INSTITUTO POLITÉCNICO DE BRAGANÇA
Escola Superior de Comunicação,
Administração e Turismo

Qualidade de Serviço em Redes IP

João Pedro Gomes

Mirandela, 2019

Lição a apresentar na Escola Superior de Comunicação, Administração e Turismo do Instituto Politécnico de Bragança para prestação de provas públicas de avaliação de competência pedagógica e técnico-científica, prevista nos n.º 9, 10 e 11 do artigo 6.º e do n.º 5 do artigo 8.º-A do Decreto-Lei n.º 207/2009, de 31 de agosto, alterado e aditado pela Lei n.º 7/2010, de 13 de maio, e pelo Decreto-Lei n.º 45/2016, de 17 de agosto, alterado pela Lei n.º 65/2017, de 9 de agosto.

Índice

Enquadramento da lição

Enquadramento da lição

Esta lição sobre "**Qualidade de Serviço em Redes IP**" está enquadrada no conteúdo programático da unidade curricular de **Redes de Comunicação III**, lecionada no 2.º semestre do 3.º ano da licenciatura em Informática e Comunicações, na Escola Superior de Comunicação, Administração e Turismo do Instituto Politécnico de Bragança.

Um dos objetivos da licenciatura é a criação de profissionais na área das redes e dos sistemas de computadores. Os principais eixos de formação do curso são as redes e sistemas de computadores, as ciências da computação e os sistemas de informação, sendo o primeiro o mais representativo em termos de créditos ECTS (*European Credit Transfer and Accumulation System*). Integradas no eixo de redes e sistemas de computação estão, entre outras, três unidades curriculares de Redes de Comunicação, lecionadas nos últimos três semestres da licenciatura e alinhadas de forma a proporcionar um encadear natural e complementar das temáticas abordadas. Em Redes de Comunicação I os alunos ficam a conhecer os fundamentos das redes de computadores, o modelo de referência OSI (*Open Systems Interconnection*), a arquitetura TCP/IP (*Transmission Control Protocol*/*Internet Protocol*), e os dispositivos e protocolos de suporte às comunicações em redes de dados e na Internet. Em Redes de Comunicação II o foco são as redes locais e as tecnologias de comutação (*switching*). Em Redes de Comunicação III abordam-se as WAN (*Wide Area Network*) e as tecnologias de encaminhamento (*routing*), complementando-se com a segurança, a gestão de redes e a otimização do tráfego.

É neste último tópico que esta lição se insere, tendo como objetivo promover a obtenção de um dos resultados da aprendizagem e competências estabelecidos na ficha da unidade curricular, a de "perceber a importância da qualidade de serviço numa rede e conhecer as técnicas de implementação" (Imagem 1 e Imagem 2).

Ficha da unidade curricular de Redes de Comunicação III

INSTITUTO POLITÉCNICO DE BRAGANÇA

Unidade Curricular	Redes de Comunicação III	Área Científica	Redes e Sistemas de Computadores
Licenciatura em	Informática e Comunicações	Escola	Escola Superior de Comunicação, Administração e Turismo
Ano Letivo	2018/2019	Ano Curricular	3
Nível	1-3	Créditos ECTS	6.0
Tipo	Semestral	Semestre	2
Código	9188-320-3203-00-18		

Horas totais de trabalho	162	Horas de Contacto	T	TP	PL	TC	S	E	OT	O
			15	-	45	-	-	-	20	-

T - Ensino Teórico; TP - Teórico Prático; PL - Prático e Laboratorial; TC - Trabalho de Campo; S - Seminário; E - Estágio; OT - Orientação Tutórica; O - Outra

Nome(s) do(s) docente(s): João Pedro Carneiro Borges Gomes

Resultados da aprendizagem e competências

No fim da unidade curricular o aluno deve ser capaz de:
1. planear e implementar encaminhamento dinâmico usando diversos protocolos de encaminhamento;
2. conhecer as principais tecnologias WAN disponíveis e saber indicar a mais apropriada em cada situação;
3. conhecer tecnologias de acesso remoto e saber implementá-las de forma segura;
4. conhecer soluções para monitorização de uma rede e saber implementá-las;
5. perceber a importância da qualidade de serviço numa rede e conhecer as técnicas de implementação;
6. conhecer e saber usar metodologias e ferramentas de diagnóstico para otimizar e resolver problemas na rede.

Pré-requisitos

Antes da unidade curricular o aluno deve ser capaz de:
1. conhecer os fundamentos das redes de computadores (Unidade curricular: Redes de Comunicação I);
2. compreender a arquitetura TCP/IP e o endereçamento IP (Unidade curricular: Redes de Comunicação I);
3. saber configurar routers e switches (Unidade curricular: Redes de Comunicação II).

Conteúdo da unidade curricular

Projeto de redes. Estudo e configuração de diversas tecnologias e serviços WAN. Acesso remoto seguro. Gestão de redes e otimização de tráfego. Monitorização, medição e registo de utilização de redes. Metodologias e ferramentas para resolução de problemas em rede.

Conteúdo da unidade curricular (versão detalhada)

1. Encaminhamento dinâmico
   - Protocolos de encaminhamento dinâmico
   - Encaminhamento dinâmico de vetor distância
   - Encaminhamento dinâmico de estado de ligação
2. Enhanced Interior Gateway Routing Protocol (EIGRP)
   - Caraterísticas
   - Operação
   - Implementação em IPv4 e IPv6
   - Configurações avançadas
   - Identificação e resolução de problemas
3. Open Shortest Path First (OSPF)
   - Caraterísticas
   - OSPF de área única
   - OSPF multiárea
   - Configurações avançadas
   - Identificação e resolução de problemas
4. Tecnologias WAN
   - Descrição e funcionamento
   - Infraestruturas
   - Seleção de tecnologias
5. Ligações Ponto-a-Ponto
   - Comunicações série
   - Point-to-Point Protocol (PPP)
   - Implementação do PPP
   - Identificação e resolução de problemas
6. Soluções de acesso remoto
   - Conexões de banda larga
   - Point-to-Point Protocol over Ethernet (PPPoE)
   - Redes Privadas Virtuais (VPN)
   - Generic Routing Encapsulation (GRE)
   - Border Gateway Protocol (BGP)
7. Listas de controlo de acesso (ACL)
   - ACL IPv4 estendidas
   - ACL IPv6
   - Identificação e resolução de problemas
8. Segurança e Monitorização
   - Segurança em redes locais
   - Simple Network Management Protocol (SNMP)
   - Monitorização
   - Soluções e Ferramentas
9. Qualidade de Serviço (QoS)
   - Requisitos
   - Modelos
   - Técnicas de implementação
10. Evolução das redes
    - Internet das Coisas (IoT)
    - Computação em nuvem e virtualização
    - Redes definidas por software (SDN)
11. Identificação e resolução de problemas na rede
    - Documentação
    - Metodologias
    - Contratos de nível de serviço (SLA)
    - Ferramentas

Imagem 1: Ficha da Unidade Curricular de Redes de Comunicação III (pág. 1)

Bibliografia recomendada

1. Odom, W. (2016). CCNA Routing and Switching ICND2 200-105 Official Cert Guide. Cisco Press. ISBN-13: 978-1587205798
2. Véstias, M. (2016). Redes Cisco - Para Profissionais (7. ª Edição Atualizada). FCA. ISBN-13: 978-972-722-828-7
3. Donahue, G. A. (2011). Network Warrior, Second Edition. O'Reilly. ISBN-13: 978-1-449-38786-0
4. Deveriya, A. (2005). Network Administrators Survival Guide. Cisco Press. ISBN-13: 978-1587052118

Métodos de ensino e de aprendizagem

Realização de aulas expositivas, demonstrações, análise e discussão de casos, atividades multimédia interativas, atividades laboratoriais, trabalhos práticos e aulas de orientação tutórica. Utilização de salas laboratoriais de redes de computadores, simuladores e plataformas de aprendizagem eletrónica.

Alternativas de avaliação

1. Contínua - (Ordinário, Trabalhador) (Final)
   - Prova Intercalar Escrita - 40% (3 provas. Nota global mínima de 8 valores. Opcional: Academia Cisco (Testes: 10%; Exame final: 10%))
   - Trabalhos Práticos - 60% (Nota mínima de 8 valores)
2. Exame final - (Ordinário, Trabalhador) (Recurso, Especial)
   - Exame Final Escrito - 40% (Nota mínima de 8 valores. Opcional: Academia Cisco (Exame final: 20%))
   - Trabalhos Laboratoriais - 60% (Nota mínima de 8 valores)

Língua em que é ministrada

Português, com apoio em inglês para alunos estrangeiros

Validação Eletrónica

João Pedro Carneiro Borges Gomes	Carlos Filipe Campos Rompante da Cunha	Vítor José Domingues Mendonça	Luisa Margarida Barata Lopes
06-03-2019	11-03-2019	28-03-2019	31-03-2019

Imagem 2: Ficha da Unidade Curricular de Redes de Comunicação III (pág. 2)

Sumário e texto da lição

INSTITUTO POLITÉCNICO DE BRAGANÇA
Escola Superior de Comunicação,
Administração e Turismo

Qualidade de Serviço em Redes IP

Texto da lição

João Pedro Gomes

Mirandela, 2019

Agradecimentos

Agradeço à minha família pelo companheirismo, serenidade e amor que sempre me proporcionaram.

Aos colegas e amigos do Departamento de Informática e Matemática da EsACT-IPB, por todo o apoio, amizade e partilha de saberes.

Índice

Índice de figuras

Índice de tabelas

1. Introdução

As primeiras redes de comunicação de dados a longa distância foram implementadas aproveitando-se as redes públicas telefónicas comutadas (PSTN). Estas redes, projetadas para o tráfego de voz, baseavam-se no princípio da comutação de circuitos, oferecendo uma largura de banda fixa, de baixa capacidade, durante toda a sessão e uma comunicação com latência desprezável. No entanto, na comunicação entre computadores temos, tipicamente, tráfego em rajada, alternando períodos de envio intenso de dados com períodos sem transmissão de dados, caraterística que não permite obter uma utilização eficiente deste tipo de redes pois inviabiliza a sua utilização por outros dispositivos em momentos de pausa.

Posteriormente, começaram a ser implementadas redes de computadores baseadas no princípio da comutação de pacotes, onde os dados são divididos e enviados em pedaços (pacotes) sendo processados e encaminhados individualmente nos dispositivos da rede ao longo de trajetos independentes. Isto permite uma utilização muito mais eficiente da rede, pois não são feitas reservas de largura de banda sendo a mesma partilhada pelos diversos fluxos de dados, mas pode provocar atrasos na comunicação. Este tipo de redes é a predominante atualmente, fruto da sua flexibilidade e viabilidade económica.

A massificação da Internet e dos seus protocolos, nomeadamente o Internet Protocol (IP), suportado por uma grande diversidade de tecnologias físicas de rede, criou as condições para a existência de uma rede global multiserviços, integrando gradualmente transmissões de dados, voz e vídeo numa única plataforma de comunicação e promovendo a convergência de redes e de serviços. Para os utilizadores, essa convergência significa conveniência, flexibilidade e a possibilidade de acesso a novos serviços.

Porém, a transmissão de tráfego com caraterísticas e requisitos tão diferentes através da mesma infraestrutura, com capacidade limitada e com níveis de utilização cada vez maiores, levanta um desafio. Como garantir que a experiência na utilização de cada um dos serviços seja comparável à existente anteriormente, com infraestruturas diferenciadas e otimizadas para cada um deles? A implementação de mecanismos de **qualidade de serviço (*Quality of Service* – QoS)** numa rede permite tratar o tráfego de uma forma diferenciada em função dos seus requisitos, permitindo ir ao encontro das necessidades das aplicações e/ou dos utilizadores. Além disso, possibilita às organizações darem um tratamento menos prioritário ao tráfego que não esteja relacionado com as suas atividades, otimizando a utilização das suas infraestruturas de capacidade limitada e garantindo que as aplicações que lhes são importantes tenham o desempenho adequado (Roughan et al. 2004).

Com o aperfeiçoamento e a evolução tecnológica nos últimos anos o uso da QoS aumentou, sendo considerado agora uma parte necessária da operação e do desenho da rede (Barreiros and Lundqvist 2016). Numa infraestrutura de rede a QoS é uma tecnologia fundamental, tal como a segurança e a alta disponibilidade o são (Szigeti et al. 2013). E, apesar dos seus fundamentos se manterem bastante estáveis, os seus mecanismos têm evoluído e adaptado às novas necessidades técnicas e organizacionais, e as estratégias para a sua implementação têm-se modificado para lidar com as novas tendências do tráfego, cada vez mais complexo e exigente, maioritariamente de vídeo e suportado por redes móveis e sem fios.

Métricas de desempenho

O desempenho de uma rede pode ser aferido por diversas métricas, salientando-se:

- **Largura de banda**: a quantidade de bits que pode ser enviada por segundo através de uma ligação física.
- **Latência (ou atraso)**: o tempo que um pacote demora a chegar ao destino.
- **Variação da latência (ou *jitter*)**: A diferença do atraso na chegada de sucessivos pacotes pertencentes ao mesmo fluxo de dados (sendo um fluxo o conjunto de dados trocados entre as mesmas aplicações, ou seja, com os mesmos endereços IP e portos, tanto de origem como de destino, num determinado período de tempo).
- **Perda de pacotes**: A quantidade de pacotes que não chegam ao destino, tipicamente indicada em percentagem.

Cada uma destas caraterísticas influenciam o tráfego, com maior ou menor impacto dependendo da natureza das aplicações, e o objetivo da utilização de mecanismos de QoS na rede é minimizar esse impacto no tráfego mais sensível. Algumas das estratégias passam por dar prioridade a esse tráfego mais sensível para manter o atraso num valor baixo e estável, reservando-lhes recursos da rede, de forma a garantir a largura de banda que necessitam e, no caso de ser necessário descartar pacotes, fazendo-o seletivamente no tráfego menos sensível a perdas.

Tipos de tráfego e as suas caraterísticas

O tipo de tráfego maioritariamente transmitido nas redes tem variado ao longo do tempo. Os dados e a voz, predominantes no passado, deram lugar ao vídeo como principal tipo de tráfego nas redes IP, e as comunicações por dispositivos móveis e sem fios superaram as comunicações de dispositivos fixos.

Segundo previsões da Cisco, em 2022 o vídeo será responsável por 82% de todo o tráfego IP (Figura 1.1) e 71% de todo o tráfego será feito sobre redes móveis e sem fios (Cisco Systems 2019).

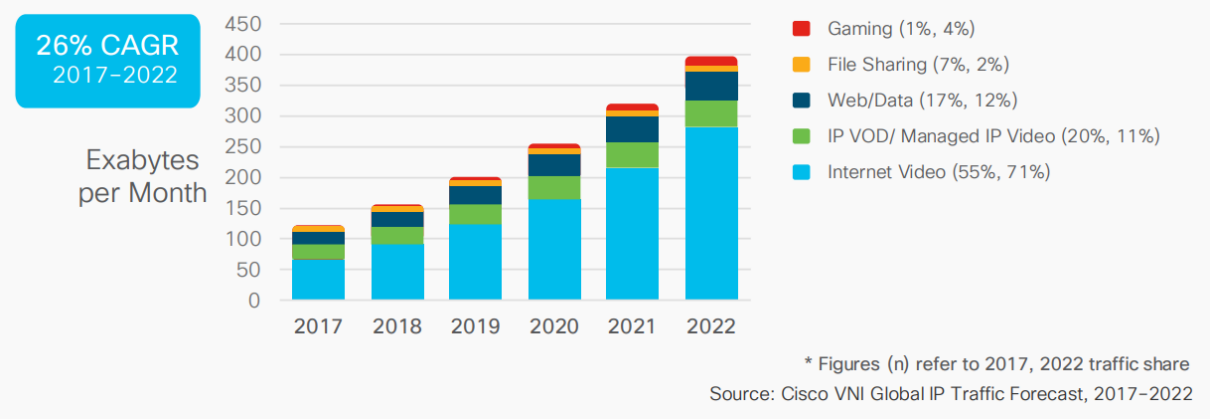

Figura 1.1:Tráfego IP global por categoria de aplicação
(Cisco Systems 2019)

A Figura 1.2 mostra uma caraterização típica do tráfego de voz, vídeo e dados, permitindo ilustrar como cada tipo tem diferentes requisitos de desempenho da rede.

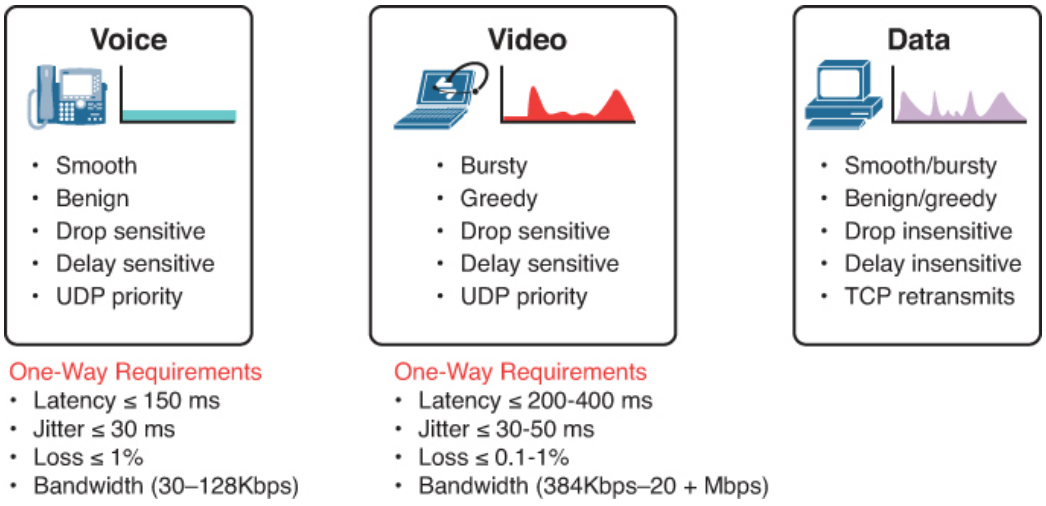

Figura 1.2:Caraterização dos principais tipos de tráfego
(Szigeti et al. 2013)

As caraterísticas indicadas para cada um destes tipos de tráfego pretendem apenas dar uma visão geral das suas diferenças. De facto, em cada um dos tipos podemos identificar muitas variantes em função da aplicação concreta. Por exemplo, no vídeo temos o caso do *streaming* (unidirecional, menos sensível ao *jitter* pela utilização de técnicas de *buffering*), da videoconferência (bidirecional e sensível ao *jitter*), entre outros.

A utilização de mecanismos de QoS numa rede permite assegurar que as diferentes aplicações obtenham os requisitos de desempenho necessários para que o utilizador final as

use de forma satisfatória. A QoS percecionada pelo utilizador, juntamente com outros fatores, é designada por **Qualidade de Experiência (QoE)**.

A quantificação da QoE é mais difícil do que da QoS, pois está dependente da subjetividade individual dos utilizadores. No entanto, a sua compreensão é fundamental para perceber quais as métricas de QoS necessárias para garantir uma boa experiência de utilização de cada aplicação.

Para permitir que o utilizador tenha a melhor experiência, é importante que haja uma abstração da própria rede e dos seus efeitos no tráfego, sendo necessário que os mecanismos de QoS funcionem ao longo de toda a rede e não apenas em parte dela. Isso não é fácil de conseguir nas redes atuais, pois estas são dinâmicas e heterogéneas, transportando tráfego das mais variadas aplicações através de diferentes tipos de tecnologia.

Para tentar resolver esta questão foram desenvolvidos vários modelos de QoS.

Modelos de QoS

Inicialmente foi proposto o modelo de **Serviços Integrados (*Integrated Services* – IntServ)**. O objetivo seria garantir a entrega dos pacotes de uma sessão através de uma reserva prévia de recursos em cada dispositivo de rede, com a indicação da largura de banda necessária e do atraso máximo permitido. Isto possibilitaria que um fluxo de dados tivesse assegurada a QoS logo de início e ao longo de toda a sessão. Não obstante, a sua implementação na Internet não é praticável pela já referida heterogeneidade da rede, entre outros motivos.

Mais tarde, o modelo de **Serviços Diferenciados (*Differentiated Services* – DiffServ)** foi desenvolvido para tentar ultrapassar essa dificuldade de implementação, através de uma abordagem mais flexível e escalável. Para tal, cada dispositivo de rede tentaria fazer um tratamento diferenciado do tráfego de acordo com as ferramentas disponíveis em cada dispositivo, sem a rigidez do IntServ mas, em contrapartida, sem oferecer a mesma garantia de QoS.

Nas infraestruturas de rede atuais o modelo DiffServ é o mais usado para obtenção de QoS, dada a sua adaptabilidade. No entanto, em contextos mais exigentes, como é o caso das redes sem fios 802.11, com a sua largura de banda variável, das redes com largura de banda escassa ou das redes com grande volume de tráfego sensível a atrasos e ao jitter, o DiffServ está a ser complementado por algumas caraterísticas do IntServ que lidam melhor com estes constrangimentos. E, dada a realidade atual, com uma utilização cada vez maior das redes sem fios e da transmissão de vídeo é de esperar que esta complementaridade seja cada vez mais explorada.

Mecanismos do QoS

Cada dispositivo de rede preparado para implementar o modelo DiffServ dispõe de diversos mecanismos que lhes permite promover a QoS na rede, podendo ser usados todos ou apenas alguns para se atingirem os objetivos de desempenho da rede pretendidos.

A passagem dos pacotes por estes mecanismos, desde a entrada até à saída de um equipamento de rede, está ilustrada na Figura 1.3. No entanto, os pacotes poderão ser sujeitos apenas a parte deste processo.

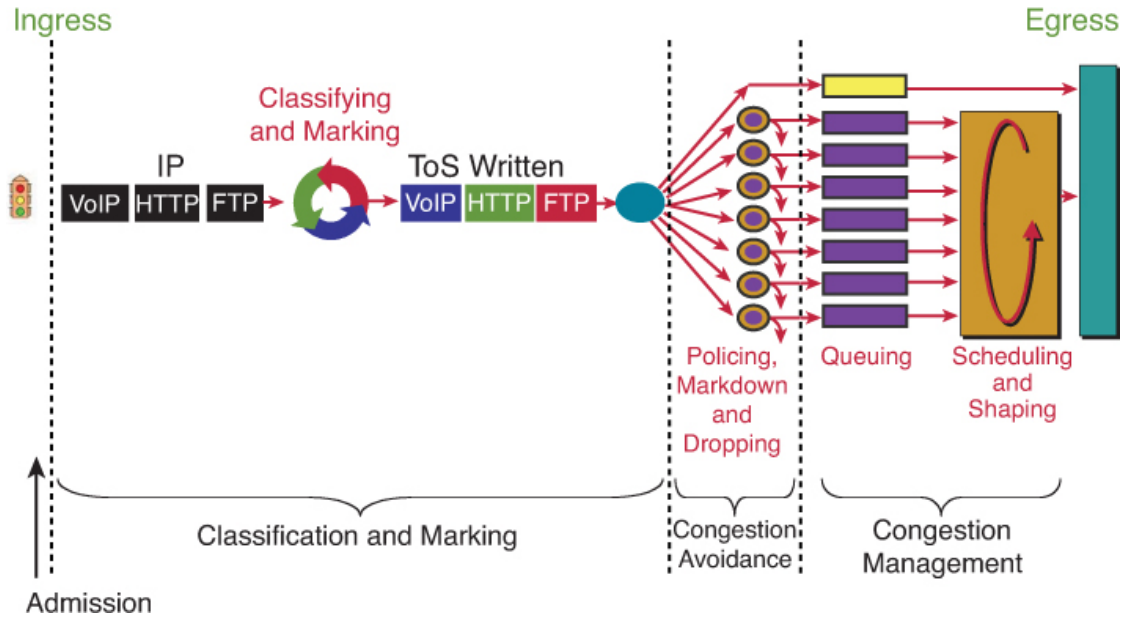

Figura 1.3: Mecanismos de QoS num dispositivo de rede (Szigeti et al. 2013)

Ao chegarem à interface de entrada os pacotes passam por uma fase de **classificação e marcação**. A **classificação** tem como objetivo a atribuição de uma classe de tráfego ao pacote ou pacotes de determinado fluxo, de acordo com os seus requisitos ou com as políticas da organização. Essa classe vai determinar o tipo de tratamento dado ao pacote posteriormente. Por exemplo, o tráfego de uma chamada de voz e o tráfego web deverão pertencem a classes diferentes pois têm necessidades de QoS diferentes. Após a classificação passa-se à **marcação** dos pacotes, através da escrita de campos específicos dos seus cabeçalhos, para que posteriormente se possa identificar facilmente a classe a que pertencem. Tanto os pacotes IPv4 como os pacotes IPv6 têm um campo específico para tal. A marcação também pode ser feita nos cabeçalhos de protocolos da camada 2, nomeadamente nos quadros 802.1Q usados nas ligações de tronco para identificação de VLAN em redes Ethernet, havendo normalmente coerência entre as marcações feitas nas diferentes camadas.

A fase seguinte tem como objetivo **evitar o congestionamento**. Para tal, a cada classe de tráfego é atribuída parte dos recursos da rede e o tráfego é monitorizado de forma a garantir que esses recursos não são excedidos. Caso tal aconteça, os pacotes são **descartados**

(técnicas de **policiamento**) ou então **atrasados**, através do envio para uma fila de espera, de modo a não ultrapassarem os limites de tráfego estabelecidos (técnicas de **modelação – *shaping***). Uma outra alternativa nesta fase é os pacotes sofrerem uma despromoção e sejam alvo de uma **remarcação** para uma classe de serviço de menor prioridade

Se a largura de banda não for suficiente para todo o tráfego a transmitir passa-se à fase de **gestão de congestionamento**, com a colocação dos pacotes em filas de espera, de acordo com a sua classe de tráfego, até haver disponibilidade para o seu envio. O tratamento dos pacotes nas várias filas é feito de acordo com determinado algoritmo de **escalonamento**, segundo um sistema de prioridades. As técnicas de moldagem, referidas no parágrafo anterior, são particularmente úteis para garantir o cumprimento de contratos de níveis de serviço (*Service Level Agreement* – SLA), agindo perante picos de tráfego e retendo os pacotes em excesso até haver novamente disponibilidade para os transmitir.

Classes de tráfego

Assim, para que o tráfego seja tratado de forma diferenciada é necessário primeiro definir como fazer essa divisão do tráfego em diferentes classes e quais os recursos a associar a cada uma. O RFC 4594 ((Babiarz, Chan, and Baker 2006) propõe o mapeamento dos diferentes tipos de tráfego em 12 classes (modelo à esquerda na Figura 1.4), numa tentativa de padronizar a sua utilização e facilitar a interoperabilidade entre redes sob diferentes administrações e entre equipamentos de diferentes fabricantes. No entanto, em muitas situações não se justifica uma divisão em tantas classes, pelo que nesses casos se faz uma divisão mais genérica. É o caso dos restantes modelos da Figura 1.4 em que o tráfego é dividido em 8 (modelo ao centro) ou em 4 classes (modelo à direita), segundo esquemas propostas pela Cisco para simplificar a implementação quando o contexto não justifica tanta granularidade.

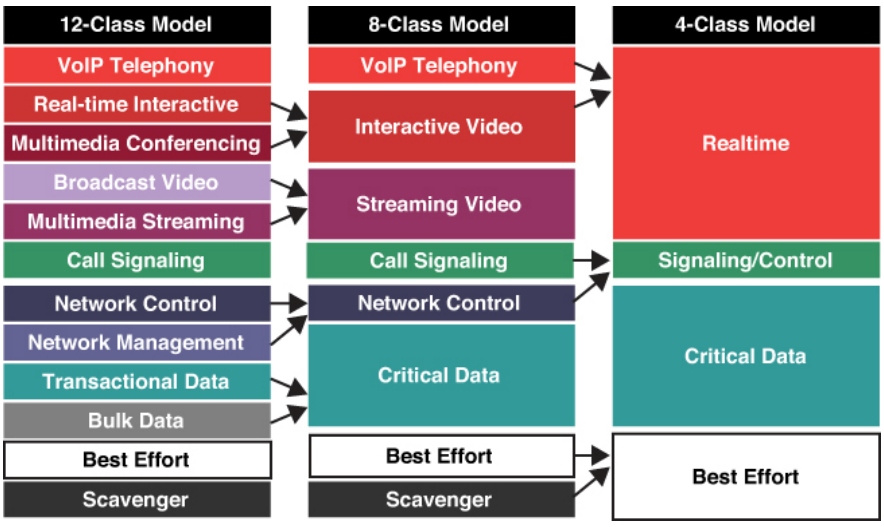

Figura 1.4: Modelos de classes de tráfego
(Szigeti et al. 2013)

2. Aplicações e desempenho da rede

Para um projeto adequado de uma solução de QoS numa rede é importante conhecerem-se as principais categorias de aplicações, os seus requisitos gerais e as recomendações de métricas a atingir na rede.

2.1. Métricas de desempenho da rede

As caraterísticas de uma rede que influenciam a QoS são a **largura de banda** disponível, o **atraso** sofrida pelos pacotes, a **variação do atraso (*jitter*)** da chegada entre pacotes e a **perda** ou erro de pacotes.

2.1.1. Largura de banda

A largura de banda é um recurso limitado e um dos fatores mais impactantes no tráfego pois a sua insuficiência provoca a degradação dos valores de outras métricas de avaliação de desempenho. Com efeito, se não houver largura de banda suficiente para transmitir todo o tráfego existente num dado momento surge um congestionamento na rede, obrigando os dispositivos a reterem temporariamente os pacotes até haver disponibilidade da sua transmissão, o que provoca o seu atraso. E, como o tempo de retenção não é constante para os vários pacotes, a variação desse atraso (*jitter*) deixa de ser nula. Além disso, se a memória disponível para o armazenamento temporário for insuficiente para todos os pacotes que entram no dispositivo ou se o tempo de retenção for excessivo pode mesmo levar ao descarte de pacotes.

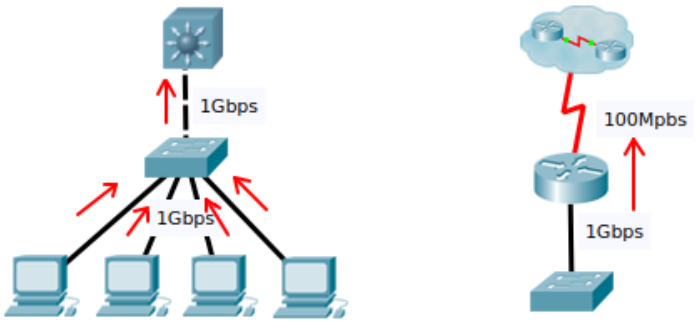

Figura 2.1: Pontos de congestionamento

Alguns dos pontos de congestionamento típicos ocorrem quando o tráfego de várias ligações converge para uma única ligação com largura de banda inferior à soma da largura de

banda das ligações agregadas, frequente em ligações de *backbone* (diagrama à esquerda da Figura 2.1), ou quando as ligações de um equipamento não têm todas a mesma largura de banda e o tráfego flui de uma ligação com maior largura de banda para uma com menor largura de banda, como acontece frequentemente na transição de LAN para WAN (diagrama à direita da Figura 2.1).

Os requisitos de largura de banda variam muito com o tipo de aplicação. Por exemplo, uma aplicação de transmissão de vídeo em alta definição exige muito mais largura de banda que uma aplicação de troca de mensagens de texto.

2.1.2. Atraso ou latência

O atraso ou latência de um pacote na rede pode ser definido como o tempo que demora desde que o primeiro bit do pacote é transmitido no dispositivo de origem até que o último bit do pacote é recebido no dispositivo de destino (Almes, Kalidindi, and Zekauskas 2016).

Esse atraso é causada por vários fatores, como ilustrado na Figura 2.2, nomeadamente:

- **Tempo de transmissão ou serialização**, o tempo que a origem demora a transmitir todos os bits do pacote. Pode ser significativo em ligações de baixa velocidade (*e.g.*, numa ligação de 1 Mbps um pacote de 1500 bytes demora 12 ms a ser transmitido).
- **Tempo de propagação**, o tempo que o sinal demora a propagar-se na ligação. Pode ser significativo em distâncias muito grandes (tipicamente 5 ms por cada 1.000 Km de fibra ótica).
- **Tempo de processamento e enfileiramento**, o tempo que um pacote demora num equipamento de rede até ser retransmitido. Inclui o tempo de encapsulamento/desencapsulamento, verificação de erros, determinação de rota, aplicação de listas de controlo de acesso, filas de espera, entre outro processamento. Varia com o tipo de equipamento e o congestionamento existente na rede.

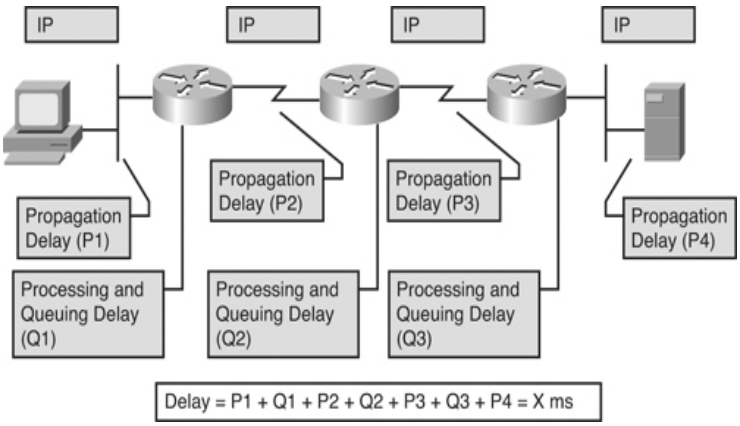

Figura 2.2: Latência na rede
(Wallace and Wallace 2011)

É importante perceber que o atraso na rede é diferente do atraso fim-a-fim entre aplicações. Este último consiste no tempo que passa entre o envio dos dados pela aplicação de origem até à sua receção pela aplicação de destino. Este atraso adiciona ao atraso na rede o atraso sofrido nos equipamentos terminais e é mais útil quando se pretende avaliar a qualidade de experiência do utilizador.

Outra forma frequente de representar o atraso, muito útil em aplicações interativas, é pelo tempo que um pacote demora a ir do dispositivo A ao dispositivo B, a ser processado no dispositivo B, e a que o pacote de resposta vá do dispositivo B novamente ao dispositivo A. A esse tempo dá-se o nome de *Round Trip Time* (RTT).

Aplicações de tempo real (chamadas de voz, por exemplo) ou que requerem interatividade são particularmente sensíveis aos atrasos. Tipicamente, para aplicações de tempo real o atraso fim-a-fim, entre aplicações, deverá ser inferior a 150ms (100ms para o atraso da rede) não sendo conveniente que ultrapasse os 400ms para aplicações interativas.

2.1.3. Variação da latência (*jitter*)

É frequente que pacotes de um mesmo fluxo de dados, mesmo que enviados com o mesmo intervalo de tempo, cheguem ao destino com diferentes atrasos pois o tempo que demoram em cada dispositivo intermédio é variável além de poderem seguir caminhos diferentes.

À variação do atraso dos diversos pacotes de um mesmo fluxo também dá-se o nome de instabilidade ou *jitter*. É usual que o cálculo dessa variação seja feito tendo como referência o pacote com menor atraso.

Aplicações de *streaming* de vídeo e de áudio são altamente sensíveis a esta instabilidade, sendo usual a utilização de técnicas de *buffering* para a minimizar, como explicado mais à frente, na secção 2.2.1. .

Como referência, uma variação fim-a-fim de menos de 50ms costuma ser apropriada para qualquer tipo de aplicação.

2.1.4. Perda de pacotes

A **fiabilidade** de uma rede mede a percentagem de pacotes que chegam ao destino sem erros. Um dos principais fatores que impedem os pacotes de chegar ao destino é o congestionamento da rede, situação em que os dispositivos intermédio ficam sobrecarregados e sem capacidade para armazenar novos pacotes, o que leva ao seu descarte.

Aplicações que não toleram a perda de dados recorrem à retransmissão dos pacotes perdidos ou com erros (como aquelas que usam o TCP como protocolo de transporte) garantindo, desta forma, a fiabilidade em troca de um maior atraso na receção dos dados.

No entanto, aplicações de tempo real não podem recorrer a essa estratégia por serem sensíveis ao atraso. Mas, normalmente, estas aplicações toleram alguma perda de dados desde que seja mínima.

É importante ter em consideração a diferença entre a perda de pacotes na rede e a perda de dados das aplicações. Uma aplicação de correio eletrónico não tolera a perda de dados mas tolera a perda de pacotes na rede pois estes podem ser retransmitidos e os dados acabarão por chegar ao destino.

2.2. Tipos de aplicações

Segundo Szigeti et al. (2013), para a generalidade dos casos é possível agrupar as principais aplicações em cinco categorias principais: **voz**, **vídeo**, **multimédia**, **dados** e **controlo**, que por sua vez podem ser divididas em algumas subcategorias, cada uma com as suas caraterísticas e requisitos, como mostra a Tabela 2.1.

Tabela 2.1: Classes de aplicação, caraterísticas e requisitos

Aplicação		**Tráfego**	**Caraterísticas e requisitos (num sentido)**			
Categoria	**Subcategoria**		**Latência**	**Jitter**	**Perda**	**Largura de banda**
Voz		Suave e benigno	Muito sensível ≤ 150 ms	Muito sensível ≤ 30 ms	Sensível ≤ 1 %	Garantia ao fluxo 20 – 320 kbps
Vídeo	*Broadcast*		Não sensível	Não sensível	Muito sensível ≤ 0,1 %	Garantia ao fluxo
	Interativas em tempo real		Muito sensível ≤ 200 ms	Muito sensível ≤ 50 ms	Muito sensível ≤ 0,1 %	Garantia ao fluxo
Multimédia	*Streaming*		Sensível ≤ 400 ms			Garantia ao fluxo (recomendado)
	Conferência		Muito sensível ≤ 200 ms		Sensível ≤ 1 %	Garantia ao fluxo
Dados	Transacional	Baixa latência	Sensível			Garantia à classe
	Em massa	Alto débito	Não sensível			Garantia à classe
	Melhor esforço	Restante tráfego	Não sensível			
	Predadora (*scavenger*)	Baixa prioridade				

Para que um utilizador consiga usar, de forma satisfatória, os diversos tipos de aplicações é necessário que a rede possa satisfazer os requisitos necessários a cada uma delas. Existem vários sítios que disponibilizam testes de qualidade de ligação que podem ser usados por utilizadores comuns, sem grandes conhecimentos técnicos. A Autoridade Nacional de Comunicações (ANACOM) disponibiliza um desses testes (https://netmede.pt/) onde, após a sua realização, apresenta um relatório com exemplos de serviços para os quais a ligação é considerada adequada, tendo como referência os valores constantes na Tabela 2.2.

Tabela 2.2: Parâmetros de desempenho aconselháveis

("Pergunte à ANACOM - Portal Do Consumidor" n.d.)

	Streaming de vídeo	**Streaming de música**	**Chamadas de voz e de vídeo**	**Jogos online em rede**	**Navegação interativa**
Velocidade download	SD > 2 Mbps Full HD > 5 Mbps 4K > 25 Mbps	> 1 Mbps	Voz > 150 Kbps Vídeo > 1 Mbps	> 5 Mbps	> 2 Mbps
Velocidade upload	-	-	Voz > 150 Kbps Vídeo > 1 Mbps	> 2 Mbps	-
Latência (*Round Trip Time*)	< 150 ms	< 150 ms	< 100 ms	< 50 ms	< 100 ms
Jitter	< 50 ms	< 50 ms	< 20 ms	< 10 ms	< 50 ms

Os valores da tabela baseiam-se em elementos da UIT-T Recommendation G.1010 e ETSI TR 102 805-1 v.1.1.1 (atendendo também às evoluções entretanto verificadas nos serviços) e em informação publicamente disponível sobre parâmetros de desempenho aconselháveis para determinados serviços e aplicações, complementada em alguns dos serviços por uma verificação em laboratório.

2.2.1. Voz

Os algoritmos normalmente aplicados na codificação de voz geram pacotes com tamanho e cadência constante (Figura 2.3), permitindo a previsibilidade da largura de banda necessária para a sua transmissão. A largura de banda necessária será função do *codec* usado no processo de codificação.

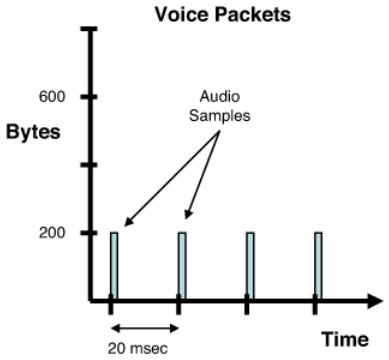

Figura 2.3: Tráfego de voz

(Szigeti et al. 2013)

Já a latência, o *jitter* e a perda de pacotes são aspetos sensíveis para o tráfego de voz, havendo apenas uma tolerância limitada.

Demasiado atraso na receção pode fazer com que as pessoas falem em simultâneo pois o destinatário pode interpretar o silêncio sentido como sendo a sua vez de falar.

A perda de pacotes provoca cortes na voz. Dada a impossibilidade prática de retransmissão de pacotes perdidos, pela sensibilidade ao atraso, uma das técnicas usadas para minimizar este problema é a de, no destino, substituir os pacotes perdidos com base no último pacote recebido, o que só é eficaz com perdas mínimas de pacotes.

Para lidar com o *jitter* a solução passa pela utilização de *buffers* que armazenam temporariamente os pacotes. Apesar de aumentar o valor do atraso total dos mesmos, isso permite disponibilizar os dados às aplicações a uma taxa constante, ocultando a variação do atraso ao utilizador (Figura 2.4).

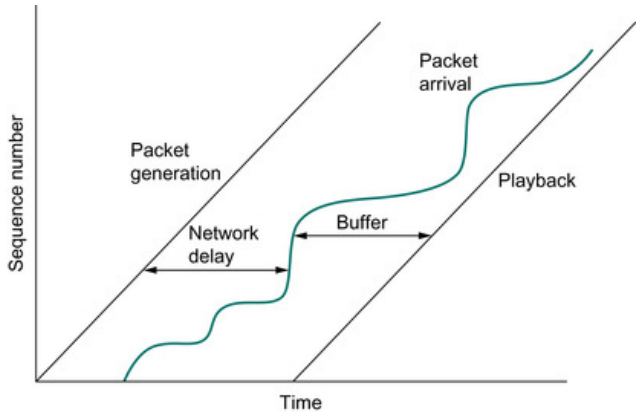

Figura 2.4: Utilização de buffers para eliminar o jitter
(Peterson and Davie 2012)

No entanto, caso o atraso seja excessivo o pacote é descartado pois já não poderá ser enviado para a aplicação em tempo útil (Figura 2.5).

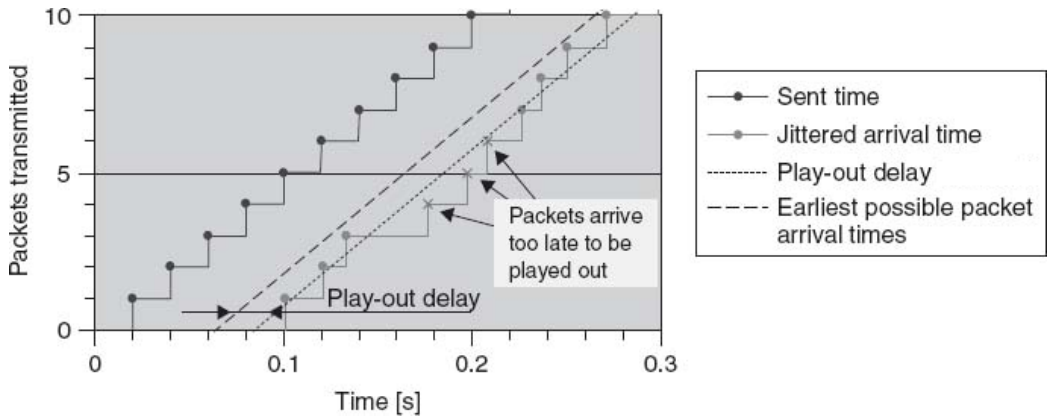

Figura 2.5: Descarte de pacotes demasiado atrasados
(Evans and Filsfils 2007)

2.2.2. Vídeo

As caraterísticas do tráfego de vídeo são muito diferentes do de voz pois a quantidade de dados transmitidos e a sua periodicidade são bastante variáveis (Figura 2.6). Isto deve-se aos *codecs* de vídeo usados que aplicam técnicas de compressão espacial e temporal, fazendo com que a quantidade de dados gerados dependa de cada imagem que constitui o vídeo e da sequência das mesmas.

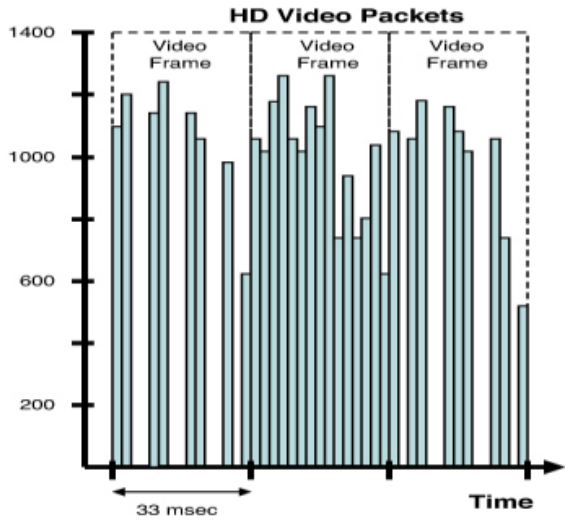

Figura 2.6: Tráfego de vídeo
(Szigeti et al. 2013)

Essa compressão é essencial para se poder diminuir de forma significativa a quantidade de dados a transmitir e, dessa forma, tornar exequível a sua transmissão pela rede, particularmente em vídeos de alta definição. Esta alta compressão torna o tráfego de vídeo muito sensível às perdas pois, se estas ocorrerem, poderão degradar significativamente parte de uma imagem ou mesmo uma sequência delas.

O tráfego de vídeo em alta definição é muito mais sensível a perdas do que o tráfego de voz pois a degradação da imagem é mais facilmente detetada pelo utilizador. Por esse motivo, a largura de banda necessária para a transmissão deve ser garantida para minimizar as perdas. O valor dessa largura de banda será função dos *codecs* usados.

Duas das subdivisões feitas nas aplicações de vídeo são as classes de *broadcast* e interativas em tempo real.

Broadcast

Esta classe é usada para fluxos de vídeo unidirecionais e não elásticos (*i.e.*, sem capacidade ou não desenhados para se adaptarem à perda de pacotes, por exemplo reduzindo a qualidade), como nas transmissões televisivas, transmissões ao vivo, ou videovigilâncias.

Nestes fluxos, a latência e a sua variação não são críticas pois, dada a sua unidirecionalidade, conseguem ser ultrapassadas recorrendo a técnicas de *buffering* ao nível das aplicações.

Interativas em tempo real

Esta classe é usada para fluxos de vídeo interativo, bidirecional e não elástico, e normalmente de alta definição, como é o caso de aplicações de telepresença.

A sensibilidade ao atraso e à sua variação é alta, como na voz, mas é dada uma tolerância para permitir os maiores tempos de processamento e de transmissão devido à maior quantidade de dados envolvidos.

2.2.3. Aplicações multimédia

As aplicações que integram conteúdos multimédia apresentam o desafio de saber como se devem ser classificados. Classificá-los como dados poderia degradar a qualidade do áudio e vídeo, mas classificá-los como aplicação de voz ou vídeo poderia sobrecarregar a largura de banda reservada para estas classes. Uma alternativa seria a separação e o tratamento independente dos componentes multimédia mas tal traria maior complexidade e riscos de dessincronismo.

Dai a recomendação de tratar este tipo de aplicações multimédia em duas classes próprias, uma para aplicações unidirecionais (*streaming*) e outra para bidirecionais (conferência).

Streaming

Esta classe é usada para aplicações multimédia unidirecionais e elásticas, como é o caso do vídeo a pedido (VoD – *Video on Demand*). Nas aplicações de VoD cada utilizador pode selecionar não só o programa que quer ver do catálogo de conteúdo multimédia disponibilizado pelo provedor do serviço mas também o momento para o fazer. Isto permite que a qualidade do conteúdo possa adaptar-se à qualidade da ligação (elasticidade) de cada utilizador.

Conferência

Esta classe é usada para aplicações multimédia bidirecionais e elásticas, como no caso das aplicações colaborativas.

2.2.4. Aplicações de dados

As aplicações de dados podem ser muitas, variadas e com diferentes requisitos, pelo que não podem ser classificadas numa única categoria. Em vez disso, podemos dividi-las nas aplicações de dados que requerem transmissão em tempo real, nas que requerem grande largura de banda, nas que não são relevantes para a organização e por isso são de menor prioridade, e nas restantes, representando esta a classe genérica.

Dados transacionais (de baixa latência)

Esta classe é usada para aplicações interativas, em que o tempo de resposta do sistema é importante para a produtividade do utilizador. É o caso de aplicações de bases de dados, ERP (*Enterprise Resource Planning*) e CRM (*Customer Relationship Management*).

Dados em massa (de alto débito)

Esta classe destina-se às aplicações de dados não interativas, a correr em segundo plano, e em que o tempo de resposta não interfere com a produtividade do utilizador. É o caso do correio eletrónico, transferência de ficheiros e operações de cópias de segurança.

Estas aplicações podem ser exigentes em termos de largura de banda, pelo que a sua colocação numa classe à parte permite limitar o seu uso excessivo.

Dados de melhor esforço

Esta classe é a predefinida para as aplicações que não pertençam a nenhuma outra categoria, o que será o caso da maioria. Como tal, deverá ser disponibilizada uma largura de banda garantida para a classe.

Predadora ou *Scavenger* (dados de baixa prioridade)

Esta classe serve para as aplicações que não são pertinentes para a organização e que, caso não sejam controladas, podem apoderar-se da largura de banda disponível e indisponibilizá-la para outras aplicações importantes. É o caso das aplicações de entretenimento, filmes, música, *BitTorrent*, entre outros. Em vez de simplesmente impedir este tipo de tráfego, enquanto houver recursos disponíveis na rede permite-se a sua passagem. No caso de congestionamento da rede este tráfego é o principal alvo de descarte de pacotes.

2.2.5. Controlo

Além do tráfego relacionado com as diferentes aplicações já vistas, o tráfego ao nível do plano de controlo dos equipamentos também deve ser considerado. Este apresenta um volume de tráfego reduzido mas que pode ser crítico para o funcionamento da rede e dos seus equipamentos. Pode ser dividido em três classes, controlo de rede, sinalização e Operação/Administração/Gestão.

Controlo de rede

Esta classe destina-se ao tráfego do plano de controlo dos equipamentos. É o caso do tráfego relacionado com protocolos de encaminhamento e de redundância, como o EIGRP (*Extended Interior Gateway Routing Protocol*), OSPF (*Open Shortest Path First*), BGP (*Border Gateway Protocol*) ou HSRP (*Hot Standby Router Protocol*).

Sinalização

Esta classe serve para o tráfego de sinalização de chamadas de voz e vídeo sobre IP, como é o caso do SIP (*Session Initiation Protocol*) e do H.323.

Operação/Administração/Gestão

Esta classe serve para tráfego de gestão e operação de rede, tal como o SSH (*Secure Shell*), SNMP (*Simple Network Management Protocol*) ou *Syslog*.

3. Modelos de QoS em redes IP

A arquitetura de base da Internet prevê que os pacotes IP sejam entregues segundo um modelo de **melhor esforço**, onde a rede tenta fazer chegar os pacotes ao destino sem dar qualquer garantia de que tal aconteça e sem oferecer um controlo do seu atraso ou da sua perda. Apesar de prático e apropriado para muitas situações, este modelo não é adequado em caso de congestionamento da rede pois não faz qualquer diferenciação no tratamento do tráfego sensível a atrasos e a perdas, levando à degradação do serviço prestado pelas respetivas aplicações associadas.

Para combater as dificuldades em lidar com tráfego com necessidades especiais o IETF (*Internet Engineering Task Force*) propôs dois modelos de QoS para redes IP:

- **Serviços Integrados (*Integrated Services* – IntServ)**, onde cada fluxo de tráfego individual poderá obter QoS garantida, através da reserva fim-a-fim dos recursos de rede necessários. No entanto, essa garantia limita a escalabilidade da sua utilização e pode ser dispendiosa.
- **Serviços Diferenciados (*Differentiated Services* – DiffServ)**, onde o tráfego é agrupado por classes, podendo cada uma delas obter QoS "quase" garantida através de tratamento preferencial, quando possível, do seu tráfego nos dispositivos de rede. Apesar de mais escalável, este modelo não oferece garantia absoluta de QoS.

3.1. Melhor esforço (*Best Effort* - BE)

No modelo de melhor esforço não é aplicado nenhum mecanismo de QoS ao tráfego sendo, por isso, o mais simples de todos. Os pacotes são atendidos por ordem de chegada e todos da mesma forma, sem qualquer tratamento preferencial. As suas caraterísticas são adequada para redes não congestionadas e para tráfego tolerante a atrasos e a perdas, mas mostram-se limitadas para gerir tráfego intolerante em situações de congestionamento.

É o modelo padrão usado nas redes IP e, consequentemente, na Internet, funcionando normalmente bastante bem, em particular para aplicações não sensíveis a atraso. Neste tipo de aplicações, quando é necessário garantir a entrega dos pacotes terão de ser os dispositivos terminais intervenientes a lidar com o processo, uma vez que a rede não se responsabiliza por tal. Essas aplicações podem recorrer, por exemplo, ao TCP (*Transmission Control Protocol*) para garantir a fiabilidade da transmissão e a entrega ordenada, sem erros e sem perda dos dados, recorrendo, entre outros, a mecanismos de retransmissão dos dados com erros ou não

recebidos. No entanto, tratando-se de aplicações de tempo real, em que o atraso e, possivelmente, a perda de pacotes são críticos, mecanismos de retransmissão de dados, como os implementados pelo TCP, não são uma solução viável pois apenas irão aumentar o atraso no recebimento dos dados. Para estas aplicações sensíveis ao atraso teria de ser a própria rede a assumir a responsabilidade de garantir atrasos mínimos, diferenciando o tratamento do tráfego, o que não é possível com o modelo de melhor esforço.

Dado as limitações deste modelo se sentirem em situações de congestionamento, uma possível solução passaria por aumentar os recursos da rede, nomeadamente ao nível da largura de banda, para que não houvesse necessidade de atrasar ou descartar pacotes. No entanto, dado o caráter dinâmico do tráfego seria difícil prever a largura de banda necessária para tal, correspondente aos valores de pico de utilização, e esse valor seria extremamente elevado em ligações de *backbone* obrigando a um aumento de custos, que é precisamente o oposto do que as organizações e as operadoras pretendem com a convergência das redes. Além disso, a disponibilidade da largura de banda ficaria comprometida no caso de falhas da rede.

3.2. Serviços integrados (*Integrated Services* – IntServ)

O desenvolvimento do modelo IntServ foi motivado pela necessidade de satisfazer os requisitos de rede das aplicações de tempo real. Foi descrito inicialmente no RFC 1633 (Braden, Clark, and Shenker 1994).

O IntServ define três classes de serviço:

- **Serviço garantido**, ou de tempo real, pensado para aplicações não elásticas, intolerantes ao atraso, ao *jitter* e às perdas, e que requeiram largura de banda assegurada, como o VoIP (*Voice over Internet Protocol*).
- **Serviço de carga controlada**, para aplicações elásticas, que suportam ligeiros atrasos, e que requeiram largura de banda assegurada. Oferece níveis de serviço semelhante ao obtido numa rede pouco congestionada com um serviço de melhor esforço. No entanto, é uma melhoria deste pois o nível de serviço mantém-se mesmo que o congestionamento se agrave.
- **Serviço de melhor esforço**, é aplicado aos fluxos que não obtiveram o serviço garantido nem o de carga controlada. Os fluxos com este serviço não tem recursos reservados para si, sendo os pacotes IP tratados de forma indiferenciada, da mesma forma que acontece na Internet atual.

Com o modelo IntServ é possível oferecer a uma aplicação de tempo real níveis de serviço garantidos, desde a origem até ao destino. Para tal, sustenta-se em dois mecanismos:

- **Reserva de recursos**: A aplicação requisita à rede um determinado nível de serviço, antes de enviar os dados, e os dispositivos ao longo do caminho reservam os recursos necessários para satisfazer esses requisitos ao longo de toda a sessão.
- **Controlo de admissão**: A aplicação só tem permissão de envio dos dados caso a rede possa satisfazer o nível de serviço requisitado. Se algum dispositivo ao longo do caminho não tiver capacidade para reservar os recursos necessários então a aplicação não pode enviar nenhuns dados.

Para a reserva de recursos da rede é usada uma abordagem orientada à conexão (Figura 3.1), havendo uma sinalização fim-a-fim do tipo de serviço e dos recursos necessários, com a participação dos dispositivos de rede por onde os pacotes do fluxo de dados vão passar.

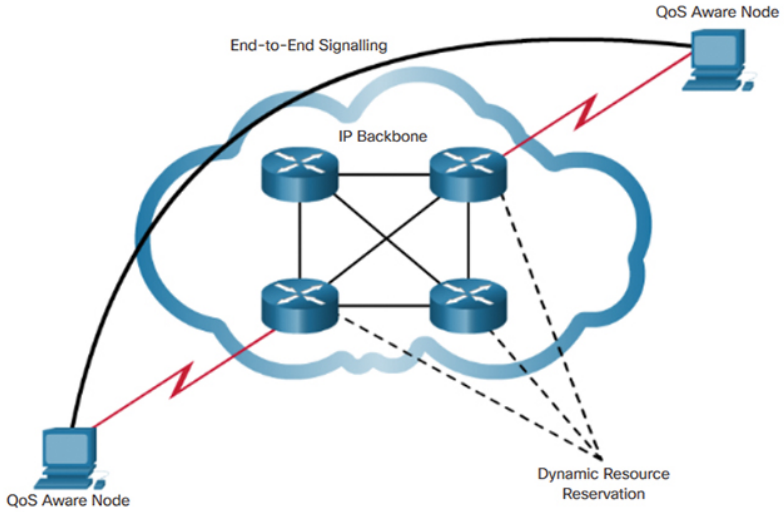

Figura 3.1: Exemplo de implementação IntServ
(Cisco Networking Academy 2017)

Para tal, o remetente indica as especificações do fluxo, um conjunto de requisitos de rede que pretende reservar, relacionados com a taxa de transmissão de dados e o atraso máximo suportado.

Essas especificações são enviadas aos equipamentos de rede que se encontram ao longo do trajeto até ao destino, devendo todos eles reservar os recursos necessários para esse fluxo pois bastaria um único equipamento sem recursos suficientes para causar o atraso de pacotes ou mesmo a sua perda. Em cada um deles é então verificada a possibilidade de reservar esses recursos. Caso não seja possível o equipamento pode recusar o fluxo ou, em alternativa, reduzir o valor de algum parâmetro das especificações em função dos recursos disponíveis e transmitir essa informação aos equipamentos seguintes até ao destino. Uma possível utilização desta última situação seria na transmissão de vídeo, por exemplo, com o destino a aceitar os recursos mais modestos oferecidos pela rede e solicitando um vídeo de menor resolução, compatível com os recursos disponibilizados.

Os dispositivos mantêm informação sobre o estado de cada um dos fluxos e, caso os mesmos se mantenham dentro dos parâmetros acordados, será concedida a largura de banda necessária para garantir a qualidade de serviço. Essa largura de banda será desperdiçada quando não estiver a ser usada pelos fluxos que a reservaram.

Uma grande vantagem deste modelo é o facto de se poder garantir QoS a cada fluxo de dados em particular. No entanto, tal acarreta várias dificuldades de implementação. Nomeadamente, é necessário que todos os dispositivos de rede por onde esse fluxo passa suportem o IntServ e, para cada fluxo, é necessário reservar recursos nos dispositivos (largura de banda, memória, processamento), tornando-se muito exigente em áreas de *backbone* e reduzindo a sua escalabilidade.

3.2.1. *Resource Reservation Protocol* (RSVP)

Para a sinalização das necessidades de QoS aos dispositivos da rede que irão encaminhar determinado fluxo de dados é proposta a utilização do *Resource Reservation Protocol* (RSVP) (Figura 3.2 e Figura 3.3).

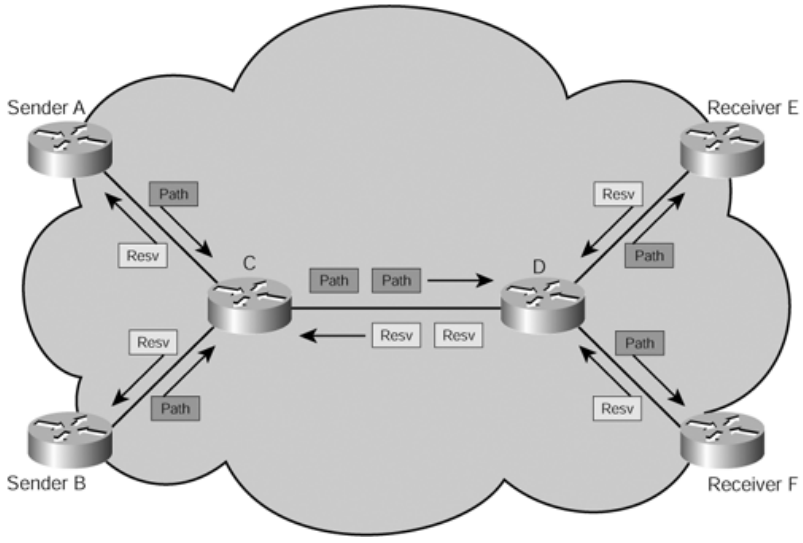

Figura 3.2: Mensagens PATH e RESV numa sessão RSVP

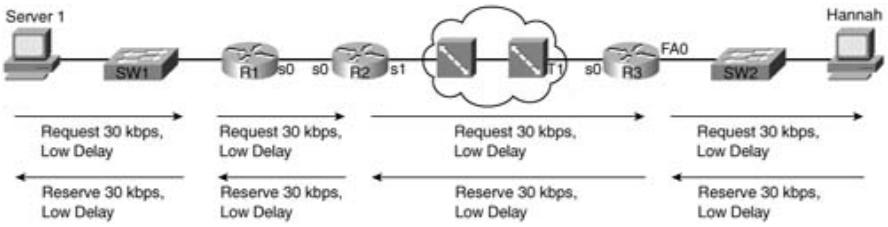

Figura 3.3: Pedido de reserva de recursos pelo RSVP
Adaptado de (Odom 2004)

O início da sinalização de uma sessão surge com o envio, pela origem do fluxo, de uma mensagem RSVP do tipo PATH (caminho), indicando as caraterísticas do tráfego que vai

enviar e os requisitos da rede necessários. A mensagem segue, de nó em nó, descobrindo o caminho até chegar ao destino final. Em cada nó, o equipamento verifica se pode satisfazer os requisitos pedidos, regista o caminho da mensagem e retransmite a mensagem para o nó seguinte.

Quando a mensagem chega ao destino este fica a saber que recursos da rede podem ser reservados para o fluxo. Perante essa informação, envia de volta uma mensagem RSVP do tipo RESV (reserva), seguindo exatamente o percurso inverso e fazendo a reserva dos recursos ao longo do trajeto.

Algumas caraterísticas do RSVP são:

- **Reservas unidirecionais**. Para reservas bidirecionais serão necessárias duas reservas unidirecionais, uma em cada sentido.
- **Suporte de tráfego *unicast* e *multicast***. Possibilita o suporte de aplicações *multicast* muitos-para-muitos e a partilha dos recursos reservados por vários fluxos, permitindo a sua otimização. Por exemplo, numa transmissão de *multicast* para vários clientes os equipamentos de rede comuns aos respetivos trajetos podem reservar os recursos necessários como se fosse para um único fluxo, partilhando-os pelos vários clientes.
- **Estado de sessão flexível**. As sessões estabelecidas não precisam de ser explicitamente finalizadas. Elas são interrompidas se não forem periodicamente renovadas, o que acontece enviando novo comando de reserva de recursos. Isso permite que uma sessão consiga recuperar no caso de falha de algum dispositivo. Além disso, dá a possibilidade de solicitar a alteração dos recursos reservados ao longo da sessão.
- **Reserva de recursos orientada ao recetor**. É o recetor que decide os recursos a pedir à rede para o fluxo de dados, o que faz sentido pois é ele que sente os efeitos da falta de QoS no tráfego.

3.3. Serviços diferenciados (*Differentiated Services* – DiffServ)

O modelo de serviços diferenciados (DiffServ) foi desenvolvido para disponibilizar qualidade de serviço ao tráfego de redes IP mas de uma forma mais simples e escalável que o modelo IntServ, apesar de não oferecer a mesma garantia.

Em vez da atribuição de níveis de serviço a fluxos de forma individualizada, os níveis de serviço são atribuídos a grupos de tráfego (classes) com requisitos similares. O DiffServ prevê mecanismos para identificar e dividir os pacotes por classes de serviço, permitindo a atribuição de diferentes níveis de serviço em função das suas necessidades e do definido previamente. A sua arquitetura foi descrita inicialmente no RFC 2475 (Blake et al. 1998).

Neste modelo, os requisitos do tráfego não são definidos pela aplicação nem é usada sinalização fim-a-fim para fazer a reserva de recursos da rede para um determinado fluxo de dados. Ao contrário, são normalmente os dispositivos de rede que decidem quais os recursos a atribuir aos pacotes que chegam com base na classe de tráfego em que esses pacotes são agregados (Figura 3.4). À medida que os pacotes atravessam a rede, cada dispositivo determina a classe a que os pacotes pertencem e trata-os de acordo com o nível de serviço correspondente. A definição do número de classes a usar, dos recursos atribuídos a cada uma e da forma como os pacotes são classificados é algo que é definido localmente em cada equipamento, assim como as ferramentas usadas para atingir os níveis de serviço do tráfego. Esta abordagem individualizada é designada por comportamento por salto (*per-hop behavior* – PHB).

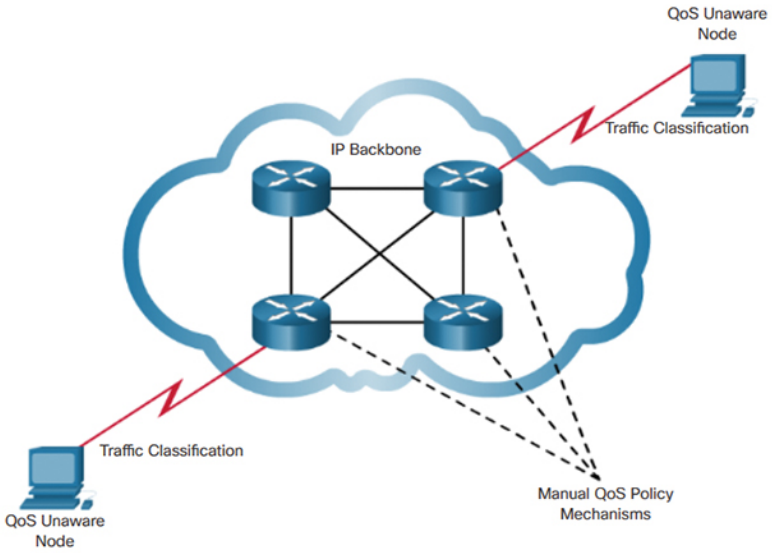

Figura 3.4: Exemplo de implementação DiffServ (Cisco Networking Academy 2017)

Como os mecanismos de QoS não são aplicados numa ótica fim-a-fim mas sim salto-a-salto, há a possibilidade do nível de serviço fornecido localmente ser diferente de dispositivo para dispositivo, comprometendo o nível de serviço fim-a-fim obtido. Apesar dos potenciais problemas criados, esta caraterística contribui para a flexibilidade e escalabilidade deste modelo. Para os ultrapassar, é necessário que haja coerência nas políticas definidas nos diversos dispositivos, o que não se torna fácil em redes sob diferente administração. Essa coerência não significa que todos os equipamentos tenham de ter exatamente as mesmas configurações mas sim que a classificação e o tratamento dado aos pacotes seja comparável ao longo da rede.

A sinalização fim-a-fim permite aos dispositivos de rede terem conhecimento do nível de serviço atribuído aos pacotes em dispositivos anteriores. Mas, como este modelo não contempla sinalização, a alternativa será colocar essa informação diretamente no cabeçalho dos pacotes (marcação), permitindo ao dispositivo seguinte conhecer a classificação feita no dispositivo anterior. Isso permite manter a coerência de classificação dos pacotes ao longo da

rede e, além disso, tratar mais rapidamente os pacotes pois evita fazê-los passar novamente pelo processo de classificação. No entanto, há sempre a possibilidade dos equipamentos ignorarem essa marcação anterior e fazerem nova classificação e remarcação.

3.4. Conclusão

O modelo de melhor esforço é o modelo padrão usado na Internet, de funcionamento simples e sem necessidade de configurações. Os resultados da sua utilização são bastante aceitáveis e é perfeitamente adequado para uma parte significativa do tráfego. No entanto, o tratamento indiferenciado do tráfego, sem garantias de largura de banda nem de atraso máximo, torna-o ineficiente para aplicações de tempo real.

O modelo IntServ permite garantir a qualidade de serviço ao nível dos fluxos individuais de tráfego. Estas caraterísticas tornam-no excelente para aplicações críticas, mas a complexidade da sua implementação e funcionamento tornam-no adequado apenas para redes controladas e de menor dimensão.

Em vez de se focar ao nível dos fluxos, o modelo DiffServ agrupa o tráfego em classes, em número e de caraterísticas variáveis e definidas em função dos objetivos estabelecidos. Essa abordagem permite uma menor complexidade de implementação e uma utilização menos exigente dos equipamentos da rede, promovendo a sua escalabilidade com a contrapartida da garantia de qualidade de serviço não ser tão elevada como no IntServ.

Os modelos IntServ e DiffServ não são mutuamente exclusivos, complementando-se e, eventualmente, podendo ser usados em simultâneo. Nas redes atuais, o modelo DiffServ é o mais usado mas os mecanismos do IntServ bem como o protocolo de sinalização RSVP são cada vez mais considerados para garantir a qualidade de serviço, dado o aumento de tráfego sensível a atrasos e a maior utilização de redes sem fios com a sua largura de banda variável.

A Tabela 3.1, na página seguinte, mostra uma comparação destes três modelos.

Dada a utilização muito mais generalizada do DiffServ e a maior flexibilidade na sua implementação, os próximos capítulos serão dedicados a aprofundar os mecanismos e ferramentas usados neste modelo.

Tabela 3.1: Caraterísticas dos modelo de QoS

	Melhor esforço	**IntServ**	**DiffServ**
Escalabilidade	Muito alta (limitada pela largura de banda)	Reduzida	Alta
Aplicabilidade	Redes IP em geral, Internet (modelo padrão)	Redes de pequena ou média dimensão	Redes de pequena, média ou grande dimensão, ISPs
Mecanismos de QoS	Não necessários		Complexos
Mecanismos de Implementação	Nenhum	Dinâmica (Por fluxo)	Estática (De longo prazo)
Garantia de serviço	Nenhuma	Total	Parcial
Tratamento preferencial de pacotes	Não	Sim	Sim
Utilização de recursos	Poucos	Intensivo	Moderados
Granularidade do controlo	Nenhum	Por fluxo ou grupos de fluxos	Tráfego agregado por classe
Abrangência do controlo	Nenhum	Fim-a-fim (em todos os dispositivos ao longo do fluxo)	Por dispositivo (possibilidade de concertação num conjunto de dispositivos)
Reserva de recursos	Não disponível	Por fluxo (em todos os dispositivos ao longo do fluxo)	Por classe de tráfego (em todos os dispositivos de um domínio)
Controlo de admissão	Não	Determinístico (Baseado em fluxos)	Estatístico (Baseado em classes de tráfego)
Apropriado para aplicações em tempo real	Não	Sim (Reserva de recursos)	Sim (LLQ)

4. Mecanismos e ferramentas de QoS

Na implementação de QoS a primeira coisa a fazer é definir os objetivos a atingir (*e.g.*, garantir a qualidade de voz nas comunicações). Depois disso, é necessário configurar os equipamentos de modo a atingir esses objetivos. Para isso é essencial conhecer as ferramentas e os mecanismos disponíveis para o efeito, bem como as capacidades dos próprios equipamentos. Neste capítulo serão conhecidos esses mecanismos e o seu modo de funcionamento, com um foco naqueles usados em redes IP sobre *Ethernet*. nomeadamente:

- **Classificação e marcação**: Os pacotes são analisados e divididos por classes (classificação), sendo os seus cabeçalhos escritos de acordo com o seu nível de serviço (marcação).
- **Policiamento e modelação**: A quantidade de tráfego é monitorizada para garantir que não excede determinados valores acordados. Os pacotes em excesso podem ser descartados (policiamento) ou colocados em espera para diminuir a sua taxa de transmissão (modelação ou *shaping*).
- **Gestão de congestionamento**: Quando uma ligação não tem capacidade suficiente para transmitir todo o tráfego necessário é necessário gerir a forma como os pacotes são colocados em filas de espera e a ordem pela qual os pacotes das várias filas vão ser enviados.
- **Prevenção de congestionamento**: Os pacotes podem ser descartados de forma preventiva para evitar congestionamento futuro.

Os mecanismos de classificação e marcação são normalmente aplicados na interface de entrada dos equipamentos, podendo ser também aplicados na interface de saída. O policiamento também pode ser feito nas duas interfaces. Já a gestão e a prevenção de congestionamento e a modelação são usadas nas interfaces de saída.

4.1. Classificação e marcação

Para se poder implementar políticas de QoS é necessário, em primeiro lugar, analisar e identificar o tráfego que chega a um dispositivo, num processo designado por **classificação**. Isso permite organizar os pacotes por classes de serviço, cada qual com diferentes níveis de serviço associados.

Após esse processo os pacotes têm, normalmente mas não necessariamente, os seus cabeçalhos escritos (**marcação**) com um valor de acordo com a sua classe.

É recomendado que a classificação e a marcação sejam feitos o mais próximo possível da origem do tráfego, por um dispositivo de confiança. Desta forma, os dispositivos seguintes poderão aplicar as políticas de acordo com a classificação já feita, sem necessidade de gastar tempo e recursos computacionais no processo de classificação.

4.1.1. Classificação

Um pacote classificado é um pacote associado a uma classe de serviço. Para haver essa classificação é necessário definir previamente quantas classes de serviço vão existir e quais as condições que determinam a associação dos pacotes a cada uma das classes.

A forma como a classificação é feita vai depender da implementação de QoS no dispositivo, podendo abranger as várias camadas do modelo OSI, pela análise da informação relativa a marcações pré-existentes, da informação relacionada com endereçamento, ou através da análise dos dados contidos nos pacotes para tentar identificar a aplicação pela sua assinatura (Tabela 4.1). A classificação pode ser feita usando uma combinação destes métodos e de forma diferente nas várias classes.

Tabela 4.1: Formas e exemplos de classificação de tráfego

<table>
<tr><th rowspan="2">Camada OSI</th><th colspan="3">Formas de classificação (exemplos)</th></tr>
<tr><th>Marcação</th><th>Endereçamento</th><th>Assinatura da aplicação</th></tr>
<tr><td>1</td><td></td><td>Interface (entrada/saída)</td><td></td></tr>
<tr><td>2</td><td>CoS (IEEE 802.1Q)
TID (IEEE 802.11)</td><td>Endereço MAC (origem/destino)</td><td></td></tr>
<tr><td>3</td><td>DSCP (IP)</td><td>Endereço IP (origem/destino)</td><td></td></tr>
<tr><td>4</td><td></td><td>Porto TCP/UDP (origem/destino)</td><td rowspan="4">Dados do pacote (deep packet inspection)</td></tr>
<tr><td>5</td><td></td><td></td></tr>
<tr><td>6</td><td></td><td></td></tr>
<tr><td>7</td><td></td><td></td></tr>
</table>

A classificação com base na marcação é a mais direta, pois analisa o valor do campo de QoS presente no quadro e/ou pacote recebido, o qual resulta de uma classificação já feita anteriormente noutro dispositivo. É o processo de classificação mais frequentemente usado.

A classificação com base no endereçamento assenta na análise da origem e/ou destino do tráfego, analisando os campos de endereçamento da camada 2 (*e.g.*, endereçamento MAC), camada 3 (*e.g.*, endereçamento IPv4 ou IPv6) ou camada 4 (*e.g.*, porto TCP ou UDP), ou mesmo em função da interface (física ou lógica) de entrada ou saída do tráfego.

Conhecendo a aplicação a que pertencem os dados ajuda no processo de atribuição de um nível de serviço. Quando falamos de aplicações que comunicam através de portos fixos ou bem conhecidos, essa tarefa fica facilitada pela simples leitura do campo de identificação dos portos usados. Mas, por vezes, isso não é suficiente, quer porque as aplicações não estão associadas a nenhum porto específico, quer porque podem estar a usar portos de outras aplicações na tentativa de ludibriar os mecanismos de filtragem de tráfego. Nestes casos, a solução passa por fazer a classificação com base na assinatura da aplicação, analisando detalhadamente os dados contidos nos pacotes (*deep packet inspection*) para tentar reconhecer algum padrão que se possa associar a determinada aplicação. Algumas aplicações podem ser identificadas apenas com os dados presentes no primeiro pacote (*e.g.*, por algum texto presente), enquanto que outras só podem ser detetadas ao fim de vários pacotes (*e.g.*, pelo volume e frequência dos dados).

O processo de classificação ocorre em todos os equipamentos e de forma independente.

4.1.2. Marcação

A marcação pode ser feita ao nível das camadas 2 e/ou 3. Feita ao nível da camada 3 tem a vantagem da informação sobre QoS poder ser transportada até ao destino. Feita ao nível da camada 2 permite que essa informação seja usada por *switches* e APs sem capacidade de analisar os cabeçalhos IP.

A marcação ao nível da camada 2 levanta alguns problemas, pois há alguma falta de uniformização no significado dos valores de QoS marcados nos quadros, não só entre redes cabladas Ethernet e redes sem fios IEEE 802.11, mas também entre diferentes fabricantes de equipamentos. Visto a marcação nos pacotes IP estar estabilizada e padronizada, é frequentemente recomendado utilizar-se como referência, ao longo do trajeto, os valores de QoS marcados nos pacotes IP, para evitar incompatibilidades. Para tal, a marcação ao nível da camada 2 poderá ser feita através de um mapeamento da marcação feita ao nível da camada 3.

4.1.2.1. Marcação na camada 2

A marcação na camada 2 em redes locais é suportada pelos padrões IEEE 802.1Q e IEEE 802.11.

Ethernet / IEEE 802.1Q

Os quadros Ethernet não possuem, nativamente, um campo para marcação de QoS. No entanto, o padrão IEEE 802.1Q, usado para permitir a implementação de VLANs em redes

Ethernet, contempla três bits (*Priority Code Point* – PCP) que podem ser usados para efeitos de diferenciação de tráfego (Figura 4.1).

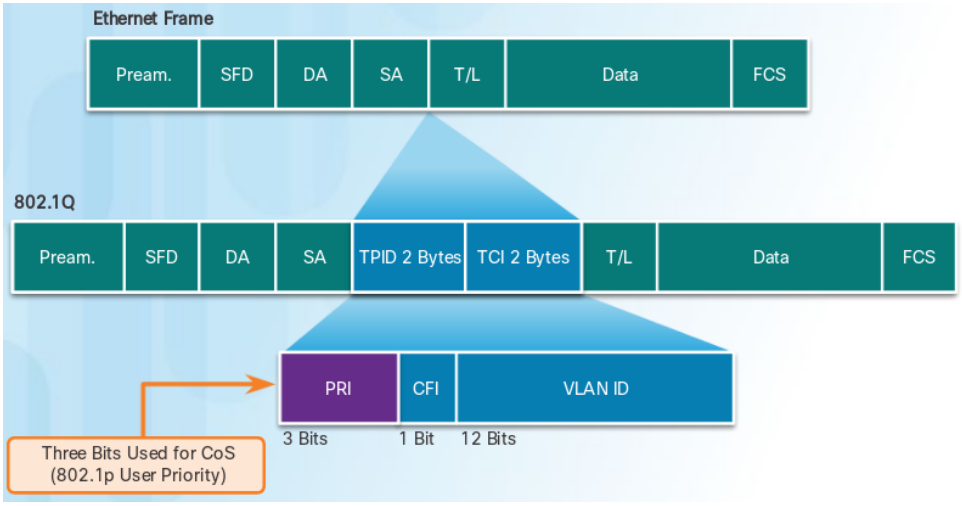

Figura 4.1: Marcação CoS em quadros IEEE 802.1Q
(Cisco Systems 2017)

Com esses três bits, definidos no padrão IEEE 802.1p, identifica-se a classe de serviço (*Class of Service* – CoS) com 8 níveis de prioridade possíveis, com o maior valor a corresponder à maior prioridade. O valor 0 nesses bits é o valor colocado por omissão nos quadros, representando o tráfego de melhor esforço, mas não sendo o que tem menor prioridade. (Tabela 4.2)

Tabela 4.2: Valores CoS em quadros 802.1Q

Valor	Prioridade	Acrónimo	Tipo de tráfego
1	**0**	BK	Segundo plano
0 (padrão)	**1**	BE	Melhor esforço
2	2	EE	Esforço excelente
3	3	CA	Aplicações críticas
4	4	VI	Vídeo
5	5	VO	Voz
6	6	IC	Controlo (entre redes)
7	7	NC	Controlo (na rede)

Os tipos de tráfego indicados são recomendações, ficando para os dispositivos a forma de implementação dos mecanismos de QoS.

IEEE 802.11 / Wi-Fi

Em redes sem fios IEEE 802.11 os quadros têm também disponível um campo para controlo de QoS (*Traffic Identifier* – TID), com três bits para identificar 8 níveis de prioridade (Figura 4.2).

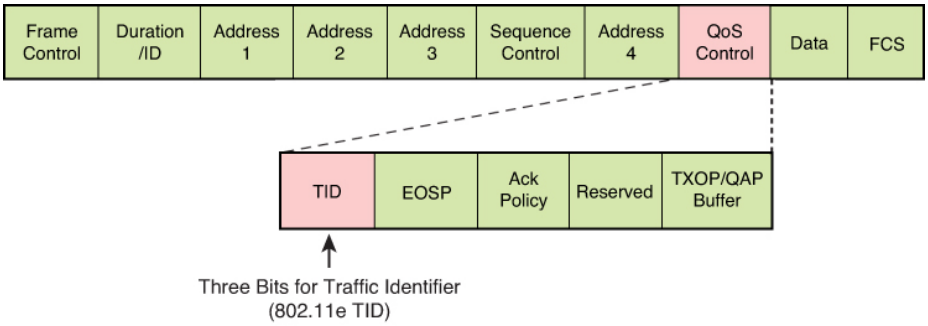

Figura 4.2: Campo de QoS em quadros IEEE 802.11 (Szigeti et al. 2013)

Os 8 níveis de prioridade têm significado similar aos valores de classe de serviço (CoS) dos quadros Ethernet 802.1Q mas com pequenas diferenças.

4.1.2.2. Marcação na camada 3

Os protocolos IPv4 e IPv6 reservam 8 bits nos cabeçalhos dos seus pacotes para marcação de QoS, antigamente designados por "Tipo de Serviço" nos pacotes IPv4 e "Classe de Tráfego" nos pacotes IPv6, estando divididos em duas partes (Figura 4.3):

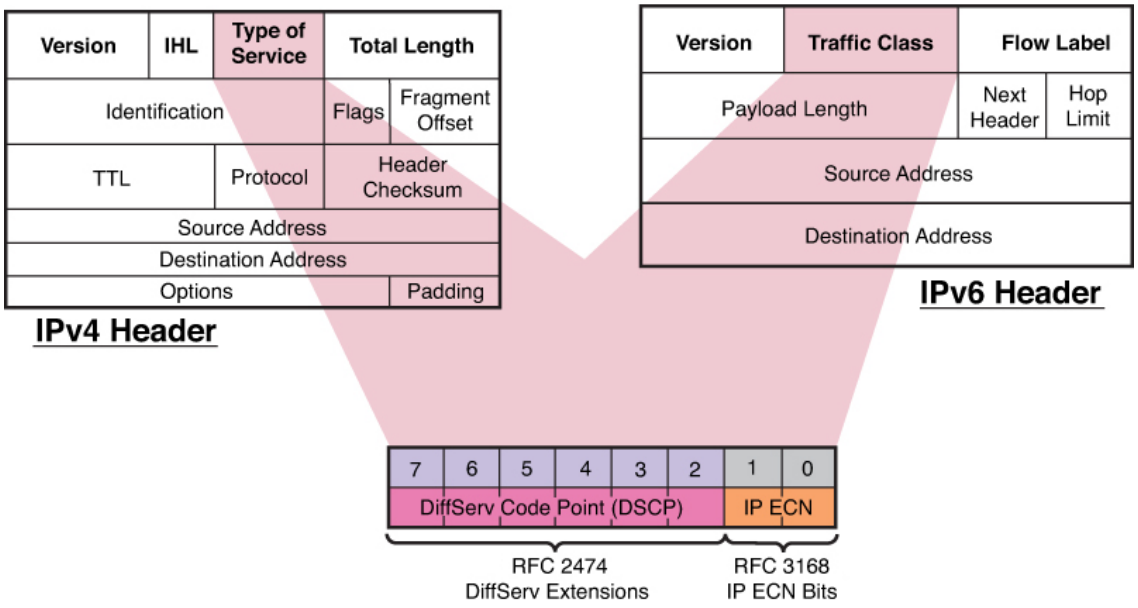

Figura 4.3: Campo para QoS nos pacotes IPv4 e IPv6 (Szigeti et al. 2013)

A primeira parte corresponde aos 6 bits mais significativos e designa-se por *Differentiated Services Code Point* (DSCP), sendo usada pelo DiffServ para a marcação da classe de serviço do pacote. A segunda parte corresponde aos 2 bits menos significativos e tem o nome de *IP Extended Congestion Notification* (ECN) mas não é usado pelo DiffServ. O objetivo é poder ser usado por um *router* para marcar um pacote que se deparou com um congestionamento. Ao receber um pacote marcado dessa forma, o destino passará a ter

conhecimento dessa situação e marcará também o pacote de resposta para que o hospedeiro de origem o saiba também, permitindo a ambos lidar com a situação a um nível superior. Por exemplo, através da diminuição do tamanho da janela TCP o que terá como consequência a diminuição do tráfego na rede.

Os três bits mais significativos do DSCP, também designados de *Class Selector* (CS) podem ser mapeados diretamente para os três bits do campo CoS em quadros Ethernet 802.1Q. (Figura 4.4)

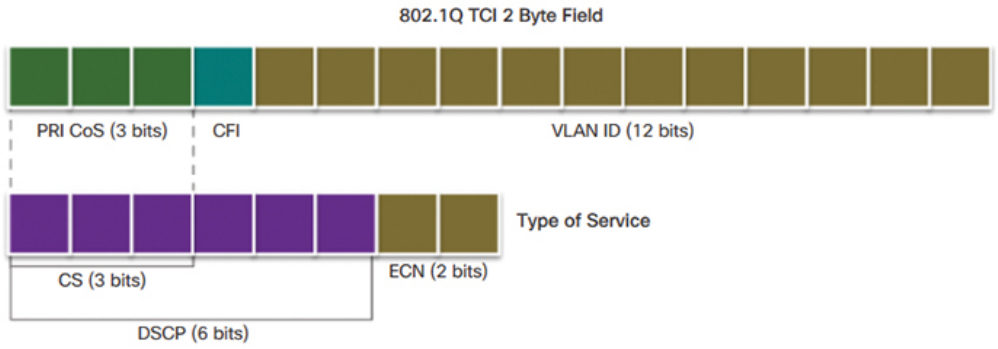

Figura 4.4: Mapeamento L3 (DSCP) para L2 (CoS)
(Cisco Networking Academy 2017)

Differentiated Services Code Point (DSCP)

O valor do DSCP serve para selecionar o comportamento a aplicar aos pacotes que chegam a um determinado equipamento de rede (comportamento por salto ou *Per-Hop-Behavior* – PHB). Esses comportamentos podem ser organizados em três grupos, aqui apresentados por ordem decrescente de prioridade:

- **Encaminhamento Expedito (*Expedited Forwarding* – EF)**

  Proporciona o menor atraso possível, sendo recomendado apenas para marcação de pacotes de voz.

  Também define valores mínimos e máximos de largura de banda para esta classe, garantindo a sua disponibilidade mas, em caso de congestionamento, podendo descartar pacotes para não prejudicar as restantes classes de tráfego.

  O valor do DSCP é 46 (**101**110), mapeando diretamente na camada 2 para CoS = 5 (tráfego de voz).

- **Encaminhamento Garantido (*Assured Forwarding* – AF)**

  Usado para um serviço de largura de banda garantida.

  Este grupo é constituído por 4 classes (AF1, AF2, AF3 e AF4), independentes, cada qual com direito a usar uma parte dos recursos do dispositivo. Dentro de cada classe, é

possível ainda diferenciar a forma como os pacotes vão ser tratados em caso de congestionamento, através de 3 níveis de preferência de descarte: baixa (1), média (2) ou alta (3).

Os recursos reservados a cada classe podem, se disponíveis, ser usados por outras classes.

No valor DSCP, os três bits mais significativos representam a classe e os três bits menos significativos a preferência de descarte.

- **Melhor Esforço (*Best-Effort* – BE)**

  É o comportamento padrão, sem implementação de QoS. O tratamento é feito por ordem de chegada e, no caso de congestionamento, os pacotes poderão ser descartados.

  O valor do DSCP é 0 (**000**000).

A Figura 4.5 mostra um resumo dos diversos tipos de valores DSCP usados e o seu significado. Por exemplo, um pacote marcado com um valor DSCP = 28 (011100) indica um nível de serviço AF32, ou seja, da classe 3 do grupo *Assured Forwarding*, e uma preferência de descarte média (2). Em caso de congestionamento, este pacote só será descartado depois de descartados os pacotes marcados como AF33, que têm uma preferência de descarte alta (3).

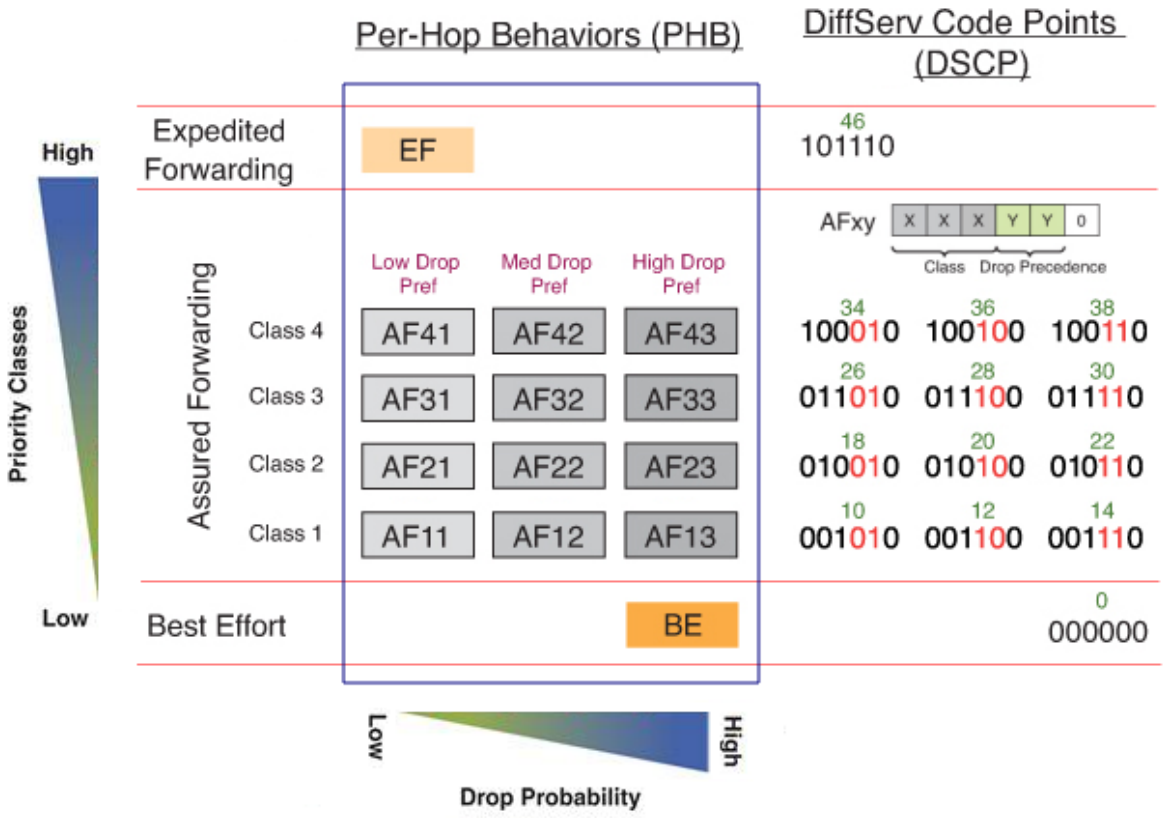

Figura 4.5: Esquema de codificação dos valores DSCP
Adaptado de (Szigeti et al. 2013) e (Joseph and Chapman 2009)

4.1.2.3. Segurança e limites de confiança

Como já mencionado, os pacotes podem chegar a um dispositivo já marcados previamente. Nesse caso, o dispositivo tem de decidir se aceita essa marcação existente ou se a ignora, sujeitando o pacote a novo processo de classificação e marcação. A decisão vai depender se o dispositivo que fez essa marcação se encontra dentro ou fora dos limites de confiança, respetivamente. (Figura 4.6)

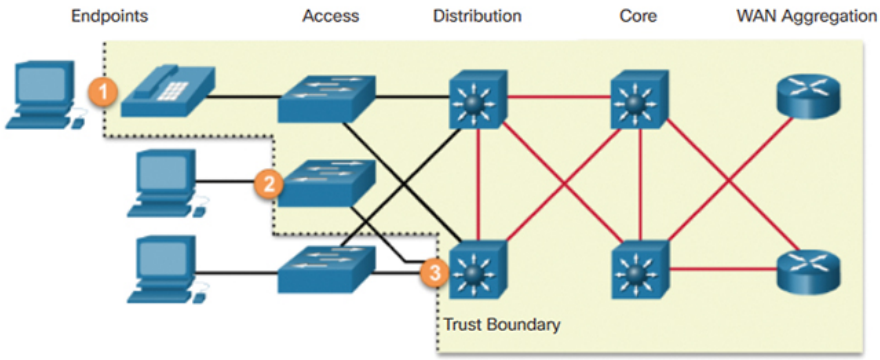

Figura 4.6: Limites de confiança
(Cisco Networking Academy 2017)

O objetivo é evitar atribuir níveis de serviço incorretos a pacotes devido a uma marcação incorreta, feita de forma deliberada ou não. Por exemplo, um utilizador poderia enviar todos os pacotes do seu computador marcados como tráfego de voz para tentar obter um melhor desempenho nas suas comunicações ou mesmo para tentar um ataque de negação de serviço ao serviço de voz.

Os domínios ou zonas de confiança estão, normalmente, na alçada de uma administração comum e incluem os equipamentos com acesso controlado (*e.g.*, *routers*, *switches*, servidores, APs, telefones IP). Dentro desse domínio as marcações dos pacotes são aceites pelos dispositivos seguintes, o que não significa que não se possam fazer novas classificações e marcações. Fora desse domínio, para lá da fronteira de confiança, encontram-se dispositivos a que os utilizadores têm acesso direto (*e.g.*, computadores, *switches* sem segurança). É nos dispositivos junto à fronteira de confiança que será apropriado fazer a classificação e marcação dos pacotes, ignorando possíveis marcações feitas fora do domínio de confiança.

Há situações em que a marcação dos pacotes pode ser considerada para lá de um limite de confiança mas de forma condicionada. Por exemplo, quando há acordos sobre utilização de recursos estabelecidos entre uma organização e o seu provedor de serviços. Na Figura 4.7 está ilustrada uma situação em que foi contratualizada uma largura de banda máxima de 10 Mbps, com possibilidade de usar duas classes de serviço, uma delas prioritária, para voz, com uma largura de banda de 2 Mbps. Neste caso, o *router* do provedor de serviços poderia aceitar a marcação vinda do *router* da organização, desde que o tráfego não excedesse os valores

contratualizados. Caso contrário, poderia remarcar o tráfego de voz acima de 2 Mbps para não prioritário ou mesmo descartar esse tráfego caso ultrapassasse os 10 Mpbs.

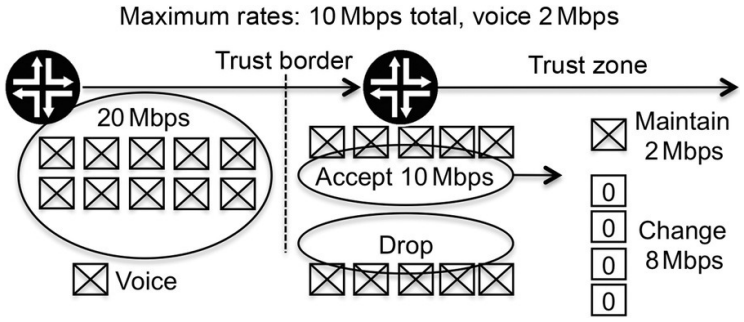

Figura 4.7: Limite de confiança entre domínios (Barreiros and Lundqvist 2016)

4.2. Policiamento e modelação

Depois dos pacotes classificados e, eventualmente, marcados, é necessário tratá-los de acordo com as políticas definidas para a sua classe. No entanto, também dentro de cada classe os pacotes poderão ter tratamento diferenciado, em função da sua taxa de chegada. Para isso, os fluxos de tráfego que chegam a um dispositivo são medidos para verificar se a quantidade de pacotes está conforme os limites estabelecidos. Ao tráfego que viole a taxa de chegada acordada podem ser aplicados diferentes mecanismos:

- **Policiamento (*policing*)**

  Neste mecanismo, a ação normal no caso de pacotes em excesso é o seu descarte imediato (*hard policing*). No entanto, é possível fazer a sua remarcação, normalmente para uma classe com maior probabilidade de descarte, para dar ainda alguma possibilidade de transmissão se houver recursos suficientes para tal (*soft policing*).

  O policiamento rígido não provoca atraso dos pacotes, pois estes ou são transmitidos imediatamente ou são descartados.

- **Modelação (*shaping*)**

  Os pacotes em excesso são atrasados, com a sua colocação em *buffers*, e transmitidos mais tarde quando o tráfego diminuir e ficar novamente dentro do limite, evitando o seu descarte.

  O efeito da modelação é estabilizar o tráfego, eliminando os picos, de modo a que taxa máxima definida não seja ultrapassada. É usado frequentemente para garantir acordos de nível de serviço (*service level agreements* – SLA) entre provedores de serviço e os seus clientes.

  O descarte também pode acontecer caso o tráfego seja demasiado e os *buffers* fiquem cheios, obrigando a descartar os pacotes que já não têm lugar nos *buffers*.

A Figura 4.8 ilustra o efeito de cada um destes mecanismos perante tráfego que viole os limites estabelecidos. O tráfego que sofre modelação fica com uma taxa de transmissão mais estável, apesar de sofrer um ligeiro atraso, pois os pacotes apenas são transmitidos quando não excederem a taxa máxima de transmissão. Já ao aplicar o policiamento não há atrasos mas o tráfego que não cumpre com a taxa máxima é simplesmente eliminado.

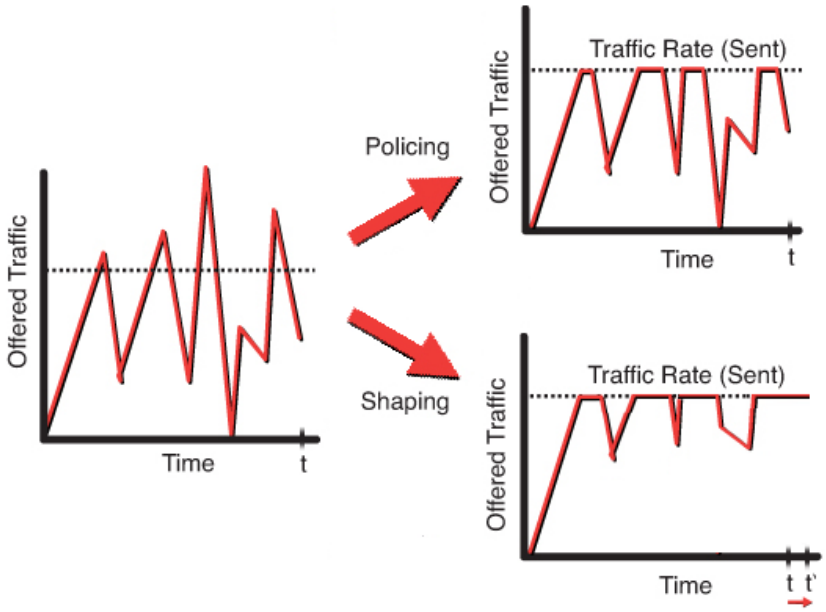

Figura 4.8: Efeito do policiamento vs shaping
Adaptado de (Szigeti et al. 2013)

O policiamento e o *shaping* não são tão adequados para aplicações de tempo real, nomeadamente de voz, já que podem provocar o atraso ou a perda de pacotes. Para este tipo de aplicações é preferível usar mecanismos de controlo de admissão de chamadas (*call admission control* – CAC). Em caso de congestionamento, a utilização deste mecanismo impede que uma nova chamada de voz seja estabelecida evitando não só que a chamada não tivesse a qualidade desejada mas também a possível degradação das outras chamadas em curso pois iria sobrecarregar a rede com mais tráfego.

Para tráfego TCP o *shaping* é preferível ao policiamento já que, apesar do TCP conseguir lidar tanto com perdas como com atrasos, as perdas de pacotes provocadas pelo policiamento iriam causar a sua retransmissão, o que contribuiria ainda mais para o congestionamento da rede.

A Tabela 4.3 mostra um resumo das caraterísticas do policiamento rígido e do *shaping* em situação de não conformidade do tráfego.

Tabela 4.3: Comparação das caraterísticas de Hard Policing e de Shaping

	Hard Policing	***Shaping***
Adaptabilidade ao congestionamento	Não	Sim
Impacto na perda de pacotes	Provoca perda de pacotes	Minimiza a perda de pacotes
Impacto na latência	Não provoca latência	Provoca latência
Impacto no *jitter*	Não provoca *jitter*	Provoca *jitter*
Impacto no tráfego TCP	Provoca retransmissões	Minimiza as retransmissões
Interface de aplicação	Entrada (recomendado) ou saída	Tipicamente saída
Recursos necessários	Mínimos	Requer *buffers*

Adaptado de (Szigeti et al. 2013)

4.3. Gestão de congestionamento

Quando a largura de banda disponível numa ligação é suficiente para a transmissão de todo o tráfego que chega a um dispositivo de rede, os pacotes são enviados de imediato. No entanto, quando não há disponibilidade para transmitir todos os pacotes de imediato entra-se num estado de congestionamento, sendo necessário recorrer a mecanismos que façam a sua gestão e que decidam como é que os recursos vão ser partilhados entre esses pacotes.

A gestão de congestionamento pode fazer-se usando técnicas de **enfileiramento (*queuing* ou *buffering*)** que tratam da colocação dos pacotes em filas (*buffers*) à espera de serem transmitidos, bem como da sua reorganização na fila de acordo com as prioridades, ou até mesmo do seu descarte caso estejam há demasiado tempo na fila ou se o *buffer* ficar cheio. A determinação da fila apropriada para cada pacote é feita com base na sua classificação e marcação prévia, processos descritos no início do capítulo (em 4.1.). Na presença de várias filas de espera é necessário definir por que ordem é que as filas vão ser atendidas e quantos pacotes de cada uma vão poder ser transmitidos a seguir, tarefa que é responsabilidade do mecanismo de **agendamento (*scheduling*)** (Figura 4.9).

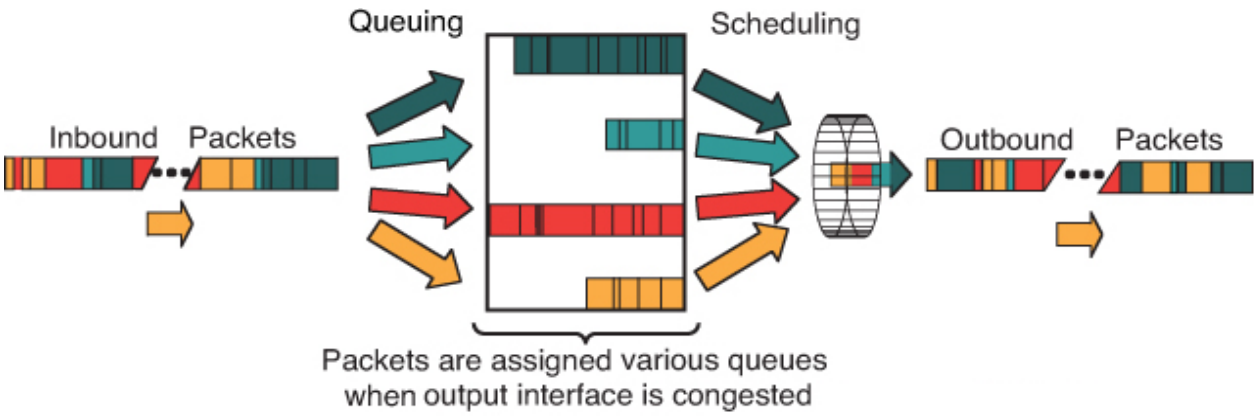

Figura 4.9: Processos de enfileiramento e de escalonamento (Szigeti et al. 2013)

A ordem pela qual as filas vão ser atendidas é decidida por um algoritmo de escalonamento, dos quais se apresentam a seguir alguns dos mais elementares:

- **Prioridade rigorosa (*strict priority*)**: Uma fila de menor prioridade só é atendida quando as filas de maior prioridade estiverem vazias. A sua simplicidade tem como inconveniente o facto de as filas menos prioritárias poderem ficar sem ser atendidas por muito tempo.
- ***Round-robin***: As filas vão sendo servidas alternadamente. É mais justa, permitindo a transmissão de pacotes de todas as filas, mas pode provocar demasiada latência em tráfego de tempo real.
- **Justo ponderado (*weighted fair*)**: As filas vão sendo servidas alternadamente mas algumas de forma mais frequente. Garante a transmissão de todas as filas e minimiza os atrasos das filas mais sensíveis. No entanto, não garante largura de banda aos fluxos de tempo real.

Para a gestão de congestionamento existem inúmeras técnicas, com diversas combinações de algoritmos de enfileiramento com algoritmos de escalonamento, e variações de fabricante para fabricante. As técnicas mais antigas, indicadas a seguir, apesar de mais simples, não lidam bem com a diversidade de tráfego a circular na rede, nomeadamente de áudio e vídeo:

- ***First-In, First-Out* (FIFO)**: Os pacotes são retransmitidos pela ordem que são recebidos.
- ***Fair Queuing* (FQ)**: A largura de banda disponível é dividida pelos vários fluxos de tráfego de forma justa.
- ***Priority Queuing* (PQ)**: Os pacotes colocados nas filas prioritárias são sempre enviados em primeiro lugar.
- ***Weighted Fair Queuing* (WFQ)**: Variante do FQ que permite atribuir ponderações às filas.

Para lidar com o tipo de tráfego encontrado nas redes atuais é necessário que as técnicas de gestão de congestionamento garantam ao tráfego mais sensível largura de banda e atraso máximo, sem retirar a possibilidade de transmissão de outro tipo de tráfego. É o caso das técnicas mais recentes, e recomendadas, que melhoram as caraterísticas das mais antigas:

- ***Class-Based Weighted Fair Queuing* (CBWFQ)**: Os fluxos são agregados por classes de tráfego.
- ***Low Latency Queuing* (LLQ)**: Adiciona ao CBWFQ uma fila prioritária para tráfego de tempo real.

4.3.1. *First-In, First-Out* (FIFO)

Nesta técnica há apenas uma fila e não há diferenciação de tráfego. Os primeiros pacotes a serem colocados na fila são também os primeiros a serem transmitidos, independentemente do seu tamanho ou da sua prioridade (Figura 4.10).

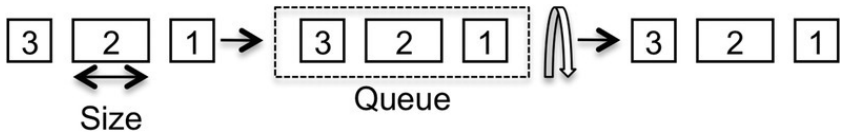

Figura 4.10: Operação FIFO
(Barreiros and Lundqvist 2016)

É o método mais simples e rápido, sendo muitas vezes o comportamento padrão dos equipamentos. É adequado se a largura de banda for suficiente para todo o tráfego e não houver congestionamento. No entanto, havendo congestionamento é provocado atraso nos pacotes, tanto maior quanto o nível de congestionamento, ou mesmo o seu descarte se a fila ficar cheia. Como o atraso e o descarte é aplicado aos pacotes independentemente do seu tipo e sem possibilidade de ser controlado, o tráfego sensível a estes parâmetros é particularmente penalizado com estas situações mas em caso de congestionamento extremo todo o tipo de tráfego sentirá a degradação do serviço. Outro inconveniente é o facto de fluxos com muitos pacotes de grande dimensão poderem sobrecarregar a fila, impedindo a transmissão do restante tráfego.

4.3.2. *Fair Queuing* (FQ)

O FQ permite colmatar algumas falhas do FIFO através da separação do tráfego por fluxos, e fazendo uma gestão justa da transmissão dos pacotes de cada um dos fluxos através de um escalonamento *round-robin*. Isso permite evitar que um fluxo que esteja a transmitir em rajada monopolize a largura de banda. Além disso, o escalonamento da transmissão de cada fluxo é feito tendo em consideração o tamanho dos pacotes e não o seu número, fazendo com que um fluxo constituído por pacotes pequenos não seja prejudicado por um fluxo constituído por pacotes grandes (Figura 4.11).

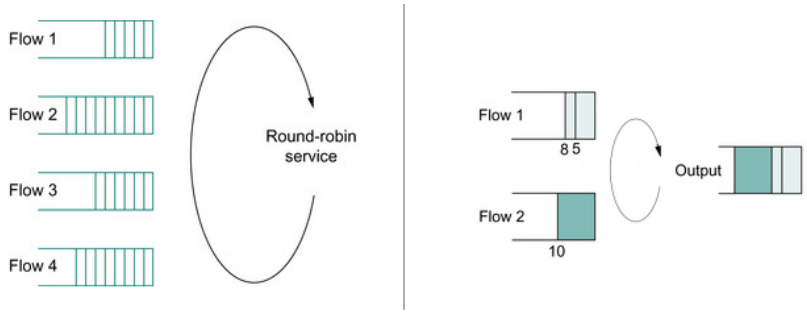

Figura 4.11: Operação FQ
Adaptado de (Peterson and Davie 2012)

Com o FQ, a largura de banda é dividida pelos vários fluxos existentes num dado momento, sendo que se um dos fluxos não estiver a transmitir a sua largura de banda poderá ser aproveitada pelos restantes fluxos. Cada fluxo terá, assim, uma largura de banda garantida de valor incerto e inversamente proporcional ao número de fluxos a transmitir num dado momento. O atraso nos pacotes também não é controlado.

4.3.3. *Priority Queuing* (PQ)

Este método permite a separação do tráfego por classes de diferentes prioridades, cada qual com a sua fila de espera. O envio do tráfego das diferentes filas é feito segundo um algoritmo de prioridade rigorosa, onde os pacotes de uma fila só são transmitidos caso não haja mais nenhum pacote em espera nas fila de maior prioridade (Figura 4.12). O tratamento dos pacotes dentro de cada fila segue um algoritmo FIFO.

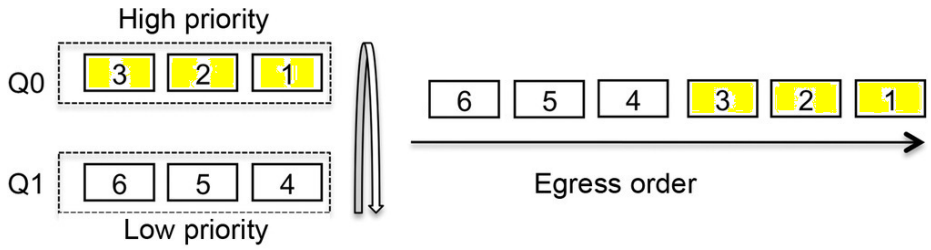

Figura 4.12: Operação do PQ
Adaptado de (Barreiros and Lundqvist 2016)

O PQ possibilita ao tráfego da fila mais prioritária valores reduzidos de latência e *jitter* mas, em contrapartida, o tráfego menos prioritário pode ficar sem largura de banda disponível e levar ao comprometimento do normal funcionamento da rede. Esta situação pode ser ultrapassada com a implementação de policiamento às filas de maior prioridade, colocando limites à sua utilização e promovendo o descarte do tráfego em excesso ou a sua despromoção para uma fila menos prioritária.

4.3.4. *Weighted Fair Queuing* (WFQ)

O WFQ é uma variação do FQ, com a possibilidade de cada fila ter uma ponderação associada. Na prática, isso significa que a percentagem da largura de banda reservada a cada uma das filas pode ser diferente. O mecanismo de escalonamento é orientado ao bit e não ao pacote, tornando-o mais justo para pacotes de tamanho menor e evitando que pacotes de maior dimensão se apoderem da largura de banda disponível (Figura 4.13).

Apesar da ideia original deste método indicar uma fila de espera por fluxo de tráfego, muitas vezes as implementações feitas agregam os fluxos em classes de tráfego, associando uma fila de espera a cada uma dessas classes.

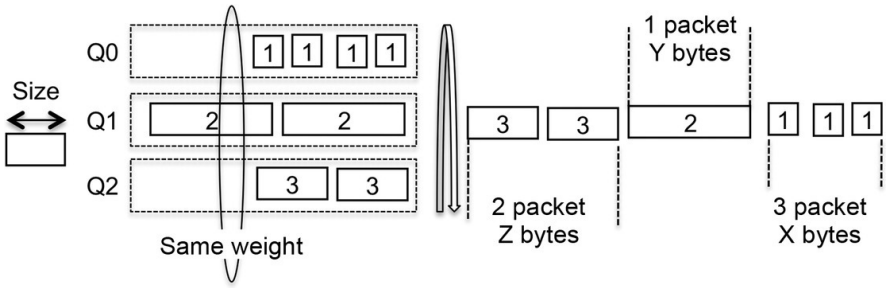

Figura 4.13: Operação WFQ
(Barreiros and Lundqvist 2016)

O WFQ melhora o serviço prestado a fluxos de tempo real, mas não garante largura de banda a fluxos individuais, apenas a agregação de fluxos de uma mesma classe.

4.3.5. *Class-Based Weighted Fair Queuing* (CBWFQ)

O CBWFQ é uma evolução do WFQ, permitindo que o tráfego seja dividido em classes criadas pelo administrador, cada uma com a sua fila de espera (Figura 4.14). A cada classe é possível atribuir algumas caraterísticas, nomeadamente, a largura de banda disponível em caso de congestionamento, o número máximo de pacotes suportados e a ponderação da respetiva fila de espera.

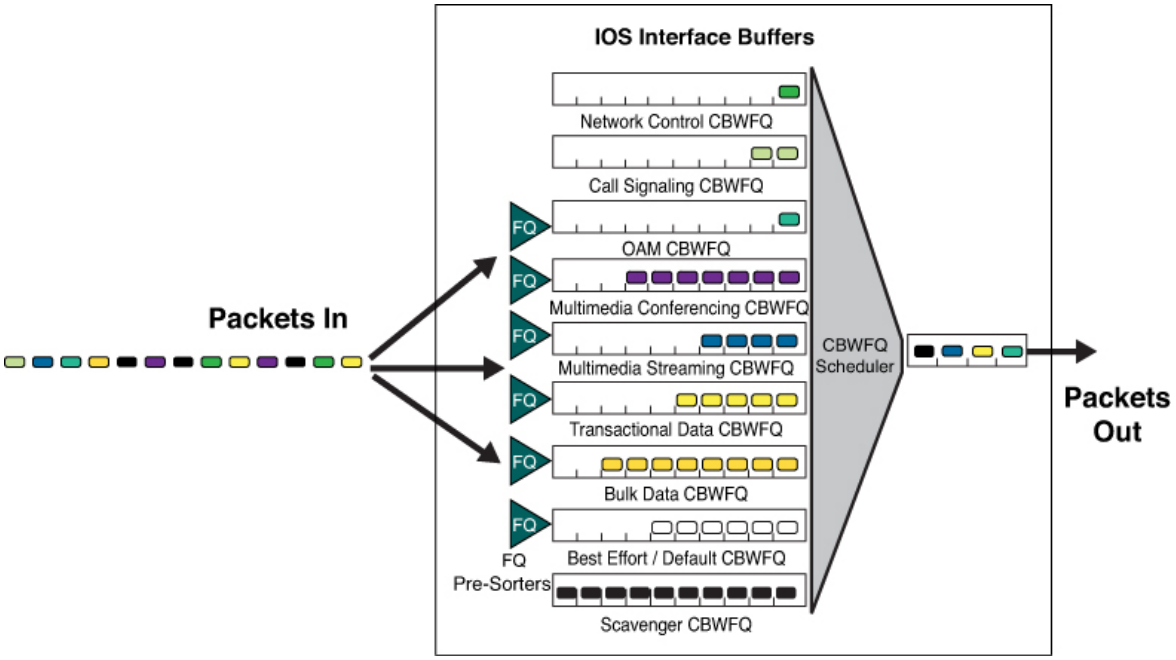

Figura 4.14: Operação do CBWFQ
(Szigeti et al. 2013)

Antes de serem colocados dentro da fila de espera respeitante à sua classe, os pacotes são pré-ordenados através do método FQ, permitindo que os pacotes dos diversos fluxos que

vão ser agregados nessa classe sejam tratados de forma justa e independente da sua quantidade e tamanho. Já dentro de cada fila os pacotes são tratados segundo um algoritmo FIFO.

4.3.6. *Low Latency Queuing* (LLQ)

O LLQ junta o PQ ao CBWFQ, tendo sido desenvolvido especificamente para permitir lidar convenientemente com o tráfego de tempo real, em particular com a voz. É criada uma fila de prioridade rigorosa (PQ), permitindo garantir largura de banda e baixa latência ao tráfego de tempo real, mas sem impedir o envio do restante tráfego, feito através do CBWFQ, fazendo deste um método adequado para os diversos tipos de tráfego (Figura 4.15).

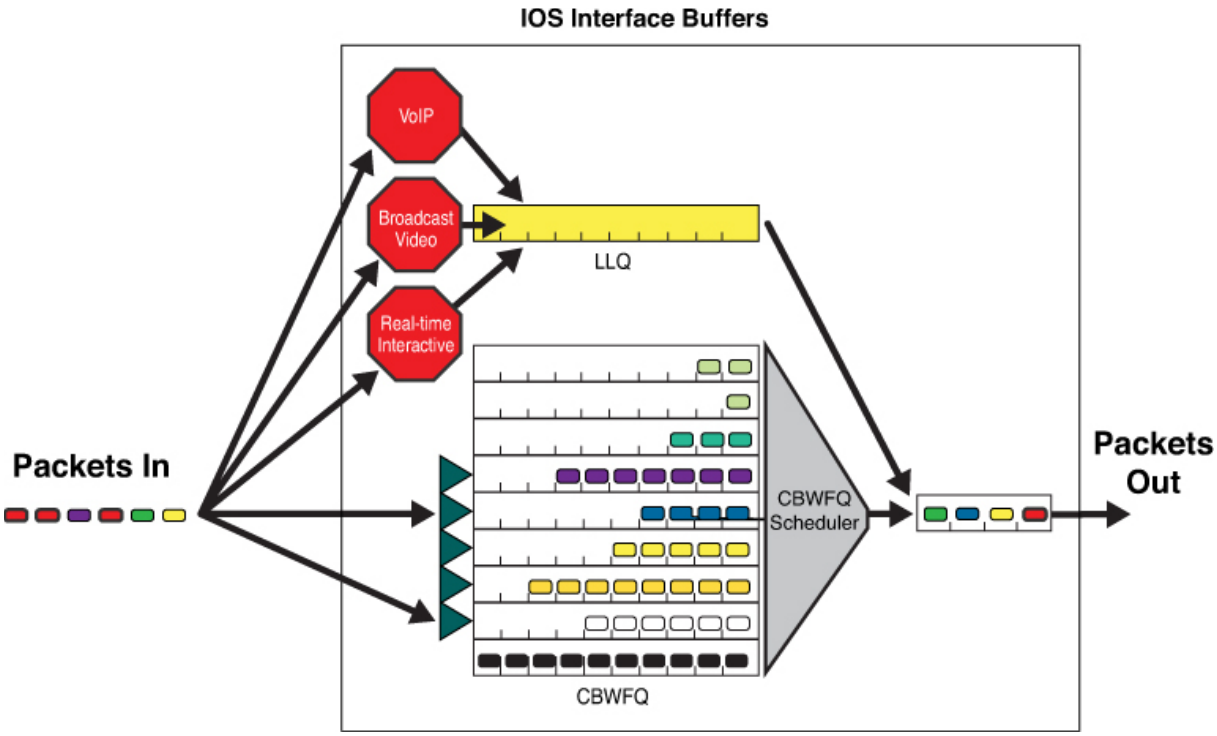

Figura 4.15: Operação do LLQ
(Szigeti et al. 2013)

Para evitar os problemas da fila prioritária esgotar os recursos às filas menos prioritárias é feito um policiamento ao tráfego dessa fila, descartando os pacotes que cheguem a uma taxa superior ao máximo estabelecido.

A Cisco recomenda que apenas o tráfego de voz seja enviado para esta fila, e que se a ligação tiver tráfego misto de voz, dados e vídeo, esta fila não reserve mais do que um terço da capacidade da ligação.

4.4. Prevenção de congestionamento

Os *buffers* associados às interfaces têm capacidade limitada. Isso significa que, se um pacote chega a um dispositivo e se depara com um *buffer* cheio terá de ser descartado, independentemente do fluxo a que pertence e da sua prioridade. A este tipo de descarte dá-se o nome de *tail drop*, pois os pacotes descartados são os que iriam para a parte final da fila.

Uma outra forma de lidar com o problema seria não deixar que os *buffers* se esgotem, descartando pacotes antes que tal acontecesse. Isso daria a possibilidade de fazer o descarte de forma seletiva, escolhendo aqueles pacotes cuja perda causaria menos impacto na rede e nas aplicações, numa estratégia designada por **prevenção de congestionamento**. Os mecanismos de prevenção de congestionamento são mais simples que os de gestão de congestionamento, baseando-se na monitorização do tráfego e no descarte de pacotes quando se prevê que os níveis de tráfego podem provocar congestionamento. Os principais mecanismos de prevenção de congestionamento são o **policiamento** e o **RED/WRED**.

A forma como o TCP lida com as perdas faz com os pacotes que transportem segmentos TCP sejam particularmente indicados para esta estratégia de descarte seletivo. A taxa de transmissão do TCP começa por ser baixa e vai aumentando enquanto não detetar problemas ou o destino não dar indicação contrária. Entre os possíveis problemas encontra-se, precisamente, a perda de segmentos. Ora, quando isso acontece o TCP baixa a taxa de transmissão na tentativa de evitar contribuir mais para um possível congestionamento da rede e retransmite os segmentos perdidos. Posteriormente, volta a aumentar progressivamente a taxa de transmissão. No entanto, se vários fluxos TCP sofrerem descarte de pacotes simultaneamente isso pode levar a um acontecimento designado por sincronização global do TCP, em que os vários emissores baixam as suas taxas de transmissão, retransmitindo os pacotes perdidos e voltando a aumentar as taxas de transmissão como se estivessem sincronizados o que contribui para o aumento de tráfego e, consequentemente, para novos congestionamentos (Figura 4.16).

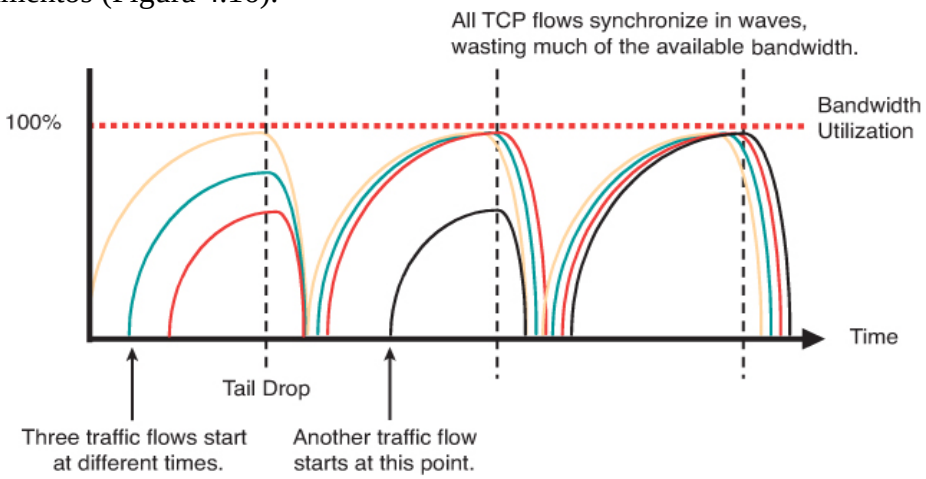

Figura 4.16: Sincronização global do TCP
(Szigeti et al. 2013)

Este tipo de descarte simultâneo é típico de quando não é feito de forma seletiva mas antes de forma indiscriminada por falta de espaço no *buffer* (*tail drop*).

4.4.1. *Random Early Detection* (RED)

O RED permite lidar com este problema. Ao contrário do *tail-drop*, em que os pacotes são colocados no *buffer* desde que haja espaço e só são descartados com o *buffer* cheio, com o RED um pacote pode ser descartado mesmo com espaço disponível para ele no *buffer*. O descarte é feito de forma aleatória, sendo que a probabilidade de ser descartado é tanto maior quanto mais cheio estiver o buffer (Figura 4.17).

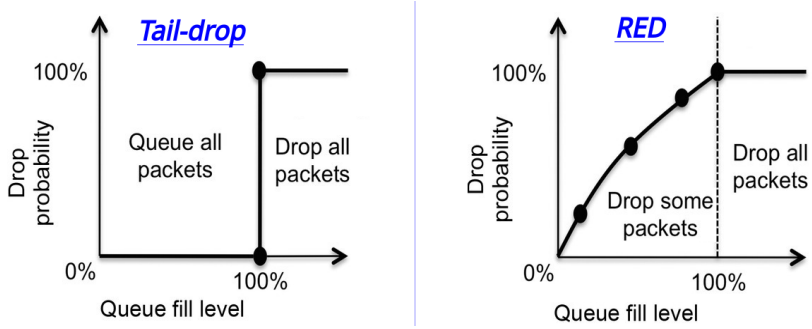

Figura 4.17: Descarte no tail-drop vs RED
Adaptado de (Barreiros and Lundqvist 2016)

O RED foi pensado para sessões TCP, mas há dúvidas sobre a sua real utilidade dada a diversidade de padrões das sessões TCP existentes atualmente e as implementações recentes do TCP, além de também não ter sido desenhado com vista ao tráfego UDP (Barreiros and Lundqvist 2016).

4.4.2. *Weighted Random Early Detection* (WRED)

A operação do WRED é similar à do RED, com a diferença de poder haver vários perfis com diferentes probabilidades de descarte para os pacotes. Com o WRED o descarte pode ser diferenciado em função da classificação dos pacotes, nomeadamente da preferência de descarte das classes AF indicada no valor DSCP. Desse modo, os pacotes marcados com maior preferência de descarte são descartados com maior probabilidade que os outros (AFx3 > AFx2 > AFx1), mesmo que já tenham entrado na fila há mais tempo (Figura 4.18).

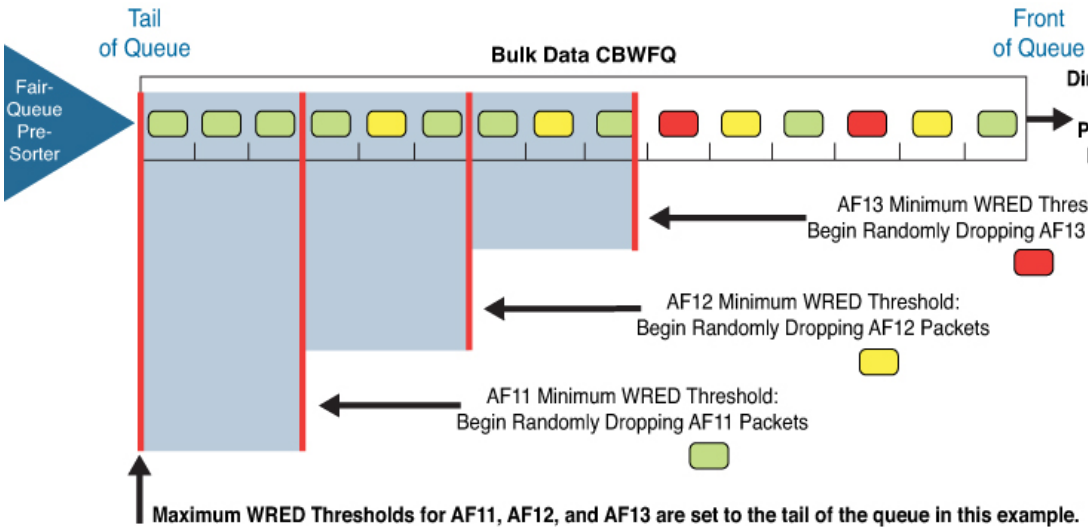

Figura 4.18: Operação WRED baseada nos valores DSCP
(Szigeti et al. 2013)

4.5. Estratégias para implementação de QoS

A implementação de mecanismos de QoS implica que os recursos da rede vão ser partilhados de forma desigual. A existência de tráfego a que vai ser atribuída prioridade de tratamento significa que vai haver outro que vai ser penalizado, pelo que um dos pontos iniciais a definir no desenho de QoS é quem vai ser beneficiado e quem vai ser prejudicado.

Application Class	Per-Hop Behavior	Admission Control	Queuing & Dropping	Application Examples
VoIP Telephony	EF	Required	Priority Queue (PQ)	Cisco IP Phones (G.711, G.729)
Broadcast Video	CS5	Required	(Optional) PQ	Cisco IP Video Surveillance / Cisco Enterprise TV
Realtime Interactive	CS4	Required	(Optional) PQ	Cisco TelePresence
Multimedia Conferencing	AF4	Required	BW Queue + DSCP WRED	Cisco Jabber, WebEx
Multimedia Streaming	AF3	Recommended	BW Queue + DSCP WRED	Cisco Digital Media System (VoDs)
Network Control	CS6		BW Queue	EIGRP, OSPF, BGP, HSRP, IKE
Call-Signaling	CS3		BW Queue	SCCP, SIP, H.323
Ops / Admin / Mgmt (OAM)	CS2		BW Queue	SNMP, SSH, Syslog
Transactional Data	AF2		BW Queue + DSCP WRED	ERP Apps, CRM Apps, Database Apps
Bulk Data	AF1		BW Queue + DSCP WRED	E-mail, FTP, Backup Apps, Content Distribution
Best Effort	DF		Default Queue + RED	Default Class
Scavenger	CS1		Min BW Queue (Deferential)	YouTube, iTunes, BitTorrent, Xbox Live

Figura 4.19: Recomendações para implementação de QoS
(Szigeti et al. 2013)

Como referência, a Figura 4.19 mostra as recomendações da Cisco para uma estratégia de QoS, baseada no RFC 4594 (Babiarz, Chan, and Baker 2006) para a definição das classes em função das aplicações, e com indicação dos mecanismos de QoS apropriados para cada uma das classes.

5. Conclusão

Com esta lição pretendeu mostrar-se as dificuldades que uma rede convergente impõe, onde diferentes tipos de aplicações têm diferentes tipos de requisitos de transmissão. Viu-se quais os principais problemas que podem influenciar a transmissão de pacotes (falta de largura de banda, latência, variação da latência e perda de pacotes) e como cada um deles influencia as diferentes aplicações.

Com esse conhecimento percebeu-se a importância da implementação de QoS numa rede, ao permitir agir sobre o tratamento dado ao tráfego, tentando adaptar as condições da rede aos requisitos do tráfego mais sensível e crítico. Para a sua implementação, deu-se a conhecer dois dos principais modelos de QoS, o IntServ e o DiffServ.

Por fim, explicaram-se os principais mecanismos usados pelos equipamento de rede para implementar QoS, nomeadamente os de classificação e marcação, policiamento, *shaping*, gestão e prevenção de congestionamento.

6. Referências Bibliográficas

Almes, G., S. Kalidindi, and M. Zekauskas. 2016. “A One-Way Delay Metric for IP Performance Metrics (IPPM).” Edited by A. Morton. https://doi.org/10.17487/RFC7679.

Babiarz, J., K. Chan, and F. Baker. 2006. “Configuration Guidelines for DiffServ Service Classes.” https://doi.org/10.17487/rfc4594.

Barreiros, Miguel, and Peter Lundqvist. 2016. *QOS-Enabled Networks : Tools and Foundations*. 2nd ed. Hoboken, United States: John Wiley and Sons Ltd.

Blake, S., D. Black, M. Carlson, E. Davies, Z. Wang, and W. Weiss. 1998. “An Architecture for Differentiated Services.” https://doi.org/10.17487/rfc2475.

Braden, R., D. Clark, and S. Shenker. 1994. “Integrated Services in the Internet Architecture: An Overview.” https://doi.org/10.17487/rfc1633.

Cisco Networking Academy, ed. 2017. *Connecting Networks v6 Companion Guide*. Cisco Press.

Cisco Systems, Inc. 2017. “CCNA R&S: Connecting Networks.” 2017. www.netacad.com.

“Cisco Visual Networking Index: Forecast and Trends, 2017-2022.” 2019. http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-481360_ns827_Networking_Solutions_White_Paper.html.

Evans, John., and Clarence. Filsfils. 2007. *Deploying IP and MPLS QoS for Multiservice Networks : Theory and Practice*. Morgan Kaufmann.

Joseph, Vinod., and Brett. Chapman. 2009. *Deploying QoS for Cisco IP and Next-Generation Networks : The Definitive Guide*. Morgan Kaufmann.

McCabe, James D. 2007. *Network Analysis, Architecture, and Design*. Elsevier/Morgan Kaufmann Publishers.

Odom, Wendell. 2004. *Cisco Qos Exam Certification Guide*. Cisco Press.

“Pergunte à ANACOM - Portal Do Consumidor.” Accessed June 25, 2019. https:/https://anacom-consumidor.inbenta.com/?content_id=990.

Peterson, Larry L., and Bruce S. Davie. 2012. *Computer Networks : A Systems Approach*. Morgan Kaufmann.

Roughan, Matthew, Subhabrata Sen, Oliver Spatscheck, and Nick Duffield. 2004. “Class-of-Service Mapping for QoS.” In *Proceedings of the 4th ACM SIGCOMM Conference on Internet Measurement - IMC ’04*, 135. New York, New York, USA: ACM Press. https://doi.org/10.1145/1028788.1028805.

Szigeti, Tim, Christina Hattingh, Robert Barton, and Kenneth Briley. 2013. *End-To-End QoS Network Design : Quality of Service for Rich-Media and Cloud Networks*. 2nd ed. Cisco Press.

Tanenbaum, Andrew S., and D. (David) Wetherall. 2011. *Computer Networks*. Pearson Prentice Hall.

Wallace, Kevin, and Kevin Wallace. 2011. *Implementing Cisco Unified Communications Voice over IP and QoS (CVOICE) Foundation Learning Guide*. Cisco Press.

Xiao, XiPeng. 2008. *Technical, Commercial, and Regulatory Challenges of QoS : An Internet Service Model Perspective*. Elsevier / Morgan Kaufmann.