

TCP/IP
QoS
Quality of Service
Resumo Arquiteturas de
Comunicação

Universidade de Aveiro

Sebastian D. González



TCP/IP
QoS
Quality of Service
Resumo Arquiteturas de
Comunicação

Dept. de Eletrónica, Telecomunicações e Informática
Universidade de Aveiro

sebastian.duque@ua.pt(103690)

23 de janeiro de 2024

Conteúdo

1	Introdução	1
2	Multiservice Networks	2
2.1	Qualidade de serviço	2
3	Como condicionar o tráfico?	5
3.1	Leaky Bucket	5
3.2	Token Bucket	6
3.3	Admission control	6
3.4	Congestion control	7
3.4.1	Tail Drop	7
3.4.2	Random Early Detection	8
3.4.3	Weighted Random Early Detection	8
3.4.4	Scheduling algorithms	9
3.4.4.1	FIFO - First In First Out	9
3.4.4.2	Priority Queueing	9
3.4.4.3	Fair Queueing	10
3.4.4.4	Weighted Fair Queueing	10
4	Integrated Services (IntServ)	11
4.1	RSVPResource Reservation Protocol RSVP	12
5	Differentiated Services (DiffServ)	13
5.0.1	Elementos funcionais	14
6	DiffServ vs Intserv	15

Lista de Figuras

2.1	Marcação de pacotes	2
2.2	Proteção de uma classe de tráfego	3
2.3	Atribuição de uma largura de banda	3
3.1	Leaky Bucket	5
3.2	Token Bucket	6
3.3	Tail Drop	7
3.4	Enter Caption	8
3.5	Enter Caption	10
4.1	Sessão RSVP	12
5.1	DiffServ vs Intserv	13
6.1	DiffServ vs Intserv	15

Glossário

DSCP Differentiated Services Code Point.

PHB Per Hop Behavior.

QoS Quality of Service.

RED Random Early Detection.

RSVP Resource Reservation Protocol.

VLL Virtual Leased Line.

WRED Weighted Random Early Detection.

Warning!!

Isto são apenas uns apontamentos realizados por uma pobre alma de MIECT, feitas a partir dos slides da disciplina e outras fontes 😈. Por favor, não usem apenas estes apontamentos como material de estudo se pretendem obter uma nota minimamente aceitável.

Dito isto, boa sorte a todos e ámen CT 🙏.

Agradecimentos aos Professores Paulo Salvador e Rui Aguiar por todo material fornecido nas aulas.

Introdução

O serviço disponível na Internet vai além dos serviços básicos de rede. Existem diversos serviços que são oferecidos na Internet, tais como Áudio/vídeo, bancos de dados, Imagens em movimento em alta definição, Redes de comunicação, "Jogos interativos"(tipo Fortinaiti e Pabagee).

Requisitos dos serviços:

⇒ Perda de pacotes

- Algumas aplicações suportam perdas de pacotes(ex: video-chamadas)
- Outras aplicações requerem 100% de sucesso na transmissão (ex transferência de arquivos, telnet)

⇒ Largura de banda

- Algumas aplicações requerem uma largura de banda mínima(ex: YouTube)
 - O buffer fica cheio
 - Grandes atrasos e algumas perdas
- Outras aplicações utilizam a largura de banda que conseguem obter (ex: "aplicações elásticas", email, transferência de arquivos)

⇒ Tempo: atraso e jitter

- Algumas aplicações requerem o mínimo de atrasos possível(ex: telefonia pela Internet, *LeagueOfLegends*, jogos multiplayer)
- Outras aplicações (não em tempo real) não apresentam limites estritos de atraso de ponta a ponta
- Algumas aplicações não reagem bem a variações de atraso (jitter)

Multiservice Networks

As aplicações multimédia assumem **best-effort network**. Como tal, existem interações entre os codecs e o comportamento da rede. As aplicações multimédia na Internet têm várias estratégias comuns:

- **Mudança dinâmica de codecs**
 - Trocando qualidade por largura de banda/resistência.
- **Armazenamento em buffer**
 - Alterando dinamicamente o tamanho do buffer.
- **Downloads progressivos**
 - Pré-carregando alguns segundos/minutos antecipadamente.

2.1 Qualidade de serviço

Para garantir a Qualidade de Serviço QoS, é necessário ter em consideração alguns princípios:

- **Marcação de pacotes**

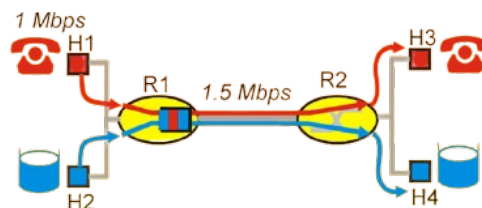


Figura 2.1: Marcação de pacotes

- É necessário a marcação de pacotes para que o router possa distinguir entre os diferentes tipos de tráfego. Para isso, novas políticas são necessárias para que o router seja capaz de fazer o tratamento dos pacotes.
- **Fornecer proteção (isolamento) de uma classe de tráfego em relação à outra**
 - Se uma dada aplicação "portar-se mal" (por exemplo, se áudio/vídeo enviar mais do que a taxa de bits declarada) é necessário haver um mecanismo de controlo que faça a marcação e policiamento na entrada da rede (para garantir a conformidade das fontes à largura de banda acordada)

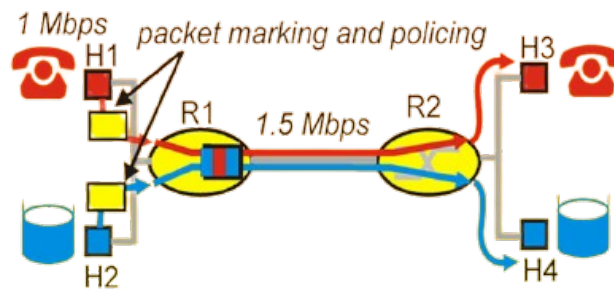


Figura 2.2: Proteção de uma classe de tráfego

- **Atribuição de uma largura de banda fixa**
 - Ao fornecer isolamento (reservar recursos dedicados a determinados fluxos), é desejável utilizar os recursos tão eficientemente quanto possível,

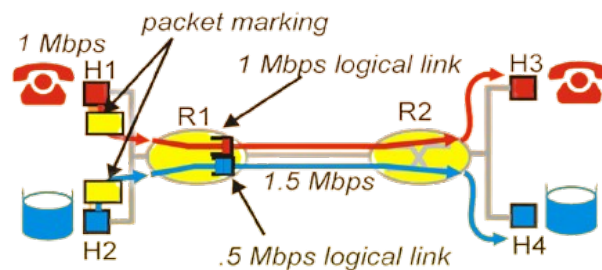
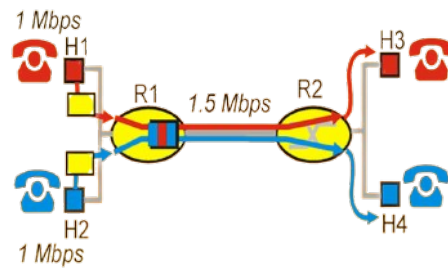


Figura 2.3: Atribuição de uma largura de banda



- Não é possível suportar pedidos que excedam a capacidade de conexão.
 - Por exemplo, numa chamada, o fluxo declara seus requisitos, e a rede pode bloquear a chamada (sinal de ocupado) se não puder suportá-los.

Como condicionar o tráfego?

Pode se fazer através de Policing ou Shaping.

- **Policing** - reduz o impacto do tráfego excessivo com perda de pacotes em excesso ou marcação com qualidade de serviço (QoS) mais baixa.
- **Shaping** - armazena tráfego, suavizando rajadas apenas permitindo o envio de tráfego a uma determinada taxa

3.1 Leaky Bucket

É um conceito utilizado para controle de tráfego de redes, especialmente na área de controle de congestionamento. Serve para evitar os congestionamentos de rede e garantir um fluxo suave de dados em uma rede.

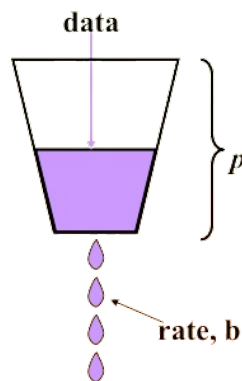


Figura 3.1: Leaky Bucket

- Dois parâmetros:
 - p : tamanho do recipiente [Bytes]
 - b : taxa de saída [B/s ou b/s]

3.2 Token Bucket

Semelhante ao Leaky bucket 3.1 o Token Bucket é um mecanismo que visa controlar o fluxo de dados na rede. Os tokens no balde representam permissões para transmitir uma unidade de dado. Se não houver tokens disponíveis, a transmissão é impedida até que tokens se tornem disponíveis.

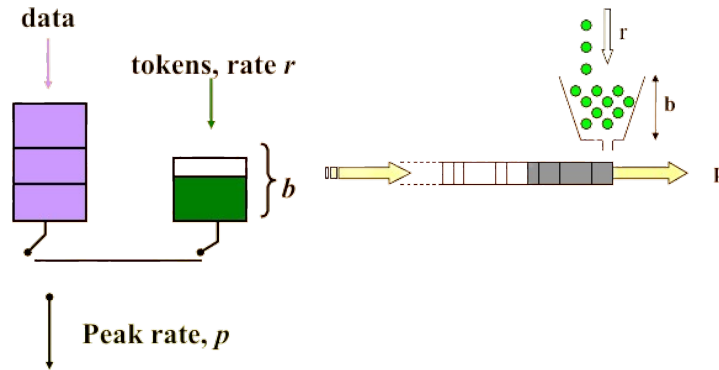


Figura 3.2: Token Bucket

- Três parâmetros:
 - b : tamanho do balde de tokens [B]
 - r : taxa de tokens [B/s ou b/s]
 - p : taxa de pico [B/s ou b/s]

Os tokens são adicionados ao balde a uma taxa constante. Essa taxa define a taxa máxima na qual os dados podem ser transmitidos e cada vez que um dado é transmitido, um token é consumido do balde. Se não houver tokens disponíveis, a transmissão é temporariamente impedida.

3.3 Admission control

Quando ocorre uma sobrecarga nos buffers do router (filas de espera), é comum descartar pacotes para evitar a sobrecarga não só nos buffers, mas também na rede como um todo. No entanto, a questão de como descartar esses pacotes é importante.

Existem várias abordagens para descartar pacotes:

1. **Último pacote a chegar:** Nesta abordagem, o último pacote que chega é descartado. Isso pode ser útil quando se deseja dar prioridade aos pacotes mais recentes em detrimento dos mais antigos.
2. **Primeiro pacote a chegar:** Aqui, o primeiro pacote que chega é descartado. Essa abordagem é útil quando se deseja dar prioridade aos pacotes mais antigos em detrimento dos mais recentes.
3. **Pacote aleatório:** Nesse caso, um pacote é escolhido aleatoriamente para ser descartado. Essa abordagem pode ser usada quando não é relevante priorizar pacotes com base em sua ordem de chegada.
4. **Pacotes diferenciados por classe:** Alguns sistemas suportam diferentes classes de serviço, cada uma com sua própria prioridade. Nesse caso, os pacotes podem ser descartados com base na classe a que pertencem, priorizando ou dando preferência a certas classes de pacotes em detrimento de outras.

3.4 Congestion control

3.4.1 Tail Drop

É uma estratégia de descarte de pacotes em que os pacotes recebidos são descartados quando o buffer está cheio.

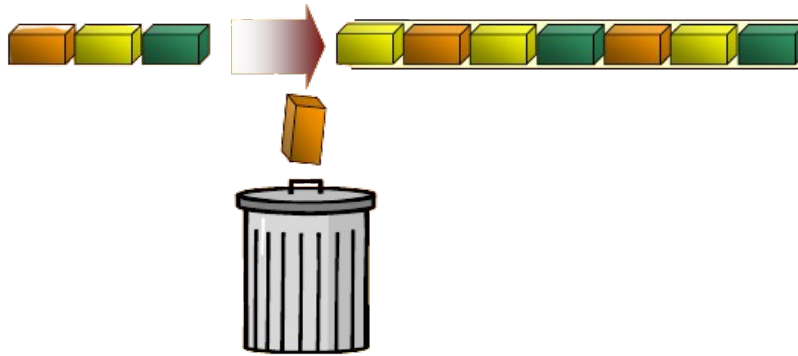


Figura 3.3: Tail Drop

Esta abordagem pode criar vários problemas e pode ser contrastada com outras estratégias de gestão de filas, como o Random Early Detection (RED) 3.4.2 , que procura descartar pacotes de forma mais controlada e preventiva antes que a fila atinja a capacidade máxima.

3.4.2 Random Early Detection

Como dito anteriormente, objetivo do RED, é evitar congestionamentos e a perda excessiva de pacotes, mantendo uma taxa de transmissão eficiente e evitando situações em que todas as filas estejam completamente cheias.

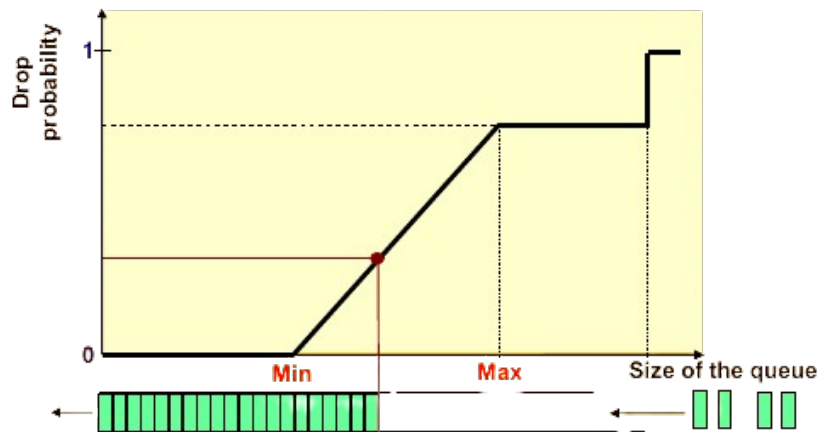


Figura 3.4: Enter Caption

Se um pacote é escolhido para descarte, isso é feito de forma aleatória, o que significa que não é sempre o último pacote a chegar, como no "tail drop". Isso proporciona uma abordagem mais justa, onde todos os pacotes têm uma chance igual de serem descartados.

3.4.3 Weighted Random Early Detection

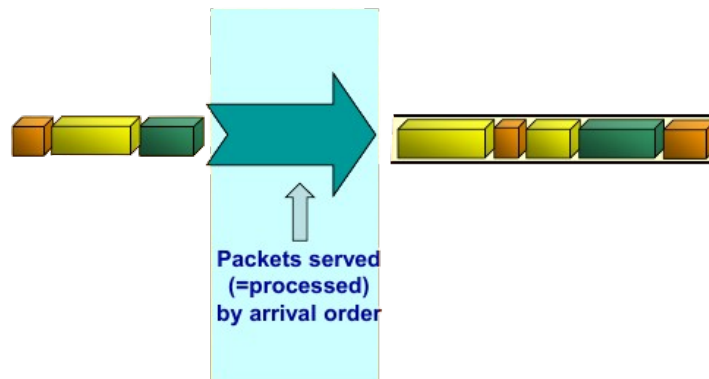
É uma extensão do RED introduz uma componente de "peso" na decisão de descartar pacotes. Em vez de simplesmente depender do comprimento absoluto da fila, o WRED leva em consideração prioridades atribuídas a diferentes classes de tráfego. Essas prioridades são definidas com base em parâmetros específicos, como a qualidade de serviço QoS desejada para cada classe de tráfego.

3.4.4 Scheduling algorithms

São utilizados para determinar a ordem em que pacotes pertencentes a diferentes fluxos são atendidos na queue.

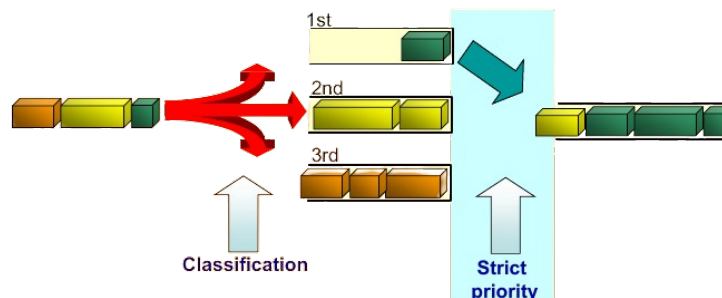
- **Work conserving scheduling** - algoritmos que buscam maximizar a utilização do servidor, assegurado que o servidor esteja sempre ocupado, desde que haja um pacote a aguardar para ser transmitido

3.4.4.1 FIFO - First In First Out



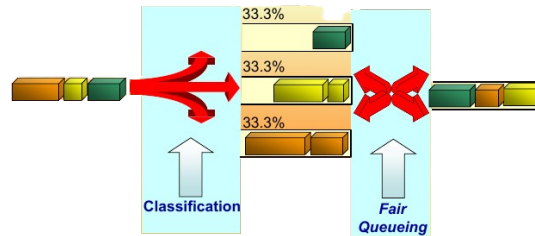
- Não realiza processamento de ordenação.
- Não permite diferenciação na qualidade de serviço.
- Fluxos com n vezes mais tráfego recebem n vezes mais serviço.
- Em filas finitas, fluxos com pacotes menores recebem mais serviço.

3.4.4.2 Priority Queueing



- Envolve a classificação do tráfego de acordo com a prioridade.
- O tráfego de maior prioridade é sempre atendido antes do tráfego de prioridades menores.
- Permite diferenciação na qualidade de serviço.
- Fluxos de maior prioridade podem impedir que fluxos de menor prioridade recebam qualquer serviço.

3.4.4.3 Fair Queueing



- Envolve a classificação do tráfego em diferentes filas.
- A largura de banda de transmissão é igualmente distribuída entre filas não vazias.
- Permite a alocação e reserva de qualidade de serviço.

3.4.4.4 Weighted Fair Queueing

- Este algoritmo assegura que cada fila atinja uma percentagem da largura de banda da conexão, pelo menos igual ao seu peso dividido pela soma dos pesos de todas as filas.

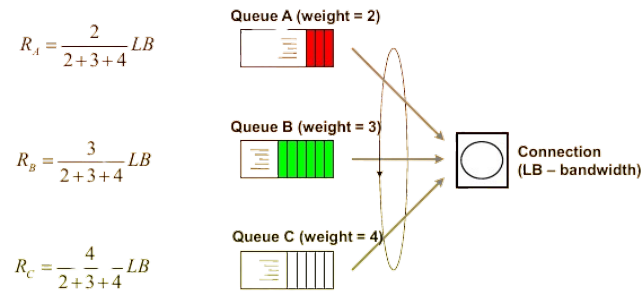
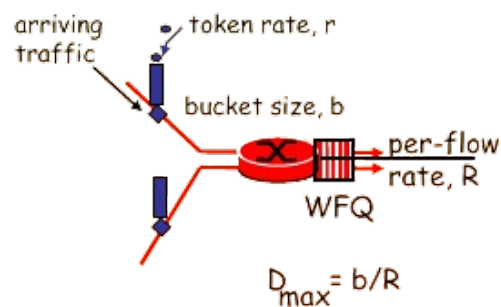


Figura 3.5: Enter Caption

Integrated Services (IntServ)

Refere-se a um modelo de serviço de rede que fornece garantias de largura de banda e qualidade de serviço para aplicações de rede. O IntServ é usado para suportar aplicações que requerem baixa latência, largura de banda garantida e qualidade de serviço consistente, como videoconferência e transmissão de áudio e vídeo em tempo real. Principais características:

- Especificações de Fluxo
- Intserv é utilizado para fluxos!
 - Routing
 - Controle de Admissão
- O remetente deve controlar o envio de pacotes usando um modelo **Token Bucket 3.2**
 - Policiamento
 - Reserva de Recursos
 - Escalonamento de Pacotes



4.1 RSVPResource Reservation Protocol RSVP

Resource Reservation Protocol (RSVP) é um protocolo de sinalização orientado para o receptor que é usado para reservar recursos em uma rede de computadores para obter um determinado nível de qualidade de serviço QoS para fluxos de aplicativos específicos. É usado para suportar aplicações que requerem baixa latência, largura de banda garantida e qualidade de serviço consistente, como videoconferência e transmissão de áudio e vídeo em tempo real. Principais características:

- RSVP é descrito na RFC 2205
 - Encapsulado em IP; tipo de protocolo = 46 (0x2E)
 - O sinal é baseado na troca de mensagens **PATH** e **RESV**:
 - * **PATH** anuncia as características de tráfego do remetente
 - * **RESV** confirma as reservas, iniciadas pelos destinatários
 - * Se a reserva não for possível, a mensagem **RESV ERR** é enviada
 - Os estados dos routers devem ser atualizados periodicamente (processo conhecido como: **Soft States**)
 - Não escalável, apenas funciona para cada fluxo

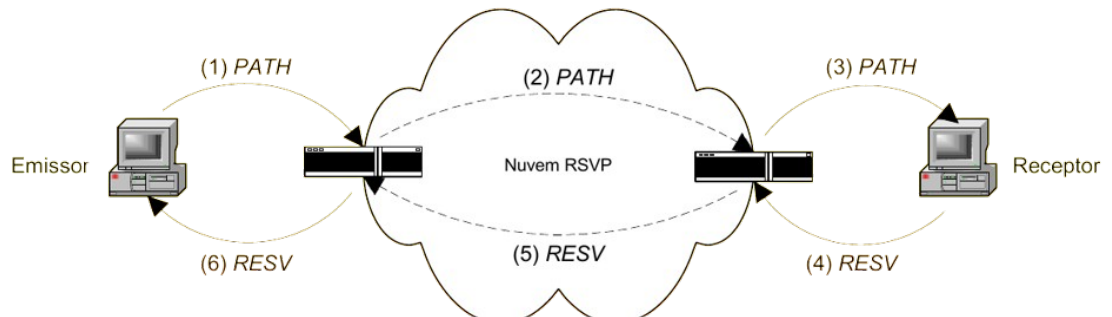


Figura 4.1: Sessão RSVP

Differentiated Services (DiffServ)

O **Differentiated Services (DiffServ)** é um modelo de serviço de rede que é usado para classificar e gerenciar o tráfego de rede, a fim de fornecer diferentes níveis de qualidade de serviço QoS para diferentes tipos de tráfego. Ao contrário do modelo **IntServ**, que fornece um mecanismo de reserva de recursos explícito para cada fluxo, o **DiffServ** classifica o tráfego em diferentes classes e fornece tratamento diferenciado com base nessa classificação. É a capacidade de discriminar serviços de maneira escalável para o núcleo, com baixa complexidade:

- Sem estado por fluxo
- Sem sinalização por fluxo

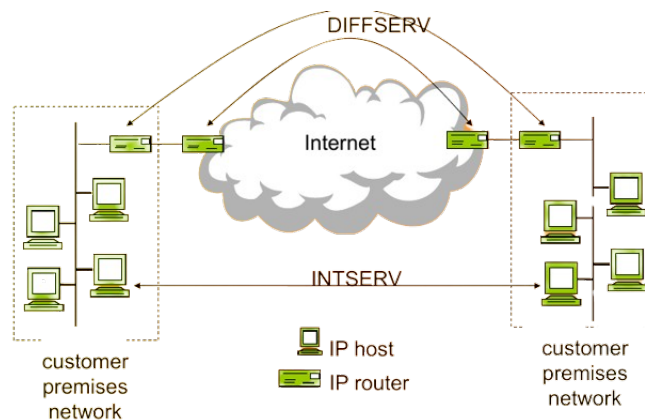


Figura 5.1: DiffServ vs Intserv

- Mais simples e eficiente do que **IntServ**:

- Com sinalização separada por serviços
- Com serviços de utilizador "mais ou menos" estáticos
- Com tráfego agregado em classes
- Sem reserva individual por link

O **DiffServ** é mais adequado para redes de grande escala e heterogêneas, onde é difícil ou impraticável estabelecer reservas e manter estados para cada fluxo e utiliza marcas simples e ferramentas de controle para simplificar a implementação no núcleo da rede (RFC2474).

5.0.1 Elementos funcionais

- **Edge (border) Routers (Fronteira):**
 - Classificam pacotes: Marcam cada pacote no campo Tipo de Serviço do cabeçalho IP.
 - Condicionamente gerenciam o tráfego: Por exemplo, eles utilizam um "Token Bucket" para verificar se o tráfego de entrada está contratado e:
 - * Atrasam o tráfego excedente ou
 - * Descartam o tráfego não conforme.
- **Routers de Núcleo (Internos):**
 - Identificam o tratamento a ser dado aos pacotes com base nas marcações e conforme um comportamento por salto Per Hop Behavior (PHB) definido.
- **PHB** - define a política e a prioridade aplicada a um pacote quando ele transita por um salto (como um roteador) em uma rede **DiffServ**. Existem dois tipos:
 - Default (DE) \rightarrow DSCP = 000000
 - * Serviço best-effort com uma única fila, gerida por FIFO.
 - AF (Assured Forwarding) (RFC2597) \rightarrow DSCP = 101110
 - * Fornece várias classes de forwarding, cada uma com diferentes níveis de precedência e drop. Ele permite a alocação de diferentes níveis de recursos de rede a diferentes classes de tráfego, permitindo que os pacotes sejam transmitidos com base em políticas específicas de drop e atraso
 - EF (Expedited Forwarding) (RFC2598) \rightarrow DSCP = aaadd0
 - * Serviço Virtual Leased Line (VLL), para tráfego crítico com Baixa latência, pouca variação no atraso, sem perdas. Os nós devem encaminhar esses pacotes o mais rápido possível. Os pacotes não podem ser perdidos ou reordenados.

DiffServ vs Intserv

	INTSERV	DIFFSERV
signaling	By the application	Network management, application
granularity	Flow	flow, source, site (aggregation)
mechanism	Endereço de destino, protocolo e número de porto	Classe de pacotes (outros mecanismos possíveis)
scope	End-to-end	Between networks, E2E

Figura 6.1: DiffServ vs Intserv