UNIVERSIDADE FEDERAL DE LAVRAS
DEPARTAMENTO DE CIÊNCIA DA COMPUTAÇÃO
PÓS-GRADUAÇÃO ADMINISTRAÇÃO EM REDES LINUX

MARCOAURÉLIO DE ARAÚJO LEAL

QoS – QUALIDADE DE SERVIÇO EM TCP/IP

Monografia apresentada ao Departamento de Ciência da Computação da Universidade Federal de Lavras, como parte das exigências do Curso de Pós-Graduação Lato Sensu "Administração de Redes Linux", para a obtenção do título de especialista.

Orientador:
Prof. Fernando Cortez Sica

LAVRAS
MinasGerais - BRASIL
2004

UNIVERSIDADE FEDERAL DE LAVRAS
DEPARTAMENTO DE CIÊNCIA DA COMPUTAÇÃO
PÓS-GRADUAÇÃO ADMINISTRAÇÃO EM REDES LINUX

MARCOAURÉLIO DE ARAÚJO LEAL

QoS – QUALIDADE DE SERVIÇO EM TCP/IP

Monografia apresentada ao Departamento de Ciência da Computação da Universidade Federal de Lavras, como parte das exigências do Curso de Pós-Graduação Lato Sensu "Administração de Redes Linux", para a obtenção do título de especialista.

Aprovado em 25 de Julho de 2004.

_____
Prof. Luiz Henrique Andrade Correia

_____
Prof. Wilian Soares Lacerda

_____
Prof. Fernando Cortez Sica (Orientador)

LAVRAS
Minas Gerais - BRASIL
2004

AGRADECIMENTOS

Gostaria de endereçar meus agradecimentos para meus pais. Aos professores do ARL pela competência de administrar um curso a distância com muita qualidade. Aos alunos da turma ARL2003S1 pelo imenso entusiasmo e companheirismo que nos impulsionaram a cada módulo e em especial aos amigos Alexandre Rossi, Cristiane Jorge e Magna Fonseca pela força e apoio nos momentos difíceis do curso.

A Deus por sua contínua proteção

LAVRAS
Minas Gerais -BRASIL
2004

DEDICATÓRIA

Para minha esposa Hellena Christina, e filhos Gabriela e Rafael por todo amor, carinho, imensa compreensão e suporte nas minhas ausências para essa grande realização.

LAVRAS
Minas Gerais -BRASIL
2004

RESUMO

As redes IP constituem o grande universo de milhões de computadores interligados em todo o mundo com uma expectativa constante de crescimento. Estas redes se desenvolveram com facilidade devido o crescimento da Internet e pela homologação do TCP/IP como protocolo de suporte às aplicações em redes e não há nenhum aceno em relação a mudanças deste panorama devido à grande massa de computadores usando TCP/IP nas suas comunicações, sejam elas caseiras ou corporativas. Sendo assim, o IP torna-se o padrão universal de suporte para aplicações, pois está presente em milhões de máquinas espalhadas por todo o mundo.

As redes TCP/IP foram desenvolvidas com o discurso de que poderiam ser usadas sobre qualquer tipo de meio físico, sendo estes de qualquer tecnologia, apresentando ou não confiabilidade, com alto ou baixo desempenho. Como o TCP/IP é um protocolo simples, ele tem algumas restrições como, por exemplo, a falta de garantia no trânsito de pacotes, atrasos, etc.

Com o crescimento e diversificação das aplicações (voz, multimídia, vídeo-conferência, etc) sobre IP, precisou-se avaliar as limitações do IP, buscando alternativas para adequá-lo à nova realidade, pois a banda está compartilhada com um número cada vez maior de usuários podendo ocorrer congestionamento e possíveis perdas de pacotes.

Para que se obtenha uma garantia de que o serviço será realizado é preciso aplicar tecnologias que permitam atingir um nível de tráfego satisfatório e confiável para os dados e aplicações.

O objetivo desta monografia é mostrar alternativas que viabilizem uma qualidade no serviço sobre IP, discutindo os parâmetros, os protocolos e os mecanismos envolvidos com a garantia de qualidade de serviço com ênfase nas redes de pacotes tipo IP, mostrando vantagens e desvantagens das tecnologias existentes para cada necessidade.

LAVRAS
Minas Gerais -BRASIL
2004

ÍNDICE

LISTA DE FIGURAS

INTRODUÇÃO

Inicialmente no capítulo 1 apresenta um breve histórico da origem do protocolo TCP/IP e uma visão geral dos modelos de referências ISO/OSI e TCP/IP.

O segundo capítulo apresenta definições sobre QoS e aborda suas aplicações. A análise dos serviços Qos é visto no capítulo 3, este apresenta a garantia de QoS , serviços diferenciados e a funcionalidade dos sistemas de QoS. Para finalizar no capítulo 4 foram feitas as conclusões finais.

As redes IP constituem o grande universo de milhões de computadores interligados em todo o mundo com uma expectativa constante de crescimento. Estas redes se desenvolveram com facilidade devido o crescimento da internet e pela homologação da suíte de protocolos TCP/IP como suporte às aplicações em redes. Não há nenhum aceno em relação a mudanças deste panorama devido à grande massa de computadores usando TCP/IP nas suas comunicações, sejam elas caseiras ou corporativas. Sendo assim, o IP torna-se o padrão mundial de suporte para aplicações, pois está presente em milhões de máquinas espalhadas por todo o mundo.

As redes TCP/IP foram desenvolvidas com o discurso de que poderiam ser usadas sobre qualquer tipo de meio físico, sendo estes de qualquer tecnologia, apresentando ou não confiabilidade, com alto ou baixo desempenho. Como o TCP/IP é um protocolo simples, ele tem algumas restrições como, por exemplo, a falta de garantia no trânsito de pacotes, atrasos, e assim por diante.

Com o crescimento e diversificação das aplicações (voz, multimídia, vídeo-conferência, etc) sobre IP, precisou-se avaliar as limitações do IP, buscando alternativas para adequá-lo à nova realidade, pois a banda está

compartilhada com um número cada vez maior de usuários podendo ocorrer congestionamento e possíveis perdas de pacotes.

Para que se obtenha uma garantia de que um determinado serviço esteja disponível é preciso aplicar tecnologias que permitam atingir um nível de tráfego satisfatório e confiável para os dados e aplicações.

O objetivo desta monografia é mostrar alternativas que viabilizem uma qualidade no serviço sobre IP, discutindo os parâmetros, os protocolos e os mecanismos envolvidos com a garantia de qualidade de serviço com ênfase nas redes de pacotes tipo IP, mostrando vantagens e desvantagens das tecnologias existentes para cada necessidade.

CAPÍTULO I – ESTUDO BÁSICO DOS PROTOCOLOS TCP/IP

1.1 - Histórico do TCP/IP

Nos anos 60, o principal setor estratégico americano, Department of Defense – DoD se interessou em um protocolo que estava sendo desenvolvido e utilizado pelas Universidades para interligação dos seus sistemas computacionais e que utilizava a tecnologia de chaveamento de pacotes. O interesse do DoD estava no desejo de manter a comunicação entre os diversos sistemas espalhados pelo mundo no caso de um desastre nuclear. O problema maior estava na compatibilidade entre os sistemas computacionais de diferentes fabricantes que possuíam diferentes sistemas operacionais, topologia e protocolos. A integração e compartilhamento dos dados passaram a ser um problema de difícil resolução.

Para solucionar esse problema foi criada a Advanced Research Projects Agency – ARPA que tinha como missão desenvolver tecnologias que pudessem ser usadas para fins militares. Como a ARPA não tinha à sua disposição cientistas e laboratórios de pesquisas, então subsidiava os projetos de empresas e universidades cujas idéias viessem de encontro com os objetivos da ARPA. (Tanenbaum, 1997)

Com essa atuação da ARPA, foi feita então uma aliança pelas universidades e fabricantes para o desenvolvimento de padrões de comunicação. Esta aliança especificou e construiu uma rede de teste de quatro nós, chamada ARPANET, e que acabou sendo a origem da internet hoje. Na década de 70, esta rede inicial evoluiu. Alguns testes demonstraram que os protocolos da ARPANET não podiam ainda ser executado através de várias redes, portanto houve um esforço adicional no sentido de mais pesquisas para o desenvolvimento de protocolos que resolvessem este novo problema, esses

protocolos serviram então como base para o modelo da suíte TCP/IP (Transmition Control Protocol / Internet Protocol).

A aceitação mundial da suíte de protocolos TCP/IP deveu-se principalmente após o desenvolvimento da versão do UNIX de Berkeley que foi desenvolvido com o apoio da ARPA a uma empresa de consultoria da Califórnia chamada BBN e a Universidade da Califórnia em Berkeley, que além de incluir protocolos que facilitavam a conexão das LAN's com a ARPANET. A conexão das LAN's com a ARPANET acabou acontecendo de forma efetiva na década de 80. (Tanenbaum, 1997)

Dentre as várias organizações e comitês que participaram deste desenvolvimento e divulgação, pode-se destacar Internet Engineering Task Force – IETF (http://www.ietf.org) cuja principal função atual é a manutenção e apoio aos padrões de internet e TCP/IP principalmente através da série de documentos Request for Comments – RFC. Estes documentos descrevem as diversas tecnologias envolvidas e servem de base para as novas tecnologias que deverão manter a compatibilidade com as anteriores dentro do possível.

Em resumo, o maior trunfo do TCP/IP é o fato destes protocolos apresentarem a interoperabilidade de comunicação entre alguns tipos de hardware, software e sistemas operacionais. Sendo assim, o impacto positivo da comunicação computacional aumenta com o número de tipos de computadores que participam da grande rede internet.

1.2- Modelo de referência ISO/OSI

Dentro deste cenário de grande variedade de sistemas operacionais, CPUs, interfaces de rede, tecnologia e várias outras variáveis, e a necessidade de interconexão entre os diversos sistemas computacionais em 1977, a International Standards Organization - ISO, criou um sub-comitê para o desenvolvimento de padrões de comunicação para promover a interoperabilidade

entre as diversas plataformas. Foi então desenvolvido o modelo de referência Open Systems Interconnection – OSI.

É importante observar que o modelo OSI é simplesmente um modelo que especifica as funções a serem implementadas pelos diversos fabricantes em suas redes. Este modelo não detalha como estas funções devem ser implementadas, deixando isto para que cada empresa/organização tenha liberdade para desenvolver.

O comitê ISO assumiu o método "dividir para conquistar", dividindo o processo complexo de comunicação em pequenas sub-tarefas (camadas), de maneira que os problemas passem a ser mais fáceis de tratar e as sub-tarefas melhor otimizadas. O modelo ISO/OSI é constituído por sete camadas, descritas sucintamente na figura 1.1 abaixo:

7	Aplicação	Esta camada funciona como uma interface de ligação entre os processos de comunicação de rede e as aplicações utilizadas pelo usuário.
6	Apresentação	Aqui os dados são convertidos e garantidos em um formato universal.
5	Sessão	Estabelece e encerra os enlaces de comunicação
4	Transporte	Efetua os processos de sequenciamento e, em alguns casos, confirmação de recebimento dos pacotes de dados.
3	Rede	O roteamento dos dados através da rede é implementado aqui.
2	Enlace	Aqui a informação é formatada em quadros (frames). Um quadro representa a exata estrutura dos dados fisicamente transmitidos através do fio ou outro meio.
1	Física	Define a conexão física entre o sist. Computacional e a rede. Especifica o conector, a pinagem, níveis de tensão, dimensões físicas, caracter. mecânicas e elétricas, etc.

Figura 1.1 – Modelo ISO/OSI

Cada camada se comunica com sua semelhante em outro computador. Quando a informação é passada de uma camada para outra inferior, um cabeçalho é adicionado aos dados para indicar de onde a informação vem e para

onde vai. O bloco de cabeçalho mais dados de uma camada, é o dado da próxima camada.

A unidade de informação muda de nome ao longo das camadas de maneira que possa sobre qual camada se está referindo pelos nomes destas unidades. A figura 1.2 relaciona os diversos nomes destas unidades de informação ao longo das camadas:

7	Aplicação	Mensagem
4	Transporte	Segmento
3	Rede	Pacote
2	Enlace	Quadro / Frame
1	Física	Bit

Figura 1.2 – Unidades de informação por camadas

Antes do desenvolvimento do modelo de camada ISO/OSI, o DoD definiu seu próprio modelo de rede conhecido como modelo DoD de rede ou também modelo Internet de rede. Posteriormente este modelo passou a ser conhecido como modelo de camadas TCP/IP.

1.3- Modelo de referência TCP/IP

O modelo de camadas ISO/OSI acabou se tornando apenas uma base para praticamente todos os protocolos desenvolvidos pela indústria. Cada desenvolvedor tem uma arquitetura que difere em detalhes às vezes fundamentais no seu desenvolvimento. Sendo assim, é de se esperar uma variação nas descrições do conjunto de protocolos TCP/IP. Segue uma comparação entre duas possíveis interpretações, esquerda e direita do modelo base ISO/OSI ao centro.

Na figura 1.3, na tabela da esquerda apresenta os principais protocolos distribuídos pelas diversas camadas, enquanto que, na tabela da direita, as funções são o destaque.

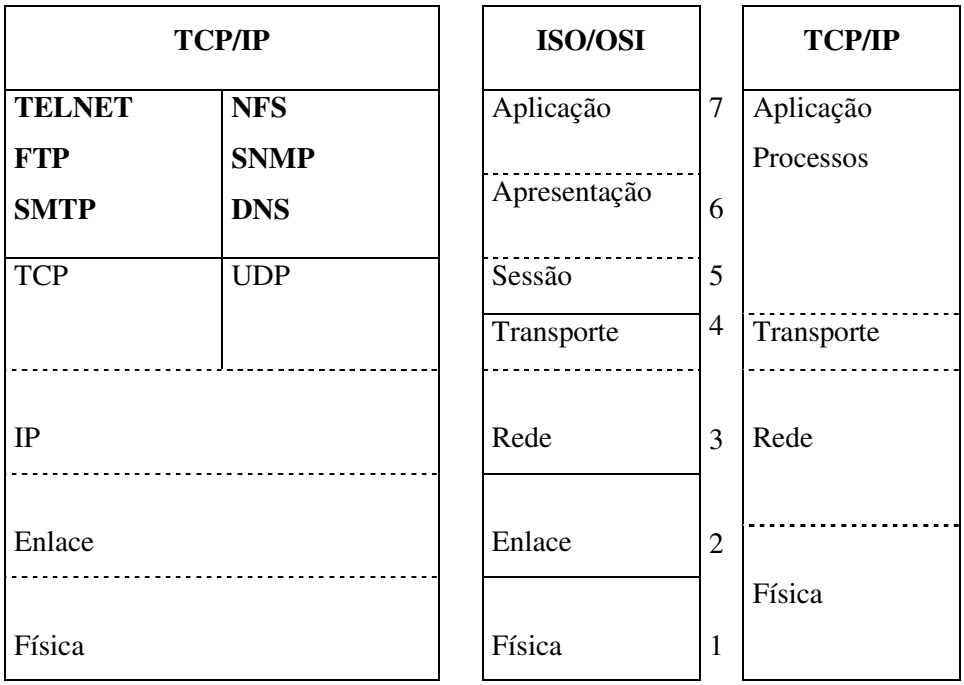

Figura 1.3- Interpretação, esquerda e direita do modelo base ISO/OSI

Na tabela da esquerda – é observado que o TCP/IP não faz distinção entre as camadas superiores. As três camadas superiores são estritamente equivalentes aos protocolos de processos da internet. Os processos possuem o nome do próprio protocolo utilizado, porém é importante não confundir o protocolo em si com a aplicação que geralmente apresenta uma interface com usuário amigável para utilização do protocolo.

No modelo ISO/OSI, a camada de transporte (4) é responsável pela liberação dos dados para o destino. No modelo internet (TCP/IP) iste é feito pelos protocolos "ponto a ponto" TCP e UPD.

Por fim, o protocolo IP é o responsável pela conexão entre os sistemas que estão se comunicando. Basicamente este protocolo se relaciona com a camada de rede (3) do modelo ISO/OSI. Este protocolo é o responsável principal do transporte da informação na rede. É nesta camada/protocolo que a informação é fragmentada no sistema fonte e reagrupada no sistema alvo. Cada um destes fragmentos pode ter caminhos diferentes pela rede de forma que os fragmentos podem chegar fora de ordem. Se, por exemplo, o fragmento posterior chegar antes do anterior, o protocolo IP no sistema destino reagrupa os pacotes na seqüência correta.

Na tabela de direita observa-se o TCP/IP como sendo constituído por 4 camadas apenas. A camada superior, camada de aplicação/processo é responsável por permitir que aplicações que possam se comunicar através de hardware e software de diferentes sistemas operacionais e plataformas. Muitas vezes este processo é chamado de cliente-servidor. A aplicação cliente em geral está em um equipamento mais simples e com uma boa interface com usuário. Esta aplicação envia requisições à aplicação servidor que normalmente está em uma plataforma mais robusta e que tem capacidade para atender várias requisições diferentes de clientes diferentes.

A camada que segue, camada de Transporte ou “Ponto a Ponto”, tem a função principal de começar e terminar uma conexão e ainda controlar o fluxo de dados e de efetuar processos de correção e verificação de erros.

A camada de rede é a responsável pelo roteamento. Comparativamente ela corresponde no modelo ISO/OSI à camada de Rede (3) e parte da camada Enlace (2). Esta camada é usada para atribuir endereço de rede (IP) ao sistema e rotear a informação para a rede correta. e ainda com a função de ligação entre as camadas superiores e os protocolos de hardware . Em essência pode-se afirmar que sem esta camada, as aplicações teriam que ser desenvolvidas para cada tipo de arquitetura de rede como, por exemplo, Ethernet ou Token Ring.

A primeira camada, camada Física, não é definida pelo TCP/IP, porém é nítida sua importância em relação à parte física da mídia de comunicação, de bits, de quadros, de endereços MAC, etc.

1.4- Camada de Rede do Modelo TCP/IP

A Camada de rede é responsável pelo endereçamento dos pacotes de informação dos dispositivos origem e destino e faz o roteamento entre as respectivas redes, se diferentes. Este roteamento é executado utilizando como base o endereço IP de origem e destino disponíveis no pacote IP.

Protocolo Internet – IP O protocolo internet é definido na camada 3 do modelo ISO/OSI. O endereço IP é composto por 32 bits divididos em 4 octetos, que são divididos em uma parte para a identificação da rede e outra parte para identificação dispositivo, chamados de identificadores de rede e de host, de acordo com o tipo de classe definido da rede ou sub-rede, que é definida pelo número de máscara.

Este protocolo, usando a parte rede do endereço ou identificador de rede, pode definir a melhor rota através de uma tabela de roteamento mantida e atualizada pelos roteadores.

Este protocolo recebe os dados da camada superior (transporte) na forma de segmentos. Ocorre então o processo de fragmentação e os conjuntos de dados passam a se chamar pacotes. Estes pacotes são então codificados para envio à camada inferior (física) para encaminhamento no meio físico.

Na figura 1.4 relacionamos as diversas partes constituintes de um pacote, o número de bits e função ou descrição.

O primeiro campo, Cabeçalho, contém informação sobre a versão do número IP (ipv4 ou ipv6) e o tipo de serviço (ToS), muito usado em aplicações que necessitem de Qualidade de Serviço (QoS).

O segundo campo, Comprimento, informa o comprimento do pacote incluindo dados e cabeçalho.

O terceiro campo, Fragmentação, instrui ao protocolo, como reagrupar pacotes quando chegam após um processo de fragmentação muito comum em interfaces defeituosas e tráfego intenso.

O quarto campo, Time to Live – TTL informa o número de roteadores que podem redirecionar o pacote. O valor é decrementado até zero a cada roteador quando então o pacote é descartado, impedindo a criação de loops e assim garantindo estabilidade ao processo de roteamento.

		Camadas	Bits
DESCRIÇÃO	CABEÇALHO	**1**	**32**
	COMPRIMENTO	**2**	**16**
	FRAGMENTAÇÃO	**3**	**16**
	TTL	**4**	**8**
	PROTOCOLO TCP OU UDP	**5**	**8**
	VERIFICAÇÃO DEERROS	**6**	**16**
	ENDEREÇO FONTE	**7**	**32**
	ENDEREÇODESTINO	**8**	**32**
	DADOS	**9**	**Xxx**

Figura 1.4 – Tabela relacionando as partes constituintes de um pacote IP.

O quinto campo informa qual protocolo deverá receber o pacote na próxima camada. Se o valor deste campo for 6, TCP, se 7, UDP.

O sexto campo, Verificação de Erro, seleciona que o processo será utilizado na detecção de erros: Cyclical Redundance Check – CRC ou Frame Check Sequence – FCS.

Os próximos campos, sétimo e oitavo, Endereço Fonte e Endereço Destino, 32 bits cada, caracterizam por completo toda informação sobre endereçamento necessário ao processo de roteamento.

O último campo contém os dados, informação na realidade, e tem tamanho livre, porém definido pelo tipo de rede sendo o MTU (Maximum Transfer Unit) igual a 1500kbytes.

Todas as informações necessárias para que o IP possa comunicar com o resto da rede estão distribuídas nestes campos, principalmente naqueles relativos ao endereçamento. É importante observar que a camada de rede utiliza estes endereços lógicos de 4x8bits, para definir as redes existentes e como conseguir obter informação delas. Entretanto, para que os dados cheguem aos hosts é

necessário um outro tipo de endereço: endereço Media Access Control – MAC ou Ethernet.

O TCP/IP define um protocolo, ARP (Address Resolution Protocol), que caracteriza a relação entre o endereço IP e o endereço MAC (Media Access Control). ARP É um protocolo de resolução de endereços, é um protocolo padrão de rede para tecnologia padrão ethernet. O protocolo de resolução de endereços é responsável pela conversão de endereços de protocolo de nível superior (endereço IP) para endereços de rede física (MAC – Media Access Control).

Em uma única rede física, os hosts individuais são conhecidos na rede pelo seu endereço físico de hardware. Os protocolos de nível superior localizam os hosts de destino na forma de um endereço simbólico (neste caso o endereço IP). Quando tal protocolo quer enviar um pacote para o endereço IP de destino w.x.y.z (ex: 10.0.1), o driver de dispositivo não entende este endereço. Assim, é fornecido um módulo (ARP) que converterá o endereço IP para o endereço físico de destino. Ele usa uma tabela (algumas vezes referida como cache de ARP), para fazer esta conversão.

Quando o endereço não é encontrado no cache de ARP, um broadcast é enviado na rede, com um formato especial chamado de solicitação ARP. Se uma das máquinas na rede reconhecerem o seu próprio endereço IP nesta solicitação, devolverá uma resposta ARP para o host solicitante. A resposta conterá o endereço físico do host e as informações da rota de origem (se o pacote tiver cruzado bridges em seu caminho).

Tanto este endereço quanto a informação da rota de origem são armazenados no cache de ARP do host solicitante. Todos os pacotes subseqüentes enviados para este endereço IP de destino podem agora ser convertido em uns endereços físicos, que é usado pelo driver de dispositivo para enviar os pacotes pela rede.

A tecnologia ATM (Asyncronous Transfer Mode – modo de transferência assíncrona) constitui uma exceção à regra, onde o ARP não pode ser implementado na camada física como foi descrito anteriormente. Por esta razão, quando um servidor ARP é usado, todos host tem de registrar-se logo na inicialização para poder decompor os endereços IP em endereços de hardware.

O ARP foi planejado para ser usado em redes que suportam o broadcast de hardware. Isto significa, por exemplo, que o ARP não funcionará em uma rede X.25.

O ARP é usado tanto em redes IEEE 802 quanto em redes Ethernet DIX mais antigas, para mapear os endereços IP para endereços físico de hardware. Para fazer isto, ele está intimamente relacionado ao driver de dispositivo desta rede. Na verdade, as especificações ARP na RFC 826 descrevem apenas a sua funcionalidade, não sua implementação. A implementação depende em grande parte do driver de dispositivo para um tipo de rede e são geralmente codificados em conjunto no microcódigo do adaptador. Se um aplicativo deseja enviar dados para um determinado endereço IP de destino, o mecanismo de roteamento IP determina primeiro o endereço IP da próxima “parada” do pacote (pode ser o

próprio host de destino, ou um roteador) e o dispositivo de hardware ao qual deveria ser enviado. Se for uma rede IEEE 802.3/4/5, o módulo ARP deve ser consultado para mapear o <tipo do protocolo, endereço do protocolo-alvo> para um endereço físico.

O módulo ARP tenta encontrar o endereço neste cache de ARP. Se encontrar o par correspondente, ele devolve o endereço físico de 48 bits para o solicitante (o driver de dispositivo) que então transmite o pacote. Se não encontrar o par nesta tabela, ele se livra do pacote (supõe que um protocolo de nível superior irá transmiti-lo) e gera um broadcast de rede de uma solicitação ARP.

Para o pacote de solicitação ARP, o endereço de hardware de destino é o único campo indefinido no pacote.

O ICMP (Internet Control Message Protocol) é uma extensão da camada do IP. É por essa razão que ele usa um cabeçalho IP, e não um cabeçalho UDP (User Datagram Protocol). O objetivo do ICMP é relatar ou testar determinadas condições na rede. O IP transmite dados e não possui outra forma de comunicação. O ICMP oferece algum mecanismo de relato de erro para o IP. Basicamente, ele permite que dispositivos de ligação entre redes (host ou roteadores) transmitam mensagens de erro ou de teste. Essas mensagens de erro podem ser que um destino de rede não pode ser alcançado ou que pode ser gerado ou respondido um pacote de solicitação de eco.

O IGMP (Internet Group Management Protocol) é uma extensão do protocolo IP que permite multicasting para o IP. O endereço de multicast já existia para o IP, mas não havia um protocolo de controle que permitisse sua existência em uma rede. O IGMP é um protocolo que opera em estações de trabalho e em roteadores, o qual permite que os roteadores determinem quais endereços de multicast existem em seus segmentos. Com esse conhecimento, os roteadores podem criar árvores de multicast, permitindo que dados de multicast

sejam recebidos e propagados para suas estações de trabalho de multicast. Os cabeçalhos IGMP são usados como base para todos os protocolos de roteamento de multicast para o Ipv4. (Soares, 1995)

1.5- Endereçamento IP e Classes

Como anteriormente, a camada do protocolo IP ou protocolo Internet, define um endereço de identificação único e através deste endereço executa serviços de roteamento que basicamente definem o caminho disponível naquele momento para comunicação entre a fonte e o destino.

O protocolo Internet (IP) necessita da atribuição de um endereço Internet (endereço IP) organizado em 4 octetos (32 bits). Estes octetos definem um único endereço dividido em uma parte que representa a rede a qual pertence o endereço, em alguns casos a sub-rede também, e por fim a representação particular daquele sistema na rede. Alguns endereços possuem significado especial:

- **Endereço 0**: Significa a próprio rede ou sistema. O endereço 0.0.0.35 referencia a estação 35 da rede local. Por exemplo, endereço 127.0.0.0 referência à estação em análise também conhecida como loopback. O endereço 152.84.40.0 referência a sub-rede 40 inteira da rede local do CBPF (Centro Brasileiro de Pesquisas Físicas) que pode ser representada por 152.84.0.0.
- **Endereço 127**: É conhecido como loopback e é utilizado em processos de diagnose. O endereço 127.0.0.1 é o próprio loopback da estação em análise.
- **Endereço 255**: Este endereço é muito utilizado em mensagens broadcast e serviços de anúncio generalizados. Uma mensagem enviada para o endereço 152.84.255.255 irá atingir todos os 255 sistemas de cada uma das 255 sub-redes da rede local do CBPF.

A figura 1.5 relaciona os diversos aspectos relevantes na definição do endereço Internet: o número de sistemas possíveis, os primeiros bits do primeiro octeto e os seus possíveis valores. Os demais octetos podem assumir livremente os valores entre 0 e 255, sempre levando em conta aqueles de significado especial.

Classe	2n	Hosts	Bits Iniciais	Primeiro Octeto
A	24	167.772	0xxx	0 – 127
B	16	65.536	10xx	128 – 191
C	8	256	110x	192 – 223
D	-	-	1110	224 – 239
E	-	-	1111	240 - 255

Figura 1.5 – Tabela relacionando a definição do endereço Internet

Os endereços **Classe A** são usados para redes muito grandes normalmente ligadas a funções educacionais e científicas. Os endereços **Classe B** são usados em redes muito grandes, normalmente atribuídos a instituições que possuíam um perfil disseminador de tecnologia e assim pudessem de alguma forma distribuir suas redes entre instituições e empresas contribuindo assim para o desenvolvimento de uma grande rede mundial. Os endereços **Classe C** são os mais difundidos, pois permite redes de 256 IP's o que parece ser um número conveniente para gerenciamento e implantação de sistemas de informação. Os endereços **Classe D** são reservados para Multicast utilizado nas aplicações de videoconferência, Multimídia, dentre outras, e por fim, os endereços **Classe E** são reservados para experimentação e desenvolvimento.

1.6 – Sub-rede IP e máscara de sub-rede

A criação de sub-redes a partir de uma rede primária é um procedimento típico na área de redes. O objetivo desta segmentação é permitir uma melhor performance da rede em termos organizacionais, estruturais e funcionais.

A idéia básica é acrescentar alguns bits ao identificador de rede do endereço de Internet. Os endereços permitidos são aqueles formados pelos bits restantes do octeto. O identificador de redes e sub-redes, a máscara de sub-rede, também são compostos por 4 octetos. A máscara é formada por bits 1 nos campos que caracterizam o endereço de rede, e bits 0 nos campos relativos ao host.

Considere uma Classe C com cada posição representada por um único bit de um endereço de 32bits:

R - > Rede H - > Host

RRRRRRRR. RRRRRRRR.RRRRRRRR.HHHHHHHH

Se esta Classe C for dividida em 8 sub-redes com 32-2(rede e broadcast)=30 hosts em cada uma delas, a máscara será 255.255.255.224 ou ainda/27 e sua representação fica:

RRRRRRRR.RRRRRRRR.RRRRRRRR.RRRHHHHH

11111111.11111111.11111111.11100000

Em um outro exemplo queremos fazer 64 sub-redes com 4-2=2 hosts permitidos por sub-redes. Neste caso a máscara seria 255.255.255.252 ou ainda /30 com a seguinte representação:

RRRRRRRR.RRRRRRRR.RRRRRRRR.RRRRRRHH

11111111.11111111.11111111.11111100

O mesmo raciocínio pode ser empregado em uma Classe B ou Classe A, mudando somente a relação entre bits 1 e bits 0, ou em outras palavras muda o octeto em análise. No caso de 2 sub-redes na Classe B teremos 255.255.128.0 ou/17 representadas por:

RRRRRRRR.RRRRRRRR.RHHHHHHH.HHHHHHHH

11111111.11111111.10000000.00000000

Vale ressaltar aqui uma operação simples implementada por todos algoritmos de roteamento que é o AND lógico entre a máscara de sub-rede e o endereço do host. Se o endereço tiver os mesmos bits 1 da máscara então este endereço pertence a sub-rede em análise e portanto o pacote pode ser enviado através de broadcast na sub-rede. Se diferir, então o pacote deve ser enviado ao gateway, pois certamente pertence à outra sub-rede.

1.7 - Comutação de Pacotes e de Circuitos

O TCP/IP permitiu a existência de comunicações abertas e a proliferação de conectividade LAN a LAN e LAN a WAN entre vários ambientes operacionais. Sua topologia e arquitetura, porém, não tinham como base os métodos empregados pela empresa telefônica: comutação de circuitos.

A empresa telefônica (AT&T), basicamente diante da idéia de uma rede de comutação de pacotes afirmou publicamente que isso jamais daria certo. Uma rede onde as informações transmitidas pudessem encontrar o seu próprio caminho na rede? Uma rede onde todo pacote de informações transmitido tivesse a mesma chance de encaminhamento? A companhia telefônica manteve sua postura de que a comutação de circuitos era o único método que deveria ser usado para voz, vídeo ou dados. A comutação por definição oferecia largura de banda garantida e, portanto, “qualidade de serviço”. Nessa época, a empresa telefônica estava correta, mas somente para voz. Voz e vídeo não podem resistir a nenhum retardo pequeno que seja (cerca de 150 mili segundos, ou 0,150 segundos), mas os dados podem! Em comutação de pacotes, o percurso é encontrado em tempo real, e toda vez o percurso deve ser igual; mas pode não ser. Além disso, as informações vão do ponto A ao ponto B.

Existem muitas diferenças entre comutação de circuitos e de pacotes. Uma delas é que, na comutação de circuitos, um percurso é construído antes do envio das informações, enquanto que na comutação de pacotes não; um percurso não é definido nem se for criado antes do envio das informações. Por exemplo, quando se faz uma chamada telefônica, a companhia telefônica cria fisicamente um circuito para essa chamada. A pessoa não pode falar (transmitir informações) até que o circuito seja criado. Esse circuito é criado via hardware. Esse percurso é um circuito físico através do sistema de rede telefônica; no entanto, a companhia telefônica está empregando no momento outras tecnologias para permitir a "comutação de circuitos virtuais" através de tecnologias como ATM – (Asynchronous Transfer Mode). Para nossa comparação, um percurso de voz é criado no hardware antes que as informações sejam passadas. Nenhuma informação está contida o sinal de voz digitalizada para indicar aos switches onde o destino está localizado. Um nó de transmissão possui a mesma chance de obter suas informações para o receptor.

Na comutação de pacotes, as informações necessárias para atingir a estação de destino estão contidas no cabeçalho das informações que estão sendo enviadas. As estações, conhecidas como roteadores, liam essas informações na rede e as encaminhavam ao longo do seu percurso. Milhares de pacotes de informações distintos podem usar o mesmo percurso para diferentes destinos.

Atualmente, é provando que a comutação de pacotes, além de ser viável, pode ser usada para voz, vídeo e dados. Foram inventadas estações mais novas e mais rápidas na rede, junto com transportes de transmissão mais rápidos. Junto com isso, existem novos protocolos de "qualidade de serviço" que permitem prioridades na rede. Determinados pacotes de informações podem "saltar" sobre os outros, para serem transmitidos primeiro.

CAPÍTULO II – DEFINIÇÃO DE QoS

2.1 - Qualidade de Serviços

A Qualidade de Serviço (QoS) pode ser definida com parâmetros específicos necessários para uma determinada aplicação do usuário. Estes parâmetros de serviços podem ser definidos em termo de largura de banda, latência e jitter, visando que a aplicação passa obter uma melhor qualidade ao longo da rede. Segundo Ferguson (1998) podemos definir Qos como: "Capacidade da rede de fornecer tratamento especial a certos tipos de tráfego previsivelmente" (Dantas, 2002)

Uma camada importante na QoS é a camada de rede que tem como objetivo específico transferência de dados fim-a-fim ou extremo-a-extremo, uma vez que trata as transferências desde o emissor até o receptor final. Neste nível, os PDU (Protocol Data Unit) tomam vulgarmente a designação de pacotes, os serviços do nível de rede que são considerados não confiáveis limitando-se a detectar a ocorrência de erros.

Uma outra camada a ser considerada é a camada de transporte que tem função específica na QoS (Qualidade de Serviço) e que recebe o serviço prestado pela camada de rede. Se o serviço da camada de rede for perfeito, o trabalho da camada de transporte será facilitado. No entanto, se o serviço de rede não for perfeito, a camada de transporte terá que servir de ponte para cobrir a distância entre o que os usuários de transporte desejam e o que a camada de rede oferece.

Ainda que à primeira vista o conceito de qualidade de serviço seja vago (fazer com que todos concordem sobre o que significa um serviço "bom" não é uma tarefa simples), a QoS pode ser definida por um número específico de parâmetros. O serviço de transporte pode permitir ao usuário determinar os valores preferenciais, os valores aceitáveis e os valores mínimos para vários

parâmetros de serviço no momento em que uma conexão é estabelecida. Alguns parâmetros também podem ser usados no transporte sem conexão. É tarefa da camada de transporte examinar esses parâmetros e, dependendo do(s) tipo(s) de serviço(s) de rede disponível(eis), determinar se é possível realizar o serviço solicitado. Os parâmetros típicos para a qualidade de serviço da camada de transporte são mostrados a seguir:

- Retardo no estabelecimento da conexão
- Probabilidade de falha no estabelecimento da conexão
- Throughput (Vazão)
- Taxa de erros residuais
- Proteção
- Prioridade
- Resiliência
- Retardo de trânsito.

Observe que poucas redes ou protocolos oferecem todos esses parâmetros. Muitas apenas tentam reduzir a taxa de erros da melhor maneira possível. Outras têm arquiteturas de QoS mais elaboradas.

O retardo no estabelecimento da conexão é o tempo transcorrido entre a solicitação de uma conexão de transporte e o recebimento de sua confirmação pelo usuário do serviço de transporte. Nessa característica também está incluído o retardo do processamento na entidade de transporte remota. A exemplo de todos os parâmetros que medem um retardo, quando menor o retardo, melhor o serviço.

A Probabilidade de falha no estabelecimento da conexão é a possibilidade de a conexão não se estabelecer dentro de um período máximo estabelecido devido a, por exemplo, um congestionamento na rede, à falta de espaço de tabela em algum lugar ou a outros problemas internos.

O parâmetro throughput calcula o número de bytes de dados do usuário transmitidos por segundo durante um determinado intervalo de tempo. O throughput é medido separadamente para cada direção.

O retardo de trânsito calcula o tempo transcorrido desde o envio de uma mensagem pelo usuário de transporte da máquina de origem até seu recebimento pelo usuário de transporte da máquina de destino. A exemplo do throughput, cada direção do transporte é analisada separadamente.

A taxa de erros residuais calcula o número de mensagens perdidas ou corrompidas em porcentagem do total enviado. Na teoria, a taxa de erros residuais deveria ser zero, pois o trabalho da camada de transporte é esconder os erros da camada de rede. Na prática, essa taxa pode apresentar um valor (baixo) finito.

O parâmetro de Proteção oferece uma forma de o usuário de transporte especificar seu interesse no fato de a camada de transporte fornecer proteção contra a leitura, ou a modificação, de dados por parte de terceiros (que utiliza "grampos" para violar a comunicação).

O parâmetro de Prioridade oferece ao usuário de transporte um modo de indicar que algumas conexões são mais importantes do que outras e, em caso de congestionamento, garantir que as conexões de maior prioridade sejam atendidas primeiras.

Por fim, o parâmetro de Resiliência oferece à camada de transporte a probabilidade de finalizar uma conexão espontaneamente devido a problemas internos ou a congestionamento.

O parâmetros QoS são especificados pelo usuário de transporte quando uma conexão é solicitada. Os valores mínimo e máximo aceitáveis podem ser fornecidos. Às vezes, ao conhecer os valores de QoS, a camada de transporte percebe imediatamente que alguns deles não podem ser alcançados. Nesse caso, ela informa ao responsável pela chamada que a tentativa de conexão falhou sem

sequer tentar contato com o destino. O relatório da falha especifica o que a causou.

Em outros casos, a camada de transporte sabe que não pode alcançar o objetivo desejado (por exemplo, um throughput de 600Mbps), mas pode atingir uma taxa mais baixa, porém aceitável (por exemplo, 150Mbps). Em seguida, a camada de transporte envia a taxa mais baixa e a mínima aceitável para a máquina remota e solicita o estabelecimento de uma conexão. Se a máquina remota não puder administrar o valor sugerido, mas conseguir administrar qualquer valor acima do mínimo, a camada de transporte fará uma contra proposta. Se a máquina remota não puder trabalhar com qualquer valor acima do mínimo, ela rejeitará a tentativa de conexão. Por fim, o usuário de transporte da máquina de origem é informado do fato de que a conexão foi estabelecida ou rejeitada. Se a conexão tiver sido estabelecida, o usuário será informado dos valores dos parâmetros acordados.Esse procedimento é chamado de **negociação de opção** (option negotiation).

Uma QoS pode ser descrita como um conjunto de parâmetros que descrevem a qualidade (por exemplo, largura de banda, utilização de buffers, prioridades, utilização da CPU etc.) de um fluxo de dados específico. A pilha do protocolo IP básica propicia somente uma QoS que é chamada de melhor tentativa. Os pacotes são transmitidos de um ponto a outro sem qualquer garantia de uma largura de banda especial ou retardo mínimo. No modelo de tráfego de melhor tentativa, as requisições na Internet são processadas conforme a estratégia do primeiro a chegar, primeiro a ser atendido. Isso significa que todas as requisições têm a mesma prioridade são processadas umas após a outra. Não há possibilidade de fazer reserva de largura de banda para conexões específicas ou aumentar a prioridade de uma requisição especial. Assim, foram desenvolvidas novas estratégias para oferecer serviços previsíveis na internet.

Hoje em dia, há dois princípios básicos para conseguir QoS na internet:

- Serviços integrados
- Serviços diferenciados

Os serviços integrados trazem melhoramentos ao modelo de rede IP para suportar transmissões em tempo real e garantir largura de banda para seqüências de dados específicas. Neste caso, definimos um fluxo de dados (stream) como uma seqüência distinguível de pacotes relacionados e transmitidos de um único emissor para um único receptor, que resulta de uma única atividade de usuário e requer a mesma QoS. (Tanenbaum, 1997)

2.2 - Qualidade de Serviços e Descritores de Tráfego

A recomendação I.350 da ITU-T (International Telecommunication Union – União Internacional de Telecomunicações) fornece a descrição das noções de qualidade de serviço (Quality of Service – QoS), desempenho da rede (Network Performance – NP) e descritores de tráfego. A descrição de QoS é tomada da recomendação E.800, onde se define a qualidade de serviço como sendo o efeito coletivo provocado pelas características de desempenho de um serviço, determinando o grau de satisfação do usuário. Tal definição engloba, originalmente, vários aspectos de diversas áreas de atuação, incluindo o nível de satisfação do usuário. Na recomendação I.350, o ITU-T achou por bem considerar como parâmetro relevante para definição da qualidade de serviço na camada ATM, somente aqueles que podem ser diretamente observáveis e mensuráveis no ponto de acesso do serviço dos usuários. Outros tipos de parâmetros não diretamente mensuráveis ou subjetivos em sua natureza não serão tratados como parâmetros para a especificação da QoS. Exemplos de parâmetros utilizados para a definição da QoS na camada ATM são: o retardo, a sensibilidade à variação estatística do retardo, a taxa de perda de células etc. A tradução da QoS específica da aplicação para a QoS adequada da camada ATM

é papel das camadas superiores de protocolo, incluindo a AAL (ATM adaptation Layer). (Murhammer, 2000)

O desempenho da rede (NP - Network Performance) é medido em termos de parâmetros utilizáveis pelo provedor dos serviços de comunicação com o propósito de projeto, configuração, operação e manutenção do sistema. Os objetivos do desempenho de rede em um SAP ATM são definidos para capturar a capacidade da rede em atender a qualidade de serviço requerido da camada ATM. As noções de QoS e NP diferem quanto ao propósito e enfoque dos parâmetros que as caracterizam. Os parâmetros de QoS são definidos sob o ponto de vista do usuário de um determinado serviço, enquanto que os parâmetros de NP são definidos sob o ponto de vista da infra-estrutura de comunicação que fornece suporte ou implementa esse serviço. Ambos os parâmetros são necessários, e os seus valores devem estar quantitativamente relacionados para que a rede possa servir efetivamente aos seus usuários. A definição dos parâmetros de QoS e NP deve tornar claro o mapeamento entre os seus valores em todos os casos onde esse mapeamento não for um para um.

A recomendação I.371 apresenta as técnicas de controle de tráfego e controle de congestionamento que deverão ser aplicados na RDSI-FL (Redes Digitais de Serviços Integrados). Tais mecanismos têm como principal objetivo garantir a manutenção da qualidade de serviço especificada e desejada pelos usuários no momento em que uma conexão ATM é estabelecida. Uma RDSI-FL deverá fornecer um determinado número de classes de serviço, cada uma associada a uma qualidade de serviço e seus parâmetros – cada conjunto de parâmetros e seus valores determina uma QoS. Adicionalmente, dentro de cada classe, características particulares de capacidade podem ser especificadas.

Um usuário requisita uma QoS específica da camada ATM através das classes QoS que a rede fornece. Isso deve fazer parte do contrato de tráfego definido no estabelecimento da conexão. É de responsabilidade da rede garantir

a qualidade de serviço negociada, desde que o usuário cumpra a sua parte no contrato de tráfego. Se o usuário violar o contrato, a rede pode não respeitar a QoS acordada.

Um usuário pode requisitar até duas classes diferentes de QoS para uma conexão ATM cada uma associada a uma taxa de perda das células (cell loss ratio – CLR). O bit de prioridade de perda de célula, por nós visto quando estudamos o cabeçalho de uma célula ATM, definirá os parâmetros QoS que deverão ser atendidos para a célula em questão.

Os Parâmetros de tráfego descrevem as características de tráfego de uma conexão ATM. Parâmetros de tráfego são agrupados em descritores de tráfego da fonte para a troca de informação entre o usuário e a rede. Podemos, assim, definir mais precisamente os descritos de tráfego como uma lista genérica de parâmetros de tráfego que podem ser utilizados para capturar as características de uma conexão ATM. Exemplos de parâmetros de tráfego são: taxa de pico de geração de células (cell peak rate), taxa média de transferência de células (avarage cell rate), duração de um pico (peak duration), explosividade (burstiness) e tipo de fonte (telefone, videofone etc.).

Se o usuário requerer dois níveis de prioridade para a conexão ATM, conforme indicado pelo bit CLP do cabeçalho de uma célula, as características intrínsecas de tráfego do fluxo de ambos os tipos de células devem ser especificados no descritor de tráfego da fonte. Isto é feitos por meio de um conjunto de parâmetros de tráfego associado com as células CLP=0, e um conjunto de parâmetros de tráfego associado com todas as células (isto é CLP=0+1).

Os procedimentos de controle de admissão fazem uso do descritor de tráfego da fonte para a alocação de recursos e para derivar parâmetros para a operação dos mecanismos de policiamentos da fonte. Todo parâmetro de tráfego

de um descritor de tráfego da fonte deve ser enquadrado pelos mecanismos de policiamento.

Os algoritmos de controle de tráfego e congestionamento requerem o conhecimento de certos parâmetros para atuarem eficientemente. Eles devem levar em consideração o descritor de tráfego da fonte, a QoS requerida e a tolerância máxima à variação de retardo da célula – tolerância máxima CDV (cell delay variation) – para decidir se uma conexão requerida pode ser aceita (isto é, se uma determinada QoS pode ser atendida.)

A função de uma camada ATM (por exemplo, a multiplexação de células) pode alterar as características de tráfego de uma conexão ATM pela introdução de uma variação do retardo. Quando células de duas ou mais conexões ATM são multiplexadas, as células de uma dada conexão podem ser retardadas enquanto células de outra conexão estão sendo inseridas na saída do multiplexador. Células também podem sofrer retardos devido ao over-head do nível físico ou a introdução de células OAM no fluxo de saída do multiplexador. Assim, alguma aleatoriedade pode ser introduzida no intervalo de tempo entre células no ponto final de uma conexão ATM. Além disso, a multiplexação AAL pode também originar a variação de retardo de células (CDV). Ora, os mecanismos de policiamento não devem descartar, ou marcar para descartar, células geradas pela fonte em acordo com o descritor de tráfego negociado. Contudo, se a CDV não for limitada no ponto onde o mecanismo de controle de policiamento é executado, não é possível projetar um mecanismo adequado (taxas de células são aumentadas e diminuídas não pela fonte, mas pela CDV, o que pode causar a ilusão de que a taxa de pico de uma fonte de tráfego está sendo violada), nem fazer o uso de uma alocação de recursos apropriada. Assim, é importante que um valor máximo para a CDV seja estabelecido entre o SAP da conexão ATM e a interface TB, entre a interface TB e a interface NNI. Esses

valores devem ser levados em conta nos mecanismos de controle de tráfego e congestionamento.

O descritor de tráfego da fonte, a QoS requerida e a tolerância máxima CDV alocada a um equipamento do usuário definem o contrato e tráfego em um ponto de referência TB. O descritor de tráfego da fonte e a QoS requerida são declaradas pelo usuário no estabelecimento da conexão, por meio de sinalização ou subscrição. Se a tolerância máxima CDV é também negociada na subscrição ou por conexão é assunto ainda em estudo.

A taxa de pico de geração de células e a tolerância máxima CDV são parâmetros obrigatórios em um contrato de tráfego. Parâmetros adicionais podem prover uma melhora significativa da utilização da rede.

Ao comparar a QoS implementada nas redes ATM e TCP/IP observa-se que em redes TCP/IP é possível fazer QoS desde que os equipamentos envolvidos na interconexão de redes já suportem essas configurações. Indo mais adiante se pode observar a dificuldade da implementação da QoS na internet, uma vez que a complexidade e elevado grau de heterogeneidade de links (lentos e rápidos) e equipamentos de interconexão de redes muitas vezes antigos e que não suportam a implementação de Qos. Este panorama demonstra a grande dificuldade de se implementar de forma efetiva de QoS para usuário domésticos, que na maioria obtêm acesso a internet por intermédio de provedores de acesso gratuito ou em outra situação aqueles usuários se encontram em algumas localidades onde a qualidade da linha telefônica é prejudicada em função da distância e da má qualidade do sistema telefônico brasileiro.

Uma iniciativa bastante promissora pode ser citada pela experiência da implementação da RNP que em 2001 montou uma rede piloto de QoS envolvendo os pontos de presença do Distrito Federal, Minas Gerais, São Paulo, Rio de Janeiro e Rio Grande do Sul. Um dos principais objetivos era adquirir conhecimento em arquitetura QoS e experiência na implantação de serviços

diferenciados dos roteadores do backbone RNP2. Durante esse projeto alguns problemas foram detectados em roteadores que de forma simultânea prestavam alguns serviços.

Essa experiência resultou em uma proposta atualmente em análise de implementação de QoS em todo backbone RNP2. Atualmente existe um grupo de trabalho dentro da RNP especializado na qualidade QoS composto por pesquisadores que estão desenvolvendo uma pesquisa aplicada junto aos usuários da RNP2 como subsídio para identificação da demanda de QoS na rede. Essa pesquisa é dirigida a todos os desenvolvedores e usuários das aplicações disponíveis nas instituições que utilizam a RNP.

Os resultados dessa pesquisa pretendem auxiliar a construção da radiografia do tráfego da rede para servir como parâmetro para a escolha da solução mais apropriada da QoS.

Pelo exposto percebe-se o grau de dificuldade não somente na parte técnica, mas também na parte operacional que deve atender a demanda de QoS em uma determinada rede. Sendo assim, a QoS embora seja necessária e indispensável para a maioria dos serviços do mundo moderno a QoS, ainda esbarra no custo e nas dificuldades operacionais de sua implementação .

2.3 - O QoS na prática

Na internet e nas intranets atuais, a largura de banda é um assunto importante. Mais e mais pessoas estão usando a internet por motivos comerciais e particulares. O montante de dados que precisa ser transmitido através da internet vem crescendo exponencialmente.

Novos aplicativos, como Real Áudio, RealVideo, Internet Phone e sistemas de videoconferência precisam cada vez de mais largura de banda que os aplicativos usados nos primeiros anos da internet. Enquanto que aplicativos internet tradicionais, como WWW, FTP ou Telnet, não toleram perda de

pacotes, mas são menos sensíveis aos retardos variáveis, a maioria dos aplicativos em tempo real apresenta exatamente o comportamento oposto, pois podem compensar uma quantidade razoável de perda de pacotes, mas são, normalmente, muito críticos com relação aos retardos variáveis. (Murrhammer, 2000)

Isso significa que sem algum tipo de controle de largura de banda, a qualidade desses fluxos de dados em tempo real depende da largura de banda disponível no momento.

Largura de banda baixa, ou mesmo largura de banda melhores e mais instáveis, causam má qualidade em transmissões de tempo real, com eventuais interrupções ou paradas definitivas da transmissão. Mesmo a qualidade de uma transmissão usando o protocolo de tempo real RTP depende da utilização do serviço de entrega IP subjacente.

Por isso, são necessários conceitos novos para garantir uma QoS específica para aplicativos em tempo real na Internet.

Por exemplo, um fluxo de dados poderia consistir de um stream de vídeo entre um par de hosts determinados. Para estabelecer a conexão de vídeo nas duas direções, são necessários dois fluxos de dados.

Cada aplicativo que inicia um fluxo de dados pode especificar a QoS exigida para esse fluxo. Se a ferramenta de videoconferência precisar de uma largura de banda mínima de 128 Kbps e um retardo de pacote mínimo de 100 ms para garantir exibição de vídeo contínua, essa QoS pode ser reservada para essa conexão.

2.4 - Transmissão Multimídia em Redes

Pode-se dividir a parte de transmissão multimídia em redes de computadores como mostra a Figura 2.1, ou seja, a parte de conferência (que requer interatividade) e a parte de transmissão de vídeo (que envolve apenas um

lado transmitindo e vários clientes recebendo). Ambas possuem necessidades diferentes para funcionarem a contento, por exemplo, as aplicações de conferência normalmente possuem necessidades mais rígidas em relação ao atraso da rede, enquanto que a transmissão unidirecional pode trabalhar com um atraso maior.

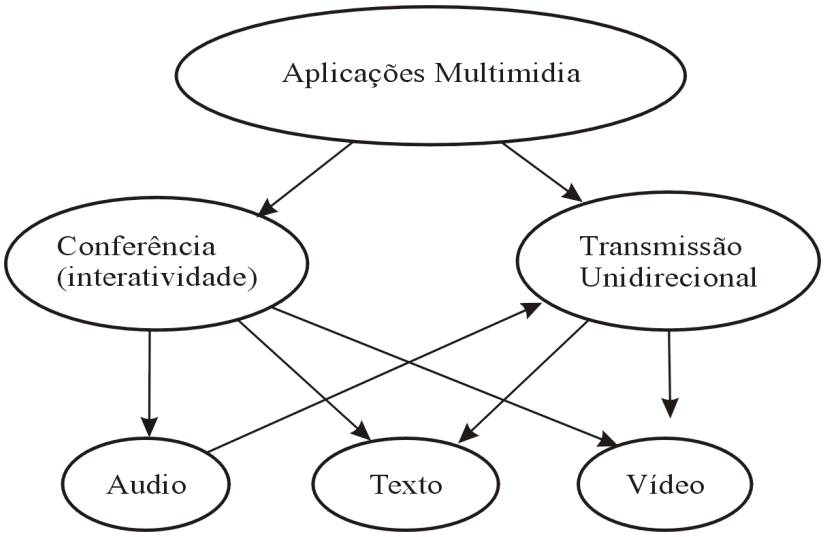

Figura 2.1 – Transmissão multimídia em rede

No item 2.5, a seguir, serão analisados com maiores detalhes os conceitos e padrões envolvidos em transmissão multimídia em redes de computadores.

2.5 - Necessidades das Aplicações

Atualmente existe uma tendência de convergência de aplicações em um único meio físico, ou seja, voz, vídeo, dados, imagens, músicas, e tudo que possa ser transformado em bits utilizando o mesmo meio físico. Entretanto, as aplicações têm características e necessidades bem diferentes umas das outras, como por exemplo, voz, que exige latência e *jitter* baixos, dados, que não tem tanta preocupação com latência e *jitter*, e videoconferência, que além de exigir latência e *jitter* baixos, ainda necessita de *skew* baixo, a fim de manter

sincronizados voz e vídeo. A seguir será feita a definição desses termos, e depois será mostrada uma tabela comparativa das necessidades das aplicações.

Latência

Em redes de computadores, latência é o tempo que um pacote leva da origem ao destino. Caso esse atraso seja muito grande, prejudica uma conversação através da rede, tornando difícil o diálogo e a interatividade necessária para certas aplicações. Á medida que o atraso aumenta, as conversas tendem a se entrelaçar, ou seja, uma pessoa não sabe se a outra a ouviu e continua falando. Após alguns milisegundos vem à resposta do interlocutor sobre a primeira pergunta efetuada, misturando as vozes. Num atraso muito grande, as pessoas devem começar a conversar utilizando códigos, tipo "câmbio", quando terminam de falar e passam a palavra ao outro. Os principais responsáveis pela latência são os atrasos de transmissão, de codificação e de empacotamento, que podem ser definidos da seguinte forma:

- Atraso de transmissão: tempo após a placa de rede ter transmitido o pacote até ele chegar na placa de rede do computador destino. Esse tempo envolve uma série de fatores, como o atraso no meio físico (por exemplo, fibra ótica, UTP, wireless), processamento em cada roteador ou switch intermediário (por exemplo, para trocar o TTL do pacote e decidir sua rota), fila de espera em cada roteador e switch intermediário, e assim por diante;
- Atraso de codificação e decodificação: sinais como voz e vídeo normalmente é codificado em um padrão, tipo PCM (G.711 a 64Kbps) para voz, ou H.261 para vídeo. Essa codificação gasta um tempo de processamento na máquina. Alguns protocolos gastam menos, como o G.711, que ocupa menos de 1ms de codificação /PAS 97a/, porém, requer 64Kbps de banda. Alguns protocolos de voz, como o G.729, requerem 25ms de codificação, mas ocupam apenas 8Kbps de banda;

- Atraso de empacotamento e desempacotamento: depois de codificado, o dado deve ser empacotado na pilha OSI a fim de ser transmitido na rede, e isso gera um atraso. Por exemplo, numa transmissão de voz a 64Kbps, ou 8000 byte por segundo, tem-se que, para preencher um pacote de dados contendo apenas 100 bytes, vai levar 12,5ms. Mais 12,5ms serão necessários no destino a fim de desempacotar os dados. Além da latência, a existência do jitter é outro fator de atraso na comunicação entre duas pessoas.

Jitter

Utilizar somente a latência não é suficiente para definir a qualidade de transmissão, pois as redes não conseguem garantir uma entrega constante de pacotes ao destino. Assim, os pacotes chegam de forma variável, como mostra a figura 2.2, ocasionando o *jitter*, que nada mais é do uma flutuação na latência, ou variação estatística do retardo.

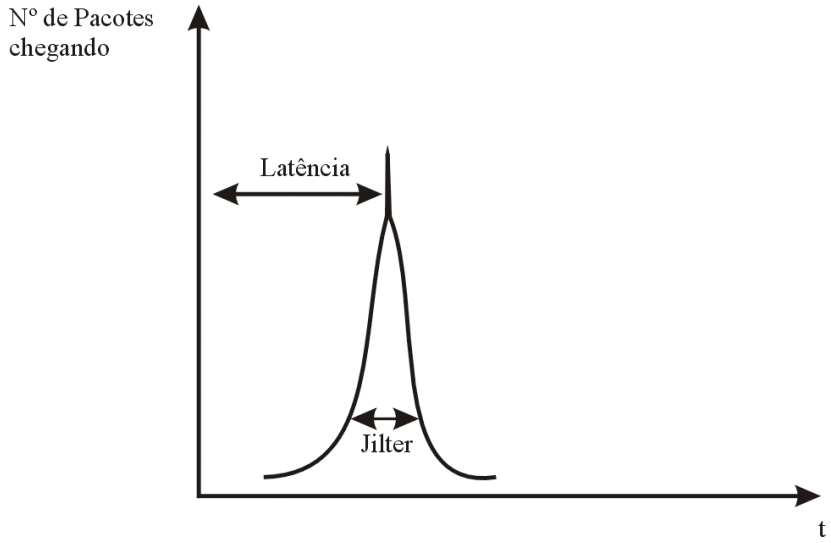

Figura 2.2 – Comparação entre latência e jitter

A conseqüência do *jitter* é que a aplicação no destino deve criar um *buffer* cujo tamanho vai depender do *jitter*, gerando mais atraso na conversação.

Esse buffer vai servir como uma reserva para manter a taxa de entrega constante no interlocutor. Daí a importância de latência e *jitter* baixos em determinadas aplicações sensíveis a esses fatores, como videoconferência.

"Skew"

O *skew* é um parâmetro utilizado para medir a diferença entre os tempos de chegada de diferentes mídias que deveriam estar sincronizadas, como mostra a Figura 2.3. Em muitas aplicações existe uma dependência entre duas mídias, como áudio e vídeo, ou vídeo e dados. Assim, numa transmissão de vídeo, o áudio deve estar sincronizado com o movimento dos lábios (ou levemente atrasado, visto que a luz viaja mais rápido que o som, e o ser humano percebe o som levemente atrasado em relação à visão). Outro exemplo é quando se tem uma transmissão de áudio explicativo e uma seta percorrendo a figura associada.

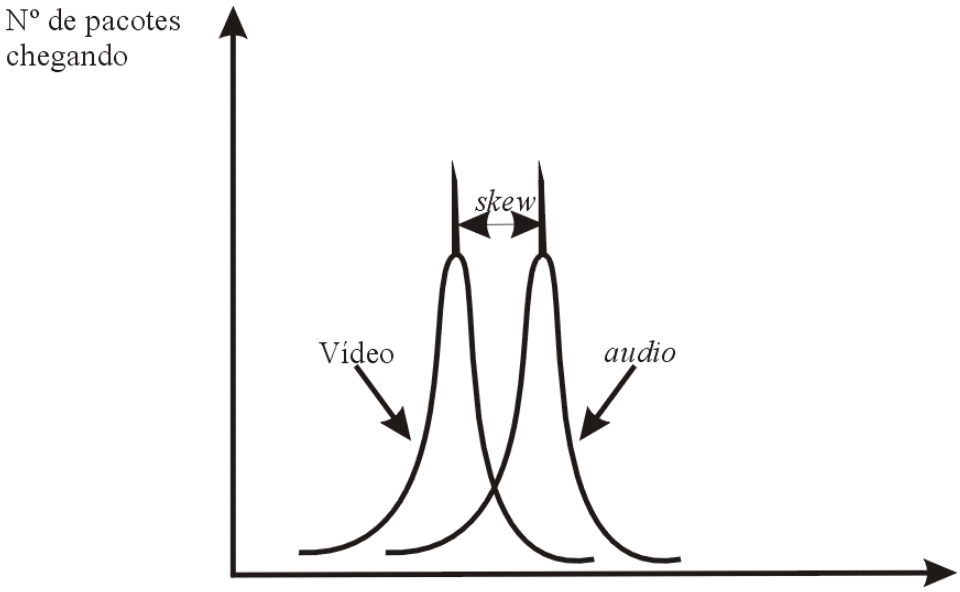

Figura 2.3 – Definição do Skew entre mídias diferentes

Tabela comparativa

A Figura 2.4 mostra algumas aplicações típicas em rede, bem como seus fatores críticos, em aplicações numa tendência de convergência nas redes.

	Telefone	Download	**TV**	Videoconferência
Latência	**Sensível**	**Insensível**	**Insensível**	Sensível
Jitter	**Sensível**	**insensível**	**Sensível**	Sensível
Skew	**-**	**Insensível**	**Sensível**	Sensível
Velocidade (largura banda)	**Baixa**	**Depende**	**Alta**	Alta

Figura 2.4 – Tabela de fatores críticos em aplicações numa tendência de convergência.

Aplicações de telefonia são sensíveis à latência e *jitter*. Caso estiverem associadas a sincronismo em alguma figura, como por exemplo, um áudio explicativo associado a uma seta se movendo numa figura, o áudio também é sensível a *skew*. Possuem velocidade baixa, de 64Kbps no padrão G.711, o mais comum em telefonia atualmente, mas pode-se chegar a apenas 8Kbps, usando a compressão no padrão G.729. (Soares, 1995)

Aplicações de *download* de dados são insensíveis à latência, *jitter* e *skew*, podem variar em necessidades de velocidade, e possuem taxa variável. Entretanto, na maior parte das vezes esse tipo de mídia não pode sofrer perdas. Pode-se imaginar o problema que pode acontecer de perdas de pacotes numa transação bancária. Já em transmissões unilaterais de áudio e vídeo, como por exemplo, TV, a latência não é tão importante, visto que não vai fazer muita diferença se a transmissão demorar 5 segundos para começar a passar. Entretanto, uma vez que começou, deve se manter até o final e com sincronismo entre áudio e vídeo, daí a necessidade de *jitter* e *skew* baixos. Aplicações de

videoconferência são muito parecidas com aplicações de voz em termos de latência e *jitter*, entretanto, possuem alta largura de banda e devem manter um baixo *skew*, pois necessitam sincronização entre áudio e vídeo.

2.6 - Qualidade de Serviço (requisitos gerais para suporte a serviço banda larga)

A camada de transporte tem como uma das principais funções a ampliação da qualidade de serviço (Quality of Service – QoS) fornecida pela camada de rede. A qualidade de serviço pode ser caracterizada por uma série de parâmetros específicos (parâmetros QoS). Entre estes podemos citar:

- O retardo no estabelecimento da conexão.
- O retardo no encerramento da conexão.
- A probabilidade de falha no estabelecimento da conexão. Isto é, a probabilidade que uma conexão não seja estabelecida dentro do retardo máximo de estabelecimento.
- A probabilidade de falha na liberação da conexão. Isto é, a fração das tentativas de liberação de conexões que não se completaram dentro do retardo máximo de encerramento.
- A vazão em cada sentido da conexão, isto é, a taxa de bits transferidos por segundo.
- O retardo de transferência médio, também em cada sentido.
- A variação estatística do retardo expressa, por exemplo, em termos da variância do retardo de transferência.
- A taxa de erro expressa em porcentagem dos bits transmitidos.
- O serviço de transporte permite ao usuário especificar valores preferências, valores aceitáveis e inaceitáveis, quando do estabelecimento de uma conexão. Alguns dos parâmetros se aplicam tanto ao serviço com conexão quanto ao serviço sem conexão. É função

da camada de transporte examinar os parâmetros requeridos e determinar se pode ou não fornecer o serviço.

- A definição da camada de transporte RM-OSI não determina a codificação ou os valores permitidos para os parâmetros QoS.

Requisitos Gerais para Suporte a Serviços de Banda Larga

Os requisitos básicos que uma rede de banda larga deve atender para dar suporte aos serviços especificados são identificados na recomendação I.211, que inclui categorias como as de: requisitos multimídia, qualidade de serviços (Quality of Service – QoS), temporização, sincronização e aspectos de sinalização.

A RDSI-FL deverá fornecer facilidades que permitam, em uma única chamada associada a um serviço, estabelecer um número de conexões que podem ser associadas a tipos específicos de tráfego. Em março de 1993, no encontro de Helsinki, o ITU-T T (International Telecommunication Union – União Internacional de Telecomunicações) aprovou uma recomendação específica para a infra-estrutura de uma rede de banda larga para dar suporte a serviços multimídia (recomendação I.374: Framework Recomendation on Network Capabilities to Support Multimedia Services).

A recomendação I.374 apresenta uma arquitetura funcional para serviços multimídia que define os elementos de controle de serviço: procedimentos executados, pelos participantes de uma chamada, para fornecer serviços multimídia. Uma chamada pode envolver a participação de várias conexões entre usuários, servidores e equipamentos de apresentação e armazenamento. As diferentes conexões podem apresentar diferentes características para atender a diferentes mídias. Os elementos de controle de serviços são utilizados para o controle das chamadas, o controle das conexões e o controle das mídias. O controle das chamadas inclui os estabelecimentos e liberação de chamadas. O

controle das conexões deve permitir o estabelecimento de conexões entre dois ou mais usuários, a inclusão de novos usuários em uma chamada, o desligamento de um participante de uma chamada e a liberação de uma conexão pertencente a uma chamada. O controle das mídias inclui a alocação e liberação de mídias em uma chamada. (Murhammer, 2000)

A qualidade de serviços (QoS) é, normalmente, um parâmetro negociado na fase de estabelecimento de uma conexão, muito embora, os procedimentos de sinalização permitam que a negociação possa ser feita também após o estabelecimento. Os parâmetros que definem uma determinada qualidade de serviço são definidos pela recomendação I.350. A recomendação I.211 reconhece que novos parâmetros podem vir a serem definidos, como a taxa de perda de células permitida (cell loss ratio). Adicionalmente, para alguns serviços, a recomendação I.211 reconhece poder ser necessária à indicação explícita, célula por célula, de uma prioridade para o descarte de células em caso de congestionamento. Essa capacidade é muito útil para minimizar a degradação da QoS para tráfegos do tipo voz ou vídeo.

CAPÍTULO III – ANÁLISE DE SERVIÇOS QoS

3.1 – Garantia de QoS

Somente o aumento na largura de banda não é suficiente para garantir a qualidade do serviço à aplicação, pois em se tratando de redes compartilhadas por múltiplos usuários e muitas vezes a longas distâncias, pode haver congestionamentos, provocando atrasos inadmissíveis em certas aplicações sensíveis, como por exemplo, voz e videoconferência. Existem algumas formas de prover qualidade de serviço às aplicações críticas: serviços integrados, serviços diferenciados, prioridade relativa e *label switching*.

3.1.1 - Prioridade Relativa

No modelo de prioridade relativa, a aplicação configura uma determinada prioridade (ou precedência) para o pacote, e os nós ao longo do caminho aplicam essa regra na hora de encaminhar o quadro. O comportamento que pode ser configurado é de atraso relativo ou prioridade de descarte. A arquitetura Diffserv pode ser considerada um refinamento desse modelo, pois especifica com maiores detalhes a importância dos domínios de tráfego, bem como os condicionadores de tráfego. Alguns exemplos desse tipo de QoS /BLA 98/ são o modelo de precedência do IPv4 definido na RFC 791, a prioridade das redes Token Ring (IEEE 802.5) e a interpretação das classes de tráfego dada no protocolo IEEE 802.1p, que será analisado a seguir.

3.1.2 - Protocolo IEEE 802.1p/Q

O protocolo IEEE 802.1p é uma técnica para priorização de tráfego em redes locais, sendo especificado na norma IEEE 802.1D – LAN Bridges /CON 99/. Através dessa técnica, é possível utilizar aplicações sensíveis a tempo em

ambientes LAN. No IEEE 802.1p, estão definidas 8 classes de tráfego. Como os pacotes Ethernet não possuem campos para priorização de tráfego, a norma 802.1p recomenda a utilização da extensão Ethernet para reconhecimento de VLANs, definida na norma 802.1Q. Essa norma adiciona 4 bytes ao pacote Ethernet a fim de reconhecimento de VLANs, e desses 4 bytes, 3 bits são reservados para priorização de tráfego.

3.1.3 - Classes de serviço no ATM

No ATM, a qualidade de serviço está especificada na camada AAL (ATM Adaptation Layer). Como as aplicações possuem necessidades diferentes, como visto no item 1.2, o ITU - T (International Telecommunication Union – União Internacional de Telecomunicações) definiu grupos de aplicações com requisitos semelhantes, baseado em três critérios:

- **Temporização entre origem e destino**: necessária ou não necessária;
- **Taxa de bit**: constante ou variável;
- **Modo de conexão**: orientado à conexão ou não.

3.2 - Serviços Integrados

O modelo de serviços integrados (IS - Integrated Services) foi definido por um grupo de trabalho da IETF (Internet Architecture Board) esse modelo de arquitetura Internet inclui o serviço de melhor tentativa usado atualmente e um novo serviço em tempo real que disponibiliza funções para reservar larguras da banda na Internet.

O IS foi desenvolvido para otimizar a utilização de redes e recursos para novos aplicativos, como multimídia em tempo real, que requer garantias de QoS. Devido aos retardos de roteamento e perdas devido ao congestionamento, os aplicativos em tempo real não funcionam muito bem na Internet atual que usa o método da melhor tentativa. Os programas de videoconferência, transmissão de

vídeo e conferências usando áudio precisam de larguras de banda garantidas a fim de obter qualidade aceitável de vídeo e de áudio. Os serviços integrados tornam isso possível dividindo o tráfego da Internet no tráfego da melhor tentativa padrão para uso tradicional e no tráfego de fluxos de dados de aplicativos como QoS garantida.

Para suportar o modelo de serviços integrados, um roteador da Internet precisa ser capaz de propiciar uma QoS apropriada para cada fluxo de dados, de acordo com o modelo do serviço. A função do roteador que propicia qualidades diferentes de serviços é chamada de controle de tráfego.

O programador de pacotes controla o direcionamento de fluxos de pacotes deferentes em hosts e roteadores com base em suas classes de serviço, usando gerenciamento de filas e vários algoritmos de programação. Ele precisa garantir que a entrega do pacote corresponda ao parâmetro de QoS de cada fluxo. Um programador de pacotes também pode policiar ou moldar o tráfego de acordo com o nível de serviços. Ele precisa ser implementado no ponto onde os pacotes são enfileirados. Esse é normalmente o nível do driver de saída em um sistema operacional e corresponde ao protocolo de camada de enlace.

O classificador de pacotes identifica os pacotes de um fluxo IP em hosts e roteadores que irão receber certo nível de serviço. Para realizar um controle efetivo de tráfego, cada pacote de entrada é mapeado pelo classificador em uma classe específica. Todos os pacotes que são classificados na mesma classe obtêm o mesmo tratamento por parte do programador de pacotes. A escolha de uma classe se baseia nos endereços de origem e de destino e no número da porta no cabeçalho do pacote existente ou em um número de classificação adicional que precisa ser adicionado a cada pacote. Uma classe pode corresponder a uma ampla categoria de fluxos de dados. Por exemplo, todos os fluxos de vídeo de uma videoconferência com vários participantes podem pertencer a uma classe de

serviço. Mas também é possível que apenas um fluxo pertença a uma classe específica de serviço.

O controle de admissão contém o algoritmo de decisão que um roteador usa para determinar se há recursos de roteamento suficientes a fim de aceitar a QoS solicitada para um novo fluxo de dados. Se não houver recursos de roteamento livres suficientes, a aceitação de um fluxo novo de dados iria prejudicar garantias anteriores e o novo fluxo precisa ser rejeitado. Se o novo fluxo for aceito, a solicitação de reserva no roteador designa o classificador de pacotes e o programador de pacotes para reservarem a QoS reservada para esse fluxo. O controle de admissão é chamado em cada roteador ao longo do caminho de reserva, para tomar uma decisão de aceitação/rejeição na hora que um host requisitar um serviço de tempo real. O algoritmo de controle de admissão precisa ser consistente com o modelo do serviço.

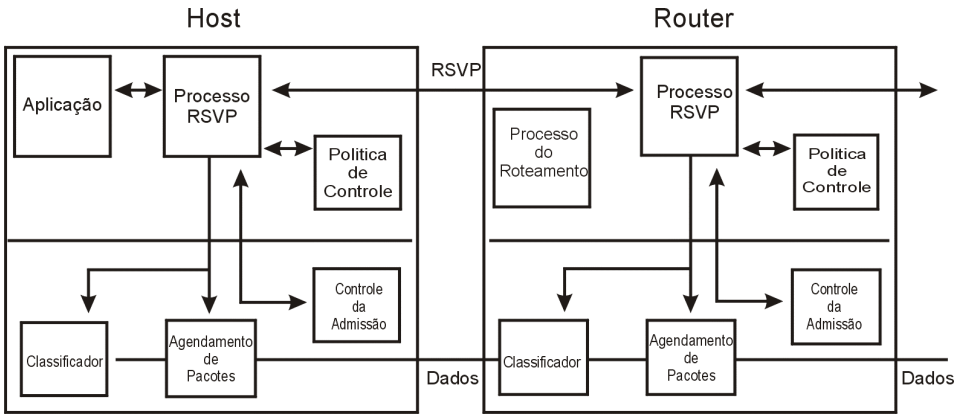

Figura 3.1 – Modelo de Serviços Integrados.

Note que o controle de admissão algumas vezes torna-se confuso com a fiscalização, que é uma função pacote a pacote processada pelo programador de pacotes. Ela garante que um host não viole suas características de tráfego definidas. Apesar disso, para garantir que as garantias de QoS sejam honradas, o controle de admissão estará preocupado com o esforço das políticas administrativas sobre as reservas de recursos. Algumas políticas serão usadas

para verificar a autenticação dos usuários para uma reserva requisitada. Requisições de reservas não autorizadas podem ser rejeitadas. O controle de admissão terá um papel importante nos custos dos recursos da Internet no futuro. A Figura 3.3 mostra a operação do modelo de serviços integrados em um host e em um roteador.

Os serviços integrados usam o RSVP (Reservation Protocol – protocolo de reserva) para a sinalização das mensagens de requisição de reservas. As instâncias IS se comunicam via RSVP para criar e manter estados de fluxos específicos nos hosts dos pontos terminais e nos roteadores ao longo do caminho de um fluxo de dados.

O aplicativo que quiser enviar pacotes de dados em um fluxo reservado se comunica com a instância de fazer reservas RSVP. O protocolo RSVP tenta fazer uma reserva de fluxo com a QoS solicitada, a qual será aceita se o aplicativo atender às restrições do plano de ação e os roteadores puderem lidar com a QoS requisitada. O RSVP informa ao classificador de pacotes e ao programador de pacotes em cada nó para processar os pacotes desse fluxo adequadamente. Se o aplicativo enviar agora os pacotes de dados para o classificador no primeiro nó, o qual classificou esse fluxo em uma classe de serviço específica de acordo com a QoS solicitada, o fluxo será reconhecido como o endereço IP do emissor e será transmitido para o programador de pacotes. Este encaminha os pacotes, dependendo de suas classes de serviço, para o roteador seguinte ou, finalmente, para o host de recepção.

Como o RSVP é um protocolo simplex, as reservas de QoS são feitas somente em uma direção, do nó emissor para o nó receptor. Se o aplicativo de nosso exemplo quiser cancelar a reserva do fluxo de dados, ele envia uma mensagem para a instância de reserva que libera os recursos da QoS reservados em todos os roteadores ao longo do caminho, podendo então esses recursos

serem usados para outros fluxos de dados. As especificações IS estão definidas na RFC 1633.

3.2.1 - Classes de serviços

O modelo de serviços integrados usa classes diferentes de serviços que são definidas pelo grupo de trabalho IETF de serviços integrados. Dependendo do aplicativo, essas classes de serviços propiciam limites mais estreitos ou tolerantes nos controles de QoS. O modelo IS atual inclui o Guaranteed Service (serviço garantido) definido na RFC 2212 e o Controlled Load Service (serviço de carga controlada) definido na RFC 2211. Para entender essas classes de serviços, alguns termos precisam ser aplicados.

Como o modelo IS fornece reservas por fluxo, a cada fluxo é atribuído um descritor de fluxo. Este define as características de tráfego e QoS para um fluxo específico de pacotes de dados. Nas especificações IS, o descritor de fluxo consiste de uma especificação de filtro e uma especificação de fluxo.

A especificação de filtro é usada para identificar os pacotes que pertencem a um fluxo específico com o endereço IP do emissor e a porta de origem. A informação da especificação de filtro é usada no classificador de pacotes. A especificação de fluxo contém um conjunto de parâmetros que são chamados de informação de chamada. É possível ordenar a informação de chamada em dois grupos:

- Especificação de Tráfego (Tspec)
- Especificação de Requisição (Rspec)

A especificação de tráfego descreve as características de tráfego requisitado. No modelo IS essa especificação é representada por um filtro chamado de token bucket (balde de fichas). Esse princípio define um mecanismo de controle de fluxo de dados que adiciona fichas (tokens) em intervalos de tempo periódicos em um buffer (o balde – bucket) e permite que um pacote de dados deixe o

emissor somente se houver pelo menos tantas fichas no balde quanto o comprimento do pacote de dados. Essa estratégia permite um controle preciso do intervalo entre dois pacotes de dados na rede. Esse sistema é especificado por dois parâmetros: a taxa de fichas ® que representa a taxa na qual as fichas são colocadas no balde e a capacidade do balde (b). Ambos, r e b têm que ser valores positivos.

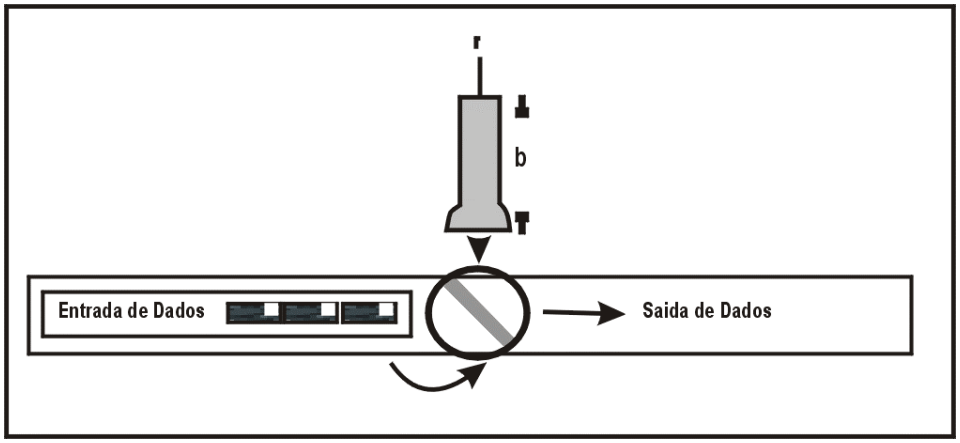

Figura 3.2 – "Token Bucket" (balde de fichas)

O parâmetro r especifica a taxa de dados em longo prazo e é medida em bytes de pacotes IP por segundo. O valor desse parâmetro pode variar de 1 byte por segundo a até 40 terabytes por segundo. O parâmetro b especifica o montante de dados momentâneos permitido pelo sistema e é medido em bytes. O valor desse parâmetro pode variar de 1 bytes a 250 gigabytes. As faixas de valores permitidas para esses parâmetros são propositadamente grandes para que o sistema esteja preparado para as tecnologias de rede do futuro. Não se espera que os elementos de rede suportem essa faixa tão ampla de valores. O tráfego que passa pelo filtro do balde de fichas tem que obedecer à regra de que, durante todos os períodos T de tempo, o montante de dados enviados não deve

exceder rT+b, onde r e b são os parâmetros do filtro. A Figura 3.4 mostra um filtro “Token Bucket”.

Dois outros parâmetros do balde de fichas também fazem parte da especificação de tráfego. A unidade policiada mínima m e o tamanho de pacote máximo M. O parâmetro m especifica o tamanho mínimo do pacote IP em bytes. Pacotes menores são contados como tendo tamanho m. O parâmetro M especifica o tamanho máximo dos pacotes em bytes que estão de acordo com as especificações de tráfego. Os elementos da rede precisam rejeitar uma requisição de serviço se o tamanho máximo de pacote requisitado for maior que o tamanho MTU do enlace. Resumindo, o filtro de balde de fichas é uma função de fiscalização que isola os pacotes que estão de acordo com a especificação de tráfego daqueles que não estão.

A especificação de requisição especifica a Qualidade de Serviço que o aplicativo quer requisitar para um fluxo específico. Essa informação depende do tipo de serviço e das necessidades do aplicativo que solicita a QoS. Ela pode consistir de uma largura de banda específica, um retardo máximo de pacote ou uma taxa de perda máxima de pacotes. Na implementação IS, a informação das especificações de tráfego e de requisição é usada no programador de pacotes. (Tanenbaum, 1997)

3.2.2 - Serviço de carga controlada

O serviço de carga controlada tem a intenção de suportar a classe de aplicativos que são altamente sensíveis às condições de sobrecarga na Internet, tal como ocorre com os aplicativos de multimídia. Esses aplicativos funcionam bem em redes não carregadas, mas degradam rapidamente em condições sobrecarregadas. Se um aplicativo usa o serviço de carga controlada, o desempenho de um fluxo de dados específico não irá degradar caso a carga da rede aumente.

O serviço de carga controlada oferece somente um nível de serviço que é intencionalmente mínimo. Não há recursos opcionais ou outras capacidades na especificação. O serviço oferece somente uma única função. Ele aproxima o serviço de melhor-tentativa em redes levemente carregadas. Isso significa que os aplicativos que fazem reserva de QoS usando os serviços de carga controlada recebem um serviço equivalente bem próximo ao serviço fornecido por um tráfego de melhor tentativa não controlado em condições de sobrecarga leve. Nesse contexto, condições levemente carregadas significam que um percentual alto de pacotes transmitidos será entregue com sucesso ao destino, e o retardo de trânsito de um percentual alto de pacotes entregues não irá exceder muito o retardo mínimo de trânsito. Cada roteador em uma rede que aceita pedidos de serviços de carga controlada precisa garantir que uma largura de banda adequada e os recursos de processamento de pacotes estejam disponíveis para processar a solicitações de reservas de QoS. Isso pode ser realizado com o controle de admissão ativo. Antes que um roteador aceite uma nova reserva de QoS, representada pela especificação de tráfego, ele precisa considerar todos os recursos importantes, tais como largura de banda de enlaces, espaço de buffer do roteador de swicth e a capacidade computacional de encaminhamento de pacotes
.

A classe de serviço de carga controlada não aceita ou não faz uso de valores-alvo específicos para parâmetros de controle como largura de banda, retardo ou perda. Aplicativos que usam os serviços de carga controlada precisam suportar e ser a prova de perdas e retardos de pacotes.

As reservas de QoS usando os serviços de carga controlada precisam fornecer uma especificação de tráfego que consista dos parâmetros **r** e **b** do balde de fichas bem como a unidade **m** policiada mínima e o tamanho **M** de pacote máximo. Uma especificação de requisição não é necessária porque os serviços de carga controlada não oferecem funções para reservar uma largura de

banda fixa ou garantir retardos de pacotes mínimos. Os serviços de carga controlada fornecem controle de QoS somente para tráfego que esteja de acordo com a especificação de tráfego fornecida no momento da montagem do pacote. Isso significa que as garantias do serviço aplicam-se somente aos pacotes que respeitam a regra do balde de fichas que diz que durante todos os períodos de tempo T, o montante de dados enviados não pode exceder rT=b.

Os serviços de carga controlada são projetados para aplicativos que podem tolerar uma quantia razoável de perda e retardo de pacotes, tal como software de aplicativos de áudio e videoconferência.

3.2.3 - Serviço garantido

O modelo de serviço garantido propicia funções que garantem que os pacotes cheguem em um tempo de entrega garantido. Isso significa que cada pacote de um fluxo que está de acordo com as especificações de tráfego vai chegar pelo menos até o tempo de retardo máximo especificado no descritor do fluxo. O serviço garantido é usado em aplicativos que precisam de uma garantia que o pacote vai chegar ao receptor não depois de certo tempo após ter sido transmitido da sua origem.

Por exemplo, os aplicativos multimídia em tempo real, como sistemas de transmissão de vídeo e áudio que usam tecnologias de sequenciamento de dados, não podem permitir que os pacotes cheguem depois do momento específico de sua exibição. Aplicativos que apresentam exigências críticas em tempo real, como a distribuição em tempo real de dados financeiros (preços compartilhados), também precisam de um serviço garantido. O modelo de serviço garantido não minimiza a variação (a diferença entre os retardos máximo e mínimo dos pacotes), mas ele controla o retardo máximo de enfileiramento.

O modelo de serviço garantido representa a extremidade final do controle de retardos em redes. Outros modelos de serviços que propiciam

controle de retardos apresentam restrições muito mais tolerantes. Por isso, o modelo de serviço garantido é somente útil se for implementado em cada roteador ao longo do caminho de reserva.

O modelo de serviço garantido fornece aos aplicativos um controle considerável sobre sus retardos. É importante entender que o retardo em uma rede IP tem duas partes: um retardo de transmissão fixa e um retardo de variável de enfileiramento. O retardo fixo depende do caminho escolhido, o qual é determinado não por serviço garantido, mas pelo mecanismo de configurações. Todos os dados de pacotes em uma rede IP têm um retardo mínimo que é limitado pela velocidade da luz e pelo tempo de retorno dos pacotes de dados em todos os roteadores do caminho de roteamento. O retardo de enfileiramento é determinado pelo serviço garantido e é controlado pelos dois parâmetros já vistos: o balde de fichas (em particular, o tamanho b do balde) e a largura de banda R solicitada pela reserva. Esses parâmetros são usados para construir o modelo de fluido para o comportamento ponta a ponta de um fluxo que usa serviços garantidos.

O modelo de fluido especifica o serviço que seria propiciado por um enlace dedicado entre emissor e receptor que tenha a largura de banda R. No modelo de fluido, o serviço de fluxo é completamente independente do serviço de outros fluxos. A definição de serviço garantido conta com o resultado de que o retardo do fluido de um fluxo obedecendo a um balde de fichas (r, b) e sendo servido por uma linha com largura de banda R é controlado por b/R enquanto R não for menor que r. O modelo de serviço garantido aproxima esse comportamento da taxa de serviço R, onde agora R é uma parte da largura de banda através do caminho de roteamento e não largura de banda de uma linha dedicada.

No modelo de serviço garantido, as especificações de tráfego e de requisição são usadas para preparar uma reserva de fluxo. A especificação de

tráfego é representada pelos parâmetros do balde de fichas. A especificação de requisição contém o parâmetro R que especifica a largura de banda da reserva de fluxo. O modelo de serviço garantido é definido na RFC 2212.

3.2.4 - O RSVP – Reservation Protocol

O modelo de Serviços Integrados usa o RSVP (Reservation Protocol – protocolo de reserva) para preparar e controlar as reservas de QoS. O RSVP é definido na RFC-2205 e tem o status de uma padrão proposto. Como o RSVP é um protocolo de controle da Internet e não um protocolo de roteamento, ele requer a existência de um protocolo de roteamento para operar. O protocolo RSVP executa baseado no IP e do UDP e precisa ser implementado em todos os roteadores no caminho de reserva. Os conceitos-chave do RSVP são fluxos e reservas.

Uma reserva RSVP se aplica a um fluxo específico de pacotes de dados em um caminho específico através dos roteadores. Um fluxo é definido como um fluxo de dados distinguível de pacotes relacionados de um único emissor para um único receptor. Se o receptor for um endereço de multicast, um fluxo pode alcançar múltiplos receptores. O RSVP fornece o mesmo serviço para fluxos de unicast e de multicast. Cada fluxo é identificado no RSVP por seu endereço IP de destino e sua porta de destino. Todos os fluxos têm um descritor de fluxo dedicado que contém a QoS que um fluxo específico requer. O protocolo RSVP não entende o conteúdo do descritor de fluxo. Ele é transportado como um objeto opaco pelo RSVP e é entregue às funções de controle de tráfego do roteador (classificador e programador de pacotes) para processamento.

Como o RSVP é um protocolo simplex, as reservas são feitas somente em uma direção. Na conexão duplex, como conferências de vídeo e áudio em

que cada emissor é também um receptor, torna-se necessário montar duas sessões RSVP para cada estação.

O protocolo RSVP é iniciado pelo receptor. Usando mensagens de sinalização RSVP, o emissor propicia uma QoS específica para o receptor que envia uma mensagem de reserva RSVP de volta com a QoS que deveria ser reservada para o fluxo do emissor para o receptor. Esse comportamento considera as exigências de QoS diferentes para receptor heterogêneos em grandes grupos de multicast. O emissor não precisa saber quais são as características de todos os possíveis receptores para estruturar as reservas.

Para estabelecer uma reserva com RSVP, os receptores enviam requisições de reservas para os emissores dependendo das capacidades de seus sistemas. Por exemplo, uma estação de trabalho rápida e um PC lento querem receber um vídeo MPEG de alta qualidade com 30 quadros por segundo que tem uma taxa de dados de 1,5 Mbps. A estação de trabalho tem capacidade suficiente para decodificar o vídeo, mas o PC só consegue decodificar 10 quadros por segundo. Se o servidor de vídeo enviar as mensagens para os dois receptores dizendo que ele pode enviar o fluxo de vídeo a 1,5 Mbps, a estação de trabalho pode retornar uma requisição de reserva para 1,5 Mbps. Mas o PC não precisa de toda a largura de banda para esse fluxo já que ele não conseguiria decodificar todos os quadros. Assim, o PC poderia enviar uma requisição de reserva para um fluxo com 10 quadros por segundo e 500 Kbps.

3.2.5 - Operação do RSVP

Uma parte básica da reserva de um recurso é o caminho. Um caminho significa o lugar por onde vai passar um fluxo de pacotes através de roteadores diferentes a partir do emissor até chegar ao receptor. Todos os pacotes que pertencem a um fluxo específico irão usar o mesmo caminho. Esse caminho é determinado se um emissor gerar mensagens de caminho RSVP que viajam no

mesmo sentido do fluxo. Cada host emissor envia periodicamente uma mensagem de caminho para cada fluxo de dados que ele origina. A mensagem de caminho contém informações de tráfego que descrevem a QoS para um fluxo específico. Como o RSVP não faz o roteamento sozinho, ele usa a informação das tabelas de roteamento em cada roteador para encaminhar as mensagens RSVP.

Se a mensagem de caminho chegar ao primeiro roteador RSVP, o roteador armazena o endereço IP do último campo da mensagem, que é o endereço do emissor. A seguir, o roteador insere seu próprio endereço IP no campo último salto, envia a mensagem de caminho para o roteador seguinte e o processo se repete até que a mensagem tenha chegado no receptor. Ao final desse processo, cada roteador saberá o endereço do roteador anterior e o caminho poderá ser acessado no sentido contrário. A Figura 3.5 mostra o processo de definição do caminho.

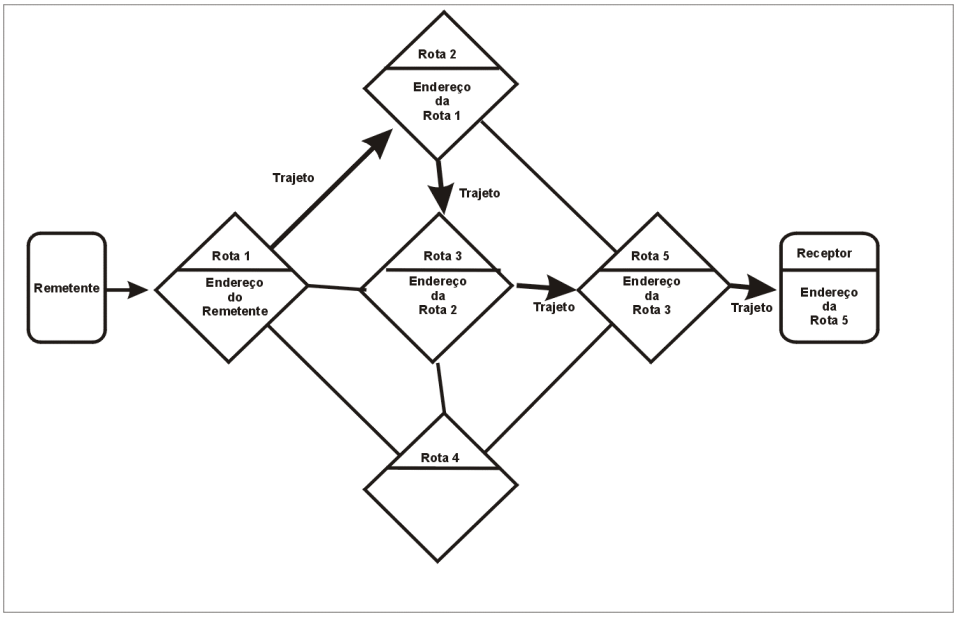

Figura 3.3 – Processo de definição de um caminho RSVP

Os roteadores que receberam uma mensagem de caminho estão preparados para processar as reserva de recursos de um fluxo de dados. Todos os pacotes que pertencem a esse fluxo irão passar pelos mesmos roteadores: o caminho definido pelas mensagens de caminho.

O estado de um sistema após enviar as mensagens de caminho é o seguinte: todos os receptores sabem que um emissor pode fornecer uma QoS especial para um fluxo e todos os roteadores sabem sobre a possível reserva de recursos para esse fluxo.

Agora, se um receptor quiser reservar QoS para esse fluxo, ele envia uma mensagem de pedido de reserva. Essa mensagem de reserva contém a QoS solicitada por esse receptor para um fluxo específico e é representada pelas especificações de filtro e de fluxo que formam o descritor do fluxo. O receptor envia a mensagem de pedido de reserva para o último roteador no caminho com o endereço que ele recebeu da mensagem de caminho. Como cada dispositivo capaz de RSVP sabe o endereço do dispositivo anterior do caminho, as mensagens de reserva percorrem o caminho no sentido oposto em direção ao emissor e estabelecem a reserva dos recursos em cada roteador. A Figura 3.6 mostra o fluxo das mensagens de reserva através dos roteadores.

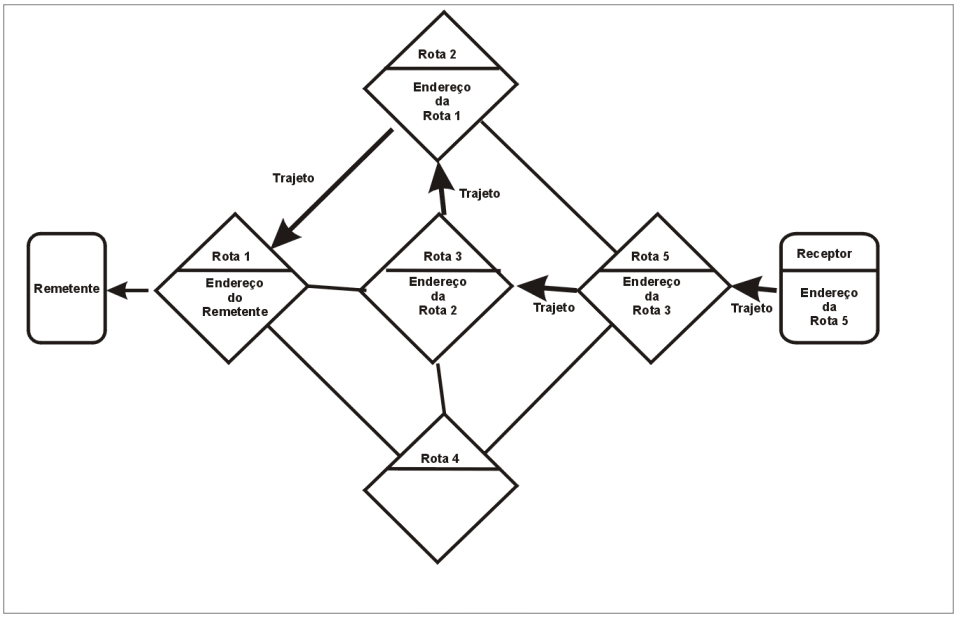

Figura 3.4 – Fluxo de mensagens de requisição de reserva RSVP

3.2.6 - Reserva de QoS no enlace

O processo RSVP passa a requisição para o controle de admissão e para a instância de controle de plano de ação do nó. O controle de admissão verifica se o roteador tem os recursos necessários para estabelecer a nova reserva de QoS e o controle de plano de ação verifica se o aplicativo tem a autorização para fazer requisições de QoS. Se um desses testes falharem, a reserva será rejeitada e o processo RSVP retornará uma mensagem de erro ResvErr (erro na requisição de reserva) para o receptor apropriado. Se os dois testes forem bem-sucedidos, então o nó vai usar as informações da especificação de fluxo para preparar o programador de pacotes. Depois disso, o classificador de pacotes irá reconhecer os pacotes que pertencem a esse fluxo e o programador de pacotes irá obter a QoS desejada definida pela especificação de fluxo. A Figura 3.7 mostra o processo de reserva em um roteador.

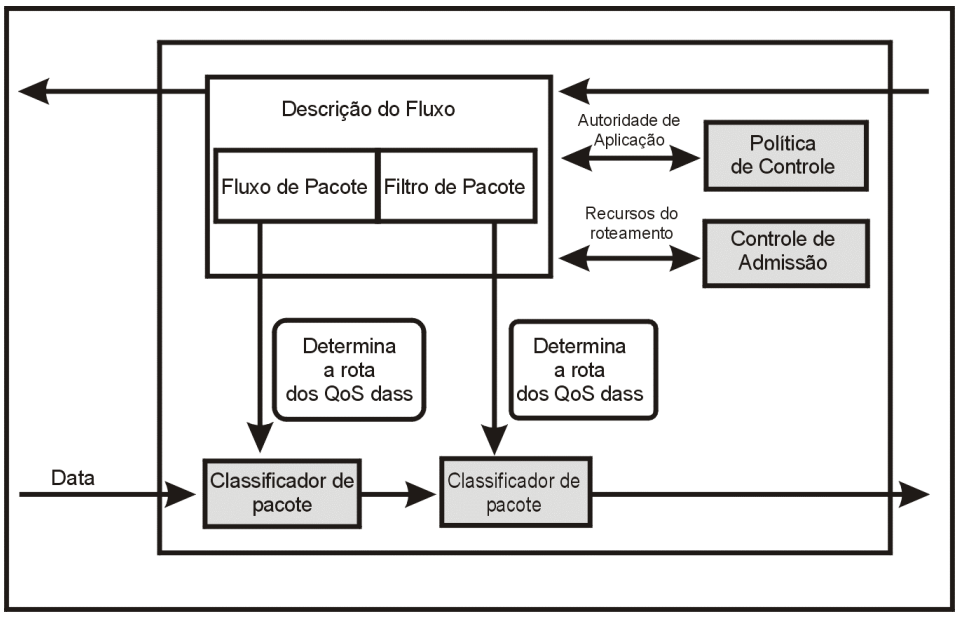

Figura 3.5 – Processo de reserva RSVP

3.2.7 - Encaminhamento da requisição de reserva

Após um teste de admissão e plano de ação bem-sucedido, uma requisição de reserva é propagada na direção do emissor. Em um ambiente de multicast, um receptor pode obter dados de vários emissores. O conjunto de hosts emissores para os quais certas requisições de reserva são propagadas é chamado de alvo da requisição. A requisição de reserva que é encaminhada por um nó após uma reserva aprovada pode diferir de uma requisição que foi recebida do salto anterior no caminho em direção ao receptor. Uma razão possível disso é que o mecanismo de controle de tráfego pode modificar a especificação de fluxo a cada salto. Outro motivo mais importante é que em um ambiente de multicast, as reservas oriundas de ramos inferiores diferentes, mas para o mesmo emissor são reunidas juntas à medida que percorrem o caminho upstream, na direção do emissor. Essa aglutinação é necessária para conservar recursos nos roteadores.

Uma requisição de reserva aprovada propaga-se na direção do emissor pela árvore de multicast até chegar a um ponto onde uma reserva existente seja igual ou maior que a que está sendo requisitada. Nesse ponto, a requisição que acaba de chegar é aglutinada com a reserva existente e não precisa mais ser passada adiante. A figura 3.8 mostra a aglutinação de reservas em um fluxo multicast.

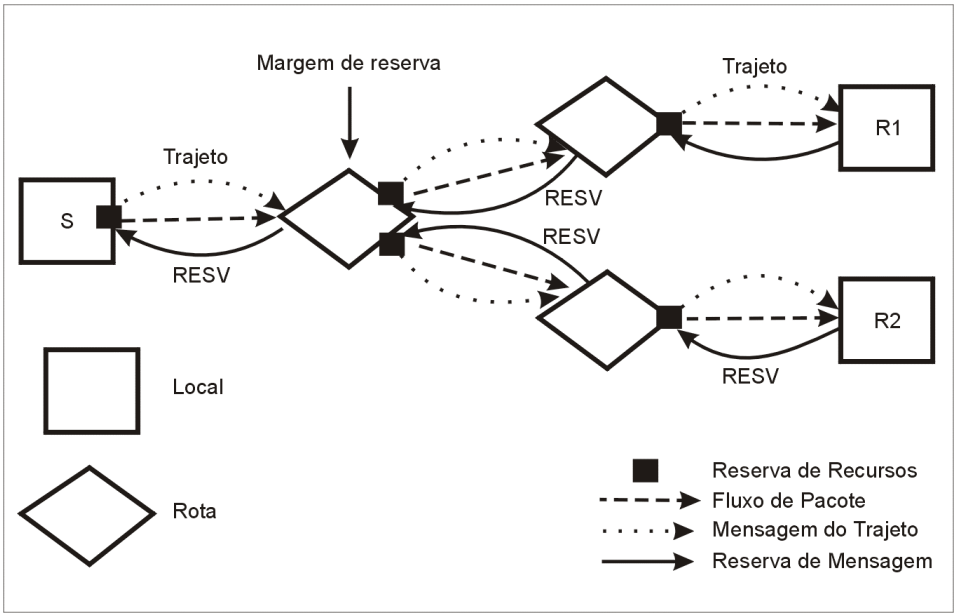

Figura 3.6 – Aglutinação de reservas RSVP em fluxos de Multicast

Se a requisição de reserva chegar ao emissor, a reserva de QoS será estabelecida em cada roteador do caminho e o aplicativo poderá começar a enviar pacotes aos receptores. O classificador de pacotes e o programador de pacotes em cada roteador garantem que os pacotes são encaminhados de acordo com a QoS requisitada.

Esse tipo de reserva é possível somente se todos os roteadores no caminho suportarem RSVP. Se apenas um roteador não suportar a reserva, o serviço não poderá ser garantido em todo o caminho por causa das restrições de

“melhor tentativa” que se aplicam aos roteadores normais. Um roteador no caminho que não suporte RSVP representaria um gargalo para o fluxo.

Um receptor que origine uma requisição de reserva também pode requisitar uma mensagem de confirmação que indique que a requisição foi instalada na rede. O receptor inclui uma requisição de confirmação na mensagem de requisição de reserva e obtém uma mensagem de confirmação se a reserva tiver sido estabelecida com sucesso.

As reservas de recursos RSVP mantêm seus estados via software nos roteadores e hosts, o que significa que uma reserva será cancelada se um RSVP não enviar mensagens de atualização ao longo do caminho para uma reserva existente. Isso permite realizar mudanças de rota sem ocasionar sobrecarga do protocolo. As mensagens de caminho também precisam ser reenviadas porque os campos de estado do caminho nos roteadores serão reinicializados após um período de tempo.

Os estados de caminho e reserva também podem ser removidos por mensagens RVSP chamadas de teardown. Há dois tipos de mensagens “teardown”:

- Mensagens Path Tear

  As mensagens “Path Tear” percorrem o caminho downstream a partir do ponto de iniciação de todos os receptores, removendo o estado do caminho bem como todos os estados de reservas dependentes em cada dispositivo capaz de RSVP.
- Mensagens ResvTear

  As mensagens “ResvTear” percorrem o caminho upstream a partir do ponto de iniciação de todos os emissores, removendo os estados de reservas em todos os roteadores e host.

Uma requisição de remoção de caminhos e reservas pode ser iniciada por emissores, receptores ou roteadores que notarem um tempo excedido de estado.

Devido ao princípio de estado de software das reservas RSVP, não é realmente necessário remover explicitamente uma reserva antiga. Mesmo assim, é recomendado que todos os hosts de ponta enviem uma requisição de remoção se uma reserva existente não for mais necessária.

3.2.8 - RSVP e Roteadores

O RSVP também pode ser executado em roteadores e funciona em conjunto com as solicitações sendo transmitidas por um aplicativo de rede. O RSVP é usado em roteadores para encaminhar solicitações de QoS para todas as estações ao longo do caminho ou caminhos de um determinado fluxo. Também cabe aos roteadores estabilizar e manter um estado de RSVP. Em outras palavras, se um aplicativo faz uma solicitação de RSVP, cada roteador deve encaminhá-lo para outro roteador na rota até a origem; sem o caminho contrário, do receptor para o remetente.

Um processo de RSVP utiliza a tabela de rotas local para obter rotas.

A QoS é implementada por uma coleção de mecanismos conhecidos como controle de tráfego. Isso inclui três mecanismos:

- Classificador de pacote: Determina a classificação de QoS's e possivelmente o roteador para cada pacote.
- Controle de admissão: Determina se recursos estão disponíveis para aceitar ou rejeitar uma solicitação.
- Programador de pacote: Arquiva a QoS prometida para cada interface de saída. Dois módulos dentro do RSVP conhecidos como *controle de admissão e controle de diretiva* são usados por uma solicitação de RSVP. O controle de admissão determina se o nó tem os recursos disponíveis para aceitar a solicitação. O controle de diretiva determina os direitos de permissão do solicitante. Se uma dessas verificações falharem, o solicitante é descartado e a mensagem é enviada de volta

para o solicitante (o aplicativo que fez a solicitação), indicando o tipo de falha. Se ambas as verificações forem removidas, os parâmetros serão definidos no classificador de pacote e no programador de pacote na esperança de obter os recursos exigidos pela solicitação.

3.3 - Serviços Diferenciados

O conceito de Serviços Diferenciados (DS) está atualmente sendo desenvolvido no grupo de trabalho DS da IETF. As especificações DS estão definidas em alguns esboços sobre a Internet IETF e não há nenhuma recomendação RFC disponível ainda.

O objetivo do desenvolvimento de DS é conseguir a possibilidade de fornecer classes diferenciadas de serviços para tráfego Internet e suportar vários tipos de aplicativos e requisitos específicos de negócios. DS oferece desempenho previsível (retardo, capacidade máxima, perda de pacotes etc.) para uma dada carga em um dado momento. A diferença entre os serviços integrados e os serviços diferenciados é que estes propiciam discriminação de serviços progressiva na Internet sem precisar de estados por fluxo e de sinalização a cada salto. Não é necessário realizar uma reserva de QoS em cada fluxo. Com DS, o tráfego Internet é dividido em diferentes classes com diferentes requisitos de QoS.

Um componente central do DS é o SLA (Service Level Agreement – acordo de nível de serviço). O SLA é um contrato de serviço entre um cliente e um provedor de serviços que especifica os detalhes da classificação de tráfego e o serviço de encaminhamento correspondente que um cliente deve receber. Um cliente poderia ser uma organização de usuários ou outro domínio DS. O provedor de serviços precisa garantir que o tráfego de um cliente, com o qual ele tem um SLA, obtém a QoS contratada. Assim, a administração da rede do

provedor de serviços precisa definir os planos de ação dos serviços apropriados e medir o desempenho da rede para garantir o desempenho de tráfego combinado.

Para distinguir os pacotes de dados de clientes diferentes em dispositivos de rede capazes de DS, os pacotes de IP são modificados em um campo específico. Um pequeno padrão de bits, chamado byte DS, cada pacote IP é usado para marcar os pacotes que irão receber um tratamento de encaminhamento particular em cada nó da rede. O byte DS usa o espaço do octeto TOS no cabeçalho IP Ipv4, "Formato de um Pacote IP", e o octeto da classe de tráfego no cabeçalho de Ipv6. Todo tráfego da rede dentro de um domínio recebe um serviço que depende da classe de tráfego especificada no byte DS.

Para oferecer os serviços em conformidade com o SLA, os mecanismos a seguir precisam ser combinados em uma rede:

- Configurar os bits do byte DS (octeto TOS) nas bordas da rede e nas fronteiras administrativos.
- Usar esses bits para determinar como os pacotes são tratados pelos roteadores dentro da rede.
- Condicionar os pacotes marcados nas fronteiras da rede de acordo com os requisitos de QoS de cada serviço.

A arquitetura DS atualmente definida propicia somente a diferenciação de serviços em um sentido e, portanto, é assimétrica. O desenvolvimento de uma arquitetura simétrica complementar é assunto atual de pesquisas. O parágrafo a seguir descreve a arquitetura com mais detalhes.

3.3.1 - Arquitetura de serviços diferenciados

Diferente dos serviços integrados, as garantias de QoS nos serviços diferenciados são estáticas e permanecem por muito tempo nos roteadores. Isso significa que os aplicativos usando DS não precisam fazer reservas de QoS para

pacotes de dados específicos. Todo o tráfego que passa por redes capazes de DS pode receber uma QoS específica. Os pacotes de dados precisam ser marcados com o byte DS que é interpretado pelos roteadores da rede.

3.3.2 - Uso de RSVP com serviços diferenciados

O protocolo RSVP habilita os aplicativos a sinalizarem para uma rede às requisições por fluxo. Os parâmetros dos serviços integrados são usados para quantificar esses requisitos visando o controle de admissão. Mas o RSVP e os serviços integrados têm algumas limitações básicas que impedem a aplicação desses mecanismos na Internet como um todo:

- A dependência do RSVP dos estados por fluxo e dos processamentos por fluxos aumenta a preocupação com a capacidade de ampliação em grandes redes.

- Hoje em dia, um pequeno número de host gera sinalização RSVP. Embora se espera que esse número cresça dramaticamente, muitos aplicativos podem nunca vir a gerar a sinalização RSVP.

- Muitos aplicativos exigem alguma forma de Qos, mas são incapazes de expressar essas necessidades usando o modelo IS.

Essas desvantagens podem ser superadas se os Serviços Integrados forem implementados somente em intranets e usarem Serviços Diferenciados na Internet como backbone.
A Figura 3.9 mostra uma estrutura de rede imaginária.

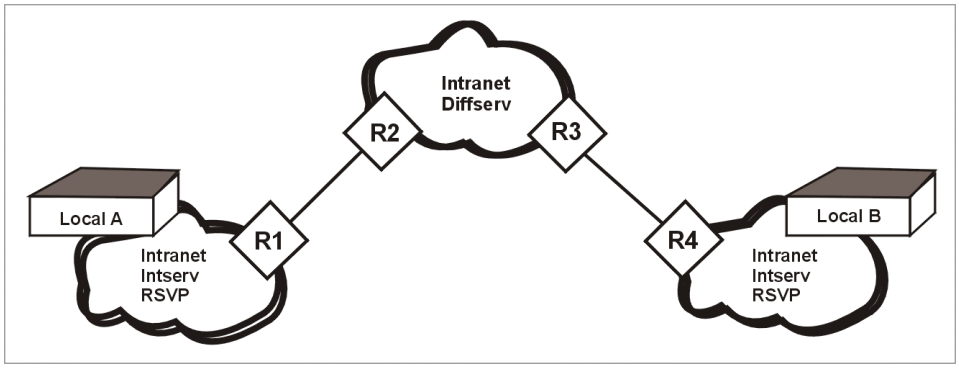

Figura 3.7 – Uso de RSVP com serviços diferenciados

Duas intranets de clientes capazes de RSVP são conectadas ao backbone Internet DS. Os roteadores R2 e R3 são roteadores de fronteira que podem condicionar o tráfego de entrada e de saída nas interfaces da rede DS com as redes IS. Em nosso exemplo, os roteadores de fronteira não são necessários para executar RSVP. Espera-se que eles implementem as funções de fiscalização do roteador DS de ingresso. Deve haver um conjunto de serviços de ponta a ponta definidos na rede DS que permite o mapeamento das reservas de fluxo RSVP para uma classe de serviço DS apropriada. Os roteadores na rede DS precisam fornecer um conjunto de comportamento por salto, que propicia o serviço de uma conexão real ponto a ponto. Deve ser possível aos aplicativos RSVP chamar níveis de serviços específicos de ponta a ponta para seus fluxos de tráfego na rede DS. Nesse modelo, as intranets IS são clientes da Internet DS.

Os roteadores de borda R1 e R4 são roteadores especiais que trabalham tanto na região RSVP/IS como na região DS da rede. Esses roteadores podem ser vistos como divididos em duas metades. Uma metade suporta RSVP padrão e faz interface com as intranets. A outra metade suporta DS e faz interface com a Internet DS. A metade RSVP precisa ser, pelo menos, capaz parcialmente de RSVP. O Roteador precisa ser capaz de processar mensagens PATH e RESV mais não é preciso que suporte classificação de pacotes e armazenamento de

estados RSVP. A metade DS do roteador propicia a interface com a função de controle de admissão na rede DS. Se o acordo de serviço entre as intranets IS e a Internet DS for estático, o serviço de controle de admissão pode ser uma tabela simples que especifica a QoS em cada nível de serviço. Se o acordo de serviço for dinâmico, o serviço de controle de admissão se comunica com as contrapartes dentro da rede DS para tomar decisões de controle de admissão com base na capacidade da rede.

Em nosso modelo, a sinalização RSVP é usada para propiciar controle de admissão para níveis de serviços específicos nas redes DS e IS. As mensagens de sinalização RSVP transportam uma descrição de QoS IS que especifica o tipo de serviço que deve ser propiciado nas regiões IS da rede. Na fronteira ente uma rede IS e uma rede DS os roteadores de borda correlacionam a QoS IS requisitadas com um nível de serviço DS apropriado. Depois disso, o roteador de borda pode prover controle de admissão para a rede DS, aceitando ou rejeitando a requisição de QoS com base na capacidade disponível no nível de serviço DS requisitado. Se uma mensagem de reserva RSVP oriunda da rede IS chegar em um roteador de borda, o descritor de fluxo RSVP será mapeado em um PHB que representa o nível de serviço correspondente na rede DS. O roteador de borda acrescenta o valor PHB à mensagem de reserva RSVP que é transportada para o host de envio. O host emissor então marca todos os pacotes de saída com esse valor de PHB. Esse método permite garantir uma QoS de ponta a ponta para aplicativos RSVP em intranets diferentes que usem a Internet DS como backbone.

3.4 - Funcionalidade dos Sistemas de QoS

Os sistemas para gerência de rede padrão não são mais suficientes para fornecer as funcionalidades adequadas à gerência das modernas redes que

fornecem serviços com QoS, portanto a seguir serão abordados algumas técnicas e classes voltadas para atender as redes que oferece QoS:

- TCP Rate Shaping (TRS): Esta técnica regula o tráfego ao interceptar informações e mudar tamanhos de janelas TCP (Transmission Control Protocol). O TRS não aborda as necessidades de outros protocolos, como UDP (User Datagram Protocol).
- Classe: uma classe não precisa de gerenciamento para um tipo de tráfego. Uma classe de aplicações de missão crítica, por exemplo, inclui diversos tipos de tráfego, consistindo em sistemas que são considerados críticos pela empresa. Esta oferta de capacidade garante que aquilo que é mais importante receba a banda necessária para prover os consumidores com qualidade.
- Class-Based Queuing (CBQ): Projetado para impedir a deterioração da banda presente em PQ. O CBQ encaminha pacotes para filas dependendo de parâmetros configurados. A todas as filas é garantido um volume mínimo de largura de banda. Classe pode ser configurada para "pedir emprestada" largura de banda, se disponível, e as demandas de tráfego direcionariam o volume total do tráfego de classes ao limite configurado.
- Priority Queuing (PQ): Pacotes são encaminhados a filas dependendo de sua prioridade. Filas com prioridade mais alta transmitem pacote antes de filas com prioridade mais baixa. Afinal, o tráfego de baixa prioridade pode aniquilar a banda.
- Weighted Fair Queuing (WFQ): WFQ atribui pesos a prioridades mais altas, aumentando os tamanhos das filas. A utilização de largura de banda em tempo real não é levada em conta.
- Hierarchical Weighted Fair Queuing (HWFQ): Variação de WFQ, a técnica usa como medida de avaliação o retardo de pacotes, no pior dos

casos, sob cenários de tráfego variados. Avalia o retardo de pacote com base em tráfego dinâmico em tempo real.

CAPÍTULO IV – CONCLUSÕES SOBRE QoS

4.1 - O Futuro dos Serviços Integrados

Até o momento não sabemos se o modelo de serviços integrados será reconhecido no futuro da Internet. Mais e mais fabricantes de roteadores suportam RSVP em seus equipamentos. Mas para fornecer IS a uns grupos grandes de usuários, muitos roteadores Internet deverão suportar RSVP.

Um ponto importante que deve ser monitorado pelos fabricantes de roteadores é a sobrecarga de controle de tráfego, em roteadores capazes de RSVP que pode reduzir o desempenho do roteador. Se mais fluxos de dados passarem por um roteador, mais sessões RSVP terão que ser processadas pelo programa monitor de execução RSVP dentro do roteador. Os fabricantes de roteadores precisam ter certeza de que em situações de alto tráfego, um roteador não fique preso administrando apenas sessões RSVP em vez de rotear os pacotes de dados e manter atualizadas as tabelas de roteamento.

Extensões futuras do módulo de controle do plano de ação podem implementar um mecanismo de prioridade que permita aos usuários enviar requisições de reservas com prioridade mais alta que outras. Se os roteadores no caminho excederem suas capacidades de roteamento, as requisições de prioridade mais alta serão favorecidas. Isso pode ser implementado com um sistema de cobrança que exija do usuário as requisições de reserva de prioridade mais alta. Se for suportado IS na Internet, terá que ser assumido que o tráfego de melhor-tentativa ainda é oferecido. Não pode acontecer de alguns roteadores ficarem bloqueados com reservas RSVP e não puderem processar o tráfego de melhor tentativa. Essa pode ser mesmo uma descrição econômica de plano de ação a ser tomada pelos provedores de acesso. Um cenário concebível é que uma

metade da capacidade de roteamento seja usada para reservas de fluxos RSVP e a outra para o tráfego convencional de melhor tentativa.

Pode ser que algum dia, se isso acontecer, serviços RSVP de ponta a ponta estejam sendo usados na Internet. No momento, os IS são usados de preferência em intranets de empresas para fornecer multimídia e outros dados em tempo real ao usuário final. Por exemplo, se todos os roteadores em uma intranet suportarem RSVP, uma transmissão de vídeo poderá ser transmitida por motivos educacionais para todas as estações de trabalho de uma empresa.

4.2 - Qualidade dá Força aos Serviços em Banda Larga

A procura desenfreada pelo aumento de largura de banda no mercado corporativo, atendendo às aplicações que otimizam o trabalho e tornam as empresas mais competitivas, trouxe a reboque a necessidade de investir em equipamentos com funcionalidades de QoS (Qualidade de serviço), que permitem maior controle do tráfego na rede. QoS, em resumo, pode ser traduzida como a percepção do usuário quanto à eficiência de um serviço de comunicação, às características de tempo de resposta e à perfeição na transferência de conteúdo.

Assim, é possível controlar e atribuir a largura de banda a um tráfego específico, a fim de fornecer níveis previsíveis de taxa de transmissão de dados em redes IP (Internet Protocol). Esse controle pode ser determinado, entre outros fatores, por dia, mês, aplicação ou tipo de usuário, priorizando o fluxo de dados e mantendo a qualidade de serviço. Além disso, torna-se fundamental para que as empresas possam orientar os investimentos em tecnologia da informação (TI), sempre tendo em vista a relação custo/benefício.

Mas se isso já é realidade em algumas empresas, que instalaram por iniciativa própria meios de controle do canal de comunicação adquirido no mercado, ainda não é tão visível como oferta de fato por parte das operadoras de

telecomunicações, cujas redes já estão preparadas tecnologicamente para oferecer QoS baseada principalmente em ATM (Asynchronous Transfer Mode) e MPLS (MultiProtocol Label Switching).

Assim, o investimento em QoS é fundamental para o atendimento tanto das grandes quanto das pequenas e médias empresas. As de maior porte possuem departamentos de telecomunicações com capacidade de gerenciamento para acompanhar os níveis de serviço. No entanto, a pressão para diminuir custos tende aos poucos a transferir essa função à operadora. Já as de menor porte não possuem pessoais nem orçamento para essa finalidade e têm de conviver com o mínimo possível de problemas. Nesse sentido, a QoS permitirá a oferta de gerenciamento, banda por demanda e VPN, entre outros serviços disponíveis no mercado internacional, que está muito mais avançado nessa área.

CAPÍTULO V - REFERÊNCIAS BIBLIOGRÁFICAS

5.1 – Referências Bibliográficas

DANTAS, Maria. **Tecnologia de Redes de Comunicação e Computadores.** Rio de Janeiro: Axcel Books do Brasil, 2002.

SOARES, Luiz Fernando Gomes; LEMOS, Guido; Colcher Sérgio. **Redes de Computadores das LANs MANs e WANs às Redes ATM.** Rio de Janeiro: Campus, 1995.

TANANBAUM, Andrew S. **Redes de Computadores.** Rio de Janeiro: Campus, 1997.

MURHAMMER, Martin W.; etal; **TCP/IP Tutorial e Técnico.** São Paulo: Makron Books do Brasil.

[1]-**Uma Ferramenta para Utilização de QoS a partir de Aplicações TCP/IP em Redes ATM Emuladas. Disponível em :<** www.cenapadne.br **>.** Acesso em 05/03/2003

[2]-**Software Cisco IOS: Qualidade de Serviço" – "Cisco Provisioned QoS Policy Manager 2.0". Disponível em : <**www.cisco.com.br > Acesso em 05/03/2003

[3]**-Qualidade de Serviço (QoS) em Redes IP Princípios Básicos, Parâmetros e Mecanismos". Disponível em : <**www.itelcon.com.br >. Acesso em 05/03/2003

[4]- **Protocolos TCP/IP". Disponível em :<** www.cbpf.br>. Acesso em 05/03/2003

[5]- Edileuza Soares "Soluções Integradas de Negócios".**Revista Nacional de Telecomunicações RNT** Ano 23 – n. 267 P.23 novembro/2001 ISSN 0102-3446.

ANEXOS

ANÁLISE DE QoS EM EQUIPAMENTOS CISCO

Equipamento CISCO IOS

Uma rede de comunicações compõe o backbone de qualquer empresa bem sucedida. Essas redes servem de transporte para uma série de aplicações, incluindo voz sensível a atraso e vídeo com alta taxa de utilização de largura de banda. Essas aplicações comerciais ampliam as capacidades e os recursos de rede, mas também complementam, agregam valor e aperfeiçoam cada processo corporativo. As redes, portanto, devem fornecer serviços seguros, previsíveis, mensuráveis e às vezes garantidos a essas aplicações. Alcançar a qualidade de serviço (QoS) exigida de ponta a ponta (gerenciando o atraso, a variação de atraso ou jitter, a largura de banda e os parâmetros de perda de pacote em uma rede), ao mesmo tempo mantendo a simplicidade, escalabilidade e gerenciabilidade é o segredo para executar uma infra-estrutura que realmente atenda à empresa.

A solução

O software Cisco IOS fornece um conjunto de ferramentas repletas de recursos e soluções de QoS para tratar das diversas necessidades de aplicações de voz, vídeo e dados. A tecnologia de QoS do Cisco IOS permite que redes complexas controlem e atendam de maneira previsível várias aplicações em redes e tipos de tráfego. Empresas de pequeno e médio porte, empresas de grande porte e provedores de serviço, todos se beneficiam ao implantar a QoS da Cisco em suas redes. Largura de banda, atraso, jitter e perda de pacote podem ser controladas com eficiência. Garantindo os resultados desejados, os recursos de QoS conduzem a serviços eficientes e previsíveis para aplicações vitais para os negócios.

Utilizando os sofisticados recursos de QoS disponíveis no software Cisco IOS, as empresas podem criar redes que se ajustam ao modelo Serviços integrados (IntServ – Integrated Services) ou ao modelo Serviços diferenciados (DiffServ – Differentiated Services) da Internet Engineering Task Force (IETF). Os recursos de QoS dos Cisco IOS também fornecem funcionalidade de valor agregado, como reconhecimento de aplicação de rede (NBAR – Network-Based Application Recognition) para classificar tráfego com base em aplicação, um agente de garantia de serviço (SAA – Service Assurance Agent) para medições de QoS de ponta a ponta e sinalização do protocolo de reserva de recurso (RSVP – Resource Reservation Protocol) para controle de admissão e reserva de recursos.

Aplicações

As empresas de pequeno e médio porte normalmente não podem arcar com as despesas de atualização contínua das velocidades de enlace em suas redes. Os recursos de QoS do software Cisco IOS fornecem uma solução alternativa para adoção das largura de banda disponíveis e seu gerenciamento de modo eficiente, visando a atender às exigências da aplicação. Mecanismos como fragmentação e intercalamento de enlace (LFI – Link Fragmentation and Interleaving), Protocolo de tempo real compactado (CRTP – Compressed Real-Time Protocol), enfileiramento moderado ponderado (WFQ – Weighted Fair Queuing) e enfileiramento de baixa latência (LLQ – Low-Latency Queuing) permitem a distribuição mais eficiente da largura de banda disponível entre as aplicações.

As empresas podem implantar os recursos de QoS IntServ e DiffServ do Cisco IOS de modo rápido e fácil em uma rede inteira. Com soluções de QoS de ponta a ponta, aplicações vitais para a empresa e de multimídia podem ser priorizadas e ter garantida a largura de banda de rede e os limites de atraso

necessários. Conexões de WAN de alto custo também podem ser utilizadas do modo mais eficiente possível, ao mesmo tempo garantindo pouco atraso, jitter e lagura de banda assegurada para voz sobre IP (VoIP). RSVP, enfileiramento moderado ponderado baseado em classe (CBWFQ – Class-Based Weighted Fair Queuing), taxa de acesso consolidada (CAR – Commited Access Rate), modelagem genérica de tráfego (GTS – Generic Traffic Shaping) e detecção antecipada aleatória ponderada (WRED – Weighted Random Early Detection) são apenas algumas das principais ferramentas do Cisco QoS para empresas. Um provedor de serviços pode oferecer redes virtuais privadas (VPNs) ativadas por QoS e serviços não-VPN para conquistar vantagem competitiva. Os recursos intimamente integrados Cisco DiffServ e comutação de rótulo multiprotocolo (MPLS – Multiprotocol Label Switching) permitem maior diferenciação com serviços IP de ponta a ponta. Provedores de serviços que fornecem a clientes serviços ATM e Frame Relay tradicionais também podem beneficiar-se dos recursos QoS IP-para-Classe de serviço (CoS) ATM da Cisco, modelagem de tráfego Frame Relay (FRTS – Frame Relay Traffic Shaping), fragmentação Frame Relay (FRF.12) e outras soluções.

Por final, o mapeamento de reservas RSVP para QoS de circuito virtual permanente (PVC) e circuito virtual comutado (SVC) ATM também é uma ferramenta de diferenciação para provedores de serviços que fornecem serviços QoS de ponta a ponta.

Tecnologia Cisco IOS QoS

As ferramentas Cisco IOS QoS são divididas em seis categorias principais:

- Classificação e marcação – Os recursos de classificação de pacote permitem que o tráfego seja particionado em vários níveis de prioridade ou classes de serviço. Os pacotes podem ser classificados de várias maneiras diferentes, de interface de entrada a reconhecimento de aplicação com base em rede

(NBAR – Network Based Application Recognition) para aplicações difíceis de classificar e listas de controle de acesso arbitrárias. A classificação é o primeiro componente da Modular QoS CLI (MQC), a estrutura de QoS simples, escalável e avançada do IOS. A MQC permite a separação clara da classificação, da política aplicada nas classes, até a aplicação de uma política de QoS em uma interface ou subinterface. Pode-se também marcar pacotes de várias maneiras (Camada 2 – 802.1p/Q/ISL, ATM CLP bit, Frame-Relay DE-bit, MPLS EXP bits etc. e camada 3 – Precedência IP, ponto de código de serviços diferenciados (DSCP – Differentiated Services Code Point), etc.) usando o componente de política-estrutura da MQC.

- Prevenção de congestionamento – O algoritmo WRED permite evitar congestionamento nas interfaces de rede fornecendo gerenciamento de buffer e permite que o tráfego TCP seja reduzido antes que os buffers sejam esvaziados. Isso ajuda a evitar derivações residuais e problemas de sincronização global, maximizando desse modo à utilização de rede e o desempenho de aplicações com base em TCP. O componente de política-estrutura da MQC comporta WRED
- Gerenciamento de congestionamento – Com freqüência uma interface de rede fica congestionada (mesmo em altas velocidades, observa-se congestionamento passageiro) e são necessárias técnicas de enfileiramento para garantir que aplicações vitais obtenham o tratamento de encaminhamento. Por exemplo, aplicações em tempo real como VoIP e comércio de ações, entre outras, podem precisar ser encaminhadas com a menor latência e jitter. (até um limite previamente estabelecido). O enfileiramento de baixa latência (LLQ – Low-Latency Queuing) da Cisco oferece tal solução. Para outro tráfego não sensível a atraso (como FTP, HTTP etc.), outras técnicas de enfileiramento como CBWFQ e rodízio de déficit modificado (MDRR – modified Deficit Round-Robin) podem ser

usados. As técnicas de enfileiramento podem ser instanciadas usando a estrutura de política da MQC, também.

- Condicionamento de tráfego – O tráfego que entra em uma rede pode ser condicionado com o uso de um gerador de políticas ou modelador. Um gerador de políticas simplesmente aplica um limite de taxa, enquanto que um modelador harmoniza o fluxo de tráfego para uma taxa especificada com o uso de buffers. Novamente, mecanismos como taxa de acesso consolidada (CAR – Committed Access Rate), modelagem genérica de tráfego (GTS – Generic Traffic shaping) e modelagem de tráfego Frame-Relay (FRTS – Frame-Relay traffic Shaping) pode ser configurados fora/dentro da estrutura MQC.
- Sinalização – O Cisco IOS, além de oferecer suporte a QoS previamente estabelecida (incluindo o modelo de serviços diferenciados (DiffSer – Differentiated Services) IETF com integrados (IETF-Integrated Services). O protocolo de reserva de recurso é o mecanismo principal para realização de Controle de Admissão para fluxos em uma rede. Um exemplo perfeito é no caso de VoIP (voz sobre IP). Uma chamada é completada somente se houver recursos disponíveis para isso, garantindo que uma chamada que esteja entrando em uma rede não sobrecarregue nem afete a qualidade de chamadas existentes. Uma outra técnica, de chamada de propagação de política QoS via BGP (QPPB – QoS Policy Propagation via BGP), permite sinalizar indiretamente (usando o atributo lista de comunidades em BGP) a prioridade de encaminhamento para pacotes destinados a um sistema autônomo, via AS ou prefixo IP. Este é um recurso muito útil para provedores de serviços e empresas de grande porte
- Mecanismos de eficiência de enlace – Tráfego de voz e vídeo contínuo utiliza o protocolo de tempo real (RTP – Real-Time Protocol). Cabeçalhos dos pacotes IP, UDP e RTP podem ser compactados de aproximadamente 40

bytes para 5 a 8 bytes. Isso economiza uma imensa quantidade de largura de banda no caso de enlaces em baixa velocidade e no suporte a um grande número de fluxos de mídia. Além disso, o FRF. 12 (especificação Frame-Relay Fórum para fragmentação de quatro) e o Cisco LFI (fragmentação e intercalamento de quadros) permitem a fragmentação de grandes pacotes de dados, intercalando-os com pacotes RTP e mantendo baixo atraso e jitter para fluxos de mídia.

Suporte de plataforma

Os recursos de QoS do Software Cisco IOS são suportados em:

- Roteadores Cisco 8xx, 16xx, 17xx, 25xx, 36xx, 4xxx, 72xx, 75xx, 85xx e 12xxx

  Switches: Catalyst 4xxx, 5xxx e 6xxx.

Principais categorias e recursos de QoS do software Cisco IOS

Categoria	**Recursos de QoS associados**
Classificação	CAR, CBWFQ, MQC
Gerenciamento de Congestionamento	Técnicas de enfileiramento: WFQ, CBWFQ, LLQ, MDRR
Prevenção de congestionamento	WRED, WEPD (em ATM)
Política e modelagem de tráfego	GTS, FRTS, CAR
Sinalização	RSVP, QPPB
Mecanismos de eficiência de enlace	LFI, cRTP

Equipamento CISCO PROVISIONED QoS

A necessidade de alta disponibilidade previsível das aplicações vitais para as empresas, aliada à demanda por avançados serviços de voz e mídia, exige tratamento diferenciado do tráfego de rede. O cisco Provisioned QoS Policy Manager (QPM-PRO) 2.0 é um capacitador-chave de qualidade de serviço (QoS) de ponta a ponta para redes convergentes. O QPM-PRO 2.0 oferece serviços diferenciados através de estruturas de rede com aplicações de voz, vídeo e dados convergentes, simplesmente aproveitando os softwares Cisco IOS e Catalyst OS com mecanismos de QoS embutidos em equipamentos de comutação e roteamento de rede local e rede de longa distância.

Resumo dos Recursos

Controle centralizado e simplificado da política – Os administradores de rede podem utilizar a interface gráfica de usuário do QPM-PRO 2.0 para configuração de QoS de ponta a ponta precisa e automatiza, instalação confiável da política, ao mesmo tempo em que eliminam fluxos de comando de dispositivo a dispositivo.

Serviços diferenciados para diversos tipos de tráfego – Obtenha níveis de serviço voltados para empresas por meio de redes corporativas utilizando o QPM-PRO 2.0 para configurar a classificação de tráfego e permitir a execução da política QoS através de dispositivos Cisco.

Suporte QoS completo para voz sobre IP – Define e aplica políticas que garantem prioridade estrita para tráfego de voz em redes Cisco A AVVID (Architecture for Voice, Video and Integrated Data).

Classificação abrangente em nível de aplicação - Parte integral da rede de conteúdo da Cisco (Cisco Content Networking), o QPM-PRO 2.0 fornece níveis de serviço adequados para aplicações vitais para empresas dando suporte para o conjunto de classificação de pacotes IP para incluir assinaturas de aplicações, URLs da Web e portas negociadas.

Gerenciamento de nível de serviço (SLM – Service Level Management) e tráfego – Somente o QPM-PRO 2.fornece um conjunto completo de ferramentas para gerenciamento de congestionamento, anulação de congestionamento e controle da largura de banda. Utilize o QPM-PRO 2.0 com a solução de gerenciamento de serviços Cisco Works2000 para aprovisionar serviços em nível de rede e manter acordos de nível de serviço (SLAs –Service Level Agreements).

Controle de acesso – Segurança ampliada através da definição de políticas de controle de acesso que permitem ou negam o transporte de pacotes para dentro e fora das interfaces de dispositivos.

Desenvolvimento e controle automatizado da política QoS – Como parte de uma arquitetura de QoS de empresas, o QPM-PRO 2.0 permite a verificação da avaliação da política de QoS, upload da configuração do dispositivo existente, visualização prévia de modificações na configuração, atualização de listas de controle de acesso (ACL – Acess Control List) por incrementos e gerenciamento da distribuição da política.

Suporte amplo de dispositivo e Cisco IOS – Somente o QPM-PRO 2.0 pode ser utilizado com mais de 20 diferentes roteadores e switches Cisco e também com uma ampla gama de versões do software IOS e Catalyst OS.

Administração inteligente da política – Ativa seletivamente mecanismos de QoS em interfaces LAN e WAN agrupados de maneira inteligente, define faixas de listas de controle de acesso (ACL) e restaura / aplica uma versão anterior da base de dados de política.

Integração com o CiscoWorks2000 – A importação de inventário de dispositivos do Resource Manager Essentials 2.0 abrevia o tempo de configuração dos dispositivos voltados para a execução da política.

Relatórios baseados na Web – Os relatórios baseados na Web são utilizados para visualizar e analisar rapidamente o gerenciamento da política de QoS.

Benefícios do QPM-PRO

O QPM-PRO 2.0 é um sistema de política de QoS escalável que facilita a definição de políticas de tráfego e automatiza diversos níveis de serviço através de qualquer topologia de rede. O produto permite serviços diferenciados em nível de rede e baseados no conteúdo, controle centralizado da política para redes de voz/vídeo/dados, configuração e instalação automatizada de Qos e controle da política de campus para WAN.

Fornecimento de serviços diferenciados para toda a rede

O aprovisionamento de recursos de rede baseado na importância relativa do tráfego de aplicação é a maneira mais eficiente para fornecer QoS diferenciada. A classificação de pacote é um recurso chave que permite que os pacotes adequados sejam selecionados para um nível de serviço específico. Ao automatizar o processo de conversão de requisitos de desempenho de aplicações para a política de QoS, o QPM-PRO 2.0 ajuda a garantir desempenho confiável para a aplicações de negócios na Internet e tráfego de voz que contenham

tráfego não crítico. Utilizando o QPM-PRO 2.0, um administrador de rede pode montar rapidamente políticas de QoS baseadas em regras que identificam e repartem o tráfego de aplicação em vários níveis de serviço, garantido que as aplicações mais importantes recebam serviço de prioridade. Por exemplo, uma empresa pode estabelecer níveis diferenciados "Ouro, Prata e Bronze" de serviços IP. Um serviço Ouro garantiria latência para o transporte de aplicações corporativas vitais como telefonia por pacotes ou de arquitetura de rede de sistemas (SNA – Systems Network Architecture). Um serviço Prata garantiria a disponibilização de aplicações mais gerais, não sensíveis à latência, como de comércio eletrônico. Um serviço Bronze poderia ser utilizado para dar suporte a certas sessões Web e de correio eletrônico enquanto os demais tráfegos seriam tratados com base no melhor esforço.

Controle e execução da política de QoS de Borda e de Backbone

O QPM-PRO 2.0 permite a criação de uma arquitetura de política de QoS para toda a rede priorizando aplicações pelo nível de serviço no perímetro da rede e então providencie a execução da política no backbone (ou núcleo) utilizando técnicas de gerenciamento de congestionamento, anulação de congestionamento de modelagem de tráfego. Esta arquitetura melhora a operação da rede executando a classificação de tráfego, marcando ou colorindo pacotes e programando na borda do campus ao mesmo tempo em que elimina a necessidade de classificar o tráfego de cada interface WAN no backbone. Além disso, os serviços Cisco IOS QoS fornecem meios para distribuir funcionalidade e responsabilidade entre funções de borda e funções de backbone. Essa distribuição de funcionalidade permite desempenho simultâneo e escalabilidade de serviços.

Na borda da rede, o QPM-PRO 2.0 é utilizado para:

- Especificar políticas que estabelecem classes de tráfego e níveis de serviço relacionados.
- Especificar políticas que definam como os recursos de rede são alocados e controlados por classe de tráfego e nível de serviço.
- Permitir o mapeamento eficiente de aplicações em níveis de serviço.
- Aplicar políticas para atender aos requisitos corporativos.

Após os pacotes terem sido marcados ou coloridos conforme o nível de serviço definido, a política de QoS é então executada no núcleo da rede ou no backbone WAN. Para o backbone da rede, o QPM-PRO 2.0 permite a execução através de um conjunto extenso de mecanismos de QoS utilizados para gerenciamento de congestionamento, como enfileiramento moderado ponderado baseado em classe (CBWFQ – Class-Based Weighted Queuing), controle de congestionamento, incluindo detecção antecipada pondera (WRED – Weighted Randon Early Detection) e modelagem de tráfego.

Para fornecer efetivamente QoS de ponta, a sinalização de rede precisa que os dispositivos de rede compartilhem a responsabilidade de fornecer prioridade de tráfego. Atualmente, software Cisco IOS e dispositivos suportam um valioso conjunto de recursos de QoS com switches e roteadores de campus e backbone, cada um deles executando funções de QoS separadas, porém em cooperação. Utilizando o QPM-PRO 2.0, os administradores podem definir os domínios da política de QoS dentro de uma rede utilizada para controlar a classificação de QoS, enfileiramento e funções da política distintas. Aproveitando as capacidades de QoS recentemente integradas aos swiches Catalyst 4000, 5000 e 6000, o QPM-PRO 2.0 agora amplia a execução da política por toda a empresa.

Controla e mantém níveis de serviços

A Cisco possui um amplo conjunto de ferramentas de gerenciamento de níveis de serviço que permite que os administradores aprovisionem, controlem e monitorem a QoS em uma base de ponta a ponta. O QPM-PRO 2.0, combinado com a solução de gerenciamento de serviços (SMS – Service Management Solution) Cisco Works2000, agrega previsibilidade à experiência da rede, permitindo que os administradores forneçam largura de banda dedicada, controle de latência e jitter e melhorem o fluxo do tráfego de rede.

O QPM-PRO 2.0 e o SMS podem ser utilizados em conjunto para um SLM de ponta a ponta com sinergia, aproveitando o padrão de serviços diferenciados (DiffServ-Differentiated Services) suportado nos roteadores e switches Cisco. Isso é obtido utilizando;

- O QPM-PRO 2.0 para classificar o tráfego na borda da rede em diversos níveis de serviço.
- O QPM-PRO 2.0 para aprovisionar níveis de serviço de ponta a ponta em roteadores e switches de rede.
- O SMS para monitorar e controlar aqueles níveis de serviço definidos pelo QPM-PRO 2.0.

A QoS para voz por pacotes

Uma das mais promissoras utilizações para redes IP é permitir o compartilhamento de tráfego de voz com tráfego tradicional de dados e LAN para LAN. Tipicamente, isso a ajuda a reduzir os custos de transmissão reduzindo o número de conexões de rede e também pelo compartilhamento de conexões e infra-estrutura existentes.

Ao instalar redes Cisco AVVID, atualmente as empresas podem optar por reduzir alguns de seus custos de voz, combinando o tráfego de voz em suas

redes IP existentes. Entretanto, para fornecer a qualidade de voz necessária, a QoS deve fazer parte da rede.

O QPM-PRO 2.0 junto com os mecanismos de QoS do Cisco IOS e Catalyst OS nas redes Cisco AVVID, fornece ao tráfego de VoIP o serviço que ele precisa, ao mesmo tempo em que fornece os níveis de serviço exigidos para o tráfego de dados.

O QPM-PRO 2.0 suporta os mecanismos de QoS no software Cisco IOS e Catalyst OS e dispositivos de campus e WAN recomendados para garantir serviço de prioridade para o tráfego de voz. Com o QPM-PRO 2.0, é possível fornecer QoS para toda a rede, para agilizar a transmissão de pacotes de voz ao mesmo tempo em que reduz o jitter utilizando os seguintes mecanismos:

- CBWFQ com

  1-Enfileiramento de baixa latência (LLQ – Low Latency Queuing) para fornecer prioridades estritas.

  2-Prioridade de protocolo de transporte em tempo real (RTP – Real-Time Transport Protocol) IP.

  3-Modelagem de tráfego genérico (GTS – Generic Traffic Shaping).

  4-Modelagem de tráfego distribuído (DTS – Distributed Traffic Shaping).

  5-Fragmentação Frame Relay (FRF – Frame Relay Fragmentation).

  6-Limitação de taxa.

- Cabeçalho de RTP compactado (cRTP – Compressed RTP)
- Fragmentação e intercalamento de enlace (LFI – Link Fragmentation and Interleaving) para conexões ponta-a-ponta
- FRTS aprimorado com Fragmentação Frame Relay (FRF12 – Frame Relay Fragmentation) e enfileiramento moderado Frame Relay e largura de banda de voz Frame Relay

- Configuração RSVP para dispositivo de campus e WAN e capacidade de programação de tráfego avançada do Catalyst 6000, incluindo o IP2Q2T.

Automatiza a configuração e instalação da QoS

Mesmo com dispositivos de rede inteligentes, a tarefa de instalar manualmente políticas de QoS em toda a rede pode estar sujeita a erros e consome tempo. O QPM-PRO 2.0 automatiza muito das etapas associadas com a definição, validação, configuração e instalação de políticas. Utilizando a interface gráfica de usuário (GUI) do QPM-PRO 2.0 pode-se instalar políticas de QoS de maneira confiável sem exigir um entendimento detalhado dos mecanismos de QoS ou da linguagem ou sintaxe de linha de comando do dispositivo (interface de linha de comando ou CLI). O QPM-PRO 2.0 elimina as demoradas tarefas de configuração de dispositivos, melhorando dessa forma a consistência da política e reduzindo o tempo para implementar a QoS na rede de empresa. Utilizando o QPM-PRO 2.0, agora é possível:

- Criar poderosas políticas baseadas em regras que combinam aplicações de porta estáticas e dinâmicas e filtros de tráfego em sistemas host.
- Ativa um valioso conjunto de serviços de QoS, incluindo gerenciamento de congestionamento, anulação de congestionamento e mecanismo de modelagem de tráfego.
- Converte as políticas de maneira eficiente para os comandos específicos de configuração de QOS, garantindo a consistência da política em todos os domínios da política.
- Faz upload das configurações de dispositivos de QoS existentes e valida as políticas antes de instalá-las na rede.
- Retorna a uma implementação de QoS anterior, reinstalando uma versão histórica da base de dados da política.

- Gera relatórios baseados na Web sobre as políticas de QoS instaladas na rede.

Durante a definição da política, o QPM-PRO 2.0 consulta os dispositivos para determinar a classe do dispositivo, tipo de interface, versão de software e recursos de QoS suportados necessários para montar uma base de dados de regras para a validação da política. Utilizando esta base de dados de regras, o QPM-PRO 2.0 guia o usuário através das definições válidas da política.

Com o QPM-PRO 2.0, as políticas de QoS são distribuídas para dispositivos de rede depois de convertidas em uma classificação, enfileiramento, limitação e modelagem dos comandos de configuração específicos, reduzindo a complexidade de configuração de uma mistura de recursos de QoS entre diferentes dispositivos de QoS entre diferentes dispositivos de QoS e versões do Cisco IOS e Catalyst OS. Finalmente, o QPM-PRO 2.0 garante o sucesso de cada distribuição da política, monitorando o status de uma distribuição de diversos dispositivos, registrando todas as alterações de configuração de interface e mantendo uma trilha de auditoria da política.

Ferramentas e serviços do QoS Policy Manager

O Cisco QoS Policy Manager compõe-se das seguintes ferramentas e serviços:

Graphical Policy Administration Console

A interface gráfica de usuário (GUI) do QPM-PRO 2.0 resume a complexidade da definição da política e valida complexas regras da política de QoS. O sistema da política mantém uma base de conhecimento que armazena informações de atributos sobre as capacidades de QoS de cada dispositivo. Essa base de conhecimento garante que se defina políticas de QoS somente para mecanismos de QoS suportados pelos dispositivos de destino e então converte essas políticas de QoS em comandos de configuração específicos para cada

interface. Este resumo e automação da política reduzem as tarefas repetitivas associadas com a definição das políticas para diversos dispositivos e versões de software, garantindo a integridade da política de QoS.

Filtros da política baseados em regras

O QOM-PRO 2.0 permite que se crie políticas de QoS flexíveis e baseadas em regras que filtram o tráfego com base nos endereços ou portas IP de origem ou de destino, protocolo, tipo de serviço (ToS – Type of Service) IP, nome dos host tipo sistema de nome domínio (DNS – Domain Name System) e também filtros de macro definidos pelo usuário. As expressões de filtro melhoram a precisão e consistência de comandos de configuração instalados na rede.

Classificação de pacotes em nível de aplicação

Parte integral da rede de conteúdo Cisco, O QPM-PRO 2.0 permite a configuração de recursos de reconhecimento de aplicações baseadas em rede (NBAR – Network-Based Application Recognition) disponíveis no software Cisco IOS que ampliam a classificação de pacotes para assinatura de aplicação baseada em contexto, URLs da Web e reconhecimento de protocolos dinâmicos.

Além disso, o QPM-PRO 2.0 agora aproveita o NBAR para colorir ou marcar pacotes e limitação de taxa. Podem ser aplicadas poderosas políticas baseadas em regras, combinando filtros de aplicação do sistema host, incluindo mapeamento de números de protocolo NBAR para obter diferenciação granular de serviços. O mecanismo de inspeção de pacote NBAR fornece classificação de aplicações que se baseiam em atribuição dinâmica de porta de protocolo de controle de transmissão (TCP)/ protocolo de pacote de usuário (UDP) e classificação de tráfego de protocolo de transferência de hipertexto (HTTP) por URL e tipo MIME (Multipurpose Internet Mail Extensions).

Também podem ser reconhecidas assinaturas adicionais de aplicação baseadas em conteúdo de pacote.

Perfis de serviços de aplicação

Pode-se definir perfis de serviços de aplicações baseados em portas de aplicação, protocolos e endereços de portas TCP/UDP. O QPM-PRO 2.0 possui aplicações TCP e UDP bem conhecidas, definidas previamente no sistema e permite que o usuário crie uma biblioteca de perfis personalizados de aplicações.

Grupos de host

Podem-se criar grupos de host com base em endereços IP, faixas de endereços IP, nome DNS ou combinação de máscaras e endereços IP. Quando da definição de políticas de QoS, o usuário pode utilizar esses grupos de host ao invés de especificar o usuário final, servidor ou endereço de rede individual. À medida que novos hosts são incluídos ou removidos, é preciso somente atualizar e reaplicar o grupo de host para a rede ao invés de reconfigurar as ACLs de diversos dispositivos.

Agrupamento de domínio da política

O recurso de agrupamento inteligente do QPM-PRO 2.0 permite que sejam definidos grupos de interface entre diversos dispositivos utilizados para aplicar uma política de QoS a um domínio de política específico. Esse recurso agiliza a distribuição das alterações de configuração da política para diversos dispositivos e garante que as listas de acesso são precisas e consistentes em toda a distribuição da política de várias interfaces.

Controle de acesso

O QPM-PRO 2.0 amplia a segurança quanto à possibilidade de permitir ou negar transporte de pacotes para dentro e para fora das interfaces. As políticas de controle de acesso podem ser ativadas ou desativadas globalmente ou especificadas com base em dispositivos. Além disso, o QPM-PRO 2.0 tem um mecanismo de filtro da política de QoS que fornece a opção de excluir tráfego específico de níveis de serviços definidos.

Serviços diferenciados consistentes

Podem ser definidas até 64 classes de serviços diferenciados, nas quais todo o tráfego pode ser classificado com base em filtros de sessão de rede para camada de aplicação. Essas classes podem ser identificadas para toda a rede com o valor de precedência de IP ou DSCP sem alterar as aplicações, dispositivos ou complicados requisitos de sinalização de rede existentes.

Execução da QoS

O QPM-PRO 2.0 suporta a execução de serviços diferenciados utilizando ACLs estendidas para definir políticas de rede para tratamento de congestionamento e alocação de largura de banda. O QPM-PRO 2.0 suporta gerenciamento de congestionamento utilizando CBWFQ, rodízio ponderado (WRR – Weighted Round Robin), enfileiramento de prioridade, enfileiramento personalizado e enfileiramento moderado ponderado (WFQ – Weighted Fair Queuing); anulação de congestionamento utilizando o WRED; limitações de largura de banda de entrada e saída utilizando a taxa de acesso consolidada (CAR – Commited Access Rate) e modelagem de acesso utilizando GTS e FRTS.

QoS de campus

O QPM-PRO 2.0 amplia o controle da política de ambientes de campus e WAN suportando os mais recentes switches Catalyst, incluindo o Catalyst 2948G-L3, 4908G-L3, 4003 e 4006 com placa de linha de camada 3 e o Catalyst 5000 e 6000 (com MSFC e o módulo FlexWAN). Agora há uma ampla gama de recursos de QoS de campus integrados. Eles incluem:

- Classificação de pacotes IP, que permite serviços de tráfego diferenciados em toda a rede com base em uma porta de entrada.
- Classificação por VLAN
- Política de largura de banda, que permite a limitação de taxa de tráfego com base na porta.
- Gerenciamento de perda de limiares, que dá preferência a tráfego de maior prioridade.
- Programação de tráfego, que aloca tráfego para filas de transmissão de saída conforme o valor de precedência IP ou DSCP.

No Catalyst 5000, o QPM-PRO 2.0 permite que se aplique rapidamente uma política de classificação com base nos endereços de origem e destino IP (Camada 3), com o UDP ou TCP e uma porta de origem e destino de camada 4. A classificação de QoS é configurada no campo ToS do cabeçalho IP no pacote, que pe então transportada para além do domínio do switch. O Catalyst 6000 oferece um valioso conjunto de capacidade de QoS, incluindo classificação de pacotes, políticas de largura de banda por porta e microfluxo e programação de tráfego, dando aos administradores a capacidade de direcionar o tráfego de alta prioridade para uma fila dedicada. Na família de switches Catalyst, o tráfego pode ser programado utilizando o WRR.

QoS de voz

O QPM-PRO 2.0 suporta diversos recursos recomendados para garantir serviço de prioridade utilizando o mais recente software Cisco IOS e dispositivos de campus e WAN. Os recursos de QoS suportados para voz incluem o CBWFQ com LLQ, prioridade RTP IP, FRTS, GTS e limitação de taxa. Os recursos de QoS adicionais suportados incluem o FRTS ampliado com FRF12 e enfileiramento moderado Frame Relay e largura de banda de voz Frame Relay, cRTP, LFI, configuração RSVP para dispositivo de campus e WAN e capacidade de tráfego Catalyst 6000, incluindo IP2Q2T.

Instalação da política

O QPM-PRO 2.0 tem diversos recursos avançados para garantir que a montagem de políticas QoS seja precisa. Com o QPM-PRO 2.0, é possível:

- Definir números ACL
- Revalidar resoluções DNS
- Fazer upload de configurações de QoS de dispositivos existentes
- Detectar alterações da política baseada em dispositivo
- Detectar versões do software Cisco IOS e do Catalyst SO (Sistema Operacional)

O componente do gerenciador de distribuição do QPM-PRO 2.0 controla e audita a distribuição de políticas de QoS para dispositivos de rede. Os recursos de controle de distribuição do sistema permitem que um administrador de rede:

- Visualize previamente todas as alterações de configuração incluindo CLI específicas de versão de software ou de dispositivos ou sintaxe CLI modular
- Instale políticas para grupos de interface executados sob a mesma imagem de software ou imagens de software diferentes
- Interrompa a distribuição da política no evento de uma falha
- Controle o progresso e as informações de histórico da tarefa

- Envie um arquivo de configuração e faça download do protocolo de transferência de arquivo trivial (TFTP – Trivial File Transfer Protocol) para os dispositivos
- Restaure uma versão anterior da base de dados de política e redistribua a mesma para a rede

Distribuição da política voltada para evento

A automatização e instalação da política criando um programa externo que ative a execução da tarefa de distribuição da política. Por meio do programa distribute_policy.exe, pode-se utilizar um programa de agendamento para automatizar a instalação de uma política baseada em eventos externos ou requisitos de agendamento.

Sistema de relatórios baseados na Web

O QPM-PRO 2.0 inclui relatórios baseados na Web que fornecem um resumo de todas as políticas de QoS instaladas na rede, com a capacidade de pesquisar detalhes da política de interface, bem como relatórios de visualização após uma ação administrativa, como o upload da configuração de um dispositivo.