VOZ SOBRE IP

TECNOLOGIAS E APLICAÇÕES

JOSÉ MARCOS CÂMARA BRITO

RA: 961064

CAPÍTULO 01 – INTRODUÇÃO

O crescimento vertiginoso que a Internet experimentou nos últimos anos colocou o protocolo IP em uma posição de destaque no contexto das redes de telecomunicações.

Os cenários de aplicação da transmissão de voz sobre IP (doravante abreviado para VoIP) são muitos e ainda há muita controvérsia a respeito, mas não há dúvida de que a tecnologia de VoIP tem potencial para permitir o oferecimento de um novo leque de serviços aos usuários de telefonia e Internet, além de poder resultar em uma diminuição do custo associado aos serviços de telefonia, particularmente de longa distância. A Figura 1 ilustra um dos cenários para implementação de telefonia e fax sobre uma rede IP [1].

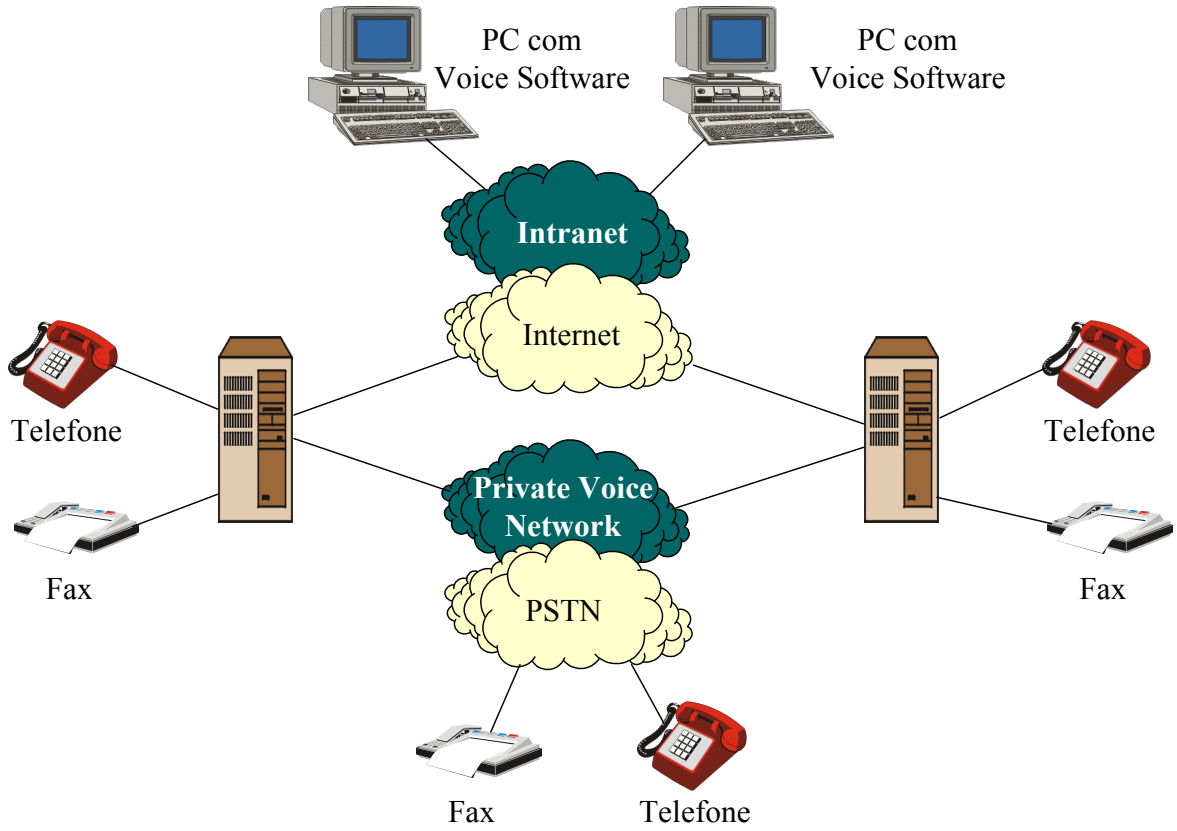


Figura 1 – Um cenário de implementação de telefonia e fax sobre rede IP.

1. ARQUITETURAS BÁSICAS

Em uma primeira abordagem podemos definir três arquiteturas básicas de implementação [3]:

ARQUITETURA PC-a-PC: Nesta arquitetura dois computadores providos de recursos multimídia, conectados a uma LAN (tipicamente no ambiente corporativo) ou, através da RPT (Rede Pública de Telefonia), a um provedor de serviços Internet (tipicamente no ambiente residencial), se comunicam para a troca de sinais de voz. Todo o tratamento do sinal de voz (amostragem, compressão e empacotamento) é realizado nos computadores, sendo a chamada de voz estabelecida com base no endereço IP do receptor (ou através de um "nome", que será convertido para um endereço IP utilizando-se um serviço de diretório público). Esta arquitetura está ilustrada na Figura 2. A arquitetura PC-a-PC possui uma variante onde o PC é substituído por um telefone com capacidade de codificação de voz e implementação do protocolo IP.

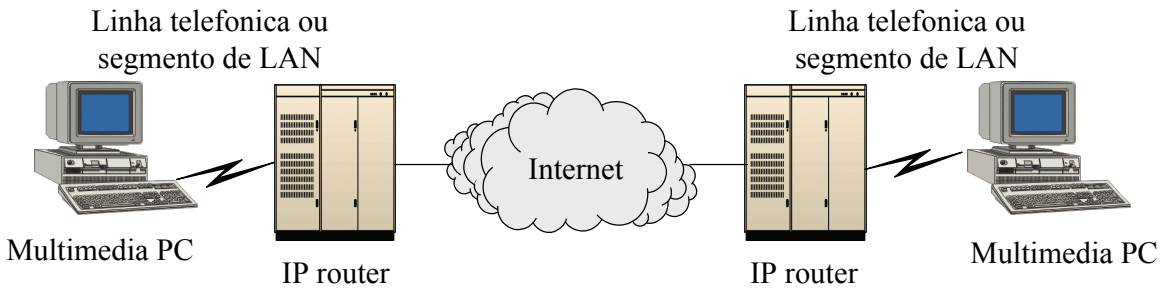


Figura 2 – Arquitetura PC-a-PC.

ARQUITETURA COM GATEWAY: Nesta arquitetura, ilustrada na Figura 3, um telefone padrão é utilizado para gerar e receber a chamada telefônica sobre a Internet. O usuário chamador disca para o Gateway de telefonia IP mais próximo de sua central telefônica local; este Gateway reconhece e valida o número telefônico do usuário chamador (para fins de autenticação e bilhetagem) e solicita a este que forneça o número do usuário de destino.

O Gateway de entrada identifica o Gateway de saída mais próximo do usuário de destino e inicia com este uma sessão para transmissão de pacotes de voz (possivelmente utilizando o protocolo H323, que será discutido posteriormente). O Gateway de saída chama o telefone receptor e, após a chamada ser atendida, a comunicação fim-a-fim tem início, com o sinal de voz sendo enviado através de datagramas IP entre os Gateways. A codificação e empacotamento do sinal de voz são feitos no Gateway de origem, enquanto a decodificação e desempacotamento são feitos no Gateway de destino. A digitalização do sinal de voz pode ser feita na central, no Gateway, ou mesmo no telefone (caso do RDSI, por exemplo).

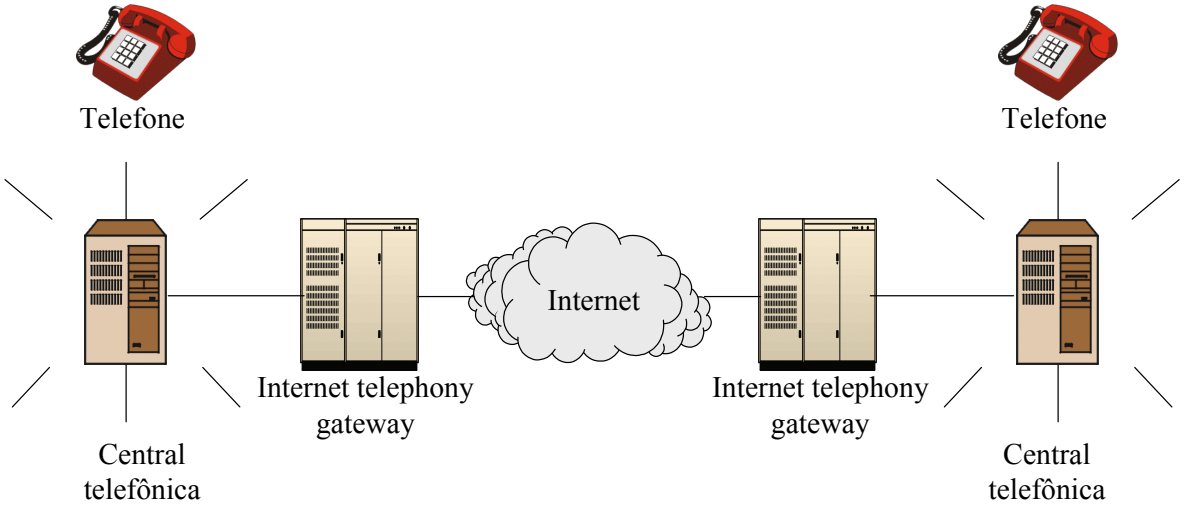


Figura 3 – Arquitetura com Gateway

ARQUITETURAS HÍBRIDAS: Naturalmente, esquemas híbridos das duas arquiteturas anteriores são possíveis e desejáveis. Nestas estruturas um usuário de um telefone padrão origina (ou recebe) uma chamada para um usuário de PC (ou telefone IP). Em tais situações, deve haver um serviço de mapeamento ou translação de endereços IP em números telefônicos. Existem quatro caminhos unidirecionais neste caso: PC-a-PC, Gateway-a-Gateway, PC-a-Gateway, Gateway-a-PC. Em todas estas arquiteturas os pontos terminais (PC ou Gateways) devem empregar o mesmo esquema de codificação de voz.

Embora as arquiteturas mostradas até então ilustrem o transporte de voz sobre a Internet, existe um consenso de que ao menos no curto/médio prazo a aplicação de VoIP para

serviços de telefonia (que denominaremos de Telefonia IP) se dará apenas em redes privadas ou Intranets, ou ainda na rede de acesso do assinante à central de comutação local [2]. A dificuldade de se imaginar, no momento, serviços de telefonia sobre a Internet reside no fato desta rede ser hoje do tipo "melhor esforço", impedindo que se possa oferecer Qualidade de Serviço (QoS) adequada ao tráfego de telefonia.

2. CENÁRIOS DE APLICAÇÕES [4]

ENTRONCAMENTO DE PABX PONTO A PONTO: Empresas que dispõem de PABXs interligados por linhas dedicadas, e que possuem uma rede WAN IP interligando os mesmos escritórios onde se encontram estes PABXs, podem eliminar a linha dedicada (tie-line) e transportar o tráfego de voz sobre a rede IP. Para tal, é necessário a introdução de Gateways de VoIP em ambas extremidades. Como os pacotes de voz serão transferidos entre endereços IP pré-definidos, não há necessidade de mecanismos complexos de conversão de número telefônico/endereço IP. A Figura 4 ilustra este cenário de aplicação.

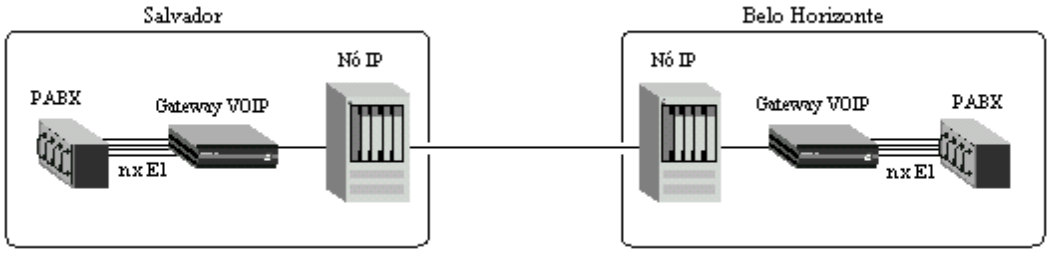


Figura 4 – Entroncamento de PABXs utilizando VoIP.

ENTRONCAMENTO DE CENTRAIS DA REDE PÚBLICA: Esta aplicação é bastante semelhante à anterior. Aqui, as operadoras de serviços de telecomunicações podem substituir os troncos, analógicos ou digitais, utilizados para interligar centrais telefônicas por enlaces IP.

TRÁFEGO DE VOZ SOBRE UMA REDE IP CORPORATIVA: Nesta configuração uma grande empresa com diversos escritórios geograficamente distribuídos pode se desfazer de

seus canais de voz e linhas dedicadas, e rotear todo o tráfego de voz através da rede IP corporativa existente (ver Figura 5).

Deve-se observar que na implementação de VoIP para empresas, além da nova comunicação suportada pela rede IP, é mantida uma boa parte dos entroncamentos com a RTPC (Rede de Telefonia Pública Comutada), que vai servir para:

- Cursar as chamadas não corporativas, ou seja, destinadas à RTPC.
- Suportar o tráfego de voz corporativa em caso de falha na rede IP.
- Suportar o excesso de tráfego corporativo em caso de congestionamento na rede IP.

Geralmente as implementações permitem que o usuário, através da discagem de códigos, possa optar por usar a rede IP corporativa ou a RTPC para encaminhar suas chamadas. Neste caso o usuário deve ser orientado para utilizar adequadamente a rede, evitando as chamadas pela RTPC, que são tarifadas, e com isso reduzindo as despesas da empresa. Em implementações mais complexas, através de um plano de numeração bem elaborado, é possível deixar esta opção sempre a cargo da própria rede, consequentemente com um melhor controle sobre os custos de telefonia.

Nesta aplicação é necessário o processo de tradução de números telefônicos em endereços IP, uma vez que existe mais de um possível destino para uma chamada. Na arquitetura ilustrada na Figura 5 esta função é executada pelo Gatekeeper.

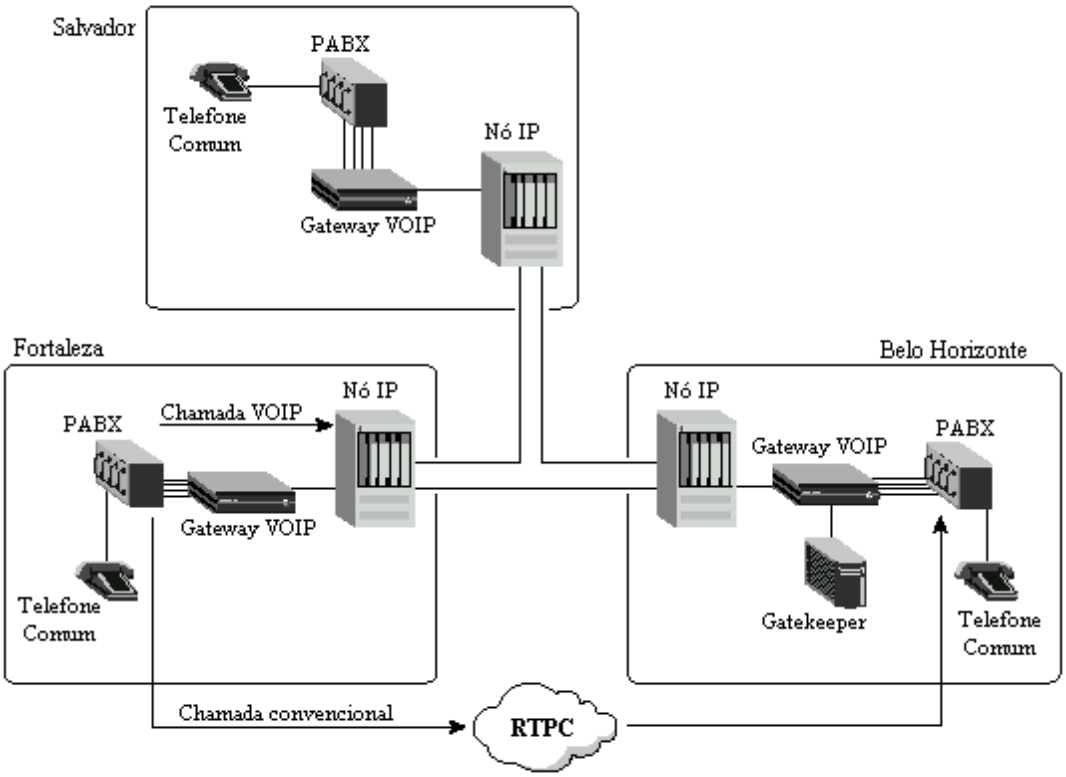


Figura 5 – Tráfego de voz corporativo.

SERVIÇO PÚBLICO DE VOZ DE LONGA DISTÂNCIA: Esta aplicação é adequada, abstraindo-se das questões legais e normativas, aos Provedores de Serviços Internet (ISP) que já dispõem de uma extensa rede de pacotes de âmbito nacional ou internacional, e como alternativa tecnológica para a implementação (ou substituição) dos backbones das empresas provedoras de serviços de telecomunicações.

A Figura 6 ilustra uma rede IP para serviços públicos que é utilizada para rotear simultaneamente tráfego de voz e dados. O backbone da rede deve ser privado e gerenciável, de modo a permitir que se alcance a QoS desejada, e pode eventualmente se basear em outra tecnologia de comutação de pacotes (como Frame Relay ou ATM). A figura ilustra a interconexão de três cidades, mas a rigor podemos admitir que uma "nuvem" IP (ou IP sobre alguma coisa) possa ser utilizada para interconectar quaisquer dois

pontos dentro da área de cobertura do provedor de serviço de telecomunicações (ou Internet).

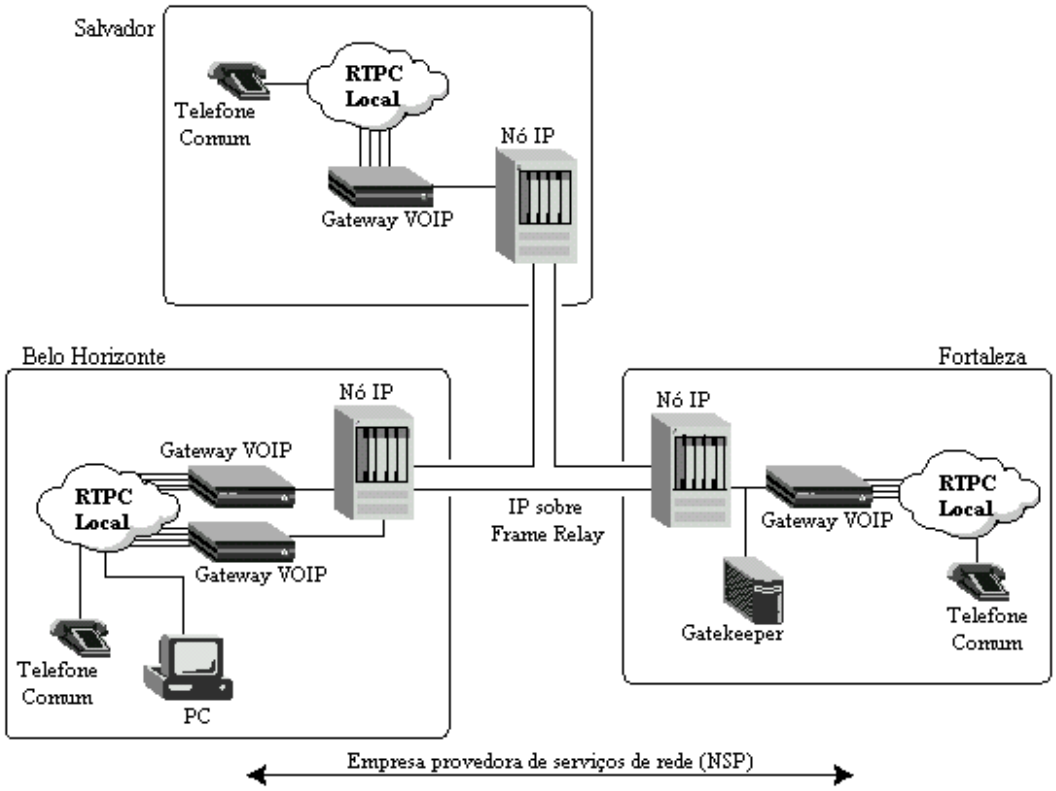


Figura 6 – Serviço público de telefonia sobre IP.

CAPÍTULO 02 – PROTOCOLOS PADRÕES

1. PASSOS PARA O ESTABELECIMENTO DE UMA CONEXÃO DE VoIP

Antes de iniciarmos a descrição dos padrões associados à transmissão de voz sobre IP, vamos, a título de ilustração, mostrar um exemplo de um estabelecimento de uma chamada de VoIP através de um provedor de serviço de telefonia sobre a Internet . O exemplo se baseia na arquitetura do padrão H.323, que será descrito no próximo item, e admite a existência da rede pública de telefonia tradicional. A Figura 7 ilustra todos os passos descritos [7]:

1) O usuário chamador disca um número de acesso ao serviço de telefonia sobre a Internet.

2) A chamada é roteada pela rede pública para o comutador de telefonia IP.

3) O Gateway solicita ao usuário chamador que informe o número do telefone de destino. Este número é enviado ao Gatekeeper.

4) O Gatekeeper determina o endereço IP do Gatekeeper de destino baseado no número do telefone de destino. Um pacote IP requisitando a informação de status (disponibilidade) do Gateway de destino é enviado ao Gatekeeper de destino.

5) O Gatekeeper de destino responde à requisição provendo as informações de disponibilidade e endereço IP do Gateway de destino. O Gatekeeper de origem transfere estas informações para o Gateway de origem.

6) O Gateway de origem estabelece um canal de comunicação com o Gateway de destino. Este canal é identificado por uma Variável de Referência de Chamada (Call Reference

Variable – CRV), que será usada por ambos os Gateways durante toda a chamada para identificar os pacotes IP associados com esta chamada em particular.

7) O Gateway de destino seleciona um tronco de saída para a rede pública e envia uma sinalização ao comutador da rede pública solicitando que o mesmo estabeleça uma chamada com o número telefônico indicado.

8) Se a chamada pode ser completada com sucesso, uma mensagem de sinalização IP é enviada pelo Gateway de destino para o Gatekeeper de destino e deste para o Gatekeeper de origem. O Gatekeeper sinaliza ao Gateway de origem, e este encaminha sinalização para a rede telefônica de origem indicando que o terminal de destino está sendo chamado (tom de campainha). Após iniciada a conversação, pacotes de voz são trocados na rede IP entre os Gateways, durante a chamada.

Qualquer sinal de "progresso de chamada" ou outros sinais na faixa de voz (por exemplo, tom de controle de chamada, tom de ocupado e outros) trafegam normalmente, assim que se estabelece um canal de áudio fim a fim. A sinalização que pode ser detectada pelas interfaces de voz (por exemplo dígitos DTMF na faixa de voz discados depois que a chamada já foi completada – Sobrediscagem) é também capturada pelo Gateway e transportada através da rede IP encapsulada no protocolo RTCP, na forma de sinalização.

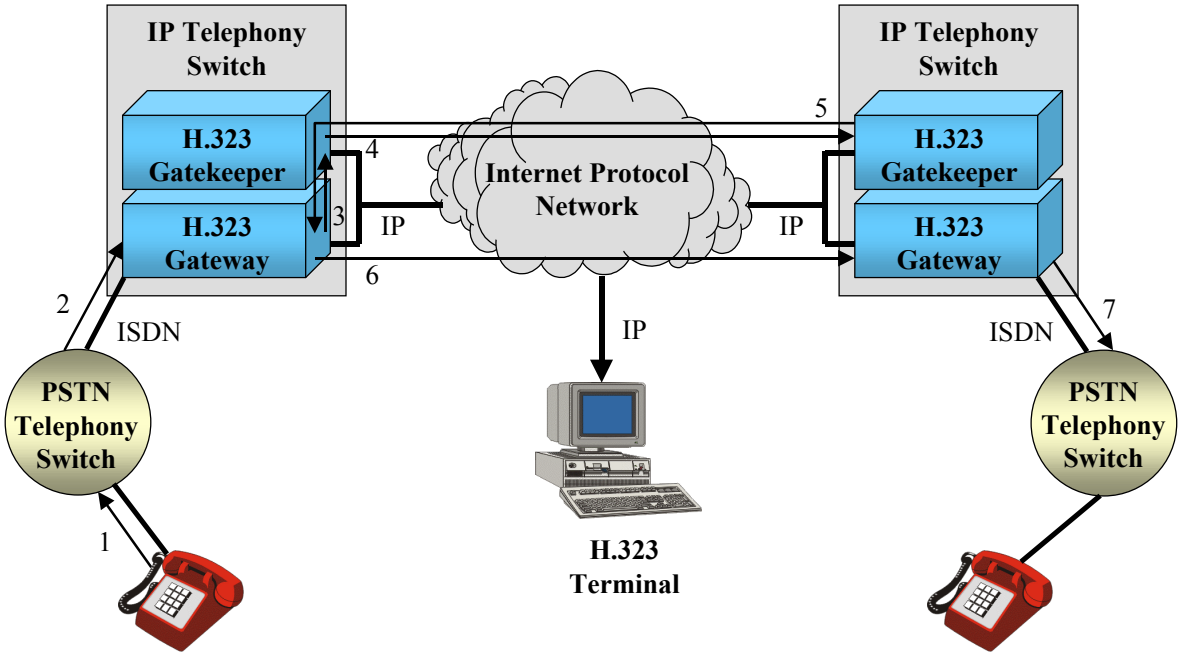


Figura 7 – Passos para o estabelecimento de uma conexão de VoIP

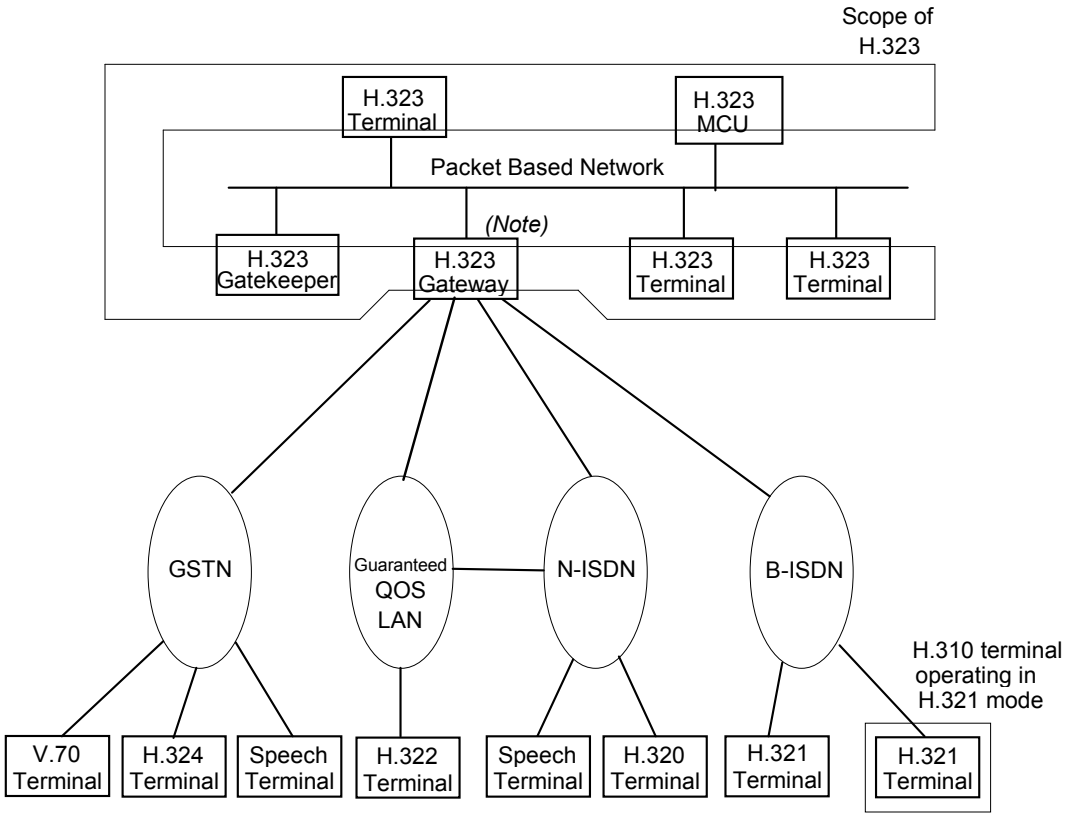
Em uma arquitetura integrada onde a prestadora de serviços de telecomunicações utiliza um backbone IP para transportar o tráfego de voz, os passos 1 a 3 listados acima se resumem a um único passo, onde o usuário disca o número do telefone de destino. A própria rede cuida de, a partir deste número, estabelecer a chamada.

2. O PADRÃO H 323 [10]

A recomendação H.323 define os requisitos para sistemas de comunicação multimídia em situações onde o transporte das informações é feito em uma rede baseada em pacotes (Packet Based Network – PBN) que não pode prover Qualidade de Serviço (QoS) garantida. As redes PBN podem incluir: redes locais (LANs), redes empresariais, redes metropolitanas (MANs), intra-redes, e inter-redes (incluindo a Internet). Elas também incluem conexões discadas ou conexões ponto-a-ponto sobre a rede pública de telefonia ou RDSI onde ocorre o transporte baseado em pacotes, tal como conexões PPP. Estas redes podem consistir de um único segmento de rede, ou pode ter topologias complexas que incorporam muitos segmentos de redes interconectados por outros enlaces de comunicação.

O sistema H.323 é composto de Terminais, Gateways, Gatekeepers, Controladores Multiponto, Processadores Multiponto e Unidades de Controle Multiponto. Mensagens de controle e procedimentos definidos na H.323 definem como estes componentes se comunicam.

Os terminais H.323 podem prover serviços de áudio e vídeo (opcionalmente) em tempo real e serviços de comunicação de dados. Os terminais H.323 podem interoperar com terminais H.310 e H.321 na RDSI-FL, terminais H.320 na RDSI-FE, terminais H.322 em redes LANs com Qualidade de Serviço Garantida, terminais H.324 e V.70 na rede pública comutada, e terminais de voz na rede pública comutada e RDSI através do uso de Gateways. Os terminais H.323 podem ser integrados em PCs ou implementados em dispositivos isolados (por exemplo: videofones). A Figura 8 ilustra a interoperabilidade dos terminais H.323.



Note: A gateway may support one or more of the GSTN, N-ISDN and/or B-ISDN connections.

Figura 8 – Interoperabilidade de terminais H.323.

Os Gatekeepers provêm controle de admissão e serviços de translação de endereços. Controladores Multiponto, Processadores Multiponto e Unidades de Controle Multiponto provêm suporte para conferências multiponto.

2.1. PILHA DE PROTOCOLOS

A H.323 define quatro pilhas de protocolos (vídeo, áudio, controle e dados), mas para aplicação de Voz sobre IP, apenas as partes de áudio e controle, sombreadas na Figura 9, são utilizadas [7].

<table>
<tr><td colspan="2">Vídeo</td><td colspan="2">Audio</td><td colspan="3">Control</td><td>Data</td></tr>
<tr><td colspan="2">H.261
H.263</td><td colspan="2">G.711
G.722
G.723
G.728
G.729</td><td rowspan="2">H.225

Terminal to gatekeeper signaling</td><td rowspan="2">H.225
Call signaling</td><td rowspan="2">H.245</td><td rowspan="2">T-120
(Multipoint data transfer)</td></tr>
<tr><td>RTP</td><td>R
T
C
P</td><td>RTP</td><td>R
T
C
P</td></tr>
<tr><td colspan="4">Unreliable transport (UDP)</td><td colspan="4">Reliable transport (TCP)</td></tr>
</table>

Figura 9 – Pilha de protocolos H.323.

Os codificadores de voz padronizados para a arquitetura H.323 são [11]:

G.711 - Utiliza a técnica PCM (Pulse Code Modulation) para digitalização do sinal de voz. A taxa de transmissão é de 64 kbps. O G.711 é um padrão reconhecido internacionalmente, largamente utilizado na conversão de sinais de voz analógicos para transmissão em redes digitais. A qualidade resultante é adequada para sinais de voz (toll quality), mas não é considerada boa para sinais de áudio.

G.722 - Utiliza uma variante da técnica ADPCM, denominada SB-ADPCM (Sub-Band Adaptative Differential Pulse Code Modulation). É utilizado nos canais B (64 kbps) da RDSI para transmissão de sinais de áudio de média qualidade (freqüências até 7 KHz). O atraso gerado na codificação é pequeno (cerca de 5 ms).

G.723.1 - O padrão ITU-T G.723.1 (uma combinação de G.721 + G.723) produz níveis de compressão digital da voz de 10:1 e 12:1, operando respectivamente a 6.3 kbps e 5.3 kbps, com maior qualidade para a taxa mais alta. A característica de largura de faixa reduzida é ideal para telefonia sobre a Internet em tempo real e para aplicações sobre linhas telefônicas convencionais. O G.723.1 se tornou um padrão emergente para a interoperabilidade da transmissão de voz em plataformas distintas. Testes demonstraram uma qualidade equivalente à qualidade comercial (toll quality) dos serviços de telefonia convencional com apenas 1/10 da largura de faixa utilizada pelos sistemas PCM atuais. A partir de 12 de março de 1997, o Forum de Voz sobre IP (VOIP) do International Multimedia Teleconferencing Consortium's (IMTC), recomendou o G.723.1 como o padrão "default" para a codificação de áudio em baixas taxas de bit no âmbito da norma H.323. O tamanho do quadro (frame) é de 30 ms e o parâmetro de lookahead é de 7.5 ms (veja definição no Capítulo 3, item 1.2.4). A complexidade do algoritmo é de 16 MIPS (Millions of Instructions per Second), com 2.2 Kbytes de memória RAM. O codificador se baseia na técnica denominada Linear Prediction Analysis-by-Synthesis Coding [6].

G.728: Utiliza a técnica LD-CELP (Low Delay Codebook Excited Linear Prediction), que é uma técnica híbrida de vocoder (codificação por vocalização) e codificação de forma de onda. O sinal de voz é limitado em 4 KHz e digitalizado a 16 Kbps.

G.729: Utiliza a técnica de codificação denominada CS-ACELP (Conjugate Structure Algebraic Codebook Excited Linear Prediction) para codificar um sinal analógico na faixa de voz em um sinal digital de 8Kbps. O tamanho do quadro (frame) é de 10ms e o lookahead delay é de 5 [ms]. A complexidade do algoritmo requer cerca de 20 MIPS de CPU e 3 Kbytes de RAM.

Uma versão mais enxuta do padrão G.729 pode ser encontrada no padrão G.729a. Este é compatível com o G.729 em termos de taxa de bits e de atraso, e requer apenas 10,5 MIPS de CPU e 2Kbytes de RAM. Por este bom desempenho com pouca exigência de capacidade de processamento, a técnica G.729a tem sido muito utilizada nos sistemas comerciais de VoIP e VoFR [4][11].

A H.323 especifica que os pacotes de voz sejam encapsulados no Protocolo RTP (Real-Time Transport Protocol) e transportados no UDP (User Datagram Protocol). Para gerenciar a qualidade da comunicação de voz na rede, utiliza-se o protocolo RTPC (Real-Time Control Protocol) [7][12].

A parte de controle do H.323 também utiliza o UDP como protocolo de transporte para estabelecer conexões entre os terminais H.323 e o Gatekeeper, que é basicamente um servidor de acesso remoto (RAS –Remote Access Server) da rede H.323, e o TCP para sinalização de chamada e canal de controle. Os protocolos H.225, que é um subconjunto do protocolo Q.931 (protocolo de sinalização da RDSI) e H.245 definem toda a operação de controle da arquitetura H.323.

2.2. COMPONENTES DA ARQUITETURA H.323

2.2.1. TERMINAL

O terminal H.323 é um dispositivo de usuário que provê comunicação (bidirecional e em tempo real) de voz, vídeo ou dados, com outro terminal H.323. A comunicação de voz é mandatória, mas a comunicação de vídeo e dados é opcional. O terminal H.323 pode também se comunicar com um Gateway H.323 ou uma MCU (Unidade de Controle Multiponto) [12].

Um exemplo de terminal H.323 é mostrado na Figura 10. O diagrama mostra as interfaces com o equipamento do usuário, codificador de vídeo, codificador de áudio, equipamento

telemático, a camada H.225.0, as funções de controle do sistema e a interface com a rede baseada em pacotes. Todos os terminais H.323 devem ter uma Unidade de Controle do Sistema, a camada H.225.0, a Interface de Rede e a Unidade de Codificação de Áudio. A Unidade de Codificação de Vídeo e Aplicações de Dados do Usuário são opcionais [10].

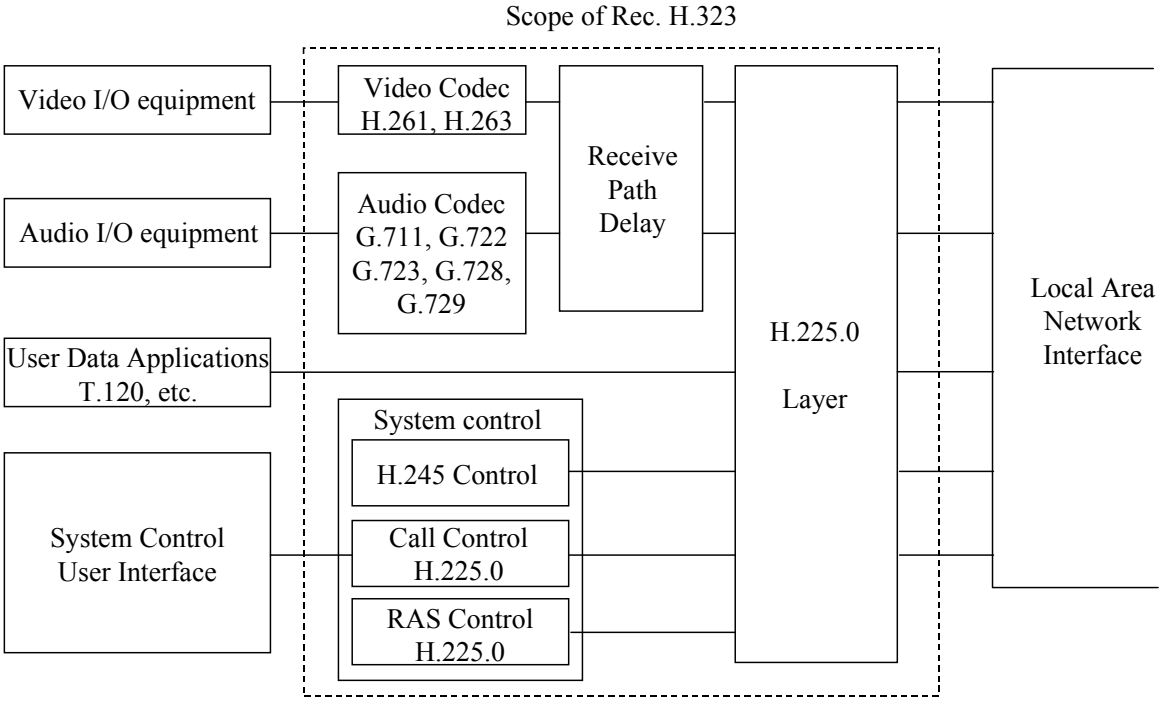


Figura 10 – Equipamento Terminal H.323

2.2.2. GATEWAY [10]

O Gateway é um dispositivo de adaptação utilizado para permitir a comunicação entre terminais H.323 e terminais não-H.323. A principal função do Gateway é a translação entre formatos de transmissão (por exemplo: H.225 para H.221), procedimentos de comunicação (por exemplo: H.245 para H.242), e formatos de áudio, vídeo e dados (por exemplo: G.711 para G.729). O Gateway também executa (em conjunto com o Gatekeeper) funções de estabelecimento e desconexão de chamadas do lado da rede local (packet based network) e da rede com comutação de circuito (rede telefônica, RDSI, etc.). Em geral, o objetivo do

Gateway é refletir as características de um terminal da rede local (H.323) para um outro terminal da rede comutada por circuitos, e vice-versa.

Um terminal H.323 pode se comunicar com outro terminal H.323 da mesma rede diretamente, sem o envolvimento de um Gateway. O Gateway pode ser omitido caso não se deseje estabelecer comunicação com terminais da rede com comutação de circuitos. É permitido a um terminal H.323 de uma rede estabelecer uma chamada de saída através de um Gateway e retornar à mesma rede através de outro Gateway, por exemplo para "bypassar" um roteador ou um enlace de baixa velocidade.

O Gateway pode também operar como uma Unidade de Controle Multiponto (MCU) que será descrita no item 2.2.4.

2.2.3. GATEKEEPER [7][10]

Embora a codificação eficiente do sinal de voz seja uma questão importante no transporte de voz sobre IP, esta não é a única responsabilidade dos Gateways ou Terminais H.323. Muitas funções de controle devem ser executadas pelo sistema H.323, incluindo o estabelecimento e desconexão de chamadas, a negociação de parâmetros da chamada (por exemplo, o tipo de codec que será utilizado), a medição de atrasos e mesmo a manutenção do enlace com mensagens de "keepalive" durante períodos de silêncio. Dentro da estrutura do H.323, estas questões são resolvidas pelos subsistemas de controle H.225 e H.245 [7].

Estas funções de controle podem ser executadas diretamente entre Terminais e Gateways H.323, ou podem ser delegadas para um outro dispositivo cuja única responsabilidade é a administração dos serviços de controle da chamada no sistema VoIP, denominado Gatekeeper. O Gatekeeper não é obrigatório no sistema H.323, mas sua utilização é comum em sistemas práticos, onde o número de equipamentos ultrapassa algumas unidades. Mais que um Gatekeeper pode estar presente e se comunicar com cada outro da rede de forma não especificada. O Gatekeeper pode ser fisicamente implementado em um terminal, MCU,

Gateway, ou outro dispositivo de rede não-H.323, embora seja uma entidade lógica independente destes dispositivos.

As principais funções do Gatekeeper são:

TRADUÇÃO DE ENDEREÇOS: o Gatekeeper permite o uso local de esquemas de endereçamento proprietários (chamados de apelidos no H.323), tais como mnemônicos, nicknames, ou endereços de e-mail. O Gatekeeper irá traduzir estes endereços em endereços IP necessários para o estabelecimento das comunicações IP. Este processo pode ser feito através de uma tabela de translação, que é atualizada através de mensagens de registro.

CONTROLE DE ADMISSÕES: O Gatekeeper é responsável por controlar o estabelecimento de chamadas entre terminais H.323, Gateways, e outros dispositivos não-H.323. A admissão de uma chamada pode ser autorizada ou negada baseado em procedimentos de autenticação do usuário, endereços de fonte ou destino, hora do dia, largura de banda disponível, ou qualquer outro critério conhecido pelo Gatekeeper. O controle de admissão pode também ser uma função nula, onde todos os pedidos seriam aceitos.

CONTROLE DE LARGURA DE FAIXA: O Gatekeeper pode controlar o número de terminais H.323 com acesso simultâneo à rede. Através de sinalização H.225, o Gatekeeper pode rejeitar chamadas de um terminal devido a limitações de largura de faixa. Esta função pode também operar durante uma chamada ativa se um terminal solicitar banda adicional. O critério para determinar se a largura de faixa disponível é suficiente para atender uma chamada entrante não é definido na H.323.

GERENCIAMENTO DE ZONA: O Gatekeeper pode coordenar as ações, associadas às funções acima, entre os dispositivos que fazem parte de sua zona de influência (dispositivos que estão sob responsabilidade do Gatekeeper). Por exemplo, o gerenciamento de zona pode requerer que não mais que 25 chamadas sejam permitidas através de um dado enlace

de baixa velocidade, de modo que a qualidade não seja degradada. Este tipo de gerenciamento pode também permitir funções tais como distribuição automática de chamada (ACD – Automatic Call Distribution) ou outros serviços associados a call-center.

SINALIZAÇÃO DE CHAMADA: O Gatekeeper pode atuar como um "proxy" de sinalização de chamada para os terminais ou Gateways sob sua responsabilidade, aliviando-os da necessidade de suportar protocolo de controle de chamada. De outra forma, o Gatekeeper pode simplesmente servir como um ponto de contato inicial, ou seja, após a admissão da chamada proposta, o Gatekeeper põe os dois terminais (ou Gateways) para trocar mensagens de sinalização diretamente.

Um Gatekeeper e todos os dispositivos sob seu controle formam uma zona H.323, que é um grupo lógico de dispositivos sob uma única autoridade administrativa. Este conceito é ilustrado na Figura 11.

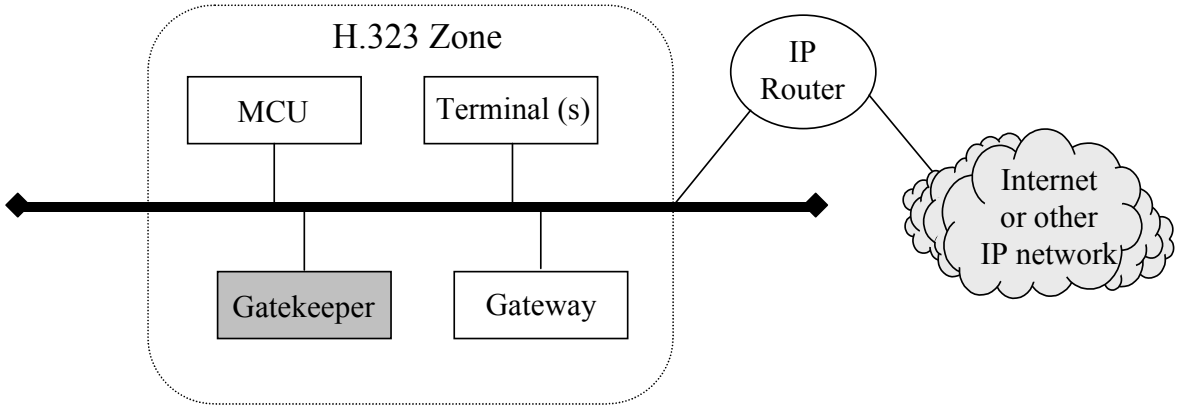


Figura 11 – Uma zona H.323.

Um terminal ou Gateway sob a responsabilidade de um Gatekeeper deve estar registrado no mesmo. O procedimento de registro deve incluir a anotação do endereço (IP e apelido) e outras informações (tais como limites de largura de faixa do canal) necessárias para o Gatekeeper agir no lugar do dispositivo. Este registro pode ser feito manualmente, através de arquivos de configuração, ou através de procedimentos de registro e descoberta definidos na H.323.

Os Gatekeeper simplificam o desenvolvimento e uso de sistemas de VoIP, centralizando e coordenando a administração da sinalização de chamada, servindo portanto como um nó de controle para todos os dispositivos em sua zona de atuação.

2.2.4. MULTIPOINT CONTROL UNIT (MCU) [10]

A Unidade de Controle Multiponto (MCU) suporta conferências entre três ou mais terminais e Gateways. Segundo o padrão H.323, uma MCU consiste de um Controlador Multiponto (MC), obrigatório, e zero ou mais Processadores Multiponto (MP).

Uma MCU típica que suporta conferências multiponto centralizadas consiste de um MC e um MP de áudio, vídeo e dados. Uma MCU típica que suporta conferências multiponto descentralizadas consiste de um MC e um MP de dados suportando a Recomendação T.120.

O MC suporta a negociação de capacidades entre todos os terminais, para se garantir um nível comum de comunicações. O MC envia um conjunto de "capacidades" aos participantes da conferência, indicando os modos de operação em que eles devem transmitir. Este conjunto de capacidades pode ser revisto pelo MC, e reenviado aos terminais, em função da adesão de novos terminais ou desistência de membros da conferência. O MP é responsável por mixar, comutar e processar áudio, vídeo, e/ou bits de dados. O MP é o processador central de voz, vídeo e dados para uma conferência multiponto. O MC e o MP podem existir em um componente dedicado ou fazer parte de outros componentes H.323.

As possibilidades de conferência multiponto são tratadas em uma variedade de métodos e configurações segundo o H.323. A recomendação usa o conceito de conferências centralizadas e descentralizadas, como descrito na Figura 12.

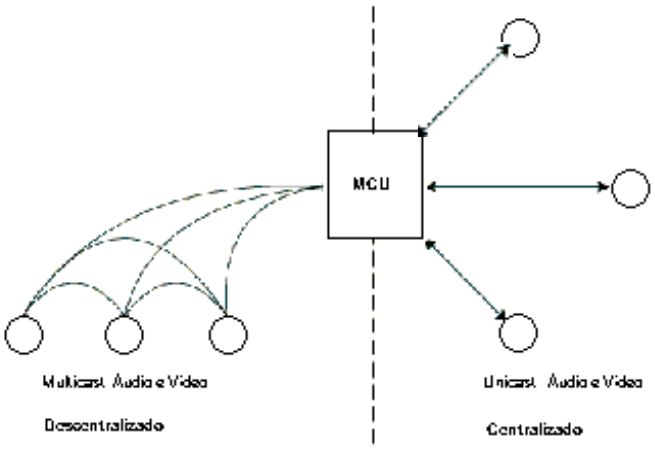


Figura 12 – Conferências centralizadas e descentralizadas.

Conferências multiponto centralizadas exigem a presença de um MCU. Todos os terminais enviam áudio, vídeo, dados e fluxos de controle para o MCU em um modo ponto-a-ponto. O MC gerencia a conferência através das funções de controle H.245 que também definem as capacidades para cada terminal. O MP recebe, processa e envia os sinais de voz, vídeo ou dados para os dispositivos participantes. O MP também pode fornecer conversão entre diferentes códigos e taxas de bits, permitindo a participação de dispositivos com diferentes modos de comunicação. A MCU pode utilizar multicast para distribuir os fluxos de áudio e vídeo se os dispositivos participantes da conferência têm capacidade para receber transmissões multicast. A distribuição multicast de dados ainda não foi definida [10].

Conferências multiponto descentralizadas podem fazer uso da tecnologia multicast de forma que terminais H.323 se comuniquem sem enviar os dados para uma MCU. O MC pode prover algumas funções de controle da conferência, tais como a "presidência" da conferência, broadcast de vídeo e seleção de vídeo. Isto pode ser feito utilizando-se o H.245. O MC recebe mensagens H.245 dos participantes da conferência e envia o controle apropriado para os outros dispositivos, para habilitar ou desabilitar seus sistemas de multicast de vídeo. Comandos T.120 podem opcionalmente prover as mesmas funções.

Outra possibilidade de implementação são as conferências multiponto híbridas, que combinam características dos tipos centralizada e descentralizada. As opções são conferência multiponto com áudio centralizado e conferência multiponto com vídeo

centralizado. Em ambos os casos, os dispositivos participantes da conferência se comunicam com o MC, de modo ponto-a-ponto, utilizando o canal de controle H.245.

2.3. ENDEREÇAMENTO [10]

O H.323 define três tipos de endereçamento: endereço de rede, identificador TSAP (Transport Layer Service Access Point), e apelido.

ENDEREÇO DE REDE: Cada entidade H.323 deve ter ao menos um endereço de rede. Este endereço identifica unicamente a entidade H.323 na rede. Algumas entidades podem compartilhar um mesmo endereço de rede (por exemplo, um terminal e um MC residente no terminal). Este endereço é específico do ambiente de rede em que o dispositivo está localizado. Diferentes ambientes de rede podem ter diferentes formatos de endereço de rede.

IDENTIFICADOR TSAP: Para cada endereço de rede, cada entidade H.323 pode ter vários identificadores TSAP, que permitem a multiplexagem de vários canais compartilhando o mesmo endereço de rede.

Três identificadores TSAP possuem seu valor especificado pela recomendação H.225: Identificador TSAP do canal de sinalização de chamada, para os dispositivos terminais (terminais, Gateways ou MCUs), identificador TSAP do canal RAS e endereço multicast de descoberta para os Gatekeepers.

Dispositivos terminais e entidades H.323 podem utilizar identificadores TSAP dinâmicos para o canal de controle H.245, canais de áudio, canais de vídeo, e canais de dados. O Gatekeeper pode utilizar um identificador TSAP dinâmico para os canais de sinalização de chamada. Os canais RAS e canais de sinalização podem ser redirecionados para identificadores TSAP dinâmicos durante o procedimento de registro.

APELIDOS: Um dispositivo H.323 pode também ter um ou mais apelidos. Um apelido pode representar o dispositivo ou conferências que o dispositivo está hospedando. O apelido provê um método alternativo de endereçamento do dispositivo. Este tipo de endereço incluí: endereços E.164, nomes alfanuméricos, endereços de e-mail, etc. Os apelidos devem ser únicos em uma zona H.323. O dispositivo pode ter mais de um apelido (inclusive mais que um do mesmo tipo), que serão transladados para o mesmo endereço de transporte. Gatekeepers, MCs e MPs não devem ter apelidos.

Quando não existe um Gatekeeper no sistema, o dispositivo chamador deve endereçar o dispositivo chamado diretamente, através do endereço de transporte do canal de sinalização de chamada do dispositivo de destino. Quando existe um Gatekeeper, o dispositivo chamado pode endereçar o dispositivo de destino por seu endereço de transporte ou por seu apelido, que será traduzido em um endereço de transporte pelo Gatekeeper.

Os endereços E.164 dos dispositivos chamados podem consistir de um código de acesso opcional seguido pelo endereço E.164. O código de acesso consiste de n dígitos (0 a 9, *,#). O número de dígitos e seu significado são definidos por cada fabricante. O objetivo deste código é permitir o envio de uma requisição de acesso ao Gateway. O Gatekeeper pode alterar este endereço antes de enviá-lo ao destino.

2.4. OPERAÇÕES DE REGISTRO, ADMISSÃO E STATUS (OPERAÇÕES RAS)

Nesta seção iremos descrever algumas funções do H.323 relacionadas a: descoberta de Gatekeeper, registro de dispositivos e gerenciamento de chamada. A titulo de ilustração, alguns exemplos de troca de mensagens entre os dispositivos terminais e o Gatekeeper, envolvendo os protocolos H.225 e H.245, para a execução desta funções serão mostrados. Várias outras possibilidades e exemplos de troca de mensagens podem ser obtidos em [10]. A definição da estrutura e conteúdo das mensagens descritas neste item, e de outras não abordadas, podem ser obtidas em [13].

O H.323 utiliza um canal lógico na rede (packet based network) para gerenciar todas as atividades de sinalização, que é denominado canal RAS (Registration, Admissions, and Status). A função de sinalização RAS utiliza mensagens H.225 para uma variedade de operações de suporte.

2.4.1. PROCEDIMENTOS DE DESCOBERTA DE GATEKEEPER

A descoberta do Gatekeeper é o processo pelo qual o dispositivo determina em que Gatekeeper ele deve se registrar. O procedimento pode ser manual, onde o dispositivo é pré-configurado com o endereço de transporte do Gatekeeper associado, ou automático. No procedimento automático a associação dispositivo-Gatekeeper pode se alterar com o tempo, devido a uma falha no Gatekeeper, por exemplo.

No método automático, um dispositivo que não sabe qual o seu Gatekeeper associado inicia um procedimento de auto-descoberta, que consiste no envio de uma mensagem multicast de requisição de Gatekeeper (GRQ), perguntando: “Quem é meu Gatekeeper?”. Esta mensagem é enviada aos endereços multicast de descoberta de Gatekeeper. Um ou mais Gatekeepers podem responder com uma mensagem de confirmação de Gatekeeper (GCF), indicando: “Eu posso ser seu Gatekeeper”. Esta mensagem contém o endereço de transporte do canal RAS do Gatekeeper. Se um Gatekeeper não deseja registrar um dispositivo ele deve retornar uma mensagem de rejeição de Gatekeeper (GRJ). Se mais que um Gatekeeper responde, o dispositivo pode escolher qual o Gatekeeper que ele deseja utilizar. Neste ponto, o dispositivo sabe qual o Gatekeeper em que ele deve fazer seu registro. A Figura 13 ilustra a troca de mensagens descrita neste parágrafo.

De modo a prover redundância no sistema, o Gatekeeper pode indicar Gatekeepers alternativos, que podem ser utilizados em caso de falha do Gatekeeper principal. Esta lista é enviada na estrutura **alternateGatekeeper** da mensagem GCF (ou da mensagem RCF, que será descrita posteriormente).

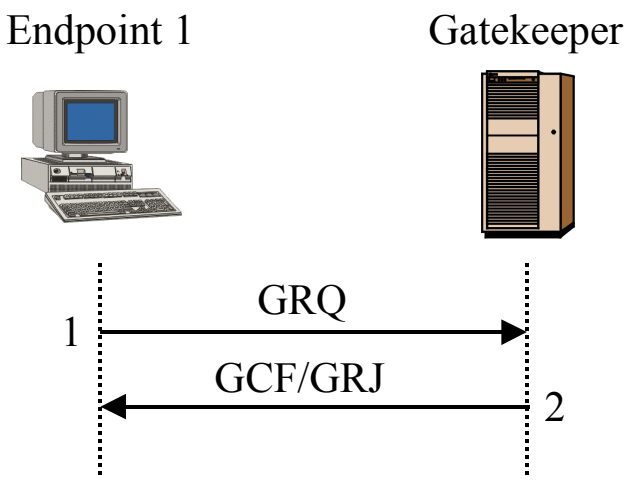


Figura 13 – Procedimento de auto-descoberta.

Se nenhum Gatekeeper responde após transcorrido tempo igual ao timeout, o dispositivo pode reenviar a mensagem GRQ (pelo menos após 5 segundos do envio da mensagem anterior).

Se o dispositivo, há qualquer momento, determina que seu registro no Gatekeeper é inválido, ele deve redescobrir seu Gatekeeper. A condição de registro inválido pode ser caracterizada pelas seguintes situações: o dispositivo envia uma mensagem de RRQ (Request Registration) ao Gatekeeper e recebe deste uma mensagem de RRJ (Registration Reject) ou não recebe nenhuma resposta.

O conteúdo específico das mensagens GRQ, GCF, e GRJ é definido na recomendação H.225.0, utilizando-se a notação de sintaxe abstrata (Abstract Syntax Notation.1 – ASN.1).

2.4.2. REGISTRO [10][12]

O registro é o procedimento pelo qual um dispositivo terminal se junta a uma zona, e informa ao Gatekeeper seu endereço de transporte e apelido. Como parte do processo de configuração todos os dispositivos devem se registrar no Gatekeeper identificado através do procedimento de descoberta. O registro deve ocorrer antes que qualquer chamada seja

iniciada e deve ocorrer periodicamente quando necessário (por exemplo, quando o dispositivo é ligado).

Um Gateway ou MCU pode registrar um ou mais endereços de transporte. O uso de múltiplos endereços pode simplificar o roteamento de chamadas para portas específicas.

O dispositivo que deseja se registrar envia uma mensagem de requisição de registro (RRQ – Registration Request) para o Gatekeeper. A mensagem é enviada para o endereço de transporte do canal RAS do Gatekeeper. O dispositivo tem o endereço de rede do Gatekeeper, que foi obtido no processo de descoberta, e conhece o identificador TSAP do canal RAS. O Gatekeeper responderá ou com uma mensagem de confirmação (RCF – Registration Confirmation) ou com uma mensagem de rejeição (RRJ – Registration Reject). Um dispositivo só pode se registrar em um único Gatekeeper.

O RRQ pode ser repetido periodicamente, tal que o Gatekeeper possa manusear múltiplas requisições do mesmo dispositivo. Quando uma mensagem RRQ chega ao Gatekeeper, as seguintes situações, quanto ao conteúdo do endereço do dispositivo na mensagem, podem ocorrer:

- Endereço de transporte e apelido idênticos a um RRQ anterior: Gatekeeper responde com RCF.
- Apelido igual a RRQ anterior e endereço de transporte diferente: Gatekeeper pode confirmar a requisição, se isto está de acordo com a política de segurança do Gatekeeper, ou rejeitar a requisição, indicando a duplicidade de registro.
- Endereço de transporte idêntico a RRQ anterior e apelido diferente: Gatekeeper deve alterar o conteúdo da tabela de translação. O Gatekeeper pode estabelecer algum método de autenticação destas mudanças.

O registro do dispositivo no Gatekeeper pode ter uma vida finita. O tempo que o registro permanecerá válido pode ser indicado pelo dispositivo no parâmetro **time_to_live**, expresso em segundos, da mensagem RRQ, enviada pelo dispositivo ao Gatekeeper. O Gatekeeper pode responder com uma mensagem RCF contendo o mesmo valor de **time_to_live** ou um

valor menor; este será o tempo de validade do registro no Gatekeeper. Antes que o tempo de validade expire, o dispositivo deve enviar uma mensagem RRQ com o bit de **keep_alive** setado, fazendo com que o contador de tempo de validade seja reinicializado. A mensagem **keep_alive** RRQ não precisa conter todas as informações de uma mensagem RRQ normal. Caso o tempo de validade expire, o dispositivo terá de se registrar novamente no Gatekeeper, através de uma mensagem RRQ normal.

O Gatekeeper deve garantir que a cada apelido esteja associado um único endereço de transporte. Contudo, um dispositivo pode indicar um endereço de transporte alternativo (backup ou redundância), através do campo **alternate_endpoint** das mensagens RAS. Isto permite a um dispositivo ter uma interface de rede secundária ou um outro dispositivo H.323 secundário como backup. Registros ambíguos devem ser rejeitados pelo Gatekeeper.

Se o dispositivo não incluir um apelido na mensagem de RRQ, o Gatekeeper pode fazer a associação de um apelido ao dispositivo, e informá-lo do conteúdo do apelido associado através da mensagem RCF.

Um dispositivo pode cancelar seu registro no Gatekeeper enviando uma mensagem de requisição de cancelamento de registro (URQ - Unregister Request), que será respondida pelo Gatekeeper com uma mensagem de confirmação de cancelamento (UCF – Unregister Confirmation). Se o dispositivo ainda não estava registrado no Gatekeeper, ele responderá com uma mensagem de rejeição de cancelamento (URJ – Unregister Reject). O cancelamento do registro permite ao dispositivo alterar o apelido associado ao seu endereço de transporte, ou vice-versa.

O Gatekeeper também pode tomar a iniciativa de cancelar o registro do dispositivo. Neste caso o Gatekeeper envia a mensagem de URQ ao dispositivo, que responde com a mensagem de UCF. Caso o dispositivo queira iniciar uma nova chamada, ele deve antes se registrar em um Gatekeeper (possivelmente em um Gatekeeper diferente daquele que cancelou o seu registro).

A Figura 14 ilustra a troca de mensagens efetuadas para o registro e cancelamento de registro de um dispositivo.

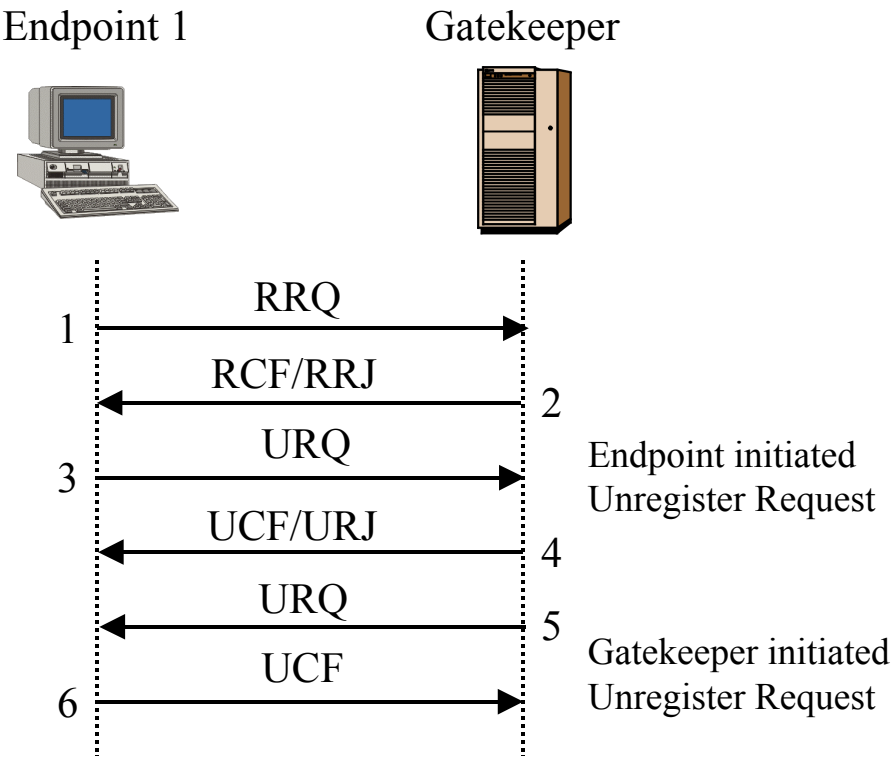


Figura 14 – Procedimento para registro no Gatekeeper.

2.4.3. ADMISSÃO (CALL SET-UP)

O canal RAS é também utilizado para a transmissão de mensagens de Admissão, Mudança de Largura de Faixa, Status, e Desconexão. Estas mensagens são trocadas entre os dispositivos terminais e o Gatekeeper e são usadas para implementar funções de controle de admissão e gerenciamento de largura de faixa.

Para iniciar o processo de admissão o dispositivo deve enviar uma mensagem de requisição (ARQ – Admissions Request) ao Gatekeeper. O Gatekeeper pode confirmar a admissão, enviando uma mensagem de confirmação de admissão (ACF – Admission Confirmation),

ou rejeitá-la, enviando uma mensagem de rejeição de admissão (ARJ – Admission Reject). A mensagem ARQ enviada pelo dispositivo especifica a largura de banda requerida para a chamada. Esta largura de banda é o limite superior da taxa de bits agregada, considerando-se todos os canais de áudio e vídeo (transmissão e recepção), excluindo-se os overheads (cabeçalhos RTP, cabeçalhos de rede, outros overheads). Os canais de dados e controle não são incluídos neste limite. O Gatekeeper pode reduzir a largura de banda da chamada, informando o terminal através da mensagem ACF. O dispositivo terminal deve garantir que a taxa de bits agregada (valor médio sobre 1 segundo) esteja abaixo da largura de banda da chamada definida. O dispositivo terminal ou o Gatekeeper podem tentar modificar a largura de banda da chamada durante a mesma, através da mensagem de requisição de mudança da largura de faixa (BRQ – Bandwidth Change Request).

2.4.4. EXEMPLO DE UMA CHAMADA H.323 [14][10]

A Figura 15 ilustra o estabelecimento de uma chamada em um sistema H.323 onde os dois dispositivos terminais estão registrados no mesmo Gatekeeper, e utiliza-se o método direto para o roteamento do canal de sinalização da chamada (mensagens H.225) e para o roteamento do canal de controle (mensagens H.245). A descrição dos métodos de roteamento possíveis será feita no item 2.4.5. As seguintes etapas são identificadas:

1. Dispositivo terminal T1 envia uma requisição de admissão (ARQ) ao Gatekeeper. O método de sinalização de chamada requisitado por T1 é o direto.
2. O Gatekeeper confirma a admissão de T1 através da mensagem ACF e confirma o método de sinalização solicitado. O Gatekeeper pode retornar o endereço de transporte do canal de sinalização de chamada do dispositivo terminal T2 na mensagem ACF.
3. T1 envia uma mensagem de setup à T2, usando o endereço de transporte fornecido pelo Gatekeeper.
4. T2 responde com uma mensagem de prosseguimento de chamada.
5. T2 envia uma requisição de admissão ao Gatekeeper (ARQ) no canal RAS.
6. O Gatekeeper confirma o registro enviando a mensagem ACF.
7. T2 alerta T1 do estabelecimento da conexão enviando uma mensagem alerting.

8. T2 confirma o estabelecimento da conexão enviando a mensagem connect. A mensagem connect contém o endereço endereço de transporte do canal de controle H.245, que será utilizado para a sinalização H.245.

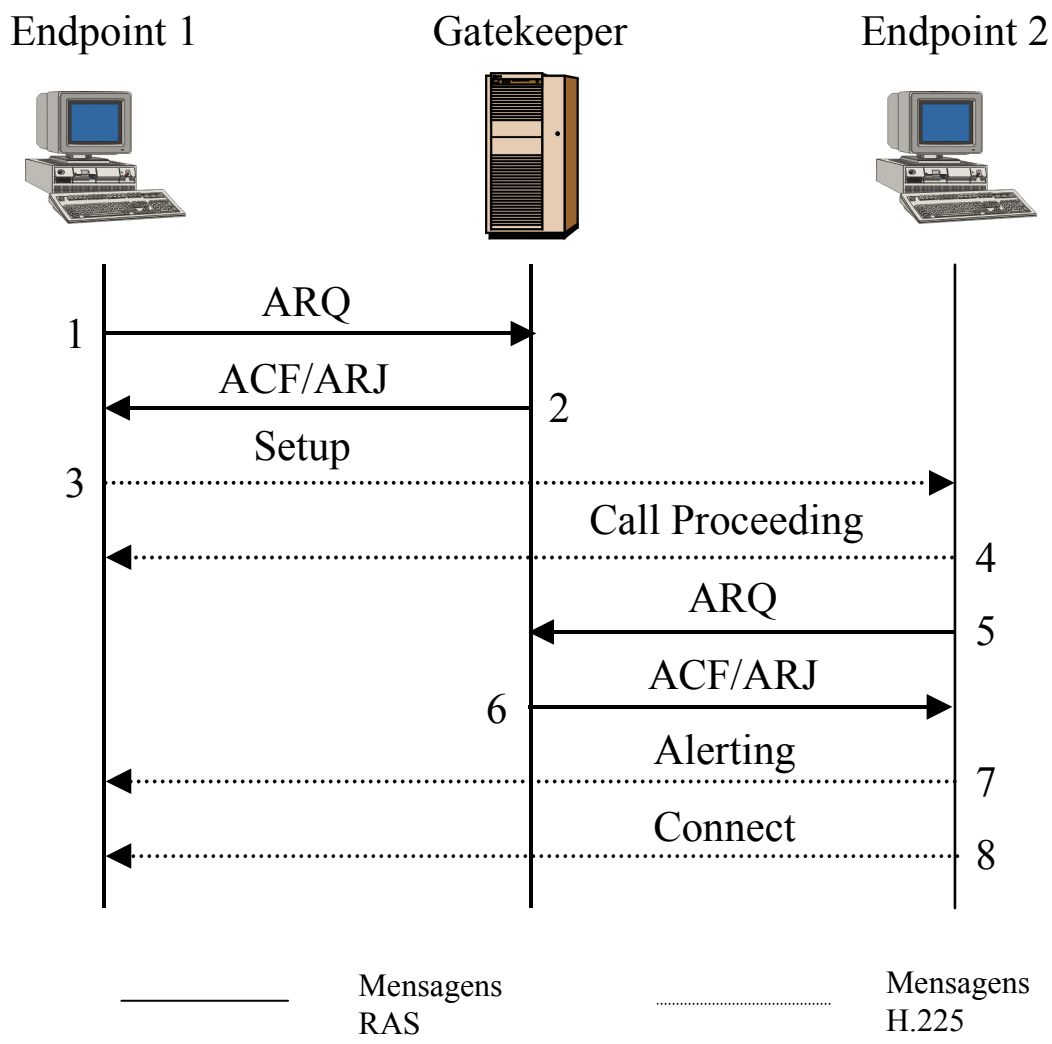


Figura 15 – Estabelecimento da chamada H.323.

O processo continua com o fluxo de sinalização de controle H.323, que utiliza mensagens H.245. A Figura 16 ilustra a troca de mensagens H.245 para o estabelecimento do canal de mídia entre T1 e T2. Os seguintes passos, em continuidade aos 8 anteriores, são identificados:

9. O canal de controle H.245 é estabelecido entre T1 e T2. T1 envia uma mensagem Terminal Capability Set para T2, iniciando a troca de informação entre T1 e T2 sobre suas capacidades.
10. T2 envia uma mensagem de reconhecimento da capacidade de T1 enviando uma mensagem Terminal Capability Set Ack.
11. T2 informa sua capacidade para T1 enviando a mensagem Terminal Capability Set.
12. T1 reconhece através da mensagem Terminal Capability Set Ack.
13. T1 abre um canal (media channel) com T2 enviando a mensagem Open Logical Channel. O endereço de transporte do canal RTCP é incluído na mensagem.
14. T2 reconhece o estabelecimento de um canal lógico unidirecional de T1 para T2, enviando a mensagem Open Logical Channel Ack. Incluído nesta mensagem estão o endereço de transporte RTP alocado por T2, a ser utilizado por T1 para o envio dos fluxos de áudio (e/ou vídeo) RTP, e o endereço RTCP recebido de T1.
15. T2 abre um canal (media channel) com T1 enviando a mensagem Open Logical Channel. O endereço de transporte do canal RTCP é incluído nesta mensagem.
16. T1 reconhece o estabelecimento de um canal lógico unidirecional de T2 para T1, enviando a mensagem Open Logical Channel Ack. Incluído nesta mensagem estão o endereço de transporte RTP alocado por T1, a ser utilizado por T2 para o envio dos fluxos de áudio (e/ou vídeo) RTP, e o endereço RTCP recebido de T2. Agora a comunicação de áudio (vídeo) bidirecional está estabelecida.

A partir de então, os pacotes de áudio podem ser enviados através do protocolo RTP, com o controle sendo feito pelo protocolo RTCP. A Figura 17 ilustra o fluxo de pacotes de áudio (vídeo) e o fluxo de controle RTCP.

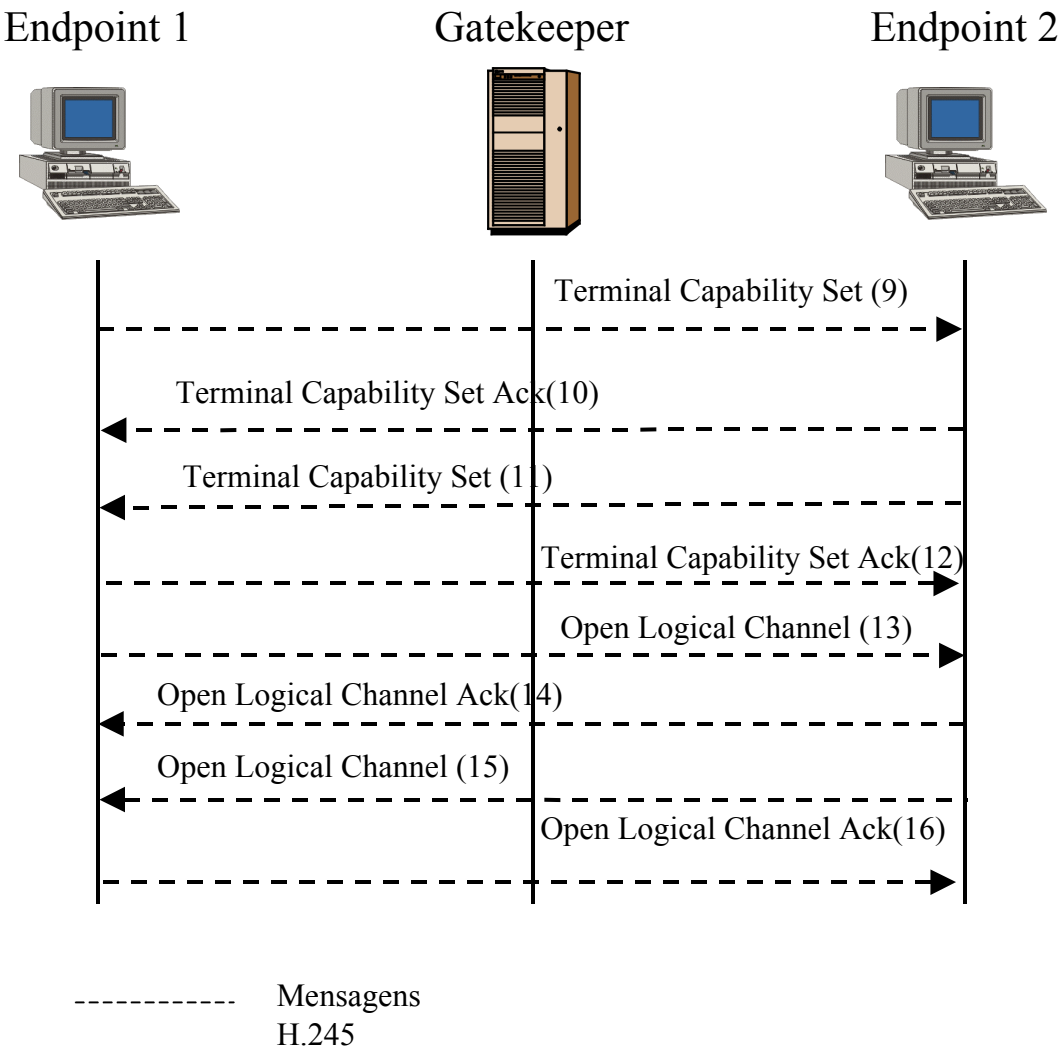


Figura 16 – Fluxo de sinalização de controle H.323

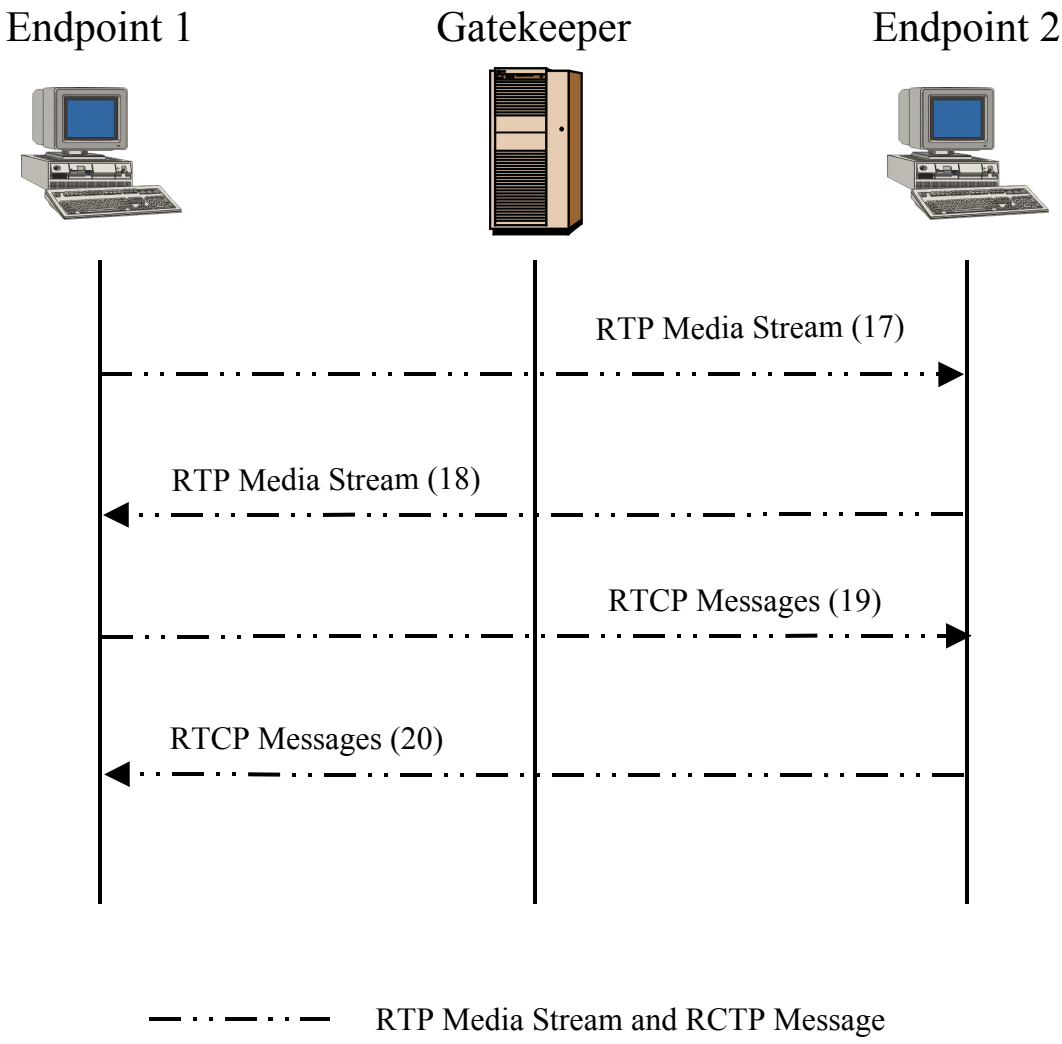


Figura 17 – Fluxo de pacotes de áudio e fluxos de controle RTCP.

Após o término da troca de informação entre T1 e T2, a chamada deve ser desfeita. Este procedimento envolve troca de mensagens H.225, H.245 e RAS, como indicado na Figura 18, onde os seguintes passos são identificados:

21. T2 inicia a desconexão. Ele envia uma mensagem (H.245) End Session Command para T1.
22. T1 confirma a desconexão enviando uma mensagem End Session Command para T2.
23. T2 completa a desconexão da chamada enviando uma mensagem (H.225) Release Complete para T1.

24. T1 e T2 se desconectam com o Gatekeeper enviando uma mensagem (RAS) de requisição de desconexão (DRQ - Disengage Request) para o Gatekeeper.
25. O Gatekeeper desconecta T1 e T2 e confirma esta ação enviando a mensagem DCF (Disengage Confirmation) para T1 e T2.

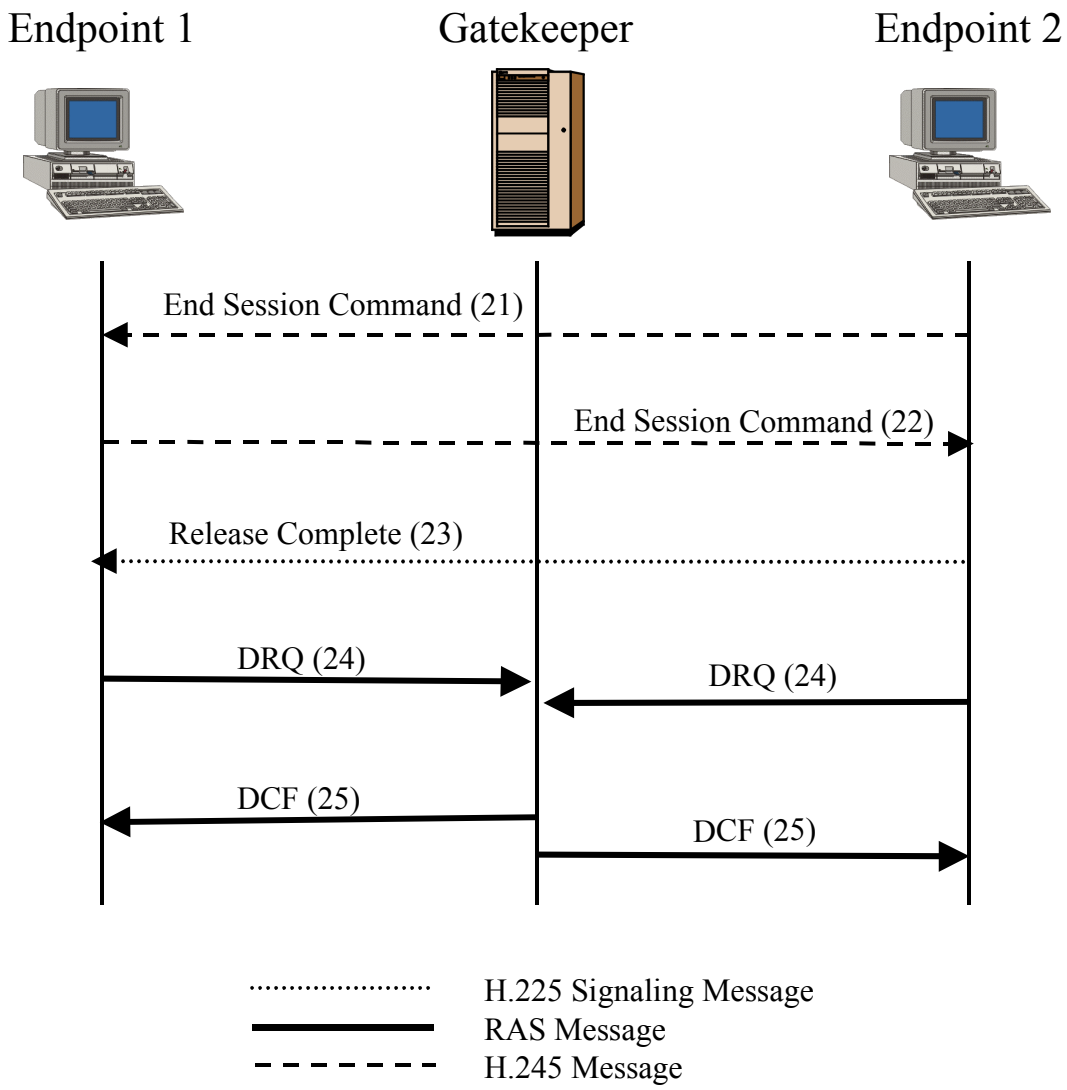


Figura 18 – Desconexão da chamada H.323

2.4.5. ROTEAMENTO DO CANAL DE SINALIZAÇÃO DE CHAMADA E CANAL DE CONTROLE [10]

As mensagens de sinalização de chamada (H.225) podem ser trocadas entre os dispositivos de duas formas. O primeiro método é chamado de Sinalização de Chamada Roteada pelo Gatekeeper, e é ilustrada na Figura 19. Neste método as mensagens de sinalização de chamada são roteadas através do Gatekeeper entre os dispositivos terminais. O segundo método é a Sinalização de Chamada Direta entre os dispositivos, ilustrada na Figura 20, onde os dispositivos terminais trocam mensagens H.225 diretamente entre si. A escolha do método a ser utilizado é feita pelo Gatekeeper.

O mesmo conceito se aplica para as mensagens de controle H.245. No método direto, ilustrado na Figura 21, o canal de controle H.245 é estabelecido diretamente entre os dispositivos terminais, enquanto no método roteado pelo Gatekeeper, ilustrado na Figura 22, as mensagens H.245 passam através de Gatekeeper.

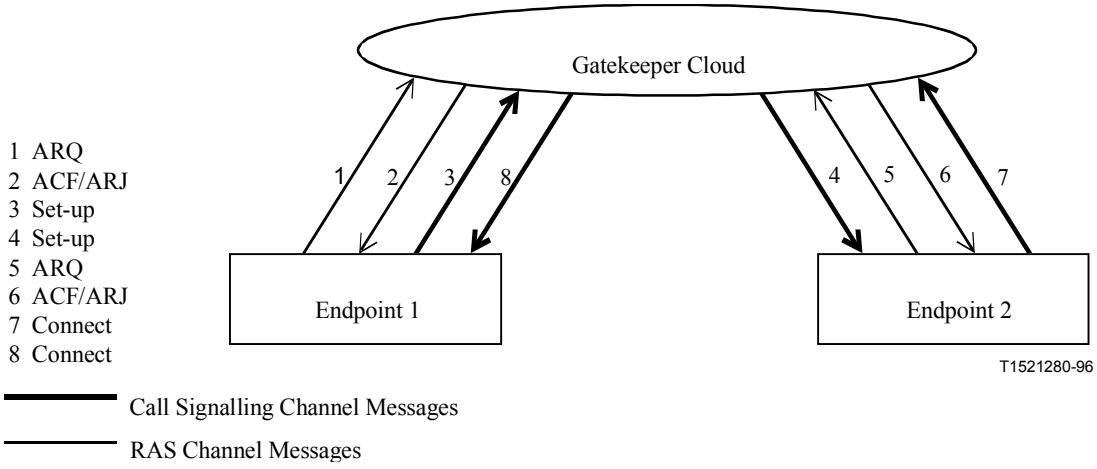


Figura 19 – Sinalização de chamada roteada pelo Gatekeeper.

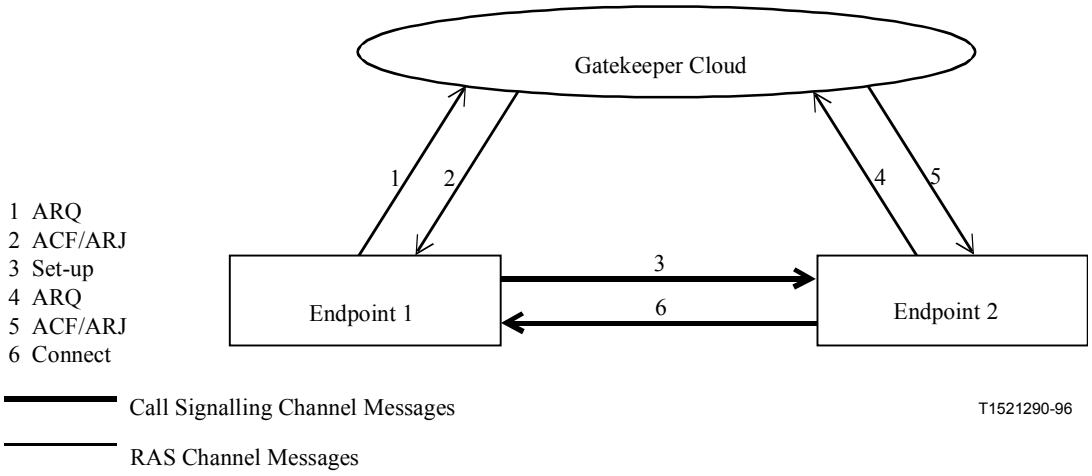


Figura 20 – Sinalização de chamada direta.

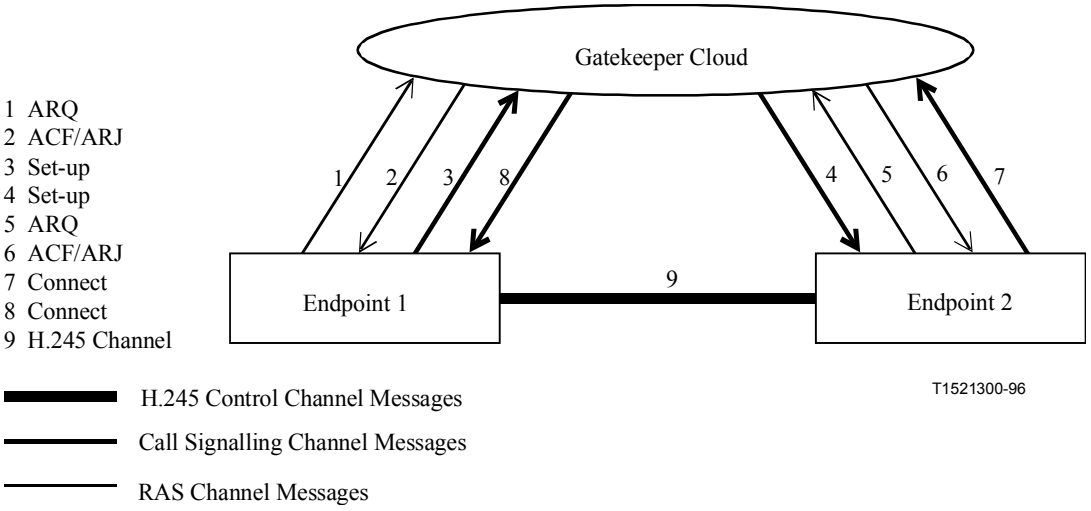


Figura 21 – Conexão de canal de controle H.245 direta.

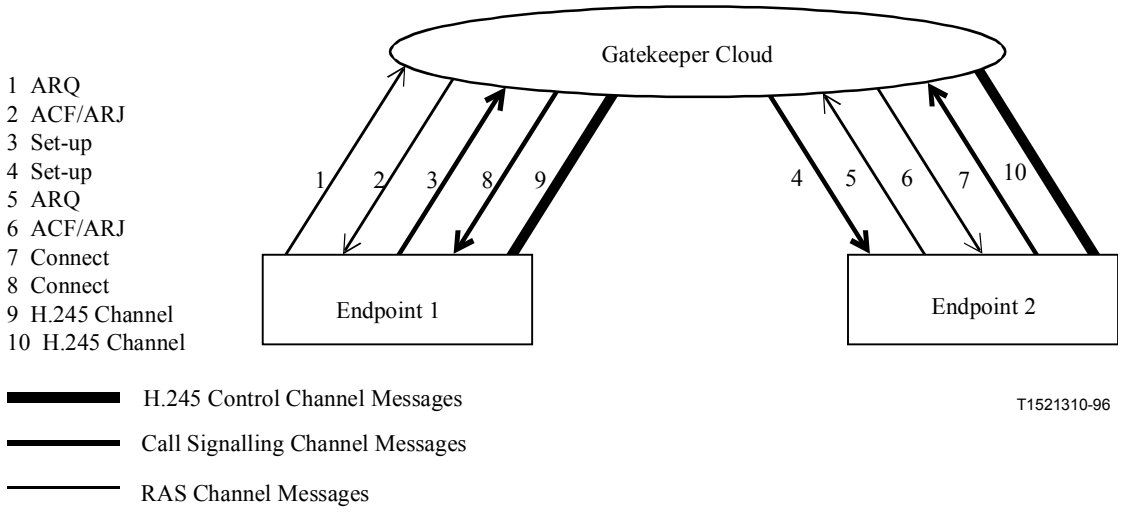


Figura 22 – Conexão de canal de controle H.245 roteada pelo Gatekeeper.

2.5. REAL-TIME TRANSPORT PROTOCOL (RTP e RTCP)

O Real-Time Transport Protocol (RTP) é um protocolo de transporte de tempo real que visa fornecer um serviço de entrega fim-a-fim para aplicações que transmitem dados em tempo real, tais como áudio e vídeo. Este protocolo está definido na RFC 1889 [15].

Além de suportar a transmissão de dados unicast, o RTP também admite a transmissão para múltiplos destinos usando a distribuição multicast.

Apesar de ser um protocolo de transporte, ele é usualmente executado como uma parte da camada de aplicação e tipicamente faz uso dos serviços de multiplexação e checksum oferecidos pelo User Datagram Protocol (UDP). Outros protocolos de transporte, tais como o TCP, também podem carregar o RTP.

O RTP é constituído de uma parte de dados (RTP) e uma parte de controle, denominada RTCP. A principal função do RTCP é prover realimentação da qualidade da distribuição dos dados [8]. O RTCP provê também suporte para conferências em tempo real com grupos

de qualquer tamanho no âmbito da Internet, assim como suporte para a sincronização de fluxos de diferentes mídias [4].

O RTCP se baseia na transmissão periódica de pacotes de controle para todos os participantes de uma sessão, utilizando os mesmos mecanismos de distribuição dos pacotes de dados. O RTCP define pacotes de report de transmissor (SR – Sender Report), utilizado para a transmissão de estatísticas por estações que são transmissoras ativas, e pacotes de report de receptor (RR – Receiver Report), utilizado para a transmissão de estatísticas de estações que não são transmissoras ativas. Uma estação é considerada transmissora ativa se ela enviou qualquer pacote de dados durante o intervalo entre a edição do penúltimo report e a edição do report atual [15].

Os pacotes RTCP contém informações importantes para a monitoração da entrega dos pacotes de áudio, tais como: jitter entre chegadas de pacotes, número de pacotes perdidos, número total de pacotes e octetos transmitidos, e outros dados úteis para a diagnose, monitoração e correção de alguns tipos de condições de erro na rede. Por exemplo, um codificador adaptativo pode comutar para pacotes menores, de mais baixa qualidade, quando o atraso fim-a-fim (ou jitter) na rede incrementa ao ponto onde o valor excessivo do atraso é mais prejudicial à fidelidade do sinal de áudio que a transmissão em menor taxa de bit [7].

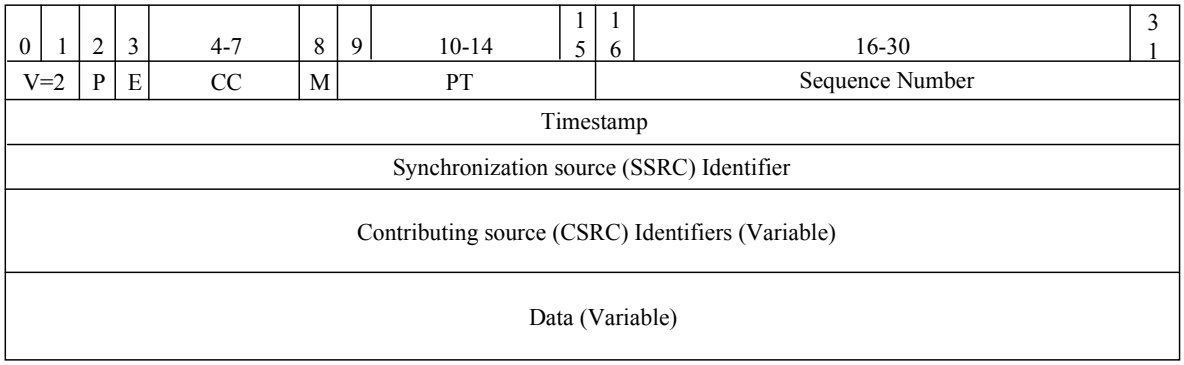
A Figura 23 mostra o quadro do protocolo RTP. As principais funções providas pelo RTP, através de campos do seu cabeçalho, são [7][15]:

IDENTIFICAÇÃO DE PAYLOAD: é essencial que os pacotes RTP entregues ao destino sejam decodificados segundo as mesmas regras utilizadas no processo de codificação. Para tal, o RTP identifica a informação que está sendo transportada associando um identificador de tipo de payload (campo PT) a cada pacote. Os tipos de payload, essencialmente codecs que podem ser usados para digitalização de áudio e vídeo, são identificados na RFC 1890.

TIMESTAMPING: o atraso variável entre a fonte e o destino em uma rede baseada em pacotes, como a Internet, faz com que os pacotes cheguem ao destino com intervalos entre pacotes irregulares. Este efeito é chamado de jitter, e pode resultar em perda significativa de qualidade quando o tráfego é de voz ou vídeo. O RTP auxilia na solução deste problema incluindo em seu cabeçalho um campo de 32 bits denominado Timestamp. O conteúdo do Timestamp reflete o instante de amostragem do primeiro octeto contido no pacote RTP. O valor associado ao primeiro pacote de um fluxo de pacotes é escolhido aleatoriamente. Para os pacotes subsequentes, o valor do Timestamp é incrementado de forma linear de acordo com o número de "ticks de clock" que ocorreram desde o último pacote.

A informação do campo Timestamp pode ser utilizada pelo Dejitter Buffer (veja item 2.1 do capítulo 3) para eliminar (ou ao menos amenizar) o jitter na rede.

NUMERAÇÃO SEQUENCIAL: as características de redes datagrama, como a Internet, não garantem a chegada em ordem dos pacotes no destino. De modo a permitir a reordenação dos pacotes, o RTP associa, através do campo Sequence Number, um número de seqüência a cada pacote enviado. Este número de seqüência pode ser utilizado também para detectar a perda de pacotes na rede. Embora não se faça, usualmente, retransmissões de pacotes perdidos em redes transportando tráfego em tempo real, a informação de perda de pacote pode ser útil no processo de decodificação. Por exemplo, se o pacote N foi perdido, o decodificador pode optar por substituí-lo pelo pacote N-1.



Where:

CC Contributor count
E Extension
M Marker
P Padding
PT Payload Type
V Version

Figura 23 – Quadro RTP.

CAPÍTULO 03 – QUALIDADE DE SERVIÇO

Embora exista uma corrente que defenda a idéia de que os usuários estão dispostos a trocar preço por qualidade, acreditamos que, para a consolidação da tecnologia de telefonia IP é necessário que o sistema seja capaz de oferecer uma qualidade no mínimo igual à hoje oferecida pela RPT. Esta crença se baseia no fato de que as estruturas tarifárias dos dois tipos de rede (Internet e Telefonia) tendem a sofrer alterações, com a tarifação da Internet deixando de ser do tipo "Flat Rate", apenas com tarifação local, e a tarifação da RPT deixando, à medida em que as operadoras implantarem seus backbones baseados em redes de pacotes (com tecnologia ATM ou mesmo IP), de ser tão dependente da distância como é hoje.

A qualidade de serviço pode ser definida como a "habilidade da rede para garantir e manter certos níveis de desempenho para cada aplicação de acordo com as necessidades específicas de cada usuário" [7].

Embora o conceito de QoS usualmente se refira à fidelidade do sinal de voz recebido, ele também pode se aplicar a outros aspectos, tais como: disponibilidade da rede, probabilidade de bloqueio, existência de serviços especiais (conferência, identificação do usuário chamador, etc), escalabilidade e penetração. Neste trabalho iremos abordar a questão da qualidade apenas no que diz respeito à fidelidade do sinal recebido, ficando os demais aspectos a serem abordados em trabalhos futuros.

1. FATORES QUE INFLUENCIAM A QUALIDADE DO SINAL DE VOZ

A qualidade de reprodução de voz na rede telefônica é fundamentalmente subjetiva, embora medidas padrões tenham sido desenvolvidas pelo ITU. Para a transmissão de voz sobre

redes de pacotes existem quatro fatores principais que impactam a qualidade do serviço: largura de faixa, atraso (fim-a-fim) de pacote, jitter de atraso e perda de pacotes.

1.1. LARGURA DE FAIXA

A largura de faixa mínima necessária para a transmissão do sinal de voz é função da técnica de codificação utilizada. A largura de faixa disponível na rede e o mecanismo de compartilhamento desta largura de faixa entre as diversas aplicações tem influência direta no atraso sofrido pelo pacote e consequentemente na qualidade de serviço resultante.

1.2. ATRASO DE PACOTE

O atraso de pacote é formalmente definido como a diferença de tempo, em segundos, entre o instante em que o terminal chamador envia o primeiro bit do pacote e o instante que o terminal chamado recebe este bit. Seu comportamento é aleatório em função da carga na rede.

Três problemas principais advêm deste atraso: o eco, a sobreposição do locutor, e a variação no intervalo entre chegadas de pacotes no receptor (jitter), devido ao comportamento aleatório do atraso.

1.2.1. ECO

Nas redes de telefonia tradicionais o eco normalmente é causado por um descasamento de impedância nas híbridas utilizadas para conversão dos 4 fios do nó de comutação para os 2 fios do cabo telefônico que vai à casa do assinante (loop local). Este descasamento de impedância faz com que uma parte do sinal transmitido seja refletido de volta à origem, fazendo com que o usuário escute sua própria fala algum tempo depois da transmissão [4].

Para o usuário, ouvir sua própria voz no receptor enquanto está falando é normal e fornece segurança quanto ao que está sendo transmitido. No entanto, ouvir a própria voz com mais de 25 [ms] de atraso passa a ser percebido como eco e pode causar desconforto para o usuário. Assim, se o atraso fim-a-fim for superior a 25 [ms] o sistema deve prover mecanismos de cancelamento de eco para minimizar seus efeitos.

1.2.2. SOBREPOSIÇÃO DO LOCUTOR

O crescimento demasiado do atraso fim-a-fim leva a uma perda de qualidade pelo ponto de vista do usuário, pois a demora na escuta do sinal de voz do assinante "A" pode levar o assinante "B" a iniciar sua fala, causando uma sobreposição dos locutores. Pelo ponto de vista do usuário o sistema passa a se assemelhar mais a um sistema half-duplex do que a uma conversação.

O limite de atraso fim-a-fim, a partir do qual a queda de qualidade é percebida, varia muito de acordo com o usuário. Resultados de testes de qualidade de voz executados pelo ITU-T, e publicados na recomendação G.114, são mostrados na Figura 24. Percebe-se da Figura que, mesmo na completa ausência de eco, mais de 10% dos usuários experimentam dificuldades para manter a conversação para atrasos (one-way) de 400 [ms] [5].

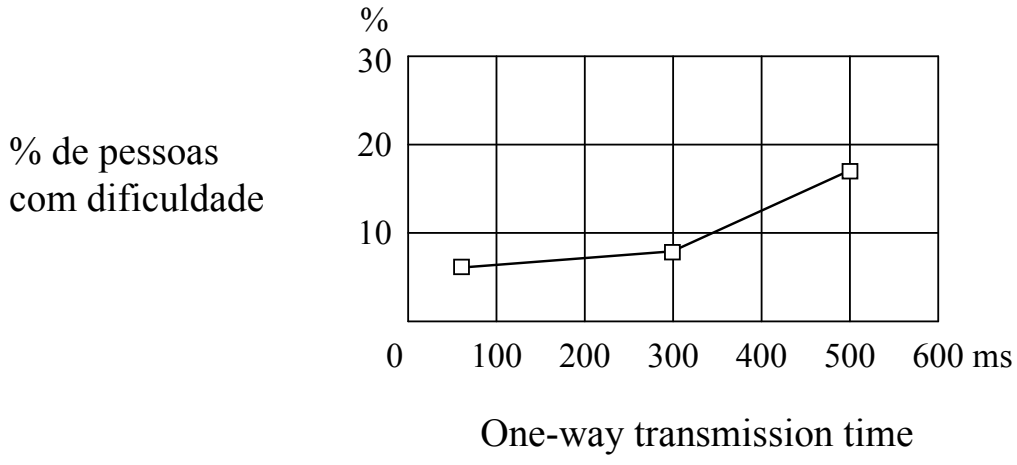


Figura 24 – Efeito do atraso na dificuldade de conversação com cancelador de eco.

Para orientar os operadores de rede e os fabricantes de equipamentos no controle do atraso na rede, o ITU-T aprovou em 1996 a recomendação G.114, que estabelece o limite máximo de atraso fim-a-fim em 400 [ms]. Vale ressaltar, que este valor é um limite máximo, após o qual a qualidade é considerada inaceitável, estabelecendo-se o limite de conforto em 200 ms, ou seja, atrasos menores que 200 [ms] são considerados aceitáveis, atrasos superiores a 400 [ms] são considerados inaceitáveis, e atrasos entre 200 [ms] e 400 [ms] definem uma área de qualidade marginal, que pode ser aceitável para algumas aplicações de voz e inaceitável para outras. [5]

1.2.3. JITTER DE ATRASO

O jitter é a variação no intervalo entre chegadas de pacotes introduzido pelo comportamento aleatório do atraso na rede.

Um método típico de contornar o problema do jitter é adicionar um buffer na recepção que acrescenta um atraso determinado, de tal forma que o atraso total experimentado pelo pacote, incluindo o atraso extra gerado pelo buffer seja igual ao máximo atraso possível na rede. Este método é razoável no ambiente de redes locais ou Intranets corporativas onde o máximo atraso é pequeno. Em redes WAN onde o atraso máximo pode assumir valores inaceitavelmente elevados, este método não é aplicável. A escolha do máximo atraso a ser introduzido pelo buffer na recepção é então uma solução de compromisso entre o atraso total admissível e a taxa de perda de pacotes. [5]

1.2.4. COMPONENTES DO ATRASO DE PACOTE

O atraso de pacote possui diversas componentes, umas de natureza fixa e outras de natureza variável, que são brevemente descritas a seguir.

ATRASO DE PROPAGAÇÃO. O atraso de propagação está relacionado com o tempo que o sinal leva para se propagar no meio de transmissão (par metálico, fibra óptica, espaço livre). Este atraso é fixo e depende do tipo do meio e da distância percorrida pelo sinal. Por

exemplo, para uma transmissão via rádio, o atraso de propagação é de 3.33 [μs/km]. Este atraso só é considerável em redes onde a distância percorrida é muito elevada, como por exemplo em redes de comunicação via satélite geoestacionário, onde a distância da ordem de 36.000 [km] resulta em um atraso de 120 [ms].

ATRASO DE CODIFICAÇÃO/DECODIFICAÇÃO. O atraso de codificação é fixo e é composto basicamente de três parcelas: tamanho do quadro e "lookahead delay", que juntos compõem o chamado atraso algorítmico, e o atraso de processamento.

Os algoritmos geralmente utilizados na codificação de voz processam quadros de tamanho fixo contendo amostras do sinal de voz. O tamanho deste quadro, em segundos, define a janela de codificação e corresponde ao atraso mínimo de codificação. O tamanho desta janela resulta de um compromisso entre a redução do atraso algorítmico (janela menor) e uma maior taxa de compressão (janela maior). Em muitos casos o algoritmo analisa, além do quadro corrente, informações contidas no quadro seguinte. Esta técnica permite que o codificador utilize a correlação entre quadros adjacentes no processo de codificação com o intuito de diminuir a taxa de transmissão (aumentar a taxa de compressão). O "lookahead delay" é o comprimento do frame seguinte que o codificador utiliza neste processo. O atraso de processamento corresponde ao tempo requerido para executar o algoritmo de codificação para um dado quadro. O tamanho do quadro e o "lookahead delay" independem da forma de implementação do algoritmo, mas o tempo de processamento pode ser minimizado com a utilização de processadores (usualmente processadores digitais de sinais) mais rápidos. Os atrasos de decodificação são da ordem da metade dos atrasos de codificação. [3][4][6]

A Tabela 1 mostra os valores destes atrasos para três tipos de codificadores comuns para transmissão de voz sobre redes de pacotes [3].

Codec	G 723.1	G 729	G 729 A
Taxa de bits	5.3 / 6.4 kbps	8 kbps	8 kbps
Tamanho do quadro	30 ms	10 ms	10 ms
Atraso de processamento	30 ms	10 ms	10 ms
Lookahead delay	7.5 ms	5 ms	5 ms
Comprimento do quadro	20/24 bytes	10 bytes	10 bytes
DSP MIPS	16	20	10.5
RAM	2200	3000	2000

Tabela 1 – Algumas características de alguns Codecs aplicáveis à VoIP.

Na Tabela 1, o comprimento do quadro corresponde ao número de bytes em um quadro codificado (excluindo o cabeçalho); o parâmetro DSP MIPS indica a mínima velocidade necessária ao processador DSP para implementar o algoritmo de codificação; e o parâmetro RAM especifica a memória mínima, em palavras de 16 bits, requerida.

ATRASO DE EMPACOTAMENTO. É o tempo necessário para se gerar um número suficiente de quadros de voz para preencher o payload do pacote IP (ou do quadro Frame Relay ou da célula ATM). Para se evitar valores excessivos para o atraso de empacotamento pode-se enviar pacotes parcialmente carregados. Deve-se notar, no entanto, que isto reduz a eficiência (overhead / informação de voz) do sistema. O atraso de empacotamento pode, dependendo da situação, absorver ou se confundir com os atrasos de codificação.

ATRASO NOS NÓS DA REDE. O principal atraso que os pacotes sofrem dentro da rede é o atraso de enfileiramento nos roteadores (ou comutadores de pacotes). Este atraso é variável e depende do tempo médio de serviço de um pacote, que é composto pelo tempo necessário para o roteador tomar a decisão de roteamento mais o tempo de transferência do pacote do buffer de entrada para o buffer de saída (tempo de chaveamento) mais o tempo de transmissão do pacote no enlace de saída, e do fator de utilização do enlace de saída

associado (carga). O atraso de enfileiramento é o principal responsável pela aleatoriedade do comportamento do atraso total experimentado pelo pacote, podendo assumir valores inaceitáveis em situações de congestionamento na rede.

ATRASO DEVIDO AO DEJITTER BUFFER. A variação do atraso (jitter) é introduzida no sistema basicamente pelo comportamento aleatório do tempo de enfileiramento dos pacotes nos roteadores, e é um fator de degradação da qualidade do sinal. A compensação desta variação é feita através de buffers (dejitter buffers) que armazenam os pacotes que chegam com atraso variável para entregá-los ao decodificador com atraso constante. No entanto, se a variação do atraso for muito elevada, o atraso adicional necessário para compensar a variação pode resultar em um atraso total fim-a-fim inaceitável. Por esta razão, defini-se um valor máximo de atraso admissível para o dejitter buffer.

1.3. PERDA DE PACOTES

As redes IP não garantem a entrega dos pacotes. Devido aos fortes requisitos de atraso impostos pelas aplicações interativas em tempo real, protocolos de transporte confiáveis, como o TCP, não podem ser utilizados. A perda de pacotes é portanto inevitável, e pode influenciar significativamente a qualidade do serviço de voz sobre IP. A perda de pacotes é definida como a percentagem de pacotes transmitidos pelo host de origem (A) que não chegam ao host de destino (B), e é devida, principalmente, a:

- Imperfeições na transmissão: problemas físicos nos equipamentos de transmissão podem resultar em perda de pacotes.
- Atraso excessivo: se o parâmetro “Time-to-Live” (TTL) definido para o pacote for excedido, o pacote é descartado pela rede.
- Congestionamento: o aumento em excesso do tráfego na rede pode resultar no overflow dos buffers dos roteadores, resultando na perda de pacotes. Além disto, se o protocolo RED (Random Early Detection) é utilizado (veja item 2.4.1), o roteador irá descartar aleatoriamente pacotes

- Overflow do buffer de dejitter: se o jitter na rede for excessivo, poderá ocorrer um overflow no buffer utilizado para compensar o jitter, com consequente perda de pacotes.

As perdas de pacotes de voz serão percebidas como "gaps" na conversação, degradando a qualidade do serviço. Contudo, uma certa percentagem de perda de pacotes, entre 3 e 5% [5], pode ser compensada por esquemas de recuperação dos Codecs. Por exemplo, o G.723.1 interpola um quadro perdido simulando as características vocais do quadro anterior e reduzindo lentamente o sinal [3]. A taxa máxima tolerável de perda de pacotes é usualmente fixada em 10% [1][3][5]. A Figura 25 mostra os limites aceitáveis para atraso e percentagem de perda de pacotes para VoIP.

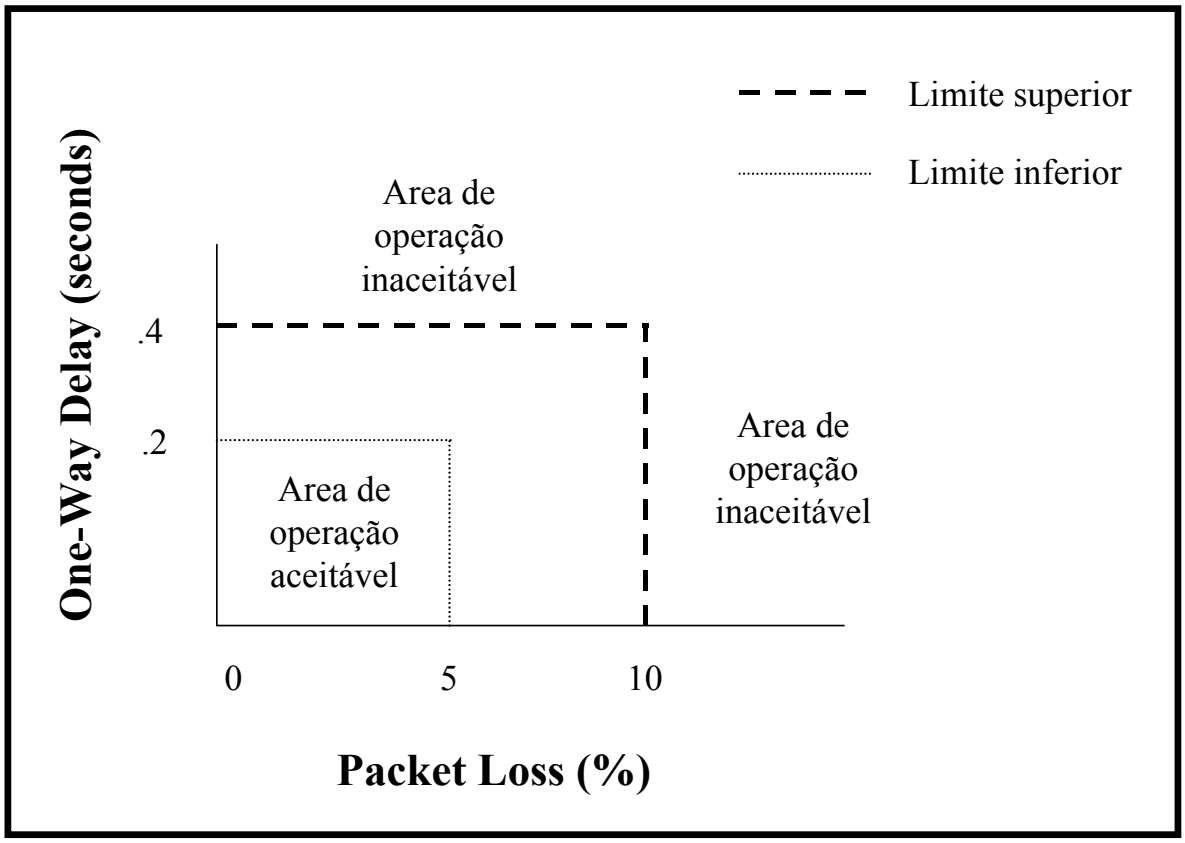


Figura 25 – Limites aceitáveis de atraso e perda de pacotes para VoIP.

Embora a perda de pacotes isolados, dentro de determinados limites, seja de menor conseqüência devido aos esquemas de recuperação utilizados pelos Codecs, perdas de pacotes em bursts, como as produzidas pela Internet, podem causar grande degradação no sinal recebido. Técnicas de correção automática de erros no receptor (FEC – Forward Error Correction) têm sido propostas para contornar perdas de pacotes em bursts de tamanho reduzido, mas ainda precisam ser melhor investigadas [3]. A desvantagem de se utilizar técnicas de FEC é que para recuperar o pacote n (onde n é o número de seqüência do pacote), é necessário que já se tenha recebido ao menos o pacote n+1. Assim, o esquema de FEC introduz um atraso adicional no mínimo equivalente ao tempo de um quadro, além do atraso de processamento para o processo de codificação e decodificação. Estes atrasos adicionais podem fazer com que o quadro seja recuperado tarde demais, ou seja, o atraso total pode exceder o limite aceitável, resultando no descarte do pacote [3].

Um esquema alternativo de recuperação de perda de pacotes em bursts através de FEC envolve a transmissão de cópias dos k quadros anteriores no pacote contendo o quadro n. Por exemplo, se k = 2, o pacote n conterá os quadros n, n - 1 e n – 2. Se o pacote n – 1 é perdido, ele ainda pode ser reconstruído do pacote n ou do pacote n + 1. Como outros esquemas de FEC, este também será mais efetivo em cenários onde o buffer do receptor tem o comprimento de vários quadros [3].

2. MECANISMOS PARA PROVER QUALIDADE DE SERVIÇO EM VoIP

Para se alcançar um nível de QoS adequado para tráfego de voz sobre uma rede IP pode-se adotar um conjunto de medidas no sentido de: garantir a banda necessária para a transmissão dos pacotes de voz (ex.: protocolos de reserva de recursos), minimizar os atrasos sofridos pelos pacotes na rede e torná-los o mais constante possível (ex.: utilizar mecanismos para priorização dos pacotes de voz, utilizar técnicas de roteamento que privilegiem as rotas de menor atraso, utilizar mecanismos mais eficientes para o encaminhamento dos pacotes nos roteadores), e eliminar ou minimizar o jitter de atraso sofrido pelos pacotes (ex. utilizar dejitter buffer).

Neste item serão analisadas as principais técnicas para se prover QoS em redes IP transportando tráfego de voz. Em geral, estas técnicas estão associadas às seguintes funções [16]:

- Classificação do tráfego, de modo a poder diferenciar um tipo de outro.
- Priorização dos pacotes de tráfego de voz.
- Policiamento e conformação do tráfego.
- Gerenciamento de congestionamento.
- Fragmentação de grandes pacotes de dados e entrelaçamento destes pacotes com os pacotes de voz.
- Garantia de largura de faixa para o tráfego de voz.
- Compensação, no receptor, da variação do atraso na rede.

2.1. DEJITTER BUFFER

Os efeitos do jitter ou variações de atraso em VoIP podem ser eliminados ou reduzidos pela utilização de buffers na recepção denominados de dejitter buffer. O dejitter buffer armazena temporariamente os pacotes de voz recebidos, introduzindo um atraso adicional antes de enviá-los ao receptor, de modo a igualar o atraso total sofrido por todos os pacotes. Por exemplo, a Figura 26 ilustra um sistema onde o dejitter buffer introduz atrasos adicionais de modo que todo pacote recebido tenha um atraso total de 120 [ms]. O pacote 1, que sofreu um atraso de 100 [ms] na rede, sofre um atraso adicional de 20 [ms], e o pacote 2, que sofreu um atraso de 90 [ms] na rede, sofre um atraso adicional de 30 [ms].

A escolha do atraso para o dejitter buffer é crítica. Para que o dejitter buffer seja capaz de eliminar completamente o efeito do jitter, sua janela de atraso deve ser igual à diferença entre o máximo e mínimo atraso na rede. Por exemplo, se o mínimo atraso na rede é de 70 [ms] e o máximo atraso é de 130 [ms], com um atraso nominal de 100 [ms], um dejitter buffer com janela de atraso de 60 [ms] (os atrasos introduzidos pelo buffer são entre 0 e 60 [ms]) é capaz de eliminar completamente o jitter, fazendo com que todos os pacotes recebidos tenham um atrasos idênticos de 130 [ms]. Este princípio está ilustrado na Figura

27, que mostra um exemplo de distribuição estatística dos atrasos na rede e o atraso total sofrido por todos os pacotes após o dejitter buffer [7].

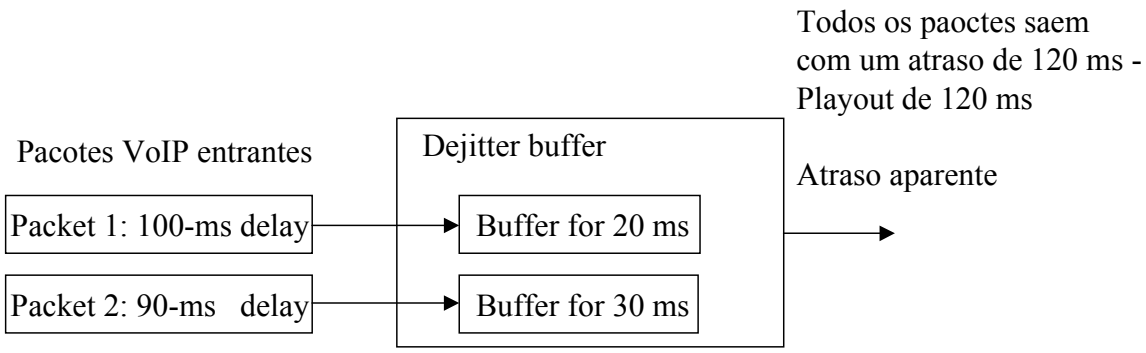


Figura 26 – Operação do Dejitter Buffer.

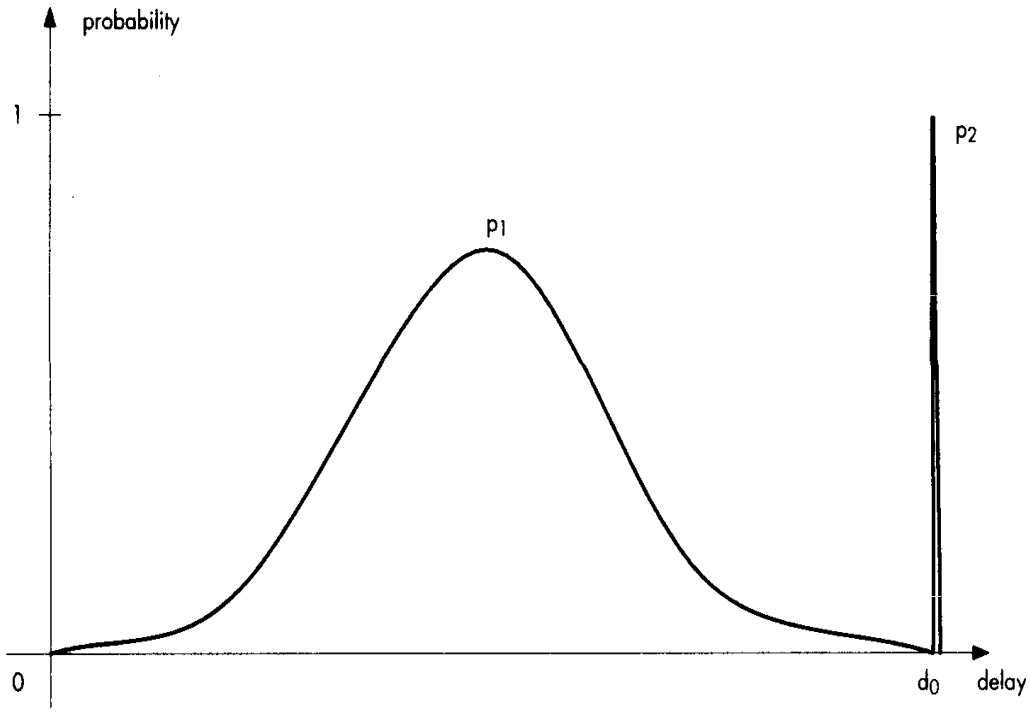


Figura 27 – Exemplo do comportamento estatístico do atraso na rede.

Se a variação do atraso na rede for muito grande, caso da Internet por exemplo, a tentativa de se eliminar o jitter aumentando-se a janela de tempo do dejitter buffer leva a pacotes sem jitter mas com atrasos totais inaceitavelmente altos, e portanto inúteis. Neste caso uma solução de compromisso deve ser adotada, e um valor aceitável para a janela de tempo do dejitter buffer fixado. Esta solução no entanto pode levar à perda de pacotes causada por atrasos excessivos na rede ou por overflow do dejitter buffer. Por exemplo, considere a seguinte situação: uma rede tem atraso nominal de 150 [ms] e utiliza um dejitter buffer com janela de atraso de 100 [ms], ou seja, o buffer atrasa os pacotes entre 0 e 100 [ms]. Admitindo-se que a distribuição do atraso na rede é simétrica em relação à média, este sistema é capaz de compensar a variação de atrasos entre 100 e 200 [ms]. Pacotes que cheguem ao dejitter buffer com atraso superior a 200 [ms] (denominados pacotes muito atrasados) não poderão ter o jitter compensado e serão descartados; por outro lado, pacotes que cheguem ao dejitter buffer com atraso inferior a 100 [ms] poderão causar o overflow do buffer e consequentemente a perda de pacotes.

Para tornar a operação do sistema mais eficiente é desejável que o tamanho da janela de tempo do dejitter buffer seja adaptativo. Ou seja, a janela de tempo do buffer aumenta (até um certo limite) ou diminui acompanhando a variação do jitter na rede. Para entender melhor o benefício desta facilidade seja o seguinte exemplo: uma rede possui um atraso nominal de 150 [ms]. Em um dado momento o atraso na rede se comporta de tal forma que o atraso mínimo é de 50 [ms] e o atraso máximo é de 500 [ms]. Para compensar o jitter a janela de tempo do dejitter buffer deveria ser de 450 [ms] (atrasos entre 0 e 450 [ms]). No entanto, como vimos anteriormente, atrasos superiores a 400 [ms] são considerados inaceitáveis, e a janela do dejitter buffer deve ser configurada para 350 [ms] (atrasos entre 0 e 350 [ms]), resultando em um atraso total de cada pacote igual a 400 [ms]. Pacotes que chegarem com atraso superior a 400 [ms] serão descartados.

Vamos admitir agora que as condições de operação da rede do exemplo anterior se alteraram e os valores do atraso mínimo e máximo se alteraram para 75 e 225 [ms] respectivamente. Se a operação do dejitter buffer for mantida, o atraso total sofrido por cada pacote continuará sendo de 400 [ms]. Este valor, embora seja definido como o

máximo tolerável, é bastante superior ao máximo aceitável para uma operação com boa qualidade, que é de 200 [ms]. Se o dejitter buffer é capaz de perceber esta alteração no comportamento da rede, ele pode alterar o tamanho de sua janela de atraso para 150 [ms], resultando em pacotes sem jitter com atraso total igual a 225 [ms], portanto mais próximo do limite aceitável de 200 [ms]. Outra opção, é estabelecer o tamanho da janela em 125 [ms], o que resultaria em pacotes com atraso total máximo de 200 [ms], portanto dentro do limite aceitável, e no descarte de pacotes que tivessem chegado ao dejitter buffer com atraso superior a 200 [ms].

A característica de adaptação do dejitter buffer é conseguida basicamente através da medição e comparação contínua do atraso dos pacotes que chegam (atraso instantâneo) com uma referência (atraso de referência). Esta referência é continuamente atualizada com base em uma média ponderada do atraso dos pacotes recebidos em um determinado período de tempo, com maior peso para os pacotes recebidos mais recentemente. Com isso consegue-se um ajuste dinâmico do tamanho da janela de tempo do dejitter buffer ao longo do tempo, de modo que o atraso instantâneo nunca se afaste muito do atraso de referência [4].

Se o atraso instantâneo oscila pouco, isso corresponde a um jitter reduzido, e o dejitter buffer é ajustado para uma pequena janela de tempo, de modo a não aumentar o atraso global fim-a-fim.

Se o atraso instantâneo começa a oscilar muito, tem-se um jitter elevado e o dejitter buffer assume uma janela de tempo maior para evitar a degradação da qualidade, no entanto o atraso global fica majorado.

Em geral, a escolha do tamanho da janela é uma solução de compromisso entre atraso do pacote e taxa de perda de pacotes. Janelas maiores resultam em maiores atrasos e menores perdas de pacotes, enquanto janelas menores resultam em atrasos menores e maiores perdas de pacotes.

A Figura 28 ilustra a interação entre atraso e perda de pacotes para uma dada distribuição de atraso na rede. A linha vertical representa o atraso total dos pacotes após o dejitter buffer (playout point). A taxa de perda de pacotes é representada pela área sob a curva à direita da linha vertical. Quando nós movemos a linha para a esquerda, o atraso total decrementa mas a taxa de perda de pacotes aumenta. Quando nós movemos a linha para a direita, as perdas se reduzem à custa de um maior atraso [3].

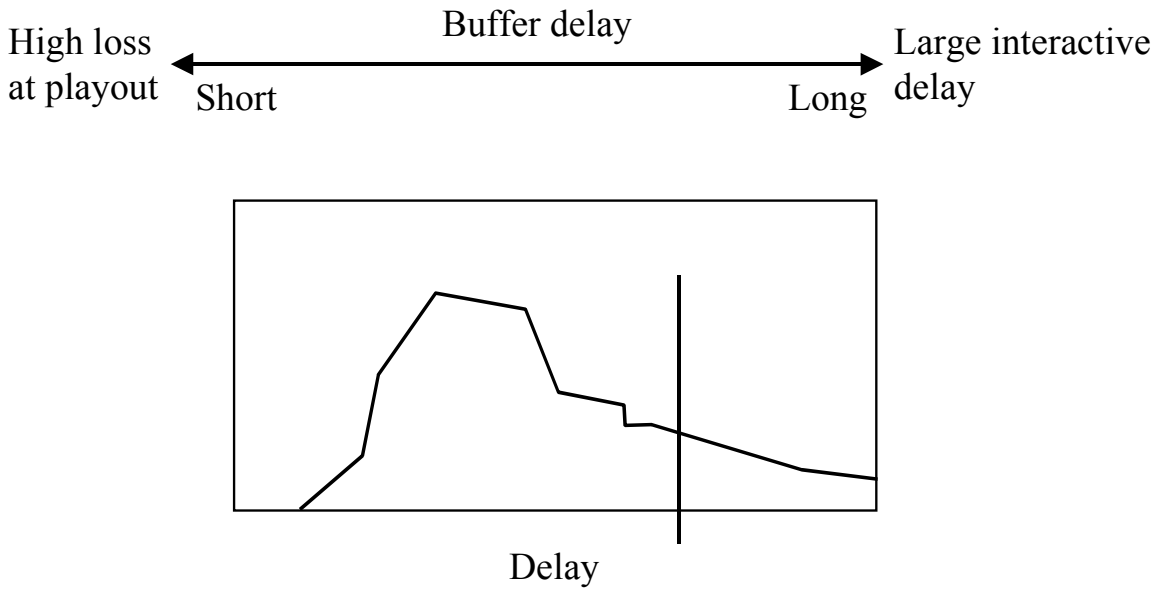


Figura 28 – Interação entre atraso e perda de pacotes.

A Figura 29 ilustra a relação do atraso e taxa de perda de pacotes com a qualidade de serviço na rede. Quatro níveis de QoS são definidos na figura: Toll quality (desejável), Good quality, Potentially useful quality e Poor quality (inaceitável) [3].

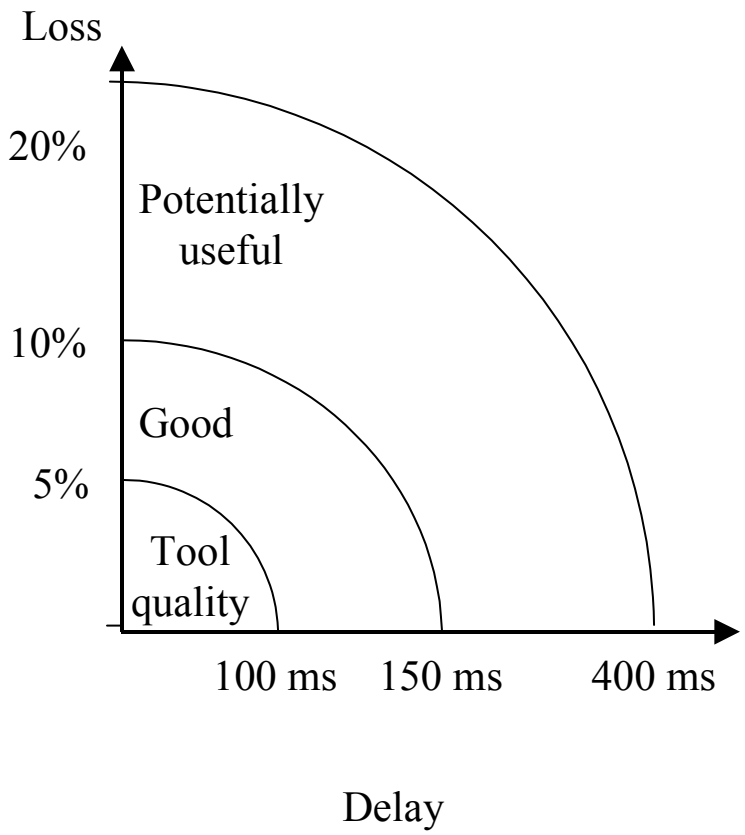


Figura 29 – Relação entre atraso, perda de pacotes e QoS.

2.2. CLASSIFICAÇÃO OU IDENTIFICAÇÃO DO TRÁFEGO

Um dos mecanismos para se alcançar o nível de QoS adequado aos diversos tipos de tráfego em uma rede de pacotes é diferenciar o tratamento que os nós da rede dispensam a cada tipo de tráfego. A classificação dos pacotes, que corresponde à identificação do tráfego transportado por cada pacote, é portanto uma das técnicas fundamentais para se obter QoS em uma rede de pacotes transportando voz.

A classificação do tráfego em si não é uma ferramenta direta para se obter QoS, mas sim uma técnica auxiliar que permitirá a implementação de outras técnicas, como por exemplo políticas de priorização da transmissão ou descarte de determinados tipos de pacote, em função do tráfego transportado.

A classificação do tráfego pode ser feita pacote a pacote (analisando a característica do tráfego de cada pacote) ou sessão a sessão (quando o transmissor negocia uma classificação fim a fim antes de transmitir). A política de classificação dos pacotes é definida pelo operador da rede, e pode se basear em diversos critérios, tais como: tipo de tráfego contido no pacote, endereço da porta física, endereço MAC, endereço IP de fonte ou destino, porta de aplicação, etc.

A classificação dos pacotes pode ser feita pelas fontes de tráfego externas, pelos dispositivos de borda, ou pelos dispositivos de backbone da rede. Quando a classificação é feita pela fonte (ou por uma outra rede à downstream), a rede pode aceitar a classificação recebida ou reclassificar o tráfego de acordo com a sua própria política. Os critérios para a classificação de tráfego podem ser tão amplos quanto "tráfego destinado à rede X" ou tão estreitos quanto "tráfego do fluxo Y". No backbone da rede a granularidade da classificação tende a ser menor, em função do grande número de fluxos existentes.

A Figura 30 mostra um exemplo de uma rede LAN interligada a uma rede WAN. Tipicamente, o tráfego é classificado na rede LAN antes de ser enviado à rede WAN. Os dispositivos da WAN utilizam a classificação, informada através dos bits de PRECEDENCE do campo ToS do cabeçalho IP por exemplo, para determinar os requisitos de serviço para o tráfego. Os dispositivos da WAN podem limitar a banda disponível para o tráfego, dar prioridade, ou mesmo mudar a classificação do tráfego [17].

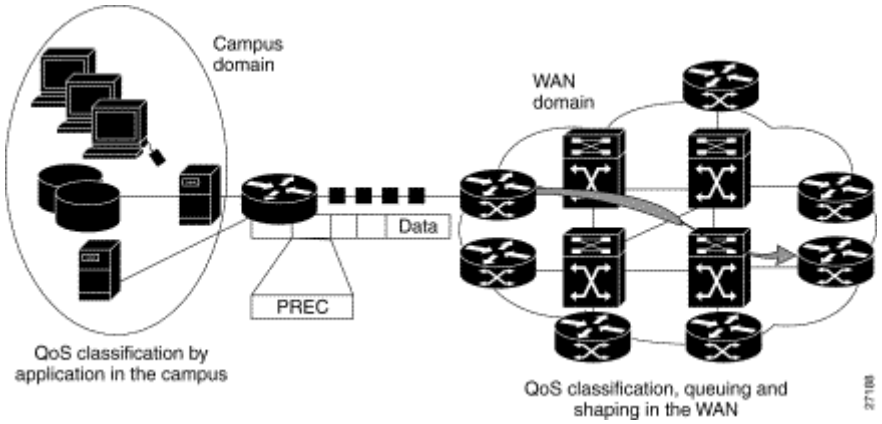


Figura 30 – QoS em redes LAN e WAN.

Os métodos de marcar os pacotes com sua classificação incluem a utilização de cabeçalhos das camadas 2, 3 ou 4, ou mesmo definindo campos especiais dentro do payload do pacote. A título de ilustração apresentaremos a seguir como a classificação pode ser feita utilizando-se: o campo ToS do cabeçalho IPv4, o campo ToS na arquitetura de serviços diferenciados, e o cabeçalho MAC estendido definido no padrão IEEE 801.D.

IP PRECEDENCE: Os três primeiros bits do campo ToS do cabeçalho IPv4, denominados bits de Precedência, definem a prioridade relativa do datagrama, estabelecendo até seis classes de serviço distintas. Os quatro bits seguintes, denominados Type of Service, consistem de 4 flags para vários tipos de serviços, e o último bit não é utilizado. A Figura 31 ilustra o campo ToS do cabeçalho IP [18].

A RFC 791 define o significado dos oito possíveis valores dos bits de Precedência, conforme indicado na Tabela 2 [18] [19].

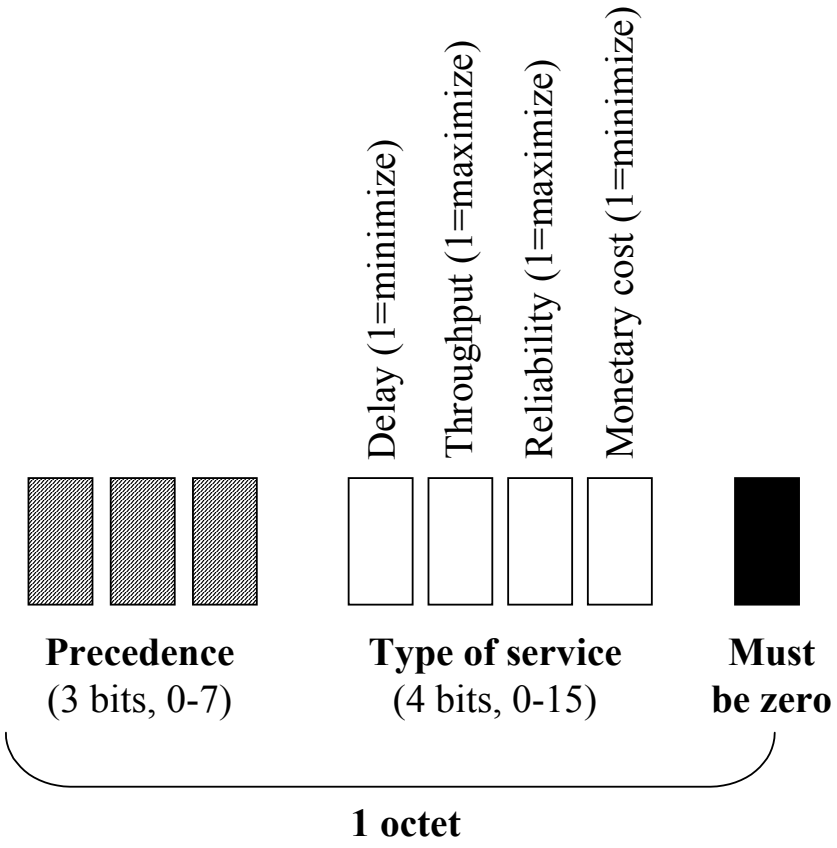


Figura 31 – Campo ToS do cabeçalho IP.

Valor dos bits de Precedência	Tipo de tráfego
000 – 0	Routine
001 – 1	Priority
010 – 2	Immediate
011 – 3	Flash
100 – 4	Flash Override
101 – 5	Critical
110 – 6	Internetwork control
111 – 7	Network control

Tabela 2 – Valores e significados dos bits de Precedência.

Embora a RFC 791 defina determinados tipos de tráfego, outras definições proprietárias pode ser feitas. Os valores 6 e 7 mostrados na Tabela 2 são reservados para informações de controle da rede, tais como atualizações de roteamento [19].

Não há nenhuma definição de como o roteador deve se comportar quando recebe um pacote com uma das prioridades mostradas na Tabela 2. A RFC 791 descreve os bits de Precedência como "uma medida de importância" do pacote [18].

De modo que cada elemento subsequente da rede possa prover o serviço com base na política estabelecida, a Precedência do pacote é definida o mais próximo possível da borda da rede. Podemos ver a definição da Precedência como uma função de borda que permitirá aos dispositivos do núcleo, ou backbone, da rede executarem funções visando obter QoS. Por exemplo, os roteadores no backbone da rede podem utilizar os bits de precedência para determinar a ordem de transmissão ou a probabilidade de descarte dos pacotes [19].

Além dos bits de precedência, os bits Type of Service também podem ser utilizados para definir o tratamento a ser dispensado ao pacote. Os bits de Precedência usualmente guiam o comportamento por hop (descarte, enfileiramento, prioridade e transmissão), enquanto os bits Type of Service guiam o comportamento inter-rede (seleção de rota, por exemplo) [18].

ARQUITETURA DE SERVIÇOS DIFERENCIADOS: A Arquitetura de Serviços Diferenciados irá redefinir o uso dos 8 bits do campo ToS do cabeçalho IP, para indicar aos dispositivos da rede que pacotes devem ser manuseados de forma especial. Uma das propostas existentes está apresentada na Figura 32, três bits definem oito classes de tráfego, e outros três definem a prioridade de um pacote dentro de uma classe [18].

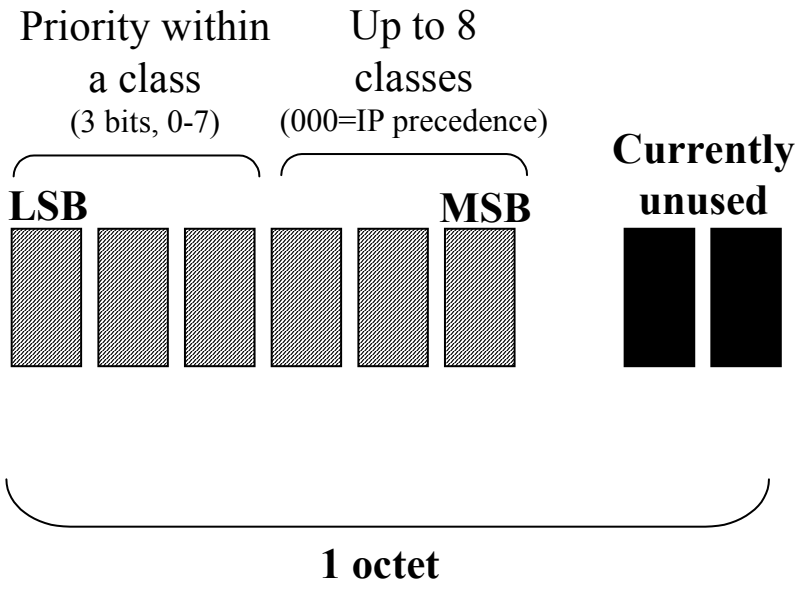


Figura 32 – Significado dos bits do campo ToS na Arquitetura DiffServ.

CABEÇALHO MAC IEEE 801.D: O padrão IEEE 802.1.D, que incluí o 802.1.p e Q, define uma extensão de 32 bits ao cabeçalho MAC das redes Ethernet e Token Ring. Doze bits deste espaço são utilizados como rótulos para redes VLAN; contudo, três bits dentro do cabeçalho 802.1.Q (definidos no padrão 802.1.p) são utilizados para sinalização de classe de serviço na rede, permitindo que se estabeleçam oito níveis de prioridades para classificação de tráfego, mas sem informação de Tipo de Serviço para indicar, por exemplo, elegibilidade para descarte. O quadro MAC com o cabeçalho estendido é ilustrado na Figura 33, enquanto o significado dos oito níveis de prioridade são mostrados na Tabela 3 [18].

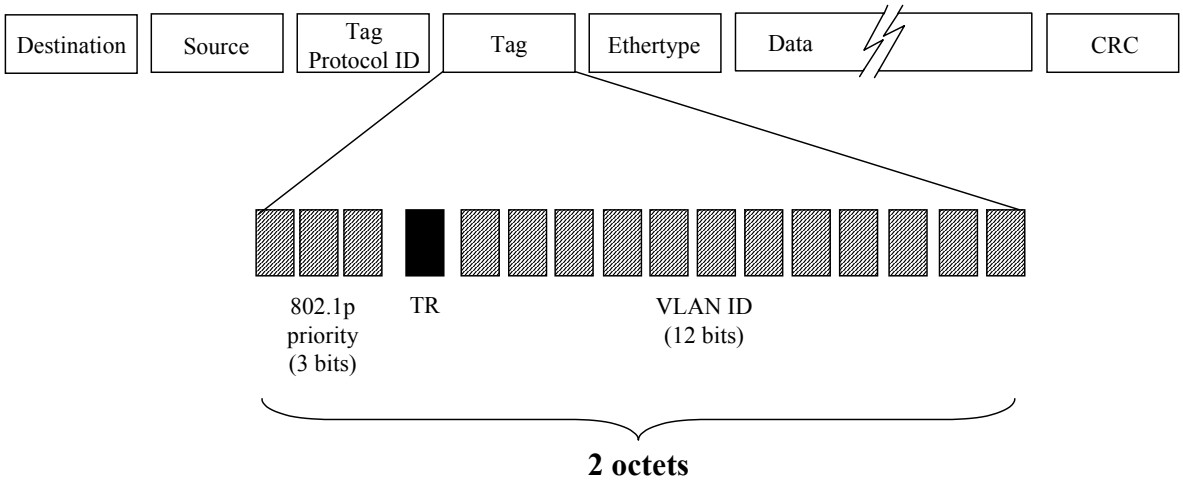


Figura 33 – Quadro MAC com cabeçalho estendido IEEE 802.1.D.

Valor	Nome	Exemplos	Características
7	Controle da rede	RIP, OSPF, BGP4	Crítico para a operação da rede
6	Voz	NetMeeting audio	Sensível a latência e jitter; largura de faixa pequena
5	Vídeo	PictureTel, Indeo	Grande largura de faixa; sensível a jitter.
4	Carga controlada	SNA Transactions	Tempo de resposta previsível, aplicações sensíveis a latência
3	Esforço excelente	SAP, SQL	Tráfego crítico (negócios) que toleram atrasos.
2	Melhor esforço	Melhor esforço	Melhor esforço
1	<default>	<default>	<default>
0	Background	FTP backups	Insensível a latência

Tabela 3 – Níveis de prioridade definidos no padrão IEEE 802.1.p.

2.3. - ENFILEIRAMENTO, PRIORIZAÇÃO E DISCIPLINA DE DESPACHO

De modo a absorver situações momentâneas de congestionamento na rede, onde a taxa de chegada de pacotes excede a capacidade do enlace de saída, os nós de uma rede de pacotes (ex: roteadores em uma rede IP) possuem buffers especiais para armazenamento temporário dos pacotes, denominados filas. A disciplina de despacho define a forma como o nó da rede irá servir os pacotes armazenados nas filas. Quando a rede transporta simultaneamente tráfego de voz e dados, deve-se associar níveis de prioridade distintos aos dois tipos de tráfego, com a disciplina de despacho priorizando o tráfego de voz, de modo a minimizar o atraso que estes pacotes sofrem em cada nó da rede.

Nos itens a seguir apresenta-se as principais disciplinas de despacho associadas a redes de pacotes, indicando sua aplicabilidade para a obtenção de QoS em redes VoIP.

2.3.1. FIRST-IN, FIRST-OUT - FIFO

Esta é a disciplina de despacho mais simples. Nenhum conceito de prioridade ou classe de tráfego é utilizado, com todos os pacotes sendo tratados igualmente. Existe uma única fila de saída, os pacotes recebidos são armazenados e enviados na mesma ordem em que chegaram.

Neste tipo de fila, fontes de tráfego mal comportadas podem consumir toda a largura de faixa disponível, tráfegos em rajada podem causar atrasos inaceitáveis em tráfegos sensíveis a atraso, e pacotes pertencentes a tráfegos de maior importância podem ser perdidos devido a overflow do buffer, causado possivelmente por tráfegos de menor importância.

Este tipo de disciplina de despacho não é, portanto, adequada para aplicações de VoIP.

2.3.2. PRIORITY QUEUEING – PQ

Nesta técnica existem filas distintas para diferentes classes de prioridades. Por exemplo, podemos ter quatro níveis de prioridade (alta, média, normal e baixa), com uma fila associada a cada nível, conforme ilustra a Figura 34.

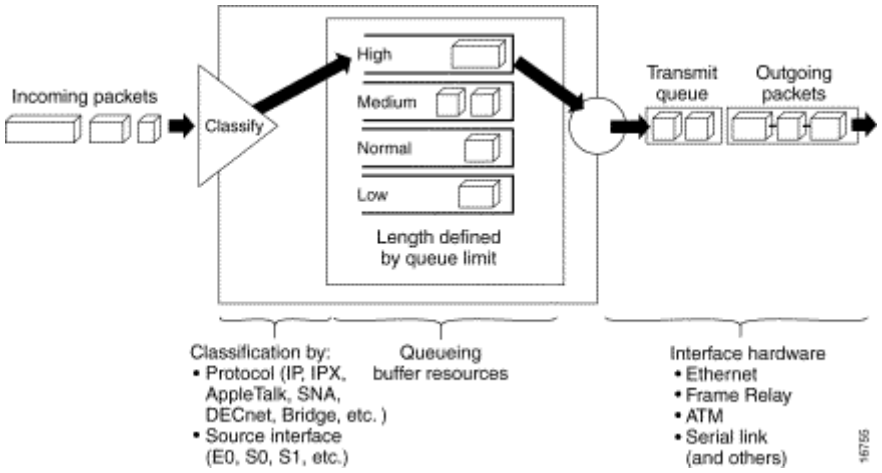


Figura 34 – Priority Queueing com quatro níveis de prioridade.

Os pacotes, uma vez classificados, são encaminhados para a fila com nível de prioridade correspondente. Durante a transmissão, o algoritmo de despacho dá tratamento preferencial absoluto à fila de maior prioridade, em detrimento das filas de menor prioridade. Ou seja, no momento da transmissão o algoritmo sempre busca um pacote na fila de alta prioridade; caso não haja pacote nesta fila, um pacote da fila de média prioridade é buscado, e assim sucessivamente até se chegar à fila de baixa prioridade.

Um volume de tráfego elevado de maior prioridade pode reter os tráfegos de menor prioridade por um tempo inaceitavelmente elevado; este fenômeno é conhecido como “starvation”. No pior caso, devido a um grande volume de tráfego de alta prioridade, por exemplo, o tráfego de baixa prioridade pode nunca ser transmitido. Para se evitar esta situação, pode-se utilizar ferramentas de formatação de tráfego ou CAR (Committed access rate), de modo a restringir a taxa de chegada de tráfego de alta prioridade [20].

A técnica Priority Queueing dá melhor resultado quando o tráfego de mais alta prioridade consome a menor quantidade de largura de faixa do canal, ou seja, possui menor volume [21].

2.3.3. CUSTOM QUEUEING – CQ

Nesta técnica tem-se uma fila para cada tipo de tráfego especificado. As filas são servidas de forma cíclica (round-robin), permitindo-se que se especifique o número de pacotes (ou bytes) a serem transmitidos de cada fila a cada ciclo de serviço. Desta forma, pode-se especificar a largura de faixa mínima do canal disponível para cada tipo de tráfego e, considerando a existência de pacotes para todos os tráfegos especificados, o valor aproximado do percentual da banda do canal utilizado por cada tipo de tráfego. A largura de faixa não utilizada por uma fila (por ausência de tráfego) é naturalmente distribuída para as demais, pelo mecanismo de despacho dos pacotes.

Um exemplo de implementação do algoritmo Custom Queueing, feito pela Cisco, é mostrado na Figura 35 e descrito a seguir [20]:

- O sistema mantém 17 filas, sendo uma para tráfego do sistema (fila 0) e 16 configuráveis pelo usuário.
- Associado a cada uma das 16 filas configuráveis existe um contador (programável) que especifica quantos bytes serão transmitidos da fila a cada ciclo de serviço. Pode-se especificar também o número máximo de pacotes em cada fila.
- Um ciclo de serviço é compreendido pelo atendimento sequencial (round-robin) de todas as 17 filas existentes.
- A primeira fila atendida é a fila 0, que é utilizada para transportar pacotes de alta prioridade do sistema, como mensagens de keepalive e de sinalização. Todos os pacotes da fila 0 são transmitidos antes que a fila 1 seja atendida.

- Quando uma das filas configuráveis está sendo atendida, os pacotes são enviados até que o número de bytes transmitido exceda o valor do contador de bytes associado, ou a fila fique vazia. Quando o número de bytes transmitidos excede o valor do contador, o pacote corrente é transmitido até o fim.
- As filas são estaticamente configuradas, não respondendo automaticamente a mudanças nas condições da rede.

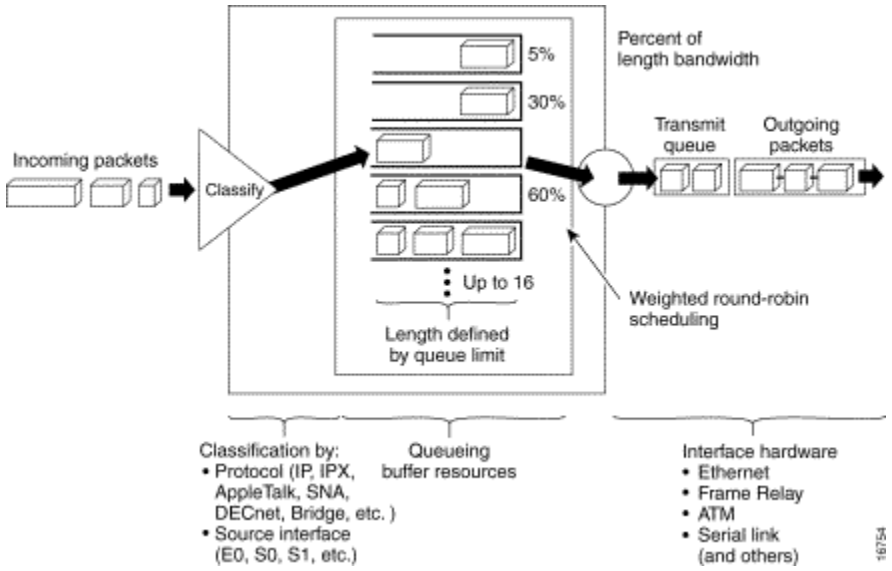


Figura 35 – Custom Queueing.

Para se obter uma dada distribuição da utilização da banda do canal entre os diversos tipos de tráfego, a escolha do valor inicializado em cada contador de bytes deve ser cuidadosa. Por exemplo, suponha que tenhamos três tipos de tráfego, um com pacotes de 500 bytes, outro com pacotes de 300 bytes e outro com pacotes de 100 bytes. Se desejarmos dividir a banda do canal igualmente entre os três, poderíamos inicializar todos os contadores com 200 bytes, por exemplo. Contudo, isto não resultaria na distribuição desejada (1/3 da banda para cada tráfego), pois a cada ciclo teríamos um pacote da primeira fila (500 bytes), um da segunda (300 bytes) e dois da terceira (2 x 100 bytes) transmitidos. A distribuição de banda resultante para as filas 1, 2 e 3 seria de 50%, 30% e 20% respectivamente.

Portanto, inicializar os contadores com valores pequenos pode resultar em uma distribuição bastante diferente da desejada. Uma solução seria inicializar os contadores com valores elevados, por exemplo 10 Kbytes para cada uma das filas do exemplo anterior, mas isto resultaria em um intervalo de tempo grande entre duas rodadas de serviço consecutivas de uma mesma fila, resultando no chamado efeito "jerky".

Para orientar na escolha do valor inicial dos contadores, a Cisco propõe o seguinte algoritmo, que parte do princípio que se conhece o tamanho dos pacotes associados a cada fila [20]:

1. Para cada fila, divida a percentagem de banda que se deseja alocar pelo tamanho do pacote em bytes. Por exemplo, assuma os seguintes tamanhos de pacotes: protocolo A = 1086 bytes, protocolo B = 291 bytes, protocolo C = 831 bytes. Se desejamos alocar 20% da banda para A, 60% para B e 20% para C, os resultados obtidos seriam: 20/1086 = 0.01842, 60/291 = 0.20619, e 20/831 = 0.02407.
2. Normalize os números obtidos dividindo-os pelo menor número. O resultado é a relação entre o número de pacotes que devem ser enviados tal que cada protocolo utilize as percentagens de banda previstas (20-60-20). No nosso exemplo teríamos 1, 11.2 e 1.3.
3. Aproxime os números obtidos no passo 2 para o inteiro superior imediato: 1, 12, 2.
4. Converta o resultado obtido no passo 3 em bytes, multiplicando o resultado pelo tamanho do pacote em cada protocolo. No nosso exemplo teríamos: 1086 (1 x 1086), 3492 (12 x 291) e 1662 (2 x 831). Este é o valor com que cada contador deve ser inicializado.
5. Determine a percentagem de banda alocada para cada protocolo: 1086/6240 = 17.4%, 3492/6240 = 56%, e 1662/6240 = 26.6%. Se a alocação resultante não for satisfatória vá para o passo de ajuste (6), caso contrário, fim.
6. Se o resultado não for satisfatório, tente ajustar mais precisamente o resultado multiplicando-se os números obtidos no passo 2 por uma constante (não necessariamente um número inteiro) e volte ao passo 3. Por exemplo, multiplicando-se por 2 e repetindo-se os passos 3, 4 e 5 obteríamos a seguinte

seqüência de transmissão e respectiva percentagem de banda: 2 pacotes de 1086 bytes do protocolo A (19% da banda), 23 pacotes de 291 bytes do protocolo B (59% da banda) e 3 pacotes de 831 bytes do protocolo C (22% da banda).

Percebe-se então que o tamanho do pacote em cada tráfego influencia de forma significativa a escolha do valor do contador e o resultado obtido.

Outro fator que afeta a distribuição da banda é o tamanho da janela. Se a janela de um protocolo particular é igual a 1, o protocolo não colocará outro pacote na fila até que ele receba um reconhecimento. Portanto, com uma janela de tamanho 1, um único pacote de cada fila será enviado por vez, mesmo que o valor do contador permita o envio de mais de um pacote. Portanto, o tamanho da janela associado a cada protocolo deve ser superior ao número de pacotes correspondente ao valor de inicialização do contador, para que o objetivo de distribuição de banda opere adequadamente.

2.3.4. WEIGHTED ROUND ROBIN – WRR

Na técnica WRR associa-se um peso a cada classe de tráfego, possivelmente com base no conteúdo do campo ToS do cabeçalho IP. Este peso é utilizado para determinar qual o percentual da banda do canal será alocado para cada classe de tráfego, de acordo com a seguinte fórmula: $P_i = (W_i/S) \times B$. Onde P_i representa a taxa (em bps) alocada para o tráfego de classe i; W_i representa o peso associado à classe de tráfego i; S é o somatório dos pesos atribuídos a todas as classes de tráfego; e B é a banda total do canal. [16]

As filas são servidas em ordem decrescente de prioridade (peso). Entretanto, contrário à operação da disciplina PQ, onde uma fila só começa a ser atendida após o atendimento pleno de todas as filas de maior prioridade, na técnica WRR o serviço passa para a próxima fila se a fila corrente ficar vazia ou se o percentual de banda atribuído a ela for ultrapassado. O controle da banda é feito através de um contador de bytes associado a cada fila, que indica o número de bytes que serão transmitidos a cada ciclo de serviço, de forma semelhante à disciplina CQ. [16][22]

2.3.5. WEIGHTED FAIR QUEUEING - WFQ

Antes de descrevermos a operação da disciplina de despacho WFQ, vamos descrever o algoritmo denominado BRR (Bit-by-bit Round Robin), no qual o WFQ se inspira. No BRR cada fluxo é mantido em uma fila de saída exclusiva e um bit de cada fluxo é enviado pelo enlace de saída a cada ciclo de serviço. O BRR, portanto, divide a banda do canal de forma equânime pelos N fluxos existentes, atribuindo a cada um a fração de 1/N da banda do canal. Esta abordagem faz com que o BRR seja um algoritmo ótimo pelo ponto de vista de justiça da distribuição dos recursos do canal entre os diversos fluxos, mas de implementação inviável, em função do overhead resultante de se transmitir um único bit por vez pelo canal. [22]

Uma disciplina de despacho denominada Fair Queueing (FQ) simula o algoritmo BRR sem a restrição de servir as filas bit-a-bit. No FQ existe uma única fila de saída[1]. Quando um pacote é recebido, o algoritmo FQ calcula o instante de tempo (t_p) em que o último bit deste pacote seria transmitido se o algoritmo BRR estivesse sendo utilizado. Este instante de tempo é tratado como um parâmetro e associado ao pacote. Os pacotes são ordenados na fila de saída em função do parâmetro t_p, em ordem crescente; ou seja, pacotes com menor valor de t_p são posicionados na fila à frente de outros pacotes com maior valor de t_p. Os pacotes são transmitidos um a um, integralmente, pelo enlace de saída, e não mais bit-a-bit como na técnica BRR. [22]

A técnica FQ busca o compartilhamento equânime do enlace por parte dos fluxos, sem diferenciar um fluxo do outro, não sendo portanto adequada em redes onde há necessidade de priorizar a transmissão de determinados tipos de tráfego, como nas redes de VoIP.

A disciplina WFQ possui o mesmo princípio da técnica FQ, oferecendo no entanto a possibilidade de se diferenciar um fluxo do outro, através de um peso atribuído a cada

[1] Uma única fila lógica, que pode estar implementada através de mais de uma fila física.

fluxo. Este peso é utilizado no momento de se calcular o valor de t_p associado a cada pacote. Ao simular o BRR, o WFQ supõe, para cada pacote, a transmissão de uma quantidade de bits proporcional ao peso associado ao fluxo (e não um único bit como no caso do FQ) [22]. Portanto, o WFQ não faz uma divisão equânime da banda entre os fluxos, mas atribui um maior percentual de banda para fluxos com maior peso.

O WFQ divide o tráfego em diferentes fluxos com base em informações do cabeçalho, tais como: endereço IP de fonte ou destino, porta TCP ou UDP de fonte ou destino, endereço MAC, identificador de conexão de enlace de dados (DLCI) do Frame Relay, e valor do campo ToS [16][20].

O WFQ permite tratar um fluxo específico ou um conjunto de fluxos agregados em uma classe de serviço (quando às vezes é denominado de CBWFQ – Class Based Weighted Fair Queueing), sendo portanto adequado tanto para a arquitetura IntServ, que opera por fluxo, quanto para a arquitetura DiffServ, que opera por classe de serviço [22][16]. A cada fluxo (ou classe de fluxos) é atribuído um peso, que será utilizado para determinar a fração de largura de banda alocada ao fluxo.

Numa aplicação em que desejamos diferenciar apenas o tráfego de voz do tráfego de dados, podemos definir apenas duas classes de fluxo: fluxo de voz e fluxo de dados. Ao fluxo de voz seria atribuído um peso maior (5 para voz e 1 para dados, por exemplo), de modo a oferecer um tratamento preferencial no que diz respeito à transmissão dos pacotes, enquanto os fluxos de dados compartilhariam a banda restante de forma equânime. A Figura 36 ilustra um sistema com duas filas, uma para tráfego de voz e outra para os fluxos de dados; para o tráfego de voz aloca-se um mínimo de 80 kbps, dos 128 kbps disponíveis no enlace. Deve-se observar que, para que se garanta a banda mínima para o tráfego de voz, o peso atribuído a este tipo de tráfego deve se ajustar dinamicamente com o perfil de tráfego da rede. Por exemplo, se o número de fluxos de dados cresce, em um dado instante, é preciso que se aumente o peso do tráfego de voz (ou diminua o peso do tráfego de dados) para que se mantenha a distribuição de banda anterior.

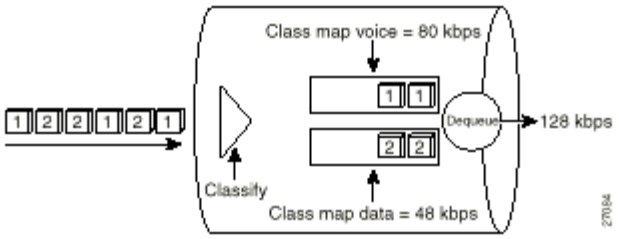


Figura 36 – Exemplo de compartilhamento de tráfego de voz e dados utilizando WFQ.

2.3.5.1. WFQ e IP PRECEDENCE

Os bits de Precedência do cabeçalho IP podem ser utilizados para estabelecer o peso associado a cada fluxo (assim como o valor do campo ToS na arquitetura DiffServ). Vamos admitir que o peso associado a cada fluxo é o valor contido nos bits de Precedência mais um, e que temos um fluxo para cada um dos 8 valores possíveis dos bits de Precedência (0 a 7). Portanto, temos oito pesos distintos, de 1 a 8, cada um associado a cada um dos oito fluxos. A distribuição da banda entre os oito fluxos será dada, então, pela divisão do peso associado a cada fluxo pelo somatório dos pesos, ou seja, o fluxo de peso *i* terá *i*/36 da capacidade do enlace. Vamos admitir agora que o número de fluxos com peso 2 aumentou para dezoito. O somatório dos pesos de todos os fluxos passa a ser 70, e um fluxo de peso *i* passa a ter *i*/70 da capacidade do enlace. Este exemplo mostra a capacidade de adaptação do WFQ às variações no comportamento do tráfego [20][23].

2.3.5.2. WFQ e RSVP

O RSVP e o WFQ podem interagir, com o RSVP utilizando o WFQ para alocar espaço nos buffers, fazer o escalonamento dos pacotes, e garantir a banda necessária para os fluxos reservados. Neste caso, a atribuição dos pesos a cada fluxo se dá em função dos parâmetros de reserva do RSVP. Esta situação pode ser utilizada, por exemplo, na implementação da arquitetura IntServ [22][20]

2.3.6. MODIFIED DEFICIT ROUND ROBIN - MDRR

Nesta técnica, implementada pela Cisco, existe um determinado número de filas (oito, por exemplo), dentre as quais uma fila, denominada LLHP (Low Latency, High Priority), possui prioridade sobre as demais. Para a fila LLHP são enviados os pacotes pertencentes à classe para a qual se deseja dar tratamento diferenciado, como por exemplo, pacotes de voz. A cada ciclo de serviço o roteador transmite primeiro todos os pacotes da LLHP, para então servir as demais filas com uma disciplina round-robin. O número de pacotes servidos de cada fila (a menos da LLHP) depende do peso associado à mesma, que é representado por um contador de bytes, de forma semelhante à descrita para a fila CQ. A Figura 37 ilustra a operação da técnica MDDR. [16]

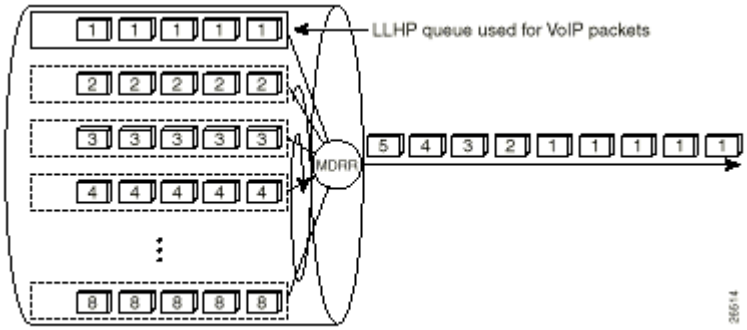


Figura 37 – Operação Strict Priority Mode da técnica MDDR.

2.4. CONTROLE DE CONGESTIONAMENTO

Técnicas de controle de congestionamento monitoram o tráfego na rede no sentido de antecipar e evitar a ocorrência de congestionamento, usualmente através do descarte de pacotes. As duas principais técnicas que operam com este objetivo são a Random Early Detection (RED) e sua versão com ponderação, Weighted Random Early Detection (WRED).

2.4.1. RANDOM EARLY DETECTION (RED)

Quando ocorre um timeout no TCP transmissor, o protocolo reduz o tamanho da janela de transmissão e inicia o processo de partida lenta (slow start), onde o tamanho da janela vai sendo aumentado gradativamente à medida em que o transmissor vai recebendo reconhecimentos positivos do receptor.

Se um pacote de um fluxo TCP é descartado pela rede, ocorrerá um timeout e o procedimento descrito no parágrafo anterior têm início. Como conseqüência da redução do tamanho da janela de transmissão, temos a redução na taxa de transmissão de pacotes.

Se a perda de pacote é devida a congestionamento no roteador, a redução da taxa de transmissão de pacotes por parte do TCP transmissor, resultante desta perda, irá aliviar a situação de congestionamento. Se a situação de congestionamento leva ao descarte de pacotes de vários fluxos distintos, teremos vários transmissores reduzindo suas janelas de transmissão e iniciando o processo de partida lenta, eliminando o congestionamento. No entanto, estes transmissores irão aumentando suas janelas de transmissão conjuntamente, até voltar ao tamanho original e, consequentemente, teremos novamente uma situação de congestionamento, que resultará em novos descartes de pacotes e no reinicio do processo. Este ciclo é conhecido como Problema de Sincronização Global. O algoritmo RED tenta evitar este problema atuando de forma preventiva, e não reativa, ao congestionamento; ou seja, o RED tenta evitar que o congestionamento ocorra.

No algoritmo RED, quando uma situação de tendência de congestionamento é detectada (o tamanho da fila ultrapassa um determinado limiar, por exemplo), inicia-se um processo de descarte aleatório de pacotes, onde a probabilidade de descarte é função da taxa de ocupação da fila, como ilustra a Figura 38. Este descarte antecipativo irá resultar na diminuição da taxa de chegada de pacotes no roteador, devido ao mecanismo de operação do TCP, e consequentemente teremos uma reversão na tendência de congestionamento.

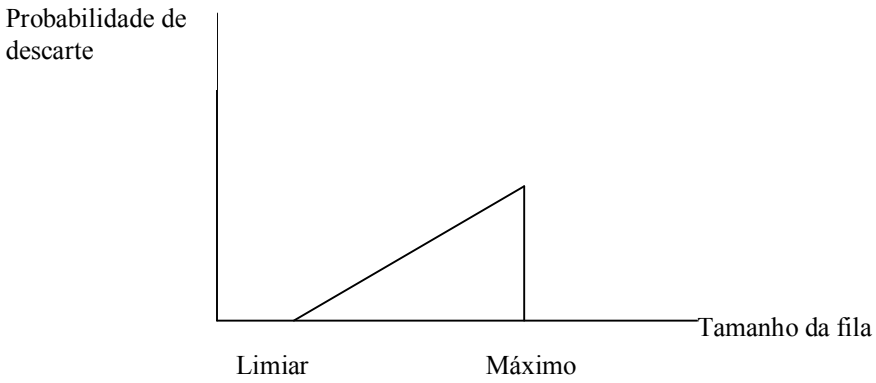


Figura 38 – Probabilidade de descarte no algoritmo RED.

O RED só funciona adequadamente em conjunto com protocolos de transporte que sejam robustos quanto à perda de pacotes, como o TCP. Se o protocolo de transporte não reage à perda de pacotes com a diminuição da taxa de transmissão de pacotes, o RED não terá nenhum efeito positivo, podendo inclusive deteriorar o desempenho do sistema pelo aumento da taxa de perda de pacotes.

2.4.2. WEIGHTED RANDOM EARLY DETECTION (WRED)

No algoritmo WRED a probabilidade de um pacote entrante ser descartado é definida pela taxa de ocupação da fila e por um peso associado ao fluxo (ou classe de fluxo) ao qual o pacote pertence. O que se busca com o WRED é que pacotes de maior prioridade tenham menor probabilidade de descarte. Por exemplo, uma probabilidade de descarte menor pode ser associada a fluxos de pacotes com maior prioridade (determinada pelo conteúdo dos bits de Precedência do campo ToS do cabeçalho IP), ou fluxos de pacotes que fizeram reserva de recursos (através do protocolo RSVP). A Figura 39 ilustra a operação do algoritmo WRED [24].

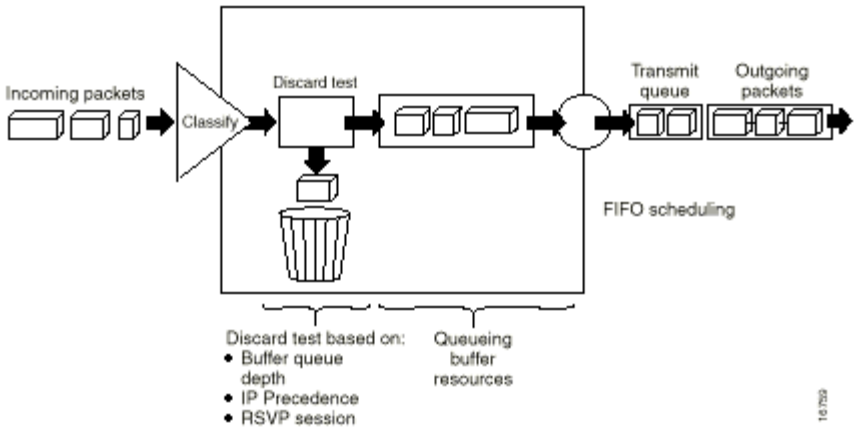


Figura 39 – Operação do algoritmo WRED.

2.4.2.1. WRED e VoIP

O uso do algoritmo WRED não resulta na priorização estrita que o tráfego de voz requer. No entanto, o WRED pode prover um tratamento preferencial aos pacotes de voz durante situações de congestionamento, minimizando a perda destes pacotes pelo descarte antecipativo de pacotes de dados, aos quais se atribui uma maior probabilidade de descarte [16].

Deve-se lembrar que o descarte de um pacote de voz não reduzirá o fluxo de chegada deste tipo de pacote, uma vez que o UDP não reage à perda de pacotes. Portanto, um fluxo muito pesado de tráfego de voz pode causar o overflow em uma fila WRED e consequentemente uma elevada taxa de perda de pacotes. Ainda, se a probabilidade de descarte, pelo WRED, associada a pacotes de voz não for muito baixa, podemos ter uma taxa de perda de pacotes inaceitável para este tipo de tráfego e a consequente perda do nível de QoS.

2.5. POLICIAMENTO E CONFORMAÇÃO DE TRÁFEGO

As funções de policiamento e conformação usualmente identificam as violações no tráfego de uma mesma maneira. Elas diferem, contudo, na forma como elas respondem a estas violações, por exemplo [25]:

- A função de policiamento usualmente descarta o tráfego que não está conforme ou o define como elegível para descarte.
- A função de conformação tipicamente atrasa o tráfego em excesso, através de mecanismos de enfileiramento, retendo os pacotes e liberando-os de maneira tal que o fluxo de saída esteja dentro dos parâmetros definidos.

A técnica Token Bucket, descrita a seguir, é a mais comumente utilizada para as funções de policiamento e conformação de tráfego. Por exemplo, os algoritmos CAR (Commited Access Rate), GTS (Generic Traffic Shaping) e FRTS (Frame Relay Traffic Shaping), implementados pela CISCO, se baseiam no Token Bucket. [25]

2.5.1. TOKEN BUCKET

O Token Bucket é uma definição formal de uma taxa de transferência. Ele possui três componentes: [25]

- Comprimento de rajada: especifica a máxima rajada (em bits) que pode ser enviada dentro de um intervalo de tempo.
- Taxa média: especifica quantos bits podem ser enviados por unidade de tempo, em média. Por definição, sobre qualquer múltiplo inteiro do intervalo, a taxa de bits da interface não excederá a taxa média. Dentro de um intervalo a taxa de bit pode exceder momentaneamente a taxa média.
- Intervalo de tempo: também chamado intervalo de medida, especifica o intervalo de tempo em que se define o comprimento de rajada e a taxa média.

O algoritmo Token Bucket opera, metaforicamente, da seguinte maneira:

- Fichas são depositadas em um balde, com capacidade para C fichas, a uma taxa constante.
- Se o balde enche de fichas, as próximas fichas que chegam são descartadas.
- A transmissão de um pacote consome do balde uma quantidade de fichas igual ao tamanho do pacote (em bytes).
- Se um pacote chega e não há fichas em quantidade suficiente no balde, o pacote é declarado não conforme e uma de duas ações pode ser tomada:
    - O pacote é descartado ou definido como elegível para descarte (alterando-se os bits de Precedência, por exemplo). Esta ação está usualmente associada à função de policiamento de tráfego.
    - O pacote é atrasado até que se tenha fichas suficientes no balde. Esta ação está usualmente associada à função de conformação de tráfego.
- Quando não se tem pacotes para transmitir, as fichas acumulam-se no balde (até sua capacidade C), permitindo que se transmita posteriormente rajadas de pacotes.

A maior rajada de dados que se pode transmitir ocorre quando o balde está cheio e chega um pacote. O tamanho desta rajada é definido pela capacidade do balde mais o intervalo de tempo dividido pela taxa de chegada de fichas no balde. Em regime permanente, a taxa de transmissão de dados não excede a taxa de chegada de fichas no balde.

Os algoritmos de policiamento e conformação de tráfego podem dispensar tratamentos distintos a fluxos (ou classes de fluxos) distintos.

2.6. FRAGMENTAÇÃO

Tráfego interativo, tal como VoIP, pode ter latência elevada devido à presença de pacotes de dados de grande extensão no sistema. Uma forma de resolver este problema de atraso é fragmentar os pacotes de dados que excederem determinado limite em pacotes menores, que serão tratados como unidades independentes pela rede.

A Figura 40 ilustra uma situação onde pacotes de voz e grandes pacotes de dados estão chegando a um roteador. Os pacotes de dados são fragmentados em pacotes menores e armazenados em fila diferente da utilizada para pacotes de voz. O algoritmo WFQ é utilizado para despacho, e dá prioridade aos pacotes de voz [26].

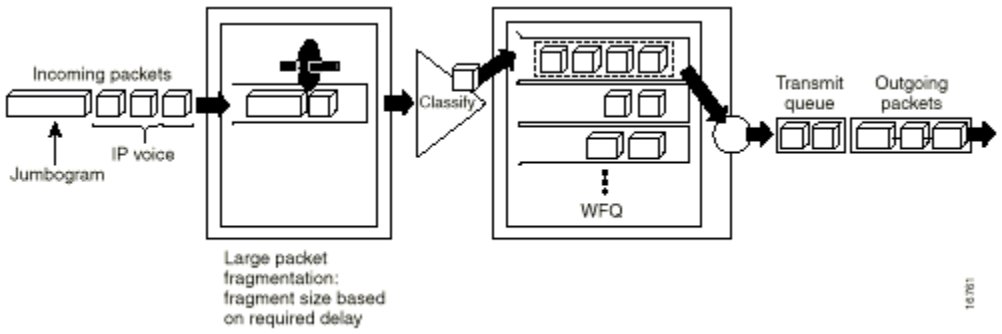


Figura 40 – Fragmentação de pacotes.

A fragmentação de pacotes diminui o desvio padrão do tamanho dos pacotes manuseados pela(s) fila(s) de saída, resultando na diminuição do tempo médio de enfileiramento de pacote e do desvio padrão deste tempo. A diminuição do tempo médio faz com que o pacote de VoIP chegue mais rapidamente ao destino, e a diminuição do desvio padrão resulte na diminuição do jitter de atraso na rede, melhorando a qualidade do sinal de VoIP. As expressões a seguir ilustram a influência da distribuição do tamanho do pacote no tempo médio de enfileiramento do pacote e no desvio padrão deste tempo, onde $E(t_s)$ representa o tempo médio de transmissão de um pacote, E(n) representa a taxa de chegada de pacotes no sistema, e ρ a taxa de utilização do servidor [27].

$$E(t_w) = \frac{\rho \cdot E(t_s)}{2(1-\rho)} \cdot \left[1 + \left(\frac{\sigma_{ts}}{E(t_s)} \right)^2 \right]$$

$$\sigma_{tw} = \sqrt{\frac{E(n)E(t_s^3)}{3(1-\rho)} + \frac{E^2(n)E^2(t_s^2)}{4(1-\rho)^2}}$$

2.7. RSVP – RESOURCE RESERVATION PROTOCOL

O RSVP é um protocolo de sinalização, concebido para a Arquitetura de Serviços Integrados da Internet, que permite aos hosts requisitarem níveis de QoS específicos para suas aplicações. Ele também é utilizado pelos roteadores para entregar requisições de QoS para outros roteadores (ou outros tipos de nós) ao longo do caminho de um fluxo. As requisições do RSVP resultam, quando possível, em reservas de recursos na rede, de modo que esta possa prover o nível de QoS solicitado [28].

O RSVP não é um protocolo de roteamento; ele utiliza os protocolos de roteamento da rede para determinar a rota a ser seguida entre origem e destino, e pode operar nos modos unicast ou multicast [28].

Todas as mensagens RSVP consistem de um cabeçalho seguido por um corpo, que contém um número variável de objetos. A Figura 41 ilustra o cabeçalho RSVP, que é comum a todas as mensagens. Os seguintes campos são identificados [12]:

- Versão: número da versão do protocolo.
- Flags: nenhum flag está definido.
- Tipo de mensagem: identifica o tipo de mensagem RSVP que está sendo enviada.
- Checksum.
- Send_TTL: O valor do IP TTL com o qual a mensagem foi enviada.
- RSVP Lenght: comprimento total da mensagem RSVP em bytes, incluindo o cabeçalho e os objetos que seguem.

<table>
<tr><td>0</td><td>1 - 2</td><td>3</td><td>4</td><td>5 - 6</td><td>7</td><td>8</td><td>9 - 15</td><td>15</td><td>16</td><td>17-30</td><td>31</td></tr>
<tr><td colspan="3">Version</td><td colspan="3">Flags</td><td colspan="4">Message type</td><td colspan="4">RSVP checksum</td></tr>
<tr><td colspan="6">Send_TTL</td><td colspan="4">Reserved</td><td colspan="4">RSVP Length</td></tr>
</table>

Figura 41 – Cabeçalho RSVP.

Cada objeto RSVP é codificado na mensagem com uma ou mais palavras de 32 bits, conforme ilustra a Figura 42. Os objetos definem as informações trocadas entre os servidores, clientes e nós (roteadores) no caminho reservado. Alguns exemplos de informações definidas pelos objetos são: identificação do destino (unicast ou multicast); endereço IP do nó RSVP-capaz que enviou a mensagem; nível de QoS desejado; estilo de reserva (ver item 2.7.1); característica do tráfego gerado pela fonte (descritor token-bucket); etc. [12][22]

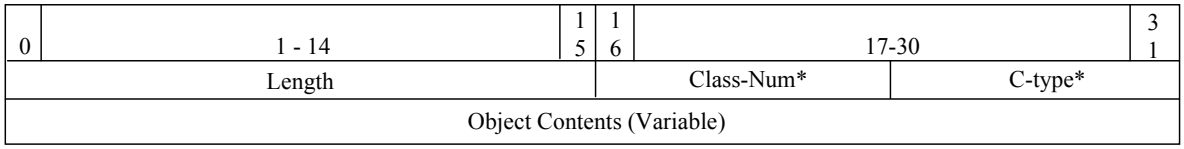


Figura 42. Objetos RSVP na mensagem.

2.7.1. ESTILOS DE RESERVA RSVP [28]

As reservas RSVP podem ser de três tipos, ou estilos: Fixed Filter, Shared Explicit, e Wildcard Filter.

WILDCARD FILTER (WF): Este estilo representa a opção: reserva “compartilhada” e ausência de controle na seleção do transmissor (“wildcard”). Assim, o estilo WF cria uma única reserva que é compartilhada pelos fluxos de todos os transmissores a upstream. O WF pode ser visto como um “duto” compartilhado, cujo tamanho é a maior das requisições de recursos feita pelos receptores, independente do número de transmissores. Uma reserva estilo WF é propagada à upstream para todos os hosts transmissores, e é automaticamente estendida para novos transmissores que surgirem .

Simbolicamente podemos representar o estilo WF como: WF { * [Q] }, onde o * indica qualquer transmissor e Q representa o nível de QoS.

FIXED FILTER (FF): Este estilo define a opção: reservas distintas e seleção explícita do transmissor. Ou seja, cria-se uma reserva distinta para cada transmissor em particular, sem compartilhamento com outros transmissores. A cada transmissor selecionado é atribuído um nível de reserva (QoS).

Simbolicamente, o estilo FF pode ser representado por: FF { S1[Q1], S2[Q2], S3[Q3], ...}, onde Si representa o transmissor i e Qi representa o nível de qualidade associado (FlowSpec).

A reserva total de um enlace para uma dada sessão é a soma de Q1, Q2, ...Q_n, onde n é o número de reservas realizadas.

SHARED EXPLICIT (SE): O estilo SE indica reserva compartilhada e seleção explícita dos transmissores; ou seja, o SE cria uma única reserva compartilhada pelos transmissores selecionados.

Podemos representar, simbolicamente, o estilo SE por: SE { (S1,S2,S3,...) [Q]}. Onde S1, S2,S3,... é a lista de transmissores e Q o nível de QoS especificado.

Reservas compartilhadas, criadas pelos estilos WF e SE, são apropriadas para aplicações multicast em que as múltiplas fontes de dados não irão, provavelmente, transmitir simultaneamente. Sinais de áudio são um exemplo de aplicação adequada para reserva compartilhada; como o número de pessoas que falam ao mesmo tempo em uma audioconferência é limitado, o receptor pode solicitar uma reserva do dobro da banda requerida para um sinal (para prever alguma sobreposição de locutor). Por outro lado, o estilo FF, que cria reservas distintas para os fluxos dos diferentes transmissores, é apropriado para sinais de vídeo.

2.7.2. MENSAGENS RSVP e OPERAÇÃO BÁSICA DO PROTOCOLO

As principais mensagens RSVP são PATH e RESV. A mensagem PATH tem por função principal construir o caminho pelo qual as mensagens RESV irão passar efetuando as reservas de recursos [22].

A operação básica do protocolo é a seguinte [29]:

- A fonte especifica as características do tráfego a ser transmitido, através de parâmetros do algoritmo Token-Bucket. Esta informação é transportada no objeto Sender Tspec.
- O RSVP da fonte envia uma mensagem PATH ao destino (ou destinos) contendo a especificação do tráfego feito pela fonte. A rota a ser seguida pela mensagem PATH é definida pelo algoritmo de roteamento, e não pelo RSVP.
- Cada roteador RSVP-capaz ao longo da rota estabelece um "path-state" que inclui o endereço do roteador RSVP-capaz imediatamente anterior (roteador que enviou a mensagem PATH - upstream). Cada roteador envia seu endereço ao vizinho posterior (downstream) através do objeto RSVP_HOP. Os roteadores podem incluir na mensagem PATH informações sobre os recursos disponíveis e o atraso aproximado que ele irá introduzir, através do objeto ADSpec. Assim, em qualquer ponto ao longo da rota, a mensagem PATH contém o endereço IP do roteador vizinho (upstream) e pode conter informações de capacidade e atraso aproximado que cada nó irá introduzir [18][29].
- Para fazer a reserva de recursos, o receptor envia uma mensagem RESV (requisição de reserva) na direção da fonte, contendo a especificação da qualidade de serviço requisitada para o fluxo de dados (objeto FlowSpec). A mensagem RESV vai do receptor à fonte através do mesmo caminho percorrido pela mensagem PATH. Isto é possível porque cada roteador armazenou o endereço do vizinho (na direção da fonte) recebido na mensagem PATH.
- Cada roteador RSVP-capaz ao longo da rota (upstream), ao receber a mensagem RESV, utiliza um processo de controle de admissão para autenticar a requisição e

alocar os recursos necessários. Se a requisição não pode ser satisfeita (devido à insuficiência de recursos, por exemplo), o roteador retorna uma mensagem de erro ao receptor (origem da mensagem RESV). Se a requisição for aceita, o roteador envia a mensagem RESV ao próximo roteador a upstream.

- Quando o último roteador (mais próximo da fonte) recebe a mensagem RESV e aceita a requisição, ele envia uma mensagem de confirmação ao receptor.
- O RSVP opera com o conceito de soft state, o que significa que o transmissor e o receptor devem enviar periodicamente mensagens de PATH e RESV para revalidar (ou atualizar) as reservas feitas. Esta característica permite reação dinâmica a alterações ocorridas na fonte do fluxo, nos parâmetros de QoS estabelecidos pelo receptor, ou na rota.

3. ARQUITETURAS PARA QoS

3.1. ARQUITETURA DE SERVIÇOS INTEGRADOS (IntServ) [30] [31] [32] [33]

O modelo de serviços integrados propõe duas classes de serviço, além do serviço usual de melhor esforço, que são:

- Serviço Garantido: para aplicações em tempo real, como VoIP, que requeiram banda garantida e limite para o atraso.
- Serviço de Carga Controlada: para aplicações que demandem serviço "melhor que melhor esforço", mas sem garantia de banda ou limite de atraso.

Na classe Serviço Garantido o fluxo é descrito utilizando-se o algoritmo Token Bucket, e esta descrição é utilizada pelos elementos da rede (roteadores, subredes, etc) para computar vários parâmetros descrevendo como os elementos devem manusear o fluxo de dados. Combinando os parâmetros dos diversos dispositivos ao longo do caminho, é possível calcular o máximo atraso que os pacotes de tal fluxo irão sofrer [33].

Para a implementação da arquitetura IntServ é necessário que os roteadores ao longo do caminho sejam capazes de reservar recursos, de modo a prover o nível de QoS desejado para cada fluxo. As aplicações devem estabelecer o caminho e reservar os recursos antes do início da transmissão dos dados. Para tal, pode-se utilizar o protocolo RSVP.

A IntServ se baseia no conceito "per-flow state", e é implementada por quatro componentes:

- Protocolo de Sinalização (RSVP): utilizado para efetuar a reserva dos recursos na rede.
- Controle de Admissão: a rotina de controle de admissão irá decidir se a requisição de recursos pode ser atendida.
- Classificador: classifica os pacotes de cada fluxo, encaminhando-os à fila adequada.
- Escalonador: gerencia o encaminhamento (despacho) dos pacotes de cada fluxo, usando um conjunto de filas e possivelmente outros recursos, como temporizadores, de modo a atender o nível de QoS associado a cada fluxo. As funções de policiamento, necessárias para verificar se o tráfego está com comportamento adequado, são consideradas como parte das ações do Escalonador [31].

A arquitetura IntServ possui os seguintes problemas [30]:

- A quantidade de informações de estado aumentam proporcionalmente ao número de fluxos, podendo resultar em uma grande sobrecarga de processamento e memória para os roteadores do backbone da rede.
- Todos os roteadores devem implementar RSVP, controle de admissão, classificação e escalonamento de pacotes.
- Para Serviço Garantido, a arquitetura tem de ser implementada por completo em toda a rede. Para serviço de carga controlada é possível uma implementação gradual, com o desenvolvimento da funcionalidade IntServ nos dispositivos que constituem os gargalos de um domínio da rede e o tunelamento das mensagens RSVP sobre a outra parte do domínio.

3.2. ARQUITETURA DE SERVIÇOS DIFERENCIADOS (DiffServ) [30]

A arquitetura DiffServ estabelece várias classes de serviços diferenciados, que podem ser especificadas, por exemplo, pelo conteúdo do byte TOS no cabeçalho IP (ver item 2.2). A classificação dos pacotes pode ser feita inicialmente pelo cliente ou pelo roteador de ingresso na rede.

Para receber um serviço diferenciado, um usuário da Internet deve firmar um Acordo de Nível de Serviço (SLA – Service Level Agreement), que irá especificar as classes de serviço suportadas e a quantidade de tráfego permitida em cada classe. O SLA pode ser estático ou dinâmico. Para o caso dinâmico deve-se utilizar um protocolo de sinalização, por exemplo RSVP, para requisitar os serviços sob demanda.

No ingresso da rede, os pacotes são classificados, policiados e possivelmente conformados. As regras de classificação, policiamento e conformação usadas nos roteadores de ingresso são derivadas do SLA. Quando um pacote proveniente de um domínio entra em outro domínio, sua classificação pode ser alterada, seguindo o SLA entre os dois domínios.

A arquitetura DiffServ é significativamente diferente da IntServ. Na DiffServ existe um número limitado de classes de serviços, e as informações de estado são proporcionais ao número de classes e não ao número de fluxos. DiffServ é portanto mais escalável que IntServ.

Utilizando-se as ferramentas de classificação, policiamento, conformação e mecanismos de despacho, vários serviços podem ser oferecidos. Por exemplo: Serviço Premium para aplicações que requeiram atraso e jitter pequenos; Serviço Garantido para aplicações que requeiram melhor confiabilidade que o Serviço Melhor Esforço pode oferecer; Serviço Olímpico, que possui as subclasses ouro, prata e bronze.

No serviço Premium, que é o mais adequado para VoIP, cada usuário tem um SLA com o provedor de serviço. O SLA especifica a taxa de bits (taxa de pico) desejada para um fluxo específico ou um agregado de fluxos. O usuário é responsável por não exceder a taxa especificada, caso contrário o excesso de tráfego será descartado pelo mecanismo de policiamento da rede. O ISP garante que a banda contratada estará disponível para o tráfego.

Através de mecanismos de classificação, o tráfego Premium é marcado, no domínio do usuário, como tráfego prioritário. O roteador de ingresso na rede DiffServ irá prover as funções de policiamento, descartando os pacotes não-conformes com o SLA, enfileiramento e despacho, de forma que os pacotes Premium sejam transmitidos antes dos pacotes das outras classes de serviço.

Através do controle de admissão, o tráfego Premium pode ser limitado a uma pequena percentagem (por exemplo, 10%) da banda de todos os enlaces de entrada. No enlace de saída os pacotes Premium são transmitidos antes dos outros, podendo ocupar até 100% da capacidade do enlace. Como os enlaces são usualmente full-duplex, a banda dos enlaces de entrada é igual a dos enlaces de saída. Portanto, se o tráfego Premium é distribuído igualmente entre os enlaces, o policiamento, controle de admissão e algoritmo de despacho, podem garantir que a taxa de serviço da fila PQ (Premium Queue) é muito maior que a taxa de chegada de pacotes. Portanto, um pacote Premium que esteja chegando ao roteador encontrará, na maioria das vezes, a fila PQ vazia ou com poucos pacotes, resultando em baixo atraso.

A agregação de tráfego pode ser um problema para o serviço Premium da arquitetura DiffServ. A Figura 43 ilustra a questão: existe uma agregação do tráfego dos roteadores de borda (BR1 a BR3) que chega ao roteador núcleo CR1, mas isto não traz problemas pois o enlace de saída de CR1 é mais rápido que os enlaces de entrada. No entanto, a agregação de tráfego na entrada de CR4 pode resultar em uma taxa de chegada de pacotes próxima da taxa de serviço, com aumento considerável do atraso. A arquitetura DiffServ sozinha não pode resolver este problema, sendo necessário a utilização de Roteamento Baseado em

Restrição/Engenharia de Tráfego para evitar a situação de congestionamento causada pelo excesso de tráfego Premium [30].

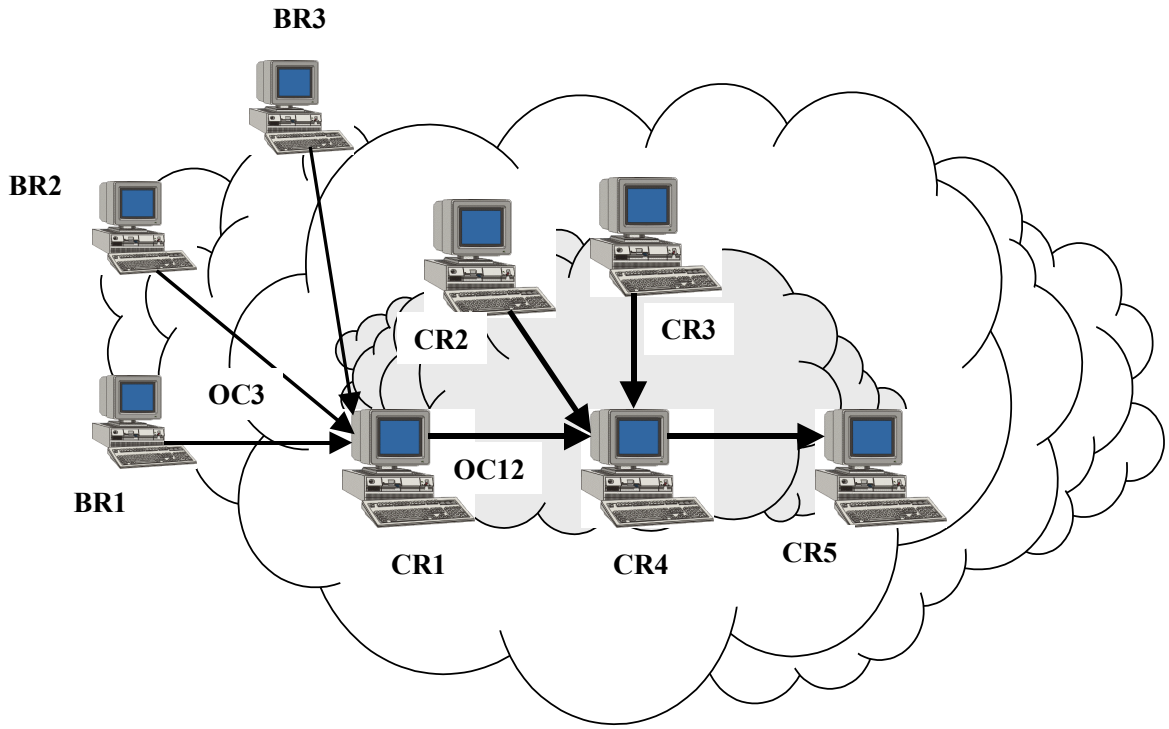


Figura 43 – Agregação de tráfego na rede DiffServ.

3.3. MULTI-PROTOCOL LABEL SWITCHING – MPLS [30][34][35]

O MPLS é um esquema de encaminhamento de pacotes que evoluiu da tecnologia Tag Switching desenvolvida pela Cisco. No modelo OSI de 7 camadas ele se situa entre as camadas 2 (enlace) e 3 (rede).

Cada pacote MPLS tem um cabeçalho que contém um label de 20 bits, um campo de Classe de Serviço (Class of Service – COS) de 3 bits, um bit (B) que indica que o label é o último de uma pilha de labels e um campo TTL (Time to Live) de 8 bits, conforme ilustrado na Figura 44. O cabeçalho MPLS é encapsulado entre o cabeçalho da camada de enlace e o cabeçalho da camada de rede. Um roteador MPLS-capaz, denominado LSR (Label

Switched Router), examina somente o label no encaminhamento do pacote. O protocolo de rede pode ser o IP ou outros, dando origem ao nome Multi-Protocol Label Switching.

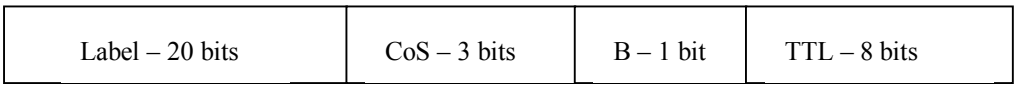


Figura 44 – Cabeçalho MPLS

O MPLS precisa de um protocolo para distribuir labels para formar Caminhos Comutados por Label (LSPs – Label Switched Paths), que pode ser o protocolo LDP (Label Distribution Protocol) ou uma extensão do RSVP. Um LSP é similar a um circuito virtual ATM, e é unidirecional do transmissor para o receptor.

O processo de alocação de labels (estabelecimento de um LSP) pode ser disparado de três maneiras: [34]

- Topology Driven: os labels são alocados em resposta ao processamento normal do tráfego de controle do protocolo de roteamento; ou seja, uma mudança topológica pode resultar na alteração do LSP.
- Request Driven: os labels são alocados em resposta ao processamento normal de tráfego de controle baseado em requisição, tal como RSVP.
- Traffic Driven: a chegada de um pacote em um LSR dispara a alocação e distribuição de labels.

Como resultado da distribuição de labels é criado, em cada LSR, uma tabela de encaminhamento dos pacotes indexada pelos labels. Cada entrada da tabela especifica como processar os pacotes que contém o label de índice.

O caminho LSP entre dois roteadores pode ser definido pelo algoritmo de roteamento da camada 3 (roteamento hop-by-hop), ou pode ser especificado explicitamente pelo LSR de origem (Explicit Route – ER). A possibilidade de definição de rotas explícitas é uma característica útil para a implementação de VoIP. Um LSP estabelecido através de Roteamento Explícito não se altera caso ocorra uma variação no roteamento de nível 3, e

tem portanto comportamento semelhante a um caminho em uma rede do tipo Circuito Virtual. O Roteamento Explícito permite também o uso do conceito de Engenharia de Tráfego para o estabelecimento dos caminhos, permitindo uma melhor distribuição do tráfego na rede e, consequentemente, a diminuição da possibilidade de ocorrência de congestionamentos.

Pacotes são classificados e roteados pelos LSRs de ingresso de um domínio MPLS-capaz. Os cabeçalhos MPLS são então inseridos. Quando um LSR recebe um pacote MPLS, o label é utilizado como índice para a consulta da tabela de encaminhamento. Isto é mais rápido que o processo de roteamento utilizado em uma rede IP normal, resultando em um menor atraso experimentado por cada pacote em cada roteador MPLS-capaz. O pacote é processado como especificado pela tabela de encaminhamento. O label de entrada é substituído pelo label de saída e o pacote é comutado para o próximo LSR. Dentro do domínio MPLS, a classificação, encaminhamento e tratamento do pacote são definidos pelos campos de label e COS.

O MPLS pode ser utilizado em conjunto com a arquitetura de Serviços Diferenciados para prover QoS. A operação dos roteadores neste caso é basicamente a mesma da descrita para a DiffServ, com as seguintes diferenças [30]:

- No ingresso da rede, em adição a todo o processamento definido pela DiffServ, um cabeçalho MPLS é inserido no pacote.
- Os roteadores núcleo processam o pacote baseados no label e no campo COS, e não no campo DS definido pela DiffServ.
- Na saída do domínio MPLS o cabeçalho é removido.

4. OUTRAS CONSIDERAÇÕES PARA VoIP

Os requisitos de QoS para VoIP dificultam sobremaneira, se não impedem, a implementação desta aplicação sobre a Internet, ao menos em sua versão atual. No entanto,

em uma rede IP controlada, a utilização das técnicas tratadas neste capítulo pode resultar no nível de QoS desejado.

Logo, a utilização de VoIP constituí uma boa alternativa para a implantação de redes multimídia corporativas, ou mesmo para a implementação de backbones, com capacidade para integração de tráfego, de empresas prestadoras de serviços de telecomunicações. A Figura 45 ilustra a utilização de algumas técnicas para prover QoS em uma rede IP corporativa com aplicação de VoIP.

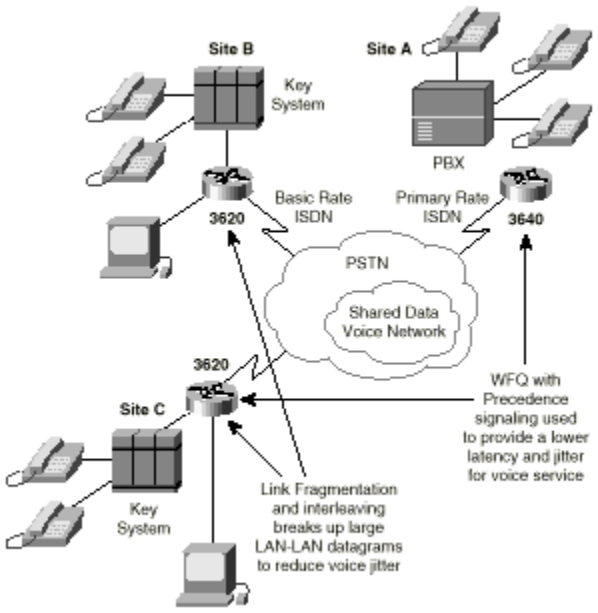


Figura 45 – Obtendo QoS para VoIP em uma rede corporativa.

No ambiente corporativo o uso da arquitetura IntServ pode ser uma boa alternativa. No backbone, devido ao grande número de fluxos, a arquitetura DiffServ, possivelmente associada ao uso de MPLS com roteamento explícito, pode ser a melhor opção. Em qualquer caso, o uso de algoritmos de despacho que priorizem o tráfego de voz é mandatório.

No que diz respeito às ferramentas para QoS, temos as seguintes considerações finais:

1. A possibilidade de alteração no caminho seguido pelos pacotes de dados durante uma conversação (mudança de rota) pode resultar em perda de qualidade. A utilização do conceito de roteamento definido pela fonte pode superar este problema. Por exemplo, pode-se fixar o caminho a ser seguido pelos pacotes como sendo aquele que os pacotes RSVP trilharam para estabelecer a reserva de recursos, e que foi definido pelo algoritmo de roteamento da rede.
2. Mesmo com a priorização dos pacotes de voz, pode-se ter perda de qualidade pelo atraso ou jitter de atraso excessivo nos nós da rede. Algoritmos de despacho que levem em conta o atraso e jitter já sofridos pelos pacotes de cada fluxo podem resultar em melhor nível de QoS.
3. Outras ferramentas utilizadas no sentido de evitar congestionamento na rede podem ser necessárias, mesmo que a priorização do tráfego de voz esteja sendo utilizada. Dentre estas ferramentas podemos citar o uso dos algoritmos RED e WRED (descritos no capítulo 3) para o tráfego de dados, e o uso de Roteamento Baseado em Restrições e Engenharia de Tráfego, não abordadas nesta versão do trabalho.

REFERÊNCIAS BIBLIOGRÁFICAS

[1] Voice over IP – Tutorial disponível em www.techguide.com.

[2] IP Telephony: An Overview – Newbridge – June 1998 – White Paper disponível em www.newbridge.com/technology/IP

[3] Kostas, Thomas J., et ali. Real-Time Voice Over Packet-Switched Networks. IEEE Network, January/February 1998, pp. 18-27.

[4] Tribuzi, André e Oliveira, Morgana Cunha. Voz sobre IP. Monografia apresentada no curso de especialização "Engenharia de Comunicação de Dados" do Instituto Nacional de Telecomunicações em Dezembro de 1999.

[5] Impact and Performance of Lucent's Internet Telephony Server (ITS) over IP Networks – Lucent Technologies – November 1997 – Artigo disponível em www.lucent.com/dns/library/pdf/white_papers/its_perform.pdf

[6] Minoli, Daniel e Minoli, Emma. Delivering Voice over IP Networks. John Wiley & Sons, Inc. New York, 1999.

[7] Prycker, Martin De. Asynchronous Transfer Mode, Solution for Broadband ISDN. Third Edition. Prentice Hall, 1995.

[8] RFC 1889 - RTP: A Transport Protocol for Real-Time Applications – January, 1996.

[9] Microlegend IP Telephony Tutorial – The IP Telephony Switch – Tutorial disponível no site www.microlegend.com

[10] Recomendação ITU-T H.323 – Packet Based Multimedia Communications Systems.

[11] Ahonen, Jarkko e Laine, Arttu. Realtime Speech and Voice Transmission on the Internet. Helsinki University of Technology. Telecommunications Software and Multimedia Laboratory. Artigo disponível em www.tcm.hut.fi/Opinnot/Tik-110.551/1997/seminar_paper.html

[12] Black, Uyless. Voice Over IP. Prentice Hall PTR. Upper Saddle River, 2000.

[13] Recomendação ITU-T H.225.0 – Media Stream Packetization and Synchronization for Visual Telephone Systems on Non-Guaranteed Quality of Service LANs.

[14] H.323 Tutorial – Web ProForums – Documento disponível no site www.webproforum.com/h323

[15] RFC 1889 – RTP: A Transport Protocol for Real-Time Applications.

[16] Quality of Service for Voice over IP Solutions Guide. CISCO SYSTEMS. Documento disponível no site www.cisco.com.

[17] – Planning for Quality of Service. Documento elaborado pela Cisco, disponível em www.cisco.com.

[18] – Croll, Alistair e Packman, Eric. Managing Bandwidth, Deploying QoS in Enterprise Networks. Prentice Hall, 2000.

[19] – Quality of Service Solutions Configuration Guide, Classification Overview. Documento elaborado pela Cisco, disponível em www.cisco.com.

[20] - Quality of Service Solutions Configuration Guide, Congestion Management Overview. Documento elaborado pela Cisco, disponível em www.cisco.com.

[21] – VoIP, Design Implementation Guide. Documento elaborado pela Cisco, disponível em www.dtr.com.br/cdrom/cc/sol/mkt/ent/ndsgn/voice_dg.htm

[22] – Magalhães, Maurício F. e Cardoso, Eleri. Qualidade de Serviço na Internet – Versão Draft. Unicamp, 1999.

[23] – Quality of Service (QoS) Networking. Documento elaborado pela Cisco, disponível em www.cisco.com.

[24] – Quality of Service Solutions Configuration Guide, Congestion Avoidance Overview. Documento elaborado pela Cisco, disponível em www.cisco.com.

[25] – Quality of Service Solutions Configuration Guide, Policing and Shaping Overview. Documento elaborado pela Cisco e disponível em www.cisco.com

[26] - Quality of Service Solutions Configuration Guide, Link Efficiency Mechanisms Overview. Documento elaborado pela Cisco e disponível em www.cisco.com

[27] – Brito, José Marcos Câmara. Projeto e Análise de Redes de Telecomunicações. Apostila de curso. Inatel, 1996.

[28] – RFC 2205 – Resource ReSerVation Protocol (RSVP), Functional Specification. Documento disponível em www.ietf.org/rfc/rfc2205.txt

[29] – QoS Protocols & Architectures. White Paper produzido por Stardust Inc, disponível em www.qosforum.com.

[30] – Xiao, Xipeng and Ni, Lionel M. – Internet QoS: A Big Picture. Department of Computer Science, Michigan State University.

[31] – RFC 1633. Integrated Services in the Internet Architecture: an Overview. July 1994. Documento disponível em www.ietf.org

[32] – Ferguson, Paul e Huston, Geoff. Quality of Service, Delivering QoS on the Internet and in Corporate Networks. John Wiley & Sons, 1998.

[33] – RFC 2212. Specification of Guaranteed Quality of Service. September 1997. Documento disponível em www.ietf.org/rfc/rfc2212.txt

[34] – A Framework for Multiprotocol Label Switching. Internet Draft, July 1999. Documento disponível em www.ietf.org/internet-drafts/draft-ietf-mpls-framework-04.txt

[35] – Granado Filho, Arlindo Garcia. MPLS, Multiprotocol Label Switching. Trabalho da disciplina IA 368, dezembro de 1998. Unicamp, SP.