

Executando Qualidade de Serviço

Índice

[Introdução](#)

[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](#)

[Introdução](#)

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?](#)

Primeiramente, determine que aplicativos são críticos para negócio e exija a 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 igualmente faz a classificação de porta secundária; vista e identificação além das portas de aplicativo.

O QDM é um aplicativo de gerenciamento de rede baseado na Web que forneça uma interface com o usuário gráfica fácil de usar configurando e monitorando funcionalidade de QoS com base

em IP avançada no 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 é intermitência, determine se há uma explosão constante ou uma explosão pequena. O tamanho do pacote do aplicativo é grande ou pequeno? O aplicativo é baseado em TCP ou em UDP?

Característica	Diretriz
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 este tipo do tráfego, você deve executar o Low Latency Queuing (LLQ) e usar uma fila de prioridade para o tráfego sensível a retardo.
O aplicativo apresenta intermitência consistente ou é uma ocupação desnecessária da largura de banda. (FTP e HTTP)	Use o WRED, o policiamento, o modelagem de tráfego, ou o Class-Based Weighted Fair Queueing (CBWFQ) 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 UDP-está baseado e não muda seu comportamento quando os pacotes estão deixados cair, não use o WRED. Use o policiamento se você precisa o taxa-limite o aplicativo; se não apenas deixe a queda traseira dos pacotes.

Conhecendo a topologia de rede

Alguns dispositivos podem precisar uma upgrade de IOS a fim tomar a vantagem as características de QoS que você quer executar. Diagramas da topologia de rede, das configurações de roteador, e da versão de software em cada ajuda do dispositivo você calcula o número de dispositivos que exigem uma upgrade de IOS. Refira a [biblioteca de ícone de Cisco](#) para os ícones que podem o ajudar a criar diagramas da rede.

- Avalie a utilização CPU em cada roteador durante períodos ocupados para ajudar a decidir

- como distribuir características de QoS entre dispositivos para compartilhar da carga.
- Classifique tipos de tráfego crítico para negócios e as relações que este tráfego atravessará. 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.
- Encontre que taxas são apoiadas em cada relação: PVCs ou subinterfaces e configure a largura de banda compatível com eles.
- Identifique enlaces lentos para ajudar a determinar onde os gargalos na rede são encontrados e para decidir como aplicar mecanismos de eficiência de link nas relações apropriadas.
- Calcule a camada 2 e a camada 3 aérea para cada tipo de mídia que transportará o tráfego crítico do negócio. Isso ajudará a calcular a quantidade correta de largura de banda necessária para cada classe.
- Uma outra parte principal de informação é se você quer proteger o tráfego baseado no aplicativo, no origem de IP e no destino, 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

Uma vez que você determina que aplicativos precisam QoS e os critérios de classificação de se usar (baseado nas características dos aplicativos), você está pronto para criar as classes baseadas nesta informação.

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 marcações estarão usadas para tratar o tráfego enquanto deixa o roteador na interface de saída.

Trabalhando a partir da extremidade em direção ao centro

Trabalhe do roteador o mais próximo ao tráfego para o núcleo. Aplique sua marcação na interface de ingresso do roteador. Na topologia abaixo, o roteador A é o lugar óbvio para marcar o tráfego e aplicar a política para dados de origem da rede A e destinado para o roteador B. O tráfego será marcado como ele entra a relação do ethernet0 do roteador a, e a política de QoS será aplicada na relação do serial0 do roteador a como sae do roteador. Se a mesma política estiver aplicada

nos ambos sentidos (de modo que o tráfego originado da rede B e destinado para a rede A recebe o mesmo tratamento), o tráfego que vem da rede B deve ser marcado como ele entra a relação de Ethernet1 do roteador o b e trata enquanto deixa o roteador na relação de Serial1.

Uma vez que o tráfego é marcado na interface de ingresso em um roteador, mantém as mesmas marcações que atravessa saltos múltiplos (a menos que se observa). Normalmente, o tráfego precisa apenas ser marcado uma vez. As políticas de QoS podem ser aplicadas nos saltos adicionais baseados nestas marcações. 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](#)

Aplice a política no sentido apropriado. Decida se a política precisa ser aplicada a uma direção ou em ambas as direções. Sempre marque e trate o tráfego tão perto à fonte como possível, como descrito em [criar uma política para marcar cada](#) seção da [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 o controle centralizado de política e automatizado, distribuição de política confiável.

[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.

Categoria	Recursos de QoS associados
Modelo de serviço de QoS	QoS provisionado (Diffserv) quando possível ou assinalado (RSVP) quando necessário.
Classificação/Marcação	Pontos de código do DiffServ ou qos-grupo ID.
Gerenciamento de	LLQ ou CBWFQ.

Congestionamento	
Evitando congestionamento	DiffServ Compliant WRED.
Eficiência do enlace	MLPPP, LFI, FRF.11, FRF.12, CRTP
Sinalização	RSVP, QPPB
Condicionadores/Vigilância de Tráfego	A classe baseou o vigilante e o Generic Traffic Shaping (GTS) ou o Frame Relay Traffic Shaping (FRTS).
Configuração/monitoramento	QPM, Modular QoS CLI (MQC), QDM

[Informações Relacionadas](#)

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