Perguntas frequentes sobre QoS do Catalyst 6500/6000

Contents

Introduction

Este documento aborda as perguntas mais frequentes (FAQ) sobre a característica Qualidade de Serviço (QoS) do Catalyst 6500/6000 com Supervisor 1 (Sup1), Supervisor 1A (Sup1A), Supervisor 2 (Sup2) e Supervisor 720 (Sup720) que executam o Catalyst OS (CatOS). Neste documento, estes switches são referidos como Catalyst 6500 (Cat6K) Switches que executam o CatOS. Consulte Configuração de PFC QoS para características de QoS nos Catalyst 6500/6000 Switches que executam o software Cisco IOS®.

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

P. A QoS está habilitada por padrão nos Switches Catalyst 6500?

A. Por padrão, a QoS não está habilitada. Execute o comando **set qos enable** para habilitar a QoS.

P. Qual é o valor padrão do ponto de código de serviços diferenciados (DSCP) atribuído aos pacotes?

A. Todo o tráfego que entra em uma porta não confiável é marcado com um DSCP de 0. Especificamente, o DSCP é marcado novamente como 0 pela porta de saída.

P. Posso configurar a QoS baseada em VLAN em um 6500?

A. A configuração padrão é baseada em porta. Você pode alterar isso se emitir o comando **set port qos** *mod*/*port* **vlan-based**.

P. Quais são os recursos de porta para cada placa de linha e como posso interpretar os recursos de fila?

A. Consulte a tabela de recursos de porta na seção Entendendo o recurso de enfileiramento de uma porta da Programação de Saída de QoS em Catalyst 6500/6000 Series Switches Executando o CatOS System Software.

P. Quais são as configurações de QoS padrão em um 6500 quando a QoS é inicialmente habilitada?

A. Consulte a seção Configuração Padrão para QoS no Catalyst 6000 da Programação de Saída de QoS nos Catalyst 6500/6000 Series Switches executando o CatOS System Software.

P. Onde cada um dos processos de QoS é executado no Catalyst 6000?

A. Programação de entrada—realizada por PINNACLE/COIL port application-specific integrated circuit (ASICs). Somente Camada 2, com ou sem uma Placa de Recurso de Política (PFC - Policy

Feature Card).

Classificação—realizada pelo supervisor ou pelo PFC através do mecanismo da lista de controle de acesso (ACL). Somente a camada 2, sem um PFC; Camada 2 ou Camada 3 com um PFC.

Policiamento—Feito pelo PFC através do mecanismo de encaminhamento de Camada 3. Camada 2 ou Camada 3 com um PFC (obrigatório).

Regravação de pacote—realizada por ASICs de porta PINNACLE/COIL. Camada 2 ou Camada 3 com base na classificação feita anteriormente.

Programação de saída—realizada por ASICs de porta PINNACLE/COIL. Camada 2 ou Camada 3 com base na classificação feita anteriormente.

P. Posso implementar recursos de QoS sem uma Placa de recurso de política (PFC)?

A. Nos Switches da família Catalyst 6000, o coração da funcionalidade de QoS reside na PFC e é um requisito para o processamento de QoS da camada 3 ou da camada 4. No entanto, um supervisor sem PFC pode ser usado para classificação e marcação de QoS de Camada 2.

P. Qual é a diferença na funcionalidade de QoS entre o Policy Feature Card 1 (PFC1) e o PFC2?

A. O PFC2 permite que você empurre a política de QoS para baixo para um Distributed Forwarding Card (DFC). O PFC2 também adiciona suporte para uma taxa de excesso, o que indica um segundo nível de policiamento no qual as ações de política podem ser tomadas. Consulte a seção Suporte de Hardware para QoS na Família Catalyst 6000 de Compreendendo a Qualidade de Serviço nos Switches da Família Catalyst 6000 para obter mais informações.

P. Qual é a classe de serviço (CoS) padrão para transmitir configurações de mapeamento de fila quando o auto qos está ativado?

A. set qos map 2q2t tx queue 2 2 cos 5,6,7

set qos map 2q2t tx queue 2 1 cos 1,2,3,4

set qos map 2q2t tx queue 1 1 cos 0

P. Qual é o mapeamento padrão de ponto de código de serviços diferenciados (DSCP) para classe de serviço (CoS)?

A. 8 a 1 (divida DSCP por 8 para obter CoS).

P. Na fila de saída, se a fila de prioridade estrita estiver saturada, o tráfego será finalmente atendido nas filas de rodízio ponderado (WRR)?

A. Não, as filas WRR não serão atendidas até que a fila de prioridade esteja completamente vazia.

P. O rodízio ponderado (WRR) determina a alocação de largura de banda com base no número de pacotes ou em um determinado número de bytes?

A. Com base em um determinado número de bytes, que podem representar mais de um pacote. O pacote final que excede os bytes alocados não é enviado. Com uma configuração de peso extremo, como 1% para a fila 1 e 99% para a fila 2, o peso exato configurado pode não ser alcançado. O switch usa um algoritmo WRR para transmitir quadros de uma fila por vez. O WRR usa um valor de peso para decidir quanto transmitir de uma fila antes de mudar para a outra. Quanto maior o peso atribuído a uma fila, mais largura de banda de transmissão será alocada a ela.

Note: O número real de bytes transmitidos não corresponde ao cálculo porque os quadros inteiros são transmitidos antes de serem transferidos para a outra fila.

P. A minha nova documentação da placa de linha 65xx diz que ela suporta DWRR. O que é o DWRR e o que ele significa?

A. O DWRR transmite das filas sem passar fome na fila de baixa prioridade, porque rastreia a sub-transmissão da fila de baixa prioridade e a compensa na próxima rodada. Se uma fila não puder enviar um pacote porque seu tamanho é maior que os bytes disponíveis, os bytes não utilizados são creditados ao próximo round.

P. Quais são os pesos padrão em uma porta 2q2t e como eu os modifico?

A. Emita o comando **set qos wrr 2q2t** *q1_weight q2_weight* para modificar os pesos padrão da Fila 1 (a fila de baixa prioridade serviu 5/260 do tempo) e da Fila 2 (a fila de alta prioridade serviu 255/260 do tempo).

P. Eu gostaria de usar o SNMP (Simple Network Management Protocol) para coletar o número de pacotes descartados por vigilantes individuais. Isso é possível? Em caso afirmativo, qual MIB é usada?

A. Sim, o SNMP suporta CISCO-QOS-PIB-MIB e CISCO-CAR-MIB.

P. Há um comando show que exibe o número de pacotes descartados pelo vigilante?

A. Os comandos **show qos statistics aggregate-policer** e **show qos statistics l3stats** exibem o número de pacotes descartados pelo vigilante.

P. Gostaria de usar o SNMP (Simple Network Management Protocol) para modificar um vigilante para que os parâmetros de taxa e intermitência possam ser alterados dinamicamente. Por exemplo, por hora do dia. Isso é possível? Em caso afirmativo, qual MIB é usada?

A. Sim, o SNMP suporta CISCO-QOS-PIB-MIB e CISCO-CAR-MIB.

P. É possível implementar QoS baseado na hora do dia—especificamente, para

modificar as taxas máxima e de pico—através do software Cisco IOS na Multilayer Switch Feature Card (MSFC) no modo híbrido? Se possível, essa QoS é feita no hardware e não pelo processador MSFC?

A. Não, isso não pode ser feito. No modo híbrido (CatOS), toda a vigilância de QoS é feita pelo supervisor.

P. Não vi uma descrição de como a taxa de vigilante e os valores de intermitência de vigilante são implementados. Eu gostaria de completar a documentação técnica sobre isso, para que eu possa entender o impacto que eles têm na minha rede.

A. Os valores de taxa de vigilante e de intermitência de vigilante são implementados desta maneira:

```
burst = sustained rate bps × 0.00025 (the leaky bucket rate) + MTU kbps
```

Por exemplo, se você deseja um vigilante de 20 Mbps e uma unidade de transmissão máxima (MTU) (em Ethernet) de 1500 bytes, então é assim que a intermitência é calculada:

```
burst = (20,000,000 bps × 0.00025) + (1500 × 0.008 kbps)
      = 5000 bps + 12 kbps
      = 17 kbps
```

No entanto, devido à granularidade do hardware do vigilante com Sup1 e Sup2, você precisa arredondar isso para 32 kbps, que é o mínimo.

Consulte estes documentos para obter mais informações sobre a implementação da taxa de vigilância e dos valores de intermitência:

- Programação da saída de QoS nos Switches da série Catalyst 6500/6000 executando o Software do sistema CatOS
- Configurando QoS

P. Planejo substituir meus Supervisores Sup1A por Sup2s. A mecânica da QoS, como a taxa de burst, muda entre Sup1A e Sup2?

A. Sim, há diferença entre dois supervisores quando um Switch Catalyst 6500 tem SUP2/PFC2. Se ele executar o Cisco Express Forwarding (CEF), o comportamento será ligeiramente diferente quando você configurar o netflow em SUP2.

P. Quais são alguns comandos que posso usar para monitorar minhas configurações de QoS?

A. Consulte a seção Monitoramento e Verificação de uma Configuração da Classificação e Marcação de QoS em Catalyst 6500/6000 Series Switches com CatOS Software.

P. Quando eu executo o código do sistema operacional Catalyst (CatOS) em um software 6500 e Cisco IOS na Multilayer Switch Feature Card (MSFC), emito os comandos de QoS no MSFC ou no supervisor?

A. Ao executar o código híbrido (CatOS), você emite os comandos de QoS no supervisor/Placa de recurso de política (PFC). O 6500 executa QoS em três locais:

- Baseado em software no MSFC
- Baseado em hardware (baseado em switching multicamada) na PFC
- Baseado em software em algumas placas de linha

Esse problema ocorre quando você trabalha com IOS híbrido (CatOS + IOS para MSFC). O CatOS e o IOS têm dois conjuntos de comandos de configuração. No entanto, quando você configura QoS no IOS nativo, por exemplo, com os mecanismos Sup32 ou Sup720 mais novos, você está mais longe do hardware e a parte da placa de linha é invisível para o usuário. Isso é importante porque a maior parte do tráfego é comutado multicamada (comutado por hardware). Portanto, ele é tratado pela lógica de PFC. O MSFC nunca vê esse tráfego. Se você não estiver configurando a QoS baseada em PFC, a maior parte do tráfego será perdida.

P. O que acontece se o comando set port qos trust não for suportado pela minha placa de linha?

A. Você pode criar uma lista de controle de acesso (ACL) de QoS para confiar no valor de ponto de código de serviços diferenciados (DSCP) do pacote recebido. Por exemplo, emita o comando **set qos acl ip test trust-dscp any**.

P. Qual é a diferença entre os vigilantes de agregação e microfluxo?

A. Consulte a classificação e policiamento com a seção PFC de Compreendendo a Qualidade de Serviço nos Switches da Família Catalyst 6000.

P. Quais comandos permitem que eu visualize estatísticas para vigilantes de agregação ou microfluxo?

A. Com o Supervisor Engine 1 e 1A, não é possível ter estatísticas de policiamento para vigilantes agregados individuais. Emita o comando **show qos statistics l3stats** para exibir as estatísticas de policiamento por sistema.

Com o Supervisor Engine 2, você pode exibir estatísticas de vigilância agregadas por vigilante com o comando **show qos statistics aggregate-policer**. Emita o comando **show mls entry qos short** para verificar as estatísticas de vigilância de microfluxo.

P. A modelagem de tráfego é suportada no Switch Catalyst 6500 (Cat6K)?

A. A modelagem de tráfego só é suportada em determinados módulos WAN para os Catalyst 6500/7600 Series, como os módulos Optical Services Modules (OSMs) e FlexWAN. Consulte Configuração da Modelagem de Tráfego Baseada em Classe e Modelagem de Tráfego para obter mais informações.

P. Quantos vigilantes de agregação ou microfluxo são suportados no Switch Catalyst 6500 (Cat6K)?

A. O Catalyst 6500/6000 oferece suporte para até 63 vigilantes de microfluxo e para até 1023 vigilantes agregados.

P. Qual é a imagem do Cisco IOS do sistema operacional Catalyst (CatOS) ou da placa de recurso do switch multicamada (MSFC) necessária para suportar policiamento?

A. O Supervisor Engine 1A suporta a vigilância de entrada no CatOS versão 5.3(1) e posterior, e Cisco IOS Software Release 12.0(7)XE e posterior.

O Supervisor Engine 2 suporta a vigilância de entrada no CatOS versão 6.1(1) e posterior, e Cisco IOS Software Release 12.1(5c)EX e posterior. No entanto, a vigilância de microfluxo é suportada somente no software Cisco IOS.

P. Atualizei de um Sup2 para um Sup720 e minhas estatísticas de taxa de tráfego policiado mostram de forma diferente com o mesmo tráfego. Por quê?

A. Uma alteração importante no policiamento no Supervisor Engine 720 é que ele pode contar o tráfego pelo comprimento da Camada 2 do quadro. Isso difere do Supervisor Engine 1 e do Supervisor Engine 2, que contam quadros IP e IPX pelo comprimento da Camada 3. Com alguns aplicativos, o comprimento das Camadas 2 e 3 pode não ser consistente. Um exemplo é um pequeno pacote de Camada 3 dentro de um grande quadro de Camada 2. Nesse caso, o Supervisor Engine 720 pode exibir uma taxa de tráfego policiado ligeiramente diferente em comparação com o Supervisor Engine 1 e o Supervisor Engine 2.

P. Como sei quais valores usar para taxa e intermitência quando configuro um vigilante?

A. Estes parâmetros controlam a operação do token bucket:

- **Rate** — Define quantos tokens são removidos em cada intervalo. Isso define efetivamente a taxa de vigilância. Todo o tráfego abaixo da taxa é considerado em perfil.
- **Intervalo** —Define a frequência com que os tokens são removidos do bucket. O intervalo é fixado em 0,00025 segundos, portanto os tokens são retirados do bucket 4.000 vezes por segundo. O intervalo não pode ser alterado.
- **Intermitência** —Define o número máximo de tokens que o bucket pode conter a qualquer momento. A intermitência não deve ser menor que a taxa de vezes que o intervalo para manter a taxa de tráfego especificada. Outra consideração é que o pacote de tamanho máximo deve caber no bucket.

Use esta equação para determinar o parâmetro de intermitência:

```
Burst = (rate bps * 0.00025 sec/interval) or (maximum packet size bits) [whichever is greater]
```

Por exemplo, se você quiser calcular o valor mínimo de intermitência necessário para sustentar uma taxa de 1 Mbps em uma rede Ethernet, a taxa é definida como 1 Mbps e o tamanho máximo do pacote Ethernet é de 1518 bytes. Esta é a equação:

```
Burst = (1,000,000 bps * 0.00025) or (1518 bytes * 8 bits/byte) = 250 or 12144
```

O resultado maior é de 12144, que pode ser arredondado para 13 kbps.

Observação: no software Cisco IOS, a taxa de vigilância é definida em bits por segundo (bps). No sistema operacional Catalyst (CatOS), ele é definido em kbps. Além disso, no software Cisco IOS,

a taxa de intermitência é definida em bytes, mas no CatOS, ela é definida em kilobits.

Observação: devido à granularidade da vigilância de hardware, a taxa exata e a intermitência são arredondadas para o valor suportado mais próximo. Certifique-se de que o valor de intermitência não seja inferior ao pacote de tamanho máximo. Caso contrário, todos os pacotes maiores que o tamanho da intermitência são cancelados.

Por exemplo, se você tentar definir a intermitência como 1518 no software Cisco IOS, ela será arredondada para 1000. Isso faz com que todos os quadros maiores que 1000 bytes sejam descartados. A solução é configurar a intermitência para 2000.

Ao configurar a taxa de burst, leve em conta que alguns protocolos, como o TCP, implementam um mecanismo de controle de fluxo que reage à perda de pacotes. Por exemplo, o TCP reduz o janelamento pela metade para cada pacote perdido. Consequentemente, quando policiada para uma determinada taxa, a utilização efetiva do link é inferior à taxa configurada. É possível aumentar a intermitência para obter melhor utilização. Um bom começo para esse tráfego é dobrar o tamanho da intermitência. Neste exemplo, o tamanho da intermitência é aumentado de 13 kbps para 26 kbps. Depois, monitore o desempenho e efetue os ajustes necessários.

Pelo mesmo motivo, não é recomendável que você avalie a operação do vigilante com tráfego orientado a conexão. Isso geralmente mostra um desempenho menor do que o permitido pelo vigilante.

P. Estou configurando QoS em um canal de porta. Há alguma restrição que eu precise saber?

A. Ao configurar a QoS em portas que fazem parte de um canal de porta no sistema operacional Catalyst (CatOS), você deve aplicar a mesma configuração a todas as portas físicas no canal de porta. Esses parâmetros devem concordar com todas as portas no canal de porta:

- Tipo de confiança de porta
- Tipo de porta de recepção (2q2t ou 1p2q2t)
- Tipo de porta de transmissão (1q4t ou 1p1q4t)
- Classe de serviço da porta padrão (CoS)
- QoS baseada em porta ou QoS baseada em VLAN
- Lista de controle de acesso (ACL) ou par de protocolos que a porta transporta

P. Por que não consigo ajustar o valor de limiar mínimo?

A. Com as versões do sistema operacional Catalyst (CatOS) anteriores à 6.2, o comando de limiar WRED (Weighted Random Early Detection) somente define o limiar máximo, enquanto o limiar mínimo é codificado para 0%. Isso é corrigido no CatOS 6.2 e posterior, o que permite a configuração do valor min-threshold.O min-threshold padrão depende da precedência. O limiar mínimo para precedência de IP 0 corresponde a metade do limiar máximo. Os valores para as precedências que permanecem estão entre metade do limiar máximo e o limite máximo em intervalos uniformemente espaçados.

P. Estou tendo dificuldades para ajustar os buffers da fila de transmissão. Há alguma restrição?

A. Se você tiver três filas (1p2q2t), a fila de rodízio ponderado (WRR) de alta prioridade e a fila de prioridade estrita devem ser definidas no mesmo nível.

P. Tenho uma placa de linha 62xx/63xx. Não posso aplicar o comando set que confia no ponto de código de serviços diferenciados (DSCP) em uma porta. Há uma limitação nesta placa de linha para recursos de QoS?

A. Sim, porque você não pode emitir os comandos **trust-dscp**, **trust-ipprec** ou **trust-cos** nas placas de linha WS-X6248-xx, WS-X6224-xx e WS-X6348-xx. O método mais fácil nesta situação é deixar todas as portas como não confiáveis e alterar a lista de controle de acesso (ACL) padrão para o comando **trust-dscp**:

```
set qos enable

set port qos 2/1-16 trust untrusted

set qos acl default-action ip trust-dscp
```

Consulte a seção Limitações das Placas de Linha WS-X6248-xx, WS-X6224-xx e WS-X6348-xx da Classificação QoS e Marcação nos Switches Catalyst 6500/6000 Series Executando Software CatOS para adição limitações específicas da placa de linha.

P. Quais versões e supervisores do sistema operacional Catalyst (CatOS) são necessários para oferecer suporte à vigilância?

A. O Supervisor Engine 1A suporta a vigilância de entrada no CatOS versão 5.3(1) e posterior e no Cisco IOS Software Release 12.0(7)XE e posterior.

Observação: é necessária uma placa auxiliar PFC (Policy Feature Card, placa de recurso de política) para policiamento com o mecanismo de supervisor 1A.

O Supervisor Engine 2 suporta a vigilância de entrada no CatOS versão 6.1(1) e posterior, e no Cisco IOS Software Release 12.1(5c)EX e posterior. O Supervisor Engine 2 suporta o parâmetro de policiamento de taxa excedente.

O Supervisor 720 suporta vigilância de entrada no nível da porta e da interface VLAN. Consulte a seção Atualização de Recursos de Policiamento para o Supervisor Engine 720 de Policiamento de QoS em Catalyst 6500/6000 Series Switches para obter mais informações sobre os recursos de policiamento do Sup720.

P. O que preciso saber sobre a configuração de QoS sobre EtherChannel?

A. Quando você configura a QoS em uma porta que faz parte de um EtherChannel no CatOS, você deve sempre configurá-la por porta. Além disso, você deve garantir que aplique a mesma configuração de QoS a todas as portas, pois o EtherChannel só pode agrupar portas com as mesmas configurações de QoS. Isso significa que você precisa configurar esses parâmetros da mesma forma:

- Tipo de confiança de porta
- Tipo de porta de recepção (2q2t ou 1p2q2t)

- Tipo de porta de transmissão (1q4t ou 1p1q4t)
- Classe de serviço da porta padrão (CoS)
- QoS baseada em porta ou QoS baseada em VLAN
- Lista de controle de acesso (ACL) ou par de protocolos que a porta transporta

P. Onde posso encontrar exemplos do uso de listas de controle de acesso (ACLs) de QoS para marcar ou policiar o tráfego?

A. Consulte o Caso 1: Marcação na seção Edge da Classificação e Marcação de QoS nos Catalyst 6500/6000 Series Switches com CatOS Software para um exemplo de marcação de tráfego.

Consulte a seção Configurar e Monitorar Vigilância no CatOS Software de Política de QoS nos Catalyst 6500/6000 Series Switches para obter um exemplo de tráfego de vigilância.

P. Qual é a diferença entre as listas de controle de acesso (ACLs) de QoS baseadas em porta e baseadas em VLAN?

A. Cada ACL de QoS pode ser aplicada a uma porta ou a uma VLAN, mas há um parâmetro de configuração adicional a ser considerado: o tipo de porta ACL. Uma porta pode ser configurada para se basear em VLAN ou em uma porta. Estes são os dois tipos de configuração:

1. Se uma porta baseada em VLAN com uma ACL aplicada for atribuída a uma VLAN que também tenha uma ACL aplicada, a ACL baseada em VLAN terá prioridade sobre a ACL baseada em porta.
2. Se uma porta baseada em porta com uma ACL aplicada for atribuída a uma VLAN que também tenha uma ACL aplicada, a ACL baseada em porta terá prioridade sobre a ACL baseada em VLAN.

Consulte Qual das quatro fontes possíveis para DSCP interno será usada? seção de Classificação e Marcação de QoS em Catalyst 6500/6000 Series Switches com CatOS Software para obter mais informações.

P. Qual é o valor típico do tamanho da intermitência a ser usado para limitação de taxa em switches de Camada 3?

A. Os switches de Camada 3 implementam uma aproximação do algoritmo de token bucket único no firmware. Um tamanho de intermitência razoável para o intervalo de taxas de tráfego é de aproximadamente 64.000 bytes. O tamanho da intermitência deve ser escolhido de forma a incluir pelo menos um pacote de tamanho máximo. Com cada pacote de chegada, o algoritmo de vigilância determina o tempo entre esse pacote e o último pacote e calcula o número de tokens gerados durante o tempo decorrido. Em seguida, ele adiciona esse número de tokens ao bucket e determina se o pacote de chegada está em conformidade ou excede aos parâmetros especificados.

P. Por que recebo um desempenho menor para o tráfego TCP com limitação de taxa?

A. Os aplicativos TCP se comportam mal quando os pacotes são descartados como resultado da limitação de taxa. Isso se deve ao esquema de janelamento inerente usado no controle de fluxo.

Você pode ajustar o parâmetro de tamanho de intermitência ou o parâmetro de taxa para obter o throughput necessário.

P. Qual é a vantagem da WRED (Weighted Random Early Detection) e como sei se minha placa de linha pode suportar WRED?

A. Para evitar congestionamento na programação de saída, o Switch Catalyst 6500 (Cat6K) suporta WRED em algumas filas de saída. Cada fila tem um limite e um tamanho configuráveis. Alguns têm WRED. WRED é um mecanismo de prevenção de congestionamento que descarta aleatoriamente pacotes com uma certa precedência de IP quando os buffers atingem um limite definido de preenchimento. WRED é uma combinação de dois recursos: queda traseira e detecção precoce aleatória (RED). A implementação inicial do sistema operacional Catalyst (CatOS) da WRED apenas definiu o limiar máximo, enquanto o limiar mínimo foi codificado para 0%. Observe que a probabilidade de queda para um pacote é sempre não nula, pois eles estão sempre acima do limiar mínimo. Esse comportamento é corrigido no CatOS 6.2 e posterior. O WRED é um mecanismo muito útil para evitar congestionamento quando o tipo de tráfego é baseado em TCP. Para outros tipos de tráfego, o RED não é muito eficiente porque o RED aproveita o mecanismo de janelamento usado pelo TCP para gerenciar o congestionamento.

Consulte a seção Entendendo o Recurso de Enfileiramento de uma Porta da Programação de Saída de QoS em Catalyst 6500/6000 Series Switches Executando o CatOS System Software para determinar se uma placa de linha ou estrutura de fila pode suportar WRED. Você também pode executar o comando **show port capabilities** para ver a estrutura da fila da sua placa de linha.

P. Qual é o ponto de código de serviços diferenciados internos (DSCP)?

A. Cada quadro tem uma classe interna de serviço (CoS) atribuída, seja o CoS recebido ou a porta padrão CoS. Isso inclui quadros não marcados que não transportam nenhum CoS real. Esse CoS interno e o DSCP recebido são gravados em um cabeçalho de pacote especial (chamado de cabeçalho de barramento de dados) e são enviados pelo barramento de dados para o mecanismo de switching. Isso acontece na placa de ingresso. Neste ponto, ainda não se sabe se esse CoS interno é transportado para o circuito integrado específico do aplicativo de saída (ASIC) e inserido no quadro de saída. Quando o cabeçalho atinge o mecanismo de comutação, o mecanismo de comutação Encoded Address Recognition Logic (EARL) atribui a cada quadro um DSCP interno. Esse DSCP interno é uma prioridade interna atribuída ao quadro pela Placa de Recurso de Política (PFC - Policy Feature Card) enquanto ele transita o switch. Não é o DSCP no cabeçalho de IPv4. É derivado de uma configuração de CoS ou tipo de serviço (ToS) existente e é usado para redefinir o CoS ou ToS à medida que o quadro sai do switch. Esse DSCP interno é atribuído a todos os quadros comutados (ou roteados) pelo PFC, inclusive quadros que não são IP.

P. Quais são as possíveis fontes para o DSCP (Internal Different Services Code Point, ponto de código de serviços diferenciados internos)?

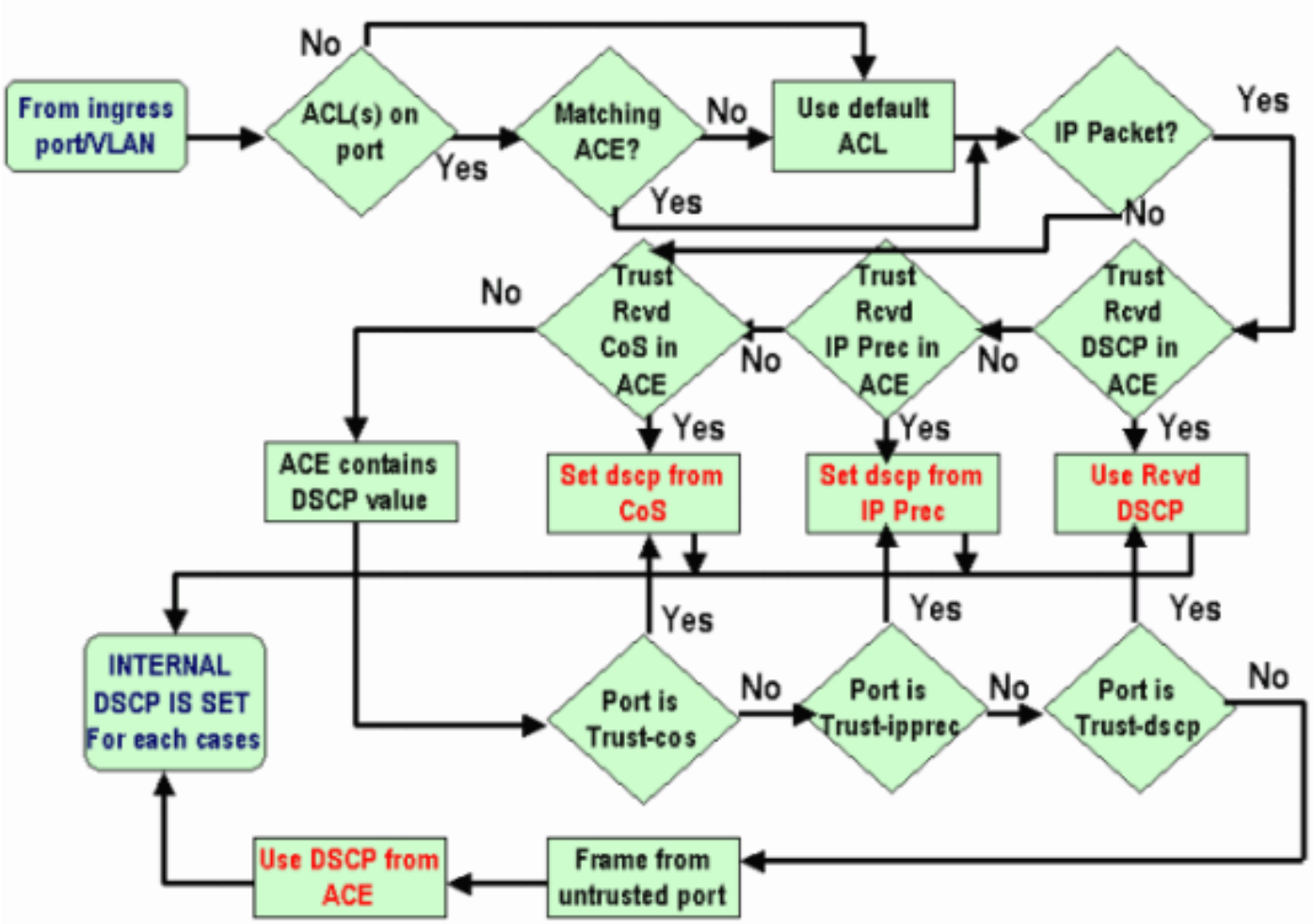
A. Consulte a seção Quatro Fontes Possíveis para DSCP Interno de Classificação e Marcação de QoS em Catalyst 6500/6000 Series Switches com CatOS Software.

P. Como é escolhido o DSCP (Internal Differated Services Code Point, ponto de código de serviços diferenciados internos)?

A. O DSCP interno depende destes fatores:

- Estado de confiança da porta
- Lista de controle de acesso (ACL) conectada à porta
- ACL padrão
- com base em VLAN ou em porta, em relação à ACL

Este fluxograma resume como o DSCP interno é escolhido com base na configuração:



P. O CBWFQ (Class-Based Weighted Fair Queuing) ou o LLQ (Low Latency Queuing) é suportado no Switch Catalyst 6500 (Cat6K)?

A. Sim, o CBWFQ permite definir uma classe de tráfego e atribuir a ela uma garantia de largura de banda mínima. O algoritmo por trás desse mecanismo é Weighted Fair Queuing (WFQ), que explica o nome. Você define classes específicas em instruções map-class para configurar o CBWFQ. Então, você atribui uma política para cada classe em um mapa de políticas. Esse mapa de política é então anexado à entrada/saída de uma interface.

P. O valor de Classe de Serviço (CoS - Class of Service) da Camada 2 é mantido para pacotes roteados?

A. Sim, o ponto de código de serviços diferenciados internos (DSCP) é usado para redefinir o CoS em quadros de saída.

P. A QoS aplica a configuração idêntica a todas as portas LAN controladas pelo

mesmo ASIC?

A. Sim, quando esses comandos são configurados, o QoS aplica uma configuração idêntica a todas as portas LAN/roteadas controladas pelo mesmo ASIC (Application Specific Integrated Circuit - Circuito Integrado Específico de Aplicativo). As configurações de QoS são propagadas para outras portas que pertencem ao mesmo ASIC, independentemente de a porta ser uma porta de acesso, porta de tronco ou uma porta roteada.

- **rcv-queue random-detect**
- **rcv-queue queue queue-limit**
- **wrr-queue queue queue-limit**
- **largura de banda da fila de erro** (exceto portas LAN Gigabit Ethernet)
- **priority-queue cos-map**
- **rcv-queue cos-map**
- **wrr-queue cos-map**
- **wrr-queue threshold**
- **limite de fila de rcv**
- **wrr-queue random-detect**
- **wrr-queue random-detect min-threshold**
- **wrr-queue random-detect max-threshold**

Quando o comando **default** ***interface*** é executado em qualquer uma das portas, o ASIC que controla a porta específica redefine a configuração de QoS para todas as portas controladas por ele.

P. Por que o comando show traffic-shape statistics não mostra um resultado positivo mesmo quando a modelagem de tráfego está configurada?

```
Router#show traffic-shape statistics
          Access Queue     Packets   Bytes     Packets   Bytes     Shaping
I/F       List   Depth                        Delayed   Delayed   Active
Et0       101    0         2         180       0         0         no
Et1              0         0         0         0         0         no
```

A. O atributo Shaping Ative tem **sim** quando os temporizadores indicam que a modelagem de tráfego ocorre e **não** se a modelagem de tráfego não ocorrer.

Você pode usar o comando **show policy-map** para verificar se o tráfego configurado funciona.

```
Router#show policy-map
  Policy Map VSD1
    Class VOICE1
      Strict Priority
      Bandwidth 10 (kbps) Burst 250 (Bytes)
    Class SIGNALS1
      Bandwidth 8 (kbps) Max Threshold 64 (packets)
    Class DATA1
      Bandwidth 15 (kbps) Max Threshold 64 (packets)
  Policy Map MQC-SHAPE-LLQ1
    Class class-default
      Traffic Shaping
         Average Rate Traffic Shaping
```

```
            CIR 63000 (bps) Max. Buffers Limit 1000 (Packets)
            Adapt to 8000 (bps)
            Voice Adapt Deactivation Timer 30 Sec
    service-policy VSD1
```

P. O Catalyst 6500 PFC suporta todos os comandos de QoS padrão?

A. O Cisco Catalyst 6500 PFC QoS tem algumas restrições e não suporta alguns comandos relacionados à QoS. Consulte estes documentos para obter a lista completa de comandos não suportados.

- Restrições de Comando do Mapa de Classe
- Restrições de Comando do Mapa de Política
- Restrições de Comando de Classe de Mapa de Política

P. Por que os contadores de CoPP de software são maiores que os contadores de CoPP de hardware?

A. Os contadores de Política de Plano de Controle de Software (CoPP - Software Control Plane Policing) são a soma de pacotes que atravessam o CoPP de hardware e a limitação da taxa de hardware. Os pacotes são primeiramente tratados por limitadores de taxa de hardware e, se não corresponderem, o hardware CoPP chega à imagem. Se o limitador de taxa de hardware permitir os pacotes, esse pacote vai para o software onde é processado pelo CoPP do software. Devido a esse software, o CoPP pode ser maior que os contadores CoPP de hardware.

Também há algumas restrições em que o CoPP não é suportado no hardware. Alguns deles são:

- CoPP não é suportado em hardware para pacotes multicast. A combinação de ACLs, limitadores de taxa de CPU multicast e proteção de software CoPP fornece proteção contra ataques de DoS multicast.
- CoPP não é suportado em hardware para pacotes de broadcast. A combinação de ACLs, controle de tempestade de tráfego e proteção de software CoPP fornece proteção contra ataques de DoS de broadcast.
- As classes que correspondem ao multicast não são aplicadas no hardware, mas no software.
- CoPP não está habilitado no hardware a menos que MLS QoS esteja habilitado globalmente com o comando **mls qos**. Se o comando **mls qos** não for inserido, o CoPP só funcionará no software e não fornecerá nenhum benefício para o hardware.

Consulte Configuração de Política de Plano de Controle (CoPP) para obter mais informações.

P. A configuração de QoS do comando padrão (interface) funciona em outras interfaces/portas?

A. Quando o comando **default** ***interface*** é emitido, a configuração não padrão é reunida, o que é semelhante ao que é exibido em **show running-config interface** ***x/y*** , e cada uma delas é definida com seus valores padrão. Isso também pode ser uma simples negação de um comando.

Se houver alguma QoS ou outros recursos configurados nessa interface, e esses comandos forem negados, eles poderão se propagar para outras interfaces da placa de linha.

Recomenda-se verificar a saída do comando **show interface** ***x/y*** **capabilities**, antes de continuar com o padrão de uma interface. Consulte O QoS aplica a configuração idêntica a todas as portas

LAN que são controladas pelo mesmo ASIC? para obter mais informações.

A saída do comando **default** ***interface*** também exibe (se houver) outras interfaces que são afetadas pela QoS e outros recursos implementados nesse ASIC de porta.

P. Posso configurar a QoS em uma interface que tenha um IP secundário?

A. Yes. Você pode configurar a QoS em um IP secundário.

Informações Relacionadas

- Programação da saída de QoS nos Switches da série Catalyst 6500/6000 executando o Software do sistema CatOS
- Classificação e Marcação QoS nos Switches da Série catalyst 6500/6000 que Executam o Software CatOs
- Políticas de QoS nos switches Catalyst 6500/6000 Series
- Suporte a Produtos de LAN
- Suporte de tecnologia de switching de LAN
- Suporte Técnico e Documentação - Cisco Systems