Índice

Introdução

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.

Q. QoS é permitido à revelia em Catalyst 6500 Switch?

A. À revelia, QoS não é permitido. Emita o **comando set qos enable** a fim permitir QoS.

Q. Que é o valor do Differentiated Services Code Point do padrão (DSCP) que é atribuído aos pacotes?

A. Todo o tráfego que entra em uma porta não-confiável é identificado por meio de um DSCP de 0. Especificamente, o DSCP é observado a 0 pela porta de saída.

Q. Posso eu estabelecer QoS com base em VLAN em uns 6500?

A. A configuração padrão é com base na porta. Você pode mudar aquele se você emite o comando VLAN-**baseado /porta** *modificação dos* **qos do set port**.

Q. Que são as potencialidades de porta para cada placa de linha e como podem mim interpretar as capacidades da fila?

A. Refira a tabela das potencialidades de porta na compreensão à potencialidade de enfileiramento de uma seção da porta da programação de emissor de QoS no Catalyst 6500/6000 series switch que executa o software do sistema de CatOS.

Q. Que são as configurações de QoS do padrão em uns 6500 quando QoS é permitido inicialmente?

A. Refira a configuração padrão para QoS na seção do catalizador 6000 da programação de emissor de QoS no Catalyst 6500/6000 series switch que executa o software do sistema de CatOS.

Q. Onde cada um dos processos de QoS é executado no catalizador 6000?

A. Programação da entrada? Feito pelos circuitos integrados específicos de aplicativo de porta PINNACLE/COIL (ASIC). Camada 2 somente, com ou sem um Policy Feature Card (PFC).

Classificação? Feito pelo supervisor ou pelo PFC através do motor do Access Control List (ACL). Camada 2 somente, sem um PFC; Camada 2 ou camada 3 com um PFC.

Policiamento? Feito pelo PFC através do Engine de encaminhamento de camada 3. Camada 2 ou camada 3 com um PFC (exigido).

Reescrita do pacote? Feito pela porta asics PINNACLE/COIL. Camada 2 ou camada 3 baseada na classificação feita previamente.

Programação de emissor? Feito pela porta asics PINNACLE/COIL. Camada 2 ou camada 3 baseada na classificação feita previamente.

Q. Posso eu executar características de QoS sem um Policy Feature Card (PFC)?

A. Nos Catalyst 6000 Family Switch, o coração da funcionalidade de QoS reside no PFC e é uma exigência para o processamento de QoS da camada 3 ou da camada 4. Contudo, um supervisor sem um PFC pode ser usado para a classificação de QoS e a marcação da camada 2.

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

A. O PFC2 deixa-o abaixar a política de QoS para um Distributed Forwarding Card (DFC). O PFC2 igualmente adiciona o apoio para uma taxa excedente, que indique um segundo nível de policiamento em que as ações de política podem ser tomadas. Refira o suporte a hardware para QoS na seção do Catalyst 6000 Family de compreender Qualidade de Serviço em Catalyst 6000 Family Switch para mais informação.

Q. Que são a classe padrão de serviço (CoS) às configurações do mapeamento do transmitir fila quando auto-qos são permitidas?

A. **fila 2 2 cos 5,6,7 do set qos map 2q2t TX**

fila 2 do set qos map 2q2t TX 1 cos 1,2,3,4

fila 1 do set qos map 2q2t TX 1 cos 0

Q. Que é o Differentiated Services Code Point do padrão (DSCP) ao traço do Classe de serviço (CoS)?

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

Q. No Enfileiramento da saída, se a fila de prioridade estrita é saturada, o tráfego é servido eventualmente nas filas do round robin ponderado (WRR)?

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

Q. O round robin ponderado (WRR) determina a alocação de largura de banda baseada no número de pacotes ou em um determinado número de bytes?

A. Baseado em um determinado número de bytes, que podem representar mais de um pacote. O pacote final que excede os bytes atribuídos não é enviado. Com uma configuração de peso extremo, tal como 1% para a fila 1 e 99% para a fila 2, o peso configurado exato não pôde ser alcançado. O interruptor usa um algoritmo WRR para transmitir quadros de uma fila de cada vez. O WRR usa um valor do peso para decidir quanto transmitir de uma fila antes que comute à outra fila. Mais alto o peso atribuído a uma fila, o mais transmite a largura de banda é-lhe atribuído.

Nota: O número de bytes real transmitido não combina o cálculo porque os todos frame são transmitidos antes que comute à outra fila.

Q. Minha documentação nova da placa de linha 65xx diz que apoia o round robin ponderado do deficit (DWRR). Que são DWRR e que significa?

A. O DWRR transmite das filas sem morrer de fome a fila de baixa prioridade, porque se mantém a par da sob-transmissão da fila de baixa prioridade e se compensa a na próxima vez. Se uma fila não pode enviar um pacote porque seu tamanho do pacote é maior do que os bytes disponíveis, a seguir os bytes não utilizados são creditados à próxima vez.

Q. Que são os pesos padrão em uma porta 2q2t, e como mim os alteram?

A. Emita o comando do **wrr 2q2t** *q1_weight q2_weight dos* **qos do grupo** a fim alterar os pesos padrão para a fila 1 (o 5/260th servido fila de prioridade baixa do tempo) e a fila 2 (o 255/260th servido fila de alta prioridade do tempo).

Q. Eu gostaria de usar o Simple Network Management Protocol (SNMP) para recolher o número de pacotes descartado pelo vigilante individual. Isso é possível? Em caso afirmativo, que MIB é usado?

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

Q. Há um comando show que indique o número de pacotes descartado pelo vigilante?

A. **As estatísticas vigilante agregado** e **comandos show qos statistics l3stats dos qos da mostra** indicam o número de pacotes descartado pelo vigilante.

Q. Eu gostaria de usar o Simple Network Management Protocol (SNMP) para alterar um vigilante de modo que a taxa e os parâmetros de intermitência pudessem ser mudados dinamicamente. Por exemplo, pelo Time Of Day. Isso é possível? Em caso afirmativo, que MIB é usado?

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

Q. É possível executar QoS tempo--dia-baseado? especificamente, para alterar o máximo e as taxas de intermitência? através do Cisco IOS Software no Multilayer Switch Feature Card (MSFC) no modo híbrido? Se possível, este QoS é feito no hardware e não pelo processador MSFC?

A. Não, isto não pode ser feito. No modo híbrido (CatOS), todo o Regulamentação QoS é feito pelo supervisor.

Q. Eu não vi uma descrição de como a taxa do vigilante e os valores de intermitência do vigilante são executados. Eu gostaria de terminar a documentação técnica nestes, de modo que eu pudesse compreender o impacto que têm em

minha rede.

A. A taxa do vigilante e os valores de intermitência do vigilante são executados desse modo:

Por exemplo, se você quer um vigilante do 20 Mbps e uma unidade de transmissão máxima (MTU) (em Ethernet) de 1500 bytes, a seguir isto é como a explosão é calculada:

Contudo, devido à granularidade do hardware de policer com Sup1 e Sup2, você precisa de arredondar este a 32 kbps, que é o mínimo.

Refira estes documentos para obter mais informações sobre da taxa do vigilante e da aplicação dos valores de intermitência:

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

Q. Eu planeio em substituir meus supervisores Sup1A com o Sup2s. Fazem os mecânicos de QoS, tais como a taxa de intermitência, a mudança entre Sup1A e o Sup2?

A. Sim, há uma diferença entre dois supervisores quando um Catalyst 6500 Switch tem o SUP2/PFC2. Se executa o Cisco Express Forwarding (CEF), a seguir o comportamento é levemente diferente quando você configura o Netflow no SUP2.

Q. Que são alguns comandos que eu posso usar o monitor meus ajustes de QoS?

A. Refira a monitoração e a verificação de uma seção de configuração da classificação de QoS e a marcação no Catalyst 6500/6000 series switch que executa o CatOS Software.

Q. Quando eu executo o código do Catalyst Operating System (CatOS) em uns 6500 e o Cisco IOS Software no Multilayer Switch Feature Card (MSFC), eu emito os comandos qos no MSFC ou no supervisor?

A. Quando você executar o código híbrido (CatOS), você emite os comandos qos no supervisor/Policy Feature Card (PFC). Os 6500 executam QoS em três lugares:

- Com base no software no MSFC
- Com base em hardware (multi-camada interruptor-baseada) no PFC
- Com base no software em algumas placas de linha

Esta edição ocorre quando você trabalha com híbrido IO (CatOS + IO para o MSFC). O CatOS e os IO têm dois grupos de comandos configuration. Contudo, quando você configura QoS sob o Native IOS, por exemplo com os motores mais novos Sup32 ou de Sup720, você é mais adicional do hardware, e a peça da placa de linha é invisível ao usuário. Isto é importante porque a maioria do tráfego é multi-camada comutada (hardware comutado). Consequentemente, é segurado pela lógica PFC. O MSFC nunca vê esse tráfego. Se você não está estabelecendo QoS PFC-baseado, a maioria do tráfego é perdido.

Q. Que acontece se o comando trust dos qos do set port não é apoiado por minha

placa de linha?

A. Você pode criar um Access Control List de QoS (ACL) para confiar o valor do Differentiated Services Code Point (DSCP) do pacote recebido. Por exemplo, emita o **comando any do Trust-dscp do teste acl IP dos qos do grupo**.

Q. Que é a diferença entre o agregado e as vigilâncias de microfluxo?

A. Refira a classificação e vigilância com a seção PFC de compreender Qualidade de Serviço em Catalyst 6000 Family Switch.

Q. Que comandos permitem que eu ver estatísticas para o agregado ou as vigilâncias de microfluxo?

A. Com Supervisor Engine 1 e 1A, não é possível ter o policiamento de policeres agregados das estatísticas de individual. Emita o **comando show qos statistics l3stats** a fim ver o por-sistema que policia estatísticas.

Com o Supervisor Engine 2, você pode ver o agregado que policia estatísticas em uma base do por-vigilante com o **comando show qos statistics aggregate-policer**. Emita o **comando show mls entry qos short** a fim verificar estatísticas de vigilância de microfluxo.

Q. O modelagem de tráfego é apoiado no interruptor do Catalyst 6500 (Cat6K)?

A. A modelagem de tráfego é suportada apenas em determinados módulos de WAN para a série Catalyst 6500/6000, como os módulos OSMs e FlexWAN. Refira configurar o Class-based traffic shaping e o modelagem de tráfego para mais informação.

Q. Quanto o agregado ou as vigilâncias de microfluxo são apoiados no interruptor do Catalyst 6500 (Cat6K)?

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

Q. Que Catalyst Operating System (CatOS) ou a imagem IOS Cisco do Multilayer Switch Feature Card (MSFC) são exigidos para apoiar o policiamento?

A. O Supervisor Engine 1A apoia o ingresso que policiam na versão catos 5.3(1) e mais atrasado, e o Cisco IOS Software Release 12.0(7)XE e Mais Recente.

O Supervisor Engine 2 apoia o ingresso que policiam na versão catos 6.1(1) e mais atrasado, e o Cisco IOS Software Release 12.1(5c)EX e Mais Recente. Contudo, a vigilância de microfluxo é apoiada somente no Cisco IOS Software.

Q. Eu promovi de Sup2 a Sup720 e minhas estatísticas policiadas da taxa de tráfego mostram diferentemente com o mesmo tráfego. Por quê?

A. Uma mudança importante no policiamento no Supervisor Engine 720 é que pode contar o tráfego pelo comprimento da camada 2 do quadro. Isto difere do Supervisor Engine 1 e do

Supervisor Engine 2, que contam quadros IP e IPX por seu comprimento da camada 3. Com alguns aplicativos, mergulhe 2 e mergulhe 3 comprimentos não pôde ser consistente. Um exemplo é um pacote pequeno da camada 3 dentro de um grande quadro da camada 2. Neste caso, o Supervisor Engine 720 pôde indicar uma taxa de tráfego policiada levemente diferente em relação ao Supervisor Engine 1 e ao Supervisor Engine 2.

Q. Como eu sei que valores a se usar para a taxa e a estourar quando eu configuro um vigilante?

A. Estes parâmetros controlam o funcionamento do Token Bucket:

- **Taxa**? 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 como os tokens são removidos frequentemente da cubeta. 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.
- **Explosão**? Define o número máximo de tokens que a cubeta pode sustentar a qualquer altura. A explosão deve ser nenhuma menos do que o tempo de taxa o intervalo a fim sustentar a taxa especificada de tráfego. Outra consideração é que o pacote de tamanho máximo deve caber no bucket.

Use esta equação a fim determinar o parâmetro de intermitência:

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

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

Nota: No Cisco IOS Software, a taxa de vigilância é definida nos bit por segundo (bps). No Catalyst Operating System (CatOS), é definida nos kbps. Também, no Cisco IOS Software, a taxa de intermitência é definida nos bytes, mas em CatOS, é definida nos kilobits.

Nota: Devido à granularidade de vigilância de hardware, à taxa exata e à explosão é arredondado ao valor suportado o mais próximo. Seja certo que o valor de intermitência é não menos que o pacote de tamanho máximo. Caso contrário, todos os pacotes maiores que o tamanho da intermitência são cancelados.

Por exemplo, se você tenta ajustar a explosão a 1518 no Cisco IOS Software, é arredondado a 1000. Isto faz com que a todos os quadros os de 1000 bytes maiores sejam deixados cair. A solução é configurar a explosão a 2000.

Quando você configura a taxa de intermitência, leve em consideração que alguns protocolos, tais como o TCP, executam um mecanismo de controle de fluxo que reaja à perda de pacotes. Por exemplo, o TCP reduz o windowing pela metade para cada pacote perdido. Consequentemente, quando policiada a uma determinada taxa, a utilização de link eficaz é mais baixa do que a taxa configurada. É possível aumentar a intermitência para obter melhor utilização. Um bom começo para tal tráfego é dobrar o tamanho de intermitência. Neste exemplo, o tamanho de intermitência é aumentado de 13 kbps a 26 kbps. Depois, monitore o desempenho e efetue os ajustes necessários.

Pela mesma razão, não se recomenda que você avalia a operação de vigilância com tráfego

orientado de conexão. Isto mostra geralmente o desempenho mais baixo do que as licenças do vigilante.

Q. Eu estou configurando QoS sobre um Canal de porta. Há alguma limitação que eu precisar de conhecer?

A. Quando você configurar QoS nas portas que são parte de um Canal de porta no Catalyst Operating System (CatOS), você deve aplicar a mesma configuração a todas as portas física no Canal de porta. Estes parâmetros devem concordar para todas as portas no Canal de porta:

- Tipo da confiabilidade da porta
- Receba o tipo de porta (2q2t ou 1p2q2t)
- Transmita o tipo de porta (1q4t ou 1p1q4t)
- Classe de serviço (CoS) da porta padrão
- QoS com base na porta ou QoS com base em VLAN
- Access Control List (ACL) ou pares do protocolo que a porta leva

Q. Por que sou eu incapaz de ajustar o valor de limiar mín?

A. Com versões do Catalyst Operating System (CatOS) mais cedo de 6.2, o comando threshold do Weighted Random Early Detection (WRED) ajustam somente o limiar máx, quando o limiar mín for codificado duramente a 0%. Isto é corrigido em CatOS 6.2 e mais atrasado, que permitem a configuração do valor de limiar mín. O limiar mín do padrão depende da precedência. O limiar mín para a Precedência IP 0 corresponde a um meio do limiar máx. Os valores para os precedentes que permanecem queda entre um meio do limiar máx, e o limiar máx em intervalos uniformemente espaçados.

Q. Eu estou tendo a dificuldade que ajusta os bufferes do transmitir fila. Há alguma limitação?

A. Se você tem três filas (1p2q2t), a fila prioritária do round robin ponderado (WRR) e a fila de prioridade estrita deve ser ajustada a mesmo nível.

Q. Eu tenho uma placa de linha 62xx/63xx. Eu não posso aplicar o comando set que o Differentiated Services Code Point das confianças (DSCP) em uma porta. Há uma limitação nesta placa de linha para características de QoS?

A. Sim, porque você não pode emitir o **Trust-dscp**, o **Trust-ipprec**, ou os **comandos trust-cos nas** placas de linha WS-X6248-xx, WS-X6224-xx, e WS-X6348-xx. O método o mais fácil é nesta situação deixar todas as portas como o não-confiável e mudar o Access Control List do padrão (ACL) ao **comando trust dscp**:

```
set qos enableset port qos 2/1-16 trust untrustedset qos acl default-action ip trust-dscp
```

Refira as limitações da seção das placas de linha WS-X6248-xx, WS-X6224-xx, e WS-X6348-xx da classificação de QoS e da marcação no Catalyst 6500/6000 series switch que executa o CatOS Software para limitações placa de linha-específicas da adição.

Q. Que versões e supervisores do Catalyst Operating System (CatOS) são exigidos para apoiar o policiamento?

A. O Supervisor Engine 1A apoia o ingresso que policia na versão catos 5.3(1) e mais atrasado, e no Cisco IOS Software Release 12.0(7)XE e Mais Recente.

Nota: Uma placa-filha do Policy Feature Card (PFC) é exigida policiando com o Supervisor Engine 1A.

O Supervisor Engine 2 apoia o ingresso que policia na versão catos 6.1(1) e mais atrasado, e no Cisco IOS Software Release 12.1(5c)EX e Mais Recente. O Supervisor Engine 2 apoia o parâmetro de vigilância da taxa excedente.

O supervisor 720 apoia o ingresso que policia a porta e nível da interface de VLAN. Refira a atualização dos recursos de vigilância para a seção do Supervisor Engine 720 do Regulamentação QoS no Catalyst 6500/6000 series switch para obter mais informações sobre dos recursos de vigilância de Sup720.

Q. Que eu preciso de saber sobre a configuração de QoS sobre o EtherChannel?

A. Quando você configura QoS em uma porta que seja parte de um EtherChannel em CatOS, você deve sempre configurar-lo em uma base por porto. Também, você deve assegurar-se de que você aplique a mesma configuração de QoS a todas as portas, porque o EtherChannel pode somente empacotar portas com as mesmas configurações de QoS. Isto significa que você precisa de configurar estes parâmetros o mesmos:

- Tipo da confiabilidade da porta
- Receba o tipo de porta (2q2t ou 1p2q2t)
- Transmita o tipo de porta (1q4t ou 1p1q4t)
- Classe de serviço (CoS) da porta padrão
- QoS com base na porta ou QoS com base em VLAN
- Access Control List (ACL) ou pares do protocolo que a porta leva

Q. Onde posso eu encontrar exemplos do uso do Access Control Lists (ACLs) de QoS marcar ou policiar o tráfego?

A. Refira o caso 1: Marcação na seção da borda da classificação de QoS e marcação no Catalyst 6500/6000 series switch que executa o CatOS Software para um exemplo do tráfego da marcação.

Refira configurar e monitore o policiamento na seção do CatOS Software do Regulamentação QoS no Catalyst 6500/6000 series switch para um exemplo de policiar o tráfego.

Q. Que é a diferença entre o Access Control Lists (ACLs) com base na porta e com base em VLAN de QoS?

A. Cada QoS ACL pode ser aplicado a uma porta ou a um VLAN, mas há um parâmetro de configuração adicional a levar em consideração: 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 configurações:

1. Se uma porta com base em VLAN com um ACL aplicado é atribuída a um VLAN que igualmente tenha um ACL aplicado, a seguir o ACL com base em VLAN toma a prioridade sobre o ACL com base na porta.

2. Se uma porta com base na porta com um ACL aplicado é atribuída a um VLAN que igualmente tenha um ACL aplicado, a seguir o ACL com base na porta toma a prioridade sobre o ACL com base em VLAN.

Refira que dos quatro origens possíveis para o DSCP interno será usado? seção da classificação de QoS e da marcação no Catalyst 6500/6000 series switch que executa o CatOS Software para mais informação.

Q. Que é o valor típico do tamanho de intermitência a ser usado para a taxa limite em switch de camada 3?

A. Os switch de camada 3 executam uma aproximação do único algoritmo de token bucket no firmware. Um tamanho de intermitência razoável para a escala das taxas de tráfego é aproximadamente 64000 bytes. O tamanho da intermitência deve ser escolhido de forma a incluir pelo menos um pacote de tamanho máximo. Com cada pacote chegando, o algoritmo de vigilância determina o tempo entre este pacote e o último pacote, e calcula o número de tokens gerados durante o tempo transcorrido. Então, adiciona este número de tokens à cubeta e determina a se o pacote chegando se conforma, ou excede os parâmetros especificados.

Q. Por que é que mim receba um desempenho mais baixo para o tráfego TCP com taxa limite?

A. Os aplicativos de TCP/IP comportam-se deficientemente quando os pacotes são deixados cair em consequência da taxa limite. Isto é devido ao esquema inerente do windowing usado no controle de fluxo. Você pode ajustar o parâmetro do tamanho de intermitência ou o parâmetro de taxa para obter o throughput requerido.

Q. Que são a vantagem do Weighted Random Early Detection (WRED), e como mim sabem se minha placa de linha pode apoiar o WRED?

A. Para a fuga de congestionamento na programação de emissor, o interruptor do Catalyst 6500 (Cat6K) apoia o WRED em algumas filas da saída. Cada fila tem um tamanho configurável e um ponto inicial. Alguns têm o WRED. O WRED é um mecanismo de fuga de congestionamento que deixe cair aleatoriamente pacotes com uma determinada Precedência IP quando os bufferes alcançam um enchimento do limiar definido. O WRED é uma combinação de duas características: queda traseira e Random Early Detection (RED). A aplicação adiantada do Catalyst Operating System (CatOS) do WRED ajustou somente o limiar máx, quando o limiar mín duro-foi codificado a 0%. Note que a probabilidade de queda para um pacote é sempre NON-nula, porque estão sempre acima do limiar mín. Este comportamento é corrigido em CatOS 6.2 e mais atrasado. O WRED é um mecanismo de fuga de congestionamento muito útil para quando o tipo de tráfego é com base em TCP. Para outros tipos de tráfego, o VERMELHO não é muito eficiente porque o VERMELHO se aproveita do mecanismo de janelamento que é usado pelo TCP para controlar a congestão.

Refira a compreensão à potencialidade de enfileiramento de uma seção da porta da programação de emissor de QoS no Catalyst 6500/6000 series switch que executa o software do sistema de CatOS a fim determinar se uma placa de linha ou uma estrutura da fila podem apoiar o WRED. Você pode igualmente emitir o **comando show port capabilities** a fim ver a estrutura da fila de sua placa de linha.

Q. Que é o Differentiated Services Code Point interno (DSCP)?

A. Cada quadro tem um Classe de serviço (CoS) interno atribuído, o CoS recebido ou a porta CoS padrão. Isto inclui os frames sem etiqueta que não levam nenhum CoS real. Este CoS interno e o DSCP recebido são escritos em um cabeçalho de pacote especial (chamado um cabeçalho de barramento de dados) e enviados sobre o barramento de dados ao mecanismo de switching. Isto acontece na placa de linha do ingresso. Neste momento, não se sabe ainda se este CoS interno está levado aos circuitos integrados do aplicativo específicos da saída (ASIC) e introduzido no frame enviado. Uma vez que o encabeçamento alcança o mecanismo de switching, a lógica de reconhecimento de endereço codificado (EARL) do mecanismo de switching atribui a cada quadro um DSCP interno. Este DSCP interno é uma prioridade interna atribuída ao quadro pelo Policy Feature Card (PFC) como ele transita pelo interruptor. Não é o DSCP no cabeçalho de IPv4. Está derivado de um CoS existente ou do Tipo de serviço (ToS) que ajustam-se, e usado para restaurar o CoS ou o ToS enquanto o quadro retira o interruptor. Esse DSCP interno é atribuído a todos os quadros comutados (ou roteados) pelo PFC, inclusive quadros que não são IP.

Q. Que são os origens possíveis para o Differentiated Services Code Point interno (DSCP)?

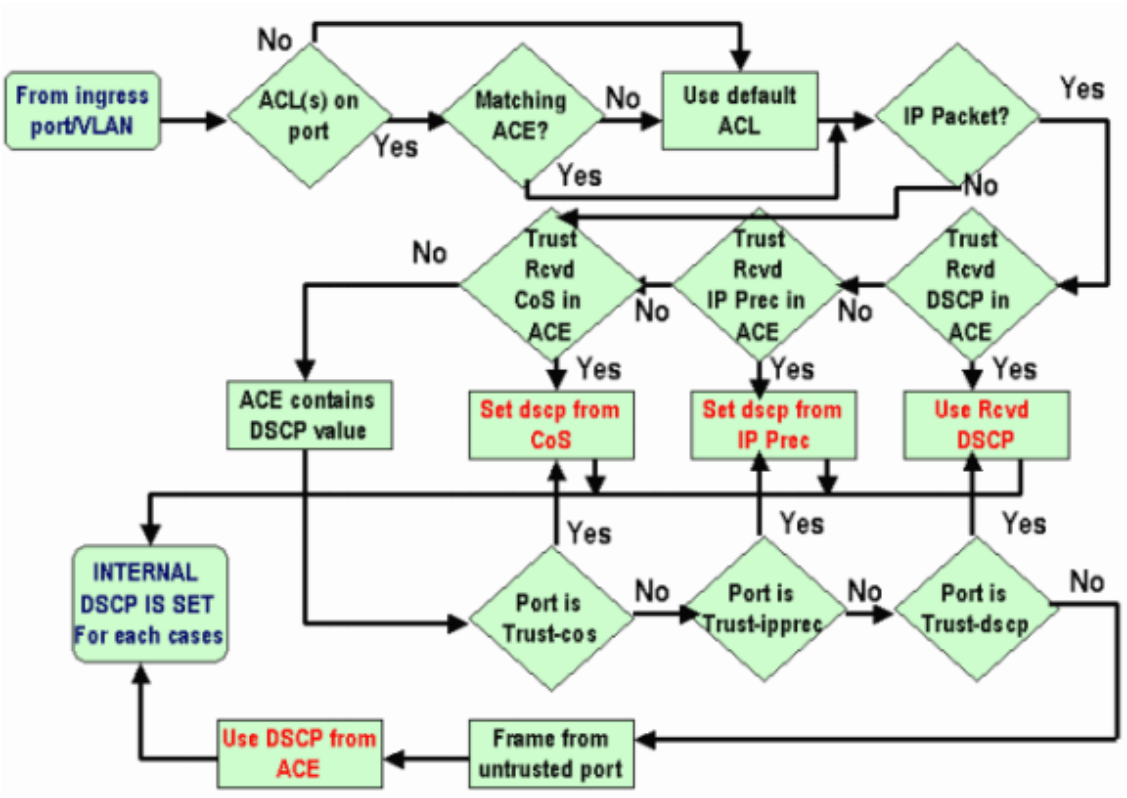
A. Refira os quatro origens possíveis para a seção do DSCP interno da classificação de QoS e da marcação no Catalyst 6500/6000 series switch que executa o CatOS Software.

Q. Como o Differentiated Services Code Point interno (DSCP) é escolhido?

A. O DSCP interno depende destes fatores:

- Port trust state
- Access Control List (ACL) anexado à porta
- ACL padrão
- Com base em VLAN ou com base na porta, com respeito ao ACL

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



Q. O Class-Based Weighted Fair Queuing (CBWFQ) ou o Low Latency Queuing (LLQ) são apoiados no interruptor do Catalyst 6500 (Cat6K)?

A. Sim, o CBWFQ permite que você defina uma classe de tráfego e atribua-lhe uma garantia de largura de banda mínima. O algoritmo atrás deste mecanismo é Weighted Fair Queuing (WFQ), que explica o nome. Você define classes específicas em indicações da classe de mapas a fim configurar o CBWFQ. Então você atribui uma política a cada classe em um mapa de política. Este mapa de política é anexado então ao de entrada/de partida de uma relação.

Q. O valor do Classe de serviço (CoS) da camada 2 é retido para pacotes roteado?

A. Sim, o Differentiated Services Code Point interno (DSCP) é usado para restaurar o CoS em quadros da saída.

Q. QoS aplica a configuração idêntica a toda a porta de LAN que são controladas pelo mesmo ASIC?

A. Sim, quando estes comandos são configurados, QoS aplica a configuração idêntica a todas as portas LAN/routed controladas pelo mesmo circuito integrado característico da aplicação (ASIC). Os ajustes de QoS são propagados a outras portas de que pertença ao mesmo ASIC independentemente se a porta é uma porta de acesso, porta de tronco ou uma porta roteada.

- a RCV-fila aleatório-detecta
- fila-limite da RCV-fila
- fila-limite do wrr-queue
- largura de banda do wrr-queue (exceto portas de LAN do Gigabit Ethernet)
- mapa COS da prioridade-fila
- mapa COS da RCV-fila
- mapa COS do wrr-queue
- ponto inicial do wrr-queue
- ponto inicial da RCV-fila
- o wrr-queue aleatório-detecta
- o wrr-queue aleatório-detecta o limiar mín
- o wrr-queue aleatório-detecta o limiar máx

Quando o comando da **interface padrão** é executado em algumas das portas, então o ASIC que controla a porta particular restaura a configuração de QoS para todas as portas controladas por ele.

Q. Por que o comando show traffic-shape statistics não mostra o resultado positivo mesmo quando o tráfego que shapping dentro é configurado?

```
Router#show traffic-shape statistics          Access Queue     Packets   Bytes     Packets
Bytes     ShapingI/F       List   Depth                          Delayed   Delayed   ActiveEt0
101    0         2         180       0         0         noEt1              0         0
0         0         0          no
```

A. O atributo ativo dando forma tem **sim** quando os temporizadores indicam que o modelagem de tráfego ocorre e **nenhum** se o modelagem de tráfego não ocorre.

Você pode usar o **comando show policy-map** a fim verificar se o tráfego configurado trabalha.

```
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
```

Q. O Catalyst 6500 PFC apoia todos os comandos qos padrão?

A. O Cisco catalyst 6500 PFC QoS tem algumas limitações e não apoia alguns comandos QoS-relacionados. Refira este a documentos para a lista completa dos comandos não apoiados.

- Limitações do comando class map
- Limitações do comando do mapa de política
- Limitações do comando class do mapa de política

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

A. O plano do controle de software que policia contadores (de CoPP) é a soma dos pacotes que atravessam o hardware CoPP e limitação da taxa do hardware. Os pacotes são segurados primeiramente por limitadores da taxa do hardware, e se não combinam, a seguir por hardware CoPP vêm representar. Se o limitador da taxa do hardware permite os pacotes, este pacote vai ao software onde é processado pelo software CoPP. Devido a este software, CoPP pode ser maior do que contadores de CoPP do hardware.

Igualmente há algumas limitações onde CoPP não é apoiado no hardware. Alguns delas são:

- CoPP não é apoiado no hardware para pacotes de transmissão múltipla. A combinação ACL, limitadores da taxa do Multicast CPU, e de software de CoPP de proteção fornece a proteção contra ataques DoS do Multicast.
- CoPP não é apoiado no hardware para pacotes de transmissão. A combinação ACL, controle de tempestade do tráfego, e de software de CoPP de proteção fornece a proteção contra ataques DoS da transmissão.
- As classes que combinam o Multicast não são aplicadas no hardware mas são aplicadas no software.
- CoPP não está permitido no hardware a menos que o MMLS QoS for permitido globalmente com o **comando mls qos**. Se o **comando mls qos** não é inscrito, CoPP trabalha somente no software e não fornece nenhum benefício ao hardware.

Refira configurar o Policiamento do plano de controle (CoPP) para mais informação.

Q. A configuração do comando qos do padrão (relação) trabalha em outras /portas das relações?

A. Quando o comando da **interface padrão** é emitido, a configuração fora de padrão está recolhida, que é similar ao que é indicado no *x/y do* **show running-config interface**, e cada um daquelas é ajustada a seus valores padrão. Esta pode ser uma negação simples de um comando demasiado.

Se há algum QoS ou outro recurso que estiverem configurados nessa relação, e naqueles comandos get negados, podem propagar a outras relações da placa de linha.

Recomenda-se verificar a saída do **comando capabilities do** *x/y da* **relação da mostra**, antes que você continue com falha de uma relação. Consulte faz QoS aplicam a configuração idêntica a toda a porta de LAN que são controladas pelo mesmo ASIC? para obter mais informações.

A saída do comando da **interface padrão** igualmente indica (eventualmente) outras relações que obtêm afetadas para QoS e outros recursos executados nessa porta ASIC.

Q. Posso eu configurar QoS em uma relação que tenha um IP secundário?

A. Sim. Você pode configurar 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
- Vigilância de QoS nos Switches das Séries Catalyst 6500/6000
- Suporte a Produtos de LAN
- Suporte de tecnologia de switching de LAN
- Suporte Técnico e Documentação - Cisco Systems