

CBPF - CENTRO BRASILEIRO DE PESQUISAS FÍSICAS

Rio de Janeiro

Notas Técnicas

CBPF-NT-012/00

dezembro 2000

**Modelos de Qualidade de Serviço
Aplicações em IP**

Nilton Alves Jr. & Kelly Soyan Pires Dominguez



MODELOS DE QUALIDADE DE SERVIÇO - APLICAÇÕES EM IP

Nilton Alves Júnior
naj@cbpf.br

Kelly Soyan Pires Dominguez
kelly@cbpf.br

Resumo

Este trabalho tem como função explicitar o conceito de Qualidade de Serviço sobre as aplicações em IP, abordando separadamente os modelos IntServ e DiffServ, juntamente com os protocolos e componentes de cada um destes. Serão vistas também as vantagens e desvantagens, permitindo uma comparação final de que modelo pode ser mais apropriado.

Palavras-chave:

Qualidade de Serviço, IntServ, DiffServ.

ÍNDICE

1 – INTRODUÇÃO.....	3
2 – <i>INTEGRATED SERVICES</i> – IntServ	4
2.1 – <i>RESOURCE RESERVATION PROTOCOL</i> – RSVP	5
2.2 – ROTINA DE CONTROLE DE ADMISSÃO	6
2.3 – CLASSIFICADOR.....	7
2.4 – ESCALONADOR.....	7
2.5 – DESVANTAGENS do IntServ.....	9
3 – <i>DIFFERENTIATED SERVICES</i> – DiffServ.....	10
3.1 – <i>DIFFERENTIATED SERVICE FIELD</i> – DS FIELD	10
3.2 – <i>SERVICE LEVEL AGREEMENT</i> – SLA	13
3.3 – <i>BANDWIDTH BROKER</i> – BB	14
3.3.1 – PROCESSO DE SINALIZAÇÃO DOS BBs	16
3.4 – DESVANTAGENS do DiffServ	18
4 – CONCLUSÃO	19
5 – REFERÊNCIAS	20

1 – Introdução

Devido ao crescimento da utilização de aplicações multimídia na *Internet*, certos recursos foram introduzidos tornando mais viável e segura a transmissão dos dados. Um desses recursos é *Quality of Service* – QoS, que se torna imprescindível quando se trata de uma aplicação de missão crítica, como por exemplo, a telemedicina.

Atualmente, na transmissão dos dados na *Internet*, é utilizada a filosofia *Best Effort*, que não provê nenhum tipo de garantia de que os pacotes enviados na rede chegarão ao seu destino.

Como muitos *hosts* estão conectados na rede ao mesmo tempo, os limites da banda de transmissão podem ser excedidos, isto é, os usuários compartilham a largura de banda com os fluxos de dados de outros usuários. De acordo com a quantidade de banda disponível e definição das rotas, os dados chegam ao seu destino. Entretanto, quando há congestionamento pacotes são descartados aleatoriamente, não garantindo que a aplicação seja executada com eficiência.

Por outro lado, com a introdução do recurso QoS podemos reservar banda para tipos diferentes de fluxo de dados, onde os pacotes não são mais descartados e a banda não excede valores pré-definidos. Por exemplo, se quisermos transmitir voz em tempo real, uma quantidade X de Mb/s será reservada para tal aplicação.

Dentro do QoS temos diferentes tipos de modelos propostos pelo ¹*Internet Engineering Task Force* – IETF, que se adequam de acordo com o tipo de aplicação e arquitetura da rede. Estes modelos são: *Integrated Service* – IntServ e *Differentiated Service* – DiffServ, respectivamente.

É possível também termos qualidade de serviço baseada no ATM (*Asynchronous Transfer Mode*), uma tecnologia que tem como aplicação nativa o QoS. Porém, devido ao fato de ser uma tecnologia altamente complexa, pode mostrar dificuldades quanto à implementação deste recurso.

¹ IETF – <http://www.ietf.org>

A seguir, nas sessões 2 e 3 abordaremos cada um dos modelos de qualidade de serviço.

2 – INTEGRATED SERVICES – IntServ

Este modelo de qualidade de serviço é caracterizado essencialmente pela reserva de recursos (largura de banda, atraso e variação do atraso ou *jitter*), antes do estabelecimento da comunicação, eliminando a idéia de *best effort*. Este serviço utiliza o protocolo de sinalização RSVP, que será abordado com mais detalhes no próximo subitem. Durante a sinalização existe troca de mensagens de controle entre emissor e receptor de forma que num determinado período de tempo possamos alocar uma faixa de banda para a transmissão dos dados.

Neste modelo temos alocação para dois tipos de serviços, além do *Best Effort*:

- ✓ *Serviços Garantidos* – aplicações que necessitam de um atraso constante. Se aproxima da idéia de termos um circuito virtual dedicado. Por exemplo, uma ligação telefônica.
- ✓ *Serviços de Carga Controlada* – aplicações que necessitam de segurança e limites para o *jitter*.

Aplicações que exigem esses tipos de serviço devem configurar caminhos e reservar recursos antes da transmissão dos dados.

A implementação do IntServ é feita por quatro componentes:

- ✓ protocolo de sinalização (RSVP),
- ✓ rotina de controle de admissão,
- ✓ classificador,
- ✓ escalonador de pacotes.

Esses componentes têm por função organizar os pacotes de forma que a qualidade do serviço seja assegurada.

2.1 - RESOURCE RESERVATION PROTOCOL (RSVP)

O RSVP é usado para gerenciar recursos ao longo do caminho no qual deseja-se utilizar aplicações que necessitem de QoS. Ele não realiza transporte de dados, é apenas um protocolo de sinalização que atua juntamente com o *Internet Control Management Protocol* - ICMP e *Internet Group Management Protocol* - IGMP.

O processo de sinalização se dá antes da transmissão dos dados e é renovado sempre que necessário. Para haver a requisição dos recursos, existem mensagens que são trocadas entre o receptor e o transmissor, são elas: *PATH* e *RESV*.

Apresentaremos aqui o processo de sinalização de uma forma simplificada, de acordo com a figura 1:

A mensagem *PATH* (*unicast* ou *multicast*) é enviada pelo transmissor, informando para o endereço de destino especificações de tráfego (largura de banda, atraso e *jitter*). Cada roteador ao longo do caminho estabelece, então, um estado de *PATH*. As mensagens desse tipo armazenam o estado de cada nó (cada roteador), por onde elas transitaram. Fornecem também o endereço do nó anterior. Para que isto realmente aconteça é necessário que todos os roteadores tenham RSVP habilitado.

Quando a mensagem *PATH* chega no receptor, este analisa as informações contidas na mensagem e seleciona os parâmetros de reserva desejados. O procedimento de reserva de recursos se inicia através da mensagem *RESV*. Essa mensagem é enviada de volta aos mesmos roteadores, estabelecendo um estado de *RESV*. Além das especificações do tráfego contidas no estado de *PATH*, o *RESV* contém especificações de pedido, que indicam que tipo de serviço, dentro do IntServ, está sendo requerido (carga controlada ou serviço garantido) e

especificações de filtro, que caracterizam os pacotes para os quais a reserva está sendo feita. Cada roteador ao longo do caminho pode aceitar ou não as requisições da mensagem *RESV*. Se a mensagem for rejeitada, o roteador enviará uma mensagem de erro para o receptor e o processo de sinalização terminará.

Quando o último roteador recebe a mensagem *RESV*, inicia-se então a comunicação propriamente dita. Temos como último roteador o mais próximo do transmissor.

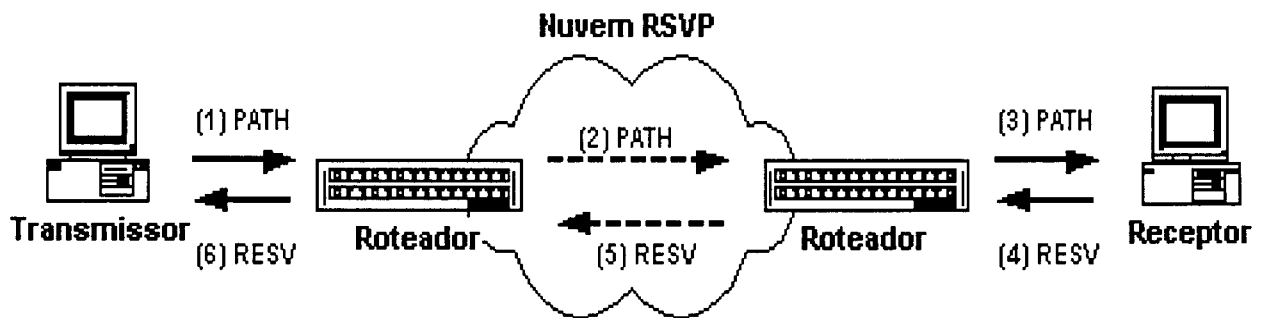


Figura 1

Como já foi dito anteriormente o RSVP trabalha em conjunto com outros componentes (controle de admissão, classificador e escalonador de pacotes) que atuam tanto nos elementos finais, transmissores e receptores, como nos roteadores.

2.2 - Rotina de controle de admissão

O controle de admissão tem somente a função de determinar se um fluxo de dados poderá ser aceito ou não, de acordo com a banda disponível.

Este componente é requisitado de forma que sua decisão não interfira nos fluxos previamente aceitos pelo roteador, isto é, os fluxos de dados que já foram aceitos não serão modificados em virtude dos outros que ainda serão estabelecidos.

2.3- Classificador

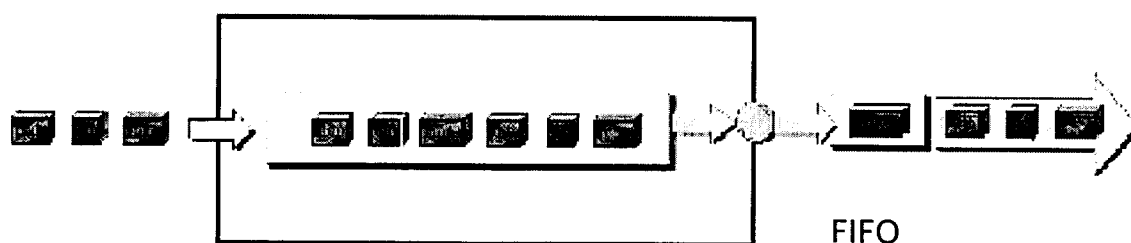
Com a introdução dos parâmetros de QoS, foi necessária uma forma de classificação mais específica dos pacotes. Além de analisarmos o endereço do destino, levamos também em consideração o número da porta e protocolo. Poderemos tomar como exemplo um fluxo de áudio que seria reconhecido por uma porta particular.

Os pacotes são marcados de modo que possamos reservar banda para determinada aplicação, esta possuindo uma prioridade na fila dentro do roteador. Quem cuida das prioridades da fila é o escalonador, que implementa algoritmos que selecionam a ordem com que os pacotes serão atendidos primeiro.

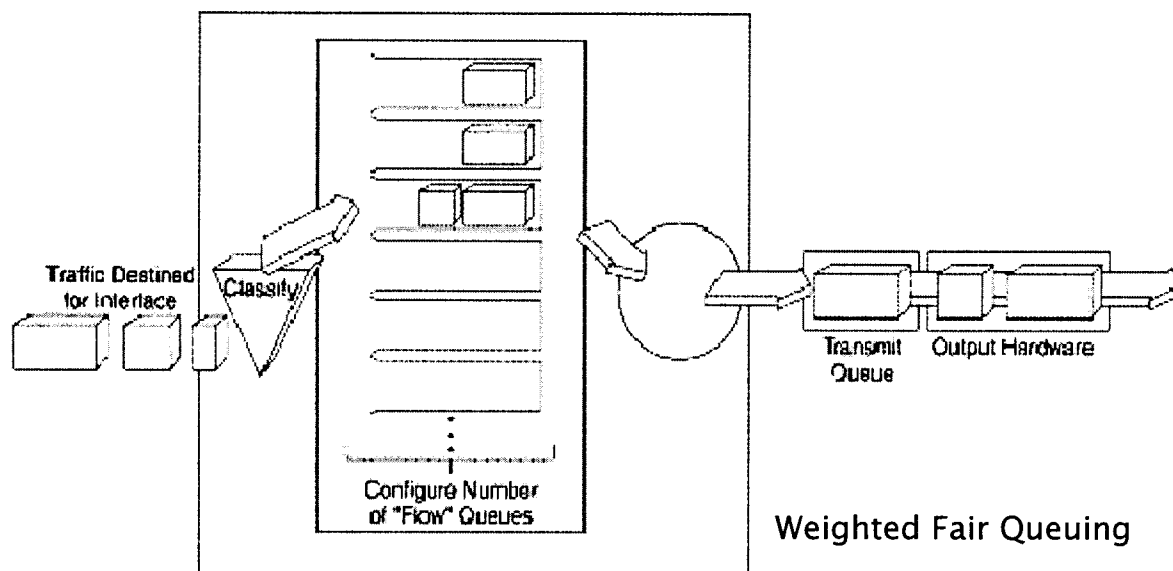
2.4-Escalonador

Como foi citado acima, o papel do escalonador é estabelecer políticas de enfileiramento e prevenção de congestionamento nas interfaces dos roteadores e *switches* nível 3, aqueles que também roteiam, para atender as prioridades do fluxo. O escalonador trabalha com algoritmos que fazem tais implementações de acordo com a necessidade de QoS para determinados serviços.

O mecanismo mais conhecido é o FIFO - *First In First Out*, onde os pacotes são tratados de acordo com a ordem de chegada. Uma fila FIFO é um mecanismo de repasse, não implementando nenhum tipo de classificação. É fácil percebermos, então, que quando estamos utilizando qualidade de serviço, este tipo de mecanismo não é adequado.



Outro algoritmo que também merece ser citado é o WFQ - *Weighted Fair Queueing*, associar pesos a cada tipo de fluxo de acordo com as prioridades de cada um. Ele trabalha da seguinte forma: o WFQ coloca para o início da fila o tráfego que tem maior prioridade, reduzindo o tempo de resposta desse fluxo. Ao mesmo tempo, no WFQ os fluxos compartilham banda com outros fluxos de menores prioridades, porém alocando uma largura de banda menor, já que os de menor prioridade têm também menor peso junto ao WFQ. Este algoritmo se adapta automaticamente às mudanças das condições de tráfego.

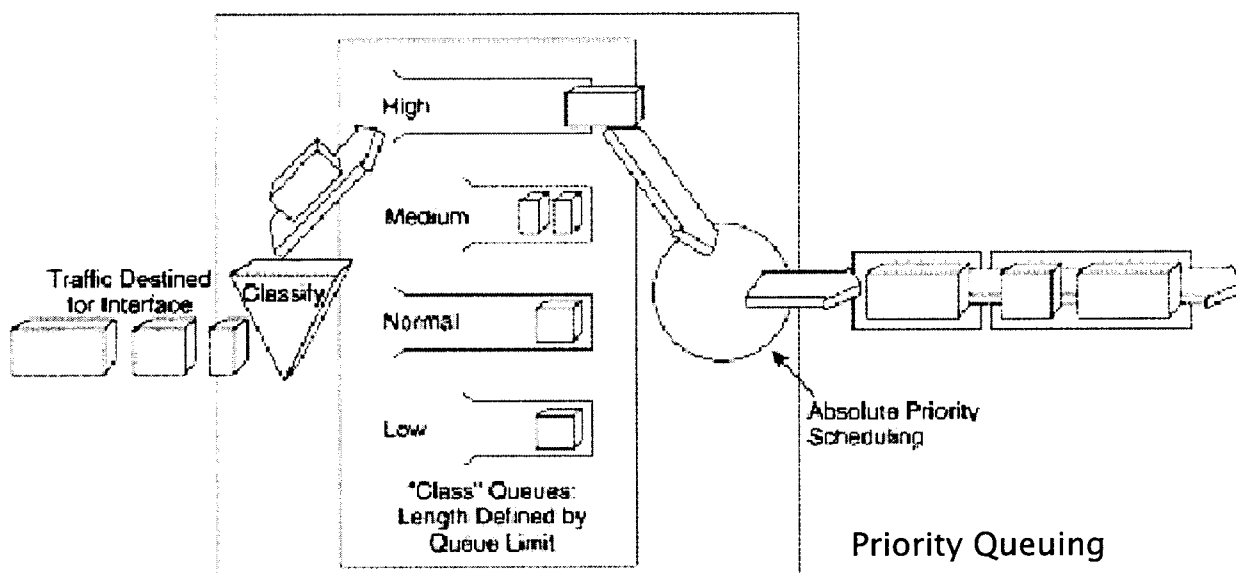


Podemos também citar o PQ - *Priority Queueing*, onde o tráfego de entrada é classificado em quatro níveis de prioridade: alta, média, baixa e normal. Os pacotes que não são marcados levam configuração padrão, isto é, são tratados de acordo com a prioridade normal.

Neste mecanismo o tráfego classificado e marcado como prioritário tem preferência absoluta em relação aos outros fluxos. Esta é uma das desvantagens do PQ, pois isso pode causar um aumento de variação de atraso e atrasos consideráveis em aplicações de menor prioridade. Numa situação extrema pode acontecer até de um fluxo com menor prioridade nunca chegar a ser enviado se o fluxo de maior prioridade ocupar toda largura de banda. Isso ocorre em conexões de baixa velocidade.

Outra desvantagem do PQ é que se um fluxo não receber classificação ele pode também não ser enviado. Por isso a necessidade da habilitação de uma fila padrão, isto é, com prioridade normal .

A classificação de um fila PQ pode ser por protocolo (IP, IPX, DecNet, SNA, etc), por interface de entrada ou por *access-list*.



2.5- DESVANTAGENS do IntServ

- ✓ A quantidade de informação de estado aumenta com o número de fluxos exigindo enorme espaço de armazenamento e gerando sobrecarga de processamento nos roteadores.
- ✓ Todos os roteadores, transmissores e receptores devem implementar RSVP, controle de admissão, classificação e escalonamento de pacotes.

3 – DIFFERENTIATED SERVICES (*DiffServ*)

Devido a problemas encontrados com a implantação do IntServ, o IETF introduziu o DiffServ, um modelo onde os pacotes são previamente marcados, de acordo com os tipos de serviços desejados.

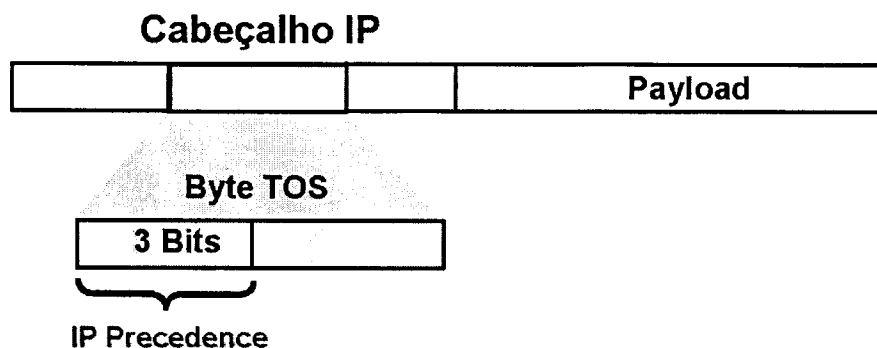
Essa marcação pode ser feita tanto pelo administrador da rede (informando quais pacotes receberão quais marcações) quanto pela habilitação de qualquer protocolo de sinalização que implemente QoS.

3.1 – Differentiated Service Field (*DS – Field*)

No cabeçalho do pacote IP existe um campo de oito *bits*, anteriormente chamado de *Type of Service – ToS*, e que passou a ser chamado de *DS – Field*, em virtude da ampliação dos serviços e do tratamento que pode ser dado a ele. É no *DS – Field* que são codificadas as classes para diferenciação de serviços.

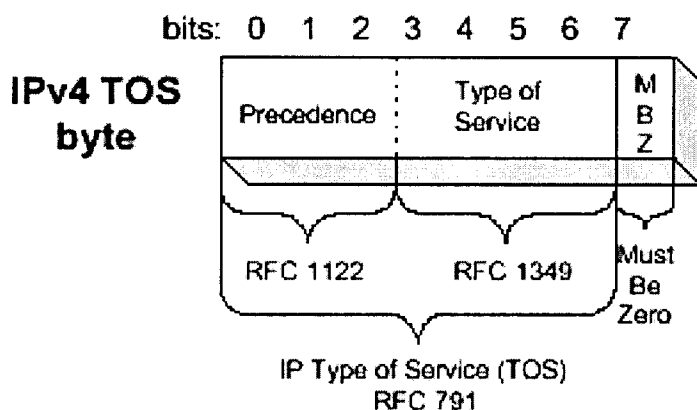
Na verdade, o ToS, que foi inicialmente definido e reservado para indicar tipos de serviços nunca foi utilizado de fato para nenhuma implementação. Com a introdução da Qualidade de Serviço foi necessário um tratamento mais específico, onde os pacotes são classificados de forma que agora o ToS, dentro do pacote IP, tenha função de explicitar os parâmetros necessários para cada serviço requerido, por exemplo: o atraso e o *jitter* sendo marcados previamente nos pacotes.

Podemos então dividir o *byte* do ToS no pacote IP em: *IP Precedence*, *TOS Field* e *MBZ (must be zero)*.



O *IP Precedence* são três *bits* que podem ser classificados de 0 a 7 de acordo com a prioridade do fluxo de pacotes. Isto é: se um pacote tem prioridade 7 (serviço de missão crítica), e outro com prioridade 5, com certeza o de maior prioridade será atendido. Outro caso é quando temos um pacote marcado com valor zero: este receberá prioridade mais baixa, podendo nunca ser atendido.

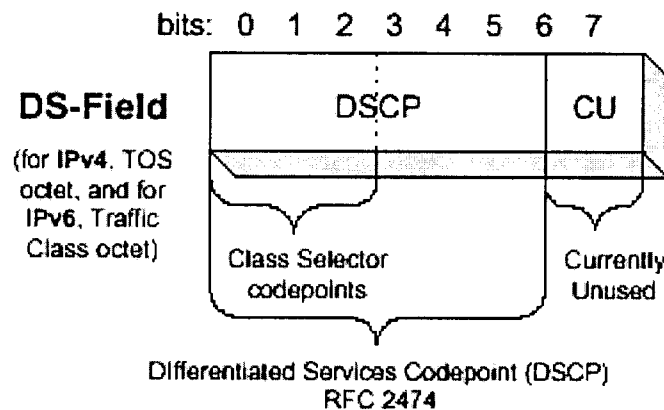
Temos também mais quatro *bits* reservados para o *ToS field*, que vão tratar exatamente de: *delay*, *throughput* e *reliability*. Sendo que os *bits* 6 e 7 do *byte* do ToS quase não são usados. Contudo, podem servir também para aplicações de controle e gerência da rede.



Como foi citado acima o bit 7 não é usado, por isso o nome de MBZ (*must be zero*).

Paralelamente, devemos analisar o *DS - Field* da seguinte forma: cada campo desse tipo especifica um tratamento diferente de encaminhamento, de acordo com sua classe de serviço. O *DS - Field* possui dois campos: DSCP e CU.

O caminho é marcado através do *DSCP - Differentiated Selector Codepoints*. O DSCP preserva o IP *Precedence* e especifica o comportamento do pacote nos *hops* (PHB - *Per Hop Behavior*).



Existem dois tipos de classificação dentro do DiffServ:

- ✓ BA - *behavior aggregate*, baseado somente no *DS codepoint*.
- ✓ MF - *Multi - field*, baseado em parâmetros como: endereço do destino, da fonte, número da porta e a própria classificação do *DS - Field*.

O DiffServ parte do princípio de que domínios adjacentes tenham acordo sobre os serviços disponibilizados. Um domínio é um conjunto de nós sob uma mesma gerência.

Os clientes podem marcar o campo DS de pacotes individuais para indicar o serviço desejado, ou podem ser marcados pelo roteador de borda e assim mandados para o receptor.

No entanto, dessa forma não sabemos quanto de banda disponível nós temos para utilizar, já que não foi feita nenhuma alocação.

É possível que um pacote com *DS Field* marcado chegue a um roteador que não provê qualidade de serviço. Nesse caso, ele pode ser remarcado passando a ser um pacote de *best effort*, podendo ser descartado.

Para isso foi inserido um componente que gerencia os recursos do domínio, tendo como função básica controlar a largura de banda, políticas e prioridades dentro e entre as organizações. Este componente é o Controlador de banda (*Bandwidth Broker* – BB), do qual falaremos posteriormente.

3.2– SERVICE LEVEL AGREEMENT (SLA)

Antes de falarmos sobre *Bandwidth Broker* é importante ressaltarmos o componente *Service Level Agreement* – SLA, que o gerencia.

O componente SLA determina quais são as classes de serviços suportadas e a quantidade de tráfego entre os domínios.

É um acordo feito entre o transmissor e o receptor determinando os limites dos parâmetros utilizados na aplicação.

O componente SLA pode se dar de duas formas: estática ou dinâmica.

É chamado de estático quando negociado de forma regular, isto é, por um determinado tempo, um mês ou um ano, por exemplo. É chamado de dinâmico quando for necessário o uso de um protocolo de sinalização e controle para o gerenciamento da banda, por exemplo, RSVP, de forma que os parâmetros estabelecidos no contrato possam se desfazer com o final da aplicação que está sendo executada.

As regras de classificação, condicionamento e escalonamento usadas nos roteadores são determinadas também pelo componente SLA, assim com o espaço nos buffers de cada roteador.

3.3 – BANDWIDTH BROKER – BB (Controlador de banda)

Quando há solicitação de um fluxo, o controlador de banda é um componente que verifica a disponibilidade de recursos e a autorização do cliente para a conexão dentro do domínio onde está sendo oferecida a qualidade de serviço.

Se encarrega também de fazer as alocações necessárias para a comunicação dentro do seu domínio e faz requisições aos controladores adjacentes, caso o pedido seja para fora do domínio.

Esse processo de solicitação de alocação de recursos é contínuo entre eles até que se chegue ao domínio do receptor. Pode-se usar o RSVP para alocação de recursos entre BBs.

Cada controlador de banda possui uma tabela de políticas estabelecidas pela SLA, que é consultada a cada solicitação de QoS que o mesmo recebe. Isto é feito por parte dos controladores vizinhos ou de outros domínios.

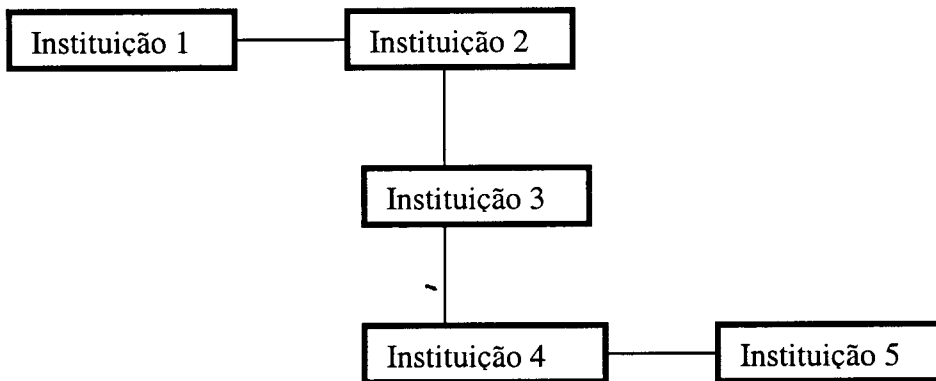
O BB deve operar tanto em intradomínio quanto interdomínio, sendo limitado pelas políticas, que dizem quanto dos recursos serão utilizados e quais usuários, do seu domínio, poderão usar.

Segue abaixo um exemplo de tabela estabelecida pelo componente SLA, que é consultada pelos Controladores de banda:

<i>Parceiro</i>	<i>REGRA</i>	<i>Total de banda</i>	<i>Total de uso</i>
Instituição 3	< 50 OK	100K	0
Instituição 1	Consulta	100K	20K

Exemplo: a Instituição 1 quer transmitir voz para Instituição 5.

Caso esta tabela esteja em algum domínio entre esses dois (Instituição2), qualquer solicitação de menos de 50Kbps feita para a Instituição 3 é aceita sem a necessidade prévia de consulta a mesma. Solicitações para Instituição 1 precisam sempre de uma consulta ao controlador de banda da Instituição 2.



O ²QBone, órgão regulamentador da *Internet2*, sugere que o BB seja capaz de executar tais funções :

- ✓ meio pelo qual uma aplicação ou roteador possa notificar uma requisição de banda
- ✓ responder para a aplicação ou roteador depois de ter configurado os roteadores para a requisição do QoS
- ✓ rejeitar a solicitação de banda
- ✓ reconfigurar roteadores
- ✓ manipular aplicações que finalizam o uso de uma faixa de banda e torná-la disponível

É responsabilidade também do controlador de banda configurar os PHBs nos roteadores. PHB é um comportamento de repasse que direciona os pacotes para filas específicas de acordo com suas prioridades, estabelecidas pela SLA.

² QBone – <http://qbone.internet2.edu>

Pode existir mais de um controlador de banda atuando num mesmo domínio, porém só um deles pode ser responsável pela comunicação entre controladores de banda de domínios adjacentes. Internamente, o controlador se comunica com os usuários ou controladores de suas sub-redes. Essa comunicação é basicamente para receber requisições e processá-las. Já com os roteadores, os controladores de banda precisam estabelecer comunicação para efeitos da configuração e gerência.

3.3.1- PROCESSO de SINALIZAÇÃO dos BBs

Quando tratamos de domínios diferentes, todos os controladores de banda do caminho precisam ser consultados da requisição que foi feita.

Entre os controladores de banda, temos processos de sinalização para alocarmos recursos. Existem dois tipos de sinalização: sinalização fim-a-fim e a sinalização com resposta imediata. Pode também ser usada uma combinação dos dois processos de sinalização.

SINALIZAÇÃO FIM-A-FIM:

Os controladores de banda são consultados um a um ao longo do caminho, antes que o usuário, que solicitou o recurso, seja informado do resultado.

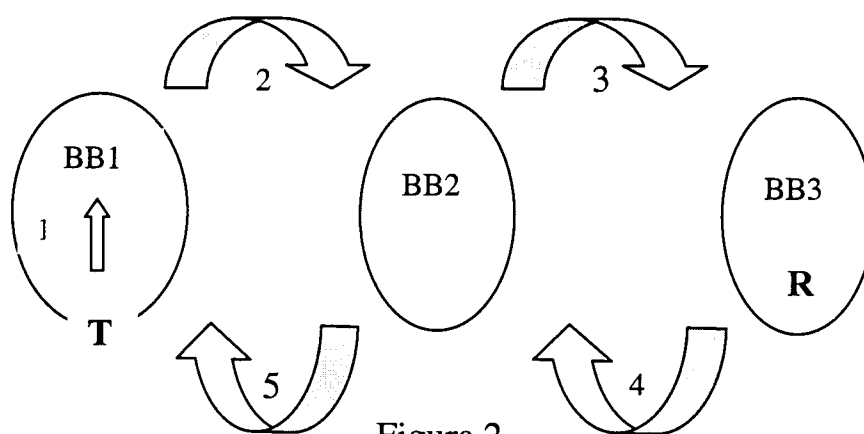


Figura 2

Procedimentos de sinalização:

1. T consulta seu BB1 (controlador de banda 1) de acordo com a requisição feita.
2. BB1 consulta BB2, que é o controlador de banda de um domínio adjacente ao BB1, também de acordo com a requisição.
3. Esse procedimento é repetido para todos os BBs subseqüentes.
4. Por fim, BB3 (presente no último nó) responde que a requisição foi aceita.
5. BB2 responde ao BB1 e este informa ao T que tudo está OK, permitindo, então que a comunicação seja estabelecida.

Se houver algum erro no caminho, uma resposta é retornada do controlador de banda que “falhou”, não sendo consultados os controladores subseqüentes (figura 2).

SINALIZAÇÃO COM RESPOSTA IMEDIATA:

Este tipo de sinalização faz com que a comunicação seja antecipada ao contrário da sinalização fim-a-fim, onde o processo de sinalização é todo estabelecido e depois é que se dá a transmissão de dados. Contudo, devido a esse fato é menos segura se a transmissão de dados tiver que ser garantida.

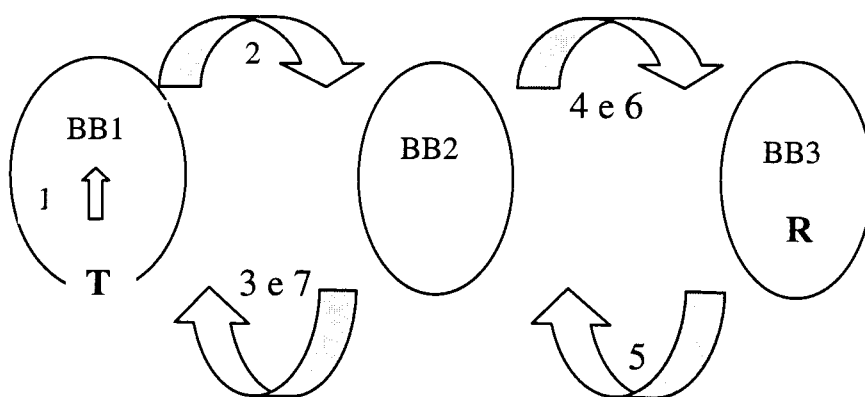


Figura 3

Procedimentos de sinalização: (figura 3)

1. T consulta seu BB1.
2. BB1 consulta BB2 de acordo com a requisição feita.
3. BB2 responde imediatamente ao BB1, que informa a T que BB2 aceitou a requisição. Assim o usuário passa a transmitir seus dados antes que o BB2 sinalize para o BB3.
4. BB2 consulta BB3.
5. BB3 informa ao BB2 que a requisição feita pode ser atendida.
6. Os dados são repassados de 2 para 3
7. BB2 informa ao BB1 que BB3 está ok.

Através do uso de mecanismos de classificação, condicionamento e escalonamento, os serviços no ambiente DiffServ podem ser classificados como:

- ✓ Serviços assegurados - para provedores de serviços que precisam de segurança em momentos de congestionamento, bem como para aplicações que exigem maior confiabilidade do que a oferecida pelo *best effort*.
- ✓ Serviços *premium* - aplicações que exijam serviços com baixo atraso e baixo *jitter*.

3.4 - DESVANTAGENS do DiffServ

- ✓ Os serviços diferenciados dão segurança ao desempenho das aplicações somente em termos relativos, assim, é mais confiável aquele que possui maior prioridade.
- ✓ Dependendo do tráfego na rede, ambas as aplicações podem ter um desempenho muito abaixo das suas reais necessidades.

4 - CONCLUSÃO

Os roteadores núcleo necessitam apenas implementar classificações de repasse (PHB). Dessa forma, operações de classificação e condicionamento no DiffServ são necessárias somente nos dispositivos de borda, não consumindo tanto o processamento dos nós internos quanto no IntServ. Neste modelo, todos os roteadores têm que utilizar classificação, condicionamento e escalonamento.

Outro ponto a favor do DiffServ é que temos um número limitado de classes de serviços, indicadas pelo *DS - Field*.

Uma vez que o serviço é alocado, a quantidade de informação de estado é proporcional ao número de classes, consumindo menor espaço nos *buffers* dos roteadores; diferente do que acontece no IntServ, onde a quantidade de informação de estado é proporcional ao número de fluxos.

A sinalização do *PATH* armazena o estado do fluxo em um roteador num determinado momento, e esta informação é repassada para os outros roteadores, ocupando lugar no *buffer*. Logo, o fluxo aumenta de acordo com os dados que trafegam na rede.

O DiffServ é o modelo mais apropriado para o uso da Qualidade de Serviço, devido ao baixo consumo de processamento dos roteadores e utilização de algoritmos complexos de controle de admissão, classificação e escalonamento somente nos roteadores de borda.

5 – REFERÊNCIAS

- “Protocolos TCP/IP” – Nota Técnica escrita por Nilton Alves Júnior. CBPF – NT – 004/00.
- “Qualidade de Serviço na *Internet*”, Ana Paula Silva dos Santos, NewsGeneration, novembro de 1999.
www.rnp.br/newsgen/9911/qos.shtml
- “O Controlador de banda”, Ana Paula Silva dos Santos, News Generation, maio de 2000, <http://www.rnp.br/newswgen/0005/bb.shtml>
- “Qualidade de Serviço em VoIP – Parte I”, Adailton J.S.Silva, News generation, maio de 2000. http://www.rnp.br/newsgen/0005/qos_voip1.shtml
- “O protocolo RSVP e o desempenho das aplicações multimídia”.Ana Luísa Pereira Schimidt, News Generation, maio de 2000.
www.rnp.br/newsgen/0005/rsvp.shtml
- “Perspectivas sobre qualidade de serviço nos protocolos da *Internet*–Estudo de caso. Aplicações de vídeo sob demanda”, Aline C.Viana, Anibal S. Jukemura, Daniela A. Xavier, Kleber Cardoso, News Generation, julho de 2000.
<http://www.rnp.br/newsgen/0007/art1.shtml>
- “QoS Protocols & Architectures” – white paper.
http://www.qosforum.com/white-papers/qosprot_v3.pdf
- “Quality of Service (QoS) Networking”
http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/qos.htm#25991
- IP QoS FAQ – <http://www.qosforum.com>
- DiffServ FAQ
http://www.cisco.com/warp/public/cc/pd/iosw/ioft/ioqo/tech/dffs_qa.htm