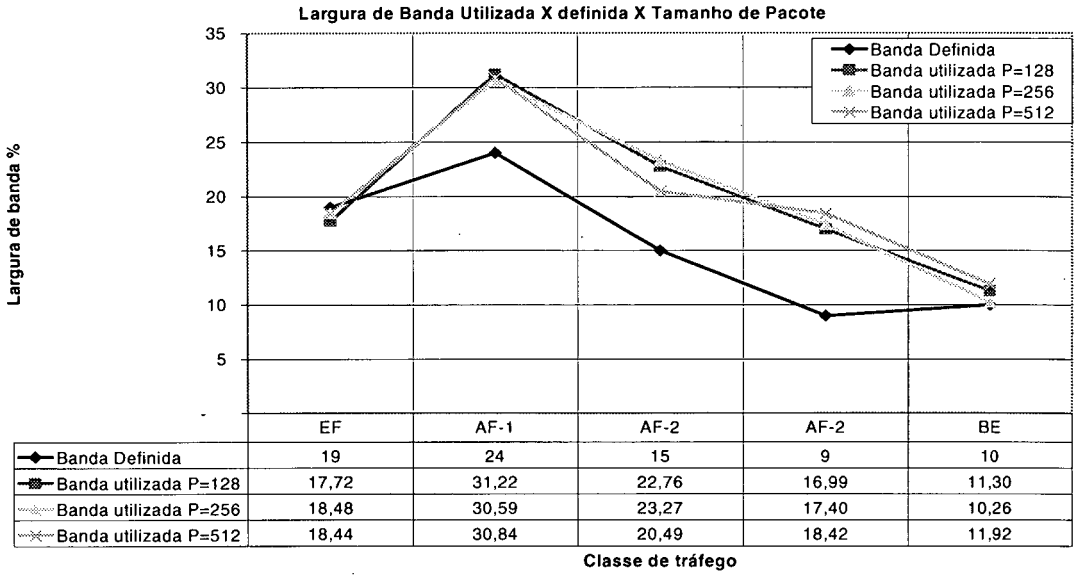


Figura 7-8 – Vazão vs. tamanho do pacote (bytes) - DS habilitado e DS não habilitado



	EF	AF-1	AF-2	AF-2	BE
Banda Definida	19	24	15	9	10
Banda utilizada P=128	17,72	31,22	22,76	16,99	11,30
Banda utilizada P=256	18,48	30,59	23,27	17,40	10,26
Banda utilizada P=512	18,44	30,84	20,49	18,42	11,92

Figura 7-9 – Largura de banda definida vs. vazão medida vs. tráfego agregado p/ classe

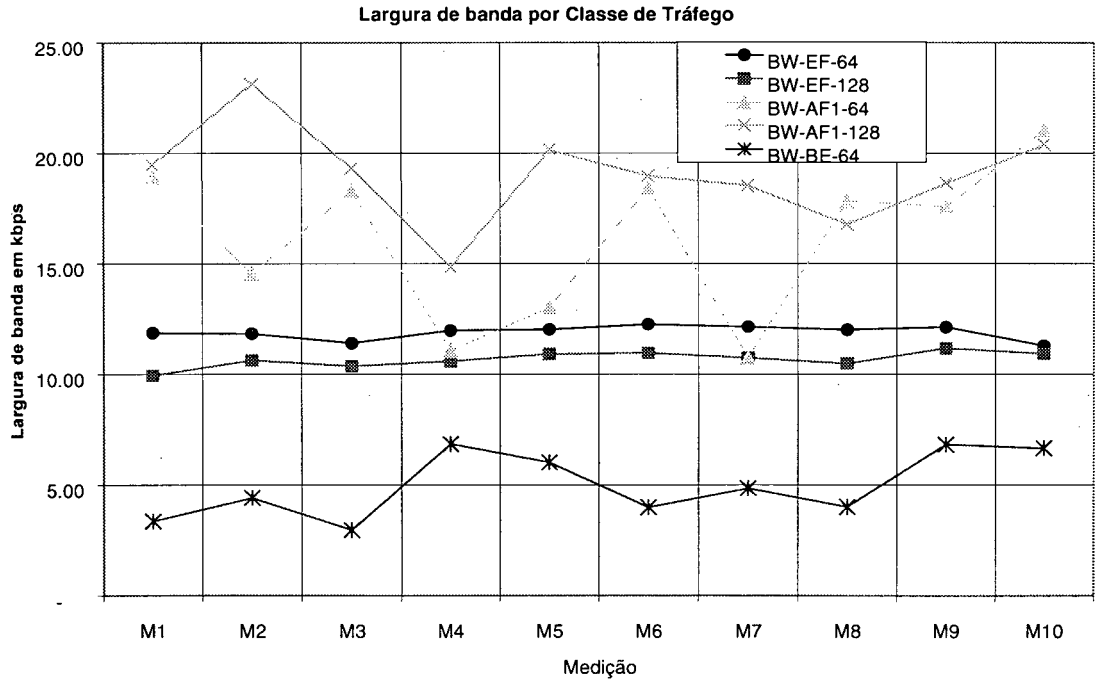


Figura 7-10 – Vazão medida por classe de tráfego, variando tamanho do pacote (bytes)

Na Figura 7-10 pode-se observar a realização de um experimento para verificar o percentual da largura de banda obtido em relação ao que foi definido para cada uma das classes. O experimento foi repetido 10 vezes e, novamente, observa-se que a largura de banda obtida para a classe EF é praticamente constante, enquanto que nas classes AF e

BE existe uma variação a cada medição. Entretanto, pode-se constatar que em todos os casos a classe de serviço consegue utilizar a largura de banda que foi reservada.

7.4 Monitoração dos roteadores

Na Tabela 7-1 são mostradas informações obtidas nos roteadores após a geração de três fluxos de tráfego na rede.

Roteador	Total de Pacotes	Pacotes Enviados	Pacotes enviados em buffers compart.	Descartes de Buffers	Descartes pelas Políticas	Pacotes Marcados verdes	Pacotes Marcados amarelos	Pacotes marcados vermelho
border1								
EF	318	194	0	0	124	N/A	N/A	N/A
AF1	339	339	269	0	0	89	12	238
BE	258	252	221	6	0	N/A	N/A	N/A
C	0	0	0	0	0	N/A	N/A	N/A
Interior1								
EF	194	190	5	0	4	N/A	N/A	N/A
AF1	339	339	6	0	0	64	18	257
BE	252	252	83	0	0	N/A	N/A	N/A
C								

Tabela 7-1 – Monitoração em border1 e interior1 representados na Figura 6-1.

Os fluxos de 128 bytes pertencem às classes (EF, AF e BE). As informações dessa tabela permitem as seguintes constatações:

- **quanto à classe EF:** Nesta classe foram recebidos 318 pacotes na interface de entrada, e destes 194 foram encaminhados através da interface congestionada e 124 pacotes descartados, ou seja, não havia, *tokens* disponíveis (no *Leaky Bucket*) e foram descartados pelo mecanismo de policiamento. Portanto a política usada para este fluxo não estaria adequada ao perfil de tráfego da aplicação e deveria sofrer ajustes para evitar descarte de pacotes. Este ajuste pode se dar no aumento da taxa de transmissão ou aumento da capacidade do *buffer ou ainda através de um ajuste na aplicação (geração de tráfego)*[11]. Para aumentar a largura de banda, pode haver a necessidade de retirar parte da largura de banda definida para os outros fluxos, senão houver disponibilidade. Contudo, aumentar a capacidade do *buffer* pode aumentar o atraso na transmissão dos pacotes; e

[11] A aplicação WSSTTCP não permite o envio controlado de carga, deixando esse ajuste por conta do controle de fluxo do TCP.

- **na classe AF1**, o excesso de tráfego pode ser claramente percebido. De fato, dos 339 pacotes transmitidos, 269 foram enviados usando *buffers* compartilhados e, além disso, houve um grande índice de pacotes marcados como amarelos e vermelhos indicando que muitas vezes o tráfego ultrapassou as taxas de serviços do regulador do serviço AF [24], [33]. A mesma conclusão feita para o serviço EF pode ser efetuada para este serviço, ou seja, a política não está adequada para o perfil de tráfego.

7.5 Conclusões - Fase I

Nesta fase, a montagem de um ambiente para realizar experimentos envolveu a implementação de um modelo representativo de uma WAN, contendo as entidades empregadas para implementar DiffServ, com dois roteadores de borda, um de interior, 13 fontes de fluxo de tráfego TCP (Figura 6-2) e seus respectivos destinatários. Uma vez definidas as políticas, perfis e ações de DiffServ foram realizados experimentos para avaliar o comportamento da rede em termos de taxa de transferência e utilização da largura de banda de cada um dos fluxos em um ambiente altamente congestionado.

Quanto ao tráfego EF foi alocado somente um fluxo. Com os resultados obtidos, pode-se verificar que o tráfego EF mantém um comportamento com pouca variação na taxa de transferência e atraso independente da carga da rede. Esta característica é importante para tráfegos com taxa constante de bits, tais como voz sobre IP.

Com relação ao tráfego AF foram definidas três classes com três fluxos em cada uma delas. Embora a largura de banda seja assegurada para os fluxos agregados, o comportamento individual de cada fluxo foi bastante variado, pois a largura de banda assegurada da classe é dividida entre os fluxos. Desta forma, esta classe é útil para tráfego em rajadas. Entretanto, recomenda-se poucos fluxos por classe, pois as garantias são para fluxos agregados e não para fluxos individuais.

Quanto ao tráfego BE, foram definidos três fluxos. Através dos resultados pode-se verificar que tanto o fluxo BE quanto o fluxo AF obtiveram largura de banda em torno de 13% superior à definida. Isto ocorre provavelmente pelo fato de que nesta

implementação DS não se pode alocar toda a largura de banda disponível. Um percentual deve ser reservado para tráfego de controle e para utilização de *buffers* compartilhados entre todas as classes de tráfego conforme descrito em [33].

Comparando-se o comportamento sem DiffServ habilitado e com DiffServ habilitado conclui-se pela efetividade dos mecanismos de QoS. De fato, os resultados obtidos comprovam que DiffServ, através da classificação, policiamento, marcação e priorização dos pacotes classificados consegue a efetivação dos serviços AF e EF, os quais podem ser utilizados para a implementação de qualidade de serviço em redes IP.

8 RESULTADOS E ANÁLISE – FASE II

Utilizando-se do método descrito na seção 6.2.8 procedeu-se a medição e análise dos dois ambientea DiffServ, o ambiente composto por nós IBM e o ambiente composto por nós CISCO.

8.1 Ambiente IBM

8.1.1 Determinação do perfil da rede – Ambiente IBM

8.1.1.1 RTT

Na Figura 8-1 é mostrado o comportamento desta métrica e na Tabela 8-1 é mostrado o RTT mínimo, médio e máximo, e a taxa de perda de pacotes ocorrida em cada uma das medições e, na última linha, é mostrada a média destes indicadores. Pode-se notar que em todas as seqüências de medições efetuadas não foi verificada a perda de pacotes. Demonstrando que o ambiente encontra-se livre de erros físicos ou mesmo de configuração.

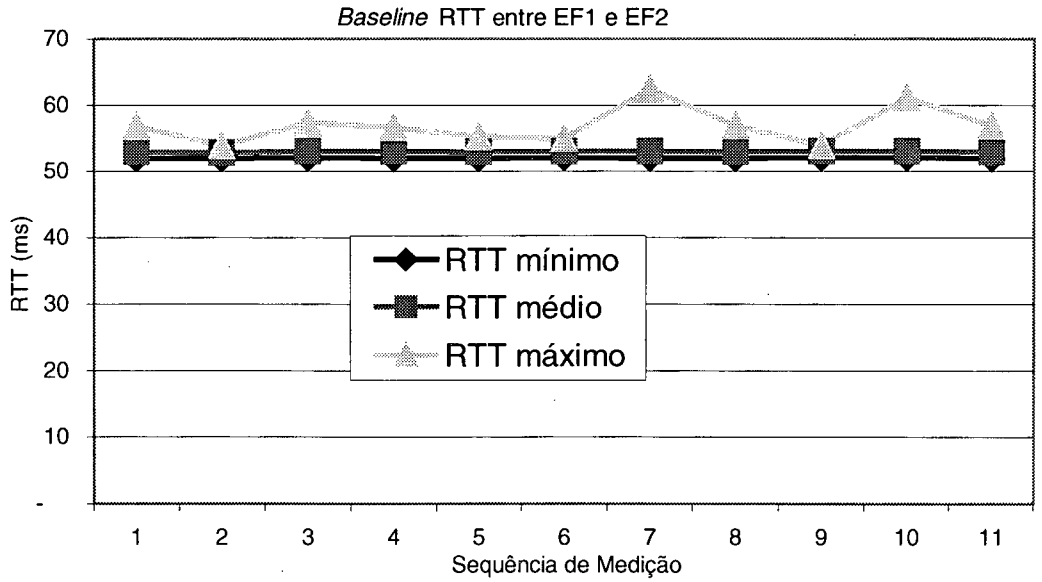


Figura 8-1 - RTT entre os sistemas EF1 e EF2 com pacotes de 84 Bytes

De: EF1 – Para: EF2				De: EF2 – Para: EF1			
RTT mínimo	RTT médio	RTT máximo	Taxa de perdas	RTT mínimo	RTT médio	RTT máximo	Taxa de perdas
52	53	57	0	52	53	56	0
52	53	54	0	52	53	57	0
52	53	57	0	52	53	54	0
52	53	57	0	52	53	55	0
52	53	55	0	52	53	59	0
52	53	55	0	52	53	58	0
52	53	62	0	52	53	56	0
52	53	57	0	52	53	59	0
52	53	54	0	52	53	58	0
52	53	61	0	52	53	61	0
52	**53**	**57**	**0**	**52**	**53**	**57**	**-**

Tabela 8-1 – RTT e taxa de perdas (%) de pacotes entre ef1 e ef2 e entre ef2 e ef1

8.1.1.2 Vazão TCP

A vazão máxima medida foi de aproximadamente 60,1 Kbps enquanto que a vazão máxima teórica para esse canal PPP é de 63,65 Kbps, conforme estimativa efetuada na seção 6.2.8.1. Na Tabela 8-2 e Figura 8-2 é mostrado o aumento da vazão total na medida em que se aumenta o tamanho do pacote, com conseqüente redução do número de transações TCP por segundo. Neste caso a vazão foi calculada a partir da medição do número de transações TCP (Request/Response) utilizando-se o *Netperf*. Uma transação TCP é contada cada vez que a estação de medição de origem receber um pacote em resposta a um pacote enviado anteriormente.

Carga	Cabeçalho	Pacote+ cabeçalho	T-ef1/ segundo	T-ef2/ segundo	T-total/ segundo	Pacotes/ segundo	Vazão (Kbps)
64	52	116	14,21	14,18	28,39	56,78	52,69
128	52	180	9,74	9,71	19,45	38,90	56,02
256	52	308	5,99	5,98	11,97	23,94	58,99
512	52	564	3,36	3,35	6,71	13,42	60,55
1024	52	1076	1,81	1,81	3,62	7,23	62,24

Tabela 8-2 – Vazão TCP melhor esforço variando o tamanho do pacote

As colunas da Tabela 8-2 têm o seguinte significado:

- carga = parte de dados do pacote IP;
- cabeçalho = cabeçalho do pacote incluindo IP e TCP;

- T-ef1/segundo = número de transações TCP (Request/Response) por segundo medidas em EF1;
- T-ef2/segundo = número de transações TCP (Request/Response) por segundo medidas em EF2;
- T-total/segundo = número de transações TCP (Request/Response) total por segundo (EF1 + EF2);
- pacotes/segundo = número de pacotes transmitidos por segundo; e
- vazão = capacidade de transmissão de um canal em uma unidade de tempo.

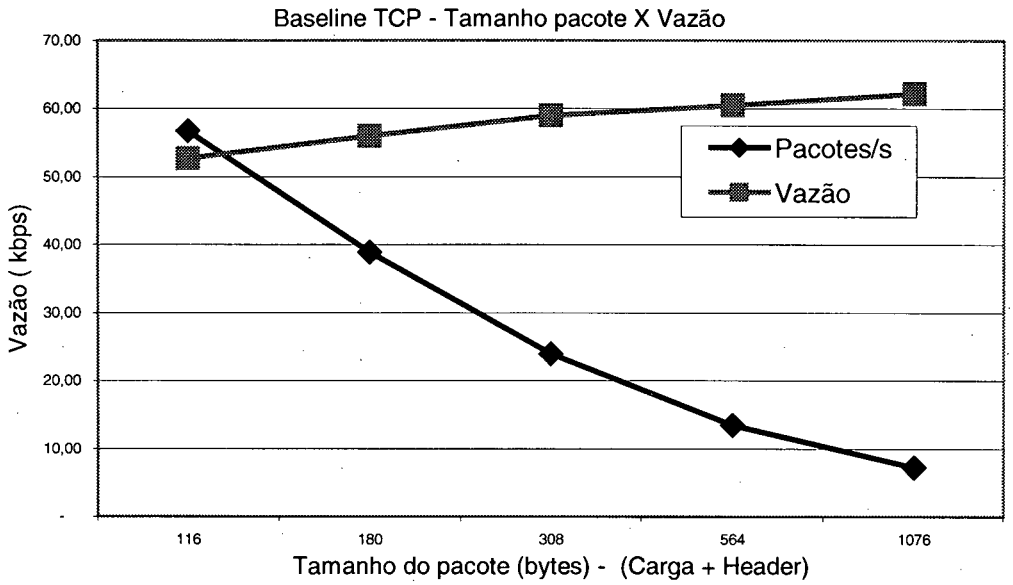


Figura 8-2 - Vazão no canal vs. tamanho do pacote

8.1.1.3 Vazão UDP

De acordo com o método de cálculo da vazão UDP apresentado na seção 6.2.8.1 a taxa de recepção de pacotes por segundo e vazão (Kbps) estimada, em cada um das direções do tráfego, é mostrada na Tabela 8-3.

Métrica	Host BE1	Host BE2
Pacotes/segundo	5,28	5,23
Vazão / Kbps	62,26	61,62

Tabela 8-3 – Número de pacotes recebidos por segundo e vazão

O perfil da rede, determinado através da avaliação do RTT entre as duas redes locais, e da medição da vazão TCP e UDP demonstra que a mesma tem um comportamento e desempenho adequado a tecnologia e a taxa de transmissão dos canais de comunicação.

8.1.2 Avaliação do RTT com e sem DS

Como descrito na seção 6.2.8.2, o tráfego melhor esforço em *background* foi gerado com o MGEN a uma taxa de 64 Kbps ou oito pacotes de 1000 bytes por segundo, em ambos os sentidos. Na Figura 8-3 , Tabela 8-4 e Tabela 8-5 observa-se que:

- o tempo de ida e volta dos pacotes ICMP (RTT) melhor esforço na presença de tráfego *background* UDP intenso apresenta atraso significativamente mais alto em comparação ao RTT do tráfego ICMP quando na classe EF, o que é esperado;
- o tráfego ICMP EF, embora tenha prioridade sobre o tráfego melhor esforço, apresenta significativo aumento no atraso quando comparado ao atraso na rede sem carga, indicando que EF não emula perfeitamente um canal dedicado; e
- embora o tráfego ICMP EF tenha sofrido atraso, não houve perda de pacotes enquanto que no tráfego ICMP melhor esforço, a taxa média de perdas foi de 19% em um sentido e de 10% no outro sentido.

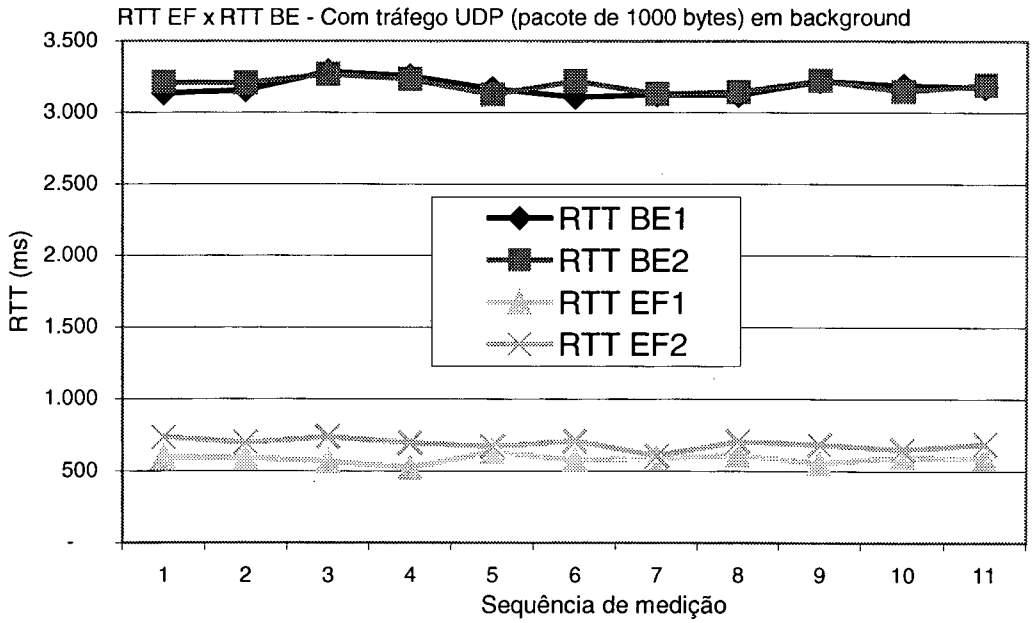


Figura 8-3 – RTT - 1 fluxo ICMP EF e 1 fluxo ICMP BE - tráfego *bg* UDP intenso

Estas três observações demonstram que em determinadas condições de tráfego os mecanismos de reserva de banda e priorização de DiffServ não foram 100% efetivos. Ajustes nesses mecanismos podem ser feitos de modo a melhor proteger o tráfego expresso. Sugerem-se estudos nesse sentido em trabalhos futuros.

De: BE1 – Para: BE2				**De: BE2 – Para: BE1**			
RTT mínimo	RTT médio	RTT máximo	Taxa de perdas (%)	RTT mínimo	RTT médio	RTT máximo	Taxa de perdas (%)
2.960	3.135	3.350	8	2.939	3.212	3.399	16
3.016	3.161	3.448	11	3.044	3.210	3.529	3
3.068	3.287	3.466	46	3.062	3.273	3.457	13
3.048	3.256	3.379	36	3.007	3.235	3.454	2
3.012	3.168	3.435	10	2.941	3.128	3.434	8
2.954	3.108	3.396	8	3.053	3.224	3.472	10
2.971	3.129	3.434	15	2.975	3.134	3.436	15
2.938	3.124	3.434	8	2.987	3.147	3.384	12
3.048	3.224	3.407	32	2.979	3.227	3.486	2
3.018	3.191	3.374	16	2.982	3.152	3.432	14
3.003	***3.178***	***3.412***	***19***	***2.997***	***3.194***	***3.448***	***10***

Tabela 8-4 - RTT e taxa de perdas - 1 fluxo ICMP BE - tráfego *bg* UDP intenso

De: EF1 – Para: EF2				**De: EF2 – Para: EF1**			
RTT mínimo	RTT médio	RTT máximo	Taxa de Perdas (%)	RTT mínimo	RTT médio	RTT máximo	Taxa de Perdas (%)
659	591	730	0	665	734	807	0
748	593	827	0	571	696	823	0
632	564	694	0	664	736	802	0
591	520	654	0	627	697	761	0
705	634	772	0	475	669	750	0
689	572	796	0	591	707	818	0
653	587	723	0	539	604	671	0
679	611	744	0	640	704	771	0
620	552	685	0	611	682	751	0
664	598	737	0	572	645	724	0
664	**582**	**736**	**0**	**595**	**687**	**768**	**0**

Tabela 8-5 – RTT e taxa de perdas - 1 fluxo ICMP EF – tráfego *bg* UDP intenso

8.1.3 Avaliação do atraso

Através da análise das figuras e tabelas abaixo tem-se uma avaliação dos resultados obtidos em relação ao atraso. Na Figura 8-4 observa-se o resultado do experimento de medição do atraso considerando em uma primeira etapa a rede somente com o tráfego

prioritário EF. Nesta situação a linha "Atraso EF1 s/BG", que representa o atraso do fluxo EF1 sem a presença de tráfego *background*, mostra o atraso no sentido de EF1 para EF2 e a linha "Atraso EF2 s/ BG", o atraso no sentido de EF2 para EF1. Pode-se notar que existe uma diferença constante de 8 ms entre a medição feita em um sentido e a medição feita no outro sentido. Essa diferença se apresenta em todos os experimentos. Desta forma, considerou-se ser esta uma característica própria do ambiente. Após a inclusão do tráfego de *background* constante de cerca de 64 Kbps com pacotes de 92 bytes (64 de carga + 28 de cabeçalho) houve um significativo aumento do atraso demonstrando que o tráfego melhor esforço tem influência direta no atraso do tráfego priorizado. Pode-se notar que a diferença de 8 ms manteve-se entre as linhas "Atraso EF1 c/ BG" e a linha "Atraso EF2 c/ BG" que representam o atraso em cada um dos sentidos do tráfego.

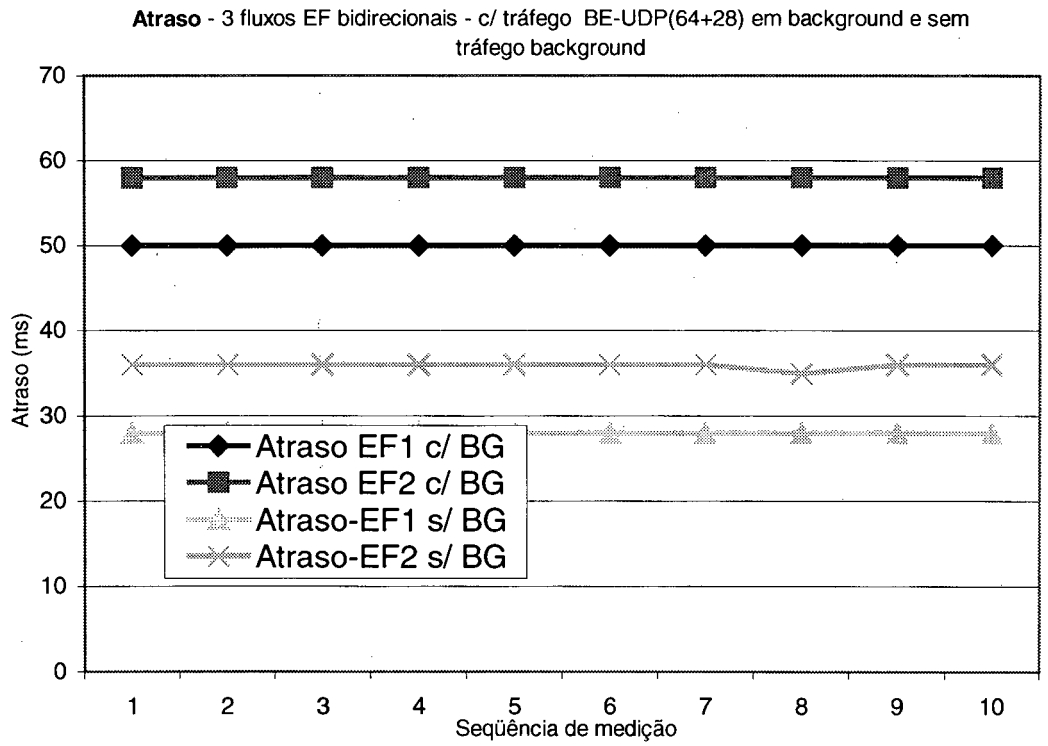


Figura 8-4 – Atraso fim-a-fim (*one-way delay*) com tráfego *bg* e sem tráfego *bg*

Constatada a influência do tráfego melhor esforço sobre o atraso no tráfego prioritário, os experimentos seguintes tiveram como objetivo tentar responder as questões abaixo:

- o tamanho do pacote do fluxo do tráfego em *background* pode influenciar no atraso?

- o tipo de tráfego em *background* TCP ou UDP faz alguma diferença? e
- a quantidade de fluxos priorizados EF é afetada de forma igual ou diferente pelo tráfego de *background*?

A Figura 8-5 mostra um conjunto de medições onde o tráfego prioritário foi de apenas um fluxo. Variou-se o tamanho dos pacotes do tráfego *background* e o tipo de transporte (TCP ou UDP). Nesta figura verifica-se que tanto com tráfego TCP quanto com tráfego UDP em *background*, a variação do tamanho do pacote afeta diretamente o atraso. Verifica-se que o tráfego UDP, em *background,* tem maior influência que o tráfego TCP, e o atraso no tráfego priorizado aumenta de forma quase diretamente proporcional ao aumento do tamanho do pacote. No caso do tráfego TCP observa-se que a influência é constante até pacotes de 256 bytes e a partir daí o atraso aumenta de forma linear, proporcional ao aumento do tamanho do pacote.

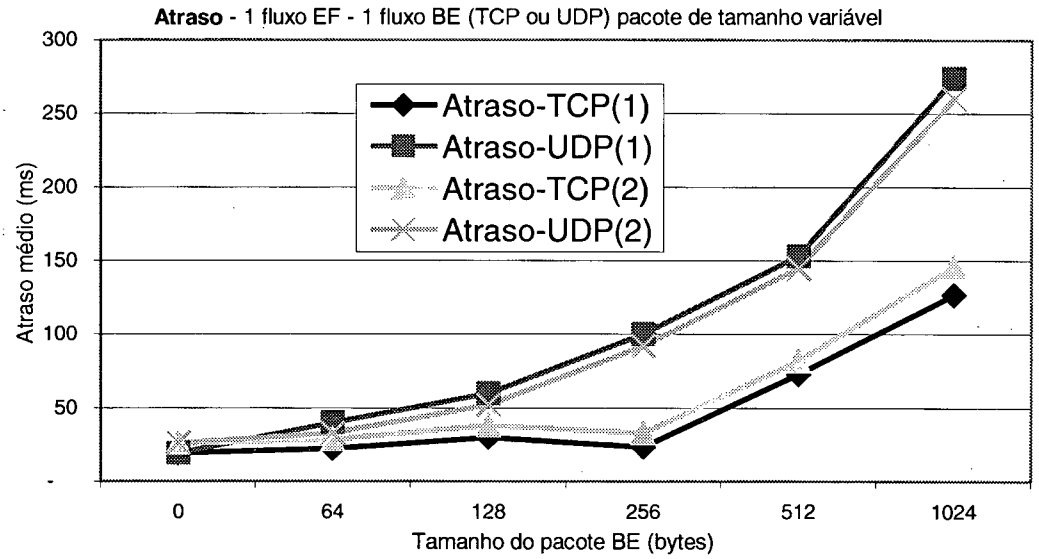


Figura 8-5 – Efeito do tamanho do pacote *bg* no atraso EF em um sentido

Este comportamento descrito anteriormente pode ser explicado da seguinte forma. O tráfego TCP, como tem confirmação e possui seu próprio mecanismo de ajuste de uso de largura de banda, provoca menos congestionamento na rede e, conseqüentemente, influencia menos no atraso do tráfego expresso EF que o tráfego UDP que é sem confirmação e opera neste caso em taxa constante de bits. Já a influência causada pela variação do tamanho dos pacotes pode ser explicada pelo próprio uso do meio de comunicação, ou seja, quanto maior o pacote mais tempo ele leva para atravessar o meio

físico entre as duas estações, mantendo este ocupado. Esta questão merece estudo futuro de modo a avaliar qual seria o comportamento da rede caso os pacotes de um determinado tamanho fossem fragmentados em diversos pacotes de tamanho menor.

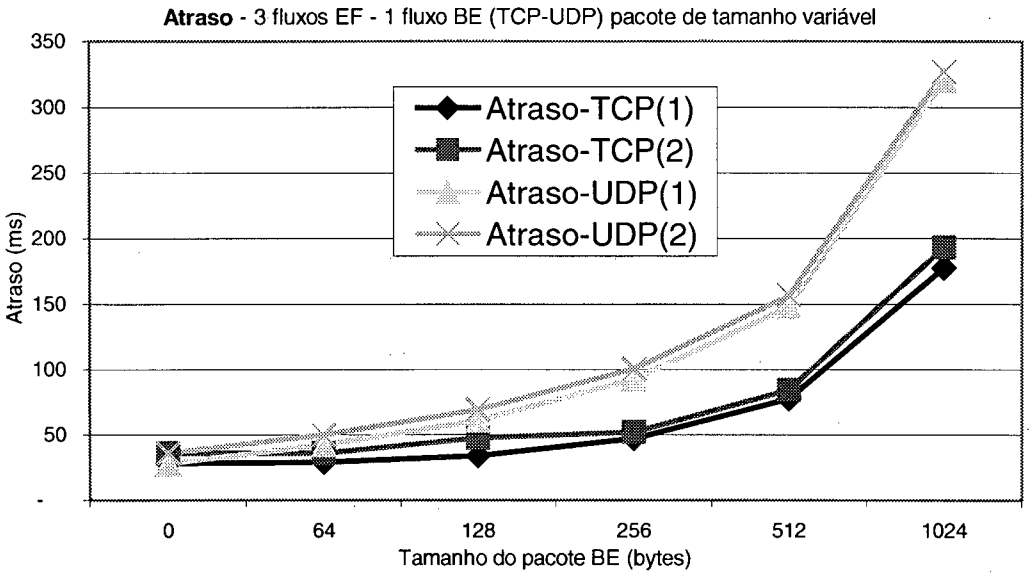


Figura 8-6 - Efeito do tamanho do pacote *bg* no atraso EF (3 fluxos) em um sentido

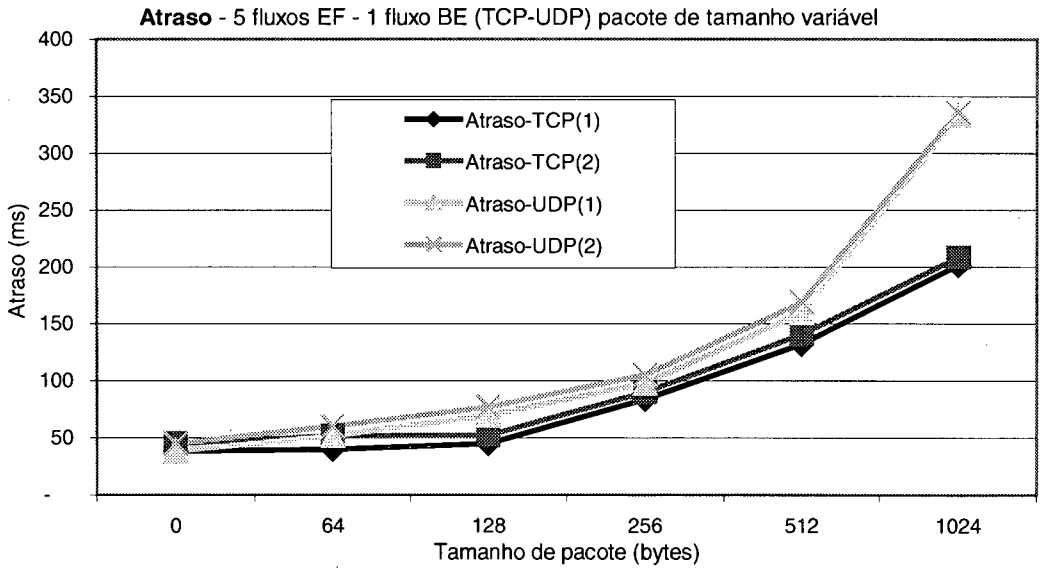


Figura 8-7 - Efeito do tamanho do pacote *bg* no atraso EF (5 fluxos) em um sentido

A Figura 8-6 e Figura 8-7 demonstram experimentos semelhantes, onde modificaram-se apenas a quantidade de fluxos EF prioritários. Pode-se notar que nesta situação o comportamento geral da curva é semelhante ao que foi mostrado na Figura 8-5 para

apenas um fluxo EF, ou seja, o valor do atraso (eixo Y) aumenta na medida em que aumenta-se o tamanho do pacote UDP ou TCP (eixo X). Entretanto, observa-se um pequeno aumento no valor do atraso médio com o aumento do número de fluxos EF.
Parte desse atraso pode ser função do próprio sistema de medição, já que existe um novo processo para cada fluxo que é introduzido na medição, podendo aumentar o uso de CPU e congestionar os *buffers* na interface de recepção.

Continuando a análise, a Figura 8-8, Figura 8-9 e Figura 8-10 nos dão uma visão que permite concluir que os três fatores analisados, tamanho do pacote, tipo de tráfego e número de fluxos EF contribuem para aumento do atraso no tráfego prioritário, e que:

- o fator que mais contribui é o tamanho do pacote do tráfego BE em *background*;
- o tráfego UDP, por ser mais intenso, sem confirmação, contribui mais para o aumento do atraso do que o tráfego TCP; e
- o número de fluxos tem uma contribuição significativa. Uma análise mais adequada desta questão em particular requer a montagem de um ambiente onde o tráfego EF seja gerado e recebido por um número maior de máquinas. Neste trabalho foram analisados somente até cinco fluxos, pois um número além desse não é viável em um único sistema.

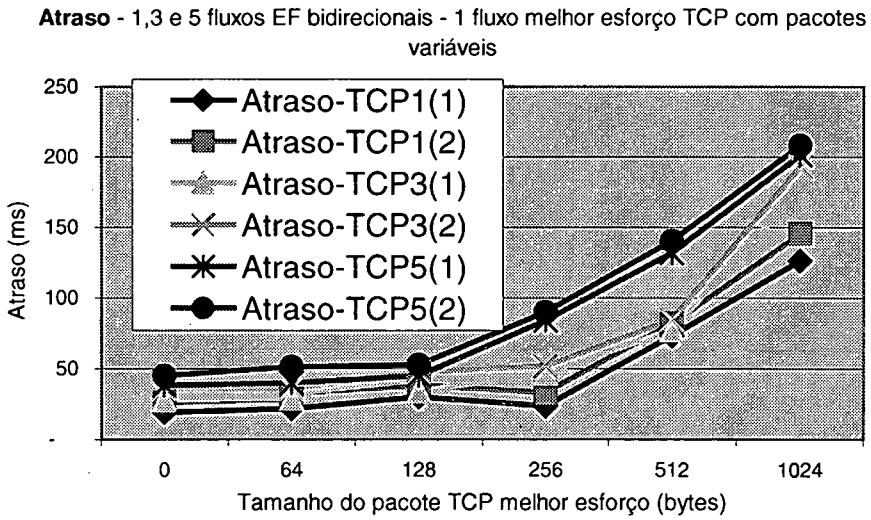


Figura 8-8 - Efeito do tamanho do pacote *bg* TCP no atraso EF – visão com 1, 3 e 5 fluxos EF em um sentido

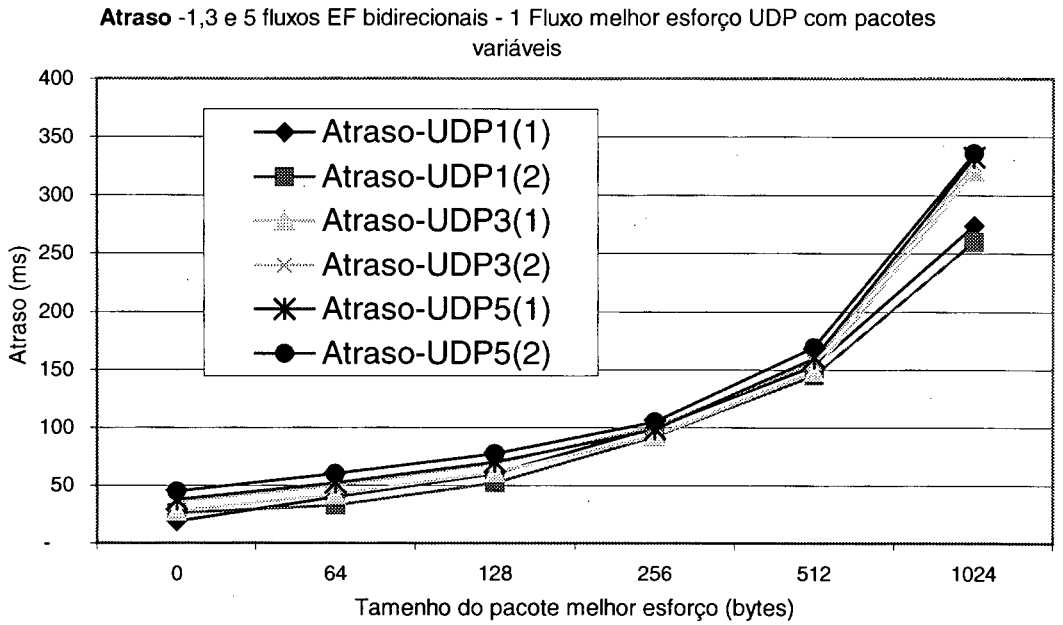


Figura 8-9 - Efeito do tamanho do pacote *bg* UDP no atraso EF – visão com 1, 3 e 5 fluxos EF em um sentido

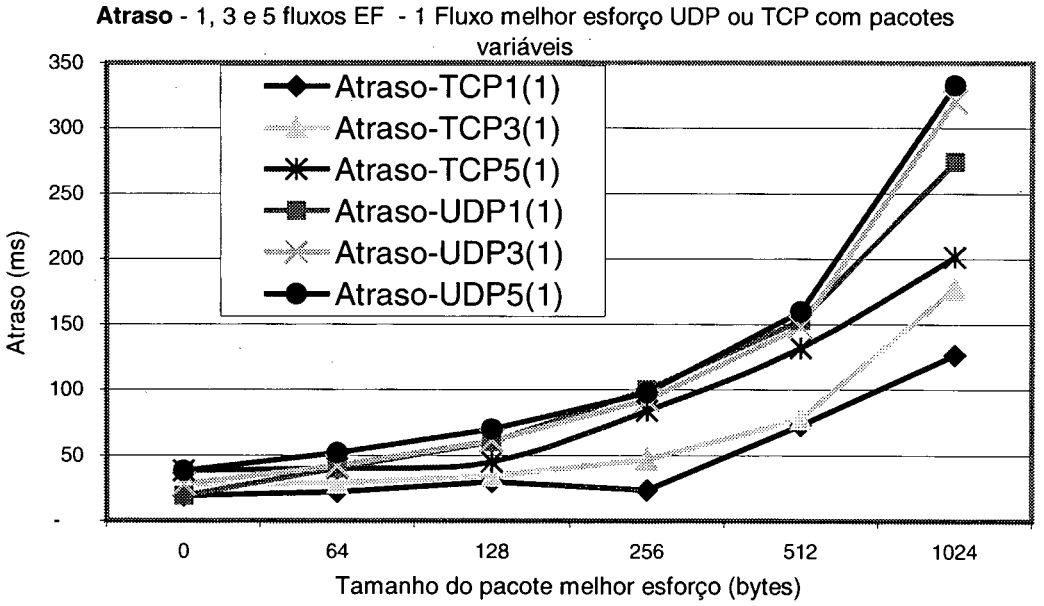


Figura 8-10 - Efeito do tamanho do pacote *bg* (TCP e UDP) no atraso EF – visão com 1, 3 e 5 fluxos EF) em um sentido

Esta conclusão fica mais clara quando é analisada a Figura 8-10 separadamente. Nesta figura são traçadas seis curvas que representam o atraso:

- Atraso-TCP1(1), Atraso-TCP3(1), Atraso-TCP5(1) – Atraso médio de 1, 3 e 5 fluxos EF, com tráfego TCP em *background*; e
- Atraso-UDP1(1), Atraso-UDP3(1), Atraso-UDP5(1) – Atraso médio de 1, 3 e 5 fluxos EF, com tráfego UDP em *background.*

Pode-se notar que o atraso aumenta significativamente na medida em que se aumenta o tamanho do pacote e que o conjunto de curvas que representam o tráfego TCP em *background* pertence ao grupo de menor atraso em relação ao conjunto de curvas que representam o tráfego UDP pelas mesmas razões explicadas anteriormente.

8.1.4 Avaliação da variação do atraso IPDV-jitter

Em uma rede com atraso constante, a variação do atraso tende a zero facilitando, desta forma, as aplicações de tempo real adaptarem seus *buffers* de transmissão e recepção.

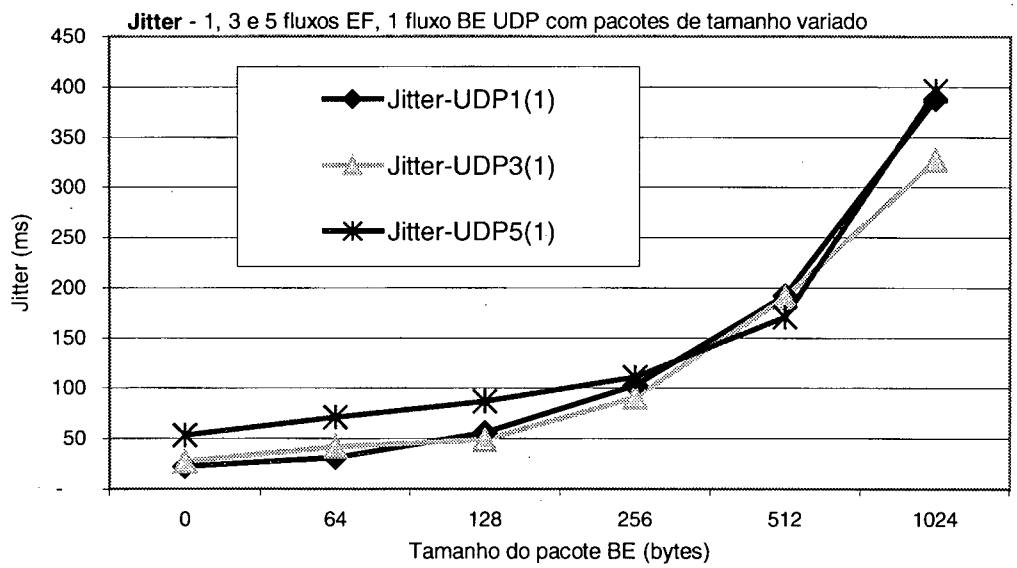


Figura 8-11 - Efeito do tamanho do pacote *bg* UDP no jitter EF – visão com 1, 3 e 5 fluxos EF em um sentido

Pela análise da Figura 8-11, Figura 8-12 e Figura 8-13 pode-se chegar as seguintes conclusões:

- a variação do atraso aumenta na medida em que aumenta o tamanho do pacote do tráfego BE em *background* independentemente do tipo de tráfego UDP ou TCP. Este fato ocorre provavelmente pelas mesmas razões atribuídas ao aumento do atraso na medida em que se aumenta o tamanho do pacote do tráfego *background.*

Ou seja, os pacotes de tamanho maior, do tráfego em *background,* têm um tempo elevado para serem transmitidos e a eles é garantido um determinado tempo de transmissão. Sendo assim, uma vez iniciada uma transmissão de um pacote do tráfego em *background* mesmo que esse tempo exceda ao valor estabelecido, a transmissão não é interrompida e, desta forma, os pacotes do tráfego priorizado tendem a ficar um tempo elevado na fila de ingresso para serem transmitidos ocasionando maior atraso e maior variação no atraso; e

- o aumento do número de fluxos EF tende a aumentar o valor da variação do atraso. Isto provavelmente acontece porque a arquitetura DS trata fluxos agregados na base *first-in-first-out,* fazendo com que alguns pacotes fiquem mais tempo enfileirados do que outros. Assim, dependendo da aplicação existe um limite para o número de fluxos agregados.

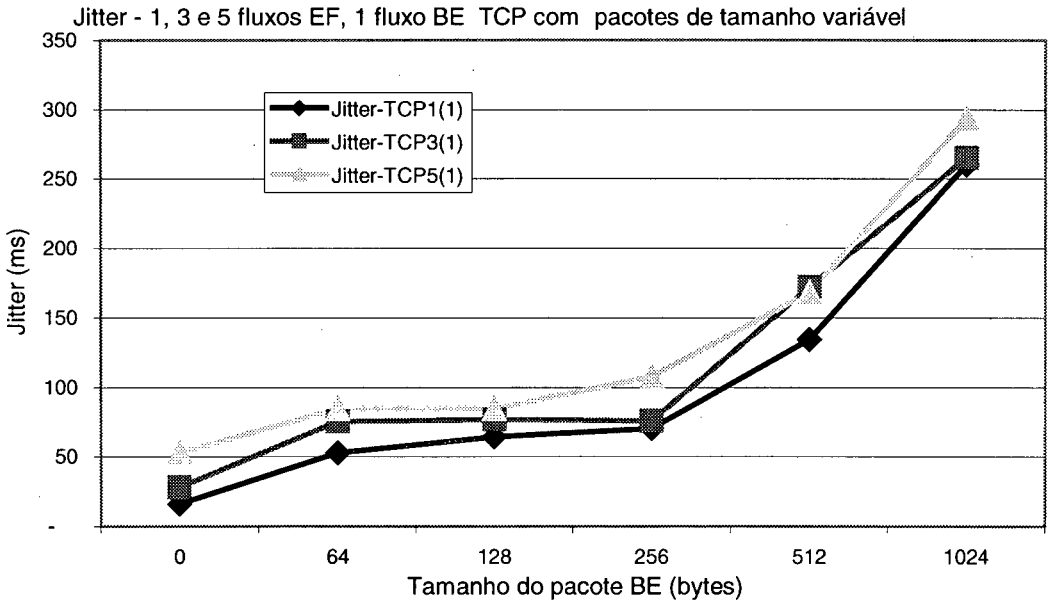


Figura 8-12 - Efeito do tamanho do pacote *bg* TCP no jitter do fluxo EF – visão com 1, 3 e 5 fluxos) em um sentido

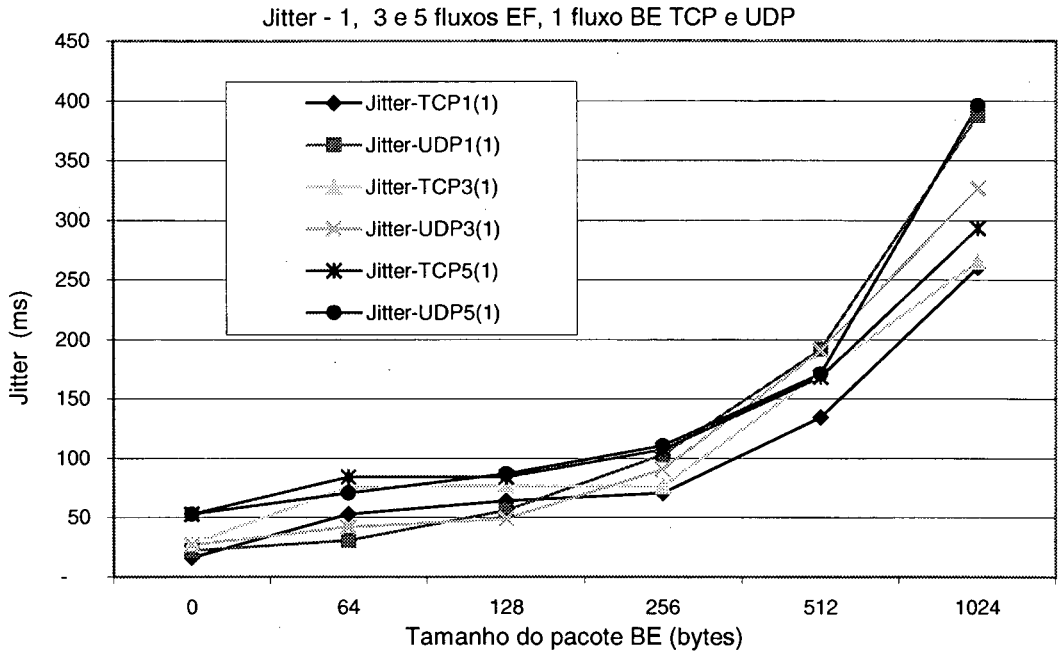


Figura 8-13 - Efeito do tamanho do pacote *bg* (TCP e UDP) no jitter do fluxo EF – visão com 1, 3 e 5 fluxos em um sentido

8.1.5 Avaliação da taxa de perdas

A tolerância a uma pequena quantidade de perdas é uma das características das aplicações de áudio e vídeo. Entretanto, quando o percentual de pacotes perdidos em uma transmissão ultrapassa certos limites, a qualidade é extremamente afetada e muitas vezes pode inviabilizar a comunicação. Neste sentido, a minimização da taxa de perdas é tão importante quanto o controle do atraso e da variação do atraso.

Analisando a Figura 8-14, Figura 8-15 e Figura 8-16, tem-se uma visão sobre a taxa de perdas medida nos experimentos realizados. Observando-se essas figuras pode-se, pelos mesmos motivos que influenciam o atraso e a variação do atraso, concluir que:

- a taxa de perdas aumenta na medida em que aumenta o tamanho do pacote do tráfego em *background*;
- o tráfego UDP em *background* exerce maior influência sobre a taxa de perdas no tráfego EF do que o tráfego TCP; e
- nestes experimentos, chama atenção e sugere investigação futura específica o percentual de perdas ocorrido quando se aumenta o número de fluxo EF de 1 para 3 e 5 fluxos. Nesta situação quando o tamanho do pacote ultrapassa a 512 bytes o

percentual de perdas varia entre 3% a 56% podendo inviabilizar determinadas aplicações.

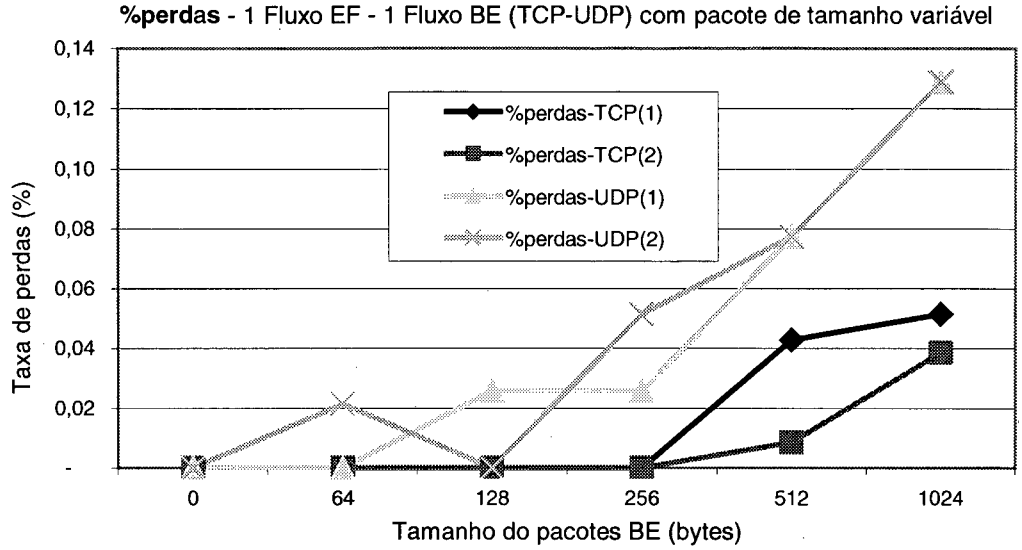


Figura 8-14 - Efeito do tamanho do pacote *bg* (TCP e UDP) na taxa de perda de pacotes EF -1 fluxo EF

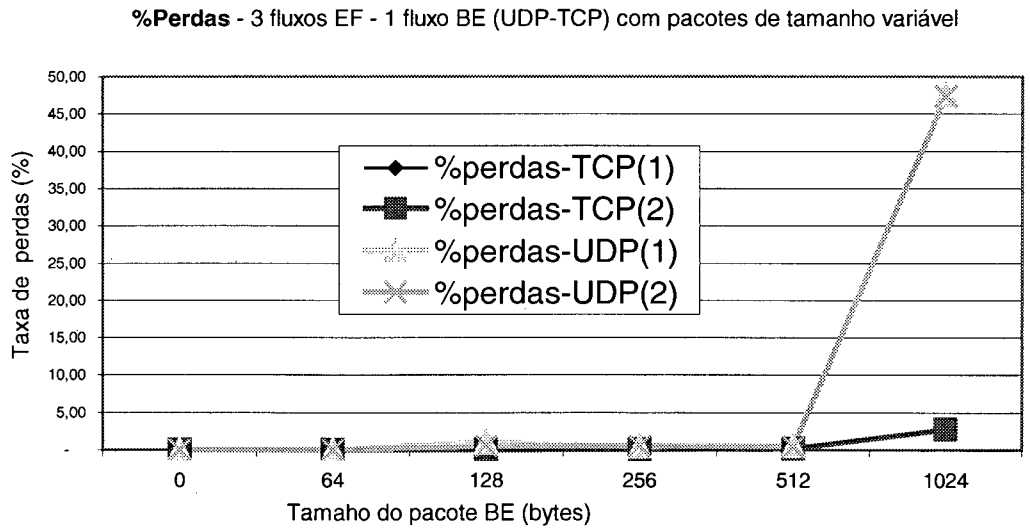
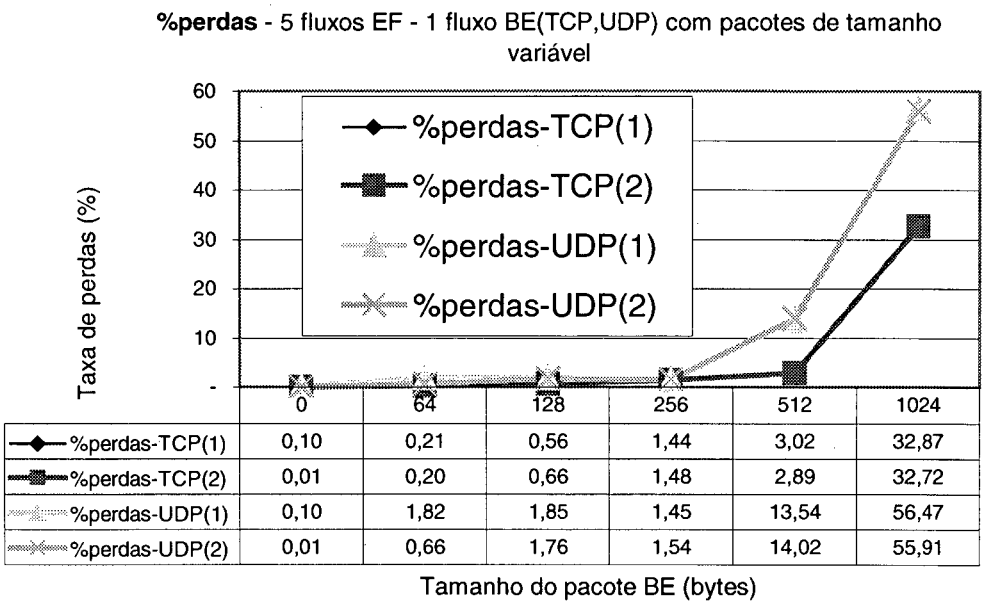


Figura 8-15 - Efeito do tamanho do pacote *bg* (TCP e UDP) na taxa de perda de pacotes EF - 3 fluxos EF



	0	64	128	256	512	1024
%perdas-TCP(1)	0,10	0,21	0,56	1,44	3,02	32,87
%perdas-TCP(2)	0,01	0,20	0,66	1,48	2,89	32,72
%perdas-UDP(1)	0,10	1,82	1,85	1,45	13,54	56,47
%perdas-UDP(2)	0,01	0,66	1,76	1,54	14,02	55,91

Figura 8-16 - Efeito do tamanho do pacote *bg* (TCP e UDP) na taxa de perda de pacotes EF - 5 fluxos EF

8.1.6 Avaliação qualitativa do tráfego de áudio

As vantagens de redução de custos e a economia de largura de banda obtidas através do transporte de voz sobre redes de pacotes estão associadas a uma determinada qualidade de serviço específica para este tipo de rede. A qualidade é determinada por fatores como o atraso, variação do atraso (**Jitter**), perdas de pacotes decorrentes da codificação e transmissão da voz através da rede.

A Figura 8-17 [19] mostra as fases do transporte de voz em redes de pacotes e os atrasos típicos em cada uma das fases em uma rede com canais de comunicação com taxas de transmissão de 64 Kbps.

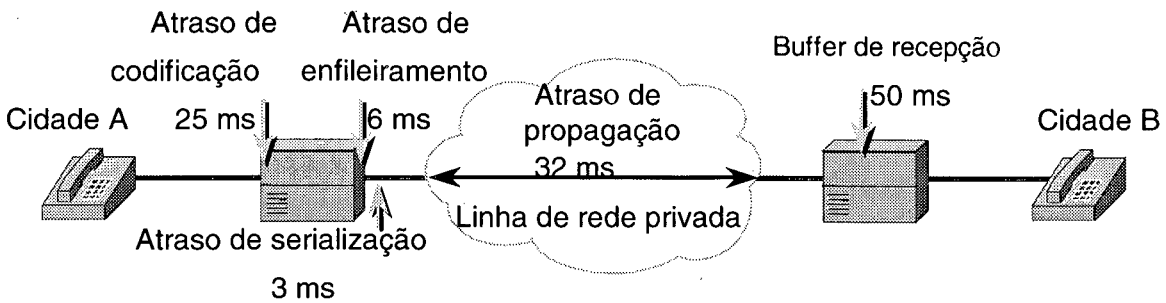


Figura 8-17 – Atrasos típicos ocorridos no transporte de voz sobre redes de pacotes.

8.1.6.1 Avaliação qualitativa do tráfego de áudio utilizando o Netmeeting

Utilizando-se da aplicação Netmeeting [34] foram realizados os seguintes experimentos de transmissão bidirecional de voz (áudio conferência) com objetivo de verificar qualitativamente os resultados das medições realizadas:

1. transmissão de 1 fluxo de voz na rede sem a presença de tráfego *background*;
2. transmissão de voz na rede com a presença de tráfego *background* e DiffServ habilitado; e
3. transmissão de voz na rede com a presença de tráfego *background* e DiffServ não habilitado.

Estado da rede	Atraso Estimado	Qualidade da voz	Comentário
DS não habilitado sem tráfego *background*	1 segundo	5	Voz percebida sem falhas (parâmetro de referência)
DS habilitado sem tráfego em *background*	1 segundo	5	Voz percebida sem falhas
DS habilitado com tráfego UDP, taxa de 64 Kbps e pacotes de 256 bytes em *background*	1 segundo	5	Voz percebida sem falhas
DS habilitado com tráfego UDP, taxa de 64 Kbps e pacotes de 512 bytes em *background*	Entre 1 e 1,5 segundos	4	Voz percebida normalmente
DS habilitado com tráfego UDP, taxa de 64 Kbps e pacotes de 1500 bytes em *background*	Entre 1,5 e 2 segundos	3,5	Voz percebida "entrecortada"
QoS não habilitado com tráfego UDP, taxa de 64 Kbps e pacotes de 1500 bytes em *background*	Superior a 15 segundos	0,5	A voz é recebida em "pedaços" muito tempo depois da transmissão

Tabela 8-6 – Qualidade da voz em diferentes situações de carga e configuração da rede

O Netmeeting não dispõe de ferramentas para coletar estatísticas sobre a transmissão em termos de atraso, taxa de perdas ou outro parâmetro relacionado a QoS, mas a medição da qualidade efetuada obedece à sensibilidade humana. Desta forma, com auxílio de um outro interlocutor, foi possível, com o uso de um cronômetro, estimar o atraso fim-a-fim e estabelecer uma pontuação para a qualidade da voz em função dos tempos do atraso medidos, em um escala que varia de 0 a 5, onde zero indica a pior qualidade e cinco a melhor qualidade. Estes resultados são mostrados na Tabela 8-6. Nesta tabela pode-se

concluir que são efetivos os mecanismos de reserva de banda e priorização de tráfego da arquitetura DS, e associar os resultados obtidos nas medições com os resultados obtidos em uma conversação ou um fluxo EF.

Experimentos utilizando mais de uma conversação simultânea não puderam ser realizados, pois demandariam a utilização de recursos de equipamentos e pessoal não disponíveis. A realização de três, cinco ou mais conversas simultâneas seriam úteis para comprovar, na prática, os resultados das medições. Sugere-se estes experimentos em trabalhos futuros, no item 9.2.

8.1.6.2 Avaliação qualitativa do tráfego de áudio utilizando o Real Server

A utilização do *Netmeeting* proporcionou a realização de um experimento de voz sobre IP bidirecional, porém esta ferramenta não dispõe de estatísticas próprias que permitam analisar o desempenho da rede quanto ao atendimento das necessidades de uma aplicação deste tipo. Utilizando-se do *Real Server* e *Real Player* foi possível obter-se informações sobre o desempenho da aplicação em diferentes condições de tráfego na rede. Neste sentido foram realizados experimentos de:

- transmissão de um fluxo de voz na rede sem a presença de tráfego *background*;
- transmissão de voz na rede com a presença de tráfego *background* e DiffServ habilitado; e
- transmissão de voz na rede com a presença de tráfego *background* e DiffServ não habilitado.

Observando-se a Tabela 8-7 e as figuras numeradas da Figura 8-18 até a Figura 8-21, tem-se a seguinte avaliação:

- Quando DS está habilitado:
    - a voz é considerada ótima ou boa com exceção da situação onde tamanho do pacote do tráfego *background* é de 1500 bytes. Neste caso o fato de a qualidade da voz não ser boa ou ótima provavelmente ocorre em função do atraso de enfileiramento; e
    - a aplicação sempre consegue a largura de banda desejada de 16 Kbps.
- Quando DS não está habilitado:

- a voz só é considerada ótima ou boa quando não há tráfego em *background* ou quando este é de baixa intensidade; e
- a aplicação somente consegue a largura de banda desejada quando não há tráfego em *background* ou este é de baixa intensidade.

Os resultados qualitativos percebidos neste experimento refletem com menos intensidade o que foi observado nas medições. Como o tráfego é unidirecional e a aplicação se adapta às condições da rede, somente em condições extremas de congestionamento esta não funcionou adequadamente.

DS Habilitado	**Tráfego *bg***	**Qualidade da voz**	**Taxa de perdas**	**Taxa de retrans-missão**	**Banda mínima requerida**	**banda média alocada**
Sim	Não	ótima	1,93	3,16	16 Kbps	16.4 Kbps
Sim	UDP-512	ótima	-	-	16 Kbps	16.6 Kbps
Sim	UDP-1024	ótima	2,06	4,56	16 Kbps	16.9 kbps
Sim	UDP-1500	truncada/ tremida	2,45	3,67	16 Kbps	16 Kbps
Não	Não	ótima	0	0,91	16 Kbps	16.4 Kbps
Não	UDP-64	boa	0	2,59	16 Kbps	16.3 Kbps
Não	UDP-1500	sem voz	38%	7,57	16 Kbps	4.1 Kbps
Não	UDP-512	truncada	-	-	16 Kbps	4.9 Kbps

Tabela 8-7 – Estatísticas de transmissão de áudio – real server

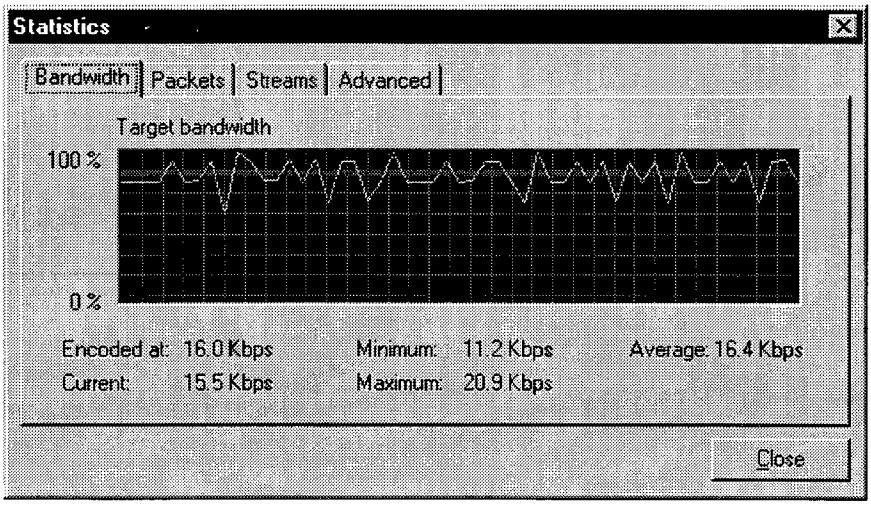


Figura 8-18 – Largura de banda utilizada - DS habilitado e sem tráfego *bg* - qualidade da voz - ótima

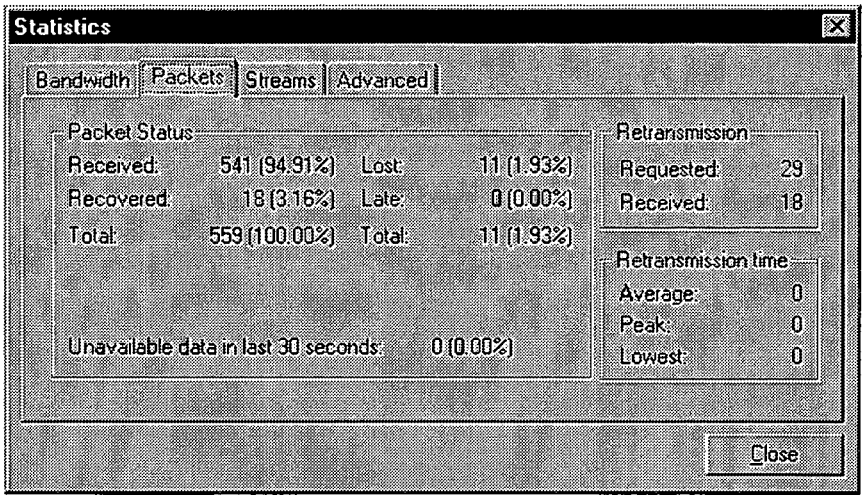


Figura 8-19 – Taxa de perda de pacotes - DS habilitado e sem tráfego bg – qualidade da voz - ótima

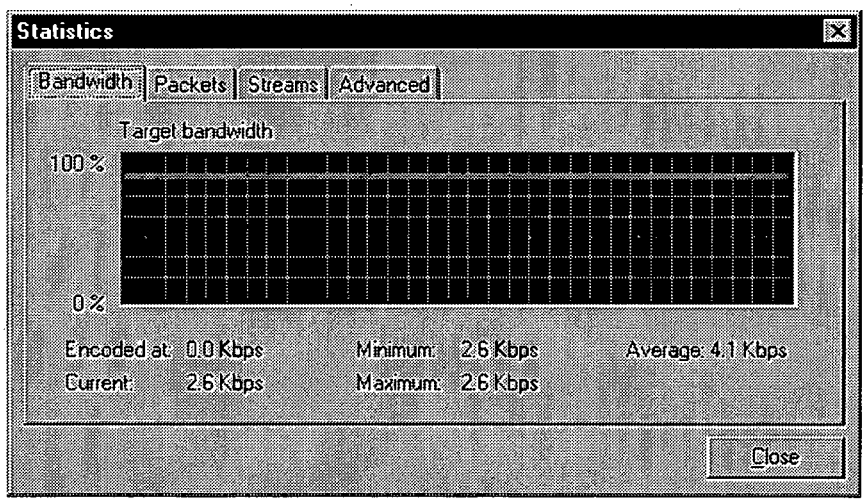


Figura 8-20 – Largura de banda utilizada – DS não habilitado e com tráfego *bg* UDP 1500 bytes – qualidade da voz - sem recepção de áudio

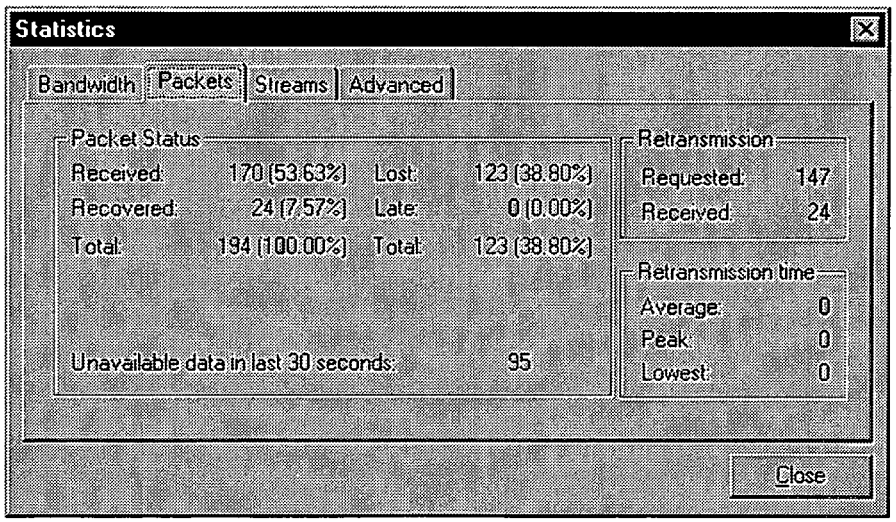


Figura 8-21 - Taxa de perda de pacotes - DS não habilitado –tráfego *bg* UDP 1500 bytes – qualidade da voz - sem recepção de áudio

8.2 Ambiente CISCO

A principal característica que diferencia este ambiente do ambiente IBM avaliado anteriormente é a velocidade dos canais de comunicação. No primeiro a taxa de transmissão do canal PPP estava limitada a 64 Kbps enquanto que neste ambiente a velocidade do PVC ATM (Circuito Virtual Permanente) foi limitada em 2 Mbps. Neste ambiente, por restrições de equipamentos com capacidade DiffServ as medições foram realizadas somente em um sentido, embora o tráfego *background* fosse bidirecional.

8.2.1 Determinação do perfil da rede

8.2.1.1 RTT

Na Figura 8-22 é mostrado o comportamento da métrica RTT e na Tabela 8-1 é mostrado o RTT mínimo, médio e máximo, e a taxa de perdas ocorrida em cada uma das medições. Na última linha é mostrada a média destes indicadores. Pode-se notar que em todas as seqüências de medições efetuadas não foi verificada perda de pacotes.

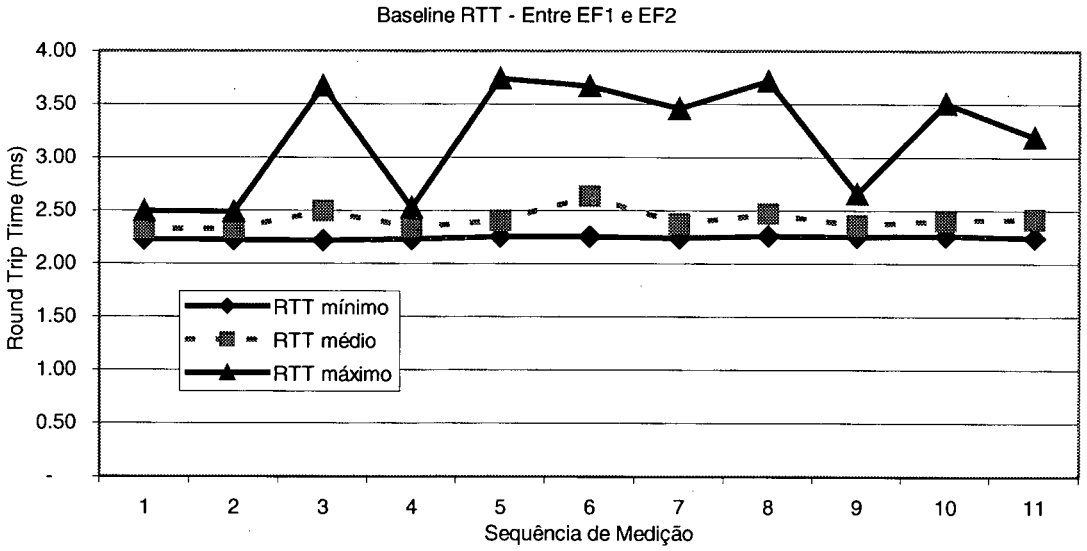


Figura 8-22 - RTT entre os sistemas EF1 e EF2 com pacotes de 84 bytes

De: EF1 – Para: EF2				De: EF1 – Para; EF2			
RTT mínimo	RTT médio	RTT máximo	Taxa de perdas	RTT mínimo	RTT médio	RTT máximo	Taxa de perdas
2,23	2,32	2,49	0	2,29	2,38	2,89	0
2,22	2,33	2,49	0	2,29	2,59	3,67	0
2,22	2,50	3,67	0	2,28	2,44	3,52	0
2,23	2,34	2,52	0	2,27	2,38	2,60	0
2,26	2,40	3,74	0	2,26	2,78	3,20	0
2,25	2,63	3,67	0	2,21	2,39	3,15	0
2,24	2,37	3,46	0	2,26	2,38	2,72	0
2,26	2,47	3,71	0	2,27	2,39	3,83	0
2,25	2,36	2,66	0	2,26	2,37	2,56	0
2,26	2,41	3,51	0	2,22	2,38	3,72	0
2,24	**2,41**	**3,19**	**0**	**2,26**	**2,45**	**3,19**	**0**

Tabela 8-8 - RTT e taxa de perdas (%) de pacotes entre ef1 e ef2 e entre ef2 e ef1

8.2.1.2 Vazão TCP

A vazão máxima, medida através do Netperf foi de aproximadamente 1706,94 Kbps como mostra a Tabela 8-9. A vazão máxima teórica para esse canal ATM, após a retirada da sobrecarga do cabeçalho da célula ATM, estimada através das expressões definidas na seção 6.2.8.1, é de 1.843 Mbps.

Tamanho do Pacote TCP	1500 bytes
Vazão de BE1 para BE 2	1706,94 Kbps
Vazão de BE2 para BE1	1704,21 Kbps

Tabela 8-9 – Vazão máxima medida através do Netperf em ambos os sentidos

Carga	Cabeçalho	Pacote+ Cabeçalho	T-BE1/ segundo	T-BE2/ segundo	T-total/ segundo	Pacotes/ segundo	Vazão Total
12	52	64	243,20	251,51	494,71	989,41	506,58
76	52	128	211,80	199,95	411,75	823,49	843,25
204	52	256	169,80	171,12	340,92	681,83	1.396,39
460	52	512	107,44	107,03	214,47	428,94	1.756,94
972	52	1024	57,54	57,57	115,10	230,20	1.885,80
1448	52	1500	40,10	40,11	80,20	160,41	1.924,88

Tabela 8-10 – Vazão TCP melhor esforço variando o tamanho do pacote

Na Tabela 8-10 e Figura 8-23 é mostrado o aumento da vazão total na medida em que se aumenta o tamanho do pacote, com conseqüente redução do número de transações

TCP por segundo. Neste caso a vazão foi calculada a partir da medição do número de transações TCP (Requet/Response) utilizando o *Netperf*.

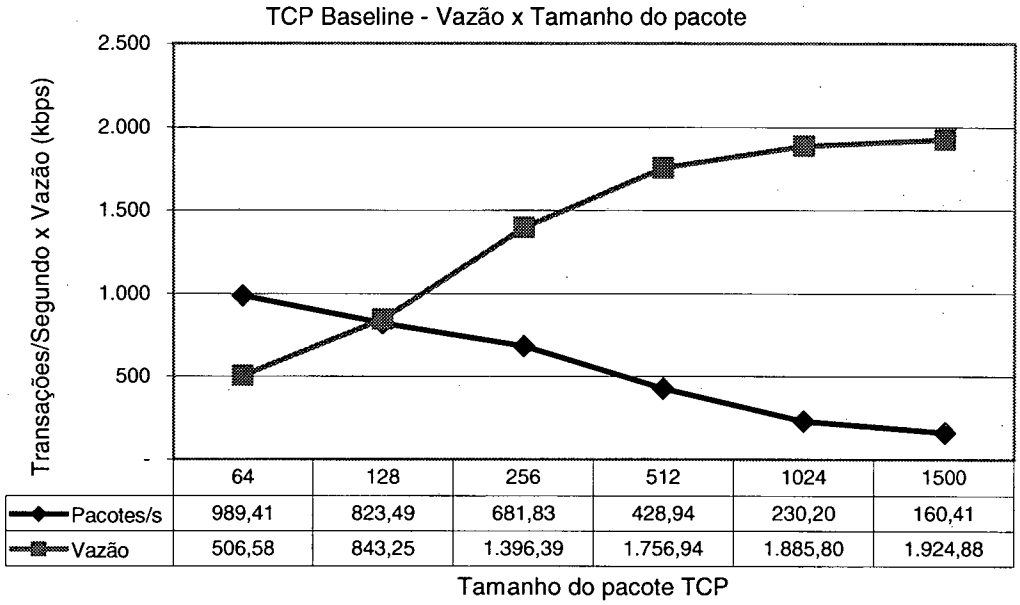


Figura 8-23 – Vazão no canal vs. tamanho do pacote

8.2.1.3 Vazão UDP

De acordo com o método de cálculo da vazão UDP apresentado na seção 6.2.8.1 a taxa de recepção de pacotes por segundo e vazão (Kbps) estimada, em cada um das direções do tráfego, é mostrada na Tabela 8-11.

Métrica \ host	Host BE1	Host BE2
Pacotes/segundo	145,53	145,25
Vazão / Kbps	1713,83	1710,40

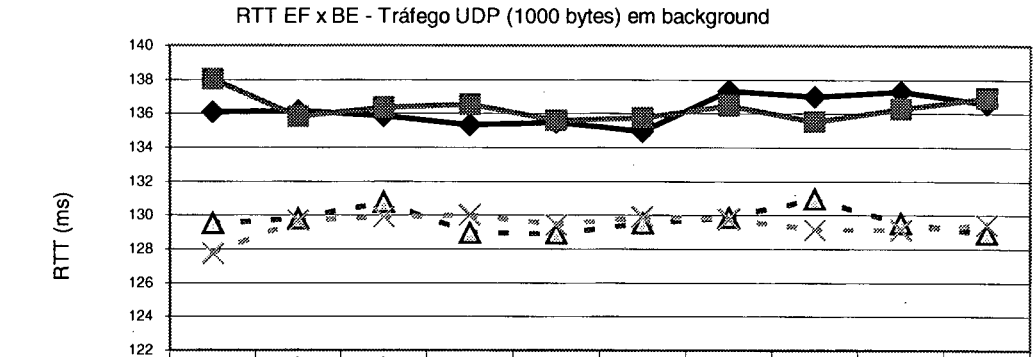
Tabela 8-11– Número de pacotes recebidos por segundo e vazão

O perfil da rede, determinado através da avaliação do RTT entre as duas redes locais, da medição da vazão (TCP e UDP) demonstra que a mesma tem um comportamento e desempenho adequado à tecnologia e velocidade dos canais de comunicação.

8.2.2 Avaliação do RTT com e sem DS

Tal como no ambiente IBM, antes de passar efetivamente a medir os parâmetros de QoS selecionados, foi verificado o comportamento do tráfego *ICMP Echo Request* e *ICMP*

Echo Reply classificado como tráfego EF e também como melhor esforço na presença de um tráfego UDP em *background* intenso.



	1	2	3	4	5	6	7	8	9	10
RTT-EF(1)	136,08	136,18	135,88	135,31	135,50	134,97	137,33	136,99	137,30	136,57
RTT-EF(2)	138,03	135,82	136,36	136,53	135,60	135,73	136,47	135,53	136,27	136,94
RTT-BE(1)	129,52	129,77	130,77	128,96	128,92	129,52	129,87	130,98	129,51	128,92
RTT-BE(2)	127,72	129,66	129,90	130,01	129,45	129,90	129,80	129,15	129,13	129,45

Figura 8-24 – RTT (Round Trip Time) de um fluxo ICMP EF e ICMP melhor esforço na presença de tráfego UDP em *background* intensivo

De: BE1 – Para: BE2				**De: BE2 – Para: BE1**			
RTT mínimo	RTT médio	RTT máximo	Taxa de perdas	RTT mínimo	RTT médio	RTT máximo	Taxa de perdas
124,37	129,52	135,26	8,00	121,88	127,72	133,89	26,00
124,57	129,77	135,19	21,00	125,05	129,66	134,87	28,00
124,46	130,77	134,95	57,00	124,04	129,90	141,14	42,00
124,00	128,96	134,48	47,00	124,36	130,01	135,15	34,00
123,66	128,92	133,86	21,00	124,47	129,45	134,52	30,00
124,34	129,52	134,95	8,00	123,95	129,90	135,14	42,00
124,80	129,87	135,29	36,00	125,05	129,80	134,47	32,00
127,04	130,98	134,85	57,00	124,42	129,15	133,90	28,00
123,92	129,51	134,80	57,00	124,17	129,13	134,75	44,00
123,66	128,92	133,86	21,00	124,47	129,45	134,52	30,00
124,48	**129,67**	**134,75**	**33,30**	**124,19**	**129,42**	**135,24**	**33,60**

Tabela 8-12 - RTT e taxa de perdas (%) de pacotes - 1 fluxo ICMP melhor esforço - tráfego UDP bg

Na Figura 8-24, Tabela 8-12 e Tabela 8-13, observa-se que:

- o tempo de ida e volta dos pacotes ICMP (RTT) melhor esforço na presença de tráfego BE em *background* UDP intenso apresenta atraso na ordem de 5% inferior ao atraso no tráfego EF nas mesmas condições. Estes resultados podem ser

explicados pelas altas taxas de perda ocorrida no tráfego melhor esforço, fazendo com que uma quantidade significativa de pacotes não entre no cálculo do atraso médio efetuado pela aplicação *ping* utilizada para esta medição;

O tráfego ICMP EF, embora tenha prioridade sobre o tráfego melhor esforço, apresenta significativo aumento no atraso quando comparado ao atraso obtido com a rede sem carga conforme mostrado na Tabela 8-8.

- Isto se deve, provavelmente, em função do maior tempo de enfileiramento dos pacotes EF aguardando a transmissão dos pacotes UDP em *background* que ocorrem em maior volume; e
- embora o tráfego ICMP EF tenha sofrido atraso, sua taxa de perdas foi nula. Já no tráfego ICMP melhor esforço a taxa de perdas em ambos os sentidos foi de 33%, em média.

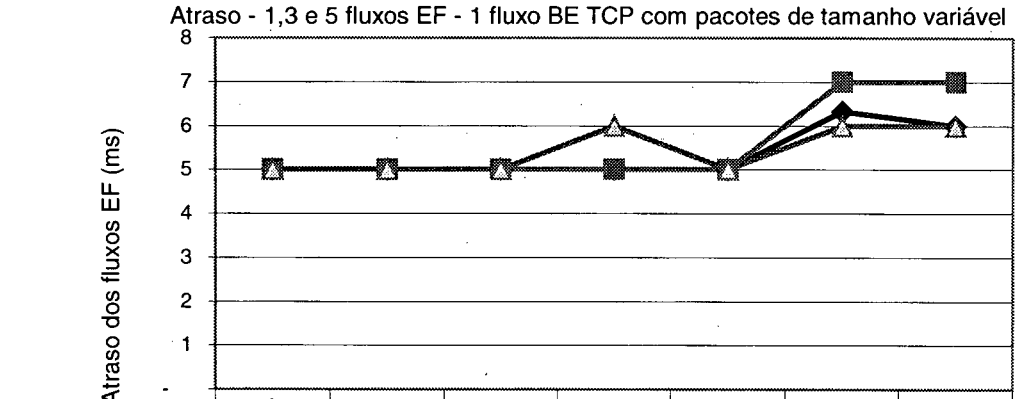
De: EF1 – Para: EF2				**De: EF2 – Para: EF1**			
RTT mínimo	RTT médio	RTT máximo	Taxa de perdas	RTT mínimo	RTT médio	RTT máximo	Taxa de perdas
124,33	136,08	148,22	0	124,96	138,03	148,32	0
125,69	136,18	148,05	0	124,66	135,82	149,99	0
124,54	135,88	145,47	0	125,50	136,36	146,50	0
125,48	135,31	144,78	0	124,05	136,53	147,92	0
125,75	135,50	145,09	0	124,78	135,60	144,65	0
124,85	134,97	145,35	0	125,82	135,73	147,65	0
125,92	137,33	148,67	0	126,46	136,47	148,12	0
124,50	136,99	148,70	0	124,44	135,53	145,42	0
124,53	137,30	148,88	0	125,42	136,27	147,69	0
127,00	136,57	146,17	0	126,66	136,94	149,08	0
125,26	136,21	146,94	0	125,28	136,33	147,53	0

Tabela 8-13 – RTT taxa de perdas (%) de pacotes - 1 fluxo EF ICMP - tráfego UDP intenso em bg

8.2.3 Avaliação do atraso

Na Figura 8-25 e Figura 8-26 tem-se respectivamente o atraso dos fluxos EF (1, 3 e 5) quando se varia o tamanho do pacote do tráfego TCP em *background* e o atraso dos fluxos EF (1, 3 e 5) quando se varia o tamanho do pacote do tráfego UDP em *background.* Na Figura 8-27 tem-se uma visão geral do atraso dos fluxos EF com tráfego *background* TCP e UDP. Da análise dos atrasos representados nestas figuras pode-se concluir que:

- nenhum dos fatores, tamanho do pacote e tipo de tráfego TCP ou UDP do tráfego *background* ou número de fluxos EF afetou o atraso dos fluxos EF a ponto de comprometer significativamente a qualidade de aplicações que envolvam transmissão de áudio e vídeo. Como se pode notar, o valor do atraso medido aumentou de 4 ms na rede sem tráfego em *background* para 18 ms com tráfego UDP e pacotes de 1500 bytes. Embora essa variação seja significativa esse valor é considerado baixo para grande parte das aplicações referidas;
- o tráfego *background* UDP apresentou efeito significativamente maior sobre o atraso do fluxo EF do que o tráfego TCP. Isto acontece, pois o tráfego TCP possui confirmação e controle de fluxo próprio. Esta característica faz com que sua intensidade diminua em caso de sobrecarga na rede e, em conseqüência, a carga total da rede também diminui; e
- o número de fluxos EF é o fator, dentre os analisados, que menos influenciou o atraso dos fluxos EF.



	0	64	128	256	512	1024	1500
Atraso-TCP(1)	5	5	5	5	5	6	6
Atraso-TCP(3)	5	5	5	5	5	7	7
Atraso-TCP(5)	5	5	5	6	5	6	6

Tamanho do pacote BE (bytes)

Figura 8-25 – Efeito do tamanho do pacote BE (TCP) no atraso dos fluxos EF

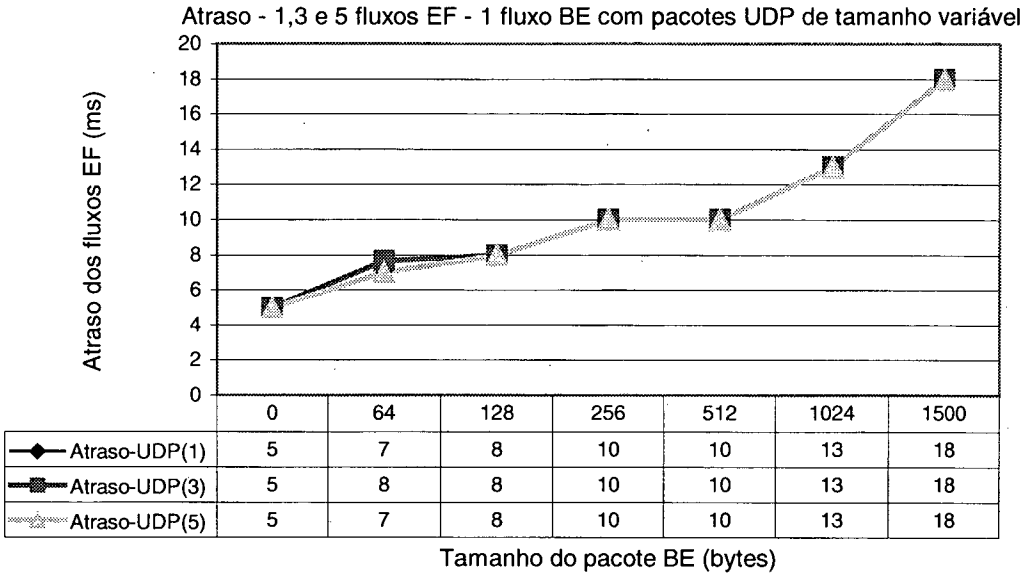


Figura 8-26 – Efeito do tamanho do pacote BE (UDP) no atraso dos fluxos EF

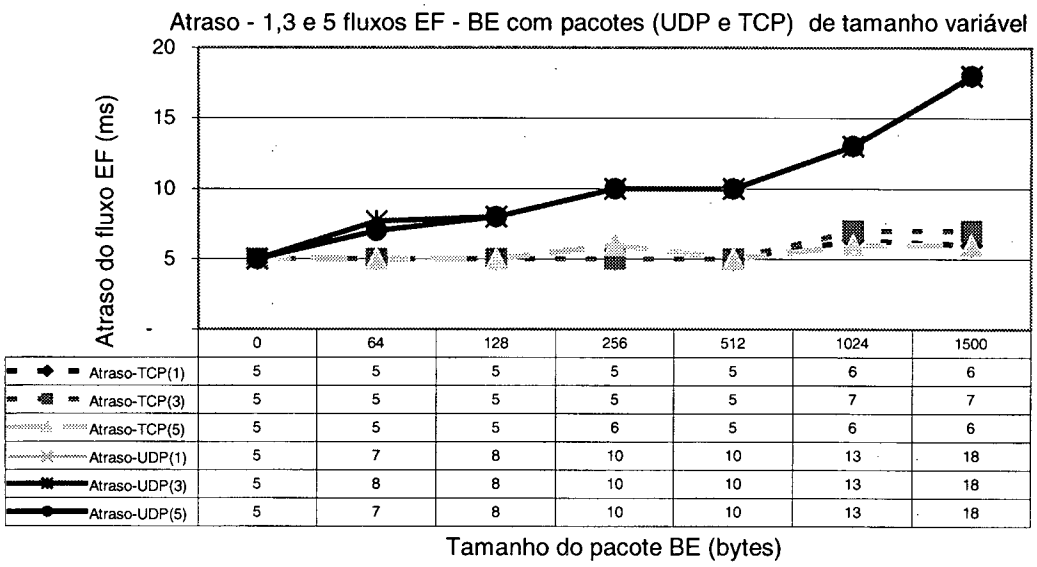
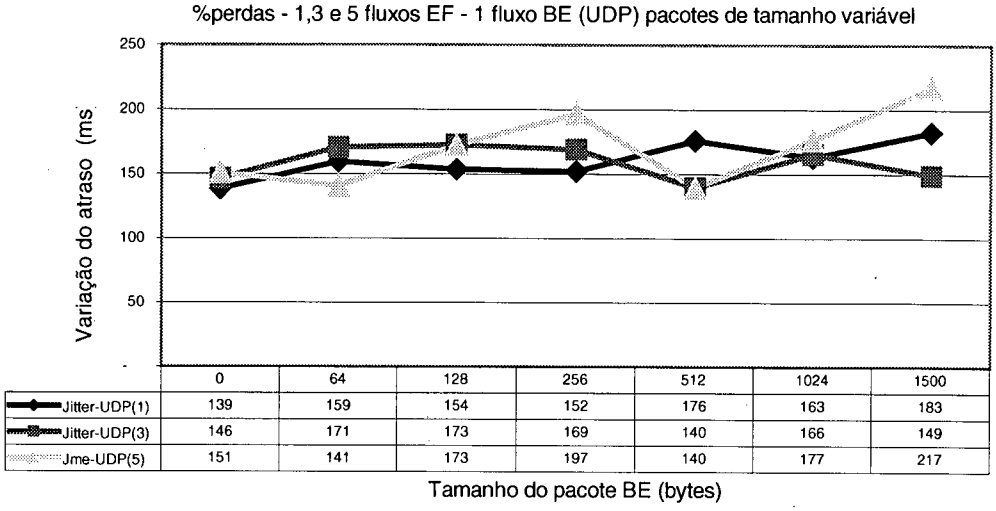


Figura 8-27 - Efeito do tamanho do pacote BE (UDP e TCP) no atraso dos fluxos EF

8.2.4 Avaliação da variação do atraso

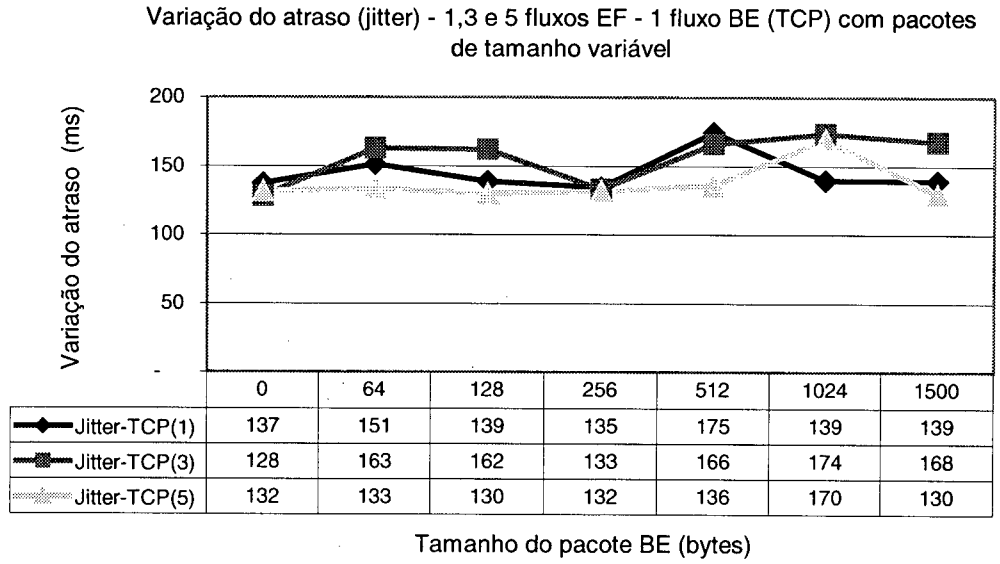
A partir do valor médio do atraso e da variação do atraso é possível inferir os valores de atraso mínimo e máximo. Na Figura 8-28 e Figura 8-29 observa-se que os valores da variação do atraso, sendo o tráfego *background* UDP ou TCP, são semelhantes, porém são bem superiores aos valores do atraso médio. Este comportamento pode indicar a necessidade de ajustes na configuração da rede de modo a garantir às aplicações um valor de *jitter* inferior aos apresentados. Estes valores, entretanto, são relativamente

constantes, facilitando às aplicações regularem o tamanho de seus *buffers* de transmissão e recepção.



	0	64	128	256	512	1024	1500
Jitter-UDP(1)	139	159	154	152	176	163	183
Jitter-UDP(3)	146	171	173	169	140	166	149
Jme-UDP(5)	151	141	173	197	140	177	217

Figura 8-28 - Efeito do tamanho do pacote BE (UDP) na variação do atraso dos fluxos EF



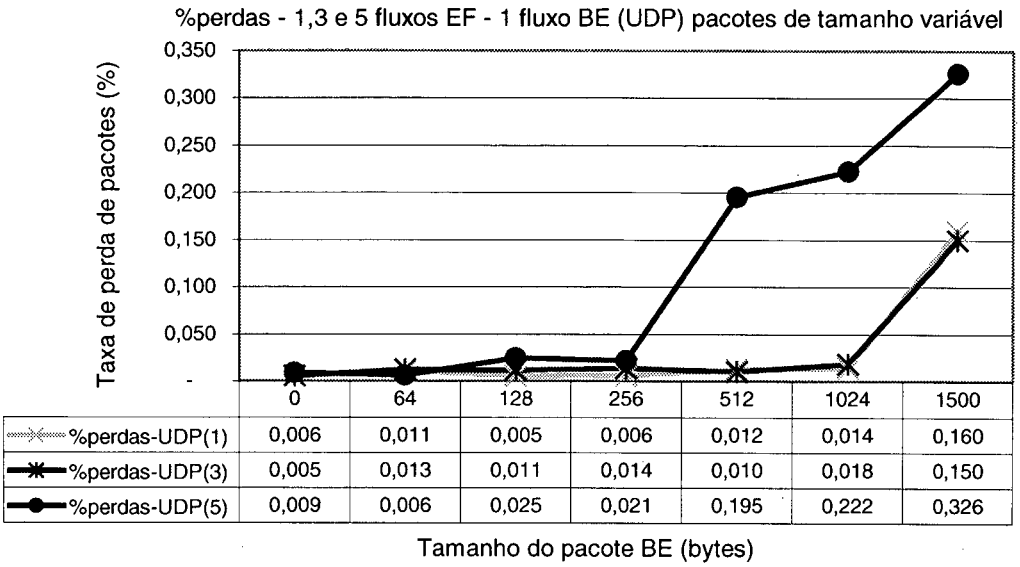
	0	64	128	256	512	1024	1500
Jitter-TCP(1)	137	151	139	135	175	139	139
Jitter-TCP(3)	128	163	162	133	166	174	168
Jitter-TCP(5)	132	133	130	132	136	170	130

Figura 8-29 - Efeito do tamanho do pacote BE (TCP) na variação do atraso dos fluxos EF

8.2.5 Avaliação da taxa de perdas

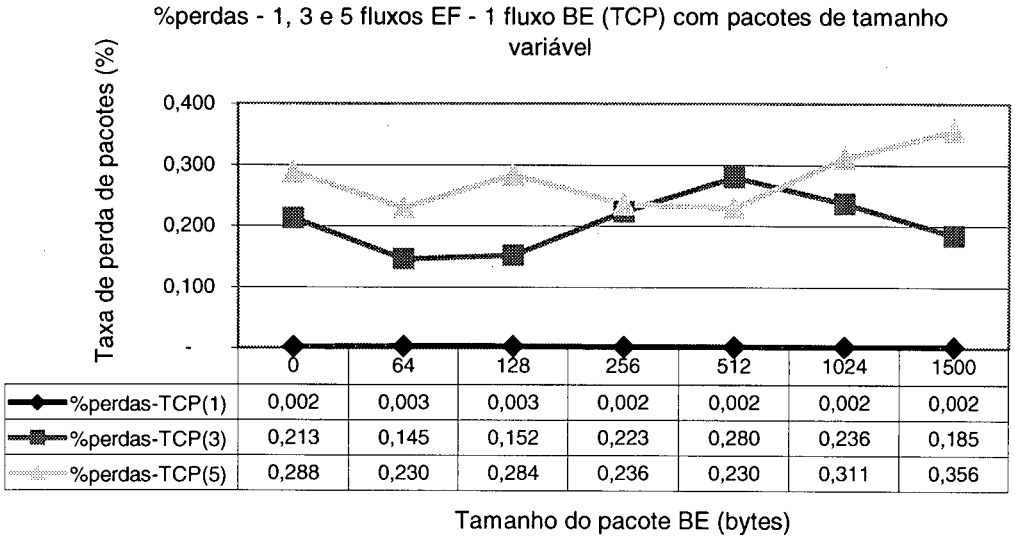
Algumas aplicações, como as de áudio e vídeo, possuem tolerância a um pequeno percentual de perda de pacotes. Entretanto, quando este percentual em uma transmissão ultrapassa certos limites a qualidade é extremamente afetada e muitas vezes pode

inviabilizar a comunicação. Neste sentido a minimização das perdas é tão importante quanto o controle do atraso e da variação do atraso.



	0	64	128	256	512	1024	1500
%perdas-UDP(1)	0,006	0,011	0,005	0,006	0,012	0,014	0,160
%perdas-UDP(3)	0,005	0,013	0,011	0,014	0,010	0,018	0,150
%perdas-UDP(5)	0,009	0,006	0,025	0,021	0,195	0,222	0,326

Figura 8-30 - Efeito do tamanho do pacote BE (UDP) na taxa de perda de pacotes dos fluxos EF



	0	64	128	256	512	1024	1500
%perdas-TCP(1)	0,002	0,003	0,003	0,002	0,002	0,002	0,002
%perdas-TCP(3)	0,213	0,145	0,152	0,223	0,280	0,236	0,185
%perdas-TCP(5)	0,288	0,230	0,284	0,236	0,230	0,311	0,356

Figura 8-31 - Efeito do tamanho do pacote BE (TCP) na taxa de perda de pacotes dos fluxos EF

Na Figura 8-30 e Figura 8-31 tem-se uma visão sobre as perdas medidas nos experimentos realizados de onde pode-se concluir que:

- a taxa de perda de pacotes nos fluxos EF se manteve extremamente baixa quando o tráfego em *background* era do tipo UDP com pacotes de tamanho de até 256 bytes; e

- a taxa de perda de pacotes, embora tenha apresentado uma variação relativamente grande quando se mudam os parâmetros do tráfego de *background* e o número de fluxos EF, estão dentro de limites aceitáveis (inferior a 0,5%), proporcionando desta forma qualidade suficiente para grande parte das aplicações envolvendo transmissão de áudio e vídeo.

8.2.6 Avaliação qualitativa de tráfego de áudio e vídeo

A avaliação qualitativa do ambiente DS CISCO, foi realizada através da transmissão de um fluxo de vídeo e áudio entre duas estações. Para esta transmissão foi utilizado um servidor Real Server e foi transmitido um vídeo codificado no formato RM a uma taxa de bits de 225 Kbps. Para esse fluxo foi feita uma reserva no roteador de ingresso de 344 kpps. Definiu-se que o tráfego com origem na rede 192.168.11.0/24 e destino para a rede 192.168.14.0/24 seria marcado com o DSCP 46 e que o tráfego excedente seria descartado. Desta forma, na interface de saída, o tráfego com DSCP igual a 46 é tratado na fila de prioridade expressa e o restante do tráfego na fila melhor esforço.

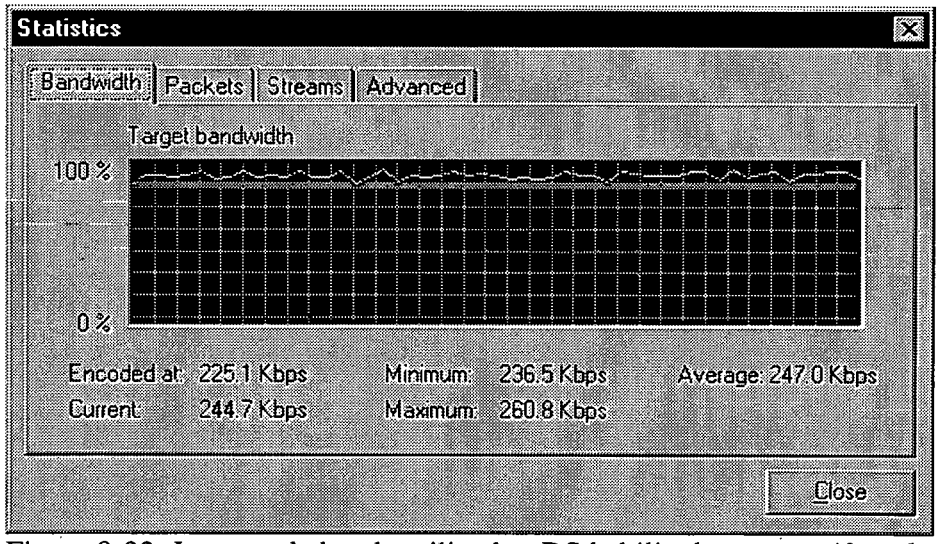


Figura 8-32- Largura de banda utilizada - DS habilitado e sem tráfego *background*

Observando-se as figuras numeradas de Figura 8-32 até Figura 8-37 pode-se fazer as seguintes afirmações:

- a aplicação consegue obter a largura de banda desejada e não experimenta perda de pacotes nas seguintes situações da rede:
  - rede sem DS habilitado e sem tráfego de *background*; e
  - rede com DS habilitado e com tráfego de *background*.

- a aplicação não consegue obter a largura de banda desejada e experimenta perda de pacotes elevada quando DS não está habilitado e existe tráfego em *background*.

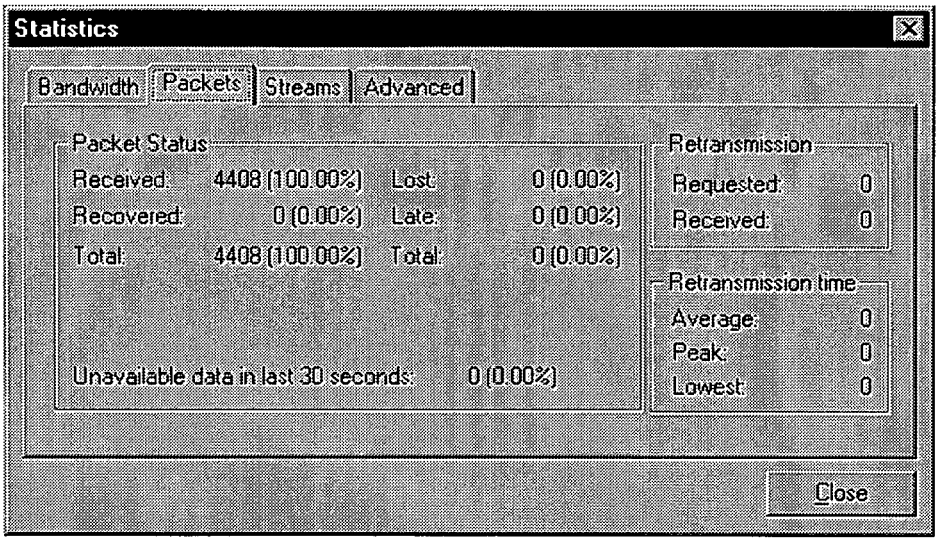


Figura 8-33 - Taxa de perda de pacotes - DS habilitado e sem tráfego *background*

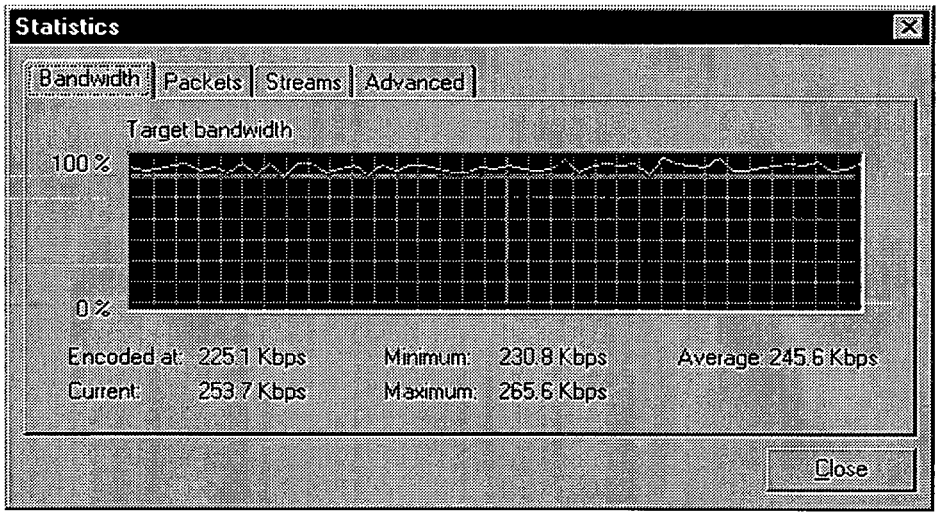


Figura 8-34 – Largura de banda utilizada - DS habilitado – tráfego *background* UDP com pacote de 1500 bytes e vazão de 2 Mbps

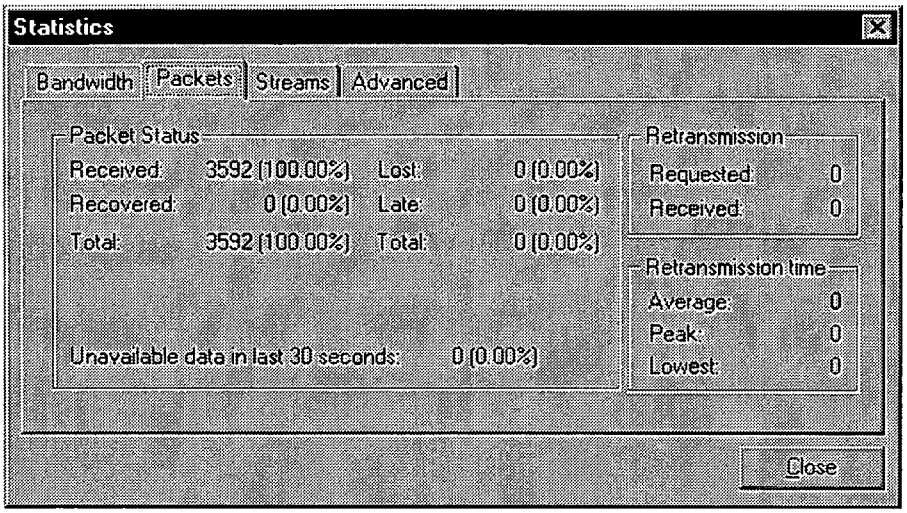


Figura 8-35 - Taxa de perda de pacotes - DS habilitado – com tráfego *background* UDP com pacote de 1500 bytes e vazão de 2 Mbps

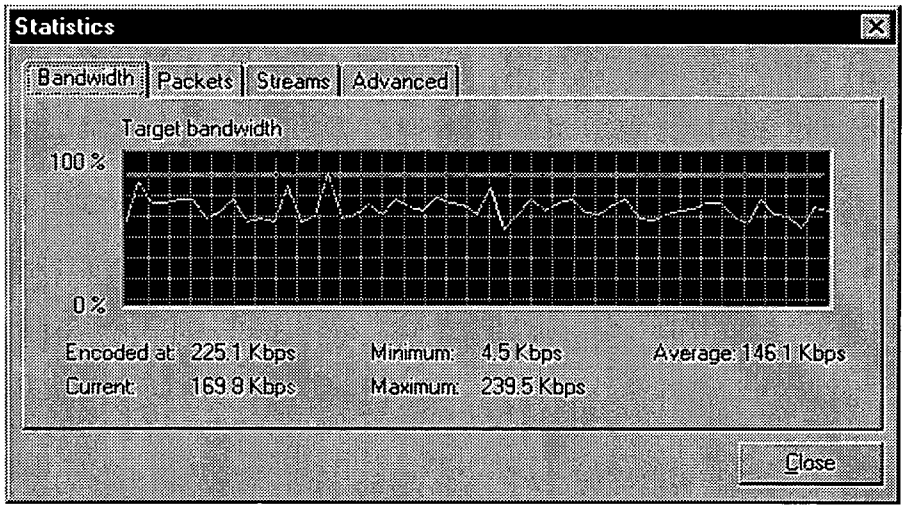


Figura 8-36 – Largura de banda utilizada - DS não habilitado – tráfego *background* UDP com pacote de 1500 bytes e vazão de 2 Mbps

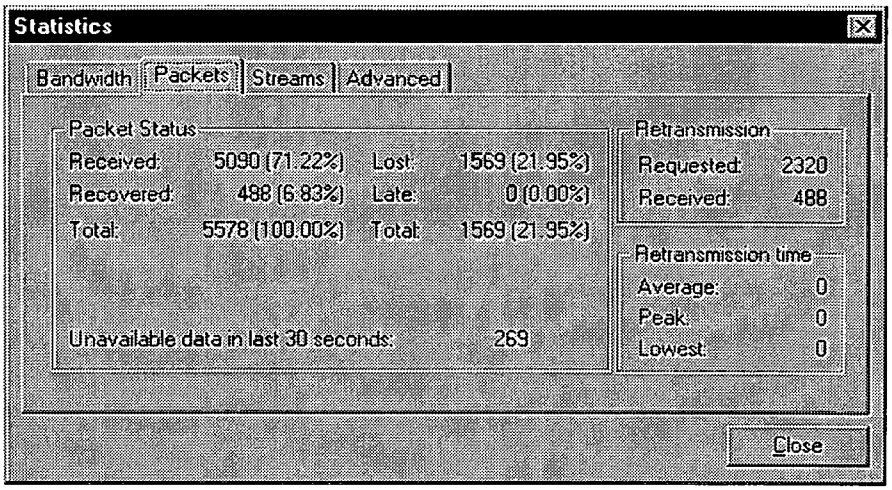


Figura 8-37 - Taxa de perda de pacotes – DS não habilitado – tráfego *background* UDP com pacote de 1500 bytes e vazão de 2 Mbps

Embora a aplicação Real Server seja do tipo adaptativa, ou seja, ela procura se adaptar às condições da rede, o que se observou é que sob condições de tráfego intenso competindo por largura de banda, a não configuração dos parâmetros de qualidade de serviço na rede inviabiliza totalmente sua utilização, pois tanto o áudio quanto o vídeo aparecem muito fragmentados, fato este que comprova os resultados obtidos nas medições.

Um outro experimento realizado neste contexto foi a transmissão de vídeo nos padrões MPEG-1 e MPEG-2 com taxas de codificação variando entre 1 Mbps e 4 Mbps. Neste caso a situação foi ainda pior. A aplicação utilizada, *Comotion UDP* da Optibase, não é do tipo adaptativa e quando na presença de tráfego em *background* competindo por largura de banda teve sua transmissão interrompida. Porém, com a devida configuração dos parâmetros de QoS, seu comportamento é adequado, independentemente do tipo de tráfego em *background.*

8.3 Conclusões - Fase II

A fase II do estudo concentrou esforço na avaliação do efeito do tráfego BE em *background* sobre os parâmetros de QoS (atraso, variação do atraso e taxa de perdas) medidos nos fluxos EF. Os resultados obtidos evidenciam que qualidade de serviço não é apenas um problema de engenharia de redes e gerência, mas é também um problema a ser estudado no âmbito da segurança de redes, pois demonstrou-se que os mecanismos para priorização do tráfego em serviços diferenciados, embora eficientes na maioria dos casos, em determinadas condições de saturação da rede são afetados pelo tráfego de *background* intenso, conforme mostram os indicadores utilizados na avaliação. Neste caso, o atraso e o *jitter* não podem ser adequadamente controlados e também ocorre significativa perda de pacotes. Na análise quantitativa este problema ficou mais evidente no ambiente DS IBM, provavelmente em função de ajustes nos algoritmos de reserva de recursos e também pela velocidade do canal de comunicação, que operando a 64 Kbps, necessita de uma quantidade de tempo elevada para transmitir os pacotes de baixa prioridade e de tamanho grande, aumentando nesse momento o tempo de fila dos pacotes de alta prioridade e, consequentemente, aumentando o atraso e indicadores relacionados. Este problema pode também ser comprovado nos experimentos da análise

qualitativa, pois nessas condições a qualidade da voz percebida foi classificada como ruim.

De forma resumida, comparando-se o comportamento esperado para os parâmetros de QoS analisados com o comportamento observado nos experimentos tem-se:

1) Segundo RFC 2598[31] – "Classe EF pode ser utilizada para suporte a aplicações com requisitos de":

- baixo atraso;
- baixa variação do atraso; e
- baixa taxa de perdas.

2) Desta forma, o comportamento esperado da classe EF na rede experimental é o comportamento semelhante ao observado na rede sem carga, qual seja:

- atraso menor que 50 ms;
- variação do atraso menor que 50 ms; e
- taxa de perda de pacotes próxima de 0%.

3) Ao invés disto o comportamento observado na classe EF ocorreu como segue:

- o atraso, a variação do atraso e a taxa de perdas dependem do tamanho do pacote e tipo de tráfego em *background;*
- seus níveis aumentam na medida em que se aumenta o tamanho do pacote do tráfego em *background;*
- o tráfego UDP influencia mais do que o tráfego TCP;
- quanto ap atraso e *jitter* o número de fluxos EF possui influência moderada; e
- quanto à taxa de perdas para um fluxo EF está dentro do esperado e para 3 ou mais fluxos EF, o valor está muito acima do esperado e necessita análise complementar.

Em uma avaliação final e resumida deste ambiente conclui-se que:

- a classe de serviços EF foi efetiva para garantia de QoS, porém apresentou restrições;
- quando o tráfego UDP em *background* possui pacotes de tamanho superior a 512 bytes o atraso é superior a 200 ms;
- um ataque "DoS" pode gerar tráfego desse tipo e, conseqüentemente, comprometer os níveis de serviços acordados; e
- a taxa de perdas observada para 3 e 5 fluxos EF deve ser melhor investigada.

Como contornos para esses problemas pode-se, em uma situação real, utilizar técnicas como a fragmentação dos pacotes, limitando-os a 512 bytes. Neste caso, pode-se utilizar o padrão *multilink ppp,* ou ainda, adicionalmente, ajustar os algoritmos de enfileiramento e formatação (*shaping*) do tráfego.

No ambiente DS CISCO também verificou-se o efeito do tráfego de baixa prioridade em *background* sobre o tráfego de alta prioridade EF. Porém, os valores obtidos para os parâmetros de QoS na análise quantitativa através das medições e também na análise qualitativa através da transferência de fluxos de aúdio e vídeo demonstraram que esse efeito não é suficiente para inviabilizar esse tipo de aplicação.

Novamente neste ambiente, a comparação do comportamento esperado para os parâmetros de QoS analisados, com o comportamento observado nos experimentos, é pertinente e faz-se a seguinte análise:

1) Segundo RFC 2598 [31] – "Classe EF pode ser utilizada para suporte a aplicações com requisitos de":

- baixo atraso;
- baixa variação do atraso; e
- baixa taxa de perdas.

2) Desta forma o comportamento esperado na classe EF na rede experimental é o comportamento semelhante ao observado na rede sem carga, qual seja:

- atraso menor que 6 ms;
- variação do atraso menor que 150 ms; e
- taxa de perda de pacotes próxima de 0%.

3) Quanto ao comportamento observado durante os experimentos tem-se o seguinte:

- atraso, variação do atraso e a taxa de perdas dependem do tamanho do pacote e tipo de tráfego em *background;*
- seus níveis aumentam na medida em que aumenta do tamanho do pacote em *background;*
- o tráfego UDP influencia mais do que o tráfego TCP;
- o número de fluxos EF possui influência muito pequena;
- quanto ao atraso (este se mantém muito baixo, menor do que 20 ms no pior caso);

- quanto à variação do atraso (este mantém valor médio entre 150 e 200 ms e esse valor, embora apresente uma constância, necessita de análise complementar, pois mesmo não existindo referências na documentação da ferramenta de medição[39], acredita-se que esta não efetue corretamente a estimativa do atraso médio. O valor esperado para a variação do atraso deveria ser próximo ao valor do atraso);
- auanto à taxa de perdas (embora estes valores sejam inferiores a 0,2%, na maioria dos casos, devem ser melhor estudados pois esta precisão pode ser melhorada.

Em uma avaliação final e resumida deste ambiente conclui-se que:

- os resultados das medições demonstraram que a classe de serviços EF foi efetiva para garantia de QoS porém não oferece o comportamento semelhante ao de um *"canal dedicado" "virtual leased line";* e
- a qualidade na transmissão de vídeo e as estatísticas referentes a largura de banda e as perdas comprovam a efetividade deste mecanismo para esse tipo de aplicação.

Também neste caso, o ajuste nos algoritmos de enfileiramento e formatação do tráfego pode ser utilizado para contornar possíveis desvios nos níveis de serviços contratados.

Por fim, o foco deste trabalho, voltado para uma análise específica sobre o efeito do tráfego BE em *background* sobre o atraso, a variação do atraso e a taxa de perdas no tráfego EF, fez com que fosse percebida a necessidade de uma ferramenta para geração de tráfego com capacidade de representar melhor as condições de uma rede real. Ou seja, uma ferramenta que possibilite a geração de tráfego TCP e UDP com pacotes de tamanhos variáveis e distribuídos ao longo da medição em percentuais parametrizáveis.

9 CONCLUSÕES

9.1 Principais contribuições

Neste trabalho elaborou-se uma pesquisa bibliográfica importante, baseada em livros, artigos publicados, RFCs e documentação de fabricantes sobre Qualidade de Serviço em redes IP. No decorrer do trabalho foram apresentados conceitos e fundamentos relacionados a QoS bem como justificativas para elaboração de pesquisas e experimentos nesta área.

Serviços Diferenciados (DiffServ) foi apresentado como solução para a implementação de QoS em redes WAN e um conjunto de experimentos foi realizado para avaliar a implementação DS em dois ambientes de testes. A implementação de QoS usando DiffServ envolveu a definição de políticas, perfis e ações em cada um dos roteadores. Cada perfil identifica os fluxos ou agregados de fluxos, enquanto que as ações determinam como serão marcados os campos DSCP de cada pacote. Através desta marcação, é alcançada a escalabilidade, uma vez que os roteadores intermediários não necessitam realizar mais a classificação MF.

Os resultados atingidos por este trabalho e sumarizados no item 7.5 (Conclusões - Fase I) e no item 8.3 (Conclusões - Fase II) indicam que esta é uma área onde o trabalho de experimentação e de pesquisa ainda se faz necessário.

Na fase I, no ambiente DS IBM, foi possível comprovar experimentalmente a efetividade dos mecanismos DS quanto ao isolamento e garantia de largura de banda para as diferentes classes de tráfego (EF, AF e BE). E na fase II, nesse mesmo ambiente, agora em uma análise mais específica quanto ao atraso, a variação do atraso e taxa de perdas, constatou-se que o tráfego BE em *background* afeta esses parâmetros de qualidade medidos no tráfego EF. Esta constatação indica a necessidade de aprofundar os estudos sobre os ajustes dos mecanismos de garantia de largura de banda e priorização de tráfego tais como os mecanismos de escalonamento, enfileiramento e ajuste de *buffers* e indica também, a necessidade de associar os estudos de qualidade de serviços à gerência de segurança, pois a detecção e eliminação de um tráfego intenso que ocorra de forma indevida irá contribuir para a garantia QoS para o tráfego prioritário.

Por outro lado, na fase II, no ambiente DS CISCO, ficou demonstrado de forma quantitativa através das medições e de forma qualitativa através de transmissões de vídeo, que Serviços Diferenciados apresentam uma solução consistente para priorização de tráfego, em particular, para as aplicações de áudio e vídeo. Evidentemente, não é uma garantia matemática, pois o tráfego BE em *background* afeta o desempenho do tráfego na classe EF, porém, é possível através de ajustes em *buffers* e/ou na utilização de diferentes algoritmos de priorização adequar-se à rede para satisfazer as necessidades das diversas aplicações.

Finalmente, conclui-se que um dos princípios fundamentais de projeto do IP que é derivado do "argumento fim-a-fim" que põe inteligência nas extremidades da rede, não pode mais vigorar de forma absoluta. Não adianta aumentar indefinidamente a largura de banda da rede como forma de garantir qualidade para as aplicações. É necessário administrar a largura de banda e priorizar certos tipos de tráfego como forma de garantir qualidade para as aplicações e evitar a contratação desnecessária de mais largura de banda encarecendo o custo de manutenção da rede.

9.2 Sugestões para trabalhos futuros

No decorrer deste trabalho verificou-se a necessidade de aprofundar os estudos e experimentos nas seguintes áreas:

9.2.1 Medições

Embora os resultados obtidos com as ferramentas utilizadas sejam considerados satisfatórios, determinadas situações de comportamento dinâmico da rede não puderam ser avaliadas por deficiências das ferramentas utilizadas. Neste trabalho ficou evidenciado que o tamanho do pacote, do tráfego melhor esforço em *background,* é o fator que mais influencia no aumento do atraso, variação do atraso e taxa de perdas. Para uma avaliação mais adequada da influência desse tipo de tráfego em uma rede real, as ferramentas para geração de tráfego do tipo melhor esforço, *background*, devem possibilitar a geração simultânea de tráfego com pacotes de tamanhos variados que

representem uma rede típica, incluindo a distribuição da quantidade de cada tamanho de pacote ao longo da medição.

9.2.2 Gerência de segurança e qualidade de serviço

Ficou demonstrado que a injeção de tráfego intenso sem confirmação, do tipo UDP com pacotes de determinados tamanhos, afeta o desempenho dos fluxos priorizados, em termos de atraso e taxa perdas. Sob estas condições, testes qualitativos demonstraram que as aplicações que possuem requisitos rígidos em relação a estes parâmetros podem ter sua qualidade afetada.

Esta constatação é um indicativo da importância do gerenciamento de segurança ao mesmo tempo em que uma rede é configurada para suportar QoS através de Serviços Diferenciados. Ataques do tipo DoS (*Denial of Service*) e DDoS (*Distributed Denial of Service*) que fazem uso intenso desse tipo de tráfego podem afetar significativamente os mecanismos de priorização e portanto devem ser detectados e possivelmente bloqueados.

9.2.3 Engenharia de tráfego

No desenvolvimento deste trabalho, principalmente nos experimentos relacionados à análise qualitativa, percebeu-se que o ajuste no tamanho dos *buffers* das filas de saída ou a mudança do algoritmo de enfileiramento de uma interface pode fazer a diferença entre uma transmissão de áudio e vídeo de boa qualidade ou falta completa de qualidade. Neste sentido, estudos que busquem a indicação, para cada tipo de tráfego, de quais ajustes nos *buffers* e quais algoritmos de enfileiramento são mais adequados em diferentes situações, podem contribuir para uma maior utilização dos mecanismos de controle de tráfego disponíveis.

9.2.4 Análise estatística

Os resultados apresentados neste trabalho se concentraram em poucas variáveis e não foi possível elaborar um estudo para estabelecer correlação entre as mesmas. Uma base de dados contendo um grande conjunto de variáveis e valores que foram utilizados para o cálculo dos valores médios apresentados está formatada e armazenada e pode ser utilizada para elaboração de uma análise estatística.

10 REFERÊNCIAS

[1] **Allen, A.O. (1994):** *Introduction to Computer Performance Analysis with Mathematica.* Academic Press.

[2] **Almes, G.; Kalidindi, S. & Zekauskas, M. (1999):** A One-Way Packet Loss Metric for IPPM, Request for Comments 2680. http://www.ietf.org/rfc/rfc2680.txt.

[3] **Almes, G.; Kalidindi, S. & Zekauskas, M.(1999):** *One-way Delay Metric for IPPM*, Request for Comments 2679. http://www.ietf.org/rfc/rfc2679.txt.

[4] ATM fórum. http://www.atmforum.org.

[5] **Baker, F. (Ed) (1995):** *Requirements for IP Version 4 Routers*, Request for Comments 1812. http://www.ietf.org/rfc/rfc1812.txt.

[6] **Bernet, Y.; Blake, S.; Grossman, D. & Smith, A. (2001):** *An Informal Management Model for Diffserv Router*, Internet Drafts. ftp://ftp.ietf.rnp.br/internet-drafts/draft-ietf-diffserv-model-06.txt.

[7] **Bernet, Y.; Durham, D. & Reichmeyer, F. (1998):** *Requirements of Diff-serv Boundary Routers* , Internet Draft .http://www.cs.wustl.edu/~luther/Classes/Cs524/DiffServ/draft-bernet-diffedge-01.html.

[8] **Bernet, Y.; Yavatkar, R.; Ford, P.; Baker, F.; Zhang, L.; Nichols, K. & Speer, M. (1998):** *A Framework for Use of RSVP with Diff-Serv Networks*, draft-ietf-diffserv-rsvp-01.txt.

[9] **Black, D.; Blake, S.; Carlson, M.; Davies, E.; Wang, Z. & Weiss, W. (1998):** *An Architecture for Differentiated Services*, Request for Comments 2475. ftp://ftp.nic.it/rfc/rfc2475.txt.

[10] **Braden, R.; Clark, D. & Shenker, S. (1994):** *Integrated Services in the Internet Architecture: an Overview*, Request for Comments 1633. http://www.ietf.org/rfc/rfc1633.txt.

[11] **Bradner S. (1991):** *Benchmarking Terminology for Network Interconnection Devices* , Request for Comments 1242, http://www.ietf.org/rfc/rfc1242.txt.

[12] **Cisco System Inc. (1999):** *Quality of Service Overview.* http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/qos_c/qcintro.htm.

[13] Cisco System Inc. (1999): *Quality of Service Solutions. White Paper* http://www.cisco.com.

[14] Cisco System Inc. (1999): *Cisco Management Information Base (MIB) User Quick Reference*. http://www.cisco.com/univercd/cc/td/doc/product/software/ios11/mbook/index.htm.

[15] Cisco System Inc. (1999): *Cisco Network Monitoring and Event Correlation Guidelines*. http://www.cisco.com/warp/public/cc/pd/wr2k/tech/cnm_rg.htm.

[16] Cisco System Inc. (1999): *Cisco Threshold Manager*. http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwfw/cww31ovr/cwwgstm.htm.

[17] Cisco System Inc. (1999): *Internetworking Technology Overview,* Chapter 46. http://www.cisco.com/.

[18] Cisco System Inc. (2001): *Committed Access Rate – CAR.* http://www.cisco.com/warp/public/732/Tech/car/.

[19] Cisco System Inc., (1998), *Packet Voice Primer*. http://www.cisco.com.

[20] DeAngelis, R. C. (1998): *Defining Service Level Agreements: An Inside-Out Approach*. The Managed View, The Journal for Tivoli Customers and Partners, v 2 i4 Fall.

[21] Demichelis, C.; Chimento P. (1999): *Instantaneous Packet Delay Variation Metric for IPPM*, ippm draft, work under progress.

[22] Differentiated Service, http://www.ietf.org/html.charters/diffserv-charter.html.

[23] Ferguson, P. & Huston, G. (1999): *Quality of Service: Delivering QoS on the Internet and in Corporate Networks* - Wiley Computer Publishing.

[24] Heinanen, J. & Guerin, R. (1999): *A Single Rate Three Color Marker,* Request for Comments 2697. http://www.ietf.org/rfc/rfc2697.txt.

[25] Heinanen, J. & Guerin, R. (1999): *A Two Rate Three Color Marker* , Request for Comments 2698. http://www.ietf.org/rfc/rfc2698.txt.

[26] Heinanen, J.; Baker, F.; Weiss, W. & Wroclawski, J. (1999): *Assured Forwarding PHB Group*, Request for Comments 2597. http://www.ietf.org/rfc/rfc2597.txt.

[27] IETF: Internet Engineering Task Force. http://www.ietf.org.

[28] Integrated Services. http://www.ietf.org/html.charters/intserv-charter.html.

[29] IP Performance Metrics. http://www.ietf.org/html.charters/ippm-charter.html.

[30] IP Provider Metric. http://www.advanced.org/IPPM.

[31] **Jacobson, V.; Nichols, K.&. Poduri, K. (1999):** *An Expedited Forwarding PHB*, Request for Comments 2598. http://www.ietf.org/rfc/rfc2598.txt.

[32] **Jones, R. (1995):** *Netperf*. http://www.netperf.org/netperf/NetperfPage.html.

[33] **Linney, L. (1999):** Differentiated Services on IBM 221x Routers, IBM Co.

[34] **Microsoft Corp.** *NetMeting*. http://www.microsoft.com/windows/netmeeting/.

[35] **Microsoft Corporation (1999):** *Quality of Service Technical White Paper*. http://msdn.microsoft.com/library/psdk/gqos/qosstart_2cdh.htm.

[36] **Morgam, Edward B., (1997):** *Voice Over Packet White Paper*, Telogy Networks Inc. http://www.telogy.com.

[37] **Murayama, Y. & Yamaguchi, S. (1998):** *DBS (Distributed Benchmark System)*. http://shika.aist-nara.ac.jp/member/yukio-m/dbs/goal.html.

[38] **Muss, M. & Slattery, T. (1985):** *TTCP –Test TCP*. Army Research Laboratory. ftp://ftp.arl.mil/pub/ttcp/.

[39] **Naval Research Laboratory (NRL):** *The Multi-Generator (MGEN) Toolset*. http://manimac.itd.nrl.navy.mil/MGEN/.

[40] **Nichols, K. & Blake, S. (Eds) (1998):** *Differentiated Services Operational Model and Definitions*, Internet-Draft. http://diffserv.lcs.mit.edu/Drafts/draft-nichols-dsopdef-00.txt.

[41] **Nichols, K. & Carpenter, B. (2001):** *Definition of Differentiated Services Per Domain Behaviors and Rules for their Specificatio*, Request for Comments 3086. http://www.ietf.org/rfc/rfc3086.txt.

[42] **Nichols, K. (Ed.) & Blake, S. (Ed). (1998):** *Differentiated Services Operational Model and Definitions*, Internet Draft. http://diffserv.lcs.mit.edu/Drafts/draft-nichols-dsopdef-00.txt.

[43] **Nichols, K.; Blake, S.; Baker, F. & Black, D. (1998):** *Definition of the Differentiated Services Filed (DS Field) in the Ipv4 and Ipv6 Headers*, Request for Comments 2474. http://www.ietf.org/rfc/rfc2474.txt.

[44] **Paxson, V.; Almes, G.; Mahdavi, J. & Mathis, M. (1998):** *Framework for IP Performance Metrics*, Request for Comments 2330. http://www.ietf.org/rfc/rfc2330.txt.

[45] **Braden, R., Ed. (1997):** *Resource ReSerVation Protocol (RSVP) – Version 1, Functional Specification,* Request for Comments 2205. ftp://ftp.nic.it/rfc/rfc2205.txt.

[46] **Guerin, R.; Blake, S. & Herzog, S. (1997):** *Aggregating RSVP-based QoS Requests*. Internet Draft. http://globecom.net/ietf/draft/draft-guerin-aggreg-rsvp-00.html.

[47] **Saltzer J.; Reed, D. & Clark, D. (1984):** *End to End Arguments in System Design* ACM Transactions in Computer Systems, Nov, 1984. http://www.reed.com/Papers/EndtoEnd.html.

[48] **Schimidt, A. G. & Minoli, D. (1997):** *Multiprotocol over ATM: Building state of the Art ATM Intranets utilizing RSVP, NHRP, LANE, flow switching, and WWW technology*, Manning Publications Co., Greenwich.

[49] **Shenker, S.; Partridge, C. & Guerin, R. (1997):** *Specification of Guaranteed Quality of Service*, Request For Coments 2212. http://www.ietf.org/rfc/rfc2211.txt.

[50] **Stardust Technologies, Inc. (1999):** *QoS protocols & architectures*, White Paper. http://www.qosforum.com/white-papers/qosprot_v3.pdf.

[51] **Stardust Technologies, Inc. (1999):** *Internet Bandwidh Management,* White Paper. http://www.qosforum.com.

[52] **Stardust Technologies, Inc. (1999):** *Introduction to QoS Policies*, White Paper. http://www.qosforum.com/white-papers/qospol_v11.pdf.

[53] **Stardust Technologies, Inc. (1999):** *The Need for QoS*, White Paper,. http://www.qosforum.com/white-papers/Need_for_QoS-v4.pdf.

[54] **Stardust Technologies, Inc., (1999):** *Frequently Asked Questions about IP Quality of Service*. http://www.qosforum.com.

[55] **Stardust Technologies, Inc., (1999):** *Technology Backgrounder - Quality of Service – Glossary of Terms*, White Paper. http://www.qosforum.com.

[56] **Teitlebaum, B. & Hans, T. (1998):** QoS Requirements for Internet2, Internet2 Technical Paper. http://www.internet2.edu/qos/may98Workshop/html/requirements.html.

[57] **Wroclawski, J. (1997):** *Specification of the Controlled-Load Network Element Service*, Request For Coments 2211. http://www.ietf.org/rfc/rfc2211.txt.

[58] **X. Xiao, L.M. Ni.(1999):** *Internet QoS: A Big Picture*, IEEE Networks Mar-99. http://www.comsoc.org/ni/private/1999/mar/pdf/Xiao.pdf.

11 ANEXO I – CONFIGURAÇÃO DS AMBIENTE IBM

11.1 Introdução

Neste anexo é mostrado como foram configurados os roteadores IBM para realização dos experimentos de medição de QoS na fase II. Na Figura 11-1 é mostrado a topologia do ambiente montado. Note-se que o ambiente é formado por três nós DS: border1, border2 e interior1.

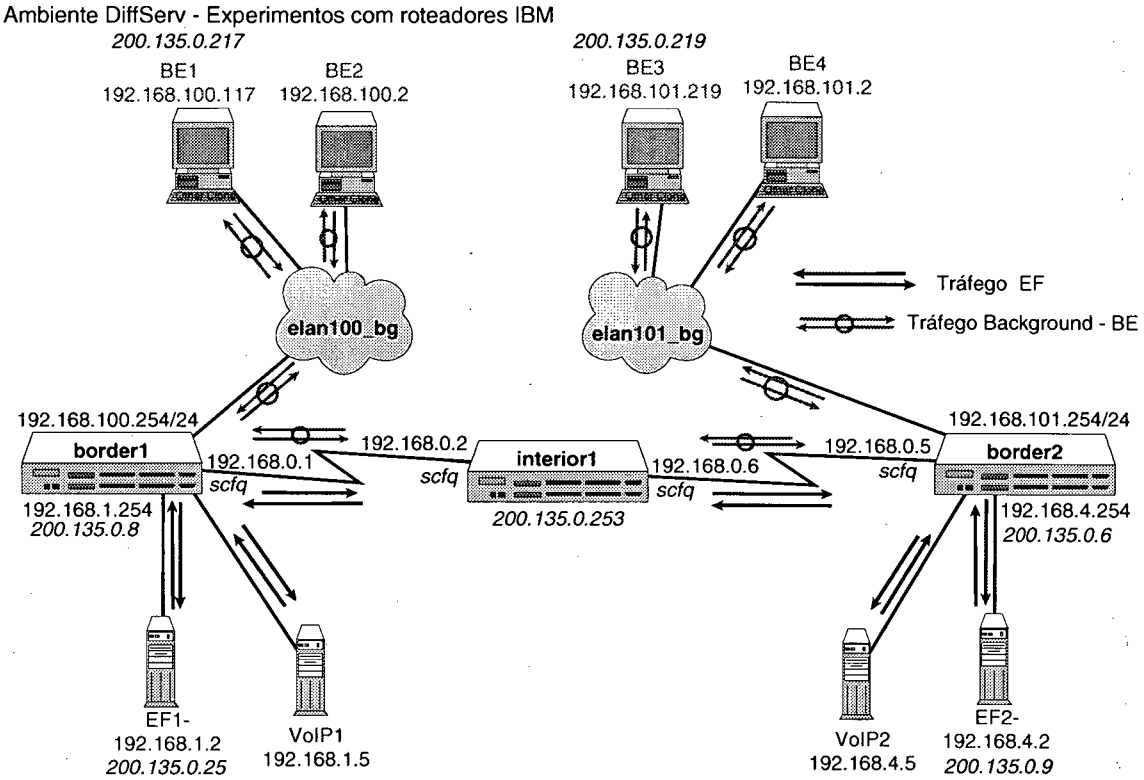


Figura 11-1 – Ambiente DS IBM – fase II

11.2 Habilitação do serviço DS

Nos roteadores IBM modelos 2210 e 2216, utilizados neste trabalho, a configuração de DS é feita em duas etapas; a primeira consiste em habilitar DS globalmente e a segunda consiste em habilitar DS em cada interface. Na Tabela 11-1 são mostrados os parâmetros de configuração utilizados nos nós DS border1, border2 e interior1.

Tomando-se como exemplo border1 tem-se:

- são definidas duas filas "NumQ"; a fila EF para o tráfego expresso e a fila AF/BE compartilhada entre o tráfego melhor esforço e "Assured";

- a interface número 1 PPP tem DS habilitado;
- o peso da fila *premium* "*Premium Wght*" é de 90 por cento. Significa que o algoritmo de escalonamento SFCQ irá atender esta fila 90% do tempo. Caso se queira reduzir o atraso nas filas AF e BE deve-se reduzir o peso da fila *premium*;
- o buffer de saída da fila *premium* "*Premium OutBuf*" tem 5500 bytes e o da fila AF/BE "*Assured OutBuf*" tem 27500 bytes;
- a fila *premium* pode alocar no máximo "*Premium MaxQoS*", 95% dos 5500 bytes assinalados para "OutBuf", os 5% restantes são utilizados para pelo sistema como *buffers* compartilhados. Este valor também significa que a soma dos requisitos de largura de banda para a fila *EF-premium*, definidos nas ações DS, não podem ultrapassar a 38% que é 95% de 40%; e
- a fila AF/BE pode utilizar apenas 80% dos 27500 bytes de "OutBuf", os 20% restantes são utilizados com *buffers* compartilhados. Este valor também significa que a soma dos requisitos de largura de banda para a fila EF/BE, definidos nas ações DS, não podem ultrapassar a 64% que é 80% de 80%.

A configuração para habilitação de DS em border2 é semelhante a border1. No nó DS interior1, duas interfaces, PPP 3 e PPP 4 estão com DS habilitado.

Uma política de DS é um mecanismo que permite relacionar um perfil de tráfego a uma ação em um determinado período de tempo. Na Tabela 11-2, tomando como exemplo o nó DS border1 temos uma política que define:

- o perfil de tráfego será selecionado, perfil de nome "border1";
- o tráfego aderente ao perfil "border1" sofrerá uma ação da ação de DS de nome "border1"; e
- esta política irá atuar sobre o tráfego no espaço de tempo definido pelo período de validade de nome "allTheTime".

Através do mecanismo de perfil de tráfego é executada a classificação dos pacotes que ingressam no domínio DS. Em geral a classificação feita nos nós DS de borda é do tipo MF (*multi-field*) e a classificação feita nos nós de interior é do tipo BA (*Behavior Aggregate*). Na Tabela 11-3 temos os perfis de tráfego para os três nós DS. A classificação feita em border1 seleciona todos os pacotes que tiverem como endereço

fonte a rede 192.168.1.0/255.255.255.0 e como endereço destino a rede 192.168.4.0/255.255.255.0, independentemente do protocolo que está sendo utilizado "proto = 0:255" e das portas fonte "sPort = 0 : 65535" e destino "dPort = 0 : 65535". O campo TOS ou DSCP deve ter valor igual a zero "TOS = x00 : x00". A classificação feita por border2 segue os mesmos critérios.

```
border1> Config>FEATURE DS
Differential Services Config
border1> DS Config>LIST ALL
System Parameters:
        DiffServ:                ENABLED
        Packet_size:             550
        Min BE Alloc (%):        10
        Min CTL Alloc (%):       5
        Number_of_Q:             2
-------------------------------------------------------------------------------
                         ---------- Premium -------   --------- Assured --------
Net If     Status  NumQ Bwdth  Wght  OutBuf  MaxQos Bwdth  Wght  OutBuf  MaxQos
Num                      (%)   (%) (bytes)     (%)   (%)   (%) (bytes)     (%)
-------------------------------------------------------------------------------
1   PPP    Enabled     2    40    90    5500      95    60    10   27500      80
border2 DS Config>LIST ALL
 System Parameters:
        DiffServ:                ENABLED
        Packet_size:             550
        Min BE Alloc (%):        10
        Min CTL Alloc (%):       5
        Number_of_Q:             2
-------------------------------------------------------------------------------
                         ---------- Premium -------   --------- Assured --------
Net If     Status  NumQ Bwdth  Wght  OutBuf  MaxQos Bwdth  Wght  OutBuf  MaxQos
Num                      (%)   (%) (bytes)     (%)   (%)   (%) (bytes)     (%)
-------------------------------------------------------------------------------
1   PPP    Enabled     2    40    90    5500      95    60    10   27500      80
interior DS Config>LIST ALL
 System Parameters:
        DiffServ:                ENABLED
        Packet_size:             550
        Min BE Alloc (%):        10
        Min CTL Alloc (%):       5
        Number_of_Q:             2
-------------------------------------------------------------------------------
                         ---------- Premium -------   --------- Assured --------
Net If     Status  NumQ Bwdth  Wght  OutBuf  MaxQos Bwdth  Wght  OutBuf  MaxQos
Num                      (%)   (%) (bytes)     (%)   (%)   (%) (bytes)     (%)
-------------------------------------------------------------------------------
3   PPP    Enabled     2    40    90    5500      95    60    10   27500      80
4   PPP    Enabled     2    40    90    5500      95    60    10   27500      80
```

Tabela 11-1 – Habilitação de DS nos nós border1, border2 e interior1

No nó DS interior1 a classificação é do tipo BA e neste caso o roteador necessita somente verificar o valor do campo TOS ou DSCP. Neste caso serão classificados todos os pacotes com valor de TOS = xB8 que foi o valor atribuído para esse campo sobre o tráfego selecionado em border1 e border2.

```
border1> Policy config>LIST ALL
Configured Policies....
Policy Name      = border1
        State:Priority =Enabled     : 5
        Profile        =border1
        Valid Period    =allTheTime
        DiffServ Action=border1
border2 Policy config>LIST ALL
Configured Policies....
Policy Name      = border2
        State:Priority =Enabled     : 5
        Profile        =border2
        Valid Period    =allTheTime
        DiffServ Action=border1
interior Policy config>LIST ALL
Configured Policies....
Policy Name      = interior
        State:Priority =Enabled     : 5
        Profile        =interior
        Valid Period    =allTheTime
        DiffServ Action=interior
```

Tabela 11-2 –Definição de políticas nos nós DS border1, border2 e interior1

```
Configured Profiles....
 Profile Name     = border1
        sAddr:Mask=     192.168.1.0 : 255.255.255.0    sPort=     0 : 65535
        dAddr:Mask=     192.168.4.0 : 255.255.255.0    dPort=     0 : 65535
        proto      =               0 : 255
        TOS        =             x00 : x00
        Remote Grp=All Users
Configured Profiles....
Profile Name     = border2
        sAddr:Mask=     192.168.4.0 : 255.255.255.0    sPort=     0 : 65535
        dAddr:Mask=     192.168.1.0 : 255.255.255.0    dPort=     0 : 65535
        proto      =               0 : 255
        TOS        =             x00 : x00
        Remote Grp=All Users
Configured Profiles....
Profile Name     = interior
        sAddr:Mask=         0.0.0.0 : 0.0.0.0          sPort=     0 : 65535
        dAddr:Mask=         0.0.0.0 : 0.0.0.0          dPort=     0 : 65535
        proto      =               0 : 255
        TOS        =             xFC : xB8
        Remote Grp=All Users
```

Tabela 11-3 – Definição dos perfis de tráfego nos nós DS border1, border2 e interior1

O tráfego selecionado nos perfis de tráfego em border1, border2 e interior1, é submetido às ações DS de mesmo nome.

Na Tabela 11-4 são definidas as ações em cada um dos nós DS configurados. Para boder1 tem-se que o nome da ação é "border1"; a instrução "DS mask:modify =xFC:xB8" indica que o campo DSCP ou ToS deve ser remarcado com o valor xB8; a fila EF-Premium deve ter uma largura de banda de 38% do total disponível que no nosso caso é 64000 bps; a aplicação deve cuidar para que a taxa de bits dessa classe de tráfego não ultrapasse, pois se isso acontecer o tráfego excedente será descartado; a ação "border2" é semelhante a ação "border1".

```
Configured DiffServ Actions....
DiffServ Name    = border1                          Type =Permit
        DS mask:modify =xFC:xB8
        Queue:BwShare  =Premium     : 38 %
        Token Rate:    = 0 bytes/sec
        Token Bucket:  = 0 bytes
Configured DiffServ Actions....
DiffServ Name    = border2                          Type =Permit
        DS mask:modify =xFC:xB8
        Queue:BwShare  =Premium     : 38 %
        Token Rate:    = 0 bytes/sec
        Token Bucket:  = 0 bytes
Configured DiffServ Actions....
DiffServ Name    = interior                         Type =Permit
        DS mask:modify =x00:x00
        Queue:BwShare  =Premium     : 38 %
        Token Rate:    = 0 bytes/sec
        Token Bucket:  = 0 bytes
```

Tabela 11-4 - Definição das ações sobre o tráfego nos nós DS border1, border2 e interior1

A ação DS definida no nó interior1 não faz marcação dos pacotes, pois esta marcação já foi feita em border1 e border2, a instrução "DS mask:modify = x00 : x00" indica que não é para fazer marcação nos pacotes. Neste nó somente é feita a medição do tráfego para garantir que o mesmo não exceda o valor máximo definido.

A implementação DS dos roteadores utilizados permite definir a data e hora em que a política irá atuar. A Tabela 11-5 mostra que esta facilidade permite que uma determinada política de QoS seja acionada automaticamente em determinada hora, de um determinado dia e de um determinado mês.

```
Configured Validity Periods
Validity Name    = allTheTime
        Duration  = Forever
        Months    = ALL
        Days      = ALL
        Hours     = All Day
```

Tabela 11-5 – Definição dos períodos de validade da política definida

12 ANEXO II – CONFIGURAÇÃO DS NO AMBIENTE CISCO

12.1 Introdução

Este anexo mostra como foram configurados os roteadores CISCO para realização dos experimentos de medição de QoS na fase II. Na Figura 12-1 é mostrada a topologia do ambiente montado. Note-se que o ambiente é formado por dois nós DS: Cisco 7507 e Cisco 7200.

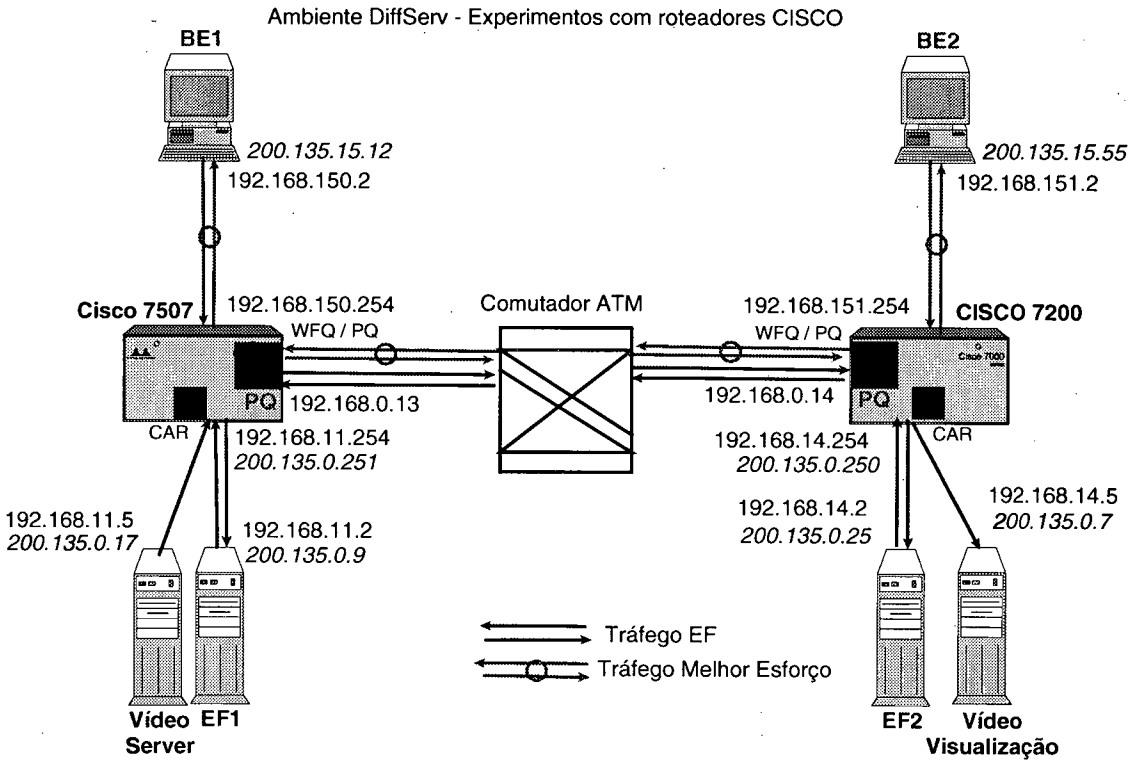


Figura 12-1 – Ambiente DS CISCO – fase II

Nos roteadores CISCO, com versão do IOS 12.0 ou superior a priorização ou tratamento diferenciado do tráfego IP é feita através da classificação e marcação dos pacotes na interface de entrada e a aplicação de um esquema de gerenciamento de filas na interface de saída que dê um tratamento distinto para cada classe.

A classificação e marcação são feitas na interface de entrada, através do mecanismo CAR conforme descrito no item 6.2.5.

A sintaxe e seqüência de comando para configuração do CAR são como segue:

- **interface** interface-type interface-number (Especifica a interface ou sub-interface. Este comando coloca o roteador no modo de configuração de interface);

- **rate-limit {input | output} [access-group [rate-limit]** *acl-index*] *bps burst-normal burst-max* **conform-action** *action* **exceed-action** *action* (Especifica uma política de taxa de bits para cada classe de tráfego. A Tabela 12-1 mostra uma descrição das ações para o caso de o tráfego estar em conformidade com a política e para o caso de o tráfego exceder);
- **access-list** *acl-index* **{deny | permit}** source source-wildcard ou **access-list** acl-index **{deny | permit}** protocol source source-wildcard destination destination-wildcard (Especifica uma lista de acesso padrão ou estendida); e
- **exit** (sai do modo de configuração de interfaces).

Palavra Chave	Descrição
continue	Avalia o próximo comando **rate-limit**
Drop	Elimina o pacote
set-prec-continue *new-prec*	Atribui valor para o campo IP Precedence e avalia o próximo comando **rate-limit**
set-prec-transmit *new-prec*	Atribui valor para o campo IP Precedence e transmite o pacote
set-dscp-continue *new-prec*	Atribui valor para o campo DSCP e avalia o próximo comando **rate-limit**
set-dscp-transmit *new-prec*	Atribui valor para o campo DSCP e transmite o pacote
transmit	Transmite o pacote

Tabela 12-1 – Opções do parâmetros conform-action e exceed-action do comando rate-limit

A priorização dos pacotes classificados e marcados na interface de entrada envolve os seguintes passos:

- definição do Class Maps;
- configuração do Class Policy no Policy Map; e
- aplicação da política de serviço e habilitação da PQ.

12.2 Segmento de configuração DS no roteador CISCO

O segmento de configuração DS CISCO, apresentado na Tabela 12-2, mostra que na interface de entrada é efetuada a classificação do tráfego. O tráfego que estiver em

conformidade com a política definida no rate-limit é transmitido para a interface de saída e o campo DSCP do cabeçalho dos pacotes é marcado com o DSCP 46. O tráfego que exceder é descartado. Nesta configuração específica a largura de banda reservada é de 344 Kbps e são classificados para essa classe, de acordo com a lista de acesso número 181, todos os pacotes que tiverem no endereço de origem um número IP pertencente a rede 192.168.11.0/255.255.255.0 e no endereço de destino um número IP pertencente a rede 192.168.14.0/255.255.255.0. Neste caso é realizada uma classificação MF.

```
Interface de entrada
Classificação, Marcação e Policiamento
interface FastEthernet1/0/0
 ip address 200.135.0.251 255.255.255.0
no ip directed-broadcast
rate-limit input access-group 181 344000 4500 7500 conform-action set-
dscp-transmit 46 exceed-action drop
 no ip route-cache cef
 ip route-cache distributed
full-duplex
!
access-list 181 permit ip 192.168.11.0 0.0.0.255 192.168.14.0
0.0.0.255
!
```

Tabela 12-2 –configuração DS – CISCO – (classificação, policiamento e marcação)

```
Interface de Saida
interface ATM4/0/0.400 point-to-point
 description Interface de teste (DiffServ)
 bandwidth 2000
 ip address 192.168.0.13 255.255.255.252
 no ip directed-broadcast
 ip accounting output-packets
 ip route-cache same-interface
 no atm enable-ilmi-trap
 pvc 0/400
  tx-ring-limit 5
  vbr-nrt 2000 2000 1
  encapsulation aal5mux ip
  service-policy out premium
 !
```

Tabela 12-3 – Configuração DS – CISCO – conexão da política de QoS na interface de saída

O segmento de configuração DS CISCO, apresentado na Tabela 12-3, mostra que na interface de saída é conectada a política para escalonamento dos pacotes. Nesta política "premium", são selecionados os algoritmos de escalonamento dos pacotes. Os pacotes

da classe "Class premium" terão uma reserva da banda de 344 Kbps e serão tratados por um algoritmo de prioridade estrita, o algoritmo *Priority Queueing* (ver item 4.1.2). Os demais pacotes da classe "class class-default" serão tratados pelo algoritmo WFQ (ver item 4.1.4).

Como se pode notar, nesta interface de saída através do "class-map premium", é realizada uma classificação de comportamento agregado BA. Neste caso são selecionados todos os pacotes com DCSP igual a 46.

O segmento de configuração DS CISCO, apresentado na Tabela 12-4, mostra uma política de QoS chamada "premium" que está associada a duas classes de serviços DS. A classe "class premium" e a classe "class-default". A primeira é a classe de serviço expresso EF, que é escalonado pelo algoritmo priority queue (seção 4.1.2) com uma reserva de banda de 344 Kbps. A classe "class-default" trata todo o restante do tráfego utilizando o escalonamento WFQ (seção 4.1.4) e o restante da largura de banda do canal.

```
! Escalonamento do tráfego
policy-map premium
  class do_nothing
   set ip precedence 2
  class premium
    priority 344
  class class-default
    fair-queue
!
class-map match-any do_nothing
  match ip precedence 1
! Define a classe premium e compara tráfego
class-map match-any premium
  description Trafego EF
  match ip dscp 46
!
```

Tabela 12-4 - Configuração DS – CISCO – (classificação, e escalonamento do tráfego)

13 ANEXO III – FERRAMENTAS DE GERAÇÃO E MEDIÇÃO DO TRÁFEGO

Neste anexo é dada uma visão geral sobre as ferramentas de medição e geração de tráfego utilizadas na fase II e são mostrados os *scripts* e parâmetros de configuração dessas ferramentas utilizados nos experimentos.

13.1 MGEN

A ferramenta MGEN é composta pelos módulos mgen para a geração de tráfego, drec para a recepção do tráfego na estação remota e o mcalc para geração das informações a partir do arquivo de saída gerado pelo drec. Esta ferramenta permite a geração controlada de tráfego UDP, sendo possível a geração de um ou mais fluxos unicast ou multicast com a taxa de bits desejada. A ferramenta permite também controlar o tempo do experimento e a variação do tamanho do pacote UDP utilizado.

Neste trabalho, esta foi a principal ferramenta de medição de desempenho utilizada. Ela foi empregada para a medição do atraso, da variação do atraso e da taxa de perda de pacotes durante a transmissão do fluxo priorizado da classe EF e também para a geração do tráfego "*background*" necessário para provocar congestionamento na rede. Nas próximas sessões são apresentados e explicados os *scripts* utilizados nos experimentos de medição do ambiente IBM e do ambiente CISCO. O MGEN roda em ambiente UNIX, neste trabalho foi utilizado no Linux Redhat 7.0. Os formatos dos comandos *mgen* e *drec* são mostrados abaixo:

```
/usr/local/MGEN/mgen -b ipaddr:porta -i eth0 -S hora -d duração -r taxa -s tamanho -p
porta
```

Onde:

-b = endereço IP e porta UDP da máquina que irá receber o tráfego;

-i = nome da interface através da qual o tráfego será gerado;

-S = hora em que o programa mgen irá iniciar a geração de tráfego;

-d = tempo da duração da geração de tráfego, em segundos;

-r = taxa de geração de pacotes por segundo;

-s = tamanho em bytes da carga do pacote = tamanho do pacote – o tamanho dos cabeçalhos IP e UDP; e

-p = número da porta UDP através da qual será gerado o tráfego (porta fonte).

```
/usr/local/MGEN/drec -b ipaddr -i eth0 -S hora -d duração -p porta-porta
```

Onde:

-b = endereço IP da máquina que irá gerar o tráfego.

-i = nome da interface onde o tráfego gerado pelo mgen irá ser recebido;

-S = hora em que o programa drec irá iniciar a recepção de tráfego;

-d = duração da recepção de tráfego em segundos; e

-p = número das portas que irão receber o tráfego gerado pelo mgen.

13.2 Netperf

O Netperf é uma ferramenta de *benchmark* para medir o desempenho de rede de computadores. Ela foi desenvolvida pela Divisão de Informação de Redes da Hewlett-Packard Company. A versão utilizada neste trabalho foi a 2.1.3 de setembro de 1997.

A ferramenta é composta de dois programas básicos – netperf e netserver. Baseado no modelo cliente-servidor, neste caso o modelo monitor-refletor, onde o tráfego é gerado de uma estação monitora com o programa netperf, até a estação refletora como netserver, onde o tráfego é refletido e retornado à estação monitora.

A terminologia do Netperf é a definida pela "Terminologia de *Benchmarking* para Equipamentos de Interconexão de Redes de Computadores" definida no RFC1242[11]. Este documento do IETF é o primeiro produto do Grupo de Trabalho de Metodologia de *Benchmarking*.

A ferramenta Netperf permite medir a latência fim-a-fim das estações. Os testes são realizados da seguinte maneira: ativar o programa netserver da ferramenta na máquina que será a refletora, e após, executa-se o script que chama o programa netperf.

O formato geral dos comandos é mostrado a seguir:

```
Comando para execução do refletor:
/usr/local/netserver
```

```
Comando para execução do programa de geração de tráfego
/usr/local/netperf/netperf –l sss –t TCP_RR –H xxx.xxx.xxx.xxx -- -r xx,yy
```

Onde:

-l = Tempo de duração da geração de tráfego em segundos;

-t = Protocolo e tipo de medição a ser realizada - neste caso o TCP_RR é a medição do número de transações *request/response* do TCP;
-H = Endereço IP da máquina remota que está executando o netserv; e
-r = tamanho do segmento de dados a ser enviado na medição e tamanho do segmento a ser respondido pelo netserv (xx,yy).

O Netperf define a configuração de diversos parâmetros, como, por exemplo, o tamanho do buffer das estações local e remota. Neste trabalho foram utilizados os parâmetros *default* do sistema operacional.

13.3 Geração e medição do tráfego no ambiente IBM

13.3.1 Geração e medição do tráfego EF

Dois *scripts* foram utilizados para execução das medições do tráfego EF, o fg-drec e o fg-mgen. Como as medições foram feitas em ambos os sentidos, procurando reproduzir uma conversação de voz, uma versão do script foi executada em cada máquina (EF1 e EF2).

Máquina EF1 #!/bin/bash h=$1 fl= $h t=300 /usr/local/MGEN/drec -b 192.168.4.2 -i eth0 -S $h -d $t -p 10200-10204,60200-60202 $fl &
Máquina EF2 #!/bin/bash h=$1 fl=eftcp$h t=300 /usr/local/MGEN/drec -b 192.168.1.2 -i eth0 -S $h -d $t -p 40000-40004,50000-50002 $fl &
Parâmetros do script fg-derec h = horário em que o programa drec irá iniciar a recepção de tráfego; fl = é o nome do arquivo que será gerado ao final da medição; e t = tempo da medição.

Tabela 13-1 – *Script* fg-drec – recepção do tráfego EF - (executado em EF1 e EF2)

Na Tabela 13-1 e Tabela 13-2 são mostrados os scripts que invocam, para execução nas máquinas EF1 e EF2, os programas drec e mgem. Os parâmetros passados para os *scripts* e para os programas também são descritos. Depois de decorrido um período de medição, um arquivo contendo dados sobre essa medição é gerado pelo programa drec. O programa mcalc cujo script de execução é mostrado na Tabela 13-3 é utilizado para

obter informações sobre o atraso, a variação do atraso, taxa de perdas e outras não utilizadas diretamente neste trabalho.

Máquina EF2

```
#!/bin/bash
h=$1
ip=192.168.4.2
rt=13
sz=40
t=300
/usr/local/MGEN/mgen -b $ip:40000 -i eth0 -S $h -d $t -r $rt -s $sz -p 10000 &
/usr/local/MGEN/mgen -b $ip:40001 -i eth0 -S $h -d $t -r $rt -s $sz -p 10001 &
/usr/local/MGEN/mgen -b $ip:40002 -i eth0 -S $h -d $t -r $rt -s $sz -p 10002 &
/usr/local/MGEN/mgen -b $ip:40003 -i eth0 -S $h -d $t -r $rt -s $sz -p 10003 &
/usr/local/MGEN/mgen -b $ip:40004 -i eth0 -S $h -d $t -r $rt -s $sz -p 10004 &
```

Máquina EF1

```
#!/bin/bash
h=$1
ip=192.168.1.2
rt=13
sz=40
t=300
/usr/local/MGEN/mgen -b $ip:10200 -i eth0 -S $h -d $t -r $rt -s $sz -p 40200 &
/usr/local/MGEN/mgen -b $ip:10201 -i eth0 -S $h -d $t -r $rt -s $sz -p 40201 &
/usr/local/MGEN/mgen -b $ip:10202 -i eth0 -S $h -d $t -r $rt -s $sz -p 40202 &
/usr/local/MGEN/mgen -b $ip:10203 -i eth0 -S $h -d $t -r $rt -s $sz -p 40203 &
/usr/local/MGEN/mgen -b $ip:10204 -i eth0 -S $h -d $t -r $rt -s $sz -p 40204 &
```

Parâmetros do script fg-mgen

h = horário em que o programa mgen irá iniciar a geração de tráfego;
ip = número IP da máquina que irá receber o tráfego gerado;
rt = taxa de geração de pacotes por segundo;
sz = tamanho em bytes da carga do pacote = tamanho do pacote – o tamanho dos cabeçalhos IP e UDP; e
t = tempo que o mgen ficará gerando tráfego.

Tabela 13-2 - *Script* fg-mgen – geração do tráfego EF - executado em EF1 e EF2

```
#!/bin/bash
/usr/local/MGEN/mcalc $1
```

Tabela 13-3 – *Script* smcalc – processa os dados dos arquivos gerados pelo drec

13.3.2 Geração do tráfego BE-UDP em "*background*"

O tráfego BE é utilizado somente para congestionar o canal de comunicação. Tal como o tráfego EF, ele também é bidirecional. Na Tabela 13-4 é mostrado o script que é utilizado para invocar o programa drec para a recepção do tráfego. Na Tabela 13-5 é mostrado o script que invoca o programa mgen. Neste script os parâmetros rt1 (taxa de geração de pacotes) e sz1 (tamanho do pacote) são alterados para alterar as condições do tráfego em *background*. A Tabela 6-7 mostra todas as variações na taxa de pacotes e tamanhos que foram utilizados.

Máquina BE1
#!/bin/bash h=$1 fl=bebg$h t=3000 /usr/local/MGEN/drec -b 192.168.101.219 -i lec3 -S $h -d $t -p 60200-60202 $fl &
Máquina BE2
h=$1 fl=bebg$h t=3000 /usr/local/MGEN/drec -b 192.168.100.217 -i lec3 -S $h -d $t -p 50000-50002 $fl &

Tabela 13-4 - *Script* bg-drec – recepção do tráfego BE - executado em BE1 e BE2

Máquina BE2
#!/bin/bash h=$1 ip=192.168.101.219 rt1=6 sz1=1472 t=3000 /usr/local/MGEN/mgen -b $ip:50000 -i lec3 -S $h -d $t -r $rt1 -s $sz1 -p 60000 &
Máquina BE2
#!/bin/bash h=$1 ip=192.168.100.217 rt1=6 sz1=1472 t=3000 /usr/local/MGEN/mgen -b $ip:60200 -i lec3 -S $h -d $t -r $rt1 -s $sz1 -p 50200 &

Tabela 13-5 - *Script* bg-mgen – geração do tráfego BE - executado em BE1 e BE2

13.3.3 Geração do tráfego BE-TCP em "*background*"

/usr/local/netperf/netserver netserver

Tabela 13-6 – *Script* bg-netsrv – recepção do tráfego BE – executado em BE1 e Be2

#!/bin/bash h=$1 ip=192.168.101.219 t=300 rate = 32 fl=tcp$1 /usr/local/netperf/netperf -l $t -t TCP_RR -H $ip -- -r rate,rate >> $fl
#!/bin/bash h=$1 ip=192.168.100.217 t=300 fl=tcp$1 /usr/local/netperf/netperf -l $t -t TCP_RR -H $ip -- -r 32,32 >> $fl

Tabela 13-7 – *Script* bg-rate – geração do tráfego BE – executado em BE1 e Be2

```
#!/bin/bash
h=$1
ip=192.168.101.219
t=300
fl=tcpthp$1
/usr/local/netperf/netperf -l $t -H $ip -f k >> $fl
```

Tabela 13-8 - *Script* bg-thp – estimativa da vazão – executado em BE1 e Be2

13.4 Geração e medição do tráfego no ambiente CISCO

13.4.1 Geração e medição do tráfego EF

No ambiente CISCO o tráfego EF foi gerado e medido somente em um sentido. Os scripts fg-drec e o fg-mgen foram utilizados, respectivamente, para rodar o programa drec para recepção do tráfego e geração do arquivo de dados da medição, e o programa mgen para a geração do tráfego.

As tabelas abaixo contêm informações semelhantes às utilizadas no ambiente IBM, variando apenas os parâmetros referentes aos números IPs das estações de geração e recepção de tráfego, e as taxas de transmissão e recepção.

Máquina EF1

```
#!/bin/bash
h=$1
fl=ef$h
t=300
/usr/local/MGEN/drec -b 192.168.14.2 -i eth0 -S $h -d $t -p 40000-40004,50000-50002 $fl &
```

Tabela 13-9 –Script fg-drec – recepção do tráfego EF - executado em EF1

Máquina EF2

```
#!/bin/bash
h=$1
ip=192.168.11.2
rt=345
sz=40
t=300
/usr/local/MGEN/mgen -b $ip:40000 -i eth0 -S $h -d $t -r $rt -s $sz -p 10000 &
/usr/local/MGEN/mgen -b $ip:40001 -i eth0 -S $h -d $t -r $rt -s $sz -p 10001 &
/usr/local/MGEN/mgen -b $ip:40002 -i eth0 -S $h -d $t -r $rt -s $sz -p 10002 &
/usr/local/MGEN/mgen -b $ip:40003 -i eth0 -S $h -d $t -r $rt -s $sz -p 10003 &
 /usr/local/MGEN/mgen -b $ip:40004 -i eth0 -S $h -d $t -r $rt -s $sz -p 10004 &
```

Tabela 13-10 – Script fg-mgen – geração do tráfego EF - executado em EF2

13.4.2 Geração do tráfego UDP BE em "*background*" no ambiente CISCO

Máquina BE1

```
#!/bin/bash
h=$1
fl=be$h
t=300
/usr/local/MGEN/drec -b 192.168.151.2 -i eth0 -S $h -d $t -p 50000-50002 $fl &
```

Tabela 13-11 – Script bg-drec – recepção do tráfego BE - executado em BE1

Máquina BE2

```
#!/bin/bash
h=$1
ip=192.168.151.2
rt1=166
sz1=1472
t=300
/usr/local/MGEN/mgen -b $ip:60200 -i eth0 -S $h -d $t -r $rt1 -s $sz1 -p 50200 &
```

Tabela 13-12 – Script bg-mgen – geração do tráfego BE - executado em BE2

13.4.3 Geração do tráfego TCP BE em "*background*" no ambiente CISCO

```
#!/bin/bash
/usr/local/netperf/netserver netserver
```

Tabela 13-13 – Script bg-netsrv – recepção do tráfego BE – executado em BE1

```
#!/bin/bash
h=$1
ip=192.168.151.2
t=300
rt=12
fl=tcp$1
/usr/local/netperf/netperf -l $t -t TCP_RR -H $ip -- -r $rt,$rt >> $fl
```

Tabela 13-14 – Script bg-rate – geração do tráfego BE – executado em BE1

```
bg-thp
 #!/bin/bash
h=$1
ip=192.168.151.2
t=300
fl=tcpthp$1
/usr/local/netperf/netperf -l $t -H $ip -f k >> $fl
```

Tabela 13-15 – Script bg-thp – estimativa da vazão – executado em BE1 e Be2