

# Perguntas mais freqüentes sobre QoS

## Índice

[Introdução](#)

[Geral](#)

[Classificação e marcação](#)

[Gerenciamento de enfileiramento e de congestionamento](#)

[Detecção antecipada aleatória ponderada \(WRED\) para prevenção de congestionamentos](#)

[Vigilância e molde](#)

[Frame Relay de Qualidade de serviço \(QoS\)](#)

[Qualidade de serviço \(QoS\) sobre ATN \(modo de transferência assíncrono\)](#)

[Voz e Qualidade de Serviço \(QoS\)](#)

[Informações Relacionadas](#)

## Introdução

Este documento abrange as Perguntas Mais Frequentes (FAQs) relacionados à Qualidade de Serviço (QoS).

## Geral

### Q. Que é Qualidade de Serviço (QoS)?

A. QoS refere a capacidade de uma rede para proporcionar o melhor serviço ao tráfego de rede selecionado sobre as várias tecnologias subjacentes que incluem o Frame Relay, o Asynchronous Transfer Mode (ATM), os Ethernet e as 802.1 redes, SONET, e redes IP-roteados.

QoS é uma coleção de tecnologias que permitem que aplicativos requisitem e recebam níveis de serviços previsíveis em termos de capacidade de throughput de dados (largura de banda), variações de latência (jitter) e retardo. Em especial, os recursos QoS fornecem um serviço de rede melhor e mais previsível através dos seguintes métodos:

- Largura de banda dedicada de apoio.
- Melhoria das características de perda.
- Impedindo e gerenciando o congestionamento de rede.
- Dando forma ao tráfego de rede.
- Definindo prioridades de tráfego na rede.

O Internet Engineering Task Force (IETF) define as duas arquiteturas a seguir para o QoS:

- Serviços Integrados (IntServ)
- Serviços diferenciados (DiffServ)

O IntServ usa o protocolo de reserva de recursos (RSVP, Resource Reservation Protocol) para

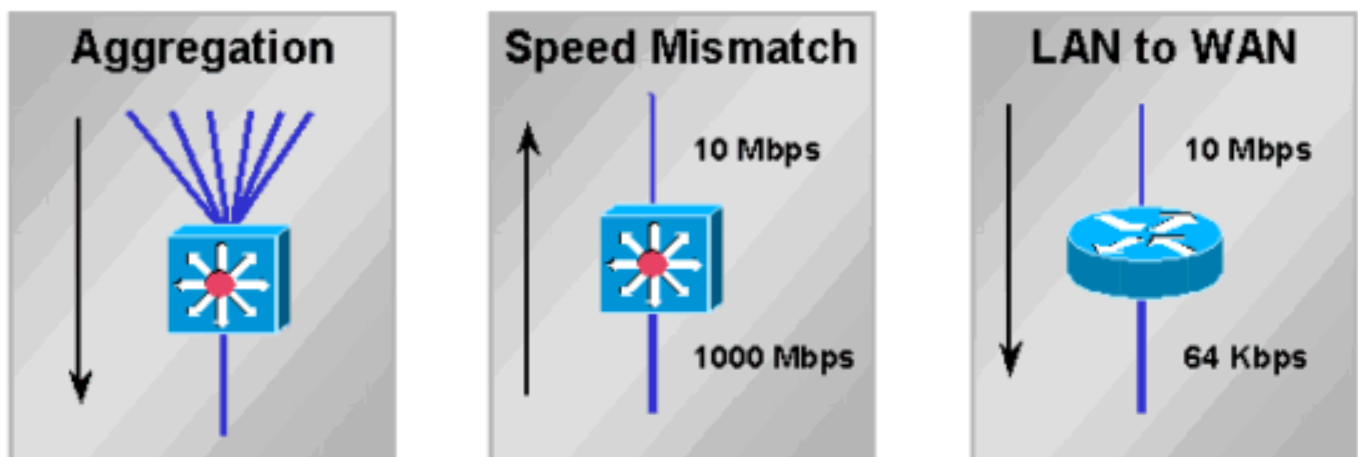
sinalizar explicitamente as necessidades de QoS de tráfego de um aplicativo com os dispositivos no caminho de ponta a ponta através da rede. Se cada dispositivo da rede ao longo do caminho puder reservar a largura de banda necessária, o aplicativo de origem pode iniciar a transmissão. A solicitação para comentários (RFC) 2205 define o RSVP, e o RFC 1633 define IntServ.

Focos do DiffServ em QoS agregado e fornecida. Em vez de sinalizar as exigências de QoS do aplicativo, o DiffServ usa um Ponto de Código DiffServ (DSCP) no cabeçalho de IP para indicar os níveis de QoS necessários. O Cisco IOS® Software Release 12.1(5)T introduziu a conformidade DiffServ nos Cisco routers. Para obter mais informações, consulte os seguintes documentos:

- [Serviço integrado no Cisco IOS 12.1](#)
- [Implementing DiffServ for End-to-End Quality of Service \(Implementando o DiffServ para a qualidade de serviço de ponta a ponta\)](#)
- [Implementando políticas de qualidade do serviço com DSCP](#)

### Q. O que são congestionamento, retardo e variação de sinal?

A. Uma relação experimenta a congestão quando é apresentado com mais tráfego do que ele pode segurar. Os pontos de congestão da rede são fortes candidatos para mecanismos de Qualidade de Serviço (QoS). A seguir está um exemplo de pontos de congestão típicos:



O congestionamento de rede resulta em atraso. Uma rede e seus dispositivos introduzem diversos tipos dos atrasos, como explicado [compreender em retardos na rede de voz de pacote de informação](#). [A variação no retardo é conhecida como jitter, conforme explicado em Entendendo jitter nas redes de voz de pacote de informação \(plataformas Cisco IOS\)](#). Necessidade do retardo e tremulação de ser controlado e minimizado para apoiar o tempo real e o tráfego interativo.

### Q. O que é MQC?

A. O MQC representa o comando line interface(cli) da Qualidade de Serviço modular (QoS). É projetado simplificar a configuração de QoS em roteadores Cisco e em Switches definindo um grupo comum da sintaxe de comando e resultar de comportamentos de QoS através das Plataformas. Este modelo substitui o modelo anterior de definição de sintaxes exclusivas para cada recurso QoS e para cada plataforma.

O MQC contém os três seguintes passos:

1. Defina uma classe de tráfego emitindo o **comando class-map**.
2. Crie uma política de tráfego, associando a classe de tráfego a um ou mais recursos de QoS por meio da emissão do comando `policy-map`.
3. Anexe a política de tráfego à relação, à subinterface, ou ao virtual circuit (VC) emitindo o **comando service-policy**.

**Nota:** Implemente as funções de condicionamento de tráfego de DiffServ, como marcação e modelagem, usando a sintaxe MQC.

Para mais informação, refira a [interface de Command-Line Qualidade de Serviço Modular](#).

## Q. O que a mensagem a política de serviço é suportada somente em interfaces VIP com DCEF habilitado significa?

A. No Versatile Interface Processors (VIP) em um Cisco 7500 Series, somente as características distribuídas do Qualidade de Serviço (QoS) são apoiadas até à data do Cisco IOS 12.1(5)T, do 12.1(5)E, e do 12.0(14)S. Permitir o Distributed Cisco Express Forwarding (dCEF) permite automaticamente o QoS distribuído.

Interfaces não-VIP, conhecidas como IPs (Processadores de interface) herdados, suportam recursos de QoS central como ativados no RSP (Processador de rota/Switch). Para obter mais informações, consulte os seguintes documentos:

- [Class-Based Weighted Fair Queueing distribuído e Weighted Random Early Detection distribuído](#)
- [Low latency queueing distribuído](#)
- [Molde de tráfego distribuído](#)
- [FRF.11 e FRF.12 distribuídos com base no processador de interface versátil para o Cisco IOS versão 12.1 T](#)

## Q. Quantas classes fazem um suporte à política do Qualidade de Serviço (QoS)?

A. Em versões do Cisco IOS anteriores a 12.2, é possível definir um máximo de 256 classes e seriam definidas até 256 classes dentro de cada política se as mesmas classes forem reutilizadas para políticas diferentes. Se você tem duas políticas, o número total de classes de ambas as políticas não deve exceder o 256. Se uma política inclui o Class-Based Weighted Fair Queueing (CBWFQ) (o significar contém uma indicação do [or priority] da largura de banda dentro de algumas das classes), o número total de classes apoiadas é 64.

Nas versões do Cisco IOS 12.2(12), 12.2(12)T, e no 12.2(12)S, esta limitação dos mapas de classe 256 globais foi mudada, e é agora possível configurar até 1024 mapas de classe globais e usar os mapas de classe 256 dentro do mesmo mapa de política.

## Q. Como as atualizações de roteamento e o Keepalives do Point-to-Point Protocol (PPP)/High-Level Data Link Control (HDLC) são processados quando uma política de serviços é aplicada?

A. O Roteadores do Cisco IOS usa os seguintes dois mecanismos para dar a prioridade a pacotes de controle:

- Precedência de IP
- pak\_priority

Ambos os mecanismos foram projetados para garantir que os principais pacotes de informações de controle não sejam soltos ou sejam soltos por último pelo roteador e pelo sistema de fila quando uma interface externa estiver congestionada. [Para obter mais informações, consulte Entendendo como Atualizações de Roteamento e Pacotes de Controle são Enfileirados em uma Interface com uma Política de Serviço QoS.](#)

## Q. O Qualidade de Serviço (QoS) é apoiado nas relações configuradas com Integrated Routing and Bridging (IRB)?

A. Não. Você não pode configurar features de QoS quando a relação é configurada para o IRB.

## Classificação e marcação

### Q. O que é pré-classificação QoS (Qualidade de Serviço)?

A. A pre-classificação de QoS permite-o de combinar sobre e classificar os índices do cabeçalho de IP original dos pacotes que submetem-se ao encapsulamento de túnel e/ou à criptografia. Esta característica não descreve o processo de copiar o valor original do byte do Tipo de serviço (ToS) do cabeçalho de pacote original ao cabeçalho de túnel. Para obter mais informações, consulte os seguintes documentos:

- [Configurando QoS para redes privadas virtuais](#)
- [Qualidade de Serviço para Redes Particulares Virtuais, Módulo de Recurso 12.2\(2\)](#)

### Q. Quais campos de cabeçalho de pacotes podem ser marcados? Que valores estão disponíveis?

A. O recurso de marcação com base em classe permite que você defina ou marque o cabeçalho da MPLS (switching de rótulo multiprotocolo), da camada 2 ou camada 3 dos seus pacotes. Para obter mais informações, consulte os seguintes documentos:

- [Configurando a marcação do pacote baseado em classe](#)
- [Quando um roteador define o bit CLP em uma célula ATM?](#)
- [Configurando a marcação de pacote em PVCs de Frame Relay](#)

### Q. Posso dar prioridade ao tráfego com base no URL?

A. Sim. O NBAR (Reconhecimento de aplicativo baseado em rede) permite que você classifique pacotes, comparando campos na camada do aplicativo. Antes da introdução de NBAR, a maioria de classificação granular era números de porta do Transmission Control Protocol (TCP) e do User Datagram Protocol (UDP) da camada 4. Para obter mais informações, consulte os seguintes documentos:

- [Reconhecimento de aplicativo baseado em rede Q&A](#)
- [Rede de aplicação de NBAR](#)
- [Utilizando Reconhecimento de Aplicativos Baseados em Rede e Listas de Controle de](#)

[Acesso para Bloqueio de Worm de Código Vermelho](#)

- [Como proteger sua rede contra o vírus Nimda](#)

## Q. Que plataformas e versões de Cisco IOS Software suportam reconhecimento de aplicativo baseado em rede (NBAR)?

A. O apoio para o NBAR é introduzido nas seguintes versões de Cisco IOS Software:

Plataforma	Versão mínima do Cisco IOS Software
7200	12.1(5)T
7100	12.1(5)T
3660	12.1(5)T
3640	12.1(5)T
3620	12.1(5)T
2600	12.1(5)T
1700	12.2(2)T

**Nota:** É necessário habilitar o Cisco Express Forwarding (CEF) para utilizar o NBAR.

O nbar distribuído (DNBAR) está disponível nas seguintes Plataformas:

Plataforma	Versão mínima do Cisco IOS Software
7500	12.2(4)T, 12.1(6)E
FlexWAN	12.1(6)E

**Nota:** A NBAR não é suportada em interfaces VLAN da MSFC (Placa de recurso de Switch multicamada) do Catalyst 6000 no Cisco série 12000 ou no RSM (Módulo de comutação de rota) para o Catalyst série 5000. Se você não vê uma plataforma particular alistada acima, contacte por favor seu representante técnico de Cisco.

## Gerenciamento de enfileiramento e de congestionamento

### Q. Que é a finalidade do enfileiramento?

A. Enfileirar-se está projetado acomodar o congestionamento temporário em uma relação de dispositivo de rede armazenando pacotes adicionais nos buffers até que a largura de banda se torne disponível. Os roteadores Cisco IOS suportam diversos métodos de enfileiramento para satisfazer as exigências variáveis de largura de banda, variação de sinal e retardo de diferentes aplicativos.

O mecanismo padrão na maioria das interfaces é First In First Out (FIFO). Alguns tipos de tráfego têm requisitos de atraso/variação de sinal mais rígidos. Assim, um dos mecanismos alternativos de enfileiramento a seguir deve ser configurado ou está habilitado por padrão:

- Weighted-Fair Queuing (WFQ)
- Enfileiramento moderado ponderado com base em classe (CBWFQ)

- LLQ (Enfileiramento de Baixa Latência), que é na verdade o CBWFQ com uma PQ (Fila de Prioridade) (conhecida como PQCBWFQ)
- Priority Queueing (PQ)
- Custom Queueing (CQ)

O enfileiramento geralmente só acontece nas interfaces externas. Um roteador enfileira pacotes que estão saindo de uma interface. Você pode policiar o tráfego de entrada, mas geralmente você não pode enfileirar de entrada (uma exceção é colocação em buffer de lado de receptor em um Cisco 7500 Series Router que usa o Distributed Cisco Express Forwarding (dCEF) para enviar pacotes do ingresso à interface de saída; para mais informação, refira [compreendendo o CPU VIP executando a 99% e lado RX em buffer](#). Em plataformas de produto avançado distribuídas, como as séries Cisco 7500 e 12000, a interface de entrada pode utilizar seus próprios buffers de pacote para armazenar tráfego em excesso comutado para uma interface de saída congestionada seguindo a decisão de switching da interface de entrada. Em condições raras, geralmente quando a interface de entrada está alimentando uma interface de saída mais lenta, a interface de entrada pode passar por erros ignorados de acréscimo quando ela funciona fora da memória do pacote. O excesso de congestionamento pode levar a quedas de filas de saída. Quedas de fila de entrada têm uma causa-raiz diferente na maioria das vezes. Para obter mais informações sobre Troubleshooting de queda, consulte o seguinte documento:

- [Troubleshooting de Quedas de Fila de Entrada e Quedas de Fila de Saída](#)

Para obter mais informações, consulte os seguintes documentos:

- [Troubleshooting de Erros "Ignorados" em um ATM Port Adapter](#)
- [Troubleshooting de Erros Ignorados e Quedas Sem Memória no Cisco 12000 Series Internet Router](#)

## Q. Como os padrões WFQ e CBWFQ funcionam?

A. O enfileiramento considerável procura atribuir uma parte justa da largura de banda de uma relação entre conversações ativa ou o IP flui. Ele classifica os pacotes em subfilas, identificados por um número de identificação de conversação, usando um algoritmo de hashing baseado em vários campos do cabeçalho de IP e no tamanho do pacote. A seguir você saberá como é calculado o peso:

- $W = K / (\text{precedência} + 1)$

K= 4096 com Cisco IOS 12.0(4)T e versões anteriores, e 32384 com 12.0(5)T e versões posteriores.

Quanto menor o peso, maior é a prioridade e o compartilhamento da largura de banda. Além do peso, o comprimento do pacote é levado em consideração.

O CBWFQ permite que você defina uma classe de tráfego e atribua-lhe uma garantia de largura de banda mínima. O algoritmo por trás desse mecanismo é o WFQ, o que explica o nome. Para configurar CBWFQ, defina classes específicas em instruções com classes de mapas. Então você atribui uma política a cada classe em um mapa de política. Esse mapa de política será anexado externamente a uma interface. Para obter mais informações, consulte os seguintes documentos:

- [Compreendendo a classe baseada em Weighted Fair Queuing em ATM](#)
- [Compreendendo a Weighted Fair Queuing em ATM](#)

**Q. Se uma classe do CBWFQ (Enfileiramento Justo e Ponderado Baseado em Classes) não está usando sua largura de banda, outras classes podem usar a largura de banda?**

A. Sim. Embora as garantias de largura de banda fornecidas emitindo os comandos bandwidth e priority tenham sido descritas com palavras como reserved e bandwidth to be set aside, nenhum dos comandos implementa uma reserva verdadeira. Significa que se uma classe de tráfego não estiver usando sua largura de banda configurada, qualquer largura de banda não utilizada é compartilhada entre as outras classes.

O sistema de filas impõe uma exceção importante a essa regra, com uma classe de prioridade. Conforme observado acima, a carga oferecida de uma classe de prioridade é medida por um vigilante de tráfego. Durante condições de congestionamento, uma classe de prioridade não pode usar excesso de largura de banda. [Para obter mais informações, consulte Comparando os comandos bandwidth e priority de uma política de serviços de QoS.](#)

**Q. O Class Based Weighted Fair Queueing (CBWFQ) é apoiado em subinterfaces?**

A. As interfaces lógicas do Cisco IOS não têm suporte inerente para um estado de congestionamento e não suportam a aplicação direta de uma política de serviços que inclua um método de enfileiramento. Em vez disso, é preciso primeiro aplicar modelagem à subinterface, utilizando GTS (Modelagem de Tráfego Genérico) ou modelagem baseada em classe. [Para obter mais informações, consulte Applying QoS Features to Ethernet Subinterfaces \(Aplicando recursos de QoS a subinterfaces Ethernet\).](#)

**Q. Qual é a diferença entre as instruções de prioridade e largura de banda em um mapa de política?**

A. Os comandos priority e bandwidth diferem em ambas funcionalidades e quais as aplicações eles tipicamente suportam. A tabela a seguir resume estas diferenças:

Função	Comando bandwidth	Comando priority
Garantia de largura de banda mínima	Sim	Sim
Garantia máxima de largura de banda	Não	Sim
Policer embutido	Não	Sim
Fornece latência baixa	Não	Sim

[Para obter mais informações, consulte Comparando os comandos bandwidth e priority de uma política de serviços de QoS.](#)

**Q. Como é calculado o limite de fila no FlexWAN e no VIP (Processadores de Interface Versáteis)?**

A. O suficiente SRAM presumido no VIP ou no FlexWAN, o limite de fila é calculado com base em um atraso máximo de 500ms com tamanho médio do pacote de 250 bytes. O seguinte é um exemplo de uma classe com o mbps de largura de banda um:

Limite da fila =  $1000000 / (250 \times 8 \times 2) = 250$

Limites de fila menores são atribuídos à medida que a quantidade de memória de pacotes disponíveis diminui e com um número maior de Circuitos Virtuais (VCs).

No exemplo a seguir, um PA-A3 está instalado em uma placa FlexWAN para o Cisco 7600 Series e está suportando diversas subinterfaces com Circuitos virtuais permanentes (PVCs) de 2 MB. A política de serviço é aplicada a cada VC.

```
class-map match-any XETRA-CLASS
  match access-group 104
class-map match-any SNA-CLASS
  match access-group 101
  match access-group 102
  match access-group 103
policy-map POLICY-2048Kbps class XETRA-CLASS bandwidth 320 class SNA-CLASS bandwidth 512
interface ATM6/0/0 no ip address no atm sonet ilmi-keepalive no ATM ilmi-keepalive ! interface
ATM6/0/0.11 point-to-point mtu 1578 bandwidth 2048 ip address 22.161.104.101 255.255.255.252 pvc
ABCD class-vc 2048Kbps-PVC service-policy out POLICY-2048Kbps
```

A interface do Modo de transferência assíncrono (ATM) obtém um limite de fila para toda a interface. O limite é uma função do total de buffers disponíveis, o número de interfaces físicas no FlexWAN e o retardo máximo de enfileiramento permitido na interface. Cada PVC obtém uma parte do limite da interface com base na SCR (Taxa média de células) ou na MCR (Taxa mínima de células) do PVC, e cada classe obtém uma parte do limite do PVC com base na sua alocação de largura de banda.

A seguinte saída de exemplo do comando show policy-map interface é derivada de um FlexWAN com buffers globais 3687. Emita o comando show buffer para ver esse valor. Cada PVC de 2 Mbps recebe 50 pacotes com base na largura de banda de PVC de 2 Mbps ( $2047/149760 \times 3687 = 50$ ). Cada classe é atribuída então uma parcela dos 50 pés, segundo as indicações da seguinte saída:

```
service-policy output: POLICY-2048Kbps
  class-map: XETRA-CLASS (match-any)
    687569 packets, 835743045 bytes
    5 minute offered rate 48000 bps, drop rate 6000 BPS
  match: access-group 104
    687569 packets, 835743045 bytes
    5 minute rate 48000 BPS
    queue size 0, queue limit 7 packets output 687668, packet drops 22 tail/random drops 22,
no buffer drops 0, other drops 0 bandwidth: kbps 320, weight 15 class-map: SNA-CLASS (match-any)
2719163 packets, 469699994 bytes 5 minute offered rate 14000 BPS, drop rate 0 BPS match: access-
group 101 1572388 packets, 229528571 bytes 5 minute rate 14000 BPS match: access-group 102
1146056 packets, 239926212 bytes 5 minute rate 0 BPS match: access-group 103 718 packets, 245211
bytes 5 minute rate 0 BPS queue size 0, queue limit 12 packets output 2719227, packet drops 0
tail/random drops 0, no buffer drops 0, other drops 0 bandwidth: kbps 512, weight 25 queue-limit
100 class-map: class-default (match-any) 6526152 packets, 1302263701 bytes 5 minute offered rate
44000 BPS, drop rate 0 BPS match: any 6526152 packets, 1302263701 bytes 5 minute rate 44000 BPS
queue size 0, queue limit 29 packets output 6526840, packet drops 259 tail/random drops 259, no
buffer drops 0, other drops 0
```

Se os seus fluxos de tráfego usarem tamanhos de pacotes grandes, a saída do comando show policy-map interface poderá reportar um valor incremental para o campo no buffer drops, pois você poderá ficar sem buffers antes de atingir o limite de filas. Neste caso, tente manualmente ajustar abaixo do fila-limite em classes da NON-prioridade. Para mais informação, refira a [compreensão do transmitir limite de fila com IP to ATM CoS](#).

**Q. Como você verifica o valor de limite da fila?**



A. Em plataformas não distribuídas, o limite de fila é 64 pacotes à revelia. A saída de exemplo a seguir foi capturada em um Cisco 3600 Series Router:

```
november# show policy-map interface s0 Serial0 Service-policy output: policy1 Class-map: class1
(match-all) 0 packets, 0 bytes 5 minute offered rate 0 BPS, drop rate 0 BPS Match: ip precedence
5 Weighted Fair Queueing Output Queue: Conversation 265 Bandwidth 30 (kbps) Max Threshold 64
(packets) !--- Max Threshold is the queue-limit. (pkts matched/bytes matched) 0/0 (depth/total
drops/no-buffer drops) 0/0/0 Class-map: class2 (match-all) 0 packets, 0 bytes 5 minute offered
rate 0 BPS, drop rate 0 BPS Match: ip precedence 2 Match: ip precedence 3 Weighted Fair Queueing
Output Queue: Conversation 266 Bandwidth 24 (kbps) Max Threshold 64 (packets) (pkts
matched/bytes matched) 0/0 (depth/total drops/no-buffer drops) 0/0/0 Class-map: class-default
(match-any) 0 packets, 0 bytes 5 minute offered rate 0 BPS, drop rate 0 BPS Match: any
```

## Q. Posso habilitar o fair queueing dentro de uma classe?

A. O Cisco 7500 Series com QoS (Qualidade de serviço) distribuída suporta enfileiramento moderado por classe. Outras Plataformas, incluindo o Cisco 7200 Series e o Cisco 2600/3600 Series, apoio tornaram mais pesado o enfileiramento considerável (WFQ) na classe de padrão classe; todas as classes de largura de banda usam FIFO.

## Q. Quais comandos posso usar para monitorar o enfileiramento?

A. Use os comandos seguintes monitorar o enfileiramento:

- **show queue {interface} {interface number}** - Em plataformas do IOS da Cisco diferentes do Cisco 7500 Series, este comando indica as filas ou as conversações ativas. Se a interface ou Circuito Virtual (VC) não estiver congestionado, nenhuma fila será listada. Na Série Cisco 7500, o comando show queue não é suportado.
- [\[vc \[\[vpi/\] vci do show queueing interface interface-number\]](#) - Isto indica as estatísticas de enfileiramento de uma relação ou de um VC. Mesmo quando não há nenhuma congestão, você ainda poderá ver aqui algumas batidas. A razão para isso é que os pacotes de processo comutados são sempre contados, independentemente de haver congestionamento. O Cisco Express Forwarding (CEF) e os pacotes de Fast-Switched não são contados, a menos que haja congestionamento. Os mecanismos de filas do legado como o Priority Queueing (PQ), o Custom Queueing (CQ), e o enfileiramento considerável tornado mais pesado (WFQ), não fornecerão estatísticas de classificação. Somente a interface da linha de comando da Qualidade de Serviço modular (MQC) - características baseadas nas imagens mais tarde do que 12.0(5)T fornece estas estatísticas.
- **show policy interface {interface}{interface number}** - o contador de pacotes conta o número de pacotes que correspondem aos critérios da classe. Esse contador é incrementado estando a interface congestionada ou não. Os `pacotes combinados` contra indicam o número de pacotes que combinam os critérios da classe quando a relação foi congestionada. Para obter informações adicionais sobre os contadores de pacote, consulte o seguinte documento: [Compreendendo os contadores de pacotes na saída de show policy-map interface](#)
- Configuração de QoS com base na classe de Cisco e estatísticas MIB - Fornece potencialidades de monitoramento do Simple Network Management Protocol (SNMP).

Q. O RSVP pode ser usado conjuntamente com o Class Based Weighted Fair Queueing (CBWFQ). Quando o Resource Reservation Protocol (RSVP) e o CBWFQ estão configurados para uma interface, eles atuam independentemente,

exibindo o mesmo comportamento que teriam se estivessem em execução isoladamente? O RSVP parece comportar-se como se o CBWFQ não é configurado em relação à disponibilidade de largura de banda, à avaliação, e à atribuição.

A. Ao usar RSVP e CB-WFQ na versão 12.1(5)T e mais recente do Software Cisco IOS, o roteador pode operar de modo que os fluxos de RSVP e as classes de CBWFQ compartilhem a largura de banda disponível em uma interface ou PVC, sem esgotamento.

O Software IOS Versão 12.2(1)T e posterior permite que o RSVP faça o controle de admissão usando o seu próprio pool "ip rsvp bandwidth", enquanto o CBWFQ faz a classificação, a vigilância e a programação de pacotes RSVP. Isso pressupõe pacotes pré-marcados pelo remetente e que os pacotes não-RSVP são marcados de forma diferente.

## Detecção antecipada aleatória ponderada (WRED) para prevenção de congestionamentos

**Q. Posso ativar ao mesmo tempo Weighted Random Early Detection (WRED) e Low Latency Queueing (LLQ) ou Class Based Weighted Fair Queueing (CBWFQ)?**

A. Sim. O enfileiramento define a ordem dos pacotes que deixam a fila. Isto significa que ele define um mecanismo de programação de pacote. Igualmente pode ser usado para fornecer a atribuição e as garantias de largura de banda mínima da largura de banda considerável. Em contraste, a Solicitação de comentário (RFC) 2475 define queda como o processo de descartar pacotes com base em regras especificadas. O mecanismo de queda padrão é a queda traseira, na qual a interface derruba pacotes quando a fila está cheia. Um mecanismo alternativo de queda é Random Early Detection (RED) e o WRED de Cisco, que começa a deixar cair pacotes aleatoriamente antes da fila está completo e procura manter uma profundidade média da fila consistente. A WRED utiliza valor de precedência de IP de pacotes para tomar uma decisão de queda diferenciada. Para mais informação, refira o [Weighted Random Early Detection \(WRED\)](#).

**Q. Como posso eu monitorar o Weighted Random Early Detection (WRED) e o ver realmente tomar o efeito?**

A. O WRED monitora a profundidade média da fila e começa a deixar cair pacotes quando o valor calculado vai acima do valor mínimo de limiar. Emita o **comando show policy-map interface** e monitore o valor médio da profundidade de fila, segundo as indicações do exemplo seguinte:

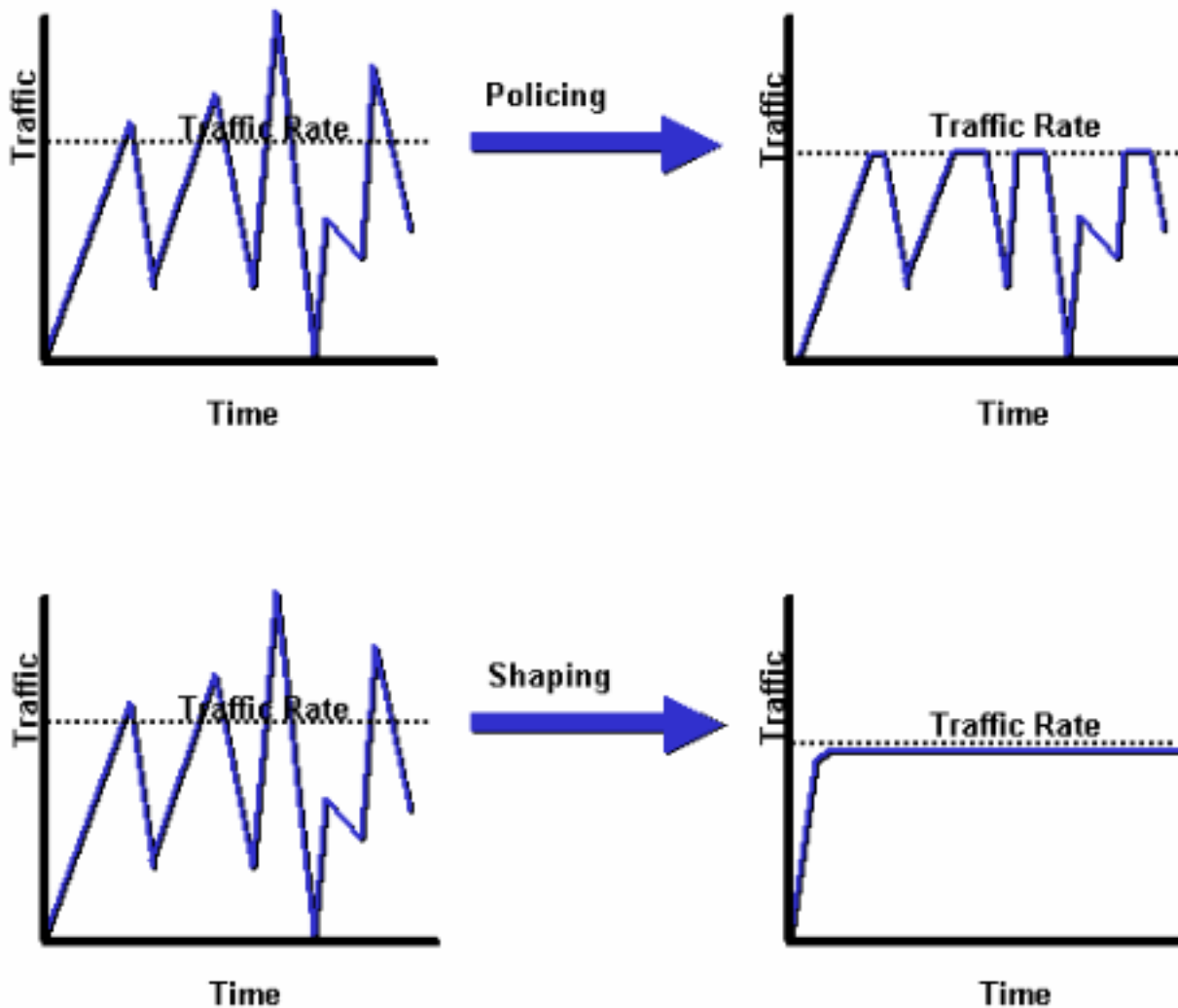
```
Router# show policy interface s2/1 Serial2/1 output : p1 Class c1 Weighted Fair Queueing Output
Queue: Conversation 265 Bandwidth 20 (%) (pkts matched/bytes matched) 168174/41370804 (pkts
discards/bytes discards/tail drops) 20438/5027748/0 mean queue depth: 39 Dscp Random drop Tail
drop Minimum Maximum Mark (Prec) pkts/bytes pkts/bytes threshold threshold probability 0(0)
2362/581052 1996/491016 20 40 1/10 1 0/0 0/0 22 40 1/10 2 0/0 0/0 24 40 1/10 [output omitted]
```

## Vigilância e molde

**Q. Qual a diferença entre vigilância e modelagem?**

A. O diagrama a seguir ilustra a diferença principal: O modelagem de tráfego retém pacotes adicionais em uma fila e programa então o excesso para uma transmissão mais atrasada sobre incrementos do tempo. O resultado da modelagem de tráfego é uma taxa de saída de pacote

facilitada. Em contrapartida, a vigilância de tráfego propaga bursts. Quando a taxa de tráfego atinge a taxa máxima configurada, o tráfego de excesso é liberado (ou remarcado). O resultado é uma taxa de saída que aparece como um dente de serra com picos e depressões.



Para mais informação, refira a [visão geral de molde e vigilância](#).

## Q. Que são um Token Bucket e como o algoritmo trabalham?

A. Um token bucket propriamente dito não possui política de descarte ou prioridade. A seguir, há um exemplo de como funciona a metáfora do token bucket:

- Os tokens são colocados em um bucket a uma certa taxa.
- Cada token é uma permissão para que a origem envie um determinado número de bits.
- Para enviar um pacote, o regulador de tráfego deve estar apto a remover do bucket um número de símbolos que seja igual em representação ao tamanho do bucket.
- Se não houver tokens suficientes no bucket para enviar um pacote, o pacote esperará até que o bucket tenha tokens suficientes (no caso de um formador) ou o pacote será descartado ou marcado (no caso de um vigilante).
- O bucket propriamente dito possui uma capacidade específica. Se o bucket for totalmente preenchido, os tokens recém-chegados serão descartados e não estarão disponíveis para pacotes futuros. Assim, a qualquer momento, o maior surto que uma origem pode enviar na rede é proporcional ao tamanho do pacote. Um token bucket permite intermitência, mas a

limita.

**Q. Com um vigilante de tráfego tal como o class-based policing, que o (Bc) do committed burst e o (Be) da intermitência excedente significam e como devem mim selecionar estes valores?**

A. Um vigilante de tráfego não faz buffer de pacotes em excesso e transmite-os mais tarde, como é o caso de um modelador. Em vez disso, o vigilante executa um envio simples ou não envia a política sem o buffer. Durante períodos de congestionamento, desde que você não pode proteger, o melhor que você pode fazer é deixar cair agressivamente pacotes menos corretamente configurando a intermitência estendida. Consequentemente, é importante compreender que o vigilante usa a explosão normal e os valores de intermitência estendido para assegurar a taxa de informação comprometida configurada (CIR) estão alcançados.

Os parâmetros de intermitência são modelados livremente na regra de buffer genérico para roteadores. A regra recomenda configurar o armazenamento em buffer igual à taxa de bits do tempo de round-trip para acomodar as janelas de protocolo de controle de transmissão (TCP) pendentes de toda as conexões em períodos de congestionamento.

A tabela a seguir descreve a finalidade e a fórmula recomendada para o normal e os valores de intermitência estendido:

Parâmetro Burst	Propósito	Fórmula recomendada
explosão do normal	<ul style="list-style-type: none"><li>• Executa uma cubeta do token padrão.</li><li>• Define o tamanho máximo do token bucket (embora tokens possam ser emprestados se Be for maior que BC).</li><li>• Determina o tamanho do token bucket já que os tokens recém-chegados serão descartados e não estarão disponíveis para futuros pacotes caso o bucket seja totalmente preenchido.</li></ul>	$\text{CIR [BPS]} * (1 \text{ byte}) / (8 \text{ bits}) * 1.5 \text{ seconds}$ <p><b>Nota:</b> 1.5 segundos são o Round Trip Time típico.</p>
intermitência estendida	<ul style="list-style-type: none"><li>• Implementa um token bucket com o recurso de intermitência estendida.</li><li>• Desabilitado ajustando o BC = seja.</li><li>• Quando o BC é igual ser, o regulador de tráfego não pode pedir tokens e deixa cair simplesmente o pacote quando os tokens insuficientes estão disponíveis.</li></ul>	$2 * \text{normal burst}$

Nem todas as plataformas utilizam ou suportam o mesmo intervalo de valores para um policer. Consulte o documento a seguir para saber os valores que são suportados em sua plataforma específica:

- [Visão geral de vigilância e modelagem](#)

**Q. Como o Committed Access Rate (CAR) ou o class-based policing decidem se um pacote se conforma ou se excede a taxa de informação comprometida (CIR)? O roteador descarta pacotes e relata uma taxa excedida mesmo se a taxa conformada for menor que a CIR configurada.**

A. Um vigilante de tráfego usa a intermitência normal e os valores de intermitência estendidos para garantir que o CIR configurado seja atingido. A definição de valores de intermitência altos o suficiente é importante para assegurar uma boa transferência. Se a intermitência for configurada com valores muito baixos, a taxa obtida poderá ser muito mais baixa do que a taxa configurada. Punir os bursts temporários pode ter um forte impacto adverso sobre o throughput do tráfego do TCP (Protocolo de controle de transmissão). Com CAR, emita o **comando show interface rate-limit** para monitorar a explosão atual e determinar se o valor indicado é consistentemente perto do (Bc) do limite e dos valores do (Be) do limite estendido.

```
rate-limit 256000 7500 7500 conform-action continue exceed-action drop rate-limit 512000 7500
7500 conform-action continue exceed-action drop router# show interfaces virtual-access 26 rate-
limit Virtual-Access26 Cable Customers Input matches: all traffic params: 256000 BPS, 7500
limit, 7500 extended limit conformed 2248 packets, 257557 bytes; action: continue exceeded 35
packets, 22392 bytes; action: drop last packet: 156ms ago, current burst: 0 bytes last cleared
00:02:49 ago, conformed 12000 BPS, exceeded 1000 BPS Output matches: all traffic params: 512000
BPS, 7500 limit, 7500 extended limit conformed 3338 packets, 4115194 bytes; action: continue
exceeded 565 packets, 797648 bytes; action: drop last packet: 188ms ago, current burst: 7392
bytes last cleared 00:02:49 ago, conformed 194000 BPS, exceeded 37000 BPS
```

Para obter mais informações, consulte os seguintes documentos:

- [Visão geral de vigilância e modelagem](#)
- [Vigilância de QoS no Catalyst 6000](#)
- [Perguntas frequentes sobre qualidade de serviço no Catalyst 4000](#)
- [Series Switch do catalizador G-L3 e WS-X4232-L3 módulos QoS FAQ da camada 3](#)

**Q. São a explosão e o limite de fila independente de se?**

A. Sim, a explosão do vigilante e o limite de fila são separados e independente de se. Você pode ver o vigilante como uma porta que permita um determinado número de pacotes (ou bytes) e a fila como uma cubeta do *limite de fila* do tamanho que guarda os pacotes admitidos antes da transmissão na rede. Idealmente, você quer sua cubeta ser grande bastante para guardar uma *explosão de bytes/pacotes* admitidos pela porta (vigilante).

## Frame Relay de Qualidade de serviço (QoS)

**Q. Quais valores devo selecionar para Taxa de Informação Comprometida (CIR), Intermitência Comprometida (BC), Intermitência em Excesso (Be) e CIR Mínimo (MinCIR)?**

A. O Formatação de tráfego frame relay, que você permite emitindo o **comando frame-relay traffic-shaping**, apoia diversos parâmetros configurável. Esses parâmetros incluem frame-relay cir, frame-relay mincir e frame-relay BC. Consulte os seguintes documentos para obter mais informações sobre como selecionar esses valores e compreender comandos show relacionados:

- [Configurando o Frame Relay Traffic Shaping em 7200 roteadores e plataformas mais baixas](#)
- [mostrar Comandos para modelagem de tráfego de Frame Relay](#)
- [VoIP por Frame Relay com qualidade de serviço \(Fragmentação, Modelagem de Tráfego, Prioridade IP RTP\)](#)

## Q. As filas de prioridade na interface principal do Frame Relay trabalham no Cisco IOS 12.1?

A. As interfaces do Frame Relay apoiam mecanismos de filas da relação e mecanismos de filas do Per-Virtual Circuit (VC). A partir do Cisco IOS 12.0(4)T, a fila de interface suporta First In First Out (FIFO) ou Per Interface Priority Queueing (PIPQ) somente quando é configurada a modelagem de tráfego de Frame Relay (FRTS). Portanto, a configuração a seguir não funcionará mais se você atualizar para o Cisco IOS 12.1.

```
interface Serial0/0
  frame-relay traffic-shaping
  bandwidth 256
  no ip address
  encapsulation frame-relay IETF
  priority-group 1

!
interface Serial0/0.1 point-to-point
  bandwidth 128
  ip address 136.238.91.214 255.255.255.252
  no ip mroute-cache
  traffic-shape rate 128000 7936 7936 1000
  traffic-shape adaptive 32000
  frame-relay interface-dlci 200 IETF
```

Se o FRTS não estiver habilitado, você poderá aplicar um método padrão BWFQ, à interface principal, que esteja atuando como uma tubulação de largura de banda única. Além disso, até o Cisco IOS 12.1.1 (T), você podia habilitar o PIPQ (Enfileiramento da Interface de Prioridade) dos PVCs (Circuitos Virtuais Permanentes de Frame Relay) em uma interface principal do Frame Relay. É possível definir PVCs com prioridade alta, média, normal ou baixa e emitir o comando `frame-relay interface-queue priority` na interface principal, conforme mostrado no exemplo a seguir:

```
interface Serial3/0
  description framerelay main interface
  no ip address
  encapsulation frame-relay
  no ip mroute-cache
  frame-relay traffic-shaping
  frame-relay interface-queue priority interface Serial3/0.103 point-to-point description frame-
  relay subinterface ip address 1.1.1.1 255.255.255.252 frame-relay interface-dlci 103 class
  frameclass map-class frame-relay frameclass frame-relay adaptive-shaping becn frame-relay cir
  60800 frame-relay BC 7600 frame-relay be 22800 frame-relay mincir 8000 service-policy output
  queueingpolicy frame-relay interface-queue priority low
```

## Q. O Frame Relay Traffic Shaping (FRTS) trabalha com Distributed Cisco Express Forwarding (dCEF) e Class Based Weighted Fair Queueing distribuído (dCBWFQ)?

A. Até à data do Cisco IOS 12.1(5)T, somente a versão distribuída das características de QoS é apoiada em VIP no Cisco 7500 Series. Para habilitar a modelagem de tráfego nas interfaces de Frame Relay, use o DTS (Modelagem de Tráfego Distribuído). Para obter mais informações, consulte os seguintes documentos:

- [FRF.11 e FRF.12 distribuídos com base no processador de interface versátil para o Cisco IOS versão 12.1 T](#)
- [Frame Relay Traffic Shaping com QoS distribuído no Cisco 7500 Series](#)

## Qualidade de serviço (QoS) sobre ATN (modo de transferência assíncrono)

### Q. Onde aplico uma política de serviço com CBWFQ e LLQ em uma interface ATM?

A. Até à data políticas de serviço de assistência do Cisco IOS 12.2, das interfaces ATM a três níveis ou interfaces lógica: interface principal, subinterface, e Circuitos Virtuais Permanentes (PVC). O local onde você aplica a política é uma função do recurso Qualidade de Serviço (QoS) que você está habilitando. As políticas de enfileiramento devem ser aplicadas por VC (circuito virtual), uma vez que a interface ATM monitora o nível de congestionamento por VC e mantém as filas para pacotes em excesso por VC. Para obter mais informações, consulte os seguintes documentos:

- [Onde aplico uma política de serviços de QoS em uma interface ATM?](#)
- [Entendendo o enfileiramento de transmissão per-VC nas interfaces PA-A3 e NM-1A ATM](#)

### Q. Que bytes são contados pelo IP ao enfileiramento do Classe de serviço (CoS) do Asynchronous Transfer Mode (ATM)?

A. Os comandos de largura de banda e prioridade configurados em uma política de serviço para habilitar os recursos Class-Based Weighted Fair Queueing (CBWFQ) e Low Latency Queueing (LLQ), respectivamente, usam um valor em Kbps que contam os mesmos bytes de sobrecarga que são contados pela saída do comando show interface. Especificamente, o sistema de enfileiramento da camada 3 conta Controle lógico de enlace/Protocolo de acesso a sub-rede (LLC/SNAP). Não considera o seguinte:

- Trailer AAL5 (ATM Adaptation Layer 5)
- Preenchendo para tornar a última célula um múltiplo par de 48 bytes.
- Cabeçalho de célula de cinco bytes
- [Quais bytes são contados pelo IP para enfileiramento de ATM CoS?](#)

### Q. Quantos circuitos virtuais (VC) podem apoiar uma política de serviços simultaneamente?

A. O seguinte documento fornece orientações úteis sobre o número de VCS ATM (Modo de Transferência Assíncrono) que pode ser suportado. Aproximadamente 200 a 300 PVCs (Circuitos virtuais permanentes) VBR-nrt foram implementados com segurança:

- [Guia de Design da Classe de serviço IP ao ATM](#)

Além disso, considere o seguinte:

- Utilize um processador potente compatível. Por exemplo, um VIP4-80 fornece significativamente o alto desempenho do que um VIP2-50.
- Uma quantidade de memória de pacote disponível. No NPE-400, até 32 MB (em um sistema com 256 MB) são reservados para o buffer de pacotes. Para um NPE-200, são reservados até 16 MB para buffers de pacotes em um sistema com 128 MB.
- As configurações com WRED por VC operando simultaneamente em até 200 PVCs de ATM foram exaustivamente testadas. A quantidade de memória do pacote no VIP2-50 que pode ser usada para as filas por VC é finita. Por exemplo, um VIP2-50 com SRAM de 8 MB fornece 1085 buffers de pacote disponíveis para IP para enfileiramento de ATM COs por-VC no qual o WRED funciona. Se 100 PVCs ATM foram configurados e todos os VCS passaram por congestionamento excessivo ao mesmo tempo (como poderia ser simulado em ambientes de teste, nos quais a origem controlada do fluxo não-TCP estaria sendo usada), então, em média, cada PVC teria aproximadamente 10 pacotes de buffer, o que pode ser muito pouco para que o WRED funcione da maneira apropriada. Dispositivos VIP2-50 com ampla SRAM são, portanto, extremamente recomendados em designs com um grande número de PVCs ATM que execução WRED por VC e que podem passar com congestionamentos ao mesmo tempo.
- Mais alto o número de PVC ativos configurados, o mais baixo sua taxa de célula sustentada (SCR) precisaria de ser, e conseqüentemente mais curto a fila exigida pelo WRED para operar sobre o PVC. Portanto, como ocorre ao usar perfis WRED padrão do recurso Classe de serviço (CoS) IP para ATM Fase 1, a configuração de limiares de queda WRED mais baixos, quando o WRED por VC está ativado em um número muito grande de PVCs ATM de baixa velocidade congestionados, minimizaria o risco de falta de buffer no VIP. A queda do buffer no VIP não resulta em um mau funcionamento. No caso de interrupção de buffer no VIP, o recurso de IP para ATM COS fase 1 simplesmente degrada para o descarte de final First In First Out (FIFO) durante o período de interrupção de buffer (ou seja, a mesma política de descarte que ocorreria se o recurso de COs de IP para ATM não estivesse ativado neste PVC).
- Número máximo de VCs simultâneos que podem ser suportados razoavelmente.

## **Q. Que hardware ATM dá suporte a recursos de IP para Classe de Serviço (CoS, Class of Service) ATM como padrão CBWFQ e LLQ (Enfileiramento de Baixa Latência)?**

A. O IP to ATM CoS refere um conjunto de recurso que é permitido em uma base do Per-Virtual Circuit (VC). Dada essa definição, IP para Classe de Serviço (CoS, Class of Service) ATM não tem suporte nos processadores de rede ATM 4500 e PA-A1 ou no processador AIP. Esse hardware ATM não suporta enfileiramento per-VC como o PA-A3 e a maioria dos módulos de rede (além do ATM-25) o define. Para obter mais informações, consulte o seguinte documento:

- [Entendendo o suporte a hardware ATM de IP to CoS ATM](#)
- [Per-VC Class-Based, Weighted Fair Queuing em plataformas baseadas em RSP](#)
- [Weighted Fair Queuing por VC com base em classe \(CBWFQ por VC\) nos Cisco 7200, 3600, e 2600 Routers](#)
- [Enfileiramento por VC no adaptador de porta ATM IMA PA-A3-8T1/E1](#)



- [Configurando o enfileiramento ATM por VC no MC3810](#)

## Voz e Qualidade de Serviço (QoS)

### Q. Como funcionam a Fragmentação e a Intercalação de Links (LFI)?

A. O tráfego interativo tal como o telnet e a Voz sobre o IP é susceptível à latência aumentada quando a rede processa grandes pacotes tais como transferências do File Transfer Protocol (FTP) sobre WAN. O retardo de pacote para o tráfego interativo é significativo quando os pacotes FTP são enfileirados em enlaces de WAN mais lentos. Foi criado um método para fragmentar pacotes maiores e enfileirar os pacotes (de voz) menores entre os fragmentos dos pacotes (de FTP) maiores. Os roteadores do Cisco IOS suportam vários mecanismos de fragmentação da camada 2. Para obter mais informações, consulte os seguintes documentos:

- [Vista geral dos mecanismos de eficiência de link](#)
- [VoIP por Frame Relay com qualidade de serviço \(Fragmentação, Modelagem de Tráfego, Prioridade IP RTP\)](#)
- [Links de VoIP por PPP com qualidade de serviço \(LLQ / prioridade IP RTP, LFI, cRTP\)](#)

### Q. Que ferramentas posso eu usar para monitorar a Voz sobre o desempenho IP?

A. Cisco oferece atualmente diversas opções para monitorar o Qualidade de Serviço (QoS) nas redes usando a Voz de Cisco sobre soluções IP. Essas soluções não avaliam a qualidade de voz por meio da PSQM (Medida perceptual de qualidade de voz), nem de alguns outros novos algoritmos propostos para esse tipo de avaliação. As ferramentas de Agilent (HP) e de NetIQ estão disponíveis por esse motivo. Contudo, Cisco oferece as ferramentas que fornecem alguma ideia da Qualidade de voz que você está experimentando medindo o atraso, do tremor e da perda de pacotes. Para mais informação, refira a [utilização do Cisco Service Assurance Agent e do Internetwork Performance Monitor para controlar Qualidade de Serviço na Voz sobre redes IP](#).

### Q. %SW\_MGR-3-CM\_ERROR\_FEATURE\_CLASS: Erro da característica do gerenciador de conexão: Classe SS: (QoS) - instale o erro, ignoram.

A. A característica instala o erro observado é um comportamento esperado quando uma configuração inválida é aplicada a um molde. Indica que a política de serviços não era aplicado devido a um conflito. Geralmente, você não deve configurar dar forma no class-default da política infantil em mapas da política hierárquica, em lugar de configurar-la na política de parentes da relação. Esta mensagem junto com o retorno de monitoramento é imprimida - para fora consequentemente.

Com políticas baseadas sessão, dar forma no class-default tem que ser feito somente a secundário-relação ou nível PVC. Dar forma na interface física não é apoiado. Se a configuração é feita na interface física, a ocorrência deste Mensagem de Erro é um comportamento esperado.

No caseof LNS, uma outra razão pôde ser que a política de serviços poderia ser fornecida através do servidor Radius quando as sessões são trazidas acima. Emita o **comando show tech** a fim ver a configuração de servidor RADIUS e a fim ver todas as políticas de serviços ilegais que estiverem instaladas através do servidor Radius quando a sessão vem acima ou bate.

## Informações Relacionadas

- [Conceitos básicos de ajuste de desempenho](#)
- [Apoio do Qualidade de Serviço \(QoS\)](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)