

Qualidade de Serviço na Internet

Carlos Alberto Kamienski, Djamel Sadok

Universidade Federal de Pernambuco, Centro de Informática, Caixa Postal 7851,
Cidade Universitária, Recife/PE, 50732-9701
{cak, jamel}@cin.ufpe.br

Resumo

A Internet passou a ser uma realidade na vida de uma grande quantidade de pessoas ao redor do mundo. Pode-se verificar, no entanto, que o serviço proporcionado hoje em dia pela Internet não é adequado para atender à demanda de aplicações avançadas, como multimídia interativa, que os usuários desejam. Aplicações avançadas somente poderão ser oferecidas com a introdução de Qualidade de Serviço (QoS), tanto na Internet atual como na Internet2.

Abstract

The Internet is a reality in the life of a lot of people around the world. However, the kind of service provided by the current Internet is not suitable to cope with advanced application demands, as interactive multimedia. Advanced applications only will be provided with the introduction of Quality of Service (QoS), both in the current Internet and in the Internet2.

1 Introdução

Qualidade de Serviço (QoS) é a pedra fundamental necessária para transformar a Internet em uma infra-estrutura capaz de proporcionar vários tipos de serviços aos usuários. A Internet2 a elegeu como uma das suas prioridades. A comunidade acadêmica, comunidade Internet e fabricantes de equipamentos estão correndo a passos largos para disponibilizar o mais cedo possível soluções que viabilizem o oferecimento de vários níveis de serviços, onde QoS pode ser contratado e mensurado.

A Internet, que inicialmente era algo exótico, limitado ao mundo acadêmico, está proporcionando às pessoas acesso a informações e serviços antes não imagináveis. No processo de revolucionar as relações pessoais e comerciais nos próximos anos, ela está aos poucos deixando de ser uma curiosidade desajeitada para se tornar uma plataforma robusta e confiável. Para atingir esse objetivo, alguns obstáculos precisam ser vencidos e respondem pelos nomes de comércio eletrônico, segurança e Qualidade de Serviço (QoS).

Para a Internet evoluir para uma plataforma abrangente de serviços integrados, os usuários devem se sentir confortáveis ao utilizar suas aplicações, a qualquer hora do dia. Da empolgação inicial sentida pelos usuários quando do início da utilização da Web, à irritação manifestada hoje em dia, pode-se concluir que o usuário realmente precisa ter suas expectativas de QoS atendidas para que qualquer projeto de rede destinado a aplicações avançadas tenha sucesso.

Esse trabalho procura apresentar uma visão abrangente e didática da área. A sua elaboração foi feita de modo a tentar transmitir para o aluno o que é QoS, por que QoS é tão importante, como pode ser implementado e onde deve ser implementado.

Os capítulos foram organizados da seguinte maneira. O Capítulo 2 apresenta uma introdução genérica sobre o tema QoS em redes de computadores. Aspectos específicos sobre QoS na Internet são abordados no Capítulo 3. As principais abordagens para oferecer QoS na Internet são apresentadas no Capítulo 4. O Capítulo 5 aborda a importância de QoS no projeto da Internet2. O Capítulo 6 comenta alguns produtos comerciais existentes que implementam QoS, de empresas como Cisco Systems, Nortel Networks e 3Com. O Capítulo 7 apresenta o simulador de rede ns e alguns resultados obtidos simulando QoS. Finalmente, algumas considerações finais são apresentadas no Capítulo 8.

2 Qualidade de Serviço em Redes

Esse capítulo visa apresentar os conceitos básicos de QoS em redes de computadores (não especificamente na Internet), explorando a área de um ponto de vista mais abrangente.

2.1 Definição de Qualidade de Serviço

Qualidade de serviço (QoS) é um dos tópicos mais confusos e difíceis de definir em redes de computadores hoje em dia [24]. O problema é que, em geral, QoS assume significados diferentes para pessoas diferentes. Algumas definições são:

- *ISO*: Na visão da ISO, QoS é definida como o efeito coletivo do desempenho de um serviço, o qual determina o grau de satisfação de um usuário do serviço [27].
- *Sistemas Multimídia Distribuídos*: Em um sistema multimídia distribuído a qualidade de serviço pode ser definida como a representação do conjunto de características qualitativas e quantitativas de um sistema multimídia distribuído, necessário para alcançar a funcionalidade de uma aplicação [53].
- *Redes de Computadores*: QoS é utilizado para definir o desempenho de uma rede relativa às necessidades das aplicações, como também o conjunto de tecnologias que possibilita às redes oferecer garantias de desempenho [47]. Em um ambiente compartilhado de rede, QoS necessariamente está relacionada à reserva de recursos. QoS pode ser interpretada como um método para oferecer alguma forma de tratamento preferencial para determinada quantidade de tráfego da rede.

A junção dos termos qualidade e serviço pode dar margem a várias interpretações e definições diferentes. No entanto, existe um certo consenso, que aparece em praticamente todas as definições de QoS, que é a capacidade de diferenciar entre tráfego e tipos de serviços, para que o usuário possa tratar uma ou mais classes de tráfego diferente das demais. O modo como isso pode ser obtido e os mecanismos utilizados variam, dando origem a duas expressões frequentemente utilizadas [24], [21]: Classes de Serviço (CoS) diferenciados e a mais genérica e ambígua Qualidade de Serviço (QoS).

Algumas pessoas podem argumentar que os dois termos, QoS e CoS, são sinônimos, mas existem diferenças sutis. QoS tem uma conotação ampla e abrangente. CoS significa que serviços podem ser categorizados em classes, onde têm um tratamento diferenciado dos demais. O principal conceito em CoS é a diferenciação. QoS algumas vezes é utilizado em um sentido mais

específico, para designar serviços que oferecem garantias estritas com relação a determinados parâmetros (como largura de banda e atraso) a seus usuários. Podemos, então, classificar QoS de acordo com o nível de garantia oferecido:

- *QoS baseado em reserva de recursos, ou rígido*, que oferece garantias para cada fluxo individualmente (esse é o tipo de QoS apresentado acima).
- *QoS baseada em priorização, ou flexível*, onde as garantias são para grupos, ou agregações de fluxos. Nesse caso, cada fluxo individual não possui garantias. CoS utiliza esse conceito, que é mais fácil de implementar, por isso mais provável de ser disponibilizado em uma rede como a Internet em um futuro próximo.

Outro componente importante para a determinação do modelo de QoS a ser fornecido aos usuários diz respeito ao tipo de tráfego que as aplicações geram e qual o comportamento esperado da rede para que elas funcionem corretamente. Com relação ao tipo de tráfego as aplicações podem ser classificadas em [10], [23]:

- *Aplicações de tempo real (não elásticas)*: Podem ser definidas como aquelas com características rígidas de reprodução (*playback*), ou seja, um fluxo de dados é empacotado na fonte e transportado através da rede ao seu destino, onde é desempacotado e reproduzido pela aplicação receptora. Essa classificação pode ainda ser quebrada em duas categorias:
 - *Aplicações tolerantes*: São aquelas que mesmo diante de variações no atraso causadas pela rede, ainda assim produzem um sinal de qualidade quando reproduzidas.
 - *Aplicações intolerantes*: Variações no atraso produzem sinais de qualidade inaceitável.
- *Aplicações elásticas (não tempo real, ou adaptáveis)*: Para esse tipo de aplicação, a recepção correta dos dados é mais importante do que a sua apresentação em uma taxa constante. Exemplos de aplicações elásticas são correio eletrônico, transferência de arquivos, consultas interativas a informações e aplicações cliente/servidor tradicionais.

2.2 Força bruta contra gerenciamento

Uma questão fundamental sobre a oferta de QoS é decidir se o custo total de gerenciar os recursos da rede é menor do que o custo de adicionar mais largura de banda em locais de congestionamento [21]. Por trás disso está a constatação de que uma rede super dimensionada não apresenta problemas de congestionamento e conseqüentemente não necessita de QoS. A necessidade de mecanismos para garantias de QoS em redes de alto desempenho é um debate caloroso [54]. Uma opinião é que com as novas tecnologias a largura de banda se tornará tão abundante e barata que QoS será obtido automaticamente. Outra opinião diz que largura de banda não elimina a necessidade de QoS. Portanto, é necessário gerenciá-la.

Gerenciar a largura de banda e demais recursos da rede é uma tarefa extremamente complexa. Tratar a miríade de pedidos por tempo de resposta, variação no atraso e capacidade, levando em consideração dimensões de aplicação, usuário, hora do dia, congestionamento e tipo de enlace é uma tarefa tão complexa que pode se tornar mais barato instalar roteadores e/ou comutadores mais velozes e enlaces de maior capacidade em termos de largura de banda. O argumento a favor de usar grande quantidade de banda é bastante conhecido, é usar a força bruta contra a técnica, o conhecimento e o bom gerenciamento.

No entanto, muitas pessoas acreditam que o método da força bruta tende a ser ingênuo, porque ele sempre considera que todos os problemas da rede podem ser resolvidos com capacidade adicional. Existem várias situações onde essa suposição não pode ser comprovada.

Muitas pessoas acreditam que, não importa quanta banda houver, novas aplicações serão inventadas para consumi-la. Logo, serão necessários mecanismos para prover QoS [30].

2.3 Expectativas, possibilidades e limitações de QoS

A introdução de QoS está cercada de fantasias, comuns nesses casos de tecnologias inovadoras que representam mudanças de paradigmas, e que certamente irão alterar qualitativamente os serviços fornecidos pelas redes de computadores no futuro. Provavelmente, a principal causa disso é a pouca experiência com QoS em redes de computadores.

- *Imperfeições na rede*: QoS não é uma ferramenta para compensar imperfeições na rede, como a venda maior que os recursos disponíveis (*overbooking* ou *over-subscription*), situações drásticas de congestionamento e projeto mal feito.
- *Mágica na rede*: QoS não é mágica, ou seja, não faz milagres. Por exemplo, QoS não altera a velocidade da luz, não cria largura de banda inexistente e não cura redes com baixo desempenho generalizado.
- *A margem de QoS é pequena*: Os mecanismos de QoS procuram dar preferência para classes de tráfego pré-determinadas na alocação de recursos, quando eles estão sob contenção. Em situações onde os recursos possuem capacidade ociosa, a utilização de mecanismos de QoS é irrelevante.
- *Igualdade ou desigualdade*: QoS é intencionalmente elitista e injusta. Alguns usuários pagam mais caro e precisam sentir claramente que têm um serviço melhor que a maioria. O aumento dos recursos destinados a uma classe de serviços certamente diminui os recursos para as demais classes.
- *Tipos de tráfego*: QoS não funciona para todo tipo de tráfego, independente do tipo de QoS e do contrato estabelecido entre provedor e usuário.

2.4 Modelo de Classificação de QoS

Um modelo de QoS é útil para auxiliar a compreensão da sua abrangência e definir com precisão os requisitos específicos da aplicação desejada. Um modelo, definido em [11] e [47], divide conceitualmente as abordagens para QoS em três dimensões:

- *Escopo*: define os limites do serviço de QoS. Um escopo fim a fim é acessível para as aplicações nos sistemas finais. Já em um escopo intermediário, os sistemas finais não requisitam diretamente a QoS que necessitam, mas são atendidos por algum elemento de rede habilitado para tal tarefa.
- *Modelo de controle*: descreve características relacionadas ao gerenciamento das requisições (pedidos) de QoS. Essas características são:
 - *Granularidade*: um pedido pode ser para um único fluxo entre sistemas finais, ou então para uma agregação de fluxos de uma rede inteira.
 - *Duração*: as requisições de QoS podem variar muito com relação à duração dos níveis de QoS solicitados (minutos, horas, dias, semanas, meses).
 - *Local de controle*: independente do escopo de QoS, um pedido pode ser controlado pelo sistema final, ou por algum sistema intermediário (*proxy*).
- *Garantia de transmissão*: é a combinação de algumas das seguintes métricas [23]:
 - *Atraso*: É o tempo necessário para um pacote percorrer a rede, medido do momento em que é transmitido pelo emissor até ser recebido pelo receptor.

- ❑ *Variação do atraso (jitter)*: É a variação no atraso fim-a-fim.
- ❑ *Largura de banda*: É a taxa de transmissão de dados máxima que pode ser sustentada entre dois pontos. Geralmente é vista como uma característica do enlace físico. O termo *vazão (throughput)* é utilizado para designar a taxa máxima que alguma aplicação ou protocolo consegue manter em uma rede.
- ❑ *Confiabilidade*: está relacionada à perda de pacotes pela rede.

2.5 QoS e as tecnologias de transmissão

Algumas tecnologias de transmissão oferecem QoS, inclusive na camada de enlace de dados.

2.5.1 QoS em redes IEEE 802

QoS em redes locais é definida pelos padrões IEEE 802.1p/Q [26], incluídos no padrão 802.1D, que define especificações para a operação de pontes MAC. O 802.1Q foi projetado para oferecer uma maneira consistente de marcar quadros para determinada LAN virtual (VLAN) dentro de um domínio de camada 2. A priorização de encaminhamento dos quadros entre as VLANs é um pré-requisito para o 802.1Q e é obtida através dos bits de prioridade do 802.1p. Por isso, algumas vezes refere-se a 802.1Q englobando também o 802.1p. No entanto, se o interesse for apenas em priorização de tráfego, e não em VLANs, então os bits 802.1p podem ser utilizados independentemente, com informação nula para os bits 802.1Q.

Sob a perspectiva de QoS, o mais importante são os bits de prioridade do 802.1p, que oferecem mecanismos de diferenciação de tráfego dentro de redes locais. Como definem níveis de prioridade essas classificações geralmente só são importantes quando o dispositivo está enfrentando congestionamento. O administrador da rede deve classificar o tráfego da sua rede entre os oito níveis, para proporcionar garantias de QoS a determinadas aplicações.

2.5.2 QoS em redes Frame Relay

Com relação a QoS, Frame Relay oferece um mecanismo simples para garantir que o tráfego submetido em excesso por algumas fontes de dados não prejudique o encaminhamento do tráfego restante. Cada circuito virtual é configurado com um CIR (Committed Information Rate, taxa de informação comprometida), na interface entre usuário e rede Frame Relay, que continuamente verifica se o tráfego submetido está de acordo com o contrato estabelecido entre usuário e provedor de serviço. O CIR permite que tráfego em rajada, acima do perfil contratado, seja submetido à rede, mas todos os quadros detectados como fora do perfil são marcados como prioritários para descarte, através do bit DE (Discard Eligible) do seu cabeçalho. Em um situação de congestionamento, os comutadores Frame Relay descartam primeiramente aqueles quadros que possuem o bit DE com valor 1.

A marcação do bit DE é realizada pelos comutadores na borda da rede e os comutadores no interior da rede utilizam três níveis básicos de limiares (*thresholds*) para gerenciar congestionamento nas suas filas. No primeiro nível de limiar de fila, a rede começa a marcar os quadros com os bits de notificação explícita de congestionamento (ECN). No segundo nível, os comutadores descartam pacotes marcados como DE, honrando seu compromisso com o tráfego que está de acordo com o CIR. É a fase de recuperação de congestionamento. A premissa básica desse método é que a capacidade dos comutadores está suficientemente dimensionada para tratar todo o tráfego que estiver de acordo com a taxa de pico comprometida. Se essa ação não for suficiente para remover a causa do congestionamento, os comutadores podem então ultrapassar o

terceiro nível de limiar de fila, que é igual ao tamanho máximo da fila. Nesse caso, todos os quadros passam a ser descartados indiscriminadamente até o congestionamento diminuir.

2.5.3 QoS em redes ATM

ATM é uma tecnologia de transmissão de alta velocidade projetada para utilização tanto em LANs quanto WANs. É uma das poucas tecnologias atualmente que consegue obter velocidades de 622 Mbps. Por esse motivo ainda é muito utilizada como tecnologia de transmissão para segmentos de alta velocidade da Internet e da Internet2. Além disso, ATM define nativamente características e parâmetros para o oferecimento de QoS. Para explorar essas características, durante o estabelecimento da conexão um transmissor pode especificar qual a categoria de serviço ele deseja, como CBR (taxa constante de bits), rt-VBR (taxa variável de bits de tempo real), nrt-VBR (taxa variável de bits sem tempo real), ABR (taxa disponível de bits) e UBR (taxa não especificada de bits).

A complexidade, juntamente com o fato de não ser uma tecnologia usada fim a fim, leva a constatação de que ATM oferece várias características interessantes para redes avançadas multi-serviços, mas sua utilização atualmente se limita a explorar a velocidade oferecida. Como recentemente surgiram tecnologias para competir com ATM em velocidade, tanto em LANs (Gigabit Ethernet) como em WANs (IP sobre SONET ou WDM) há um questionamento muito grande dos reais benefícios em se implantar essa tecnologia.

2.6 Mecanismos de implementação de QoS

A implementação de QoS em redes de computadores está associada à existência de mecanismos de condicionamento de tráfego, políticas de filas (disciplinas de serviço), reserva de recursos e controle de admissão.

O condicionamento de tráfego está relacionado com o policiamento realizado para garantir que o tráfego entre usuário e provedor esteja dentro de perfis definidos em um contrato de serviço. O condicionamento envolve a classificação dos pacotes, medição do tráfego e uma subsequente ação, para os pacotes que não estão dentro do perfil de tráfego contratado. A classificação geralmente é realizada através da inspeção dos campos de cabeçalho do pacote/quadro, mas pode também se basear em porta de entrada ou saída, por exemplo.

Estando o tráfego classificado, ele deve ser medido de acordo com níveis pré-definidos em termos de largura de banda e rajada permitida. O principal mecanismo de implementação utilizado é o balde de fichas (*token bucket*), mostrado na Figura 1. Ele é definido por uma taxa de dados r e uma rajada b . A analogia é imaginar um balde com uma determinada capacidade máxima que contém fichas que são inseridas regularmente. Uma ficha corresponde à permissão para transmitir uma quantidade de bits. Quando chega um pacote, o seu tamanho é comparado com a quantidade de fichas no balde. Se existir uma quantidade suficiente de fichas, o pacote é enviado. Senão, geralmente é inserido em uma fila para que aguarde até haver fichas suficientes no balde. Isso é chamado de suavização ou moldagem de tráfego. Caso o tamanho da fila seja zero, todos os pacotes fora do perfil (que não encontram fichas suficientes) são descartados.

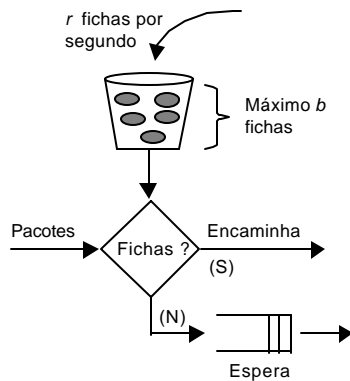


Figura 1 – Balde de fichas (token bucket)

Os mecanismos de filas são utilizados para escolher qual o próximo pacote a ser enviado em um determinado enlace. Entre alguns mecanismos de filas normalmente implementados em dispositivos de redes estão FIFO (DropTail), Fila com Prioridade, Circular (Round Robin) e Fila Justa com Pesos (WFQ). Em uma fila FIFO todos os pacotes são inseridos no final e retirados do início. Quando ela estiver cheia, os pacotes são descartados. A Fila com Prioridade (Figura 2a), na verdade é composta de várias filas, cada uma para um nível de prioridade, estabelecido após uma classificação dos pacotes. Primeiramente são encaminhados todos os pacotes da fila de maior prioridade, e então as outras filas são tratadas em ordem decrescente de nível de prioridade. Uma fila circular encaminha alternadamente pacotes de várias filas, geralmente associadas a Classes de Serviços. WFQ (Figura 2b) é uma espécie de fila circular que analisa fluxos individualmente e procura encaminhar os pacotes de todos de maneira a haver um compartilhamento justo do enlace. Os fluxos são agrupados em classes e a cada classe é atribuído um peso, que corresponde ao percentual do tempo do enlace destinado a ela.

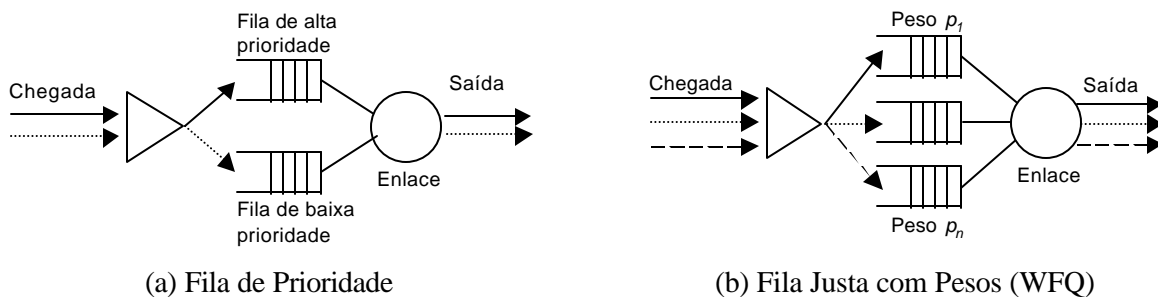


Figura 2 – Políticas de filas

3 Qualidade de Serviço na Internet

Esse capítulo apresenta o contexto onde se insere o tema QoS na Internet. Procura apresentar os motivos pelos quais a Internet não tem QoS hoje em dia e quais os desafios a serem vencidos.

3.1 Conceitos básicos dos protocolos TCP/IP

Por várias razões [46], o modelo OSI não se tornou um padrão de fato para fabricantes e usuários de produtos da área de redes. Essa função foi assumida pelo conjunto de protocolos TCP/IP, utilizado na Internet. Outras razões para sua adoção são simplicidade, em relação aos padrões da ISO e rapidez com que os padrões são criados. O nome TCP/IP diz respeito aos seus dois principais protocolos, o TCP (Transmission Control Protocol) e o IP (Internet Protocol). O termo genérico TCP/IP geralmente se refere a tudo que é relacionado com os protocolos TCP e IP [43]. Pode incluir outros protocolos, aplicações e mesmo o meio físico da rede. Um termo mais preciso seria “tecnologia TCP/IP”, ou mesmo “modelo TCP/IP” e “arquitetura TCP/IP”.

3.1.1 A arquitetura TCP/IP

Geralmente é aceito que a arquitetura TCP/IP possui quatro camadas: aplicação, transporte, inter-rede e interface de rede. A rigor os padrões TCP/IP somente são definidos a partir da camada de inter-rede. A camada de interface de rede não é efetivamente uma camada, mas apenas uma interface. Qualquer tecnologia de rede pode ser utilizada para a transmissão dos dados em uma rede TCP/IP, desde padrões mundialmente aceitos, até implementações proprietárias.

A camada de aplicação da arquitetura TCP/IP contém protocolos de alto nível, entre os quais o protocolo de terminal virtual (TELNET), o protocolo de transferência de hipertextos (HTTP), o protocolo de transferência de arquivos (FTP) e o protocolo de correio eletrônico (SMTP).

A camada de transporte fornece à camada de aplicação serviços para estabelecer comunicação entre as entidades dos protocolos de aplicação que desejam se comunicar nos sistemas finais (*hosts*). Dois protocolos fim a fim foram definidos na camada de transporte, o TCP, que é orientado a conexões e o UDP (User Datagram Protocol) que não é orientado a conexões. Alguns protocolos de aplicação utilizam o TCP e outros o UDP, dependendo do tipo de serviço que eles precisam.

A camada de inter-rede é a “cola” que une os protocolos de camadas superiores com as tecnologias de transmissão das camadas inferiores. Essa camada integra toda a arquitetura e sua tarefa é permitir que os sistemas finais injetem pacotes na rede e transmiti-los ao seu destino, independentemente do tipo de rede que existe abaixo dela. O protocolo que se responsabiliza por essa tarefa é o IP.

A camada de interface de rede, conforme já foi falado, apenas engloba as tecnologias de rede que podem ser utilizadas pelo protocolo IP para transmitir os pacotes. Como o protocolo IP faz poucas exigências da rede subjacente, basicamente qualquer rede pode ser utilizada para essa finalidade. Algumas tecnologias, como ATM e X.25, são baseadas em circuitos virtuais (o IP é baseado em datagramas) e já executam parte das funções dos protocolos TCP/IP.

3.1.2 O protocolo IP

O protocolo IP trabalha com o conceito de datagramas, ou seja, pacotes de dados transmitidos na rede através de um serviço sem conexão. Todos os datagramas carregam os endereço fonte e destino e são roteados independentemente através da rede. A estrutura de um datagrama IP pode ser dividida em duas partes: cabeçalho e dados¹. O cabeçalho tem uma parte fixa de 20 bytes e uma parte opcional de tamanho variável.

¹ Carga útil (*payload*) de dados transportada em um datagrama.

Os campos mais importantes relacionados a QoS são aqueles que identificam um fluxo e o campo que define o tipo de serviço que o pacote receberá. Não há um consenso geral sobre a definição de fluxo, mas uma definição bastante aceita identifica um fluxo pelo conjunto de 5 campos, sendo 3 campos do cabeçalho IP e dois campos do cabeçalho TCP ou UDP. Os campos do protocolo IP são *Source Address* (endereço de origem), *Destination Address* (endereço de destino) e Protocol (identifica o protocolo, geralmente TCP ou UDP). Os dois campos dos protocolos TCP e UDP que completam a definição de fluxo são porta de origem e de destino (portas são usadas para identificar aplicações). O campo *Type of Service*, foi originalmente concebido para oferecer diferentes tipos de serviços em redes TCP/IP.

3.1.3 Roteamento e encaminhamento

A principal função da camada de inter-redes é rotear pacotes da máquina de origem para a máquina de destino. O termo roteamento, no entanto, é utilizado para designar duas atividades distintas e independentes que ocorrem nos roteadores. A primeira é o estabelecimento dos melhores caminhos (rotas), os quais os pacotes devem seguir e pode ser consistentemente chamada de roteamento. A segunda é o processo de despachar cada pacote ao seu destino final ou a um próximo roteador, de acordo com informações existentes sobre as rotas. Esse processo é melhor definido como encaminhamento.

O estabelecimento das melhores rotas pode ser executado de modo estático ou dinâmico. Roteamento estático significa que alguém (uma pessoa) é responsável por manter essas informações atualizadas configurando manualmente os roteadores. As informações a respeito das rotas são mantidas pelos roteadores em tabelas de roteamento, onde cada linha identifica uma rede de destino (preferencialmente) ou sistema final. A tabela de roteamento contém basicamente a rede de destino (ou sistema final), a interface (placa de rede ou modem) de saída e o endereço IP do próximo roteador, se for o caso. A rede ou sistema final é identificado pelo endereço IP de destino presente nos pacotes.

3.2 Princípios da arquitetura Internet

Uma das realizações mais notáveis da Internet não é necessariamente o que ela é capaz de fazer hoje, mas o fato de ter assumido as dimensões atuais, comparada aos seus propósitos iniciais. Ela iniciou com objetivos bem modestos, não foi projetada para ser utilizada por milhões de pessoas no mundo inteiro. Com toda certeza, o conjunto de princípios que balizou o seu aparecimento e que hoje suporta a sua evolução é o grande responsável por isso. Na verdade, esses princípios também não são imutáveis. “O princípio da mudança constante talvez seja o único princípio da Internet que deveria sobreviver indefinidamente” [14]. Essa característica permite que grandes transformações se acomodem naturalmente na estrutura da Internet.

A tecnologia da Internet é baseada em um princípio, chamado de argumento fim a fim [40], que determina que toda a inteligência deve ser depositada nos sistemas finais e a rede deve executar tarefas muito simples. O argumento fim a fim sugere que as funções localizadas nos níveis inferiores de um sistema podem ser redundantes ou de pouco valor, quando comparadas com o custo de implementá-las nesse nível. Em geral, para serem completa e corretamente implementadas, as funções precisam do conhecimento e ajuda dos níveis superiores, que estão localizadas nos pontos finais de um sistema de comunicação. Algumas vezes, versões incompletas da função podem ser implementadas pelo sistema de comunicação para melhorar o desempenho. Esse caso pode ser visto no controle de erros realizado por algumas

implementações de camada de enlace de dados. Com alguns meios de transmissão, como comunicação sem fio, é útil controlar os erros [46], mas a função está incompleta, pois não tem a dimensão fim a fim.

3.2.1 Os objetivos iniciais

O objetivo fundamental do projeto inicial da Internet foi desenvolver uma técnica efetiva para a utilização multiplexada das redes de computadores existentes [19]. Como esse objetivo tem uma interpretação muito ampla, uma lista mais detalhada de objetivos é útil para auxiliar a compreensão:

1. Sobrevivência: A comunicação deve continuar, independente da falha de roteadores ou redes inteiras.
2. Tipos de serviço: Deve suportar múltiplos tipos de serviços de comunicação.
3. Diversidade de redes: Deve acomodar uma grande diversidade de redes. Para isso, a única suposição que o protocolo IP faz sobre a rede subjacente é que ela seja capaz de transmitir os pacotes de um lado para outro.
4. Gerenciamento: Deve permitir o gerenciamento distribuído dos recursos da Internet.
5. Custos: A arquitetura Internet deve ter uma boa relação custo/desempenho.
6. Expansão: A inclusão de novos computadores deve ser feita facilmente.
7. Contabilidade: Os recursos utilizados devem poder ser contabilizados.

É importante compreender que esses objetivos estão em ordem de importância e uma rede completamente diferente surgiria se essa ordem fosse alterada. Como a rede foi concebida com para operar em um contexto militar, a sobrevivência foi encarada como o principal objetivo. Já a contabilidade não mereceu muita atenção e hoje em dia está sendo necessária, mas é dificultada pelas características da rede. Uma rede projetada principalmente para uso comercial, certamente trocaria de posição esses dois objetivos. Com toda certeza, as características da Internet atual se devem principalmente a uma forte influência dos três primeiros objetivos.

3.2.2 O Serviço de Melhor Esforço

O protocolo IP oferece um serviço sem conexão baseado em datagramas, que não garante a entrega dos datagramas a tempo, não garante que eles cheguem ao destino na ordem correta e nem mesmo garante que eles cheguem no destino. As características citadas anteriormente são importantes para compreender esse comportamento. Os roteadores fazem o melhor que podem, se esforçam ao máximo, mas não podem fazer garantias a respeito da entrega dos pacotes. Esse tipo de serviço sem conexão é conhecido como serviço de Melhor Esforço (*Best Effort*, BE).

No serviço de melhor esforço, a rede tenta encaminhar todos os pacotes o mais rápido possível, mas não pode fazer qualquer tipo de garantia quantitativa sobre a Qualidade de Serviço. Além disso, o tráfego de dados é por natureza imprevisível e em rajadas, de modo que surge o problema de congestionamento, pois não é economicamente viável prover a rede para satisfazer as demandas de pico [31]. No entanto, bons resultados podem ser obtidos com o serviço de melhor esforço, se políticas de gerenciamento de filas e técnicas de controle de congestionamento apropriadas forem utilizadas [13].

3.3 Controle de Congestionamento

Congestionamentos em redes de computadores são basicamente um problema de compartilhamento de recursos [56]. Eles ocorrem quando os sistemas finais inserem na rede uma

quantidade maior de pacotes do que ela é capaz de tratar. Na Internet, a ocorrência de congestionamentos é devido à natureza imprevisível e em rajadas do tráfego de dados e o serviço de melhor esforço não supõe nenhum tipo de controle de admissão nem reserva de recursos para limitar a influência desses fatores. São uma consequência natural dos princípios utilizados na arquitetura da Internet. Por serem inevitáveis, os fluxos podem se beneficiar se participarem ativamente do controle de congestionamentos.

Existem duas atividades distintas relacionadas ao controle ou gerenciamento de congestionamento [30], [31], [28]. A primeira é a prevenção de congestionamento que tenta detectar possíveis condições que levem a congestionamentos futuros e executar procedimentos para impedi-los. A segunda é a recuperação de congestionamento, que atua na rede quando um congestionamento já ocorreu para que ela volte ao seu estado normal.

Na Internet o controle de congestionamento é realizado fim a fim, na camada de transporte, mas somente pelo protocolo TCP. A taxa de transmissão de dados do protocolo TCP é controlada pelas condições da rede e por isso os fluxos TCP são chamados de “compreensivos” ou “responsáveis”, porque respondem positivamente às notificações de congestionamentos [Bra98]. O UDP, por outro lado, não realiza nenhum tipo de controle de congestionamento. Em face a congestionamentos, os fluxos UDP não diminuem a taxa de transmissão de dados, a não ser que as aplicações o façam [13]. Por isso, são chamados de “agressivos” ou “não compreensivos”. Como cerca de 90% dos pacotes na Internet pertencem a fluxos TCP [49], em geral os congestionamentos são resolvidos de maneira adequada, apesar de várias implementações TCP existentes estarem incorretas [38].

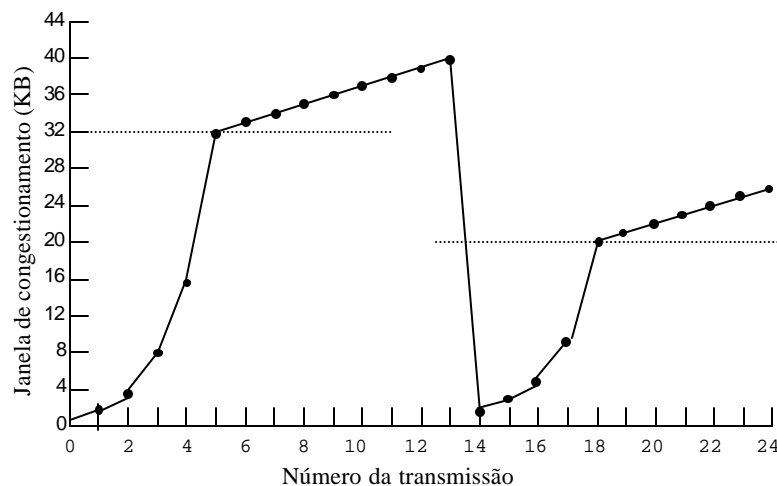


Figura 3 – Comportamento do controle de congestionamento do TCP

Os algoritmos de controle de congestionamento do protocolo TCP (que foram criados por Van Jacobson [28]), são padronizados pela RFC 1122 e são apresentados com mais detalhes na RFC 2581 [2]. São quatro os algoritmos utilizados pelo TCP: *slow start*, *congestion avoidance*, *fast retransmit* e *fast recovery*. O objetivo global deles é levar a rede a um estado estável de plena utilização, permitindo a introdução de um novo pacote à medida que outro pacote é retirado. Desse modo, os recursos na rede não são desperdiçados, ao mesmo tempo que os congestionamentos são evitados. Cada transmissor TCP fica o tempo todo monitorando a rede, tentando transmitir o máximo de segmentos possível.

O fato de o protocolo TCP diminuir sua taxa de transmissão quando detecta a perda de pacotes faz com que esse mecanismo exerça uma grande influência na obtenção das garantias de QoS estabelecidas, sobretudo com relação à largura de banda. As estratégias de implementação de QoS freqüentemente estabelecem uma taxa de dados máxima para que fluxos ou conjunto de fluxos possam transmitir. Caso os fluxos extrapolem essa taxa de pico, várias ações podem ser tomadas. Uma delas é descartar pacotes, o que leva fluxos TCP a diminuir sua janela de transmissão. Conseqüentemente, por um determinado período de tempo a taxa máxima permitida não é alcançada o que significa desperdício de recursos contratados.

3.4 A necessidade de Qualidade de Serviço na Internet

A Internet atual é um ambiente comercial que apresenta muitos desafios. Embora a demanda seja alta para uso empresarial e residencial, o seu modelo comercial apresenta problemas fundamentais. Os provedores de acesso à Internet (ISPs) vêm aumentando a capacidade de suas redes substancialmente ano a ano [37], mas enfrentam severas limitações em oferecer uma maior variedade de diferenciação nos serviços. Como resultado disso, eles têm obtido pouco retorno nos investimentos de ampliação da capacidade. Até o presente momento, a Internet pode ser descrita como uma rede de acesso [16], oferecendo conectividade entre quaisquer dois pontos. A diferenciação possível em termos de preço e qualidade está na largura de banda do enlace de acesso do usuário até o provedor.

Essas restrições aos provedores também interferem com os usuários, que não encontram serviços de maior valor agregado para comprar e geralmente ficam desapontados com a falta de Qualidade de Serviço inevitável. Por exemplo, embora aplicações de vídeo sejam possíveis na Internet, a qualidade das imagens impede a sua utilização para a maior parte dos usuários interessados. Por outro lado, dados de aplicações de missão crítica para as empresas competem em nível de igualdade com o tráfego residencial nos horários de pico. A causa disso é o modelo de serviço único (melhor esforço), que trata todos os pacotes com igualdade e não oferece garantias de transmissão.

Está se tornando cada vez mais visível, para usuários e provedores, que o modelo de serviço único e tarifação por largura de banda do canal de acesso tem que ser modificado para atender às novas demandas. Em um provedor de Internet típico, na maior parte do dia a rede fica subutilizada. Nas horas de pico, a demanda dos usuários costuma ser maior do que a largura de banda disponível, o que leva a um desempenho abaixo do esperado.

A simplicidade do protocolo IP é a causa do seu grande sucesso e espantosa escalabilidade, que deixa toda a complexidade para os sistemas finais. Com o tremendo crescimento da Internet nos últimos anos, as fraquezas do IP estão cada vez mais visíveis [45]. A ocorrência de congestionamentos nos roteadores torna atrasos e perdas de pacotes inevitáveis. Conforme mencionado anteriormente, tanto usuários quanto provedores querem romper com essa situação.

Tanto IP, quanto largura de banda são necessários, mas nenhum dos dois é suficiente para as necessidades de todas as aplicações sob todas as condições possíveis [45]. O modelo de melhor esforço não consegue sempre oferecer um serviço usável, que o torna inadequado para várias aplicações. Mesmo em redes com pouca carga, atrasos na entrega dos pacotes podem apresentar grandes variações, afetando negativamente aplicações com restrições de tempo real. Para oferecer garantias de serviço (algum tipo de confiabilidade quantificável), os serviços IP precisam ser suplementados. Para isso, é necessário adicionar algum tipo de inteligência (leia-se complexidade) à rede, para que ela possa diferenciar tráfego e possibilitar níveis diferentes de

serviços para usuários e aplicações distintos. Redes IP necessitam de mecanismos de gerenciamento ativo da largura de banda, ou em outras palavras, necessitam de QoS.

Ao proporcionar QoS, que essencialmente permite um usuário receber serviço melhor do que outro, cria-se um incentivo ao roubo. Como resultado, QoS necessita da aplicação de políticas, através de uma infra-estrutura de gerenciamento apropriada. Entretanto, não é possível aplicar políticas a menos que se possa identificar e confiar nos usuários da rede. Isso requer um infra-estrutura de autenticação. Adicionalmente, como QoS oferece serviços de valor agregado, a utilização deve ser cobrada, o que requer uma infra-estrutura de contabilização e cobrança.

Esses três serviços de suporte (Gerenciamento de Políticas, Autenticação e Contabilização/Cobrança) são essenciais para o sucesso de QoS. Todos apresentam desafios técnicos que estão sendo estudados e representam novas oportunidades de negócio e pesquisa que oferecem incentivos adicionais à viabilização de QoS na Internet.

4 Abordagens para QoS na Internet

Esse capítulo apresenta as cinco principais abordagens que estão sendo discutidas atualmente para o oferecimento de QoS na Internet e os relacionamentos que podem existir entre elas. Existe uma grande interesse acadêmico e comercial (fabricantes, provedores) nesse tema, mas o principal fórum de discussão está no âmbito da IETF (Internet Engineering Task Force), o órgão responsável pelas questões de engenharia de curto prazo na Internet.

4.1 Serviços Integrados (IntServ)

A Internet tradicionalmente oferece um único modelo de serviço, chamado de melhor esforço (Seção 3.2.2), que apresenta um desempenho razoável para aplicações elásticas, como transferências de arquivos e mensagens de correio eletrônico. Entretanto, à medida que nós avançamos em direção à era das comunicações multimídia, estão sendo desenvolvidas novas aplicações de tempo real com uma grande sensibilidade ao atraso da rede. Para essas aplicações o modelo de melhor esforço é totalmente inadequado, mesmo em redes com cargas leves. Embora esse problema possa ser aliviado introduzindo o maior grau possível de adaptabilidade em certas aplicações, existe uma necessidade de garantias mais rígidas em termos de largura de banda, atraso e perda de pacotes.

Nesse contexto, a IETF criou o grupo de trabalho IntServ para viabilizar o surgimento de uma rede de serviços integrados. O termo serviços integrados é empregado para designar um modelo de serviços para a Internet que inclui o serviço de melhor esforço, serviços de tempo real e serviços de compartilhamento controlado de enlace [10]. Os objetivos iniciais do grupo IntServ são a criação de um modelo de serviços integrados e de um modelo de referência para implementação. Como resultado já foram produzidas várias RFCs e alguns dos tópicos mais importantes são abordados a seguir.

4.1.1 O Modelo de Referência para Implementação

O modelo visa estender a funcionalidade básica dos roteadores para habilitá-los a participar de uma rede de serviços integrados. Ele inclui quatro componentes: o escalonador de pacotes, a rotina de controle de admissão, o classificador e o protocolo de reserva de recursos. Em princípio, a reserva de recursos pode ser executada por qualquer protocolo que seja compatível com o

modelo, mas na prática o protocolo RSVP [12] é o padrão de fato, tanto que se refere com frequência à arquitetura IntServ/RSVP. Devido à sua importância, o RSVP é apresentado na Seção 4.1.4 e os demais componentes são apresentados a seguir:

- *Escalonador de pacotes*: gerencia o encaminhamento dos vários fluxos de dados, usando alguma política de filas (Seção 2.6) e possivelmente também outro tipo de mecanismo. O escalonador deve ser implementado no local onde os pacotes são enfileirados e deve haver uma comunicação com a interface da camada de enlace de dados para controlar a alocação da largura de banda entre os fluxos. Outro componente importante que pode ser considerado parte do escalonador de pacotes é o *avaliador*, que mede características de tráfego dos fluxos para auxiliar o escalonamento de pacotes e o controle de admissão.
- *Classificador*: mapeia pacotes que chegam em determinadas classes, onde todos os pacotes em uma classe recebem o mesmo tratamento. Classe aqui é uma abstração e cada roteador pode mapear um mesmo pacote para uma classe diferente. Geralmente corresponde a um fluxo específico.
- *Controle de admissão*: implementa o algoritmo que um roteador usa para determinar se um novo fluxo pode ter seu pedido de QoS atendido sem interferir nas garantias feitas anteriormente. É algo semelhante ao que ocorre no sistema telefônico, onde nós ouvimos um “sinal de ocupado” quando o sistema não tem recursos disponíveis para atender a chamada que está sendo feita. Nesse caso, significa que alguns fluxos podem ter seus pedidos de recursos rejeitados por falta de recursos em algum dos roteadores.

4.1.2 O Serviço de QoS Garantido

O Serviço Garantido [41] é uma classe de QoS proporcionado pelo modelo de serviços integrados que oferece um nível assegurado de largura de banda, um limite rígido de atraso fim a fim e uma proteção contra a perda de pacotes nas filas, para os pacotes que estiverem obedecendo o perfil de tráfego contratado. É direcionado para aplicações com requisitos rígidos de tempo real, como certas aplicações multimídia intolerantes (Seção 2.1), que precisam de uma garantia firme de que um pacote não irá chegar no destino depois de um tempo maior que um limite especificado. Esse serviço não oferece garantia mínima da variação do atraso, ele simplesmente garante um atraso máximo gerado pelas filas.

A obtenção de um limite máximo para o atraso exige que todos os roteadores no caminho suportem o serviço garantido. O comportamento fim a fim oferecido por uma série de roteadores que implementam o serviço garantido é um nível assegurado de largura de banda para um determinado fluxo que, quando utilizado por um fluxo que está sendo policiado, produz um serviço com atraso limitado para todos os pacotes que estejam dentro do perfil.

Para ter acesso a esse serviço, as aplicações descrevem os seus fluxos através de um balde de fichas (Seção 2.6) e a partir dos valores de taxa e rajada, cada roteador calcula vários parâmetros descrevendo como ele tem que tratar os pacotes desses fluxos. Combinando os parâmetros dos vários roteadores em um caminho, é possível calcular o atraso máximo que um pacote irá experimentar quando transmitido por aquele caminho. Uma vez que as aplicações podem controlar os valores de taxa e rajada dos fluxos, elas conseguem obter uma garantia provada matematicamente sobre o atraso máximo dos seus pacotes.

O serviço garantido necessita de controle de admissão para operar de acordo com as especificações. Teoricamente, ele pode ser utilizado com qualquer protocolo de reserva de recursos, mas apenas para a sua utilização em conjunto com o RSVP foi especificada.

4.1.3 O Serviço de Carga Controlada

O Serviço de Carga Controlada [54] não oferece garantias quantitativas rígidas, como o Serviço Garantido. O comportamento fim a fim oferecido para uma aplicação por uma série de roteadores que implementa esse serviço se assemelha ao comportamento visto por aplicações que estão recebendo o serviço de melhor esforço em uma rede apenas levemente carregada (ou seja, sem nenhuma situação grave de congestionamento). As garantias que as aplicações têm são:

- Um percentual muito alto de pacotes transmitidos chegarão com sucesso no receptor (deve se aproximar da taxa básica de erros do meio de transmissão, ou seja, pouquíssimos descartes em filas são permitidos).
- O atraso sofrido por um alto percentual dos pacotes não deverá exceder muito o atraso mínimo sofrido por um pacote dentro de um fluxo. Ou seja, a maior parte dos pacotes deve ter um atraso muito próximo do atraso mínimo.

Para assegurar que essas condições serão válidas, aplicações que requisitam o serviço de carga controlada devem fornecer aos roteadores uma estimativa do tráfego de dados que elas irão gerar, chamada de TSpec, que é baseada em um balde de fichas. Como resposta, o serviço assegura que a aplicação terá a sua disposição recursos dos roteadores suficientes para processar adequadamente todos os pacotes que estiverem de acordo com a especificação contida no TSpec. Por outro lado, pacotes introduzidos na rede fora das especificações, poderão ser descartados, ou enfrentar um atraso mais significativo.

O objetivo do serviço de carga controlada é suportar um ampla classe de aplicações que tem sido desenvolvidas para a Internet atual, mas que não funcionam em situações de carga alta na rede. Alguns membros dessa classe são as aplicações de tempo real adaptáveis, atualmente sendo oferecidas inclusive comercialmente. Essas aplicações têm mostrado que funcionam bem com redes com carga leve, mas a qualidade se degrada rapidamente em condições de congestionamento. Um serviço que imita redes com carga leve é útil para essas aplicações.

As aplicações podem solicitar o serviço de carga controlada antes de iniciar as transmissões, ou então somente quando elas detectam que o serviço de melhor esforço não está oferecendo um desempenho aceitável. A primeira estratégia oferece uma maior garantia de que o nível de QoS não irá mudar enquanto durar a sessão. A segunda estratégia é mais flexível e barata, pois o serviço com tarifação mais alta não é utilizado durante todo o tempo de duração da sessão.

4.1.4 O Protocolo RSVP

O RSVP (Resource Reservation Protocol) [12], é um protocolo desenvolvido para realizar reserva de recursos em uma rede de serviços integrados. O RSVP é utilizado por sistemas finais para requisitar à rede níveis específicos de QoS para as aplicações. Também é utilizado pelos roteadores para repassar as requisições de QoS para todos os outros roteadores que estiverem no caminho entre fonte e destino e para estabelecer e manter informações de estado que possibilitam oferecer o serviço desejado. As requisições RSVP geralmente terão como resultado a reserva de recursos feita em todos os roteadores no caminho dos dados.

Algumas características importantes do protocolo RSVP são:

- O RSVP faz reservas para aplicações tanto de unidifusão como para multidifusão, se adaptando dinamicamente às alterações dos membros de um grupo ou de rotas.
- O RSVP é simplex, ou seja, faz reservas somente para fluxos unidirecionais. Para obter reservas duplex, deve-se solicitar duas reservas simplex distintas nos dois sentidos.
- No RSVP quem inicia e mantém reservas para os fluxos é o receptor dos dados.

- O estado das reservas no RSVP é “leve” (*soft-state*), ou seja, tem um tempo máximo de validade depois do qual ele expira. O receptor constantemente “refresca” o estado das reservas. Isso permite que ele se adapte automaticamente a alterações no roteamento.
- O RSVP não é um protocolo de roteamento. Ele usa as rotas escolhidas por qualquer protocolo de roteamento em uso atualmente ou que venha a ser utilizado no futuro.
- O RSVP transporta e mantém informações sobre o controle de tráfego e controle de políticas que são tratadas por outros módulos. O controle de tráfego, no caso, é exercido pelos outros módulos do IntServ.
- O RSVP oferece vários estilos de reservas, para se adaptar a uma grande variedade de aplicações e usos.
- Roteadores que não implementam RSVP podem estar presentes no caminho, que suas mensagens são encaminhadas transparentemente.
- O RSVP suporta tanto o IPv4 quanto o IPv6.

As duas mensagens mais importantes do protocolo RSVP são PATH, que é originado no transmissor e RESV, que é originado no receptor. Os principais objetivos da mensagem PATH são informar o receptor sobre as características de tráfego da requisição do transmissor e sobre o caminho fim a fim entre eles. Além disso, a mensagem PATH instala informações de roteamento reverso em todos os nós por onde passa, para que a mensagem RESV possa percorrer o mesmo caminho. PATH não faz a reserva, ela é feita pela mensagem RESV, enviado pelo receptor. As informações de roteamento reverso são necessárias porque é comum que a comunicação nos dois sentidos siga caminhos distintos. Sem essas informações, as reservas de recursos poderiam ser feitas em roteadores diferentes daqueles por onde os dados vão passar.

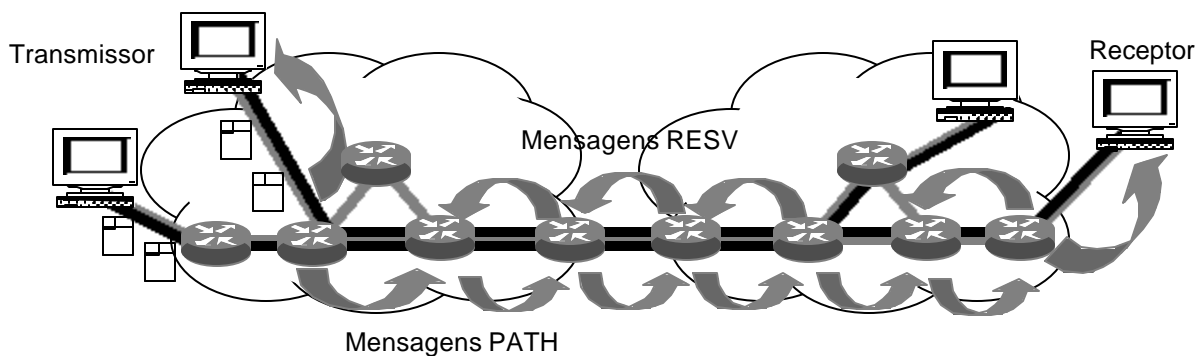


Figura 4 – Sinalização RSVP

Após receber uma mensagem PATH, um receptor envia uma mensagem RESV de volta ao último roteador solicitando uma reserva de recursos de acordo com os parâmetros especificados em PATH. Essa mensagem é reencaminhada para todos os roteadores no caminho, até chegar no transmissor. Cada roteador pode aceitar ou rejeitar a reserva de recursos solicitada, de acordo com a quantidade de recursos disponíveis e a política de controle de admissão adotada. Se a requisição é rejeitada, o roteador envia um mensagem de erro para o receptor e a sinalização é encerrada. Se a requisição é aceita, largura de banda do enlace e espaço em *buffers* são alocados para o fluxo e informações de estado relacionadas ao fluxo são instalados no roteador. A Figura 4 apresenta a sinalização realizada pelo protocolo RSVP.

4.1.5 Problemas com IntServ

O modelo de serviço formado por IntServ e RSVP atualmente é considerado como não sendo escalável para ser utilizado em uma rede de grande dimensão, como a Internet pública. Os principais problemas são [54]:

- A quantidade de informação de estado cresce proporcionalmente ao número de fluxos que um roteador tem que tratar. Isso impõe uma grande sobrecarga aos roteadores, em termos de capacidade de armazenamento e processamento considerando que roteadores de núcleo na Internet tratam simultaneamente milhares de fluxos.
- Para cada fluxo deve haver sinalização a cada nó (sistema final ou roteador). A troca de informações de sinalização é muito grande, inclusive porque o RSVP trabalha com estado leve, prejudicando a escalabilidade.
- As exigências para os roteadores são bastante altas. Todos têm que implementar RSVP, classificação, controle de admissão e escalonamento de pacotes.

4.2 Serviços Diferenciados (DiffServ)

Com base nas limitações encontradas no IntServ, foi proposta a Arquitetura de Serviços Diferenciados (DiffServ) que oferece QoS na Internet com escalabilidade: sem estado para cada fluxo e sinalização a cada nó. Escalabilidade pretende ser obtida através da agregação de fluxos em grandes conjuntos (chamados de BA, Behavior Aggregate), provisionamento de recursos para essas agregações (sem protocolo de reserva dinâmica de recursos) e separação das funções dos roteadores de borda e de núcleo. Roteadores de borda são aqueles que se comunicam com roteadores de outros domínios, enquanto que roteadores de centro somente se comunicam internamente. Redes que implementam DiffServ são chamadas Domínios DS e os roteadores habilitadas são chamados nós DS.

Apesar de ser escalável, DiffServ não oferece a garantia de recursos para todos os fluxos, como o IntServ. As reservas de recursos são feitas para agregações (BAs). Um fluxo individual pode não atingir as suas necessidades em termos dos parâmetros de QoS, como largura de banda e atraso. Esse tipo de QoS algumas vezes é chamado de Classes de Serviço (CoS). Nesses casos, garantias somente podem ser obtidas através do correto provisionamento dos recursos da rede.

4.2.1 Serviços e Contratos

Domínios DS negociam entre si contratos de serviço (SLAs – Service Level Agreements) que visam o oferecimento de garantias mínimas de QoS para as aplicações dos usuários. Todos os pacotes que fluem de um domínio para outro são fiscalizados (policiados) nos roteadores de borda para verificar sua conformidade com os contratos. No centro da rede, os roteadores simplesmente encaminham os pacotes para os seus destinos, oferecendo algumas garantias de QoS a determinados pacotes. Ou seja, pacotes distintos podem ter tratamentos distintos nos roteadores, para sua aderência a seus requisitos de QoS. Esse tratamento específico de encaminhamento é chamado de PHB (Per-Hop Behavior). Todos os pacotes que pertencem a um mesmo BA em um Domínio DS são tratados em todos os roteadores pelo mesmo PHB, que é identificado através do DSCP (DS Code Point), um código de bits inserido no campo TOS (agora renomeado para DS Field) do cabeçalho IP.

A arquitetura DiffServ define um serviço como o “tratamento global de um determinado subconjunto do tráfego de um usuário dentro de um Domínio DS, ou fim a fim”. Mas, embora

receba o nome de “serviços diferenciados”, o grupo de trabalho DiffServ do IETF não tem a intenção de padronizar serviços, mas os mecanismos que serão usados pelos provedores para oferecer os serviços aos usuários.

Em cada borda entre Domínios DS os aspectos técnicos e comerciais dos serviços oferecidos são definidos na forma de SLAs, que especifica as características gerais, o desempenho que o usuário para esperar desses serviços e formas de cobrança e tarifação. Como os serviços DiffServ são unidirecionais, as duas direções tem que ser tratadas separadamente em um SLA. O oferecimento de um serviços fim a fim é realizado através da concatenação de vários Domínios DS, onde os SLAs são negociados em cada uma das bordas entre os domínios existentes. A arquitetura lógica DiffServ, com os vários domínios e SLAs nas bordas é mostrada na Figura 5. Um domínio usuário de um serviço não estabelece um SLA direto com o domínio final do serviço, a não ser que haja uma ligação direta entre eles. Caso contrário, ele negocia com próximo Domínio DS no caminho e assim por diante até o domínio final.

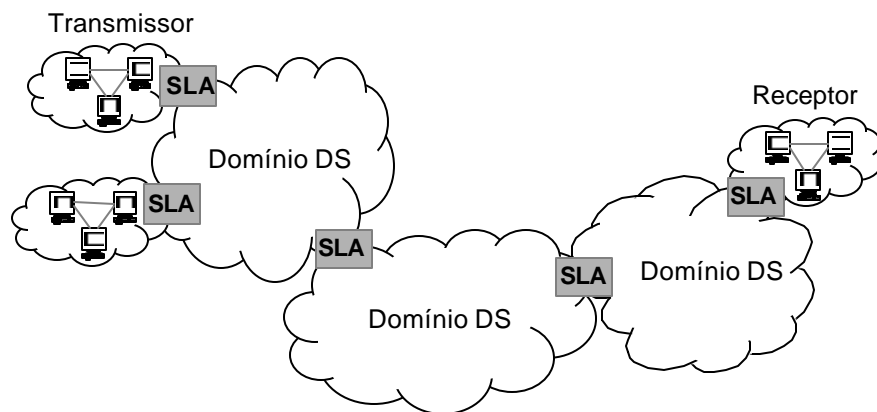


Figura 5 – Arquitetura lógica DiffServ

Uma parte importante do SLA é a especificação de condicionamento de tráfego, que define entre outras coisas alguns parâmetros detalhados do desempenho do serviço, como níveis esperados de vazão, atraso e perda de pacotes. Além disso, define perfis de tráfego, através de parâmetros de balde de fichas, que definem as características do tráfego como também as ações que podem ser tomadas caso o usuário não cumpra as especificações.

4.2.2 Condicionamento de Tráfego

As atividades referentes ao policiamento dos pacotes nos roteadores de borda para averiguar sua adequação ao perfil de tráfego contratado são coletivamente chamadas de condicionamento de tráfego. O condicionamento envolve a classificação dos pacotes, medição do tráfego e uma subsequente ação, dependendo da aderência dos pacotes ao perfil de tráfego contratado. A Figura 6 mostra os possíveis estágios de um elemento condicionador de tráfego.

O Classificador é o primeiro elemento envolvido no processo de condicionamento de tráfego. Ele seleciona os pacotes recebidos nas interfaces de entrada baseado no conteúdo de alguma parte do seu cabeçalho. Foram definidos dois tipos principais de classificadores. O Classificador BA (Behavior Aggregate) classifica os pacotes baseado somente no conteúdo do campo DSCP. Esse caso ocorre quando o domínio anterior é compatível com DiffServ e os pacotes já vêm marcados. Quando o domínio anterior não é habilitado para enviar os pacotes com

o campo DSCP previamente marcado, o classificador pode avaliar vários campos dos pacotes. Nesse caso, ele é chamado de Classificador MF (Multi-Field). Em ambos os casos, o resultado da classificação é o enquadramento do pacote em um BA válido no domínio e o seu encaminhamento para um processamento posterior. Por exemplo, se o classificador detectar que o pacote está usando o serviço de melhor esforço, ele provavelmente será encaminhado normalmente sem nenhum processamento adicional. Caso o pacote pertença a um BA para o qual foi definido um perfil de tráfego, ele é geralmente encaminhado para a fase de medição.

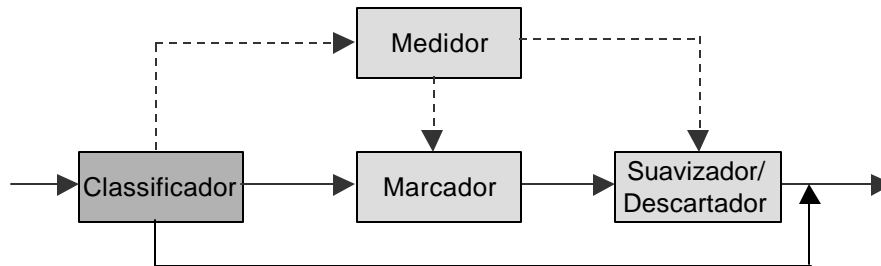


Figura 6 – Condicionador de tráfego

O Medidor de tráfego mede as propriedades temporais de um fluxo de pacotes selecionados pelo classificador de acordo com o perfil de tráfego especificado. Embora vários mecanismos de medição possam ser utilizados, o mais apropriado é o balde de fichas. O medidor então descobre quais pacotes estão dentro ou fora do perfil. Pacotes fora do perfil são aqueles que chegam quando não existem fichas suficientes no balde. Em termos mais genéricos, os conceitos de “dentro” e “fora” do perfil podem ser estendidos para múltiplos níveis de conformidade. Por exemplo, é possível definir um medidor com várias taxas e rajadas e então comparar os pacotes com esses valores para obter uma avaliação mais precisa das características do tráfego.

Com base no resultado da medição, os pacotes são encaminhados para um estágio onde uma ação de condicionamento é realizada. A ação depende do serviço oferecido, mas, em geral, pode ser suavização, descarte, marcação ou contabilização para posterior cobrança. Geralmente não é aplicada nenhuma ação em pacotes dentro do perfil, a não ser no caso do Classificador MF, após o qual os pacotes tem que ser marcados para um DSCP específico.

O Suavizador é um elemento que introduz um atraso nos pacotes fora do perfil até que o balde tenha fichas suficientes para encaminhá-lo. Ou seja, ele molda o tráfego para que forçosamente fique dentro do perfil contratado. Um suavizador geralmente implementa uma fila com tamanho limitado. Quando a fila está cheia, os pacotes subseqüentes são descartados.

O Descartador descarta pacotes que foram considerados fora do perfil pelo medidor, para que o fluxo seja considerado dentro do perfil. Esse processo é também chamado de policiamento do tráfego. Um descartador pode ser implementado como um caso especial de um suavizador, no qual o tamanho da fila é zero.

O Marcador é um componente totalmente necessário no caso de os pacotes serem classificados por um Classificador MF, para que os roteadores de núcleo posteriores possam classificar os pacotes com um Classificador BA. Ele é utilizado também quando os dois domínios utilizam valores do DSCP diferentes para o mesmo BA. Outra função é para rebaixar de classe pacotes fora do perfil.

Um Monitor é um elemento que pode ser utilizado para contabilizar a utilização para cobrança em caso de tráfego fora do perfil. O SLA pode prever que todo tráfego fora do perfil

será encaminhado, mas haverá uma taxa extra. Esse componente, no entanto, não é padronizado pela arquitetura DiffServ.

Em um Domínio DS, em geral o condicionamento de tráfego é necessário somente nos roteadores de borda. Como esses roteadores geralmente têm um volume de tráfego menor que os roteadores de núcleo, o impacto no desempenho não é significativo. Roteadores de núcleo, que recebem maior volume de tráfego, dedicam a maior parte dos seus recursos na atividade de encaminhar pacotes, de acordo com o seu PHB. A combinação da aplicação do PHB no centro da rede com o condicionamento de tráfego na borda, permite a criação de vários serviços.

4.2.3 BAs e PHBs

Um BA (Behavior Aggregate) é definido formalmente como “uma coleção de pacotes com o mesmo DSCP que estão cruzando um enlace em uma determinada direção em um Domínio DS” [9]. A quantidade de pacotes que pertencem a um determinado BA pode aumentar ou diminuir à nos vários roteadores, à medida que fluxos iniciam e terminam neles. Em uma analogia com o sistema de tráfego rodoviário, o conjunto de carros que trafega de um ponto a outro se altera conforme surgem novos cruzamentos onde vários carros entram e saem do caminho principal. A definição de BA é diferente da definição de serviço. BAs são blocos de construção técnicos para construir serviços fim a fim, que inclui regras, PHBs e configurações específicas. Os usuários vêem somente os serviços, não os BAs.

A implementação de um BA requer que todos os pacotes recebam o mesmo tratamento de encaminhamento (PHB) nos roteadores por onde passam. Um PHB é uma descrição de um comportamento de encaminhamento observável externamente de um roteador DS, aplicado a um determinado BA. O PHB é a maneira como um roteador aloca recursos para os BAs, e é em cima desse mecanismo local que serviços são construídos. A maneira mais simples de implementar um PHB é destinar a ele um determinado percentual de utilização da largura de banda de um enlace de saída.

Atualmente estão sendo padronizados dois tipos de PHBs: Encaminhamento Expresso (EF) [28] e Encaminhamento Assegurado (AF) [25]. Além desses, DiffServ deve ser compatível com as implementações e usos já existentes [35]. Foram definidos um PHB default, ou PHB BE (Best Effort), para o comportamento de encaminhamento de tráfego de melhor esforço e PHBs CSC (Class Selector Compliant) para compatibilidade com implementações existentes de IP Precedence, um padrão antigo para especificar precedência de pacotes IP.

O grupo de PHBs AF² pode ser utilizado por um Domínio DS provedor para oferecer níveis diferentes de garantias de encaminhamento para pacotes recebidos de um Domínio DS cliente. Foram definidas quatro classes AF, cada uma com três níveis de precedência para descarte, portanto ocupando doze códigos DSCP diferentes para sua implementação. Para cada uma das classes são alocados recursos nos roteadores, como largura de banda e *buffers*. Os pacotes são marcados para uma das quatro classes de acordo com o tratamento de encaminhamento desejado pelo cliente. O nível de precedência determina quais pacotes serão descartados primeiro pelos roteadores em caso de congestionamento. Uma boa maneira de marcar os pacotes para um determinado nível de descarte é no condicionamento de tráfego, de acordo com o resultado da medição. Dessa forma, em um roteador DS, o nível de garantia de encaminhamento de um pacote

² Atualmente, considera-se o AF como uma classe (de acordo com o conceito do paradigma de objetos) de grupos de PHB, onde cada um das quatro “classes” representa um instância com três PHBs, que são os níveis de precedência.

depende da quantidade de recursos alocados para a classe, a carga atual da classe AF e em caso de congestionamento, o nível de descarte do pacote.

A motivação para os PHBs AF é a demanda existente na Internet atualmente por encaminhamento assegurado de pacotes IP. Em uma aplicação típica, uma companhia usa a Internet para interconectar seus escritórios que estão geograficamente distribuídos e quer uma garantia de que os pacotes dentro dessa Intranet são encaminhados com alta probabilidade, se o tráfego agregado de cada escritório não excede o perfil contratado. Outro exemplo pode ser o de uma empresa que realiza vendas na Internet e que deseja que os pacotes de todos os usuários que a acessarem sejam encaminhados preferencialmente em relação ao tráfego de melhor esforço. O AF pode ser usado para implementar um serviço mais um menos semelhante ao serviço de carga controlada do IntServ, mas ele é muito mais flexível do que isso.

O PHB EF define garantias mais rígidas de QoS para aplicações muito sensíveis a variações de características temporais da rede. Ele pode ser utilizado para implementar um serviço com pouco atraso, pouca variação do atraso (*jitter*) e largura de banda garantida. Para os usuários, esse serviço, conhecido como Premium, parece com uma “linha privativa virtual”. O PHB EF é a opção DiffServ para encaminhar tráfego de aplicações multimídia e de tempo real.

Perda de pacotes, atrasos e variações no atraso ocorrem devido a existência de filas nos roteadores. Portanto, o PHB EF é definido como um tratamento de encaminhamento para uma agregação de fluxos DiffServ onde a taxa de saída dos pacotes de qualquer roteador DiffServ deve ser maior que a taxa de entrada. Isso evita a formação de filas e conseqüentemente a manutenção das garantias de QoS oferecidas por esse PHB. O tráfego EF deve receber essa taxa de saída independentemente da intensidade de qualquer outro tipo de tráfego (BE, CSC ou AF) em um determinado roteador. Em média, a taxa alcançada pelo tráfego EF deve ser no mínimo a taxa configurada, medida em qualquer escala de tempo maior que o tempo necessário para enviar um pacote. Se a taxa fosse calculada em intervalos de tempo maiores, a média poderia estar adequada, mas em certos momentos poderia atingir níveis inaceitáveis.

4.2.4 Provisionamento

O oferecimento de serviços consistentes por um Domínio DS depende da quantidade de recursos alocados para os PHBs nos roteadores e da quantidade real de tráfego que eles têm que tratar em cada PHB. No caso do PHB EF, a especificação do padrão estabelece que não deve ser submetido um volume de tráfego maior que a taxa de saída alocada para ele. Esse assunto é muito importante e traz algumas perguntas que não tiveram até o presente momento uma resposta satisfatória: Como provisionar os roteadores para tratar adequadamente o volume de tráfego direcionado aos vários PHBs que eles recebem ? Como garantir que o volume de tráfego submetido a um roteador não irá exceder a quantidade de recursos provisionada ?

Provisionamento se refere à determinação e alocação de recursos necessários nos vários pontos da rede. Provisionamento físico ocorre quando é necessária a inclusão ou remoção de recursos físicos nos roteadores. Provisionamento lógico opera através da modificação de parâmetros operacionais dentro de um equipamento físico para alterar o compartilhamento relativo dos recursos do equipamento entre os PHBs implementados. O provisionamento pode ser feito estaticamente, de acordo com padrões de tráfego preestabelecidos, ou pode se adaptar dinamicamente ao volume de tráfego efetivo em cada PHB.

A quantidade de tráfego aceita em um Domínio DS pode ser controlada facilmente nas bordas através de mecanismos de condicionamento de tráfego. Porém, não é tão óbvio o controle

da fusão e separação do tráfego entre os vários BAs à medida que os pacotes fluem através da rede. Ou seja, pode-se controlar o tráfego nas bordas, mas não é sempre possível saber a quantidade de tráfego destinada a um determinado PHB que irá chegar em um roteador de centro. Além disso, muitas redes fazem sub-provisionamento, ou seja, alocam uma quantidade menor de recursos a um PHB do que seria necessário para tratar todo o volume de tráfego contratado.

4.3 Multiprotocol Label Switching (MPLS)

Na Internet, quando um roteador recebe um pacote, ele faz uma busca na sua tabela de roteamento e então, baseado no endereço IP do pacote, decide para onde enviá-lo (Seção 3.1.3). Essa busca pode levar bastante tempo, dependendo do tamanho da tabela de cada roteador. MPLS (Multiprotocol Label Switching) [37] rompe com esse paradigma, usando um rótulo de tamanho fixo a partir do qual o roteador decide por onde enviar os pacotes. MPLS é na realidade a padronização de várias implementações existentes no mercado da técnica de encaminhamento baseado em rótulos. Essa forma de encaminhamento proporciona algumas vantagens em relação a maneira tradicional, como: a) melhor desempenho no encaminhamento de pacotes; b) criação de caminhos entre roteadores; e c) possibilidade de associar requisitos de QoS baseados no rótulo carregado pelos pacotes.

MPLS é um esquema de encaminhamento que opera entre as camadas de rede (camada 3) e de enlace de dados (camada 2) do modelo RM-OSI/ISO. Cada pacote MPLS tem um cabeçalho específico, que contém um rótulo de 20 bits, um campo indicando a Classe de Serviço de 3 bits, um indicador de pilha de rótulos de 1 bit e um campo TTL (Time to Live) de 8 bits. O cabeçalho MPLS é encapsulado entre o cabeçalho de camada de rede e o cabeçalho de camada de enlace de dados, ou então sobreposto em algum campo específico da camada de enlace de dados, como o campo VPI/VCI do ATM. Um roteador MPLS, chamado de LSR (Label Switching Router), examina somente o rótulo para encaminhar os pacotes. MPLS é chamado de multiprotocolo porque qualquer protocolo de rede pode ser utilizado, embora esteja padronizado por enquanto apenas o protocolo IP. Os caminhos que os pacotes percorrem de um roteador a outro são chamados de LSPs (Label Switching Paths). Na entrada de um domínio MPLS, o roteador insere o cabeçalho nos pacotes, que são encaminhados através dele até um roteador de saída, que remove o cabeçalho e encaminha o pacote para o próximo domínio.

4.3.1 Visão Geral

À medida que um pacote trafega em uma rede não orientada a conexões (como a Internet), cada roteador faz uma decisão de encaminhamento independente, que tem que ser repetida em todos os roteadores ao longo do caminho. Cada roteador escolhe qual o próximo salto (next hop) baseado na sua análise do cabeçalho do pacote e a sua tabela de roteamento local. Na realidade, o cabeçalho dos pacotes possui muito mais informações do que são necessárias para somente encontrar o próximo salto.

Para encontrar o próximo salto, na realidade são necessárias duas funções distintas, uma relacionada ao plano de controle (onde roda o protocolo de roteamento) e outra relacionada ao plano de encaminhamento (também chamado de caminho dos dados). A Figura 7 ilustra os planos de controle e de encaminhamento em um roteador. A primeira função divide o conjunto inteiro de pacotes possíveis em um conjunto de Classes de Equivalência de Encaminhamento (FECs, Forwarding Equivalence Classes). FEC é um nome genérico, pois MPLS não é específico para nenhum protocolo, mas em redes IP cada FEC pode ser vista como uma entrada na tabela de

roteamento. A segunda função mapeia cada FEC para algum determinado roteador que é o próximo salto. Todos os pacotes mapeados para uma FEC são iguais, com relação à decisão de encaminhamento, ou seja, todos os pacotes que pertencem a uma determinada FEC e que trafegam por um roteador seguirão pelo mesmo caminho.

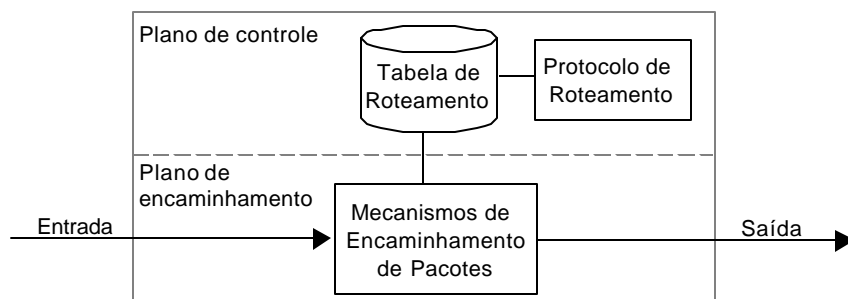


Figura 7 – Planos de controle e encaminhamento de um roteador

MPLS desvincula essas duas funções, atribuindo um pacote a uma FEC específica apenas uma vez, quando o pacote entra na rede. A informação sobre a FEC à qual um pacote pertence é então codificada como um rótulo que é inserido no pacote, conforme mencionado anteriormente. Nos roteadores subseqüentes o cabeçalho do pacote não é mais analisado e não há mais busca na tabela de roteamento. O rótulo é utilizado como um índice em uma tabela que especifica o próximo salto e um novo rótulo. A distribuição de rótulos não é global em um domínio, ela é local a um determinado par de roteadores. O roteador troca o rótulo antigo pelo rótulo novo e encaminha o pacote para o próximo salto.

MPLS apresenta algumas vantagens em relação ao encaminhamento IP tradicional:

- O encaminhamento MPLS pode ser feito por *switches* que conseguem fazer comutação baseada em rótulos, mas não podem analisar os cabeçalhos de rede, como o caso de *switches* ATM.
- O roteador de entrada pode utilizar informações que não estão disponíveis no cabeçalho IP, como a interface de entrada, para fazer o mapeamento entre FECs e rótulos. O encaminhamento IP convencional não pode fazer isso, porque os roteadores de núcleo não têm acesso a essa informação.
- Pacotes que entram na rede através de roteadores diferentes podem seguir caminhos distintos, porque a decisão de mapeamento de FECs para rótulos é local a cada roteador.
- O algoritmo que faz o mapeamento FEC/rótulo pode se tornar cada vez mais complexo, sem que isso tenha nenhum impacto no desempenho dos roteadores de núcleo.
- Como resultado do algoritmo de mapeamento, pode-se forçar um pacote a seguir uma rota diferente daquela que ele seguiria baseado no caminho mais curto, descoberta pelo protocolo de roteamento.
- MPLS permite a utilização de uma pilha de rótulos, que permite a criação de vários níveis de túneis dentro dos LSPs (caminhos MPLS).

4.3.2 Encaminhamento baseado em rótulos

O encaminhamento baseado em rótulos realizado pelo MPLS utiliza dois tipos de tabelas que fazem mapeamentos distintos, conforme ilustrado na Figura 8. Em ambas, cada entrada é chamada de NHLFE (Next Hop Label Forwarding Entry) e contém as seguintes informações:

- O roteador que é o próximo salto do pacote.
- Uma operação para ser realizado na pilha de rótulos do pacote, que pode ser no seu caso mais simples é a troca do rótulo antigo pelo rótulo novo.
- Outras informações relevantes, como os níveis de QoS dispensados ao pacote.

Quando um roteador recebe um pacote que está sem um rótulo, ele utiliza a tabela FTN (FEC-to-NHLFE) para mapear cada FEC para uma NHLFE. Quando o pacote chega no roteador com um rótulo, ele utiliza a ILM (Incoming Label Map), que encontra a NHLFE usando o rótulo como índice.

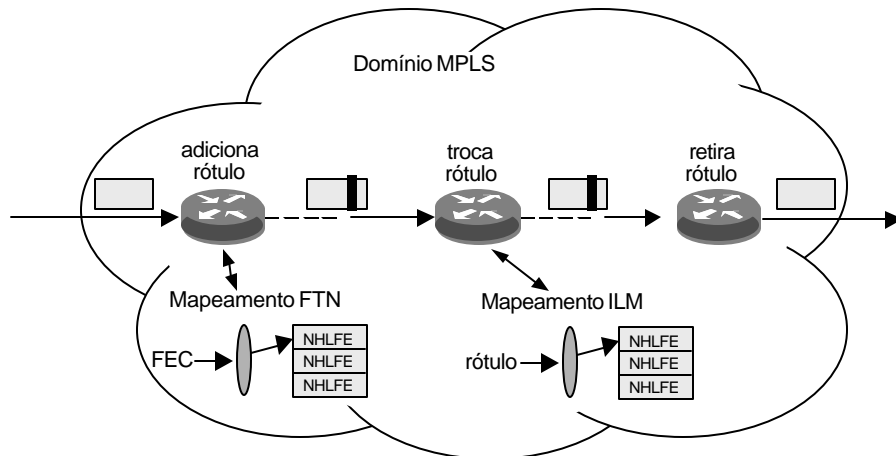


Figura 8 – Encaminhamento de pacotes em um domínio MPLS

O processo de usar a FTN e a ILM para encaminhar pacotes é conhecido como “troca de rótulos” (label swapping). Dependendo se o pacote vem rotulado ou não ele usa ou a ILM ou a FTN para fazer o mapeamento para uma NHLFE. Um LSR (roteador MPLS) sempre encontra o próximo salto a partir da NHLFE, mesmo que ele tenha a capacidade de realizar o encaminhamento IP convencional.

4.3.3 Aplicações de MPLS

Uma vantagem direta da utilização de MPLS é substituir o encaminhamento tradicional IP pelo encaminhamento baseado em rótulos, que é um processo consideravelmente mais rápido. Entretanto, somente isso não seria um motivo suficiente para a adoção de MPLS, uma vez que a tecnologia de roteadores de alta velocidade atual já permite fazer buscas muito rápidas na tabela de roteamento.

Uma das principais aplicações para MPLS hoje é a Engenharia de Tráfego, que será discutida na Seção 4.5. Ela permite alterar o caminho normal que alguns pacotes seguiriam caso fossem encaminhados pelo esquema convencional, ou seja, pelo caminho mais curto, escolhido pelo protocolo de roteamento. O MPLS consegue forçar pacotes a seguirem certas rotas preestabelecidas, o que é impossível no esquema convencional.

Outra aplicação para MPLS é a emulação redes orientadas a conexão, como Frame Relay ou ATM. Uma vez que MPLS é um mecanismo orientado a conexão, ele pode ser utilizado para emular qualquer serviço orientado a conexão não confiável com um LSP. Isso permite que uma rede integrada baseada em datagramas ofereça serviços legados aos seus usuários usando uma única infra-estrutura.

MPLS pode ser utilizado também para facilitar a integração de IP com ATM. A interligação de roteadores através de uma sub-rede ATM requer a configuração de vários circuitos virtuais, no pior caso $N(N-1) / 2$ circuitos virtuais, onde N é o número de roteadores. Usando roteadores MPLS e fazendo uma atualização dos *switches* ATM permite fácil integração entre ambas as tecnologias. *Switches* ATM podem se comportar como LSRs, fazendo o encaminhamento baseado em rótulos.

MPLS também permite facilmente a configuração de Redes Privadas Virtuais (VPNs). Empresas usam VPNs para criar túneis seguros entre matrizes e filiais ou entre parceiros comerciais. Normalmente esse tipo de comunicação utiliza linhas privadas, porque a Internet é considerada insegura para transportar informações confidenciais. Com MPLS pode-se criar uma VPN usando o serviço de emulação de Frame Relay, ou então configurando roteadores MPLS nas redes dos usuários para serem o início e o final de LSPs. Dentro dos LSPs a comunicação apresenta um alto nível de segurança.

4.4 Roteamento baseado em QoS (QoSR)

O roteamento utilizado atualmente na Internet é direcionado para conectividade e tipicamente suporta somente o serviço de melhor esforço. Os protocolos atuais de roteamento usados na Internet, como OSPF e RIP, procuram sempre encontrar o menor caminho, baseados em uma única métrica, como peso administrativo ou quantidade de saltos. Esses protocolos são “oportunistas”, sempre procuram encontrar o menor caminho, mesmo quando ele não é o mais adequado, ou a troca freqüente de um caminho para outro pode gerar instabilidade. Caminhos alternativos com custos aceitáveis, mas não ótimos, não podem ser utilizados para rotear tráfego. No máximo, alguns protocolos aceitam manter rotas com custos exatamente iguais e distribuir o tráfego entre elas.

Roteamento baseado em QoS (QoS Routing) [20] é um mecanismo de roteamento que seleciona o caminho percorrido pelos pacotes de um fluxo baseado no conhecimento da disponibilidade de recursos da rede, bem como nos requisitos de QoS dos fluxos, como largura de banda e atraso.

4.4.1 QoSR e Roteamento Baseado em Restrições

Roteamento Baseado em Restrições (Constraint-Based Routing) é o processo de computar rotas que são sujeitas a múltiplas restrições [54]. Seu desenvolvimento está evoluindo a partir de QoSR e QoSR pode ser considerado uma variação de Roteamento Baseado em Restrições, onde as restrições são requisitos de QoS. Outras restrições utilizadas podem ser custo monetário e políticas de segurança. Uma vez que o interesse desse trabalho está em QoS, a discussão será direcionada especificamente para QoSR.

QoSR deverá estender o paradigma de roteamento na Internet de três maneiras básicas. Em primeiro lugar, para suportar tráfego baseado em novos serviços, proporcionados por IntServ ou DiffServ, caminhos múltiplos entre roteadores devem ser encontrados, cada um com as suas características de QoS. Algumas desses serviços irão necessitar da distribuição de mais do que uma métrica, como largura de banda e atraso. Em segundo lugar, o roteamento oportunístico utilizado atualmente na Internet direciona o tráfego para uma nova rota tão logo que um caminho “melhor” seja encontrado. O tráfego é redirecionado do caminho antigo, mesmo que ele esteja apto a satisfazer as necessidades dos fluxos. Além de gerar grande instabilidade, aumento a variação do atraso dos fluxos, as escolhas de roteamento nem sempre são adequadas. Em terceiro

lugar, caminhos alternativos não são suportados, mesmo que possam atender às características de várias aplicações.

Por isso, QoS SR pode encontrar um caminho mais longo, mas muito menos sobrecarregado que o caminho mais curto, que geralmente é o mais congestionado. O tráfego na rede, dessa forma, pode ser distribuído mais igualmente.

4.4.2 QoS SR e Reserva de Recursos

É importante entender a diferença entre QoS SR e reserva de recursos. Protocolos de reserva de recursos, como o RSVP, oferecem um método para requisitar e reservar recursos da rede, mas eles não proporcionam nenhum mecanismo para encontrar um caminho que tenha recursos suficientes para satisfazer os níveis de QoS requisitados. Por outro lado, QoS SR permite a determinação de um caminho com uma grande chance de acomodar a requisição de QoS, mas não inclui um mecanismo para reservar os recursos necessários.

Conseqüentemente, as duas técnicas são complementares e geralmente implementadas em conjunto. Essa combinação permite exercer um controle significativo sobre rotas e recursos, ao custo de informações adicionais de estado e tempo de configuração. Por exemplo, um protocolo como o RSVP pode ser utilizado para disparar certas computações pelo mecanismo QoS SR que irão atender às necessidades específicas do fluxo.

4.4.3 Objetivos de QoS SR

Uma das grandes diferenças entre QoS SR e o roteamento convencional é a manutenção de estado sobre a capacidade dos recursos da rede em atender requisitos de QoS. Os seus principais objetivos são:

- Determinação dinâmica de possíveis caminhos: Embora QoS SR possa encontrar um caminho que atenda os requisitos de QoS de um fluxo, o direcionamento do tráfego para ele pode depender de outras restrições (Roteamento Baseado em Restrições).
- Otimização da utilização dos recursos: Um esquema de QoS SR pode auxiliar na utilização eficiente dos recursos da rede, aumentando a vazão total alcançada pela rede. Caminhos ociosos podem ser encontrados para satisfazer demandas por requisitos específicos de QoS, o que é impossível com o roteamento convencional. Isso pode ser usado para realizar Engenharia de Tráfego.
- Degradação graciosa de desempenho: O roteamento dependente de estado pode compensar problemas transientes na rede, escolhendo caminhos alternativos, que permitem que as aplicações melhor se adaptem as condições momentâneas da rede.

4.4.4 Custo de QoS SR

Calcular rotas com base em restrições de QoS é um processo mais caro que atual paradigma de roteamento da Internet. A questão é saber o ponto ótimo onde a melhoria em desempenho pela adoção de QoS SR vale a pena comparado com a aumento nos custos. O custo adicional gerado pelo QoS SR tem dois componentes principais [3]: custo computacional e sobrecarga de protocolo.

O custo computacional é devido ao algoritmo mais sofisticado para escolha dos caminhos e à necessidade de processá-lo mais frequentemente. Dependendo da quantidade e do tipo de métricas que são utilizadas para o cálculo das rotas, o algoritmo pode se tornar NP completo [54]. Em geral, existem soluções polinomiais que envolvem o uso de largura de banda e alguma outra

métrica (atraso, variação do atraso, confiabilidade), mas assim mesmo o processamento é complexo. No entanto, os avanços tecnológicos permitem que se diminua a importância do custo computacional pela utilização de processadores mais velozes e memórias maiores.

A sobrecarga de protocolo ocorre devido à necessidade de distribuir atualizações sobre o estado dos recursos da rede entre os roteadores envolvidos no processamento das rotas. Essas atualizações se traduzem em aumento do tráfego e processamento na rede. Conforme a quantidade de informações transmitidas e a frequência com que isso é feito, essa distribuição das atualizações pode influenciar negativamente vários outros aspectos, como largura de banda e espaço de armazenamento. Então, o custo adicional proveniente da sobrecarga de protocolo é mais difícil de ser tratado e representa um empecilho maior para a plena utilização de QoS.

O custo computacional e a sobrecarga de protocolo também têm uma relação direta entre eles. Quanto mais informações forem utilizadas e maior a frequência das atualizações, maior será a necessidade de processamento para manter as rotas atualizadas. Por outro lado, se as atualizações forem muito infrequentes, é possível que os valores não representem a realidade e induzam à escolha de rotas inadequadas. Por isso, várias propostas têm sido apresentadas, no sentido de limitar a frequência das atualizações e o custo computacional, possibilitando a escolha de rotas de tal maneira que permita a obtenção de benefícios individuais para os fluxos, bem como uma melhor utilização global da rede.

4.5 Engenharia de Tráfego (TE)

Engenharia de Tráfego (Traffic Engineering - TE) é o processo de arranjar como o tráfego flui através da rede para que congestionamentos causados pela utilização desigual da rede possam ser evitados. A Engenharia de Tráfego é direcionada à otimização de desempenho de redes operacionais. Em geral, ela engloba a aplicação de princípios tecnológicos e científicos para medir, modelar, caracterizar e controlar o tráfego na Internet e a aplicação dessas técnicas e conhecimentos para atingir determinados objetivos de desempenho [6].

Um objetivo central da Engenharia de Tráfego na Internet é facilitar a operação eficiente e confiável da rede enquanto que ao mesmo tempo otimiza a sua utilização e desempenho. A Engenharia de Tráfego já é atualmente uma função indispensável em grandes redes por causa do custo alto dos equipamentos e da natureza comercial e competitiva da Internet. Como altera o fluxo normal dos pacotes, ela pode ser utilizada para atender a requisitos de QoS de determinados fluxos de dados.

Engenharia de Tráfego é um processo, que pode ser implementado através de diversos mecanismos, como configuração manual, utilização de características específicas das tecnologias de transmissão de camada de enlace de dados, determinação de rotas adequadas através de QoS e fixação de rotas com MPLS. Além disso, pode-se realizar Engenharia de Tráfego para uma rede convencional que oferece o serviço de melhor esforço, ou para redes que oferecem níveis de QoS, como IntServ/RSVP ou DiffServ.

4.5.1 Problemas com os Protocolos de Roteamento

Engenharia de Tráfego é algo necessário na Internet principalmente porque os protocolos de roteamento interno (IGP, Interior Gateway Protocol), usam sempre o menor caminho para encaminhar o tráfego e isso contribui significativamente para aumentar os problemas de congestionamento ocorridos dentro de Sistemas Autônomos: Esses protocolos (ex.: OSPF ou RIP) são orientados à topologia da rede e usam como métrica a quantidade de saltos ou o peso

administrativo (Esse problema já foi discutido na Seção 4.4). Fatores como a largura de banda disponível e as características do tráfego não são levados em consideração nas decisões de roteamento. Conseqüentemente, sempre irá ocorrer congestionamento, quando:

- O caminho mais curto de várias fontes de dados converge para alguns enlaces específicos.
- O tráfego de uma determinada fonte de dados é roteado através de um enlace que não tem suficiente largura de banda para encaminhá-lo adequadamente.

Esse tipo de cenário se manifesta mesmo quando existem caminhos alternativos com capacidade ociosa suficiente para encaminhar o tráfego excedente. Ou seja, a utilização dos protocolos de roteamento baseados no menor caminho tende a degradar o desempenho observado pelos fluxos de dados, mesmo quando existem recursos suficientes para tratar todo o tráfego.

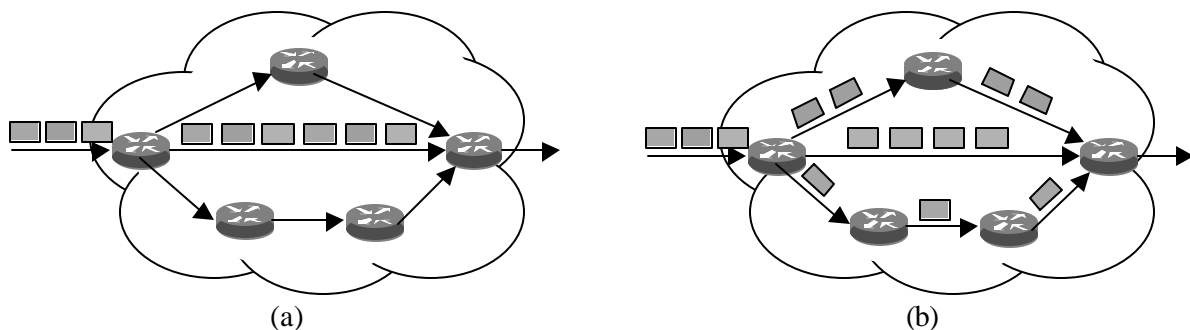


Figura 9 – Encaminhamento de pacotes; a) sem TE; b) com TE

A Figura 9 ilustra o tratamento que a TE pode dar a certos tipos de tráfego, encaminhando pacotes por caminhos diferentes, dependendo das políticas adotadas. Em um domínio sem TE, todos os pacotes devem ser encaminhados pelo caminho mais curto, no caso, o caminho do meio.

4.5.2 Objetivos de Desempenho

Otimizar o desempenho de redes operacionais envolve objetivos orientados ao tráfego e a recursos [5]. Os objetivos de desempenho orientados ao tráfego incluem os aspectos relacionados à melhoria dos níveis de QoS oferecidos aos fluxos de dados. Na Internet atual, com o modelo de serviço de melhor esforço, esses objetivos incluem: minimização da perda de pacotes (o mais importante), minimização do atraso e maximização da vazão. Em uma rede de serviços diferenciados, com várias classes de serviços que necessitam limite máximo e mínimos para certas métricas de QoS, os objetivos orientados ao tráfego assumem uma importância ainda maior. Principalmente, porque em última análise o que mais importa é como os usuários da rede sentem o desempenho dos serviços utilizados. Em uma rede de melhor esforço, a noção de desempenho assume critérios muito subjetivos para o usuário. Em uma rede que oferece níveis de QoS, ele tem como mensurar e exigir o desempenho contratado.

Os objetivos orientados a recursos incluem aspectos relacionados à otimização da utilização dos recursos da rede. O gerenciamento eficiente dos recursos é a melhor maneira de alcançar esses objetivos. Mais especificamente, é importante garantir que os recursos de alguns segmentos da rede não fiquem superutilizados e congestionados, enquanto que outros segmentos com caminhos alternativos para o tráfego tem recursos ociosos. A largura de banda é o principal recursos nas redes atuais. Portanto, uma das funções principais da Engenharia de Tráfego é

gerenciar eficientemente os recursos de largura de banda. Existe uma discussão sobre o valor desse tipo de interferência no encaminhamento de pacotes na rede, uma vez que as modernas tecnologias estão oferecendo cada vez mais largura de banda a um custo menor (veja discussão na Seção 2.2). No entanto, até o presente momento, a solução com o melhor custo/desempenho para grandes redes e realizar alguma forma de Engenharia de Tráfego.

4.5.3 Estilos de Engenharia de Tráfego

Existem várias escolhas que podem ser feitas para a realização da TE, que definem o estilo que está sendo adotado. Uma classificação de algumas das possibilidades existentes inclui:

- TE dependente de tempo ou de estado: Na TE dependente de tempo, informações históricas baseadas em variações sazonais são utilizadas para pré-programar planos de roteamento. Nesse estilo não há interferências na rede para que ela se adapte a variações aleatórias nos padrões de tráfego ou alteração das condições da rede. Na TE dependente de estado, ou adaptável, os planos de roteamento são adaptados para representar condições atuais da rede.
- TE *online* ou *offline*: Os planos de roteamento necessários para a realização da Engenharia de Tráfego podem ser computados *online* ou *offline*. Tipicamente, quando a Engenharia de Tráfego é realizada com informações passadas a computação pode ser feita *offline*. Esse estilo permite a utilização de algoritmos mais complexos e processamento mais demorado. Quando é necessário que o roteamento se adapte às condições atuais da rede, é necessária a TE *online*.
- TE centralizada ou distribuída: No caso de TE com controle centralizado, existe uma autoridade central que coleta todas as informações, calcula todos os planos de roteamento e então distribui para todos os roteadores. No caso distribuído, a seleção de rotas é executada por cada roteador de maneira autônoma, baseado nas condições atuais da rede.
- TE com informações globais ou locais: O algoritmo de TE pode precisar de informações globais, de toda a rede onde está sendo realizada a TE, ou informações locais, somente de uma parte dela. Informações locais do estado dos recursos pode ser suficiente quando se está utilizando TE distribuída.
- TE prescritiva ou descritiva: Os resultados da TE podem recomendar ações a serem realizadas, ou seja, prescrever soluções. Alternativamente, pode somente descrever os problemas, sem apontar soluções específicas. As informações podem servir como base para que administradores de rede façam intervenções manuais. A TE prescritiva pode detectar problemas e apontar soluções corretivas, ou então, prescrever ações que podem melhorar o desempenho da rede mesmo que não haja nenhum problema de desempenho.
- TE com laço aberto ou fechado: A TE com laço aberto ocorre quando não são levadas em consideração informações de realimentação (*feedback*) da rede, mas apenas informações locais do roteador. Quando as informações obtidas da rede influenciam nas decisões, a TE está utilizando controle com laço fechado.

4.6 Relacionamento entre as Abordagens

Embora haja sobreposição de interesses entre as abordagens apresentadas, existem muitos aspectos ortogonais entre elas. Por solucionar problemas distintos, é possível combiná-las em uma única arquitetura integrada para QoS na Internet. Acredita-se que na prática é improvável

que essas abordagens sejam utilizadas individualmente, mas em conjunto, para formar uma verdadeira plataforma onde se pode oferecer serviços fim a fim [44]. Como não se sabe exatamente qual é a melhor forma de oferecer QoS na Internet, as especificações de padronização de interfaces entre as abordagens ainda não estão prontas.

É importante que se faça uma distinção entre as funções de cada uma das abordagens apresentadas para facilitar a compreensão de como elas podem interagir. IntServ e DiffServ representam o rompimento com o modelo tradicional de melhor esforço utilizado na Internet, para oferecer serviços com garantias de QoS. Representam visões distintas dos mecanismos que devem ser utilizados. IntServ é baseado em reserva de recursos e pode oferecer garantias rígidas a determinados fluxos de dados. O empecilho para sua utilização em larga escala para a construção de serviços fim a fim na Internet é sua falta de escalabilidade (Seção 0). DiffServ é uma arquitetura considerada escalável, mas que apenas oferece garantias para agregações de fluxos. Por isso, atualmente é considerada a abordagem que mais provavelmente será utilizada para QoS na Internet. No entanto, IntServ pode ser utilizada com sucesso em segmentos de rede onde escalabilidade não representa um grande problema.

MPLS é uma técnica de encaminhamento de pacotes, não necessariamente direcionada para o provimento de QoS. Pode ser utilizada para construir caminhos escolhidos explicitamente, que têm recursos suficientes para sustentar as necessidades de desempenho de certos fluxos de dados. Além disso, os pacotes que trafegam por esses caminhos podem receber tratamento diferenciado dentro dos roteadores. MPLS representa um rompimento (ou uma evolução) com o mecanismo tradicional de encaminhamento de pacotes da Internet, chamado de salto a salto (*hop-by-hop*).

QoS é uma técnica de roteamento, que encontra caminhos que atendem às necessidades de QoS de terminados fluxos. Não é uma técnica de oferecimento de QoS, apenas indica qual a rota mais adequada para que os níveis de QoS possam ser mantidos. Sem algum mecanismo de provimento de QoS, como IntServ ou DiffServ, é possível que, quando os pacotes forem roteados por um caminho escolhido por QoS, ele já não atenda mais às suas necessidades. Além disso, ele não é um mecanismo de encaminhamento, ou seja, pode descobrir novas rotas, mas não tem como forçar pacotes de certos fluxos a seguirem obrigatoriamente essas rotas. Portanto, sua utilização faz mais sentido quando se modifica o mecanismo de encaminhamento básico, por exemplo, com MPLS.

Engenharia de Tráfego (TE) não é uma técnica específica, mas um processo de gerenciar o tráfego na Internet. Pode ser realizada manualmente, usando mecanismos das tecnologias de transmissão para desviar tráfego por caminhos alternativos (como por exemplo, usando caminhos virtuais ATM), ou utilizando alguma técnica automatizada que tem conhecimento das informações da camada IP da Internet, como as apresentadas anteriormente. Ou seja, dados os seus objetivos de desempenho, TE pode ser considerada como um processo que necessita de ferramentas, as quais podem ser baseadas em IntServ/RSVP, DiffServ, MPLS e QoS. Uma maneira de realizar TE usando as abordagens acima poderia ser:

- Fluxos requisitam níveis de QoS desejados, ou certas classes de serviço são configuradas com algum tipo de provisionamento dinâmico de recursos.
- QoS encontra rotas adequadas às necessidades de QoS do tráfego na rede.
- MPLS é usado para fixar fluxos às rotas adequadas.
- Dependendo da necessidade e trecho da rede em questão, RSVP pode ser utilizado para fazer reservas de recursos, ou agregações de fluxos podem ser formadas para receber encaminhamento de acordo com os PHBs DiffServ.

Não é necessário utilizar todas as abordagens em conjunto (talvez a relação custo/benefício nem mesmo seja boa). Alguns padrões estão sendo desenvolvidos para a utilização conjunta de algumas abordagens. Alguns exemplos são:

- TE com MPLS [5] e RSVP [32], para IntServ e DiffServ [6]. Uso de QoSR em TE [20].
- Interoperabilidade entre redes IntServ e DiffServ [8].
- Utilização de DiffServ em uma rede MPLS [22].

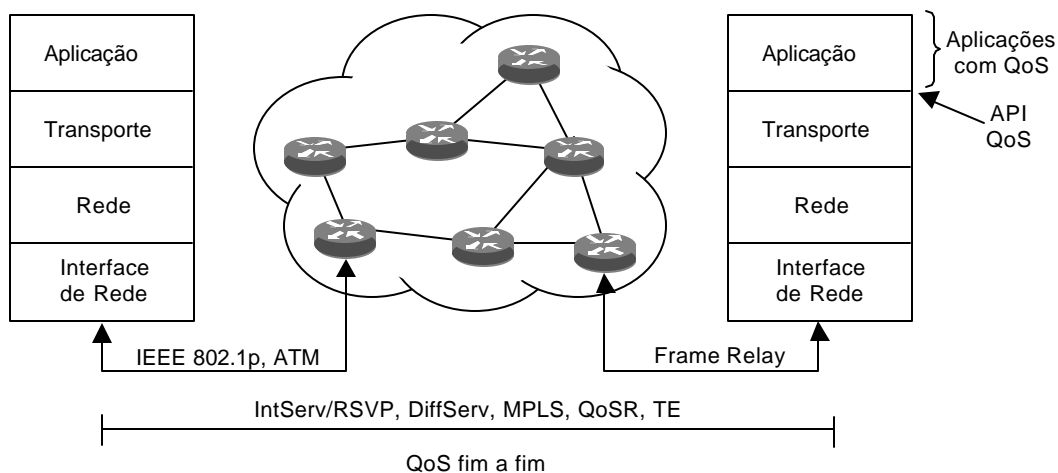


Figura 10 – Arquitetura de QoS fim a fim e de cima a baixo

Na realidade, uma arquitetura completa para QoS deve incluir mecanismos para controle de QoS na camada de enlace de dados (Seções 2.5.1, 2.5.2 e 2.5.3), inclusive em redes móveis[15], além de recursos de sistemas distribuídos[4], como APIs, para oferecer QoS às aplicações. A Figura 10 ilustra a situação da construção de uma arquitetura completa de cima para baixo (em termos de camadas de rede) e fim a fim (envolvendo múltiplos domínios distintos) para QoS na Internet.

5 A Internet2 e QoS

O objetivo desse capítulo é apresentar a Internet2, suas aplicações e principalmente a estratégia adotada para oferecer QoS, através do projeto QBone.

5.1 A Internet2

A Internet2 é um projeto desenvolvido pelaUCAID (University Corporation for Advanced Internet Development), um grupo de universidades americanas, que visa possibilitar a utilização de aplicações avançadas em redes de computadores [51]. Cerca de 150 universidades e várias corporações estão trabalhando para disponibilizar aplicações, tais como telemedicina, bibliotecas digitais e laboratórios virtuais, que não são possíveis atualmente devido à tecnologia utilizada.

Assim como a Internet surgiu de pesquisas acadêmicas e governamentais nos anos 80, a Internet2 está ajudando a desenvolver e testar novas tecnologias, como Ipv6, multidifusão, e Qualidade de Serviço (QoS). Dando suporte a essas tecnologias está uma infra-estrutura extremamente veloz, baseada em enlaces óticos, com tecnologias como SONET e WDM.

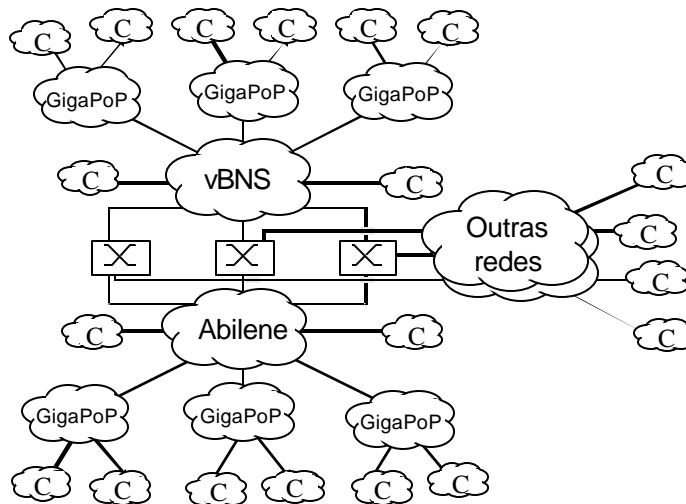


Figura 11 – Topologia genérica da Internet2

A topologia da Internet2 pode ser vista na Figura 11. Redes de Campus (C), se conectam a pontos de presença de gigabits (gigaPoPs) ou diretamente às grandes redes de *backbone*, como Abilene [49], vBNS [33] e outras redes americanas e internacionais.

5.2 Abilene e vBNS

Abilene é uma rede de alto desempenho desenvolvida pela UCAID em conjunto com a Qwest Communications, Nortel e Cisco Systems. Um objetivo importante do projeto Abilene é oferecer uma rede de *backbone* para as instituições conectadas na Internet2. Abilene está em operação desde o início de 1999, e desde o início de 2000 oferece conexão à Internet2 aos participantes de costa a costa dos Estados Unidos. Abilene atinge velocidades de até 2,4 Gbps, pretendendo atingir 9,6 Gbps em breve usando tecnologia IP sobre Sonet e conecta vários gigaPoPs. Abilene irá permitir aos membros da Internet2 o desenvolvimento de aplicações avançadas de rede e ela própria tem o objetivo de explorar as fronteiras da pesquisa em redes.

vBNS (very high performance *Backbone Network Service*) é uma rede americana que praticamente abrange o país inteiro e opera a uma velocidade de 622 Mbps. Lançada em 1995, é um produto de uma cooperação de 5 anos entre a NSF (National Science Foundation, um órgão do governo de fomento à pesquisa) e a empresa de telecomunicações MCI. Usa uma rede da MCI com tecnologias avançadas de comutação e transmissão baseadas em fibras ótica, ATM e Sonet.

A rede vBNS foi projetada para a comunidade científica e de pesquisa e originalmente oferecia uma interconexão de alta velocidade entre centros de supercomputação. Atualmente conecta também outras instituições de pesquisa, além dos centros de computação originais. Um dos objetivos da vBNS é o desenvolvimento de serviços IP avançados, como QoS.

Abilene é a principal rede para fornecer acesso à Internet2. Como as duas estão interligadas, algumas participantes podem ter acesso a Internet2 partindo da vBNS ou de alguma outra rede de alta velocidade conectada à Abilene.

5.3 Aplicações

O objetivo principal da Internet2 é possibilitar a utilização de aplicações avançadas de rede. Alguns exemplos são apresentados a seguir.

5.3.1 LearningWare – Software educacional

Learningware surge da observação de que existe atualmente pouco software educacional de alta qualidade disponível para educação em ambientes distribuídos. A maioria dos softwares educacionais existentes foi desenvolvida para uso local, especialmente aqueles que incorporam multimídia. A Internet2, com alta velocidade e opções de qualidade de serviço, é uma oportunidade para trabalhar em uma arquitetura para o desenvolvimento de aplicações para *learningware* e aplicações relacionadas com a educação distribuída.

5.3.2 Bibliotecas Digitais

Existem pesquisas que demonstram a viabilidade da utilização da Internet atual no desenvolvimento de sistemas de biblioteca digital. Mas, os novos serviços previstos para a Internet2 oferecem oportunidades para abrir novos caminhos nas pesquisas em Bibliotecas Digitais. Grandes quantidades de largura de banda (alta taxa de transmissão de dados) e reservas de banda permitem que materiais como mídias digitais contínuas (áudio e vídeo) deixem de ser utilizados estritamente em pesquisas e possam ser aproveitados para usos mais amplos.

5.3.3 Tele-imersão

Tele-imersão tem potencial para mudar significativamente os paradigmas educacionais, científicos e de produção. Ela difere de esforços anteriores em Realidade Virtual de várias maneiras, permitindo que pessoas em locais diferentes compartilhem um único ambiente virtual. Aplicações de tele-imersão necessitam de avanços na infra-estrutura da Internet, por suas características de comunicação síncrona, dependente de tempo, com baixo latência e grande largura de banda. Devido a essas características a comunidade científica decidiu adotar a tele-imersão como uma das principais aplicações de teste para a Internet2. A lógica é simples: se a rede pode tratar de tele-imersão, ela pode tratar qualquer coisa.

5.3.4 Laboratório Virtual

Um Laboratório Virtual é um ambiente de resolução de problemas distribuído e heterogêneo, que possibilita um grupo de pesquisadores localizados em qualquer ponto do mundo trabalhar juntos em um conjunto de projetos comuns. Como em qualquer outro laboratório, as ferramentas e técnicas são específicas ao domínio da pesquisa, mas os requisitos básicos de infra-estrutura são comuns entre as áreas. Um laboratório virtual tem algumas aplicações relacionadas com tele-imersão, mas esse não é um requisito fundamental. A Internet2 pretende abrigar em poucos anos uma série de experiências de laboratórios virtuais que estão sendo desenvolvidos atualmente por universidades e empresas.

5.4 O Projeto QBone

O QBone [48] constitui-se em uma plataforma de testes para QoS, onde vários aspectos relacionados à introdução de novos serviços baseados no protocolo IP podem ser explorados. Sua estrutura é baseada em Serviços Diferenciados. Mais especificamente, inicialmente foi está sendo implementado o serviço Premium, que emula uma linha privativa de dados, utilizando o PHB EF. Aplicações avançadas de rede, como as pretendidas pela Internet2, necessitam garantias mais rígidas, como aqueles fornecidas pelo PHB EF.

Além de viabilizar as aplicações de rede, o QBone é em si uma plataforma para avaliar o comportamento de DiffServ quando implementado em uma rede operacional de longa distância. Algumas questões a serem estudadas são: como realizar controle de admissão para redes sem conexão, quais as implicações de DiffServ na Engenharia de Tráfego, como projetar protocolos para a reserva de recursos entre domínios DiffServ, como oferecer reservas antecipadas (por exemplo, para planejar cursos de educação à distância), ou quais protocolos são necessários para implementar multidifusão (*multicast*) em DiffServ.

Além dos requisitos especificados na arquitetura DiffServ, a arquitetura QBone contém algumas inovações, como uma infra-estrutura integrada de medição e procedimentos para estabelecer reservas entre domínios. Um requisito de alto nível do QBone é a contigüidade. Diferente de outras tecnologias, como IPv6 e multidifusão, QoS para ser implementada necessita de um conjunto contíguo de redes (Domínios DS) para oferecer serviços com garantias fim a fim.

Cada rede QBone deve ter uma borda administrativa bem definida, através da qual ela se comunica com seus Domínios DS QBone vizinhos. Devem ser especificadas especificações de serviço (SLS, uma simplificação do SLA) bilaterais entre os domínios envolvidos, que especificam como o tráfego será classificado, policiado e encaminhado pelos roteadores de borda. Embora os SLSs sejam de responsabilidade dos domínios, existe um conjunto mínimo de características que devem estar presentes para suportar os serviços QBone.

6 Produtos Comerciais

Esse capítulo trata dos mecanismos para QoS, que alguns fabricantes de equipamentos para a Internet e redes corporativas disponibilizam atualmente.

6.1 Cisco Systems

A Cisco é a empresa que domina o mercado de roteadores para a Internet e está muito avançada em pesquisas e implementação de produtos para QoS na Internet.

6.1.1 Comutação de rótulos: Tag Switching

Tag Switching [18] é uma das técnicas precursoras do MPLS, oferecida pela Cisco, que utiliza o conceito de “troca de rótulos”, associando uma etiqueta (*tag*) a cada pacote ou célula que trafega na rede. O processamento ocorre de maneira semelhante ao MPLS. Uma rede Tag Switching consiste dos seguintes elementos:

- Roteadores de borda (*tag edge routers*): atribuem etiquetas para os pacotes e realizam outras funções de valor agregado.
- Comutadores de etiquetas (*tag switches*): encaminham os pacotes/células com base nas suas etiquetas. Podem também realizar funções completas de roteamento de Camada 3 e comutação de Camada 2.
- Protocolo de distribuição de etiquetas (TDP, *Tag Distribution Protocol*): em conjunto com algum protocolo de roteamento, é utilizado para distribuir informações entre os equipamentos em uma rede Tag Switching.

Tag Switching pode ser implementado em uma série de equipamentos, como roteadores ou comutadores ATM. A implementação em roteadores e comutadores ATM não necessita de

modificações de hardware, embora hardware especializado poderia melhorar o desempenho. A implementação pode ser feita através de atualização de software, o que facilita a sua instalação em redes já existentes.

6.1.2 Cisco IOS QoS

O Cisco IOS [16] (Internetworking Operating System) oferece uma série de soluções baseadas em QoS que permitem aos administradores de redes solucionar problemas causados pelo aumento de tráfego na rede e por novas demandas de aplicações. Os mecanismos de QoS do Cisco IOS são configurados em cada roteador e podem ser habilitados em cada interface de rede. O IOS QoS oferece três funções principais:

- Gerenciamento de congestionamento: refere-se aos mecanismos utilizados pelos roteadores para priorizar o encaminhamento de determinados pacotes em situações de congestionamento. Inclui as políticas de filas FIFO, fila de prioridade (PQ), fila customizada (CQ) e fila justa com pesos WFQ (ver Seção 2.6). CQ permite criar uma fila para cada classe de serviço desejada e atribuir uma porção fixa da largura de banda a cada uma, que então são servidas de maneira circular. Ou seja, permite implementar um mecanismo conhecido com WRR (Weighted Round Robin).
- Prevenção de congestionamento: oferece o mecanismo WRED (Weighted Random Early Detection) para prevenir a ocorrência de congestionamentos. O WRED é uma variação do algoritmo RED, que descarta pacotes aleatoriamente com antecedência para impedir que a fila do roteador transborde.
- Condicionamento de tráfego: permite configurar ferramentas para classificação, medição (com um balde de fichas), suavização e policiamento do tráfego.

Como resultado de um processo de classificação, os pacotes podem ser marcados com algum valor específico no campo IP Precedence, e posteriormente podem ser tratados com base nesse campo. Por exemplo, as filas CQ e WFQ podem distinguir entre classes de tráfego baseados nos valores do campo IP Precedence. O IOS QoS oferece também sinalização para reserva de recursos, através do protocolo RSVP.

6.2 3Com

A 3Com oferece QoS principalmente na sua linha de comutadores de camadas 2 e 3, mas também em roteadores. A estratégia da 3Com [1] para oferecer vários níveis de serviços diferenciados é baseada principalmente em priorização de tráfego e em reservas de recursos, tanto estáticas quanto dinâmicas. Priorização de tráfego é oferecido com um mecanismo para classificar o tráfego e então encaminhá-lo para a fila mais adequada, em um esquema de Fila de Prioridade (PQ). Os equipamentos 3Com aceitam priorização de quadros Ethernet, células ATM ou pacotes IP.

A 3Com possui também mecanismos para implementar a política de fila conhecida como WRR, que destina porções da largura de banda para determinadas classes de tráfego, conforme valores percentuais configurados com antecedência. Reservas dinâmicas podem ser feitas com o protocolo RSVP.

6.3 Nortel Networks

O Preside Quality of Service [36], da Nortel Networks, é uma solução de gerenciamento de políticas que oferece três elementos, provisionamento, execução e verificação das políticas de QoS. A Nortel não oferece simplesmente mecanismos para serem configurados em roteadores individuais, mas a possibilidade de implantação de uma política de QoS mais geral. A estratégia de QoS na Internet da Nortel para provedores de serviços é baseada em DiffServ. Além disso, também estão sendo implementadas algumas características de IntServ, para QoS fim a fim.

A funcionalidade básica do Preside QoS inclui suporte a filtros para implementação de DiffServ, que englobam mecanismos de condicionamento de tráfego (classificação, medição, etc.) e implementação de PHBs (políticas de filas). Além disso, a classificação dos pacotes para o filtro pode ser feita com base em qualquer campo dos cabeçalhos IP/TCP/UDP e permite a configuração desses filtros com base em usuários, hora do dia, roteadores de acesso, ou outras políticas desejadas.

7 O Network Simulator (ns)

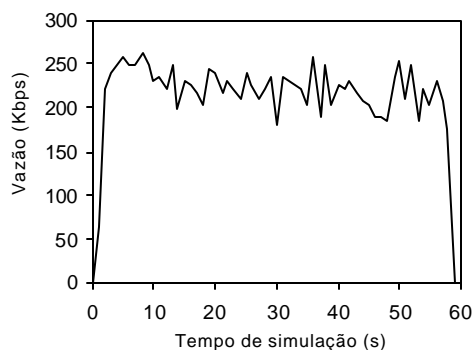
Esse capítulo apresenta o simulador de rede ns (network simulator) [7], [52] versão 2, que está sendo desenvolvido dentro do projeto VINT, por algumas universidade e centros de pesquisa americanas. O ns possui funcionalidades específicas para simular a Internet, o que o faz uma ferramenta poderosa para configurar simulações complexas rapidamente e também para comparação de resultados de pesquisas. O ns está sofrendo constante manutenção pelos provedores do projeto VINT, além de receber contribuições de pessoas e grupos de pesquisa de diferentes partes do mundo. Praticamente toda a funcionalidade existente na Internet está implementada no ns, como o protocolo IP, TCP, UDP, FTP, HTTP e protocolos de roteamento.

O ns executa a simulação e pode gerar vários arquivos como resultados, que podem ser utilizados para construir tabelas e gráficos. Junto com o ns é distribuído um software para animação da simulação, o nam (network animator), que pode ser executado após o término da simulação para a sua visualização. O nam utiliza um arquivo de *trace*, gerado pelo ns.

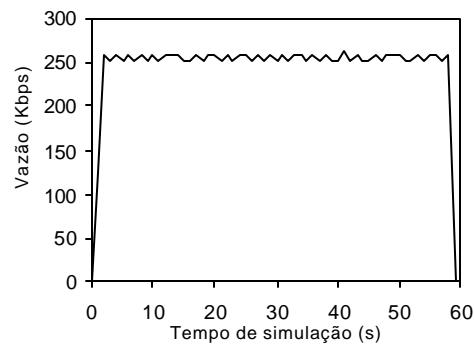
Em termos de QoS, a distribuição básica do ns somente inclui funcionalidade para IntServ. Entretanto, é possível obter contribuições que incluem DiffServ, MPLS e RSVP. A seguir serão apresentados alguns resultados obtidos em teste com QoS no ns.

7.1 DiffServ

A Figura 12 mostra os resultados de simulação usando um fluxo CBR configurado com uma taxa de 256 Kbps (Taxa Constante de Bits, tipicamente usada para dados de tempo real) e dez fluxos de melhor esforço, compartilhando um enlace de 1 Mbps. Sem a utilização de DiffServ, pode-se ver que a vazão alcançada pelo fluxo CBR não consegue manter os 256 Kbps originais porque ele é compartilhado com o tráfego de melhor esforço. Com a utilização de DiffServ com o PHB EF, a rede pode garantir o nível de QoS desejado pela aplicação.



(a)

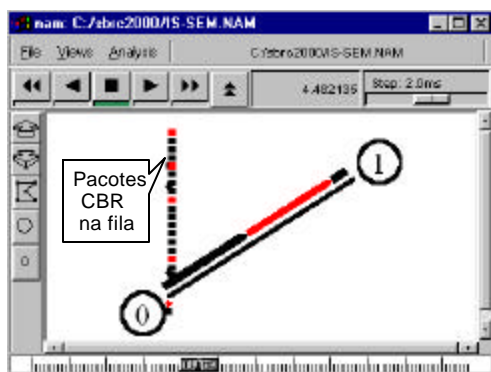


(b)

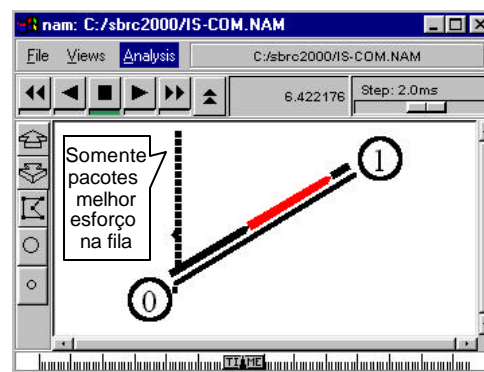
Figura 12 – Vazão de fontes de dados: a) Sem DiffServ; b) Com DiffServ

7.2 IntServ

A Figura 13 mostra o estado da fila em um roteador em uma situação com e sem o uso de IntServ, para a mesma situação do exemplo anterior. Sem IntServ, os pacotes de todos os fluxos são descartados indiscriminadamente. Com o uso de IntServ, apenas os pacotes de melhor esforço são descartados. Todos os pacotes CBR são encaminhados.



(a)



(b)

Figura 13 – Uso das filas no nam: a) Sem IntServ; b) Com IntServ

7.3 Engenharia de Tráfego com MPLS

A Figura 14 mostra uma rede com três caminhos alternativos no nam. O caminho do meio é o mais curto, portanto é o escolhido pelo protocolo de roteamento e todos os pacotes são encaminhados por ele em uma situação normal. Usando MPLS para fazer Engenharia de Tráfego, pode-se dividir o tráfego pelos caminhos alternativos e fazer uma melhor utilização da rede.

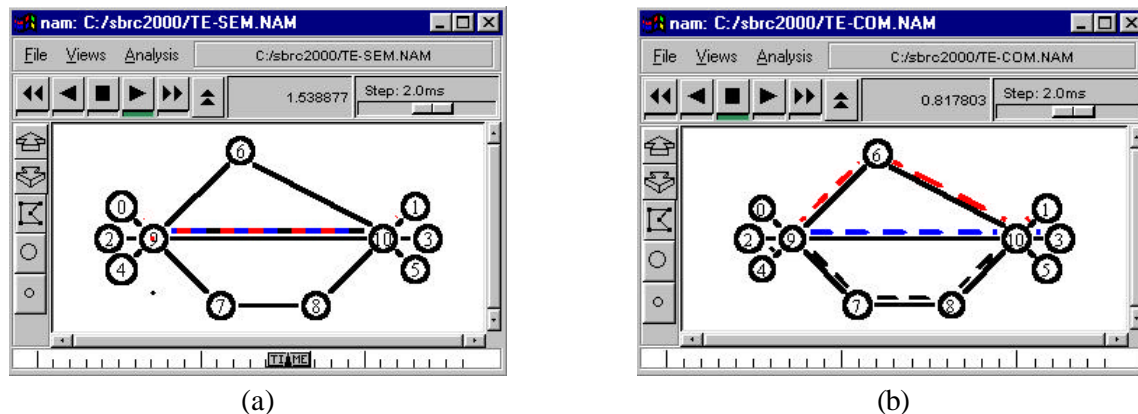


Figura 14 – Animação no nam: a) Sem TE; b) Com TE

8 Conclusão

A introdução de QoS na Internet não é simplesmente um assunto de pesquisa, mas uma exigência real do mercado. Provedores de serviço desejam oferecer a seus clientes serviços com vários níveis de diferenciação em qualidade e preços. Os usuários, por outro lado, desejam utilizar aplicações multimídia a qualquer hora do dia, o que é impossível atualmente pela falta crônica de qualidade na Internet. Somente em redes locais ou super-provisionadas é possível hoje em dia oferecer voz sobre IP, videoconferência, vídeo sob demanda, canais de rádio e televisão e uma série aplicações que cada vez mais estão motivando usuários, provedores e fornecedores tradicionais de conteúdo.

Alguns fabricantes de equipamentos já fornecem soluções parciais para QoS na Internet atualmente, mas a grande maioria dos profissionais da área, mesmo os mais experientes não sabe utilizá-los adequadamente. Isso significa que, mesmo não existindo ainda nenhuma solução de adoção global na Internet, é possível melhorar o desempenho de redes corporativas com a adoção de medidas simples de QoS.

Esperamos que, através desse trabalho, o aluno tenha uma visão clara do problema e algumas possíveis soluções, que podem ser utilizadas no seu trabalho profissional, ou como embasamento para estudos e pesquisas nessa área.

Bibliografia

- [1] 3Com Corporation, “3Com’s Strategy for Delivering Differentiated Service Levels”, White Paper, 1998.
- [2] Allman, M, Paxson, V. & Stevens W., “TCP Congestion Control”, RFC 2581, Abril 1999.
- [3] Apostolopoulos, G. et. al., “Quality of Service Based Routing: A Performance Perspective”, ACM SIGCOMM ’98, Agosto, 1998.
- [4] Aurrecochea, C., Campbell, A. T. & Hauw, L., “A Survey of QoS Architectures”, ACM Multimedia Systems Journal, Special Issue on QoS Architectures, Maio 1998.

- [5] Awduche, D. et al., “Requirements for Traffic Engineering over MPLS”, RFC 2702, Setembro 1999.
- [6] Awduche, D. et al., “A Framework for Internet Traffic Engineering”, Internet Draft, <draft-ietf-te-framework-01.txt>, Maio 2000.
- [7] Bajaj, S. et al., “Improving Simulation for Network Research”, Relatório Técnico, USC, Setembro 1999.
- [8] Bernet, Y. et al., “A Framework For Integrated Services Operation Over DiffServ Networks”, Internet Draft, <draft-ietf-issll-diffserv-rsvp-03.txt>, Setembro 1999.
- [9] Black, D. et al., “An Architecture for Differentiated Services”, RFC 2475, Dezembro 1998.
- [10] Braden, R., Clark, D. & Shenker, S., “Integrated Services in the Internet Architecture: an Overview”, RFC 1633, Junho 1994.
- [11] Bradner, S. et al., “Internet Protocol Quality of Service Problem Statement”, Internet Draft, <draft-bradner-qos-problem-00.txt>, Setembro 1997.
- [12] Braden, R. et al., “Resource ReSerVation Protocol (RSVP) – Version 1 Functional Specification”, RFC 2205, Setembro 1997.
- [13] Braden, R., et al., “Recommendations on Queue Management and Congestion Avoidance in the Internet”, RFC 2309, Abril 1998.
- [14] Carpenter, B., “Architectural Principles of the Internet”, RFC 1958, Junho 1996.
- [15] Chalmers, D. & Sloman, M., “A Survey of Quality of Service in Mobile Computing Environments”, IEEE Communications Surveys, 2º trimestre 1999.
- [16] Cisco Systems, “The Business Case for Advanced Services”, White Paper, 1997.
- [17] Cisco Systems, “Cisco IOS Software - Quality of Service Solutions”, White Paper, 1998.
- [18] Cisco Systems, “Tag Switching: Uniting Routing and Switching for Scalable”, High-Performance Services, White Paper, 1998.
- [19] Clark, D. D., “The Design Philosophy of the DARPA Internet Protocols”, ACM SIGCOMM ’88, Agosto 1988.
- [20] Crawley, E. et al., “A Framework for QoS-based Routing in the Internet”, RFC 2386, Agosto 1998.
- [21] Croll, A. & Packman, E., “Managing Bandwidth: Deploying QoS in Enterprise Networks”, Prentice Hall, 1999.
- [22] Faucher, F. L. et al., “MPLS Support of Differentiated Services”, Internet Draft, <draft-ietf-MPLS-diff-ext-03.txt>, Fevereiro 2000.
- [23] Ferguson, P. & Huston, G., “Quality of Service in the Internet: Fact, Fiction, or Compromise?”, INET ’98, Julho 1998.
- [24] Ferguson, P. & Huston, G., “Quality of Service: Delivering QoS on the Internet and in Corporate Networks”, John Wiley & Sons, 1998.
- [25] Heinaman, J. et al., “Assured Forwarding PHB Group”, RFC 2597, Junho 1999.
- [26] IEEE, “Draft Standard for Virtual Bridged Local Area Networks”, Draft IEEE 802.1Q, 1998.
- [27] ISO/IEC DIS 13236, “Information Technology - Quality of Service – Framework”, ISO/OSI/ODP, Julho 1995.
- [28] Jacobson, V., “Congestion avoidance and control”, ACM SIGCOMM’88, Agosto 1988.
- [29] Jacobson, V., Nichols, K. & Poduri, K., “An Expedited Forwarding PHB”, RFC 2598, Junho 1999.
- [30] Jain, R., “Myths about Congestion Management in High Speed Networks”, Internetworking: Res. And Exp., vol.3, 1992.

- [31] Lefelhocz, C. et. al., Congestion Control for Best-Effort Service: Why We Need A New Paradigm, IEEE Network, Janeiro 1996.
- [32] Li, T. & Rekhter, Y., “A Provider Architecture for Differentiated Services and Traffic Engineering (PASTE)”, RFC 2430, Outubro 1998.
- [33] MCI & NSF, “very High Performance Backbone Network Service”, <http://www.vbns.net>.
- [34] Microsoft, “Quality of Service Technical White Paper”, Microsoft Windows 2000 Server, White Paper, 1999.
- [35] Nichols, K. et. al., “Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers”, RFC 2474, Dezembro 1998.
- [36] Nortel Networks, “Preside Quality of Service”, White Paper, 1999.
- [37] Odlyzko, A. P., “The Current State and Likely Evolution of the Internet”, IEEE Globecom 99, Dezembro 1999.
- [38] Paxson, V., et. al., “Known TCP Implementation Problems”, Internet RFC 2525, Março 1999.
- [39] Rosen, E. et al., Multiprotocol Label Switching Architecture, Internet Draft, <draft-ietf-mpls-arch-06.txt>, Agosto 1999.
- [40] Saltzer, J., Reed, D. & Clark, D., “End-to-End Arguments in System Design”, ACM Transactions on Computer Systems, Novembro 1984.
- [41] Shenker, S., “Specification of Guaranteed Quality of Service”, RFC 2212, Setembro 1997.
- [42] Siqueira, F., “The Design of a Generic QoS Architecture for Open Systems”, Technical Report, Trinity College Dublin, 1997.
- [43] Socolofsky, T. & Kale, C., “A TCP/IP Tutorial”, RFC 1180, Janeiro 1991.
- [44] Stardust.com, Inc., “QoS Protocols & Architectures”, White Paper, Julho 1999.
- [45] Stardust.com, Inc., “The Need for QoS”, White Paper, Julho 1999.
- [46] Tanenbaum, A. S., “Computer Networks”, Prentice Hall, 3rd ed., 1996.
- [47] Teitelman, B. & Hanss, T., “QoS Requirements for Internet2”, Internet2 QoS Work Group Draft, Abril 1998.
- [48] Teitelman, B., “Internet2 QBone: Building a Testbed for IP Differentiated Services”, IEEE Network Magazine, Setembro 1999.
- [49] Thomson, K., Miller, G. J. & Wilder, R., “Wide-Area Internet Traffic Patterns and Characteristics, IEEE Network”, Novembro 1997.
- [50]UCAID, “Abilene Project”, <http://www.internet2.edu/abilene>
- [51]UCAID, “Internet2 Project”, <http://www.internet2.edu>
- [52] VINT Network Simulator (versão 2), <http://www-mash.cs.berkeley.edu/ns>.
- [53] Vogel, L. A. et al., “Distributed Multimedia and QoS: A Survey”, IEEE Multimedia, Verão 1995.
- [54] Wroclawski, J., “Specification of the Controlled-Load Network Element Service”, RFC 2211, Setembro 1997.
- [55] Xiao, X. & Ni, L. M., “Internet QoS: A Big Picture”, IEEE Network, Março 1999.
- [56] Yang, C.-Q. & Reddy, A. V. S., “A Taxonomy for Congestion Control Algorithms in Packet Switching Networks”, IEEE Network Magazine, Julho 1995.