Controle de Congestionamento e Qualidade de Serviço (QoS)
Prof. Marco Antonio da Silva Barbosa
Disciplina – Projeto de Redes de Computadores

Sumário

1 INTRODUÇÃO

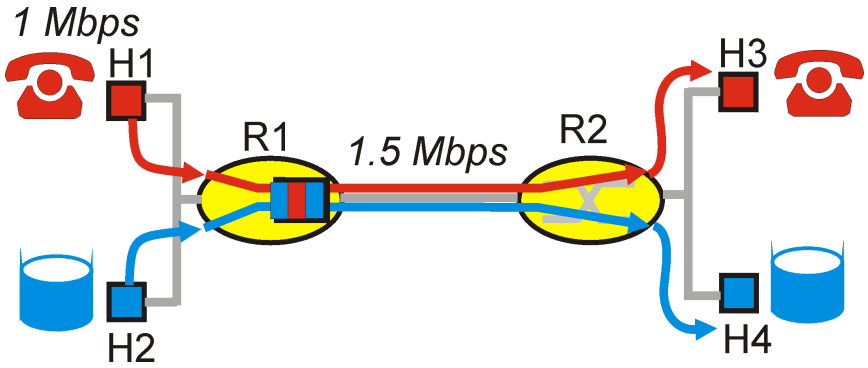
Desde o surgimento da Internet temos acompanhado uma variação no comportamento dos usuários por consumo de aplicações. Na década de 80 as principais aplicações usadas pelos usuários eram e-mail e ftp, na década de 90 veio o interesse em massa por navegação (www), nos últimos anos os usuários tomaram gosto por aplicações p2p e a tendência já indica que até 2016 voip e multimídia serão as aplicações de maior interesse, ou seja, aquelas que mais consumirão link na Internet.

Em outras palavras, ontem você gostava de ler e-mails, pulou para navegação, adora pegar suas músicas e filmes, mas a tendência agora é assistir vídeos e conversar em tempo real com seus amigos e em breve assistir tv pela Internet com NetFlix, Globo.com, etc.

E daí? Estas novas aplicações exigem muito mais da rede de computadores, tanto no aspecto de volume de dados transferidos como em parâmetros de qualidade de serviço que devem ser atendidos para que o usuário tenha uma experiência de uso agradável. Você não quer assistir o vídeo quicando e nem conversar no Skype sem ver a pessoa do outro lado.

O que acontece em um enlace de 1.5Mbps quando ocorrer à transmissão simultânea de uma chamada de Voz com uma transmissão de arquivo via FTP? A figura 1 exemplifica a situação e neste caso encontramos o congestionamento, veja que o buffer do Roteador 1 começa a encher porque o canal de 1.5 Mbps não dá conta da vazão. Afetando os serviços de voz entre H1 e H3.

Figura 1. Exemplo de uma rede congestionada



Neste sentido surge a discussão desta unidade que procura apresentar soluções para este problema. Discutiremos aspectos de QoS (Qualidade de Serviço), técnicas de controle de Congestionamento e os protocolos IntServ e DiffServ. Posso dizer que isto é uma introdução do tema, pois tem outras técnicas que não vou discutir neste material por por entender que não é foco desta matéria, mas tenha certeza que é a tendência das redes para os próximos anos, como vocês já devem ter percebido quando falamos dos protocolos de longa distância que já vem se preocupando com alternativas para alcançar QoS.

2 QOS (QUALIDADE DE SERVIÇO)

Atualmente a Internet oferece serviços de melhor esforço sem garantia de entrega (melhor esforço significa que se chegar chegou e no tempo que der), sem controle de admissão (novas conexões podem entrar congestionando ainda mais uma rede que pode estar lotada) e sem classificação de tráfego (sem dar condições aos equipamentos priorizar pacotes mais importantes). Esse serviço é,

muitas vezes, suficiente para um tráfego que não seja sensível a atrasos, como é o caso de transferência de arquivos e e-mail. Esse tráfego é conhecido por elástico, pois é maleável o suficiente para funcionar em condições de atraso, entretanto as aplicações do futuro da internet precisarão de qualidade, exemplo disto, como já dissemos são Voz sobre IP (VoIP) e transmissão de vídeo em tempo real, aplicações sensíveis à atrasos.

Segundo Forouzan, 2012, a **qualidade de serviço, QoS**, refere-se a um conjunto de técnicas e mecanismos que garantem o desempenho da rede, com o objetivo de oferecer um serviço previsível para um programa da camada de aplicação.

Tradicionalmente, são atribuídos quatro tipos de características a um fluxo de dados:

- Confiabilidade: **confiabilidade** é uma característica que um fluxo precisa para entregar os pacotes ao destino. A falta de confiabilidade significa a perda de um pacote ou de uma confirmação, o que implica retransmissão. Entretanto, a sensibilidade de diferentes aplicações à confiabilidade varia. Ex. Aplicações como correio e a web são mais sensíveis à confiabilidade que telefonia ou audioconferência. Ou ainda, correio e a web não aceitam perder pacotes já aplicações de telefonia e audioconferência funcionam bem mesmo perdendo alguns poucos pacotes;
- Atraso: atraso da origem até o destino (ou latência) é outra característica dos fluxos. Novamente, as aplicações podem tolerar o atraso em graus diferentes. Nesse caso, aplicações de telefonia, audioconferência, videoconferência e acesso remoto exigem um atraso reduzido, enquanto na transferência de arquivos ou e-mail, o atraso é menos importante. O atraso total[1] de um pacote pode ser expresso algebricamente da seguinte forma:

Latência = Tempo de vôo + (Tamanho do pacote / Largura de banda).

Tempo de vôo – É o tempo para que o primeiro bit do pacote chegue no receptor, incluindo o atraso de propagação pelos links e os atrasos decorrentes de outro hardware na rede, como repetidores de link e switches de rede.

Tempo de Transmissão (tamanho do pacote/largura de banda): Esse é o tempo para que o pacote passe pela rede, sem incluir o tempo de vôo. Uma forma de medi-lo é a diferença no tempo entre quando o primeiro bit do pacote chega no receptor e quando o último bit desse pacote chega no receptor. Por definição, o tempo de transmissão é igual ao tamanho do pacote dividido pela largura de banda de dados dos links de rede.

- Jitter: é a variação de atraso para pacotes que pertencem ao mesmo fluxo. Por exemplo, se quatro pacotes forem enviados nos instantes de tempo 0, 1, 2 e 3, e chegarem ao destino nos instantes 20, 21, 22 e 23, todos apresentam o mesmo atraso, de 20 unidades de tempo. Por outro lado, se os quatro pacotes anteriores chegarem ao destino nos instantes 21, 23, 24 e 28, eles tem diferentes atrasos. Para aplicações de áudio e vídeo o segundo caso é inaceitável. Essas aplicações não toleram jitter.
- Largura de banda: Diferentes aplicações exigem diferentes larguras de banda. Em aplicações de videoconferência é necessário Mbits por segundo para atualizar uma tela, enquanto um e-mail pode nem sequer chegar a 100 Kbits por segundo. A Largura de banda ou taxa de transmissão é o valor em bits por segundo que está sendo transmitido.

[1] Desconsiderando-se os overheads de envio e recebimento.

Aplicação	Confiabilidade	Atraso	Jitter	Largura de Banda
FTP	Alta	Baixa	Baixa	Média
HTTP	Alta	Média	Baixa	Média
Áudio sob demanda	Baixa	Baixa	Alta	Média
Vídeo sob demanda	Baixa	Baixa	Alta	Alta
Voz sobre IP	Baixa	Alta	Alta	Baixa
Vídeo sobre IP	Baixa	Alta	Alta	Alta

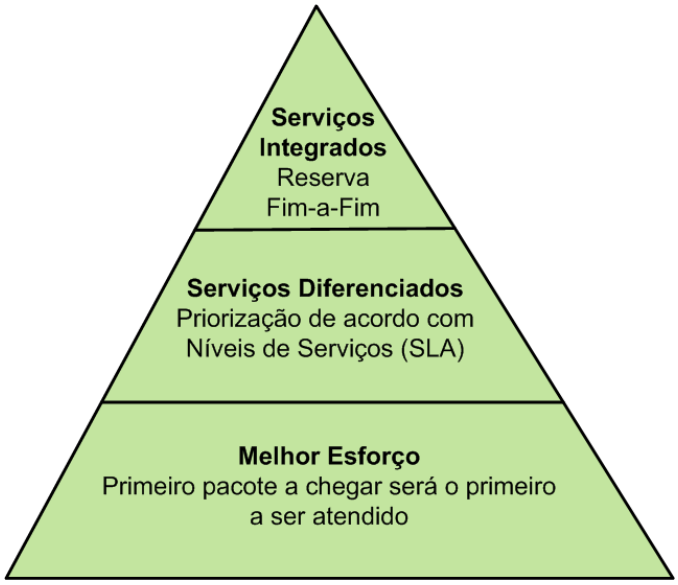
Tabela 1 – Sensibilidade das aplicações a características do fluxo.

Para oferecer QoS o trafego deve passar por 4 princípios básicos:

- Marcação: Marque os pacotes para que o roteador possa diferenciar diferentes tipos de classe.
- Isolação: Separe uma classe de outra.
- Alocação: Aloque uma porção de banda para cada classe de serviço (politica)
- Admissão: A capacidade do link estourou? Bloqueie!

Em termos das técnicas podemos indicar a pirâmide da figura 2 que mostra em sua base o mais básico da transmissão que não trata nenhuma regra e entrega o tráfego com melhor esforço, em seguida uma técnica que agrega os tráfegos em grupos priorizando o trafego do grupo (DiffServ) por fim a técnica que trata cada fluxo fim-a-fim, mais especialista (IntServ). Vamos discutir cada técnica em detalhes durante este texto.

Figura 2. Pirâmide de Qos de trafego na rede



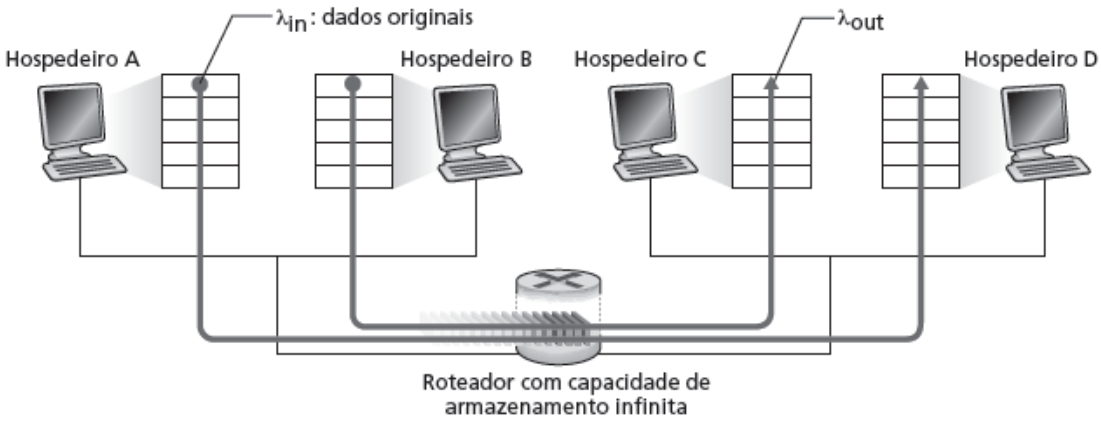
3 CONGESTIONAMENTO

Os requisitos de cada aplicação só não são atendidos porque os recursos são finitos, o link de dados e a capacidade de processamento dos equipamentos de rede causam retardo na transmissão dos pacotes. Se os links de Internet tivessem velocidade ilimitada, os pacotes não ficariam retidos nos

buffers dos roteadores, logo não teríamos atrasos e todas as aplicações funcionariam de forma ótima. Bom, mas isto é praticamente impossível acontecer, pois temos como padrão ocupar por completo qualquer recurso que nos é oferecido.

Então vamos entender o que é congestionamento e a partir daí pensar em trata-lo com as técnicas de QoS. Informalmente falando o congestionamento acontece quando muitas fontes enviam muitos dados ao mesmo tempo para rede tratar. Estes tráfegos mesmo tendo destinos diferentes tendem a passar por alguns saltos que podem se tornar o gargalo da rede. Veja o exemplo da figura 3 ou mesmo da figura 1. Mesmo o roteador da figura 3 tendo um buffer infinito o pacote pode ficar tanto tempo no roteador aguardando sua vez para ser transmitido que quando chegar ao destino já não tem validade, ou mesmo ter sido retransmitido pela origem.

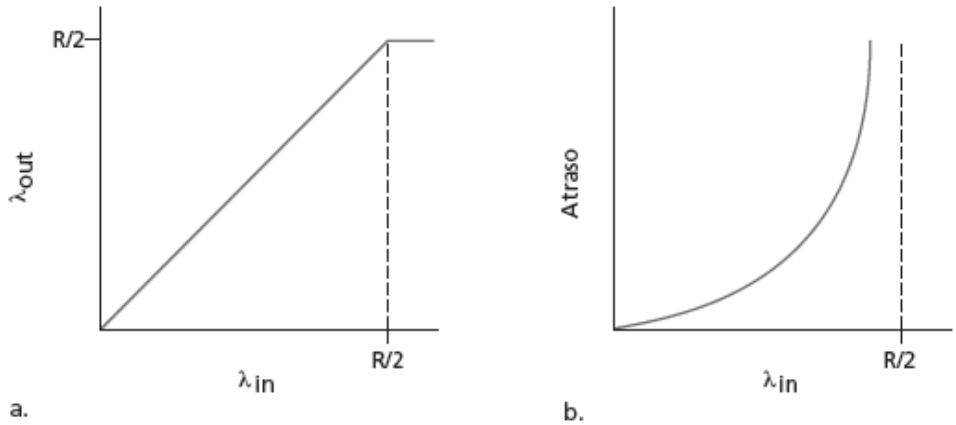
Figura 3. Rede com Roteador de Buffer infinito.



Em uma situação real onde temos buffers limitados o resultado é que teremos perdas de pacotes ou atrasos na transmissão se o link não estiver dando conta da transmissão.

A figura 4 na letra a mostra o consumo progressivo do link até se atingir seu limite, atingido seu limite a tendência é que os pacotes comecem a aumentar o tempo de atraso conforme apresentado na letra b da mesma figura.

Figura 4. Cosumo de link e atraso de pacote.



Como vimos, uma vez congestionada a rede, o pacote pode chegar atrasado ao destino ou simplesmente ser descartado por um roteador por que não há espaço em buffer para armazená-lo. Neste sentido foram desenvolvidas algumas técnicas para controle de congestionamento.

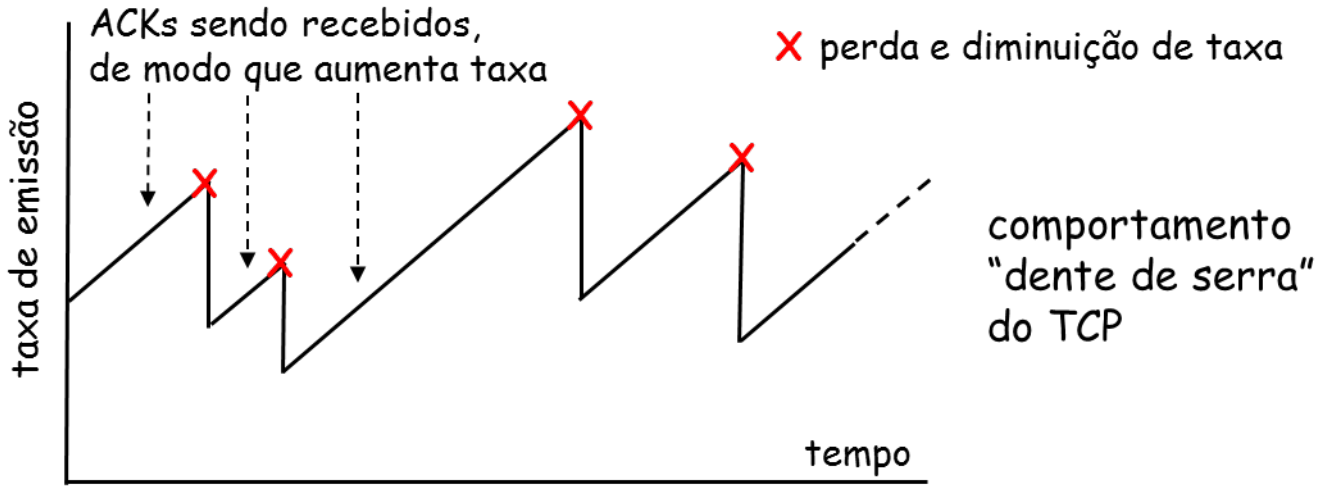
3.1 CONTROLE FIM-A-FIM

A ideia por traz desta técnica é que nenhum pacote será enviado por ninguém para indicar que a rede está congestionada, o congestionamento será deduzido em função da perda de pacote e atraso porque o destinatário não vai mandar a confirmação a tempo antes do timeout do remetente estourar. Você lembra do timeout usado na janela deslizante do TCP? Vou recordar, todo pacote enviado via TCP de um computador recebe um timeout para que seja aguardada uma confirmação de recebimento, se esta confirmação não chegar o transmissor retransmiti o mesmo pacote, pois entende que o pacote foi perdido e ainda mais, no nosso caso, ele vai entender que a rede está congestionada!

A grande dúvida é que um computador não sabe quantos pacotes por segundo ele pode mandar antes da rede congestionar. A proposta deste controle é que a taxa de transmissão, ou seja, a quantidade de pacotes vá sendo aumentada à medida que as confirmações cheguem e quando um timeout for detectado o transmissor vai entender que a rede está congestionada e vai reduzir sua taxa de transmissão e voltar a subir repetindo o processo até estabilizar a velocidade, só que a taxa de crescimento vai ser menor a cada vez que for detectada uma perda. Ou ainda, o transmissor vai "procurando uma largura de banda" que a rede suporta aumentando a taxa de transmissão no recebimento do ACK (confirmação) até por fim acontecer uma perda, depois diminui a taxa de transmissão. O processo continua sempre aumentando na chegada de um ACK e diminuindo na perda de uma confirmação, temos que lembrar que a largura de banda da rede disponível está sempre variando dependendo de outras conexões na rede.

A figura 5 mostra a lógica da proposta do controle de congestionamento fim a fim. A taxa de transmissão vai aumentando até que ocorra uma perda de confirmação o que conduz o transmissor a reduzir sua taxa de transmissão para volta a subir até cair novamente ..... O x na figura identifica os momentos onde o transmissor estourou o tempo de espera pela confirmação de um pacote e entendeu que a rede estaria congestionada, forçando-o a reduzir a taxa de transmissão.

Figura 5. Controle fim a fim feito pelo TCP.



3.1.1 TCP TAHOE

Podemos ter várias implementações para esta proposta, uma é conhecida como TCP Tahoe que possui um algoritmo denominado de partida lenta, que na verdade não tem nada de lento, pois o seu crescimento é exponencial como pode ser visto na figura 6 e 8. A cada confirmação recebida são

devolvidos 2 pacotes, isto é feito até se alcançar um limite e daí em diante o crescimento é feito de forma linear como é demonstrado na figura 7 e 8.

Figura 6. Partida lenta do TCP Tahoe.

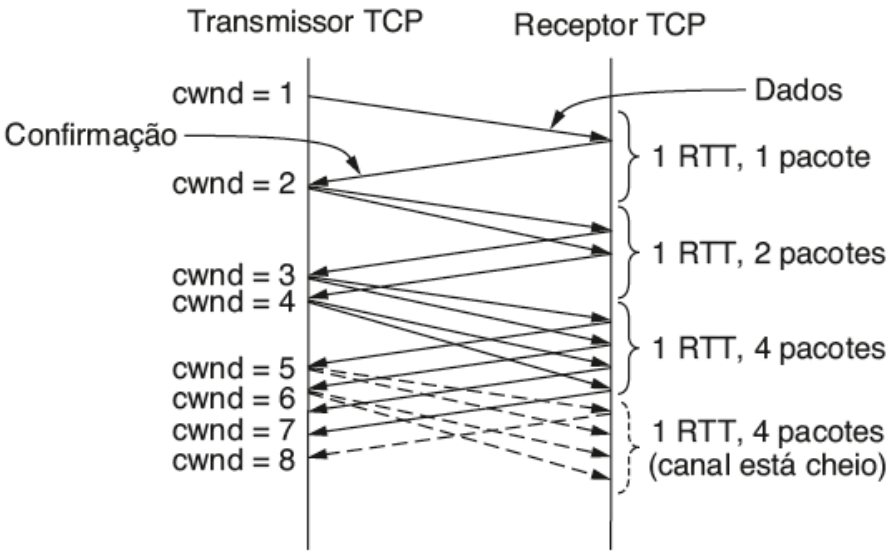
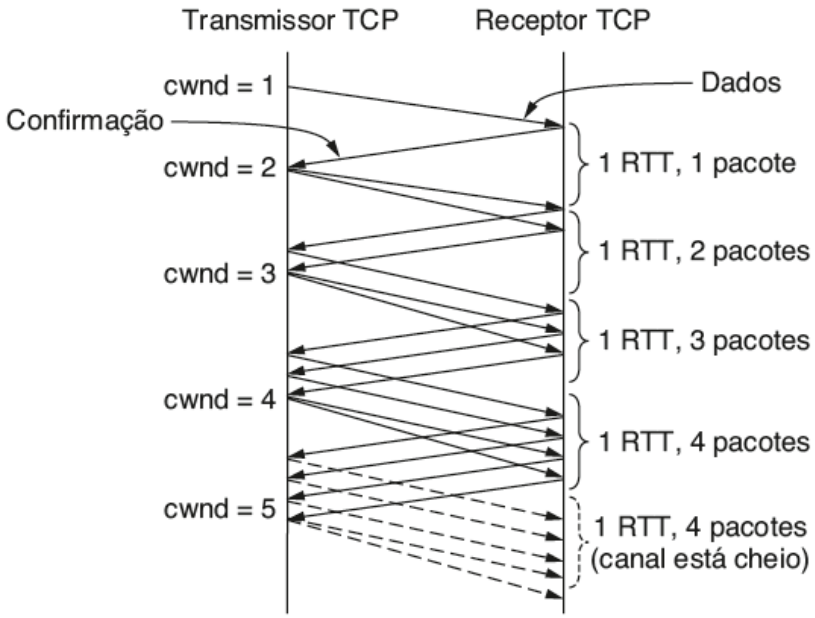
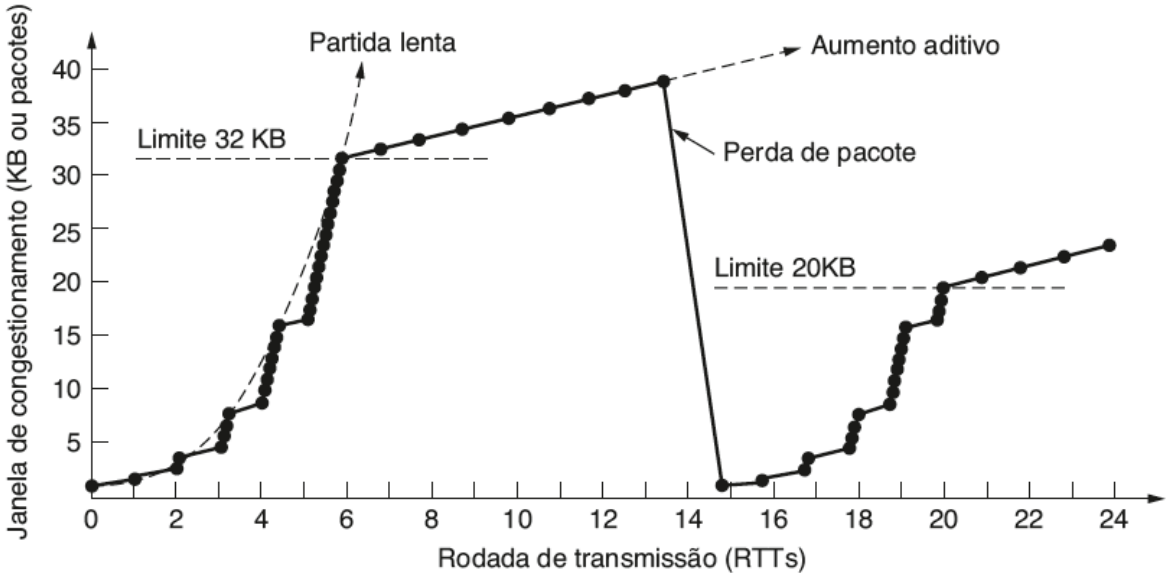


Figura 7. Aumento aditivo TCP Tahoe.



O resultado final da aplicação destes dois processos, crescimento exponencial até um limite e depois linear a partir deste ponto resulta o gráfico da figura 8, onde podemos também observar o efeito quando uma perda de pacotes é detectada. Ao detectar uma perda a taxa de transmissão volta a zero e o limite para o crescimento exponencial é reduzido.

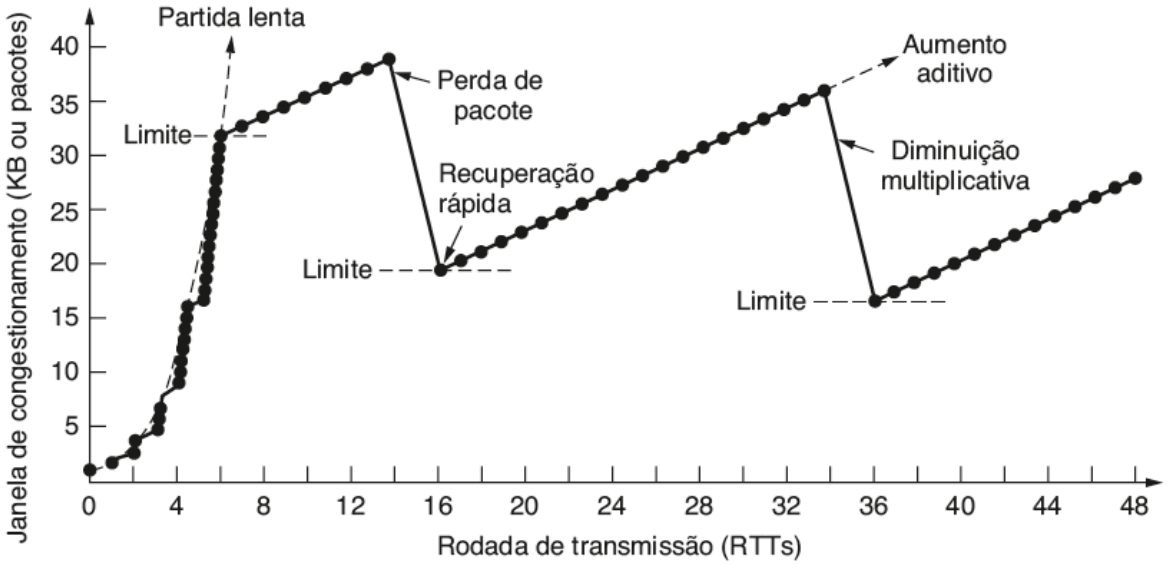
Figura 8. Partida lenta seguida por aumento aditivo no TCP Tahoe



3.1.2 TCP RENO

Outra implementação desta política de redução na taxa de transmissão do TCP é conhecida como TCP Reno. Neste caso, a partida da transmissão também é dita lenta, ou seja, exponencial até determinado ponto e em seguida com crescimento incremental. Ao ser detectada a perda da confirmação a taxa de transmissão é dividida por dois ao invés de voltar a zero! Mas o crescimento volta a ser linear diferente do TCP Tahoe que era exponencial até certo ponto e linear em seguida. A figura 9 representa esta implementação.

Figura 9. Implementação do TCP Reno com Aumento aditivo e decremento multiplicativo (AIMD)



Este modelo é conhecido também como **AIMD** (Additive Increase Multiplicative Decrease – Aumento aditivo e decremento multiplicativo), a figura 9 indica isto a partir do ponto de "perda de pacote" quando a velocidade foi decrementada por uma conta de multiplicação por 0,5 e o crescimento voltou de forma incremental e não mais exponencial como havia sido no começo da transmissão.

3.2 CONTROLE ASSISTIDO PELA REDE

Alguns tipos de rede oferecem controles que emitem pacotes para o destino ou origem reportando explicitamente a ocorrência do congestionamento para que as mesmas tomem providência. Podemos recordar do bit ECN do Frame Relay que podia ser setado no pacote para indicar para os roteadores que a rede estava congestionada e desta forma o roteador poderia procurar por outra rota.

O ATM é outro exemplo com bit no cabeçalho para indicar congestionamento na rede e o propósito é que alguma reação seja tomada pelos roteadores ou mesmo pelos equipamentos que estão gerando o tráfego para que o problema seja corrigido.

Não vamos levantar todas as alternativas existentes aqui neste documento, mas acho importante apontar esta situação que identifica claramente ao host o congestionamento na rede e não deixa que os mesmo suponham a existência do congestionamento pelo fato de uma perda de confirmação.

4 INTSERV

Os controles de congestionamento apresentados no item 3 não garantem em nenhum momento para uma aplicação de que ela terá qualquer um de seus requisitos atendidos. O objetivo das técnicas vistas anteriormente foi manter a rede sem congestionamento, que assim como o trânsito de veículos uma vez congestionado o resultado só tende a piorar para todas as aplicações de forma geral.

Neste momento vamos descrever técnicas que procuram reservar recursos para as aplicações específicas, de forma que os roteadores só aceitam aquele fluxo se eles tiverem condições de atender aos parâmetros de qualidade solicitado pela aplicação, como se fosse um circuito virtual.

IntServ ou Serviços Integrados foi projetado para estabelecer QoS fim-a-fim para fluxos individuais de pacotes, também conhecidos como fluxos (*Flows*). Para tanto, é usado um protocolo de sinalização chamado RSVP (*Resource Reservation Protocol*). Este protocolo exige que os roteadores tenham capacidade de reserva de recursos (buffers, largura de banda) e que mantenham essas informações para cada aplicação que esteja naquele momento mantendo comunicação entre dois pontos da Internet. A reserva de recursos é negociada antes de iniciar a comunicação.

Apenas a título informativo, existem várias RFCs que tratam o assunto, veja uma lista abaixo e o que cada uma trata em linhas gerais:

- RFC 1633 - Integrated Services in the Internet Architecture: an Overview
- RFC 2205 - Resource Reservation Protocol - Version 1 Functional Specification
- RFC 2210 - The Use of RSVP with IETF Integrated Services
- RFC 2211 - Specification of the Controlled-Load Network Element Service
- RFC 2212 - Specification of Guaranteed Quality of Service
- RFC 2215 - General Characterization Parameters for Integrated Services

O IntServ admite duas classes de serviços, ou seja a aplicação ao negociar com os roteadores pode solicitar a reserva de recursos com níveis de exigência distintos, conforme a descrição abaixo:

- Serviços Garantidos: para aplicações que requerem que o atraso dos pacotes não exceda um valor pré-definido, que deve ser garantido.

- *Serviços com carga controlada*: para aplicações que são tolerantes e se adaptam a perdas ocasionais de pacotes

A implementação do IntServ é feita por quatro componentes:

- Protocolo de sinalização (RSVP): é um protocolo de sinalização usado por emissores, receptores e roteadores para reservar recursos na rede e para manter a informação de estado associada, criado em 1993, incluem mensagens de PATH (fornecem aos receptores informações sobre as características do tráfego do(s) emissor(es) e do percurso) e RESV (informam o que o deve ser esperado do tráfego, classe e requisitos). Ou seja, os equipamentos envolvidos naquele trafego ficam mandando estes pacotes na rede para garantir que os recursos serão reservados e mantidos durante toda a comunicação daquela aplicação, por exemplo, uma comunicação voip, uma videoconferência, etc.
- Controle de admissão: como o nome diz o fluxo daquela aplicação só será aceito se o equipamento conseguir atender a reserva solicitada. Por exemplo, para fazer uma vídeo conferência de um ponto A para um ponto B eu preciso de 512 Kbps em todos os trechos se algum dos segmentos não suportar a velocidade a comunicação não terá início.
- Classificador: O classificador identificará a que fluxo cada pacote pertence para conseguir processar o próximo passo.
- Escalonador de pacotes: encaminhar os pacotes atendendo as regras de reserva garantidas durante o protocolo de sinalização.

Aparentemente esta proposta do IntServ implantado, graças ao RSVP, é a oitava maravilha do mundo se não fossem algumas restrições, entre elas podemos enumerar:

- Necessidade de implementação do RSVP em todos os roteadores da rede, transmissores e receptores, realidade não existente na Internet hoje, os roteadores não possuem este software disponível então mesmo que seu computador tenha e o computador do destinatário tenha o RSVP instalado, os equipamentos no meio do caminho não terão suporte.

- Necessidade de implementação de controle de admissão, classificação e escalonamento em todos os roteadores, transmissores e receptores.

- Cada fluxo de comunicação que quisesse ter QoS teria que ser tratado de forma independente pelos roteadores pelos quais fosse passar, a sobrecarga no processamento dos roteadores seria altíssima.

5 DIFFSERV

Apesar de muito boa à solução anterior, a implantação da mesma em larga escala, com a internet é inviável. Mas por quê? Existem "zilhões" de sessões ocorrendo simultaneamente na Internet, será que os roteadores dariam conta de manter informações de reserva de recursos para cada sessão que passasse por ele? Sendo assim, uma variação foi proposta. Ao invés de pensarmos em cada fluxo reservando recurso específico, a reserva é feita para classes de fluxos, por exemplo, reservo 30% do link e processamento para voip, 20% para videoconferência, etc. É claro que isso cria outro problema, quem

garante que não terei tantas aplicações voip concorrendo entre elas que os 30% não seja pouco. É como se fosse à pista de trânsito reservada de ônibus que em certos momentos fica congestionada por causa da quantidade de ônibus trafegando na pista reservada.

Em uma definição mais formal podemos descrever DiffServ ou Serviços Diferenciados como sendo um método utilizado na tentativa de conseguir qualidade de serviço (QoS) em grandes redes, como a Internet, operando sobre grandes volumes de dados em oposição a fluxos ou reservas individuais. A negociação é feita para todos os pacotes de uma determinada classe e os acordos resultantes são chamados de "Acordos de nível de serviço".

Acordos especificam quais as classes de tráfego serão Servidas, as garantias de cada classe e o volume de dados. O transmissor utiliza o campo ToS (*Type of Service)* do cabeçalho IPv4 e *Traffic Class* do cabeçalho IPv6, para atribuir diferentes prioridades aos pacotes. Posteriormente designado de DiffServ Code Point (DSCP) no cabeçalho IP.

Para quem não lembra veja os cabeçalhos do ipv4, o terceiro campo é o Type of Service (ToS) e ipv6 o segundo campo é o Traffic Class na figura 10.

Figura 10. Cabeçalho IPv4 e Ipv6.

Fonte 1. Cisco Sytems

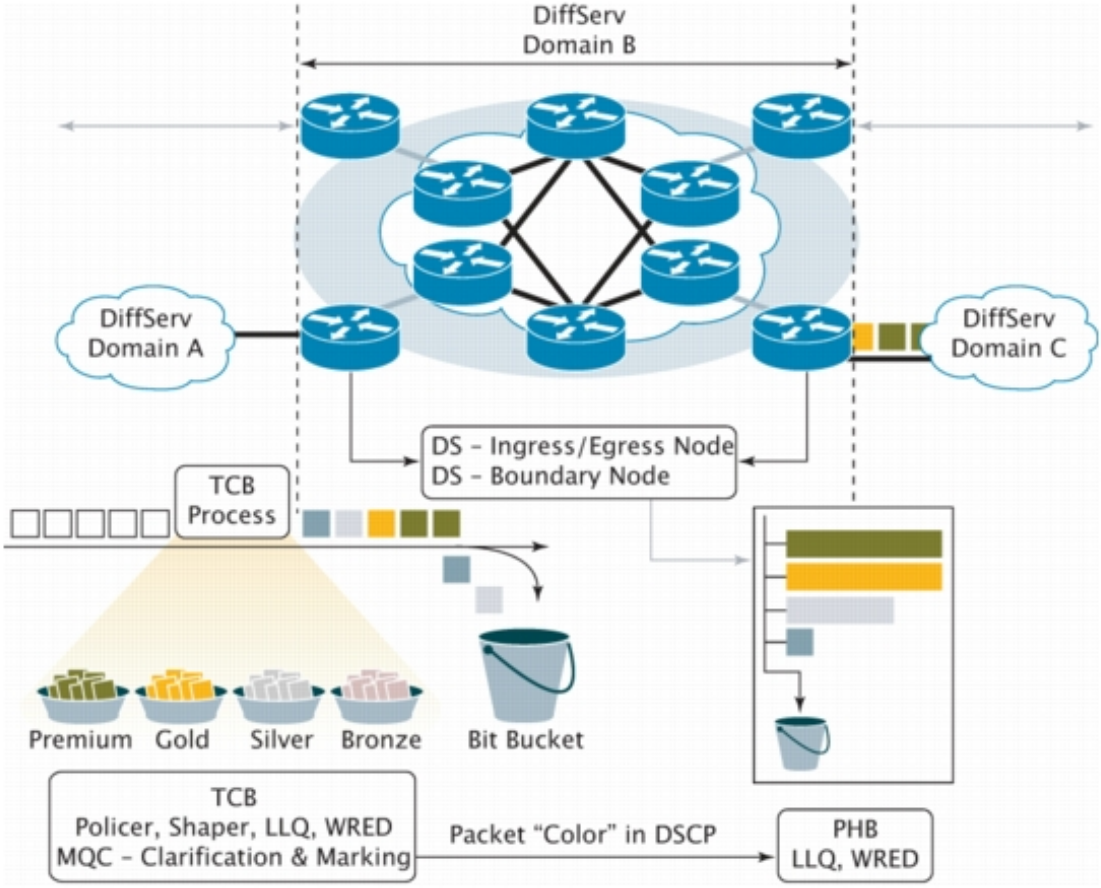
Vou tentar deixar mais claro como as coisas acontecem. Veja a figura 11. Nela temos um domínio DiffServ formada por um conjunto de roteadores que disponibilizam serviço de QoS, nela temos roteadores de borda que fazem a interface com a rede local dos clientes. Nas redes locais até podemos ter tráfego de fluxos individuais em switchs mais poderosos, mas ao chegar ao roteador de borda o tráfego será classificado em classe. Estes Roteadores de borda vão classificar os tráfegos conforme as classes que iremos descrever depois e mandar para os roteadores Core que estão dentro da rede (os roteadores de Core estão dentro do que na figura estão na área de Domínio B). O roteador de borda é o que tem a seta de Domínio A e Domínio C.

Os roteadores de borda vão classificar o tráfego nas categorias:

- **Premium:** Taxa de pico de transmissão e o retardo extremamente baixo. Ex.: Voz e Vídeo.
- **Assegurado:** definido por uma largura de faixa contratada. Pacotes com perfis diferenciados. Pacotes fora de perfil podem ser descartados durante congestionamento. Ex.: Acesso à Banco de Dados
- **Olímpico:** Dividida pelas categorias (Ouro, Prata e Bronze). Em momentos de congestionamento, a categoria ouro irá obter a maior faixa, seguida pela categoria prata e bronze.

Repare na figura 11 que os pacotes vão chegando ao processador TCB no DiffServ Domain A sem classificação (todos estão representados em branco) e saem classificados como Premium, Gold, etc e sendo necessário alguns vão sendo descartados ou colocados em um balde de contenção para dar prioridade as outras classes mais importantes. Uma vez classificados os acordos de serviços vão sendo atendidos e o tráfego entregue no Domínio de destino, em nosso caso no Domínio C.

Figura 11. Fluxo de transmissão do DiffServ



Fonte 2. Cisco Systems

Poderíamos explorar mais o assunto e descrever melhor outros aspectos deste protocolos e outros que existem, mas ficaremos neste ponto em função da ementa sugerida para disciplina, mas este é o futuro da Internet e uma boa área para especialização.