Avaliação do Serviço Assegurado para a Diferenciação de Serviços na Internet*

José Ferreira de Rezende
rezende@gta.ufrj.br
Grupo de Teleinformática e Automação (GTA)
COPPE/UFRJ
Caixa Postal 68504 - 21945.970 - Rio de Janeiro - RJ
http://www.gta.ufrj.br

Resumo

Este artigo enfoca o modelo de diferenciação de serviços como base para a provisão de QoS na Internet. Ele tem como objetivo avaliar o desempenho de fluxos atravessando domínios, onde os nós implementam o PHB de Encaminhamento Assegurado. Uma série de mecanismos, tais como a marcação de pacotes de acordo com perfis de serviço e o gerenciamento ativo de filas, foram implementados no simulador ns-2 para realizar esta avaliação. Os fluxos que exigem garantias de QoS são tráfegos TCP, do tipo FTP, competindo com tráfegos de melhor esforço do tipo FTP, HTTP, CBR e ON-OFF. Os resultados obtidos mostram a adequação deste serviço no fornecimento de garantias de QoS e revelam os problemas de justiça no compartilhamento da banda passante.

Abstract

This article focuses on the differentiated services model as a basis for the provision of QoS in the Internet. It has as objective to evaluate the performance of traffic flows crossing domains where nodes implement the Assured Forwarding PHB. A series of mechanisms, such as the marking of packets in accordance with traffic profiles and the active queue management, had been implemented in the ns-2 simulator to carry through this evaluation. The evaluated traffic requiring QoS guarantees are TCP traffic, FTP-like, competing with best effort traffics such as FTP, HTTP, CBR and ON-OFF. The results obtained show the adequacy of this service in the supply of QoS guarantees and disclose to the problems of fairness in the bandwidth sharing.

*Este trabalho foi realizado com recursos da UFRJ, FUJB, CNPq, CAPES, COFECUB, REENGE e FAPERJ.

1 Introdução

A atual arquitetura de rede da Internet foi projetada para o envio de informações usando um modelo de serviço de melhor esforço (*best effort*), ou seja, sem quaisquer garantias de vazão, atraso ou outro requisito de QoS. A banda passante destinada a cada fluxo será a maior possível enquanto não houver nenhum tipo de congestionamento. Neste último caso, haverá descarte de pacotes com conseqüente queda na taxa de transmissão. Os problemas de congestionamento na Internet se devem, por um lado, ao crescimento vertiginoso do tráfego na Internet e, por outro lado, ao tipo de tráfego transportado pela rede. Normalmente, o tráfego na Internet é em rajada, acarretando momentos de sobrecarga na rede nos casos de simultaneidade no envio de dados por diversas fontes. Nos momentos de sobrecarga, ocorre a perda de dados o que acarreta numa inibição de transmissão de dados das chamadas fontes cooperantes.

Além do crescimento do número de estações conectadas, que dobra a cada 56 semanas, assim como de servidores Web que dobra a cada 23 semanas, a Internet vem sendo usada cada vez mais no transporte de informação multimídia, tais como imagens, voz e vídeo. Com o aumento da capacidade de processamento dos computadores pessoais e o surgimento de novas aplicações multimídia distribuídas, a Internet tende a receber uma maior quantidade deste tipo de tráfego. O modelo de melhor esforço adotado pela Internet para o envio de informações não atende aos requisitos destas novas aplicações. Propostas estão sendo estudadas de modo a prover diferentes níveis de serviço, ou seja, serviços com uma determinada QoS, na Internet. As propostas se dividem basicamente em duas linhas: o uso de reserva de recursos e o uso do campo ToS (*Type of Service*) do cabeçalho IP. Estas propostas são denominadas Serviços Integrados [1] e Serviços Diferenciados [2], respectivamente.

A primeira proposta provê a discriminação de serviços através da explícita alocação e reserva de recursos. Este modelo, baseado no protocolo RSVP (Resource ReSerVation Protocol) [3, 4, 5], fornece uma base sólida para a especificação de diferentes classes de serviços, mas requer grandes mudanças na infra-estrutura da Internet, além de exigir um grande volume de sinalização e de estados por nó. A abordagem que faz uso do ToS visa definir um conjunto simples de mecanismos para tratar os pacotes com diferentes prioridades refletidas nos bits do campo ToS. Este último modelo, não necessita de um estado para cada fluxo e de sinalização a cada nó, o que aumenta a sua escalabilidade.

Este artigo enfoca o modelo de diferenciação de serviços como base para a provisão de QoS na Internet. Na proposta desenvolvida pelo grupo de trabalho de Serviços Diferenciados (*Differentiated Services - DiffServ*, a idéia é renomear o campo ToS do cabeçalho IP, denominando-o de DS (*Differentiated Service*). Ao ingressar num domínio que implementa serviços diferenciados, os pacotes de um fluxo de tráfego terão este campo marcado de acordo com o contrato estabelecido entre o usuário que gera o fluxo e o responsável pelo domínio. A partir da análise deste campo em cada pacote, o domínio pode prover diferentes tratamentos aos pacotes de cada fluxo transportados pela rede [6]. Este tratamento, denominado de Comportamento por Nó (*Per Hop Behavior* - PHB), é definido em cada nó da rede. Dois PHBs estão atualmente em ampla discussão dentro da proposta do Diffserv, são eles, o PHB de Encaminhamento Expresso (*Expedited Forwarding PHB* - EF-PHB) [7] e o PHB de Encaminhamento Assegurado (*Assured PHB* - AF-PHB) [8]. Estes tratamentos por nó, aplicados a fluxos individuais ou agregados que atravessam o domínio de diferenciação de serviços, quando acoplados a mecanismos de condicionamento de tráfego nas bordas da rede fornecem um serviço fim-a-fim cuja semântica ainda não está claramente definida. Com isso, uma avaliação apurada e exaustiva do nível de serviço oferecido por estes mecanismos precisa ser realizada antes da sua disponibilização.

Este artigo tem como objetivo avaliar o desempenho de fluxos atravessando domínios que implementam a diferenciação de serviços através do PHB de Encaminhamento Assegurado. Para medir o desempenho obtido por estes fluxos, este serviço foi implementado no simulador ns-2 [9]. Para isto, foi necessário implementar mecanismos de escalonamento de pacotes, de condicionamento de tráfego, tais como a marcação de pacotes de acordo com perfis de serviço; e ainda mecanismos de gerenciamento de filas ativo que implementam o AF-PHB, fornecendo níveis de preferência de descarte de pacotes. Os tipos de fluxos avaliados são tráfegos TCP, do tipo FTP, que atravessam um domínio de diferenciação de serviços. Para obter uma maior acurácia nos resultados de simulação, os tráfegos de melhor esforço que competem com os tráfegos com requisitos de QoS são tanto de longa duração (FTP) quanto de curta duração (HTTP). Estes últimos representam uma grande parcela do tráfego atualmente veículado na Internet. Este artigo está organizado da seguinte maneira. A seção 2 especifica o serviço Assegurado, detalhando as características do AF-PHB. Na seção 3, é descrito o mecanismo de gerenciamento ativo de filas que implementa este PHB. Na seção 4 são apresentados os resultados de simulação obtidos, assim como uma análise destes resultados. Finalmente, na seção 5 são apresentadas as conclusões e as perspectivas deste trabalho.

2 Serviço de Encaminhamento Assegurado

Este modelo de serviço se baseia não numa garantia estrita, mas numa expectativa de serviço que será obtida por um determinado tráfego quando existirem momentos de congestionamento. O controle de admissão exerce papel importante neste modelo, pois ele é encarregado de garantir a existência dos recursos necessários durante todo o percurso da origem ao destino. Um perfil associado a cada tráfego define o serviço esperado por este. A definição de um fluxo de tráfego pode ser baseada em qualquer combinação de campos presentes no cabeçalho IP. Desta forma, é possível oferecer diferentes níveis de granularidade à agregação dos diferentes fluxos de tráfego que chegam aos roteadores de fronteira do domínio de diferenciação de serviços. No interior da rede não há identificação de fluxos, por isto o roteador de fronteira é responsável por manter o maior grau possível de discriminação entre os fluxos.

Mecanismos de condicionamento de tráfego atuam nas fronteiras da rede de forma a controlar a quantidade de tráfego do tipo Assegurado (tráfego AF) que entra ou sai do domínio. Tais ações de condicionamento de tráfego podem incluir suavização de tráfego, descarte de pacotes, e o mais importante, marcação dos pacotes de acordo com um perfil de serviço. A figura 1 mostra um classificador de pacotes junto com os elementos de condicionamento de tráfego definidos na arquitetura de Diferenciação de Serviços [2]. O medidor é usado para comparar um tráfego com o perfil contratado. O seu estado em relação a um pacote pode ser usado para afetar as ações do marcador, do policiador ou do suavizador.

No serviço de Encaminhamento Assegurado existe uma garantia que os pacotes

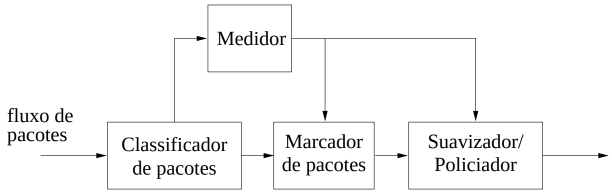


Figura 1: Elementos de condicionamento de tráfego.

marcados serão encaminhados com uma alta probabilidade, contanto que o tráfego agregado não exceda a taxa contratada, definida pelo perfil de serviço. No entanto, é permitido que um usuário exceda o perfil contratado, sabendo que o tráfego em excesso não será entregue com a mesma probabilidade do tráfego que está dentro do perfil. Conforme os pacotes são encaminhados pela rede e agregados a outros fluxos os roteadores na fronteira de outras regiões somente policiam esta agregação de fluxos. O tratamento em cada nó é definido através do AF-PHB, descrito a seguir.

2.1 AF-PHB

O AF-PHB, especificado em [8], é a maneira pela qual um provedor de um domínio de diferenciação de serviços oferece diferentes níveis de garantias de encaminhamento de pacotes IP de um usuário deste domínio. O AF-PHB provê a entrega destes pacotes em quatro classes independentes, chamadas classes AF (*Assured Forwarding*), onde cada classe tem alocada em cada nó do domínio uma certa quantidade de recursos (*buffer* e banda passante). Os pacotes IP que desejam utilizar os serviços providos pelo AF-PHB devem pertencer à uma destas classes de acordo com o contrato estabelecido.

Dentro de cada classe AF, um pacote IP pode ser marcado (pelo usuário ou pelo domínio DS) com um dentre três diferentes níveis de preferência de descarte. No caso de congestionamento, a preferência de descarte de um pacote determina a importância relativa do pacote dentro da classe AF. Um nó DS congestionado deve evitar que os pacotes com um menor valor de preferência sejam perdidos, através do descarte preferencial de pacotes com um mais alto valor de preferência de descarte. Portanto, num nó DS, o nível de garantia de encaminhamento de um pacote IP depende da quantidade de recursos alocada para a classe AF a qual o pacote pertence, da carga atual da classe AF, e, em caso de congestionamento no interior da classe, da preferência de descarte do pacote.

Uma implementação do AF-PHB deve tentar minimizar congestionamentos duradouros, mas permitindo congestionamentos curtos resultantes de rajadas. Isto é, ela deve detectar e reagir a congestionamentos duradouros dentro de cada classe através do descarte de pacotes e enfileirar rajadas de pacotes que causam congestionamentos curtos. Isto requer um algoritmo de gerenciamento ativo de filas que será discutido na próxima seção.

3 Gerenciamento ativo de filas

Para que um mecanismo de gerenciamento ativo de filas atenda aos requisitos do serviço Assegurado ele deve conter uma função que monitore o nível de congestionamento instantâneo e compute um nível de congestionamento suavizado. O algoritmo de descarte usa este nível de congestionamento suavizado para determinar quando pacotes deverão ser descartados. Também, o algoritmo de descarte deve ser insensível às características do tráfego dos fluxos num curto espaço de tempo. Isto é, fluxos com diferentes formas de rajadas curtas, mas com taxas de pacotes de longo prazo idênticas devem ter seus pacotes descartados com uma probabilidade essencialmente idêntica. Isto pode ser conseguido pelo uso da aleatoriedade na função de descarte. Um exemplo de tal algoritmo é o RED (*Random Early Detection*) [10].

RED é um mecanismo implementado nos roteadores, projetado para ser usado em conjunto com o protocolo TCP. Neste mecanismo, o roteador monitora o tamanho da sua fila, e quando ele detecta um congestionamento iminente, ele notifica de forma implícita a fonte, de forma que esta ajuste sua janela de congestionamento. Na verdade, a fonte é notificada através do descarte de um de seus pacotes. Desta maneira, a fonte será efetivamente notificada pelo estouro da temporização correspondente ao pacote descartado[1]. O roteador RED descarta pacotes mais cedo do que ele deveria, para que a fonte diminua sua janela de congestionamento mais cedo do que ela normalmente o teria feito. Em outras palavras, o roteador descarta uns poucos pacotes causando uma diminuição na taxa de envio da fonte, com a esperança de que ele não venha a descartar um número muito maior de pacotes mais tarde.

Quando um roteador RED utiliza uma fila FIFO, ao invés de esperar que a fila se torne completamente cheia e então ser forçado a descartar cada pacote que chega, ele decide descartar cada pacote com uma certa probabilidade sempre que o tamanho da fila excede um determinado nível. O roteador computa o tamanho médio da fila ($avglen$) utilizando uma média ponderada por uma variável q_{weight} de maneira similar àquela utilizada na computação dos temporizadores do TCP. Na realidade, RED utiliza dois patamares na sua fila (min_thresh,max_thresh), onde $min\_thresh < max\_thresh$. Quando um pacote chega no roteador, e o $avglen$ é menor do que o limite inferior, ele coloca o pacote na fila. Quando $avglen$ é maior que o limite superior o pacote é sempre descartado. Se o $avglen$ se encontra entre os dois limites, então o novo pacote é descartado com uma probabilidade p, onde p é uma função do tamanho médio da fila e do tempo decorrido desde o descarte do último pacote.

A probabilidade com que um roteador RED decide descartar um pacote é proporcional à parcela da banda passante que este fluxo está usando neste roteador, ou seja, quanto mais pacotes um fluxo envia, maior é a probabilidade com que seus pacotes serão selecionados para descarte. Esta probabilidade tem um limite superior dada pelo parâmetro RED P_{max}. Quanto maior for P_{max}, maior será a agressividade do algoritmo no descarte de pacotes. Isto é exemplificado pela simulação de duas conexões TCP entre os nós S1-S3 e S2-S4 compartilhando o gargalo entre os roteadores R1 e R2, como mostrado na figura 2. A figura 3 mostra o tamanho instantâneo e médio da fila de saída do roteador RED R1 quando é variado o valor de P_{max}. Quando o P_{max} é maior (figura 3.b), o algoritmo descarta um maior número

[1] O TCP detecta possíveis congestionamentos através de temporizadores (ou ACKs duplicados).

de pacotes, provocando uma diminuição da taxa de envio das conexões TCP, o que traz o tamanho médio da fila para um valor mais próximo do min_thresh.

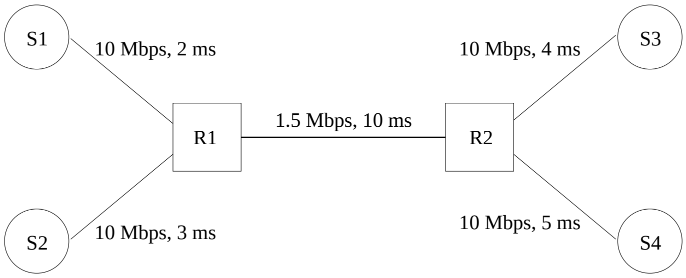
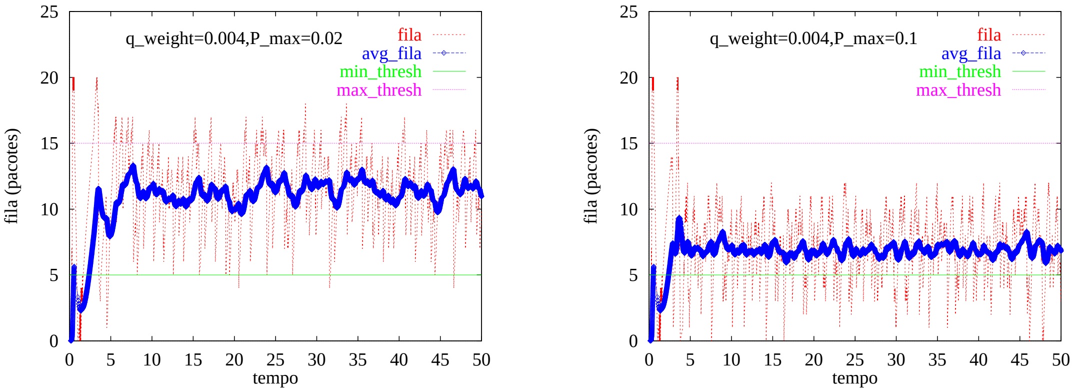


Figura 2: rede de simulação RED.



(a) $P_{max} = 0.02$

(b) $P_{max} = 0.1$

Figura 3: tamanho médio e instantâneo da fila RED.

Um grande número de análises e simulações foram feitas para determinar os valores ótimos para os vários parâmetros do algoritmo RED. No entanto, todas estas análises dependem da caracterização da carga da rede, que influencia diretamente o tamanho da fila. Por exemplo, se o tráfego é muito variável (*bursty*), o min_thresh deve ser suficientemente grande para manter uma alta utilização do enlace. E também, a diferença entre os dois limiares deve ser maior do que o incremento do tamanho médio da fila em um RTT (*round-trip-time*). É considerada uma boa regra, dado a mistura de tráfego encontrada na Internet atualmente, utilizar $max\_thresh = 2 * min\_thresh$.

3.1 Gerenciamento ativo de filas no Serviço Assegurado

Como dito anteriormente, os roteadores na fronteira do domínio DS monitoram e marcam os pacotes de fluxos individuais ou agregados de uma classe AF de acordo com diferentes níveis de preferência de descarte. Quando apenas dois níveis de preferência de descarte são utilizados, os pacotes de um fluxo que obedecem o perfil de serviço contratado são marcados como *IN* (*in-profile*) e os pacotes que estão além do perfil de serviço são marcados como OUT (*out-of-profile*). Neste caso, o gerenciamento das filas nos roteadores internos ao domínio de diferenciação de serviços é normalmente realizado pela adoção de dois algoritmos RED: um para pacotes que estão em conformidade com o perfil de tráfego definido, ou seja, os pacotes marcados com *IN*, e outro para os pacotes OUT. Este mecanismo é conhecido por RIO (RED com *IN* e OUT) [11]. O primeiro algoritmo RED é configurado de maneira mais agressiva que o segundo, visando o descarte prioritário de pacotes OUT. O objetivo é reduzir os efeitos do congestionamento antes da necessidade de descarte de pacotes *IN*.

O algoritmo RIO calcula um tamanho médio da fila para pacotes *IN*, e outro para todos os pacotes na fila (*IN*+OUT). Na chegada de um pacote, RIO verifica se este pacote é *IN* ou OUT. Se ele é um pacote *IN*, o roteador calcula o tamanho médio da fila somente dos pacotes *IN* (avg_{IN}), e também, o tamanho médio da fila levando em conta todos os pacotes (avg_{TOTAL}). A probabilidade de descarte de um pacote *IN* depende de avg_{IN}, e a probabilidade de descarte de pacotes OUT depende de avg_{TOTAL}. Como ilustrado na figura 4, existem três parâmetros para cada algoritmo RED. Os três parâmetros, min_{IN}, max_{IN} e P_{maxIN}, definem a fase de operação normal $[0, min_{IN})$, a fase onde se evita o congestionamento $[min_{IN}, max_{IN})$, e a fase de controle de congestionamento $[max_{IN}, \infty)$ para pacotes *IN*. Da mesma forma, min_{OUT}, max_{OUT} e P_{maxOUT}, definem as fases correspondentes para os pacotes OUT.

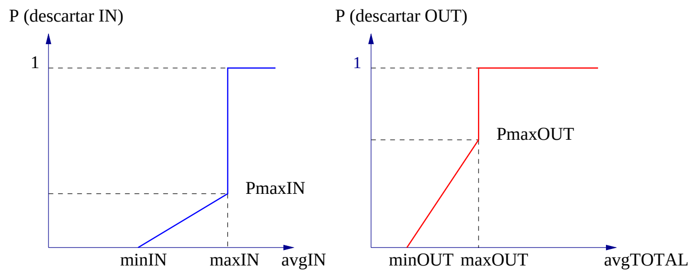


Figura 4: parâmetros do algoritmo RIO.

A discriminação contra pacotes OUT no RIO é criada por uma escolha cuidadosa dos parâmetros (min_{IN},max_{IN},P_{maxIN}) e (min_{OUT},max_{OUT},P_{maxOUT}). Um roteador é mais agressivo no descarte de pacotes OUT de três formas. Primeiro, ele descarta pacotes OUT muito mais cedo do que ele descarta pacotes *IN*, isso é feito pela escolha de um min_{OUT} menor do que min_{IN}. Segundo, na fase onde se evita o congestionamento, ele descarta pacotes OUT com uma mais alta probabilidade, escolhendo um P_{maxOUT} maior do que P_{maxIN}. Terceiro, ele entra em fase de controle de congestionamento para os pacotes OUT muito antes do que para pacotes *IN*, pela escolha de max_{OUT} muito menor do que max_{IN}. Essencialmente, RIO descarta pacotes OUT primeiro quando ele detecta um congestionamento incipiente, e descarta todos os pacotes OUT se o congestionamento persiste. Quando, o roteador é inundado por pacotes *IN*, o roteador descarta pacotes *IN* na esperança de controlar o congestionamento. Numa rede bem provisionada, isto nunca deveria acontecer. Quando um roteador está operando persistentemente na fase de controle de congestionamento, descartando pacotes *IN*, isto é uma indicação clara de que a rede está mal provisionada.

A escolha de avg_{TOTAL} para determinar a probabilidade de descarte de pacotes *OUT* é sutil. Diferentemente de pacotes *IN*, para os quais a rede deve estar apropriadamente provisionada, os pacotes *OUT* representam tráfego oportunista, e não existe uma indicação válida de qual quantidade de pacotes *OUT* é adequada. Se o tamanho médio da fila dos pacotes *OUT* fosse utilizado para controlar o descarte de pacotes *OUT*, a escolha dos três parâmetros correspondentes seria difícil, e não existe uma correlação intuitiva direta com os parâmetros correspondentes para os pacotes *IN*. Pela utilização do avg_{TOTAL}, os roteadores podem manter pequenos tamanhos de fila e uma alta vazão independentemente do tipo de mistura de tráfego que eles recebem.

Através deste mecanismo de descarte seletivo espera-se obter uma melhor vazão para pacotes *IN* do que para pacotes *OUT*. Com uma provisão apropriada de recursos para a rede, isto resultaria em garantias de banda passante contanto que o tráfego *IN* não exceda as capacidades dos enlaces da rede. Sem mecanismos de reserva de recursos ou roteamento com QoS, os roteadores de fronteira não podem antever como todos os fluxos serão roteados no interior do domínio de serviços diferenciados. Consequentemente, é possível que ocasionalmente o tráfego *IN* possa exceder a capacidade de um determinado enlace, resultando em perda de garantias. A vazão alcançada é o resultado da interação das ações dos roteadores no interior da rede, do emissor, do marcador de pacotes e da interação entre os diferentes fluxos. Mais especificamente, a vazão depende da política de descarte de pacotes adotada pelos roteadores e da política de reação do protocolo à perdas.

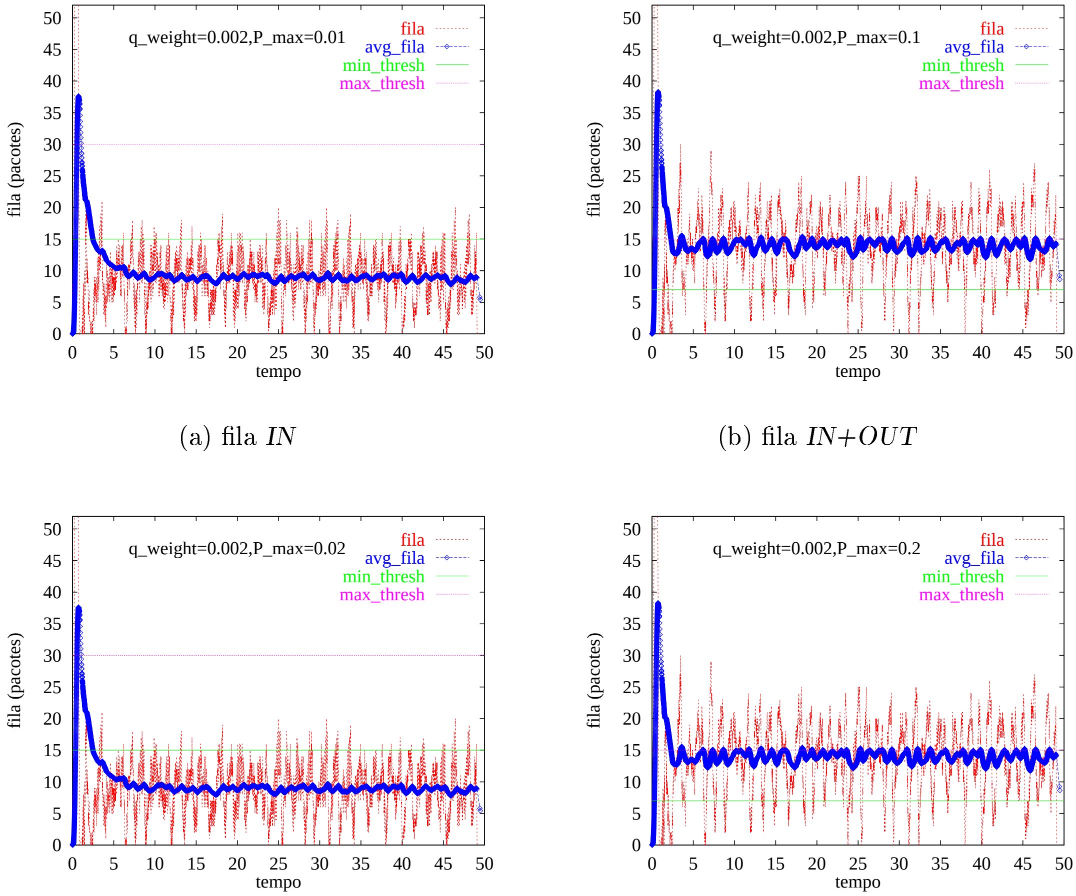
Para mostrar o comportamento da fila de um roteador RIO, foi realizada uma simulação com 10 conexões TCP compartilhando um enlace como na topologia da figura 2. Nesta simulação, cinco conexões utilizam um perfil de serviço de 50 Kbps e cinco conexões com um perfil de 200 Kbps. Todo o tráfego em excesso desses perfis são marcados como *OUT*. As figuras 5.a e 5.b mostram, respectivamente, o tamanho instantâneo e médio das filas *IN* e *IN+OUT*. Os roteadores R1 e R2 implementam o algoritmo RIO com os parâmetros [15,30.0.002,0.01][2] para a fila *IN* e [7,15,0.002,0.1] para a fila *IN+OUT*. As figuras 5.c e 5.d mostram o resultado obtido neste mesmo cenário quando são utilizados os seguintes parâmetros para as filas *IN* e *IN+OUT*, respectivamente: [15,30,0.002,0.02] e [7,15,0.002,0.2].

4 Simulação do serviço Assegurado

Para a simulação do serviço Assegurado, realizada no simulador ns [9], foi necessário implementar os mecanismos que compõe este serviço. Dentre os mecanismos implementados estão os mecanismos de condicionamento de tráfego, tais como policiadores e mecanismos de marcação de pacotes de acordo com perfis de serviço, além do mecanismo de gerenciamento ativo de filas que implementa o próprio AF-PHB: o RIO.

Dentre os mecanismos utilizados para checar a conformidade nos roteadores de fronteira, e assim marcar os pacotes, estão o mecanismo de estimativa de taxa (*rate estimator*) [11] e o *leaky-bucket*. O primeiro, mede a taxa de envio de um fluxo e marca os pacotes quando a taxa medida ultrapassa um certo limiar. Neste trabalho foi utilizado o segundo mecanismo que permite medir a quantidade de dados que um

[2] [min_thresh, max_thresh, q_{weight}, P_{max}]



(a) fila *IN* (b) fila *IN+OUT*

(c) fila *IN* (d) fila *IN+OUT*

Figura 5: simulação RIO.

fluxo gera em qualquer intervalo de tempo. Se a quantidade de dados excede um certo limiar, o *leaky-bucket* marca os pacotes deste fluxo (figura 6). Especificamente, os pacotes que chegam no *leaky-bucket* e encontram uma ficha são marcados como *IN* e imediatamente enviados. Aqueles que não encontram uma ficha são marcados como *OUT* (ou não recebem nenhuma marcação). A taxa de preenchimento do balde é igual à taxa esperada pelo usuário, ou seja, o perfil de serviço para o qual o serviço Assegurado deve fornecer garantias. O tamanho do balde, ou seja, o tamanho da rajada permitida é uma parâmetro cuja influência no desempenho deve ser avaliada.

Quando a marcação de pacotes é realizada nas estações, ou seja fora do domínio de diferenciação de serviços, o mecanismo de policiamento deve garantir que o tráfego agregado entrando no domínio não ultrapasse a soma dos perfis de serviço utilizados pelas estações. Quando a marcação é feita pelo roteador de fronteira do domínio, este policiamento não é necessário.

4.1 Topologia

A topologia utilizada nas simulações é mostrada na figura 7. A escolha da topologia seguiu uma série de critérios, visando tornar os resultados os mais reais possíveis:

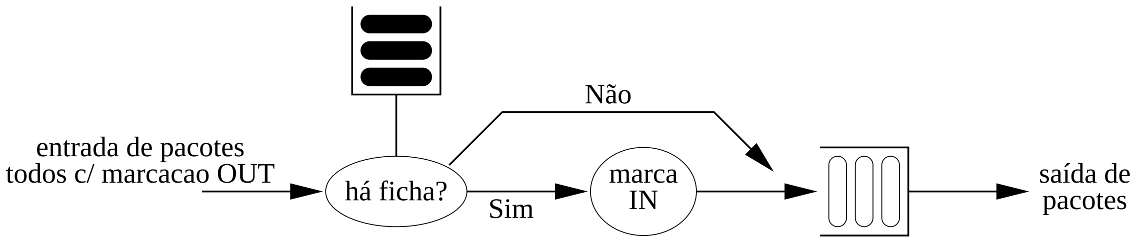


Figura 6: marcador para o serviço Assegurado.

- as conexões monitoradas (conexões 8-17) apresentam diferentes RTTs (*round-trip times*), com a finalidade de considerar o efeito deste parâmetro na banda passante obtida por um fluxo TCP. O RTT de cada conexão é variado através da escolha aleatória do retardo de propagação (entre 1ms e 20ms) das fontes ao nó 0.

- os valores dos RTTs foram escolhidos de forma que os fluxos TCP consigam atingir uma vazão considerável (o produto retardo*banda passante).

- geração de tráfego no caminho reverso dos fluxos monitorados de forma que os reconhecimentos (*ACKs*) destes fluxos sofram os efeitos da mistura com um tráfego real. Um desses efeitos é a compressão dos *ACKs*, ou seja, os *ACKs* chegam em rajadas devido às filas encontradas no caminho reverso. Isto pode causar a injeção de pacotes pelo emissor numa taxa maior do que a rede pode suportar. As setas da figura 7 indicam as direções dos fluxos gerados.

- criação do efeito de agregação, ou seja, os enlaces de acesso têm uma capacidade maior do que aquela do enlace de gargalo (*bottleneck link*), de modo que rajadas se formem neste último enlace. Na topologia usada na simulação, o enlace de gargalo é aquele entre os nós 1 e 2.

4.2 Tráfego de melhor-esforço com controle de congestionamento

Nesta simulações, os tráfegos de melhor esforço que competem com o tráfego do serviço Assegurado é uma mistura de tráfegos que utilizam controle de congestionamento fim-a-fim. Estes tráfegos são de longa-duração (FTP) e de curta-duração (HTTP). Numa primeira simulação foi avaliado a justiça no compartilhamento da banda passante do serviço Assegurado, quando utilizado por 10 conexões TCP, de TCP1 a TCP10, conectadas do nó 8 até ao 17. Cada conexão i tem um perfil de serviço igual a p_i que obedece a equação 1. Para checar a conformidade do tráfego gerada por cada conexão TCP foi utilizado um *leaky-bucket* com um tamanho do balde de 20 pacotes (ou segmentos TCP), onde cada segmento tem um tamanho de 1000 bytes. Foram utilizados os seguintes parâmetros para as filas *IN* e *IN+OUT*, respectivamente: [15,30,0.002,0.02] e [7,15,0.002,0.1].

$$p_i = i * p_1, \quad \text{onde } i = 1..10 \tag{1}$$

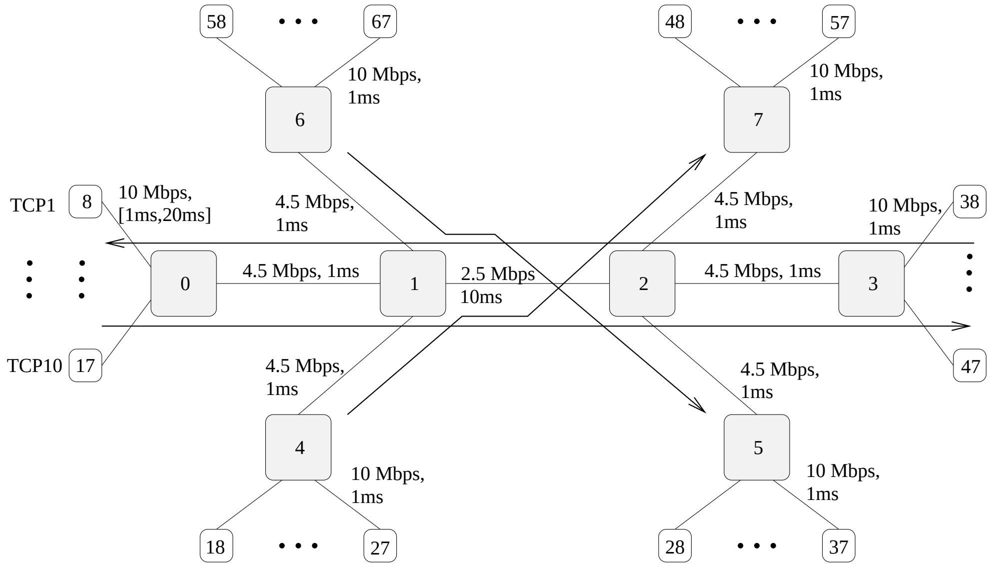


Figura 7: topologia utilizada.

Na curva da figura 8 é mostrada a vazão (*goodput*) obtida pelas conexões com o menor e o maior perfil de serviço, TCP1 e TCP10 respectivamente, em função da banda passante reservada. A banda passante total é mostrada como uma porcentagem da capacidade do enlace de gargalo. Para aumentar esta banda passante foi variado o valor do perfil de serviço de cada conexão de acordo com a equação 1, fazendo variar o valor de p_1. Nesta curva é também mostrado a banda passante justa que deveria ser alocada pra cada uma destas conexões. O cálculo deste valor é feito através da equação 2. O resultado mostra que cada conexão obtem um banda passante maior do que a considerada justa. Para todas as outras conexões desta simulação foi observado o mesmo comportamento. Isto se deve ao fato de que o tráfego oportunista (marcado como OUT) acaba passando pela rede sem ser descartado, aumentando assim a vazão observada.

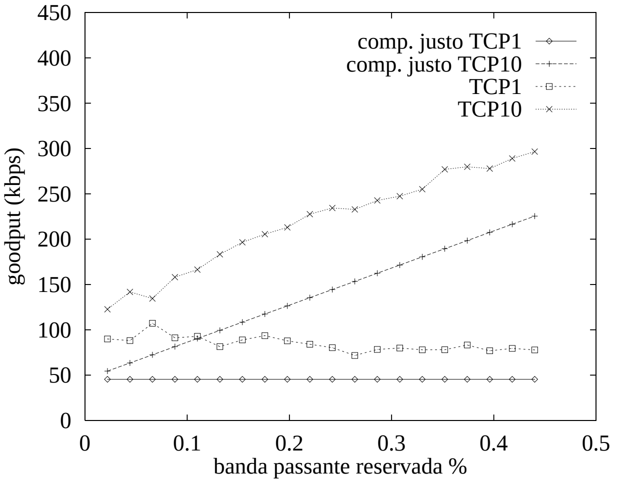


Figura 8: vazão das conexões TCP e justiça.

$$bpjusta_i = p_i + \frac{C_{gargalo} - \sum_{i=1}^{10} p_i}{\sum_{i=1}^{10} p_i} * p_1 \qquad (2)$$

Como aconselhado por Juha, a banda passante alocada para o serviço Assegurado não deve ultrapassar 40% da capacidade do enlace de gargalo. No caso desta simulação, isto é refletido pela equação 3.

$$\sum_{i=1}^{10} p_i < 0.4 * C_{gargalo} \quad \text{onde } C_{gargalo}\text{=2.5 Mbps} \qquad (3)$$

Numa segunda simulação foi variado o tamanho do balde do *leaky-bucket* que checa a conformidade do tráfego. A figura 9.a mostra a vazão obtida pelas conexões TCP1 até TCP5 e a figura 9.b mostra das conexões TCP6 até TCP10 em função do tamanho do balde em número de pacotes. O perfil de serviço de cada conexão é dado por $p_1 = 18kbps$, ou seja aproximadamente 40% da capacidade total do enlace de gargalo.

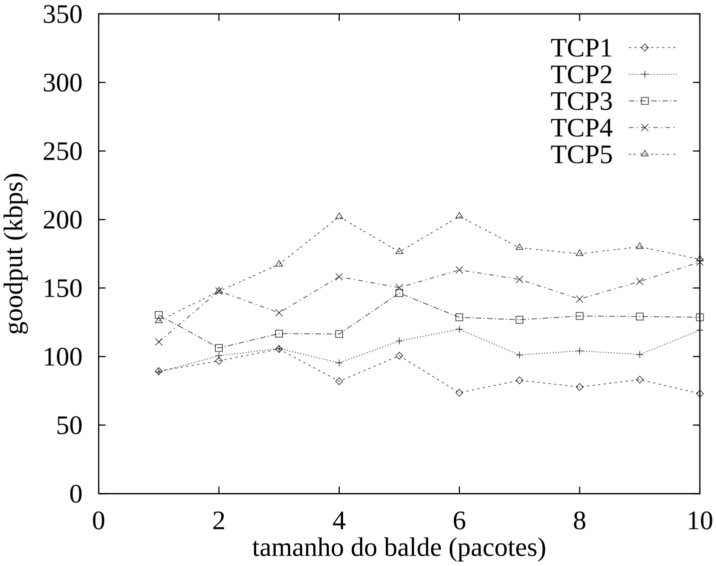
Os resultados mostram que a vazão das conexões com um maior perfil de serviço (TCP6-TCP10) é mais sensível ao tamanho do balde do que aquelas com um menor perfil de serviço. Somente a partir de cinco pacotes estas conexões atingem um valor estável. Quanto menor é o tamanho do balde maior é a probabilidade de haver perdas de créditos. Esta perda reduz a taxa de marcação efetiva do tráfego da conexão para um valor abaixo do perfil contratado. Nas conexões com um maior perfil de serviço, o balde é preenchido com uma maior taxa, aumenta ainda mais a perda de créditos. Quando o balde é aumentado, essas conexões voltam a obter uma taxa de marcação correspondente ao perfil contratado.

Os gráficos das figuras 10.a e 10.b mostram o número de pacotes *IN* e *OUT* de todas as conexões para um balde com tamanho de 1 e 5 pacotes, respectivamente. Estes resultados mostram que aumentando o tamanho do balde, as conexões com um maior perfil de serviço aumentam a taxa de marcação de pacotes *IN*. Isto indica que existe um favorecimento das conexões com uma maior taxa reservada em detrimento das conexões com menores taxas.

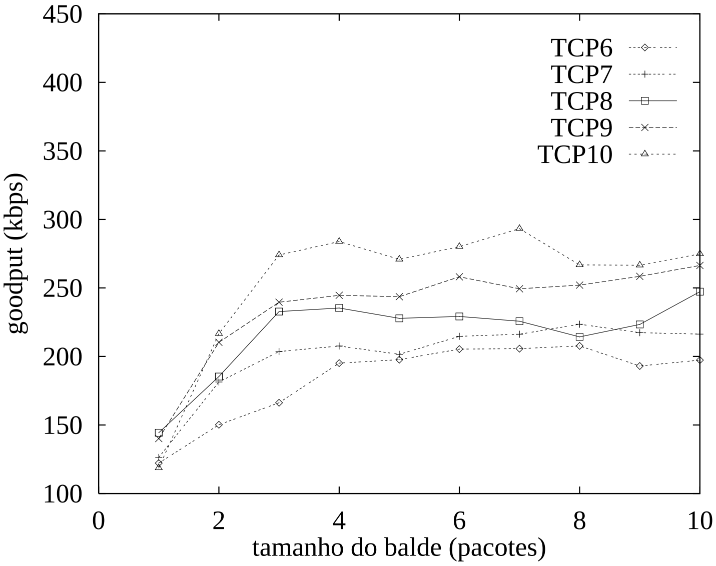
4.3 Tráfego de melhor-esforço sem controle de congestionamento

Nestas simulações, além da mistura de tráfego FTP e HTTP, são incluídos tráfegos de melhor esforço que não utilizam controle de congestionamento, representadas por fontes UDP que geram tráfegos em taxa constante ou em rajadas. Estas fontes, ditas não-cooperantes, não diminuem sua taxa de emissão em caso de congestionamento. O que pode agravar ainda mais o estado da rede.

Nas figuras 11.a e 11.b são mostradas as vazões obtidas pelas conexões TCP1 e TCP10 quando competindo com tráfegos de taxa constante e em rajadas, respectivamente. Nestas simulações foram utilizadas 10 fontes cujo tráfego percorrem o mesmo caminho das conexões TCP observadas, isto é, indo do nó 0 ao nó 3. A soma das taxas de emissão das fontes CBR é igual a 60% da capacidade total do enlace de gargalo, ou seja, igual a 1.5 Mbps. Estas fontes utilizam pacotes com tamanho de 1500 bytes. As fontes on-off são caracterizadas por um tempo de silêncio e de atividade de 0.6 e 0.4 ms, respectivamente. A taxa média de cada fonte on-off é



(a) TCP1-TCP5

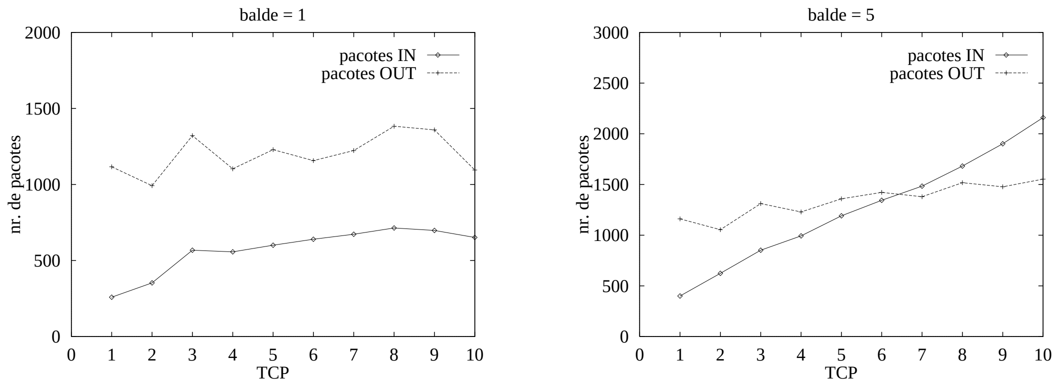


(b) TCP6-TCP10

Figura 9: vazão das conexões TCP em função do tamanho do balde.

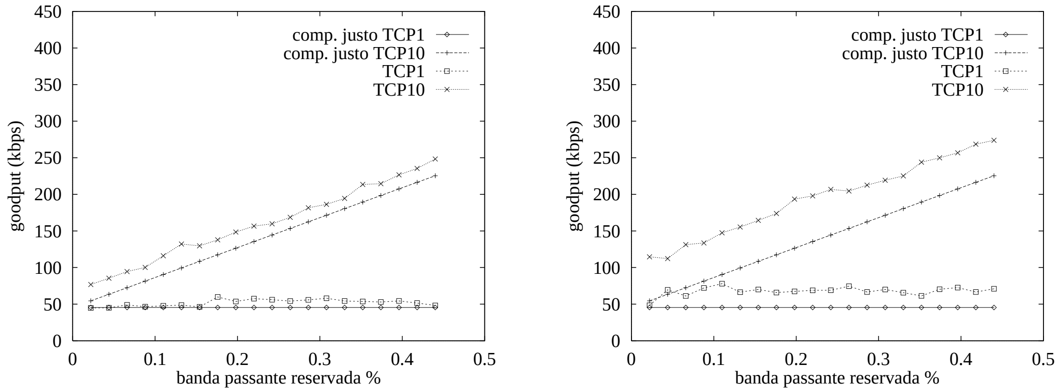
de 150 Kbps, totalizando novamente 60% da capacidade total do enlace de gargalo. Assim como nas fontes CBR, o tamanho do pacote utilizado é de 1500 bytes.

Os resultados mostram que mesmo quando competindo com tráfegos não cooperantes, o mecanismo RIO protege os pacotes *IN* dos fluxos com taxa reservada dos pacotes de melhor esforço, garantindo assim o perfil de tráfego contratado.



(a) balde=1 (b) balde=5

Figura 10: pacotes *IN* e *OUT* em função do tamanho do balde.



(a) tráfego *CBR* (b) tráfego *ON-OFF*

Figura 11: vazão das conexões TCP com fontes não cooperantes.

5 Conclusões

Neste artigo foi apresentado o modelo de serviço Assegurado, atualmente em ampla discussão no grupo de trabalho de Diferenciação de Serviços na Internet *DiffServ*. Para avaliar o desempenho de fluxos TCP atravessando um domínio DS que implementa este serviço, uma série de mecanismos, tais como a marcação de pacotes de acordo com perfis de serviço e o gerenciamento ativo de filas, foram implementados no simulador ns-2. Os resultados obtidos via simulação mostram que este serviço é capaz de oferecer garantias de QoS desde que a rede seja bem provisionada. Nas simulações realizadas, o tráfego Assegurado continua recebendo o perfil de serviço contratado, mesmo em presença de fluxos não cooperantes, ou seja, aqueles que não realizam um controle de congestionamento fim-a-fim. Dentre os mecanismos avaliados, estão o RIO e o *leaky-bucket* usado para verificar a conformidade dos pacotes. Simulação foram feitas para avaliar a influência do tamanho do balde na vazão obtida pelas conexões TCP. Como perspectivas para este trabalho estão a avaliação do serviço Assegurado para o transporte de voz na Internet e a implementação e a avaliação de um mecanismo de gerenciamento ativo de filas com mais de dois valores de preferência de descarte.

Referências

[1] R. Braden and D. Clark, "Integrated Services in the Internet Architecture: an Overview," *Internet RFC*, Jun. 1994. `rfc1633`.

[2] S. Blake, D. Black, M. Carlson, E Davies, Z. Wang, and W. Weiss, "An Architecture for Differentiated Services," *Internet RFC*, Dec. 1998. `rfc2475`.

[3] S. Deering, D. Estrin, S. Shenker, and D. Zappala, "RSVP: A New Resource ReSerVation Protocol," *IEEE Network Magazine*, pp. 8–18, Sept. 1993.

[4] L. Zhang, S. Berson, S. Herzog, and S. Jamin, "Resource ReSerVation Protocol (RSVP) – Version 1 Functional Specification," *Internet RFC*, Sep. 1997. `rfc2205`.

[5] J. Wroclawski, "The Use of RSVP with IETF Integrated Services," *Internet RFC*, Sep. 1997. `rfc2210`.

[6] K. Nichols, S. Blake, F. Baker, and D. Black, "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers," *Internet RFC*, Dec. 1998. `rfc2474`.

[7] V. Jacobson, K. Nichols, and K. Poduri, "An Expedited Forwarding PHB," *Internet draft*, Nov. 1998. `draft-ietf-diffserv-phb-ef-01`.

[8] J. Heinanen, F. Baker, W. Weiss, and J. Wroclawski, "Assured Forwarding PHB Group," *Internet draft*, Jan. 1999. `draft-ietf-diffserv-af-04`.

[9] Network Simulator – NS (version 2), `http://www-mash.cs.berkeley.edu/ns/`

[10] S. Floyd and V. Jacobson, "Random Early Detection Gateways for Congestion Avoidance," *IEEE/ACM Transactions on Networking*, vol. 1, no. 4, pp. 397–413, Aug. 1993.

[11] D. Clark and W. Fang, "Explicit Allocation of Best Effort Packet Delivery Service," *IEEE/ACM Transactions on Networking*, vol. 6, no. 4, pp. 362-373, Aug. 1998.