

# Implementação da qualidade de serviço

## Contents

[Introduction](#)

[Quais aplicativos precisam de QoS?](#)

[Entendendo as características dos aplicativos](#)

[Conhecendo a topologia de rede](#)

[Tamanhos dos cabeçalhos da camada de enlace](#)

[Criando classes com base nos critérios](#)

[Criando uma política para marcar cada classe](#)

[Trabalhando a partir da extremidade em direção ao centro](#)

[Desenvolvendo a política para tratar o tráfego](#)

[Aplicando a política](#)

[Usando o QoS Policy Manager \(QPM\) para monitorar os efeitos da política](#)

[Recomendações de QoS para propósitos gerais](#)

[Informações Relacionadas](#)

## [Introduction](#)

Este documento fornece diretrizes de alto nível para a implementação de Qualidade de Serviço (QoS, Quality of Service) em uma rede que serve de transporte para vários aplicativos, incluindo aplicativos sensíveis a retardo e de largura de banda intensiva. Esses aplicativos podem melhorar processos de negócios, mas forçam os recursos da rede. O QoS pode fornecer serviços seguros, previsíveis, mensuráveis e garantidos para esses aplicativos por meio do gerenciamento de atrasos, variação de atraso (jitter), largura de banda e perda de pacotes em uma rede.

## [Quais aplicativos precisam de QoS?](#)

Primeiro, determine quais aplicativos são essenciais para a empresa e exigem proteção. Pode ser necessário analisar todos os aplicativos que estão competindo pelos recursos da rede. Se for o caso, use Contabilidade de fluxo de rede, Reconhecimento de aplicativo baseado em rede (NBAR) ou Gerenciador de dispositivo QoS (QDM) para analisar os padrões de tráfego na rede.

O NetFlow Accounting fornece detalhes sobre o tráfego de rede e pode ser usado para capturar a precedência ou a classificação de tráfego associada a cada fluxo.

NBAR é uma ferramenta de classificação que pode identificar o tráfego até a camada de aplicativo. Essa ferramenta fornece estatísticas por interface, por protocolo e bidirecionais para cada fluxo de tráfego que está atravessando uma interface. O NBAR também classifica o subporto; procurando e identificando além das portas do aplicativo.

O QDM é um aplicativo de gerenciamento de rede baseado na Web que fornece uma interface gráfica de usuário fácil de usar para configurar e monitorar a funcionalidade avançada de QoS

baseada em IP em roteadores.

## Entendendo as características dos aplicativos

É importante compreender as características dos aplicativos que precisam de proteção. Alguns aplicativos tendem a ser sensíveis à perda de latência ou de pacote, enquanto outros são considerados “agressivos” porque não são intermitentes nem consome muita largura de banda. Se o aplicativo estiver intermitente, determine se há uma intermitência constante ou uma intermitência pequena. O tamanho do pacote do aplicativo é grande ou pequeno? O aplicativo é baseado em TCP ou em UDP?

<b>Característica</b>	<b>Diretriz</b>
Aplicativo sensível a retardo ou a perda. (Voz e vídeo em tempo real)	Não use WRED, modelagem de tráfego, fragmentação (FRF-12) nem vigilância. Para esse tipo de tráfego, você deve implementar o LLQ (Low Latency Queuing) e usar uma fila de prioridade para o tráfego sensível a atrasos.
O aplicativo apresenta intermitência consistente ou é uma ocupação desnecessária da largura de banda. (FTP e HTTP)	Use WRED, policiamento, modelagem de tráfego ou CBWFQ (Class-Based Weighted Fair Queueing) para garantir a largura de banda.
Aplicativo baseado em TCP.	Use WRED já que pacotes perdidos fazem com que o TCP se retire e entre novamente usando um algoritmo de inicialização lenta. Se o tráfego for baseado em UDP e não alterar seu comportamento quando os pacotes forem descartados, não use WRED. Use o policiamento se precisar limitar a taxa do aplicativo; caso contrário, deixe os pacotes cair.

## Conhecendo a topologia de rede

Alguns dispositivos podem precisar de uma atualização do IOS para aproveitar os recursos de QoS que você deseja implementar. Diagramas da topologia de rede, das configurações do roteador e da versão do software em cada dispositivo ajudam a estimar o número de dispositivos que exigem uma atualização do IOS. Consulte a [Biblioteca de Ícones da Cisco](#) para obter ícones que podem ajudá-lo a criar diagramas de rede.

- Avalie a utilização da CPU em cada roteador durante os períodos de ocupado para ajudar a

- decidir como distribuir recursos de QoS entre os dispositivos para compartilhar a carga.
- Classifique os tipos de tráfego críticos para os negócios e as interfaces pelas quais esse tráfego passará. Escolha os grupos ou classes de prioridades a serem criados para atingir as metas de QoS para a sua rede.
  - Determine o retardo máximo com que os aplicativos mais críticos podem lidar e ajuste os parâmetros de intermitência nos condicionadores de tráfego (vigilantes ou formadores de tráfego) para acomodar esse retardo.
  - Descubra quais taxas são suportadas em cada interface: PVCs ou subinterfaces e configure a largura de banda compatível com eles.
  - Identificar links lentos para ajudar a determinar onde os gargalos na rede estão localizados e decidir como aplicar mecanismos de Eficiência de Link nas interfaces apropriadas.
  - Calcule a sobrecarga da Camada 2 e da Camada 3 para cada tipo de mídia que transportará o tráfego crítico da empresa. Isso ajudará a calcular a quantidade correta de largura de banda necessária para cada classe.
  - Outra informação importante é se você deseja proteger o tráfego com base no aplicativo, na origem e no destino IP, ou ambos.

## Tamanhos dos cabeçalhos da camada de enlace

Tipo de mídia	Cabeçalho da Camada de Link
Ethernet	14 Bytes
PPP	6 Bytes
Frame Relay	4 Bytes
ATM	5 bytes/célula

## Criando classes com base nos critérios

Depois de determinar quais aplicativos precisam de QoS e os critérios de classificação a serem usados (com base nas características dos aplicativos), você estará pronto para criar classes com base nessas informações.

## Criando uma política para marcar cada classe

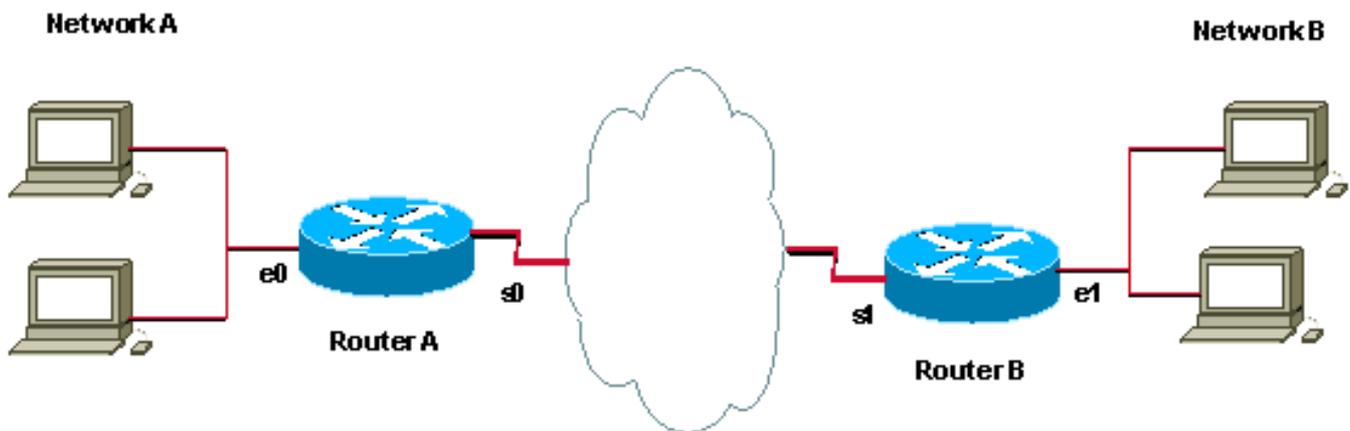
Crie uma política para marcar cada classe de tráfego com os valores de prioridade apropriados (use o DSCP (Ponto de controle de serviços diferenciados) ou a precedência de IP). O tráfego será marcado à medida que ingressa no roteador pela interface de entrada. As marcas serão usadas para tratar o tráfego quando ele deixar o roteador na interface de saída.

## Trabalhando a partir da extremidade em direção ao centro

Trabalhe do roteador mais próximo do tráfego em direção ao núcleo. Aplique sua marcação na interface de entrada do roteador. Na topologia abaixo, o Roteador A é o lugar óbvio para marcar o tráfego e aplicar a política para os dados originados da Rede A e destinados ao Roteador B. O tráfego será marcado à medida que entra na interface Ethernet0 do Roteador A, e a política de QoS será aplicada na interface Serial0 do Roteador A à medida que ele sai do roteador. Se a mesma política deve ser aplicada em ambas as direções (de modo que o tráfego originado da

Rede B e destinado à Rede A receba o mesmo tratamento), o tráfego proveniente da Rede B deve ser marcado à medida que entra na interface Ethernet1 do Roteador B e tratado à medida que deixa o roteador na interface Serial1.

Quando o tráfego é marcado na interface de ingresso em um roteador, ele mantém as mesmas marcas que atravessa vários saltos (a menos que seja marcado novamente). Normalmente, o tráfego precisa apenas ser marcado uma vez. As políticas de QoS podem ser aplicadas em saltos adicionais com base nessas marcas. Você só deverá remarcar caso esse tráfego chegue de um domínio não confiável.



## [Desenvolvendo a política para tratar o tráfego](#)

Agora que você marcou o tráfego, poderá usar as marcações para criar uma política e fazer a classificação do tráfego no restante dos segmentos de rede. Recomendamos manter a política simples, utilizando no máximo quatro classes.

Se possível, implemente e teste uma implementação de QoS em um ambiente de laboratório. Implemente-a na rede ativa após estar satisfeito com os resultados.

## [Aplicando a política](#)

Aplique a política na direção apropriada. Decida se a política precisa ser aplicada a uma direção ou em ambas as direções. Sempre marque e trate o tráfego o mais perto possível da origem, conforme descrito na seção [Criação de uma Política para Marcar Cada Classe](#) deste documento.

Recomendamos aplicar a mesma política em ambas as direções, para filtrar tráfego vindo e destinado a ambos os lados da estação. Isso significa que você deve aplicar a mesma política externa na interface serial do Roteador A e na interface serial do Roteador B.

## [Usando o QoS Policy Manager \(QPM\) para monitorar os efeitos da política](#)

Use o [QPM](#) como um sistema completo para controle centralizado de políticas e implantação automatizada e confiável de políticas.

## Recomendações de QoS para propósitos gerais

A seguir, uma lista das categorias de QoS e alguns dos recursos de QoS mais amplamente utilizados, associados a cada categoria.

<b>Categoria</b>	<b>Recursos de QoS associados</b>
Modelo de serviço de QoS	QoS provisionado (Diffserv) quando possível ou assinalado (RSVP) quando necessário.
Classificação/Marcação	Pontos de código Diffserv ou ID de grupo qos.
Gerenciamento de Congestionamento	LLQ ou CBWFQ.
Evitando congestionamento	<a href="#">WRED</a> compatível com Diffserv.
Eficiência do enlace	MLPPP, LFI, FRF.11, FRF.12, CRTP
Sinalização	RSVP, QPPB
Condicionadores/Vigilância de Tráfego	Política baseada em classe e modelagem de tráfego genérico (GTS) ou formatação de tráfego de frame-relay (FRTS).
Configuração/monitoramento	QPM, Modular QoS CLI (MQC), QDM

## Informações Relacionadas

- [página de suporte de QoS](#)
- [Página de suporte aos protocolos de roteamento IP](#)
- [Página de Suporte do IP Routing](#)
- [Página de suporte de IS-IS](#)
- [Suporte Técnico - Cisco Systems](#)