Entendendo a qualidade do serviço nos Switches da família Catalyst 6000

Índice

- Introdução
- Definindo a QoS da camada 2
- A necessidade de QoS em um Switch
- Suporte de hardware para QoS no Catalyst 6000 Family
- Suporte para QoS ao software da família Catalyst 6000
- Mecanismos de prioridade em IP e Ethernet
- Fluxo de QoS no Catalyst 6000 Family
- Filas, buffer, limiares e mapeamentos
- WRED ou WRR
- Configurando o QoS com base na porta ASIC no Catalyst 6000 Family
- Classificação e vigilância com o PFC
- Common Open Policy Server
- Informações Relacionadas

Introdução

Este documento explica as características de qualidade de serviço (QoS) disponíveis nos switches da família Catalyst 6000. Este documento abrange os recursos de configuração da qualidade de serviço (QoS) e fornece alguns exemplos de como a QoS pode ser implementada.

Este documento não é significado ser um manual de configuração. Os exemplos de configuração são usados durante todo este papel para ajudar na explicação das características de QoS do hardware e software do Catalyst 6000 Family. Para a referência da sintaxe para estruturas de comando qos, refira por favor a seguintes configuração e guias de comando para o Catalyst 6000

Family:

- Catalyst 6500 Family Switch

Definindo a QoS da camada 2

Quando muitos puderem pensar que QoS no Switches da camada 2 (L2) é simplesmente sobre frames da Ethernet da prioridade, não muitos realizam que envolve muito mais. O L2 QoS envolve o seguinte:

1. **Programação da fila de entrada:** quando o quadro entra na porta, pode ser atribuído a um de um número de filas com base em portas antes de ser programado para Switching em uma porta de saída. Tipicamente, as filas múltiplas são usadas onde o tráfego diferente exige níveis de serviço diferentes, ou onde a latência do interruptor deve ser mantida a um mínimo. Por exemplo, o IP baseou o vídeo e os dados de voz exigem a latência baixa, tão lá podem ser uma necessidade de comutar estes dados antes de comutar outros dados tais como o File Transfer Protocol (FTP), Web, email, telnet, e assim por diante.

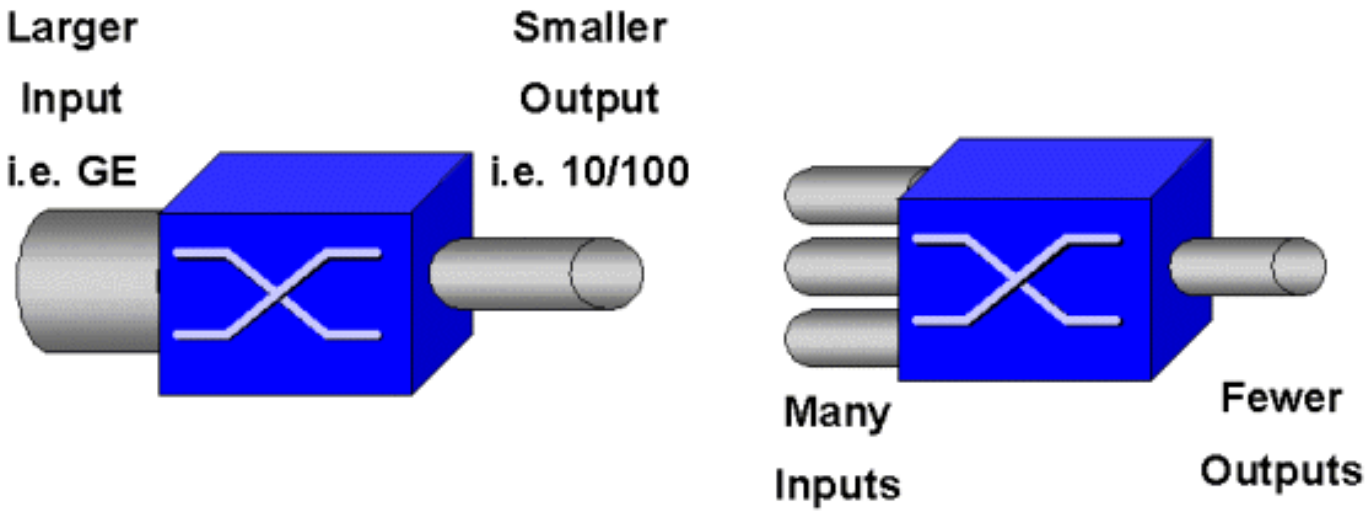
2. **Classificação** o processo de classificação envolve inspecionar campos diferentes no encabeçamento dos Ethernet L2, junto com campos no cabeçalho IP (camada 3 (o L3)) e o encabeçamento do protocolo Protocolo de control de transmisión (TCP)/protocolo de datagrama de usuário (TCP/UDP) (camada 4 (L4)) para ajudar em determinar o nível do serviço que será aplicado ao quadro como ela transita pelo interruptor.
3. **Vigilância:** policiar é o processo de inspecionar um frame da Ethernet para ver se excedeu uma taxa de tráfego pré-definida dentro de um determinado tempo de frame (tipicamente, este tempo de frame é um número fixo interno ao interruptor). Se esse quadro for fora de perfil (isto é, é parte de um fluxo de dados além do limite de taxa pré-definida), pode ou ser deixado cair ou o valor do Classe de serviço (CoS) pode ser marcado para baixo.
4. **Regravando:** o processo de reescrita é a capacidade do interruptor para alterar o CoS no cabeçalho de Ethernet ou nos bit do Tipo de serviço (ToS) no encabeçamento IPV4.
5. **Programação de fila de saída:** após os processos da reescrita, o interruptor colocará o frame da Ethernet em uma fila de partida apropriada (da saída) para comutar. O interruptor executará o gerenciamento de buffer nesta fila assegurando-se de que o buffer não transborde. Fará tipicamente este utilizando um algoritmo (VERMELHO) do Random Early Discard, por meio de que os quadros aleatórios são removidos (deixado cair) da fila. O RED ponderado (WRED) é um derivado do RED (usado por determinados módulos da família Catalyst 6000), pelo qual os valores de CoS são inspecionados para determinar quais quadros serão descartados. Quando os buffers atingem limites predefinidos, quadros com prioridade menor são normalmente descartados, mantendo os quadros com a prioridade maior na fila.

Este documento explica com maiores detalhes cada um dos mecanismos acima e como se relacionam ao Catalyst 6000 Family nas seguintes seções.

A necessidade de QoS em um Switch

As Placas-mãe de grande porte, milhões de pacotes comutados por segundo, e NON-obstruindo

o Switches são tudo sinônimas com muito Switches hoje. Por que um QoS é necessário? A resposta é devido a um congestionamento.



Um interruptor pode ser o interruptor o mais rápido no mundo, mas se você tem qualquer uma das duas encenações mostradas na figura acima, que interruptor experimentará a congestão. Na época da congestão, se as características de Tratamento de Congestionamento não são no lugar, os pacotes serão deixados cair. Quando os pacotes são descartados, as retransmissões ocorrem. Ao ocorrerem retransmissões, a carga da rede pode aumentar. Nas redes que são congestionadas já, isto pode adicionar aos problemas de desempenho existentes e para promover potencialmente degrade o desempenho.

Com redes convergentes, o gerenciamento do congestionamento é ainda mais crítico. O tráfego sensível da latência tal como a Voz e o vídeo pode severamente ser impactado se os atrasos são incorridos. Simplesmente adicionar mais bufferes a um interruptor igualmente não aliviará necessariamente problemas de congestionamento. O tráfego sensível da latência precisa de ser comutado o mais rápido possível. Primeiramente, você precisa de identificar este tráfego importante com as técnicas de classificação, e executa então técnicas de gerenciamento de buffer para evitar o tráfego mais prioritário de ser deixado cair durante a congestão. Finalmente, você precisa de incorporar técnicas da programação para comutar o mais rapidamente possível pacotes importantes das filas. Porque você lerá dentro este documento, o Catalyst 6000 Family executa todas estas técnicas, fazendo seu subsistema QoS um do mais detalhado na indústria hoje.

Todas as técnicas QoS descritas na seção anterior serão exploradas com maiores detalhes durante todo este documento.

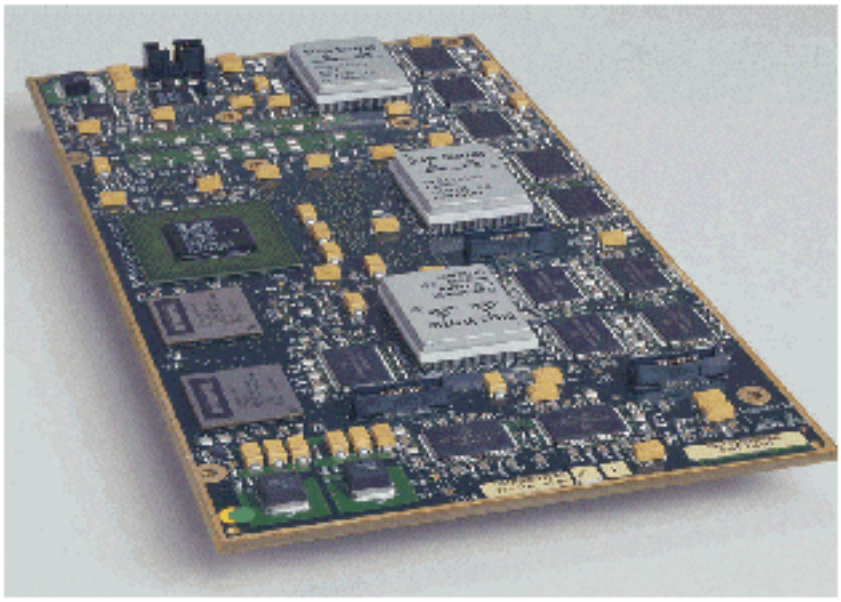
Suporte de hardware para QoS no Catalyst 6000 Family

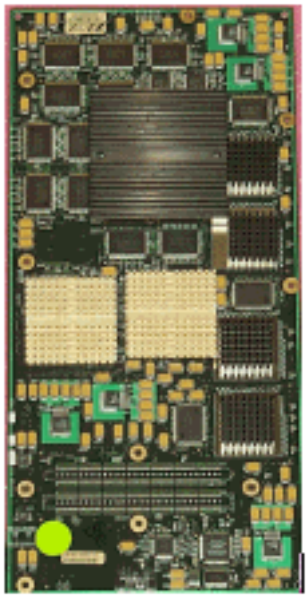
Para apoiar QoS no Catalyst 6000 Family, algum suporte a hardware é exigido. O hardware que apoia QoS inclui o Multilayer Switch Feature Card (MSFC), o Policy Feature Card (PFC), e os circuitos integrados característicos da aplicação da porta (ASIC) nas placas de linha elas mesmas. Este documento não abordará as capacidades de QoS do MSFC; em vez diz, se concentrará nas capacidades de QoS do PFC e nos ASICs das placas de linha.

PFC

O PFC versão 1 é uma placa secundária acomodada no Supervisor I (SupI) e o Supervisor IA

(SupIA) da família Catalyst 6000. O PFC2 é versão aprimorada do PFC1 e é fornecido com o novo Supervisor II (SupII) e alguns ASICs novos integrados na placa. Quando o PFC1 e o PFC2 forem sabidos primeiramente para sua aceleração de hardware do interruptor L3, QoS é uma de suas outras finalidades. Os PFC são mostrados abaixo.





Embora PFC 1 e PFC2 sejam essencialmente iguais, existem algumas diferenças na funcionalidade QoS. A saber, o PFC2 adiciona o seguinte:

1. A capacidade de aplicar a política de QoS em uma DFC (Placa de encaminhamento distribuído).

2. As decisões sobre vigilância são ligeiramente diferentes. o PFC1 e o PFC2 apoiam o policiamento normal por meio de que os quadros estão deixados cair ou marcados para baixo se um agregado ou a política de micro-fluxo retorna uma decisão fora de perfil. Contudo, o PFC2 adiciona o apoio para uma taxa excedente, que indique um segundo nível de policiamento que as ações de política podem ser tomadas em.

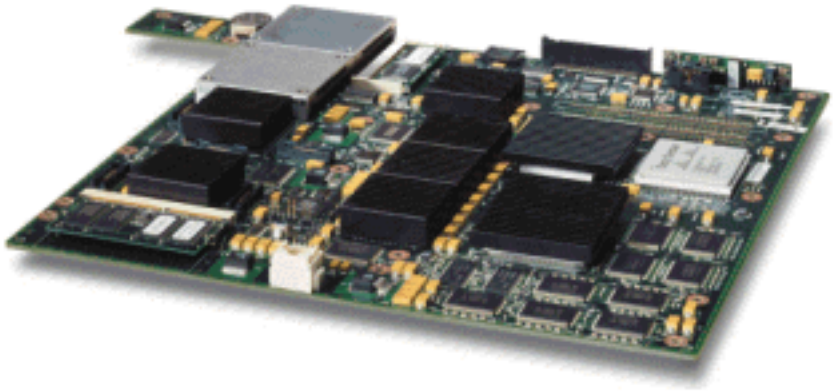
Quando um vigilante da taxa excedente é definido, os pacotes podem ser deixados cair ou marcado abaixo de quando excedem a taxa excedente. Se um nível da vigilância em excesso é ajustado, o mapeamento de DSCP adicional está usado para substituir o valor original DSCP com

um valor marcado-para baixo. Se somente um nível normal da polícia é ajustado, o mapeamento de DSCP normal está usado. O nível da vigilância em excesso terá a precedência para selecionar regras do mapeamento quando ambos os níveis da polícia são ajustados.

Éimportante notar que as funções de QoS descritas neste documento executado pelos ASIC mencionados rendem níveis altos do desempenho. O desempenho de QoS em um Catalyst 6000 Family básica (sem módulo de Switch Fabric) produz 15 MPPS. Os ganhos adicionais de desempenho podem ser conseguidos para QoS se os DFC são usados.

DFC

O DFC pode ser anexado ao WS-X6516-GBIC como uma opção. Contudo, é uma solução padrão no cartão WS-X6816-GBIC. Pode igualmente ser apoiado em outras placas de linha futuras da tela tais como a placa de linha recentemente introduzida da tela 10/100 (WS-X6548-RJ45), a placa de linha da tela RJ21 (WS-X6548-RJ21), e a placa de linha 100FX (WS-X6524-MM-FX). O DFC é mostrado a seguir.



O DFC permite que a placa de linha da tela (barra transversal conectada) execute o switching local. A fim fazer isto, deve igualmente apoiar todas as políticas de QoS que forem definidas para o interruptor. O administrador não pode diretamente configurar o DFC; um pouco, vem sob o controle do mestre MSFC/PFC no supervisor ativo. O PFC preliminar abaixará uma tabela do banco de informação de encaminhamento (FIB), que dê ao DFC suas tabelas do forwarding L2 e L3. Igualmente abaixará uma cópia das políticas de QoS de modo que sejam igualmente locais à placa de linha. No seguimento disto, as decisões do switching local podem prover a cópia local de todas as políticas de QoS que fornecem velocidades de processamento de QoS do hardware e que rendem um Distributed Switching mais alto dos níveis de desempenho embora.

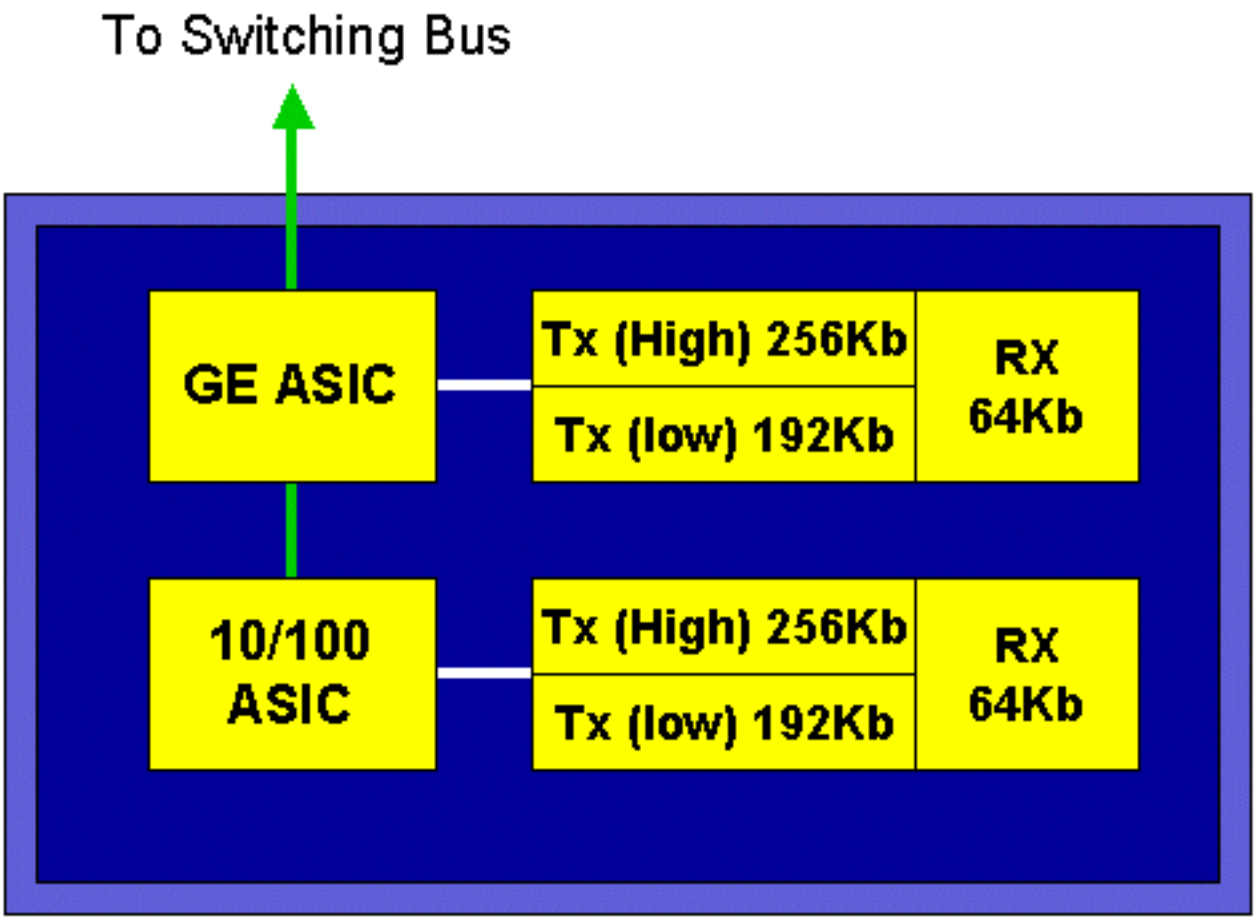
A porta baseou ASIC

Para completar a imagem do hardware, cada uma das placas de linha implementam um número de ASICs. Aqueles ASIC executam as filas, a proteção, e os pontos iniciais usados para o armazenamento temporário dos quadros enquanto transitam pelo interruptor. Nas placas 10/100, uma combinação de ASICs é usada para suprir as 48 portas 10/100.

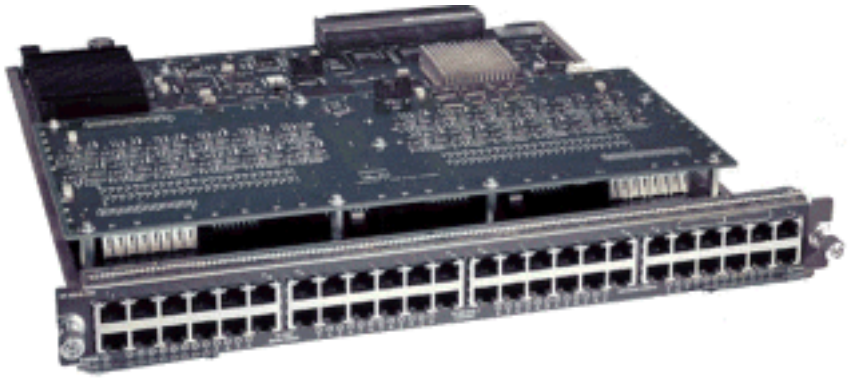
Placas de linha do original 10/100 (WS-X6348-RJ45)

OS ASICs de 10/100 fornecem uma série de filas de Recepção (Rx) e Transmissão (Tx) para cada porta 10/100. Os ASICs fornecem 128 K de buffer por porta 10/100. Refira os Release Note para detalhes no que pela proteção da porta está disponível em cada placa de linha. Cada porta nesta placa de linha apoia uma fila RX e duas o alto e baixo denotado TX filas. Isto é mostrado no

diagrama abaixo.



No diagrama acima, cada 10/100 ASIC fornecem uma fuga para 12 10/100 das portas. Para cada porta de 10/100, os bufferes 128 K são fornecidos. O 128 K dos bufferes é rachado entre cada um das três filas. As figuras mostradas na fila acima não são o padrão, entretanto elas podem ser uma representação do que poderia ser configurado. A fila Rx única fica com 16 K e a memória restante (112 K) é dividida entre as duas filas Tx. À revelia (em Cactos), a fila alta obtém 20 por cento deste espaço e a baixa fila obtém 80 por cento. No Catalyst IOS, o padrão é dar os por cento altos da fila 10 e a baixa fila 90 por cento.

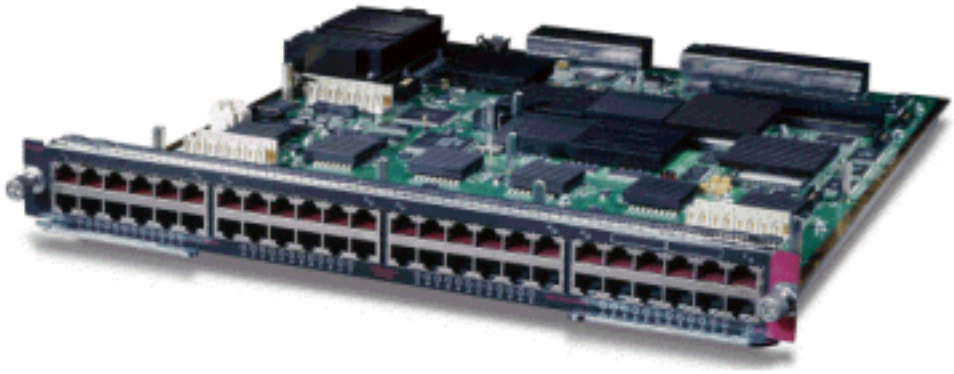


Quando o cartão fornecer o buffer de estágio dual, simplesmente 10/100 de proteção baseada ASIC está disponível para ser manipulado durante a configuração de QoS.

Placas de linha da tela 10/100 (WS-X6548-RJ45)

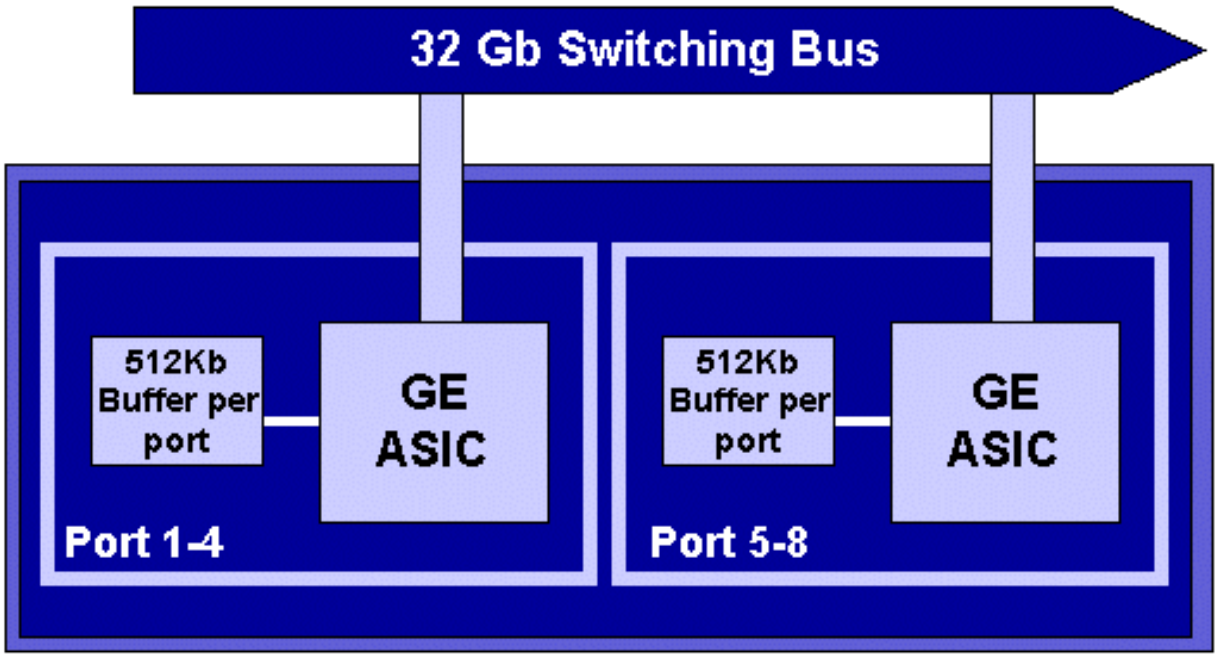
As novas ASICs de 10/100 fornecem uma série de filas Rx e TX para cada porta 10/100. Os ASIC fornecem um pool compartilhado da memória disponível através das portas de 10/100. Refira os

Release Note para detalhes no que pela proteção da porta está disponível em cada placa de linha. Cada porta nesta placa de linha apoia duas filas RX e três filas TX. Uma fila RX e uma fila cada um TX são denotadas como uma fila de prioridade absoluta. Ela age como uma fila de latência baixa, que é ideal para tráfego sensível à latência, como o tráfego de Voz sobre IP (VoIP).

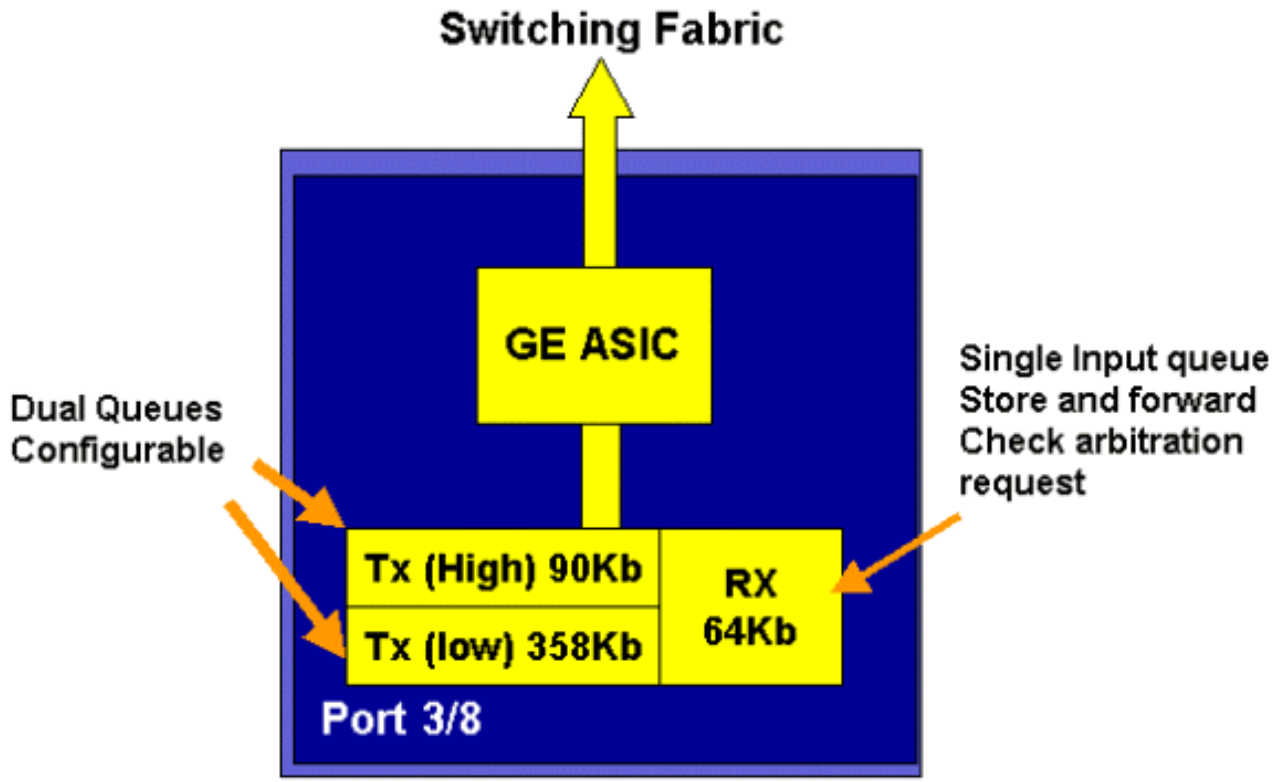


Placas de linha GE (WS-X6408A, WS-X6516, WS-X6816)

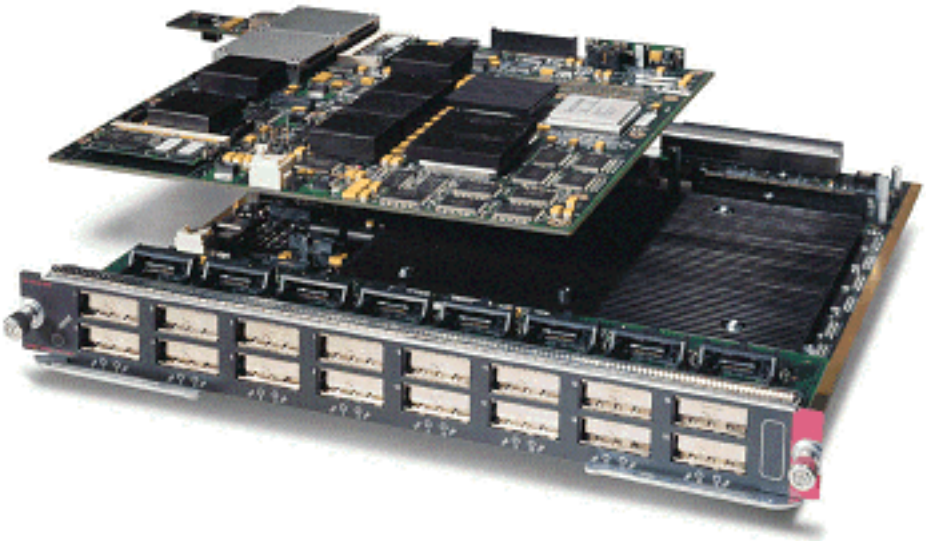
Para placas de linha GE, o ASIC fornece 512 K por da proteção da porta. Uma representação da placa de linha do oito portas GE é mostrada no diagrama abaixo.



Como com as portas de 10/100, cada porta GE tem três filas, um RX e duas filas TX. Este é o padrão da placa de linha WS-X6408-GBIC, e está mostrado no diagrama abaixo.



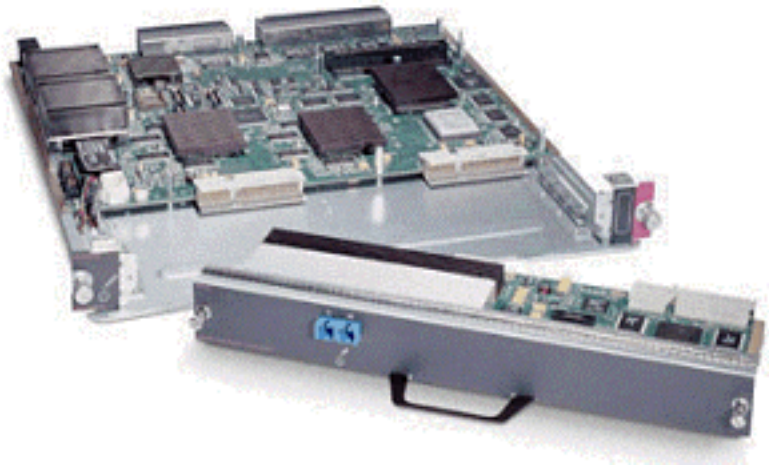
Nas placas GE de 16 portas mais recentes, nas portas GBIC em SupIA e SupII e na placa GE de 8 portas WS-X6408A-GBIC, são fornecidas duas filas extras de prioridade máxima (SP). Uma das filas SP é atribuída como uma fila Rx e a outra, como uma fila TX. Esta fila SP é usada primeiramente para o tráfego sensível de enfileiramento da latência tal como a Voz. Com a fila SP, qualquer dado colocado nessa fila será processado antes do dado nas filhas alta e baixas. Somente quando a fila SP é vontade vazia as filas do alto e baixo esteja prestado serviços de manutenção.



Placas de linha 10 GE (WS-X6502-10GE)

Na última metade 2001, Cisco introduziu um grupo de placas de linha 10 GE que fornecem uma porta de 10 GE pela placa de linha. Este módulo toma um entalhe dos 6000 chassis. A placa de linha 10 GE apoia QoS. Para a porta 10 GE, fornece duas filas RX e três filas TX. Uma fila RX e uma fila cada um TX são designadas como uma fila SP. A proteção é fornecida igualmente para a

porta, fornecendo um total de 256 K da colocação em buffer RX e de 64 MB da colocação em buffer TX. Esta porta implementa uma estrutura de fila de 1p1q8t para o lado Rx e uma estrutura de fila de 1p2q1t para o lado TX. As estruturas de fila são detalhadas adiante neste documento.



Sumário do QoS Hardware do Catalyst 6000 Family

Os componentes de hardware que executam o QoS acima funcionam no Catalyst 6000 Family são detalhados na tabela abaixo.

QoS Process	Catalyst 6500 Component that performs function
Input Scheduling	Performed by port ASIC's L2 only with or without the PFC
Classification	Performed by Supervisor or PFC L2 only is done by Supervisor L2/3 is done by PFC
Policing	Done by PFC via L3 forwarding Engine
Packet Re-write	Done by port ASIC's L2/L3 based on classification done in point 2 above
Output Scheduling	Done by port ASIC's L2/L3 based on classification done in point 2 above

Suporte para QoS ao software da família Catalyst 6000

O Catalyst 6000 Family apoia dois sistemas operacionais. A plataforma do software original, CatOS, derivou-se da base de código usada na plataforma do Catalyst 5000. Mais recentemente, Cisco introduziu o ® do Cisco IOS integrado (modo nativo) (conhecido previamente como o Native IOS), que usa uma base de código derivada do roteador Cisco IO. Ambas as plataformas de OS (Cactos e Cisco IOS integrado (modo nativo)) execute o suporte de software para permitir QoS na plataforma familiar do Catalyst 6000 Switch usando o hardware descrito nas seções anterior.

Note: Este documento utiliza exemplos de configuração de ambas as plataformas de SO.

Mecanismos de prioridade em IP e Ethernet

Para que alguns serviços de QoS sejam aplicados aos dados, deve haver uma maneira de etiquetar ou dar a prioridade a um pacote IP ou a um frame da Ethernet. O ToS e os campos de CoS são usados para conseguir este.

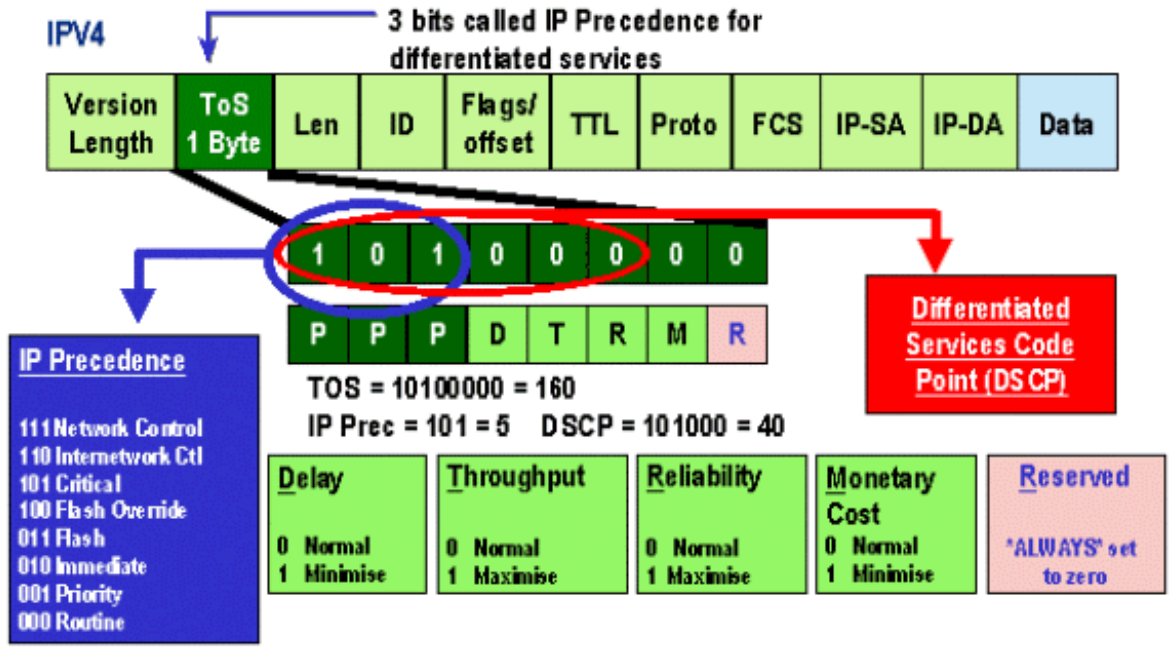
ToS

O ToS é um campo do byte que exista em um encabeçamento IPV4. O campo ToS consiste em oito bits, dos quais os três primeiros são utilizados para indicar a prioridade do pacote IP. Esses três primeiros bits são mencionados como os bits de precedência de IP. Estes bit podem ser ajustados zero a sete, com o zero que são a mais baixa prioridade e os sete que são a prioridade mais alta. O suporte está disponível para definir a presença IP no IOS por vários anos. O suporte a reinicialização de precedência do IP pode ser proporcionado pelo MSFC ou pelo PFC (independente do MSFC). Uma configuração confiável do não-confiável pode igualmente limpar para fora todas as configurações de precedência IP em um frame de entrada.

Os valores que podem ser definidos para precedência de IP são os seguintes:

IP Precedence bits	IP Precedence Value
000	Routine
001	Priority
010	Intermediate
011	Flash
100	Flash Override
101	Critical
110	Internetwork Control
111	Network Control

O diagrama abaixo representa os bits de precedência do IP no cabeçalho de ToS. Os três Bits mais significativos (MSB) são interpretados como bits de precedência de IP.



Mais recentemente, o uso do campo ToS foi expandido para abranger os seis MSB, referidos

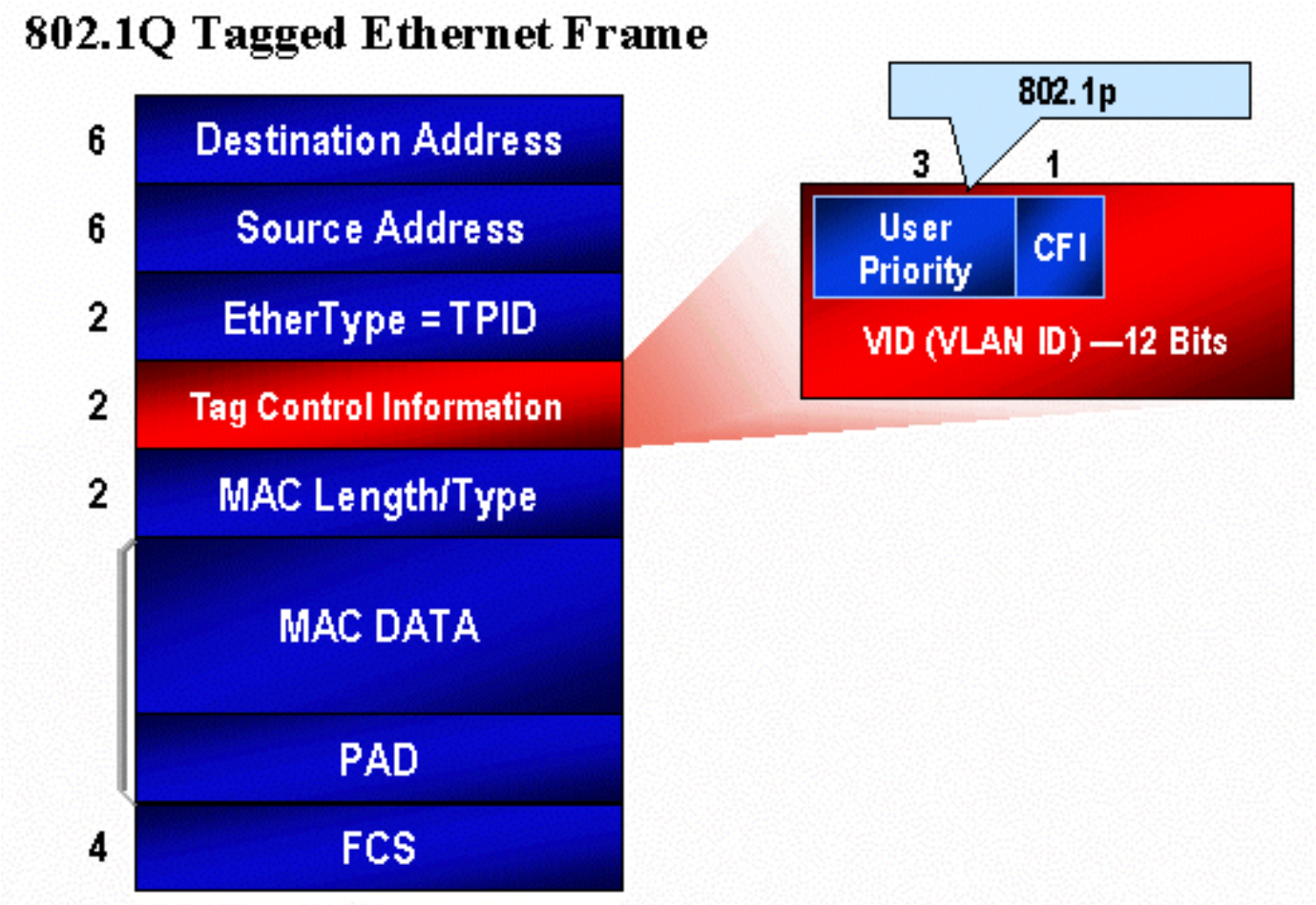
como o DSCP. O DSCP conduz a 64 valores de prioridade (dois à potência de seis) que podem ser atribuídos ao pacote IP.

A família Catalyst 6000 pode manipular o ToS. Isso pode ser alcançado por meio do PFC e do MSFC. Quando um quadro entra o interruptor, ele estará atribuído um valor DSCP. Este valor DSCP é usado internamente no interruptor para atribuir os níveis do serviço (políticas de QoS) definidos pelo administrador. O DSCP pode já existir em um quadro e ser utilizado ou o DSCP pode ser derivado de um CoS existente, precedência de IP ou DSCP no quadro (a porta deve ser confiável). Um mapa é usado internamente no interruptor para derivar o DSCP. Com oito valores possíveis de precedência de CoS/IP e 64 valores possíveis de DSCP, o mapa padrão irá mapear CoS/IPPrec 0 para DSCP 0, CoS/IPPrec 1 para DSCP 7, CoS/IPPrec 2 para DSCP 15 e assim por diante. Estes mapeamentos padrão podem ser cancelados pelo administrador. Quando o quadro estiver programado para uma porta de saída, o CoS pode ser regravado e o valor de DSCP é usado para derivar o novo CoS.

CoS

CoS refere três bit em um cabeçalho de ISL ou em um encabeçamento do 802.1Q que estão usados para indicar a prioridade do frame da Ethernet enquanto passa através de uma rede comutada. Para fins deste documento, nós referimos somente o uso do encabeçamento do 802.1Q. Os bits CoS do cabeçalho 802.1Q são comumente chamados de bits do 802.1p. Não surpreendentemente, há três bit de CoS, que combina o número de bit usados para a Precedência IP. Em muitas redes, para manter o End to End de QoS, um pacote pode atravessar os domínios L2 e L3. Para manter o QoC, ToS pode ser mapeado para CoS e vice-versa.

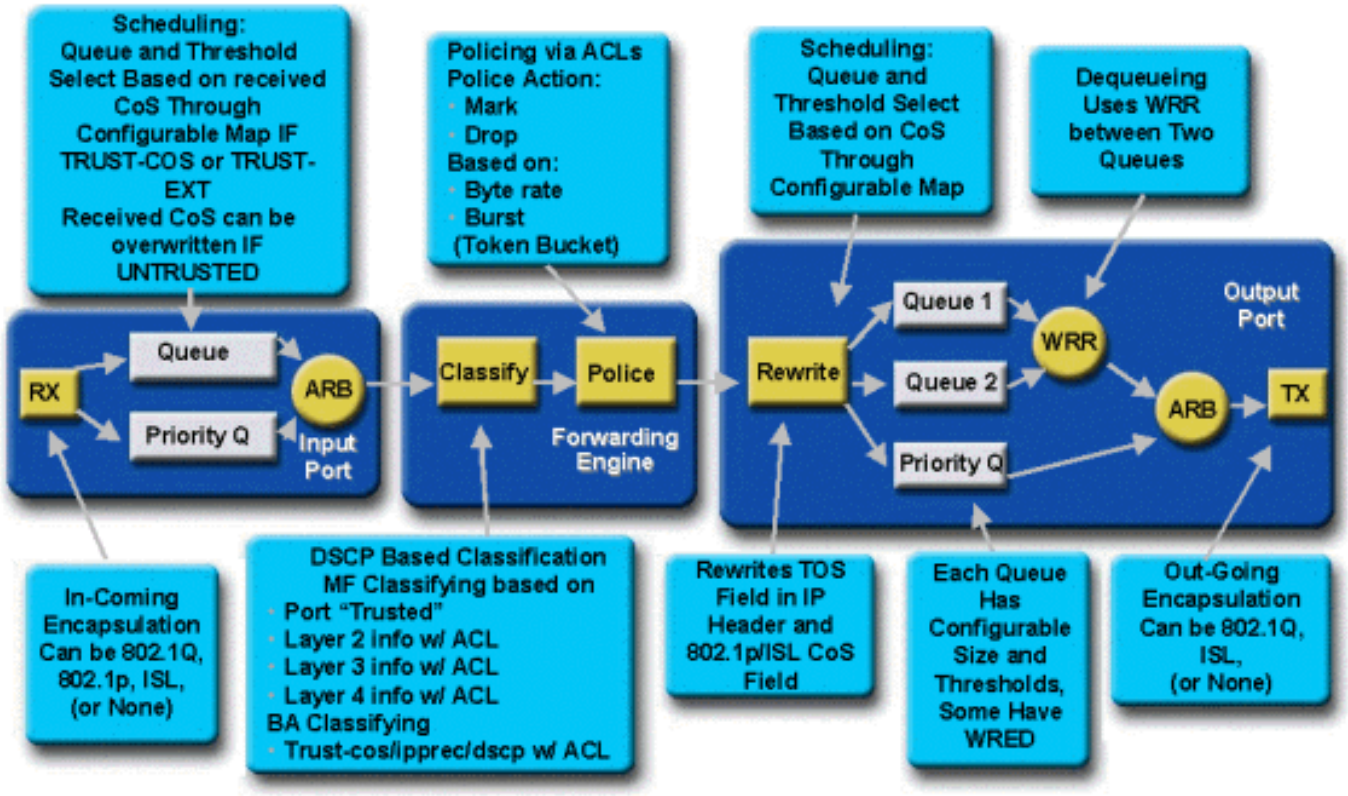
O diagrama abaixo é uma estrutura de Ethernet rotulada com um campo 802.1Q, que consiste em um Ethertipo de dois bytes e de um rótulo de dois bytes. Dentro da etiqueta de dois-byte são os bit da prioridade de usuário (conhecidos como 802.1p).



Fluxo de QoS no Catalyst 6000 Family

QoS no Catalyst 6000 Family é a maioria de implementação abrangente de QoS em todo o Switches atual do Cisco catalyst. As seguintes seções descrevem como os vários processos de QoS são aplicados a um quadro como ele transitam pelo interruptor.

Mais cedo neste documento, notou-se que há um número de elementos de QoS que muito o Switches L2 e L3 pode oferecer. Esses elementos são: classificação, programação da fila de entrada, política, regravação e programação da fila de saída. A diferença em relação à família Catalyst 6000 é que esses elementos de QoS são aplicados por um mecanismo da L2 que tem um insight nos detalhes da L3 e da L4 e também informações de cabeçalho da L2. o diagrama a seguir resume como a família Catalyst 6000 implementa estes elementos.



Um quadro incorpora o interruptor e é processado inicialmente pela porta ASIC que recebeu o quadro. Colocará o quadro em uma fila RX. Segundo a placa de linha do Catalyst 6000 Family, haverá uma ou dois filas RX.

A porta ASIC usará os bits CoS como indicador da fila que deverá receber o quadro (se várias filas de entrada existirem). Se a porta é classificada como o não-confiável, a porta ASIC pode overwrite os bit existentes de CoS baseados em um valor pré-definido.

O quadro é então passado ao mecanismo de encaminhamento L2/L3 (PFC), que o classificará e opcionalmente o vigiará (limite de taxa). A classificação é o processo de atribuir ao quadro um valor DSCP, que seja usado internamente pelo interruptor processando o quadro. O DSCP será derivado de um do seguinte:

1. Um conjunto de valores existente DSCP antes do quadro que incorpora o interruptor
2. Bits de precedência do IP já definidos no cabeçalho IPV4. Porque há 64 valores DSCP e somente oito valores de precedência IP, o administrador configurará um mapeamento que seja usado pelo interruptor para derivar o DSCP. Os mapeamentos padrão são no lugar se o administrador não configurar os mapas.
3. Os bit recebidos de CoS já ajustados antes do quadro que incorpora o interruptor. Assim como ocorre com a precedência IP, existe um máximo de oito valores CoS, sendo que cada um deve ser mapeado para um dos valores 64 DSCP. Este mapa pode ser configurado ou o interruptor pode usar o mapa padrão no lugar.
4. Defina para o quadro utilizando um valor padrão de DSCP, normalmente atribuído por uma entrada de Lista de controle de acesso (ACL).

Depois que um valor DSCP é atribuído ao quadro, o policiamento (taxa que limita) é aplicado, se uma configuração de vigilância existir. A vigilância limitará o fluxo de dados através do PFC, descartando ou diminuindo o tráfego que estiver fora de perfil. Fora de perfil é um termo usado para indicar que o tráfego excedeu um limite definido pelo administrador como a quantidade de bit por segundo que o PFC enviará. O tráfego fora de perfil pode ser reduzido ou o valor de CoS

pode ser marcado. No momento, PFC1 e PFC2 não oferecem suporte à vigilância de entrada (taxa limite). O suporte para policiamento de entrada e de saída estará disponível com a versão de um novo PFC.

O PFC passará então o quadro à porta de saída para processar. Neste momento, um processo da reescrita é invocado para alterar os valores de CoS no quadro e o valor ToS no encabeçamento IPV4. Isto é derivado do DSCP interno. O frame será colocado em uma fila de transmissão no valor CoS correspondente, pronto para a transmissão. Enquanto o quadro estiver na fila, a porta ASIC monitorará os buffers e implementará o WRED para evitar o excesso de buffers. Um algoritmo de escalonamento WRR é usado então para programar e transmitir quadros da porta de saída

Cada um das seções abaixo explorará este fluxo que dá com maiores detalhes exemplos de configuração para cada um das etapas descritas acima.

Filas, Buffers, Limiares e Mapeamentos

Antes que a configuração de QoS esteja descrita em detalhe, determinados termos devem ser explicados mais para assegurar-se de que você compreenda inteiramente os recursos de configuração de QoS do interruptor.

Filas

Cada porta no interruptor tem uma série de filas de entrada e de saída que são usadas como áreas de armazenamento temporário para dados. As placas de linha do Catalyst 6000 Family executam números diferentes de filas para cada porta. Geralmente, as filas são implementadas no ASICs do hardware para cada porta. Nas placas de ingresso da família Catalyst 6000 de primeira geração, a configuração típica era uma fila de entrada e duas filas de saída. Em umas placas de linha mais novas (10/100 e GE), o ASIC executa um grupo extra de duas filas (uma entra e uma output) tendo por resultado duas filas de entrada e três filas de saída. Essas duas filas extras são filas SP especiais usadas para tráfego de latência sensível como VoIP. São atendidos de maneira SP. Ou seja, se um quadro chegar na fila SP, a programação de quadros nas filas mais baixas será interrompido para processar o quadro na fila SP. A programação dos pacotes de recomeço de fila(s) inferior(es) será feita somente quando a fila de SP estiver vazia.

Quando um quadro chegar a uma porta (para entrada ou saída) em horários de congestionamento, ele será colocado em uma fila. A decisão sobre em qual fila a estrutura será colocada geralmente é feita com base no valor de CoS no cabeçalho de Ethernet da estrutura recebida.

Na saída, um algoritmo de programação será empregado para esvaziar a fila de TX (saída). WRR é a técnica utilizada para se alcançar isso. Para cada fila, uma ponderação é usada para ditar quanto dados serão esvaziados da fila antes de se mover na fila seguinte. A pesagem atribuída pelo administrador é um número de 1 a 255 e isso é atribuído a cada fila TX.

Bufferes

Cada fila é atribuída uma certa quantidade do espaço de buffer para armazenar dados de trânsito. A memória é residente no ASIC de porta e é dividida e alocada por porta. Para cada porta GE, o GE ASIC atribui 512 K do espaço de buffer. Para 10/100 das portas, a porta ASIC reserva 64 K ou 128 K (segundo a placa de linha) por da proteção da porta. Esse espaço de buffer é então dividido entre a fila Rx (de ingresso) e as filas TX (de saída).

Limiares

Um aspecto da transmissão de dados normal é que, se um pacote for descartado, ele acabará sendo retransmitido (fluxos de TCP). Na época da congestão, isto pode adicionar à carga na rede e potencialmente fazer com que os bufferes sobrecarreguem ainda mais. Como meio de assegurar-se de que os bufferes não transbordem, o Catalyst 6000 Family Switch emprega um número de técnicas para evitar este do acontecimento.

Os pontos iniciais são os níveis imaginários atribuídos pelo interruptor (ou pelo administrador) que definem os pontos da utilização em que o algoritmo do Tratamento de Congestionamento pode começar deixar cair dados da fila. Nas portas da família Catalyst 6000, há normalmente quatro limites que são associados às filas de entrada. Há geralmente dois pontos iniciais associados com as filas de saída.

Esses limiares também são distribuídos, no contexto do QoS, como um meio de atribuir quadros com diferentes prioridades para tais limiares. Enquanto o buffer começa a se encher e os pontos iniciais estão rompidos, o administrador pode traçar prioridades diferentes aos pontos iniciais diferentes que indicam ao interruptor que molda deve ser deixado cair quando um ponto inicial é excedido.

Mapeamentos

Nas filas e nas seções do ponto inicial acima, mencionou-se que o valor de CoS no frame da Ethernet está usado para determinar qual fila para colocar o quadro e em que ponto do suplemento de buffer está acima um quadro elegível ser deixado cair. Essa é a finalidade dos mapeamentos.

Quando o QoS está configurado na família Catalyst 6000, são habilitados mapeamentos padrão que definem o seguinte:

- em quais quadros de limites com valores de CoS específicos são elegíveis para serem soltos
- que fila um quadro é colocado (baseado em seu valor de CoS)

Enquanto os mapeamentos padrão existirem, eles poderão ser substituídos pelo administrador. O mapeamento existe para o seguinte:

- Valores de CoS em um frame de entrada a um valor DSCP
- Valores de precedência IP em um frame de entrada a um valor DSCP
- Valores DSCP a um valor de CoS para um frame enviado
- Valores de CoS aos limiares de queda em filas de recepção
- Valores de CoS aos limiares de queda em transmitir fila
- Valores do mapa de DSCP para os quadros que excedem o policiamento de indicações
- Valores de CoS a um quadro com um endereço MAC de destino específico

WRED e WRR

WRED e WRR são dois algoritmos extremamente potentes que fazem parte da família Catalyst 6000. o WRED e o WRR usam o caractere de prioridade (CoS) dentro de um frame da Ethernet para fornecer o gerenciamento de buffer e a programação externa aumentados. B

WRED

O WRED é um algoritmo do gerenciamento de buffer empregado pelo Catalyst 6000 Family para minimizar o impacto do tráfego de alta prioridade deixando cair na época da congestão. O WRED é baseado no algoritmo vermelho.

A fim compreender o VERMELHO e o WRED, revisite o conceito do Gerenciamento do fluxo de TCP. O gerenciamento de fluxo assegura-se de que o remetente de TCP não oprima a rede. O algoritmo de inicio lento TCP é parte da solução para lidar com isso. Dita que quando um fluxo começa, um pacote único está enviado antes que espere um reconhecimento. Dois pacotes são enviados antes de um ACK ser recebido, aumentando gradualmente o número de pacotes enviados antes do ACK (reconhecimento) ser recebido. Isto continuará até que o fluxo alcance um nível de transmissão (isto é, envia o número *x de* pacotes) que a rede possa segurar sem a carga que incorre a congestão. Se a congestão ocorre, o algoritmo slowstart estrangulará suporta o tamanho de janela (isto é, o número dos pacotes enviados antes de esperar um reconhecimento), assim reduzindo o desempenho geral para essa sessão de TCP (fluxo).

O RED monitorará uma fila assim que ela começar a ser preenchida. Uma vez que um determinado ponto inicial foi excedido, os pacotes começarão ser deixados cair aleatoriamente. Nenhuma consideração é dada aos fluxos específicos; um pouco, os pacotes aleatórios serão deixados cair. Esses pacotes podem ser de fluxos de prioridade alta ou baixa. Os pacotes descartado podem ser parte de um fluxo único ou uns fluxos de TCP múltiplos. Se os fluxos múltiplos são impactados, como descrito acima, este pode ter um impacto considerável em cada um flui tamanho de janela.

Diferente do RED, o WRED não é aleatório ao eliminar quadros. O WRED leva em consideração a prioridade das estruturas (no caso da família Catalyst 6000, ele usa o valor CoS). Com WRED, o administrador atribui quadros com certos valores de CoS a limites específicos. Quando esses limiares forem excedidos, os quadros com valores de CoS que estiverem mapeados para esses limiares estarão elegíveis para desconexão. Outros quadros com valores de CoS atribuídos aos thresholds mais altos são mantidos na fila. Este processo permite uns fluxos mais prioritários ser mantido intactos mantendo seus tamanhos de janela maiores intactos e minimizando a latência envolvida em obter os pacotes do remetente ao receptor.

Como você sabe se sua placa de linha apoia o WRED? Emita o comando seguinte. Na saída, verificação para a seção que indica o apoio para o WRED nessa porta.

```
Console> show qos info config 2/1
QoS setting in NVRAM:
QoS is enabled
Port 2/1 has 2 transmit queue with 2 drop thresholds (2q2t).
Port 2/1 has 1 receive queue with 4 drop thresholds (1q4t).
Interface type:vlan-based
ACL attached:
The qos trust type is set to untrusted.
Default CoS = 0
Queue and Threshold Mapping:
Queue Threshold CoS
----- --------- ---------------
1     1         0 1
1     2         2 3
2     1         4 5
2     2         6 7
Rx drop thresholds:
```

```
Rx drop thresholds are disabled for untrusted ports.
Queue #  Thresholds - percentage (abs values)
-------  ---------------------------------------
1        50% 60% 80% 100%
TX drop thresholds:
Queue #  Thresholds - percentage (abs values)
-------  ---------------------------------------
1        40% 100%
2        40% 100%
TX WRED thresholds:
WRED feature is not supported for this port_type.
!-- Look for this. Queue Sizes: Queue # Sizes - percentage (abs values) ------- ----------------
--------------------- 1 80% 2 20% WRR Configuration of ports with speed 1000MBPS: Queue # Ratios
(abs values) ------- ----------------------------------- 1 100 2 255 Console> (enable)
```

Caso o WRED não estiver disponível em uma porta, a porta usará um método da queda traseira do gerenciamento de buffer. A queda traseira, como o nome indica, simplesmente descarta os quadros recebidos quando os buffers forem completamente utilizados.

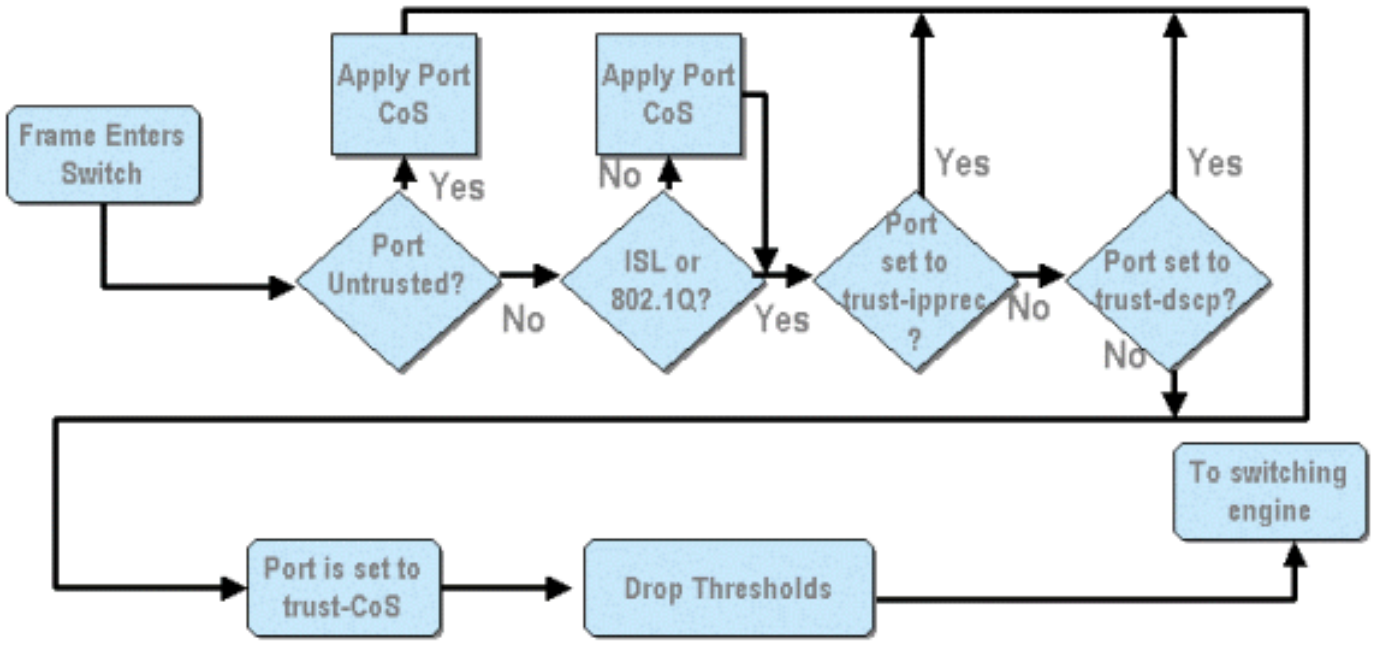
WRR

O WRR é usado para programar o tráfego de saída das filas TX. Um algoritmo redondo de Robin normal alternará entre as filas TX que enviam um número igual de pacotes de cada fila antes de mover-se para a fila seguinte. O aspecto ponderado do WRR permite que o algoritmo de programação inspecione um peso que foi atribuído à fila. Isso permite acesso definido a filas para uma parte maior da largura de banda. O algoritmo de escalonamento WRR esvaziará para fora mais dados das filas identificadas do que outras filas, assim fornecendo uma polarização para filas designadas.

A configuração para o WRR e os outros aspectos do que foram descritas acima são explicados nas seguintes seções.

Configurando o QoS com base na porta ASIC no Catalyst 6000 Family

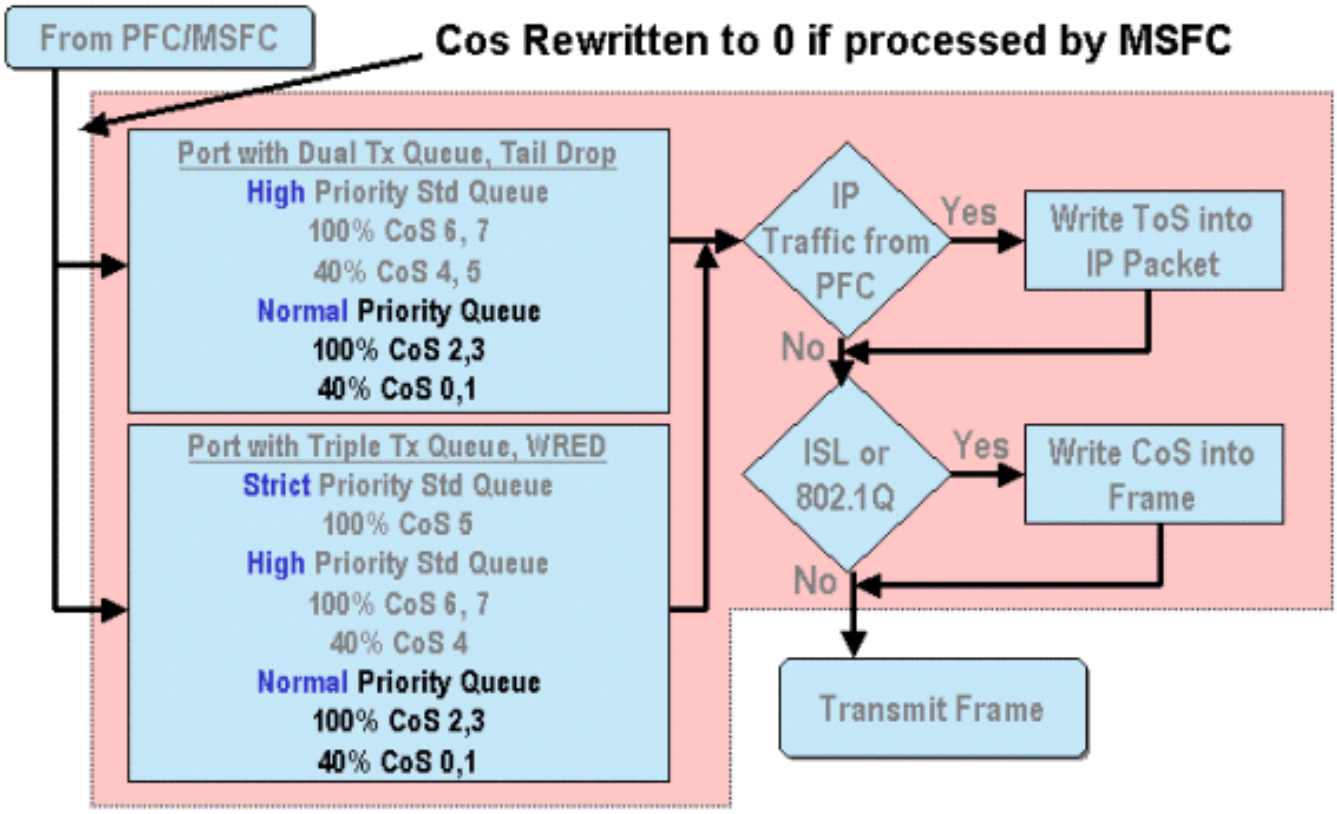
A configuração de QoS instrui a porta ASIC ou o PFC para executar uma ação QoS. As seções a seguir examinarão a configuração de QoS para estes dois processos. Na porta ASIC, a configuração QoS afeta os fluxos de tráfego de entrada e saída.



Do diagrama acima, pode-se ver que os seguintes processos da configuração de QoS se aplicam:

1. estados confiáveis de portas

2. aplicação de CoS baseado em porta
3. Atribuição de limiar de queda de recebimento
4 CoS aos mapas do limiar de queda RX



Quando um quadro é processado por MSFC ou PFC, é passado para a porta de saída ASIC para posterior processamento. Todos os quadros processados pelo MSFC terão seus valores de CoS restaurados a zero. Isso deve ser levado em consideração para o processamento de QoS nas portas externas.

O diagrama acima mostra o processamento de QoS executado pela porta ASIC para o tráfego de saída. Alguns dos processos acionados no processamento de saída QoS incluem o seguinte:

1. Atribuições de queda traseira de TX e limiar de WRED
2. CoS à queda traseira TX e aos mapas WRED

Também, não mostrado no diagrama acima, é o processo de atribuir novamente o CoS ao frame externo usando um DSCP ao mapa COS.

As seguintes seções examinam os recursos de configuração de QoS dos ASIC baseados porta com maiores detalhes.

Note: Um ponto importante a fazer é que quando os comandos qos são invocados usando Cactos, se aplicam tipicamente a todas as portas com o tipo de fila especificado. Por exemplo, se um limiar de queda WRED é aplicado às portas com tipo de fila 1p2q2t, este limiar de queda WRED é aplicado a todas as portas em todas as placas de linha que apoiam este tipo de fila. Com o Cat IOS, os comandos do QoS são geralmente aplicados no nível da interface.

Habilitando o QoS

Antes que toda a configuração de QoS possa ocorrer no Catalyst 6000 Family, QoS deve primeiramente ser permitido no interruptor. Para fazer isso, emita o seguinte comando:

CatOS

```
Console> (enable) set qos enable
!-- QoS is enabled. Console> (enable)
```

Cisco IOS integrado (modo nativo)

```
Cat6500(config)# mls qos
```

Quando QoS é permitido no Catalyst 6000 Family, o interruptor ajustará uma série de padrões de QoS para o interruptor. Estes padrões incluem os seguintes ajustes:

QoS Feature	Default setting
Trust state of each port	Un-trusted
Receive Queue drop threshold percentages	Threshold 1 – 50% Threshold 2 – 60% Threshold 3 – 80% Threshold 4 – 100%
Transmit Queue drop threshold percentages	Low priority queue threshold 1 – 80% Low priority queue threshold 2 – 100% High priority queue threshold 1 – 80% High priority queue threshold 2 – 100%
CoS value to Drop threshold mapping	Receive queue 1/drop threshold 1: CoS 0 and 1 Transmit queue 1/drop threshold 1: CoS 0 and 1 Receive queue 1/drop threshold 2: CoS 2 and 3 Transmit queue 1/drop threshold 2: CoS 2 and 3 Receive queue 1/drop threshold 3: CoS 4 and 5 Transmit queue 2/drop threshold 1: CoS 4 and 5 Receive queue 1/drop threshold 4: CoS 6 and 7
	Transmit queue 2/drop threshold 2: CoS 6 and 7
CoS to DSCP Mapping (DSCP set from CoS value)	CoS 0 = DSCP 0 CoS 1 = DSCP 8 CoS 2 = DSCP 16 CoS 3 = DSCP 24 CoS 4 = DSCP 32 CoS 5 = DSCP 40 CoS 6 = DSCP 48 CoS 7 = DSCP 56
IP Precedence to DSCP Map (DSCP set from IP Precedence value)	IP precedence 0 = DSCP 0 IP precedence 1 = DSCP 8 IP precedence 2 = DSCP 16 IP precedence 3 = DSCP 24 IP precedence 4 = DSCP 32 IP precedence 5 = DSCP 40 IP precedence 6 = DSCP 48 IP precedence 7 = DSCP 56
DSCP to CoS map (CoS set from DSCP values)	DSCP 0-7 = CoS 0 DSCP 8-15 = CoS 1 DSCP 16-23 = CoS 2 DSCP 24-31 = CoS 3 DSCP 32-39 = CoS 4 DSCP 40-47 = CoS 5 DSCP 48-55 = CoS 6 DSCP 56-63 = CoS 7

Portas confiáveis e não confiáveis

Toda a porta dada no Catalyst 6000 Family pode ser configurada como confiado ou UN-confiado o estado de confiança das ordens da porta como marca, classifica, e programa o quadro como ele transita pelo interruptor. À revelia, todas as portas estão no estado não-confiável.

Portas Não-Confiáveis (Configuração Padrão de Portas)

Caso a porta seja configurada como não confiável, um quadro, depois de entrar inicialmente na porta, terá seus valores CoS e ToS zerados pela porta ASIC. Isto significa que o quadro estará dado o mais baixo serviço de prioridade em seu trajeto através do interruptor.

Alternativamente, o administrador pode restaurar o valor de CoS de todo o frame da Ethernet que entrar em uma porta não-confiável a um valor predeterminado. Configurando isto será discutido em uma seção mais recente.

Ajustar a porta como o não-confiável instruirá o interruptor para não executar nenhuma fuga de congestionamento. A fuga de congestionamento é o método usado para deixar cair os quadros baseados em seus valores de CoS uma vez que excedem os pontos iniciais definidos para essa fila. Todos os quadros que entram nesta porta serão ingualmente elegíveis ser deixado cair uma vez que os bufferes alcançam 100 por cento.

Em Cactos, um 10/100 ou a porta GE podem ser configurados como o não-confiável emitindo o comando seguinte:

CatOS

```
Console> (enable) set port qos 3/16 trust untrusted
!-- Port 3/16 qos set to untrusted. Console> (enable)
```

Esse comando configura a porta 16 do módulo 3 como não confiável.

Note: Para o Cisco IOS integrado (modo nativo), o software atualmente apoia somente a confiança do ajuste para portas GE.

Cisco IOS integrado (modo nativo)

```
Cat6500(config)# interface gigabitethernet 1/1
Cat6500(config-if)# no mls qos trust
```

No exemplo acima, nós incorporamos a configuração da interface e não aplicamos **nenhum** formulário do comando ajustar a porta como o não-confiável desde que é IO.

Portas Confiáveis

Às vezes, os frames da Ethernet que incorporam um interruptor terão um ajuste de CoS ou ToS que o administrador quer o interruptor manter enquanto o quadro transita pelo interruptor. Para este tráfego, o administrador pode ajustar o estado de confiança de uma porta onde esse tráfego entra o interruptor como confiado.

Como mencionado mais cedo, o interruptor usa um valor DSCP internamente para atribuir um nível predeterminado do serviço a esse quadro. Porque um quadro entra em uma porta confiável, o administrador pode configurar a porta para olhar o CoS existente, a Precedência IP, ou o valor DSCP para ajustar o valor DSCP interno. Alternativamente, o administrador pode ajustar um DSCP predefinido a cada pacote que entra na porta.

A configuração do estado de confiança de uma porta como confiável pode ser alcançada emitindo o seguinte comando:

CatOS

```
Console> (enable) set port qos 3/16 trust trust-cos
!-- Port 3/16 qos set to trust-COs Console> (enable)
```

Esse comando é aplicável na placa WS-X6548-RJ45 e define o estado de confiança da porta 3/16 como confiável. O interruptor usará o conjunto de valores de CoS no frame de entrada para ajustar o DSCP interno. O DSCP é derivado do um ou outro um mapa padrão que seja criado quando QoS foi permitido no interruptor, ou alternativamente de um mapa definido pelo administrador. No lugar das palavras-chave Trust-CoS, o administrador pode igualmente usar o Trust-dscp ou as palavras-chave trust-ipprec.

Em placas de ingresso 10/100 anteriores (WS-X6348-RJ45 e WS-X6248-RJ45), a confiança de portas precisa ser definida emitindo o comando set qos acl. Neste comando, um estado de confiança pode ser atribuído por um parâmetro secundário do **comando set qos acl**. A configuração de trust CoS não é suportada para portas dessas placas de linha, conforme descrito abaixo.

```
Console> (enable) set port qos 4/1 trust trust-COs
Trust type trust-COs not supported on this port.
!-- Trust-COs not supported, use acl instead. Rx thresholds are enabled on port 4/1. !-- Need to
turn on input queue scheduling. Port 4/1 qos set to untrusted. !-- Trust-COs not supported, so
port is set to untrusted.
```

O comando acima indica que se exige para permitir a programação da fila de entrada. Portanto, para portas 10/100 em placas de linha WS-X6248-RJ45 e WS-X6348-RJ45, o comando set port qos x/y trust trust-COs deve estar ainda configurado, apesar de que o ALC deve ser utilizado para configurar estados de confiança.

Com Cisco IOS integrado (modo nativo), o ajuste da confiança pode ser executado em uma relação GE e em 10/100 das portas na placa de linha WS-X6548-RJ45 nova.

Cisco IOS integrado (modo nativo)

```
Cat6500(config)# interface gigabitethernet 5/4
Cat6500(config-if)# mls qos trust ip-precedence
Cat6500(config-if)#
```

Este exemplo configura o estado de confiança da porta GE 5/4 como confiável. O valor de precedência de IP do quadro será usado para derivar o valor do DSCP.

Classificação de entrada e COS baseada em porta de configuração

No ingresso a uma porta de switch, um frame da Ethernet pode ter seu CoS mudado se encontra um dos seguintes dois critérios:

1. a porta está configurada como não confiável, ou
2. a estrutura de Ethernet não tem um valor COS existente já configurado.

Se você deseja reconfigurar o CoS de um ethernet frame entrante, você deve emitir o comando

seguinte:

CatOS

```
Console> (enable) set port qos 3/16 cos 3
!-- Port 3/16 qos set to 3. Console> (enable)
```

Esse comando configura os COs de quadros Ethernet de entrada na porta 16 do módulo 3 para um valor de 3 quando um quadro não marcado chega ou quando a porta está configurada como não confiável.

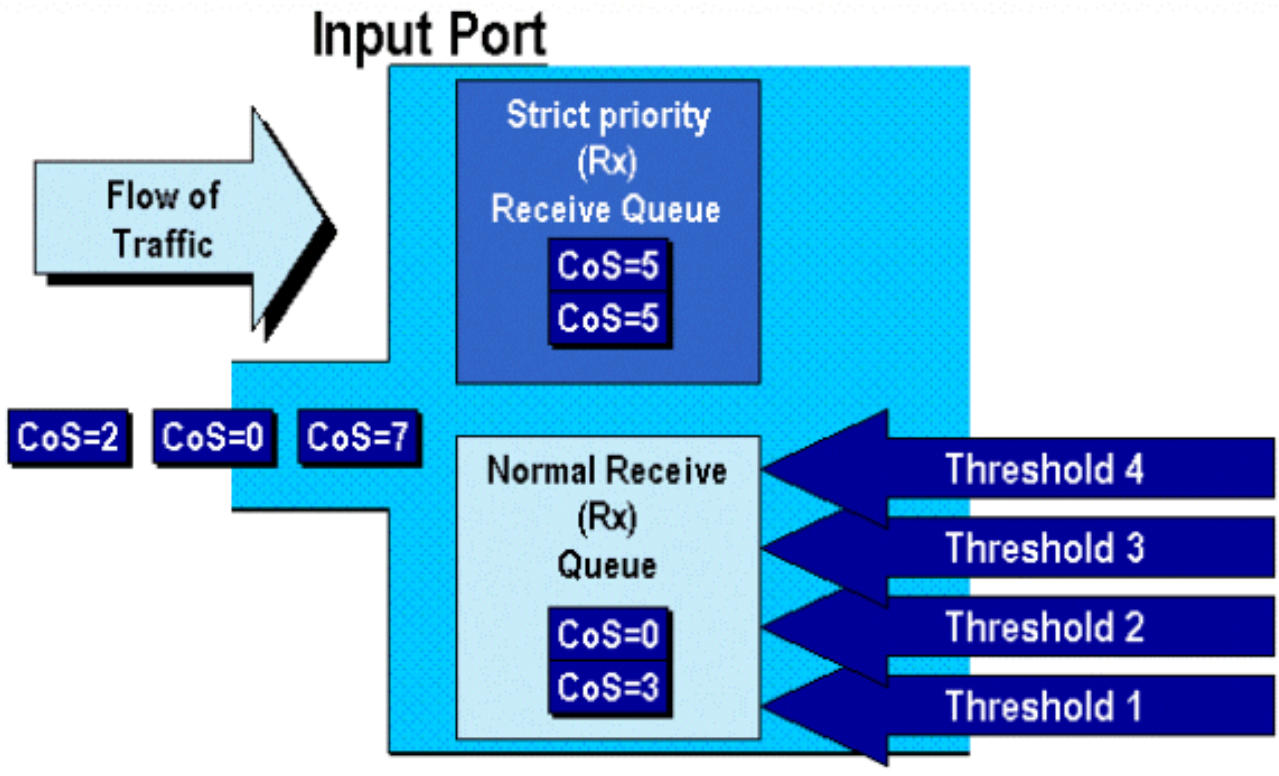
Cisco IOS integrado (modo nativo)

```
Cat6500(config)# interface fastethernet 5/13
Cat6500(config-if)# mls qos COs 4
Cat6500(config-if)#
```

Este conjuntos de comandos os CO dos ethernet frame entrantes na porta 13 no módulo 5 a um valor de 4 quando um frame não marcado chegar ou se a porta está ajustada ao não-confiável.

Configure Rx Drop Thresholds

No ingresso à porta de switch, o quadro será colocado em uma fila RX. Para evitar o excesso de buffers, a porta ASIC implementa quatro limiares em cada fila Rx e usa esses limiares para identificar quadros que podem ser descartados uma vez que esses limiares são excedidos. O ASIC de porta irá utilizar o valor de COs de conjunto de quadros para identificar quais quadros podem ser derrubados quando um limiar é excedido. Esse recurso permite que os quadros com prioridade mais elevada permaneçam no buffer por mais tempo quando ocorre congestionamento.



Segundo as indicações do diagrama acima, os quadros chegam e são colocados na fila.

Enquanto a fila começa se encher, os pontos iniciais estão monitorados pela porta ASIC. Quando um limiar é rompido, estruturas com valores de CO identificados pelo administrador são descartadas aleatoriamente da fila. Os mapeamentos de limiar padrão para uma fila 1a4t (encontrados nas placas de ingresso WS-X6248-RJ45 e WS-X6348-RJ45) são os seguintes:

- o ponto inicial 1 é ajustado a 50% e os valores 0 e 1 CO são traçados a este ponto inicial
- o ponto inicial 2 é ajustado a 60% e os valores 2 e 3 CO são traçados a este ponto inicial
- o ponto inicial 3 é ajustado a 80% e os valores 4 e 5 CO são traçados a este ponto inicial
- o limiar 4 é definido para 100% e os valores COs 6 e 7 são mapeados para este limiar

Para (encontrado em portas GE) uma fila 1P1q4t, os mapeamentos padrão são como segue:

- o ponto inicial 1 é ajustado a 50% e os valores 0 e 1 CO são traçados a este ponto inicial
- o ponto inicial 2 é ajustado a 60% e os valores 2 e 3 CO são traçados a este ponto inicial
- o ponto inicial 3 é ajustado a 80% e os valores 4 CO são traçados a este ponto inicial
- o limiar 4 é definido para 100% e os valores COs 6 e 7 são mapeados para este limiar
- O valor CO de 5 é traçado à fila de prioridade estrita

Para um 1p1q0t (encontrado em 10/100 move na placa de linha WS-X6548-RJ45), os mapeamentos padrão são como segue:

- Os quadros com CO 5 vão à fila SP RX (fila 2), onde o interruptor deixa cair frames de entrada somente quando o buffer da fila de recepção SP tem 100 por cento completo.
- Os quadros com CO 0, 1, 2,3, 4, 6, ou 7 vão à fila do padrão RX. O interruptor deixa cair frames de entrada quando o buffer da RX-fila tem 100 por cento completo.

Esses limiares de queda podem ser alterados pelo administrador. Também, os valores do padrão CO que são traçados a cada ponto inicial podem igualmente ser mudados. As placas de linha diferentes executam aplicações diferentes da fila RX. Um sumário dos tipos de fila é mostrado abaixo.

CatOS

```
Console> (enable) set qos drop-threshold 1q4t rx queue 1 20 40 75 100
!-- Rx drop thresholds for queue 1 set at 20%, 40%, 75%, and 100%. Console> (enable)
```

Esse comando define os limites de queda de recebimento de todas as portas de entrada com uma fila e quatro limiares (significa 1q4t) para 20%, 40%, 75% e 100%.

O comando emitido no Integrated Cisco IOS (Modo Nativo) é mostrado a seguir.

Cisco IOS integrado (modo nativo)

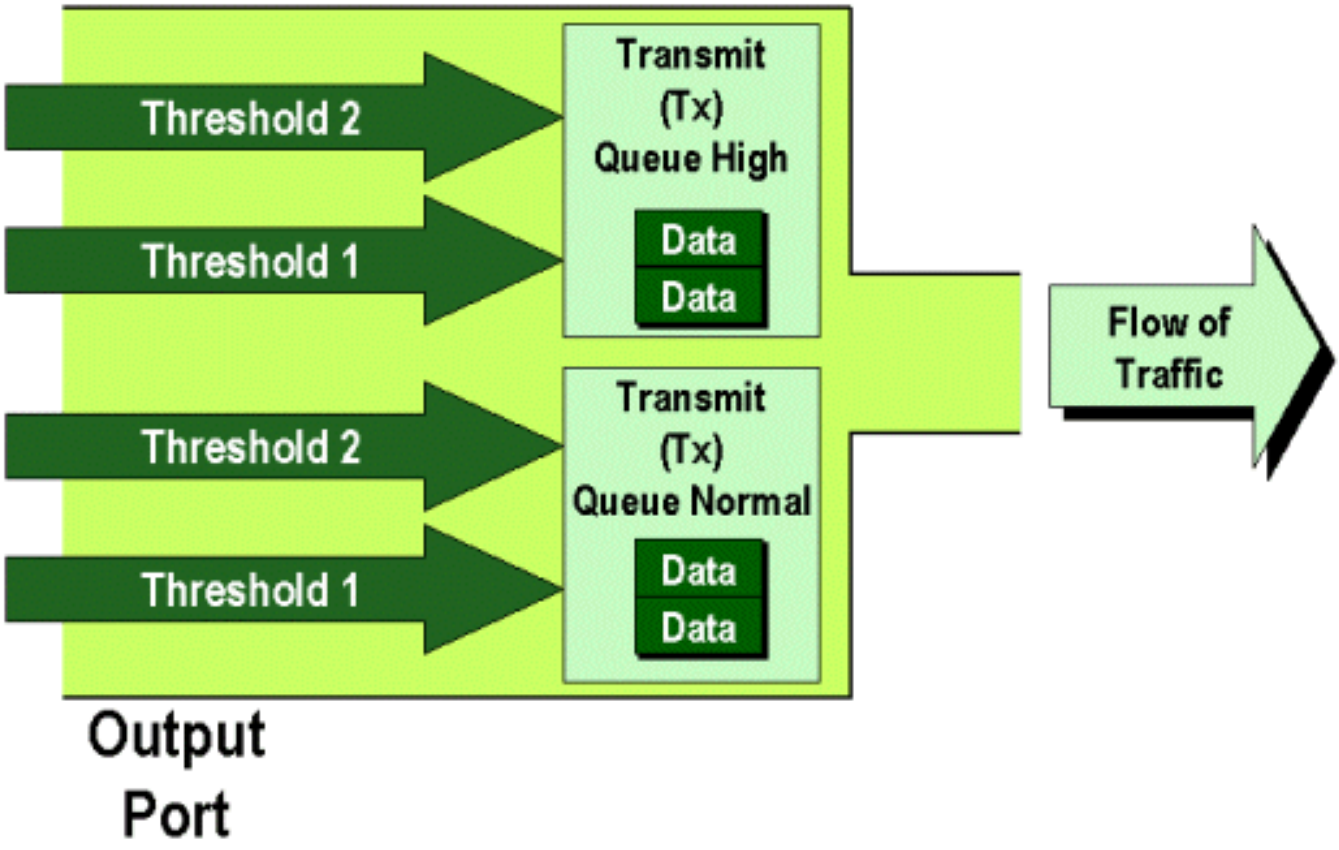
```
Cat6500(config-if)# wrr-queue threshold 1 40 50
Cat6500(config-if)# wrr-queue threshold 2 60 100

!-- Configures the 4 thresholds for a 1q4t rx queue and. Cat6500(config-if)# rcv-queue threshold
1 60 75 85 100

!-- Configures for a 1p1q4t rx queue, which applies to !-- the new WS-X6548-RJ45 10/100 line
card.
```

Os limiares de queda de Rx devem ser habilitados pelo administrador. Atualmente, o **comando set**

port qos x/y trust trust-cos deve ser usado para ativar os limiares de queda RX (onde *x* é o número de módulo e *y* é a porta nesse módulo).

Configuração de limiares TX Drop

Em uma porta de saída, essa porta terá dois limites TX usados como parte do mecanismo de evasão de congestionamento, fila 1 e fila 2. A fila 1 é representada como a fila padrão de baixa prioridade e a fila 2 é representada como a fila padrão de alta prioridade. Segundo as placas de linha usadas, empregarão uma queda traseira ou um algoritmo de gerenciamento do limite de WRED. Ambos os algoritmos empregam dois pontos iniciais para cada fila TX.



O administrador pode configurar manualmente os limiares da seguinte maneira:

CatOS

```
Console> (enable) set qos drop-threshold 2q2t TX queue 1 40 100
!-- TX drop thresholds for queue 1 set at 40% and 100%. Console> (enable)
```

Este conjuntos de comandos os limiares de queda TX para a fila 1 para todas as portas emissora com duas filas e dois pontos iniciais (denota 2q2t) a 40% e a 100%.

```
Console> (enable) set qos wred 1p2q2t TX queue 1  60 100
!-- WRED thresholds for queue 1 set at 60% 100% on all WRED-capable 1p2q2t ports. Console>
(enable)
```

Esse comando configura os limiares de queda do WRED para fila 1 para todas as portas de saída com uma fila SP, duas filas normais e dois limiares (indica 1p2q2t) para 60% e 100%. A fila 1 é definida como a fila de prioridade normal baixa e apresenta a prioridade mais baixa. A fila 2 é a fila normal prioritária e tem uma prioridade mais alta do que enfileirar 1. filas 3 é a fila SP e é

prestado serviços de manutenção antes de todas filas restantes nessa porta.

O comando equivalente emitido no Cisco IOS integrado (modo nativo) é mostrado abaixo.

Cisco IOS integrado (modo nativo)

```
Cat6500(config-if)# wrr-queue random-detect max-threshold  1 40 100
Cat6500(config-if)#
```

Isto define os limiares de queda WRED de uma porta 1p2q2t para a fila 1 em 40% do limiar 1 (TX) e 100% do limiar 2 (TX).

O WRED também poderá ser desabilitado se necessário no Cisco IOS Integrado (Modo Nativo). O método usado para fazer isto é usar formulário **n" do** comando. Um exemplo de desabilitar o WRED é mostrado como segue:

Cisco IOS integrado (modo nativo)

```
Cat6500(config-if)# no wrr-queue random-detect queue_id
```

Traçando o MAC address aos valores CO

Além do que o ajuste de CO baseados em uma definição de porta global, o interruptor permite que o administrador ajuste valores CO baseados no endereço MAC de destino e no ID de VLAN. Isto permite os quadros destinados para que os alvos específicos sejam etiquetados com um valor predeterminado CO. Esta configuração pode ser feita emitindo o comando a seguir:

CatOS

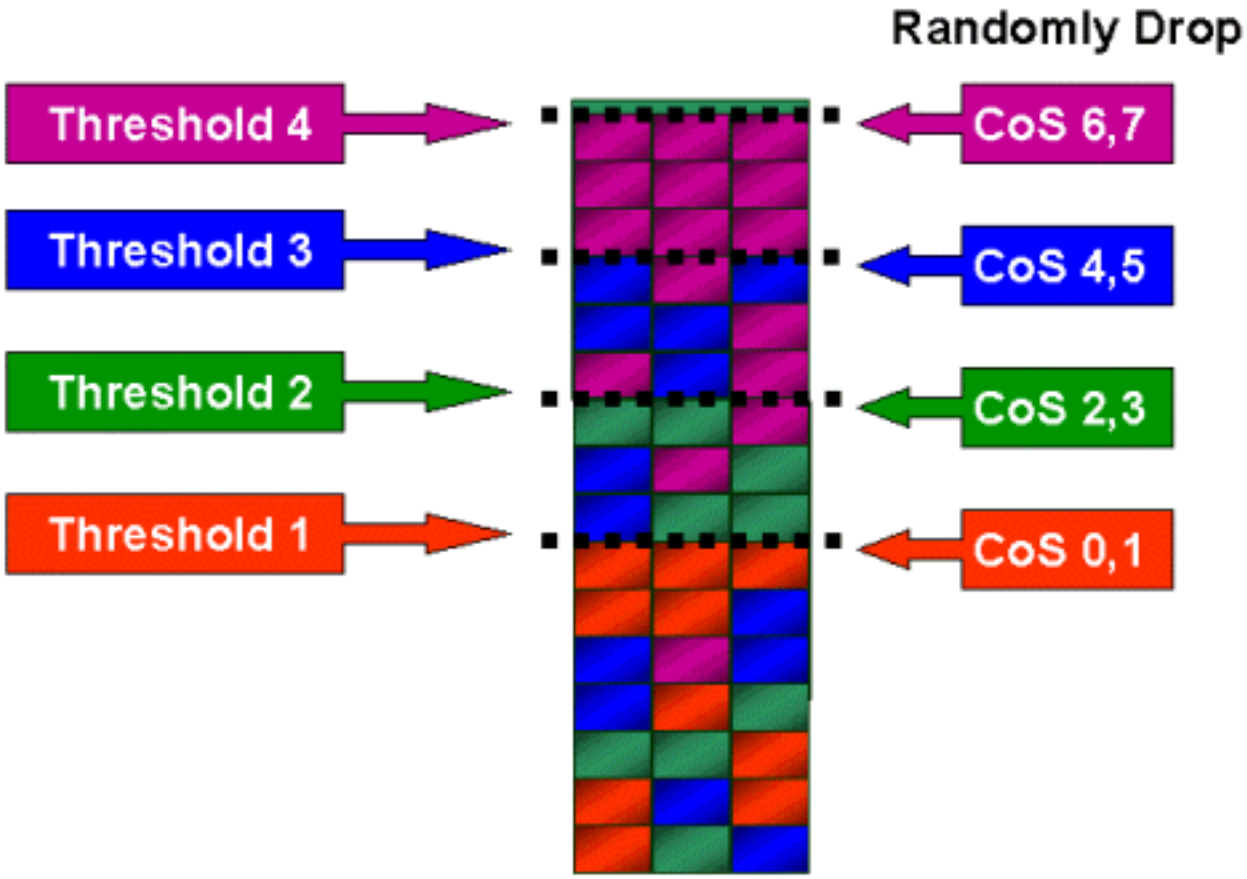
```
Console> (enable) set qos Mac-COs 00-00-0c-33-2a-4e 200 5
!-- COs 5 is assigned to 00-00-0c-33-2a-4e VLAN 200. Console> (enable)
```

Este comando configura um COs de 5 para qualquer quadro cujo endereço MAC de destino seja 00-00-0c-33-2a-4e que tenha vindo da VLAN 200.

Não há nenhum comando equivalente no Cisco IOS integrado (modo nativo). Isso ocorre porque este comando é suportado apenas quando não há uma PFC presente e o Integrated Cisco IOS (modo Nativo) requer uma PFC para funcionar.

Traçando CO aos pontos iniciais

Depois que os pontos iniciais foram configurados, o administrador pode então atribuir valores CO a estes pontos iniciais, de modo que quando o ponto inicial foi excedido, os quadros com valores CoS específicos possam ser deixados cair. Normalmente, o administrador atribuirá quadros de prioridade inferior aos limiares inferiores, mantendo assim o tráfego de prioridade superior na fila, caso ocorra congestionamento.



A figura acima mostra uma fila de entrada com quatro limiares e como os valores de COs foram atribuídos a cada limite.

A seguinte saída apresenta como os valores de COs podem ser mapeados para limiares:

CatOS

```
Console> (enable) set qos map 2q2t 1 1 COs 0 1
!-- QoS TX priority queue and threshold mapped to COs successfully. Console> (enable)
```

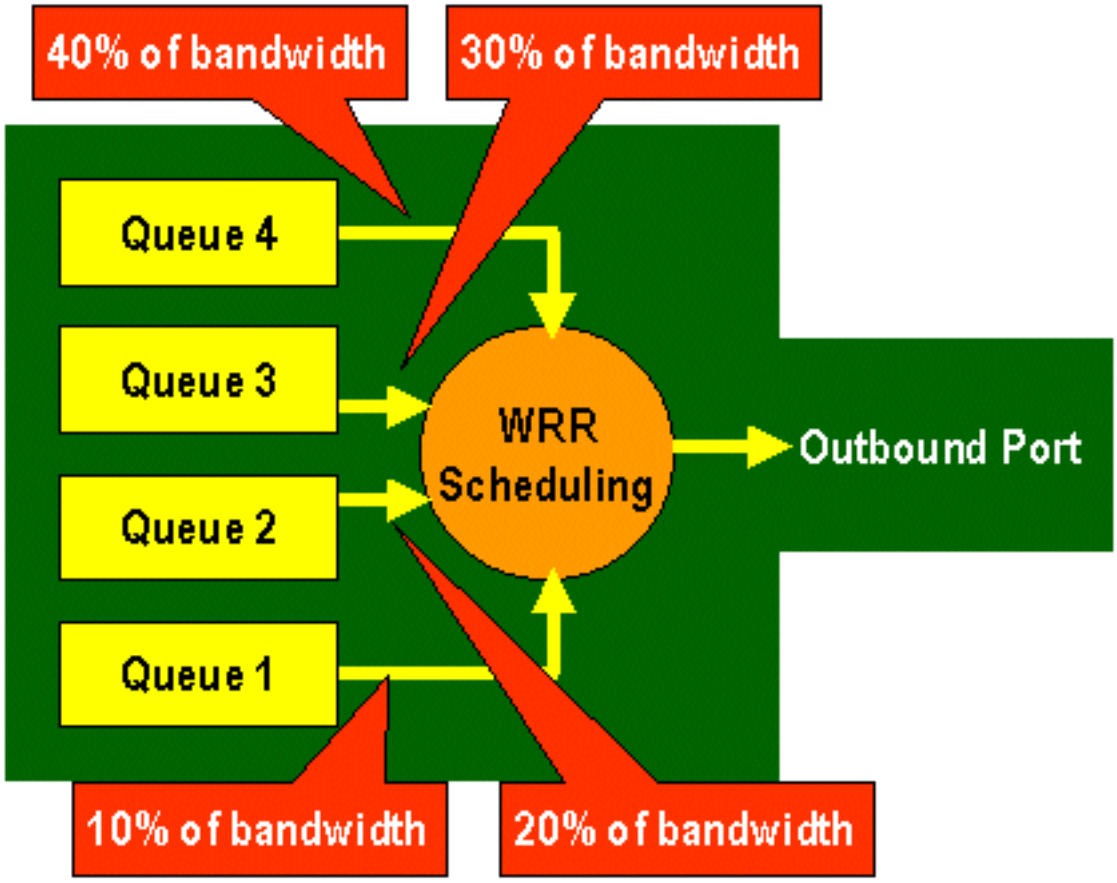
Este comando atribui valores CO de 0 e de 1 para enfileirar 1, o ponto inicial 1. O comando equivalente no Cisco IOS integrado (modo nativo) é mostrado abaixo.

Cisco IOS integrado (modo nativo)

```
Cat6500(config-if)# wrr-queue COs-map  1  1  0  1
Cat6500(config-if)#
```

Configuração da largura de banda em filas TX

Se uma estrutura for colocada em uma fila de saída, ela será transmitida com o uso de um algoritmo output-scheduling. O processo do programador de saída usa o WRR para transmitir quadros a partir das filas de saída. Segundo o hardware da placa de linha que está sendo usado, há dois, três, ou quatro transmitir fila pela porta.



Nas placas de ingresso WS-X6248 e WS-X6348 (com estruturas de fila 2q2t), duas filas TX são usadas pelo mecanismo WRR para programação. Nas placas de linha WS-X6548 (com uma estrutura da fila 1p3q1t) há quatro filas TX. Destas quatro filas TX, três filas TX são prestadas serviços de manutenção pelo algoritmo WRR (a última fila TX é uma fila SP). Em placas de linha GE, há três filas TX (que usam uma estrutura da fila 1p2q2t); uma destas filas é uma fila SP assim os serviços do algoritmo WRR somente duas filas TX.

Tipicamente, o administrador atribuirá um peso à fila TX. O WRR trabalha olhando a ponderação atribuída à fila de porta, que é usada internamente pelo interruptor para determinar quanto tráfego será transmitido antes de se mover na fila seguinte. Um valor da ponderação entre de 1 e de 255 pode ser atribuído a cada um da fila de porta.

CatOS

```
Console> (enable) set qos wrr 2q2t 40 80
!-- QoS wrr ratio set successfully. Console> (enable)
```

Este comando atribui uma ponderação de 40 para enfileirar 1 e 80 para enfileirar 2. Isto significa eficazmente umas duas a umas relações (80 40 = 2 a 1) da largura de banda atribuída entre as duas filas. Este comando tem efeito em todas as portas com duas filas e dois limiares.

O comando equivalente emitido no Cisco IOS integrado (modo nativo) é mostrado abaixo.

Cisco IOS integrado (modo nativo)

```
Cat6500(config-if)# wrr-queue bandwidth 1 3
```

```
Cat6500(config-if)#
```

Os dados acima representam uma proporção de três para um entre as duas filas. Você observará que a Versão do IOS do gato deste comando se aplica a uma relação específica somente.

DSCP ao traço CO

Depois de colocado o frame na porta de saída, a porta ASCII usará os COs atribuídos para executar fuga de congestionamento (ou seja, WRED) e também utilizará os COs para determinar a programação do frame (ou seja, a transmissão do frame). Neste momento, o interruptor usará um mapa padrão para tomar o DSCP atribuído e para traçar aquele de volta a um valor CO. Este mapa padrão é indicado nesta tabela.

Alternativamente, o administrador pode criar um mapa que seja usado pelo interruptor para tomar o valor DSCP interno atribuído e para criar um valor novo CO para o quadro. Os exemplos de como você usaria Cactos e Cisco IOS integrado (modo nativo) para conseguir este são mostrados abaixo.

CatOS

```
Console> (enable) set qos dscp-cos--map 20-30:5 10-15:3 45-52:7
!-- QoS dscp-cos-map set successfully. Console> (enable)
```

O comando acima traça os valores 20 DSCP completamente a 30 a um valor CO de 5, os valores 10 DSCP com 15 ao CO de 3, e o DSCP avalia 45 embora a 52 a um valor CO do 7. Todos valores restantes DSCP usam o mapa padrão criado quando QoS foi permitido no interruptor.

O comando equivalente emitido no Cisco IOS integrado (modo nativo) é mostrado abaixo.

Cisco IOS integrado (modo nativo)

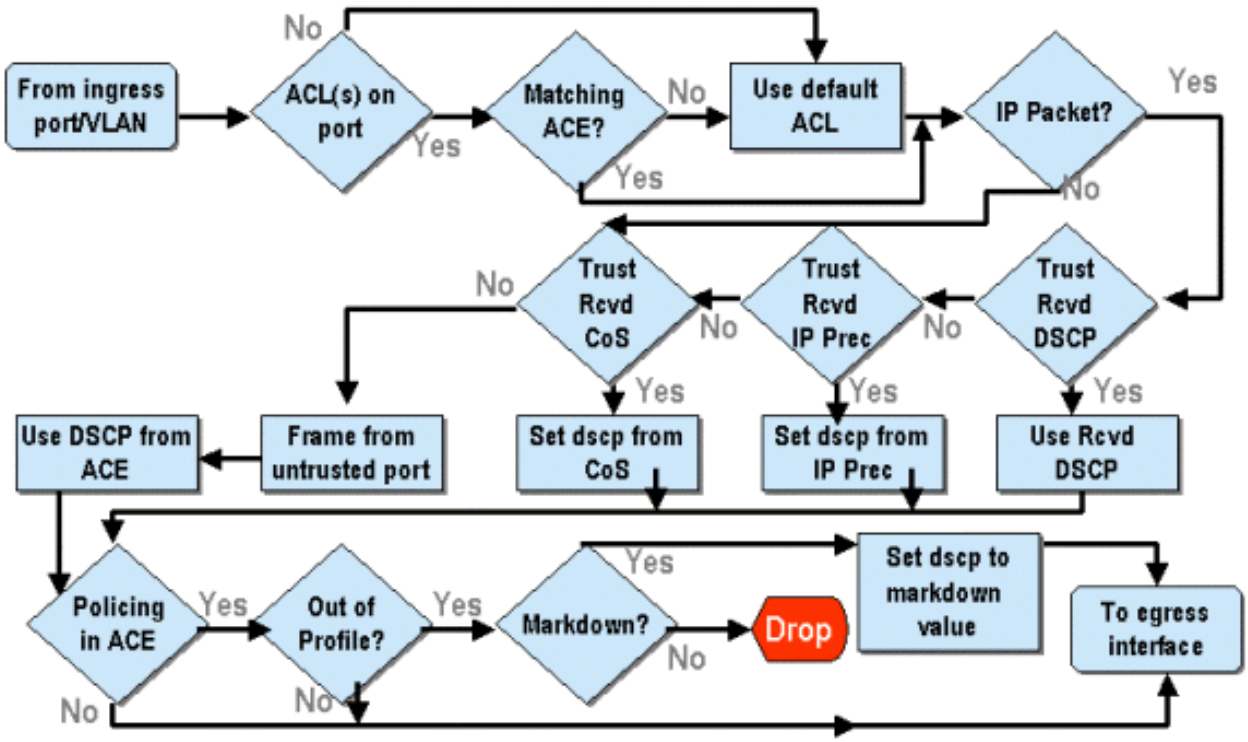
```
Cat6500(config)# mls qos map dscp-cos 20 30 40 50 52 10 1 to 3
Cat6500(config)#
```

Configura os valores DSCP de 20, 30, 40, 50, 52, 10 e 1 para um valor de 3 de COs.

Classificação e vigilância com o PFC

O PFC apoia a classificação e o policiamento dos quadros. A classificação pode usar um ACL para atribuir (marca) um frame de entrada com uma prioridade (DSCP). Policiar permite que um córrego do tráfego seja limitado a uma certa quantidade de largura de banda.

As seguintes seções descreverão estas capacidades no PFC da perspectiva do Cactos e das plataformas de OS do Cisco IOS integrado (modo nativo). Os processos aplicados pelo PFC são mostrados no seguinte diagrama:



Configurar o policiamento no Catalyst 6000 Family com Cactos

A função de vigilância é dividida em duas seções, uma para CatOS e uma para Cisco IOS integrado (modo nativo). Ambos conseguem o mesmo resultado final, mas são configurados e executados em maneiras diferentes.

Vigilância

O PFC apoia a capacidade ao tráfego de entrada do limite de taxa (ou a polícia) ao interruptor e pode reduzir o fluxo do tráfego a um limite predefinido. O tráfego excedente a esse limite pode ser descartado ou ter o valor DSCP marcado no quadro como menor.

A limitação da taxa da saída (saída) não é apoiada atualmente no PFC1 ou no PFC2. Isto será adicionado em uma nova revisão do PFC de planeamento para a segunda metade de 2002 que apoiará o policiamento da saída (ou a saída).

Policiar é apoiado no Cactos e no Cisco IOS integrado novo (modo nativo), embora a configuração destas características seja muito diferente. As seguintes seções descreverão a configuração de vigilância nas duas plataformas de OS.

Agregados e microfluxos (Cactos)

Os agregados e os microfluxos são termos usados para definir o espaço do policiamento que o PFC executa.

Um microfluxo define o policiamento de um fluxo único. Um fluxo é definido por uma sessão com um MAC address original SA/DA, endereço IP de Um ou Mais Servidores Cisco ICM NT SA/DA, e números de porta TCP/UDP. Para cada fluxo novo que é iniciado através de uma porta de um VLAN, o microfluxo pode ser usado para limitar a quantidade de dados recebidos para esse fluxo pelo interruptor. Na definição de microflow, os pacotes que excedem o limite de taxa prescrito podem ou ser deixados cair ou têm seu valor DSCP marcado para baixo.

Semelhante a um microfluxo, um agregado pode ser usado para limitar a taxa de tráfego.

Contudo, a taxa agregada aplica-se a todo o tráfego de entrada em uma porta ou em um VLAN que combine um QoS especificado ACL. Você pode ver o agregado como o policiamento do tráfego cumulativo que aquele combina o perfil na entrada de controle de acesso (ACE).

O agregado e o microfluxo definem a quantidade de tráfego que pode ser aceitada no interruptor. Um agregado e um microfluxo podem ser atribuídos ao mesmo tempo a uma porta ou a um VLAN.

Ao definir microfluxos, pode-se definir até 63 deles e até 1023 agregados.

Entradas de controle de acesso e QoS ACL (Cactos)

Um QoS ACL consiste em uma lista de ACE que definem um grupo de QoS ordena que os usos PFC processar frames de entrada. Os ás são similares a um Router Access Control List (RACL). O ACE define critérios de classificação, marcação e vigilância para um quadro de entrada. Se um frame de entrada combina os critérios ajustados no ACE, o Engine de QoS processará o quadro (como julgado pelo ACE).

Todo o processamento de QoS é feito no hardware, assim que permitir o Regulamentação QoS não impacta o desempenho do interruptor.

O PFC2 apoia atualmente até 500 ACL e aqueles ACL podem consistir em até 32000 ás (no total). Os números reais ACE dependerão dos outros serviços definidos e da memória disponível no PFC.

Existem três tipos de ACEs que podem ser definidos. São eles: IP, IPX e MAC. Os ás IP e IPX inspecionam a informação de cabeçalho L3, visto que os ás baseados MAC inspecionam somente a informação de cabeçalho L2. Deve-se igualmente notar que os ás MAC podem somente ser aplicados a não-IP e ao tráfego diferente de IPX.

Criando regras de vigilância

O processo de criar uma regra de vigilância envolve criar um agregado (ou o microfluxo), traçando então esse agregado (ou microfluxo) a um ACE.

Se, por exemplo, a exigência era limitar todo o tráfego IP recebido na porta 5/3 a um máximo do 20 MB, as duas etapas mencionadas acima devem ser configuradas.

Primeiramente, o exemplo pede todo o tráfego IP recebido para ser limitado. Isso implica que um vigilante agregado deve ser definido. Um exemplo deste pôde ser como segue:

```
Console> (enable) set qos policer aggregate test-flow rate 20000 burst 13 policed-dscp
!-- Hardware programming in progress !-- QoS policer for aggregate test-flow created
successfully. Console> (enable)
```

Criamos um agregado chamado de fluxo de teste. Define uma taxa de 20000 KBPS (20MBPS) e uma explosão de 13. As palavras-chave de DSCP vigiadas indicam que todos os dados que excedem esta política terão seu valor DSCP marcado para baixo como especificado em um mapa do mapa de DSCP (um padrão um existe ou este pode ser alterado pelo administrador). Uma substituição a usar as palavras-chave de DSCP vigiadas é usar a palavra-chave da gota. A palavra-chave drop simplesmente descartará todo o tráfego fora de perfil (tráfego que fica fora do valor de intermitência distribuído).

A facilidade de vigilância funciona em um esquema de vazamento de token bucket, no sentido de

que você define uma intermitência (quantidade de dados em bits por segundo que você aceitará em um dado intervalo (fixo) de tempo) e, depois, a taxa (definida como a quantidade de dados que você retirará daquele bucket em um único segundo). Todos os dados que transbordarem esta cubeta ou são deixados cair ou têm seu DSCP marcado para baixo. O período de tempo (ou intervalo) especificado mencionado acima é de 0,00025 segundos (ou 1/4000 segundo) e é fixo (isto é, não é possível utilizar nenhum comando de configuração para alterar esse número).

O número 13 do exemplo acima representa uma cubeta que aceite até 13,000 bit dos dados cada 1/4000th de um segundo. Isto relaciona-se ao 52 MB um o segundo (13K * (1/0.00025) ou 13K * 4000). Você deve sempre verificar se a intermitência está configurada para ser igual ou superior à taxa na qual deseja enviar dados. Ou seja a explosão deve ser superior ou igual à quantidade mínima de dados que você deseja transmitir por um período dado. Se a explosão conduz a uma figura mais baixa ao que você especificou como sua taxa, o limite de taxa igualará a explosão. Ou seja se você define uma taxa de 20 MBPS e de uma explosão que calcule a 15MBPS, sua taxa somente obterá nunca a 15MBPS. A próxima pergunta que você pode ter é por que 13?. Lembre-se de que o burst define a profundidade do token bucket, ou, em outras palavras, a profundidade do bucket utilizado para receber os dados que chegam a cada 1/4000 de segundo. Assim, a explosão podia ser todo o número apoiado em uma taxa de dados superior ou igual a no 20 MB da chegada um o segundo. O burst mínimo que poderia ser usado para um limite de taxa de 20 MB é 20000/4000 = 5.

Durante o processamento do vigilante, o algoritmo de vigilância começa preenchendo o token bucket com um complemento completo de tokens. O número de tokens é igual ao valor do burst. Assim, se o valor de intermitência é 13, o número de tokens nos iguais 13,000 da cubeta. Para cada 1/4000th de um segundo, o algoritmo de vigilância mandará uma quantidade de dados iguais à taxa definida dividida por 4000. Para cada bit (dígito binário) dos dados enviados, consome um token da cubeta. No fim do intervalo, reabastecerá a cubeta com um grupo novo de tokens. O número de tokens que substitui é definido pela taxa/4000. Considere o exemplo acima compreender isto:

```
Console> (enable) set qos policer aggregate test-flow rate 20000 burst 13
```

Supõe que esta é uma porta do 100 MBPS e nós estamos enviando em um córrego constante do 100 MBPS na porta. Nós sabemos que este igualará a uma taxa recebida de 100,000,000 bit por segundo. Os parâmetros aqui são uma taxa de 20000 e explosão de 13. No intervalo de tempo t0, há um complemento direto de tokens na cubeta (que é 13,000). No intervalo de tempo t0, nós mandaremos o primeiro conjunto de dados chegar na porta. Para este intervalo de tempo, a taxa de chegada será bit por segundo de 100,000,000/4000 = 25,000. Porque nosso Token Bucket tem somente uma profundidade de 13,000 tokens, simplesmente 13,000 bit dos 25,000 bit que chegam na porta neste intervalo são elegíveis para ser enviada e 12,000 bit são deixados cair.

A taxa especificada define uma taxa de encaminhamento de 20,000,000 bit por segundo, que iguale 5,000 bit enviados pelo 1/4000th intervalo. Para cada 5,000 bit enviados, há 5,000 tokens consumidos. No T1 do intervalo de tempo, outros 25,000 bit dos dados chegam, mas a cubeta deixa cair 12,000 bit. O bucket é reposto com tokens definidos como a taxa / 4000 (que equivale a 5.000 novos tokens). O algoritmo emite, em seguida, o próximo complemento de dados, que se iguala a outros 5.000 bits de dados (isso consome outros 5.000 tokens), e assim por diante, em cada intervalo.

Essencialmente, todos os dados que vêm além da profundidade do repositório (explosão definida) são deixados cair. Dados deixados sobre depois que os dados estiveram enviados (de harmonização indicado a taxa) são deixados cair igualmente, fazendo a maneira para o grupo seguinte de dados de chegada. Um pacote incompleto é um que não esteve recebido inteiramente dentro do intervalo de tempo não está deixado cair mas é mantido até que esteja

recebido inteiramente na porta.

Esse número de burst supõe um fluxo constante de tráfego. Contudo, nas redes do mundo real, os dados não são constantes e seu fluxo é determinado pelos tamanhos da janela TCP, que incorporam reconhecimentos TCP na sequência da transmissão. Para levar em consideração os problemas de tamanhos de janela de TCP, é recomendado que o valor de burst seja dobrado. No exemplo acima, o valor sugerido de 13 seria configurado realmente como 26.

Outro aspecto importante é que no intervalo de tempo 0, ou seja, no início do ciclo de vigilância, o token bucket estará repleto de tokens.

Essa política de agregação agora deve ser incorporada ao ACE de QoS. O ACE é o lugar onde a especificação é feita para combinar um grupo de critérios a um frame de entrada. Considere o seguinte exemplo. Você deseja aplicar o agregado definido acima para todo o tráfego IP, mas especificamente para o tráfego com origem da sub-rede 10.5.x.x e com destino para a sub-rede 203.100.45.x. O ACE pareceria com o seguinte:

```
Console> (enable) set qos acl ip test-acl trust-dscp aggregate test-flow tcp 10.5.0.0
203.100.45.0
!-- Test-acl editbuffer modified. Issue the commit command to apply changes.
Console> (enable)
```

O comando acima criou um ACE IP (indicado pelo uso do comando set qos acl ip), que agora está associado a um ACL QoS chamado test-acl. Aces subseqüentes criados e associados ao ACL test-acl são incluídos ao final da lista ACE. A entrada ACE tem o fluxo de teste agregado associado. Todos os fluxos de TCP com uma sub-rede de origem de 10.5.0.0 e sub-rede de destino de 203.100.45.0 terão esta política aplicada a ela.

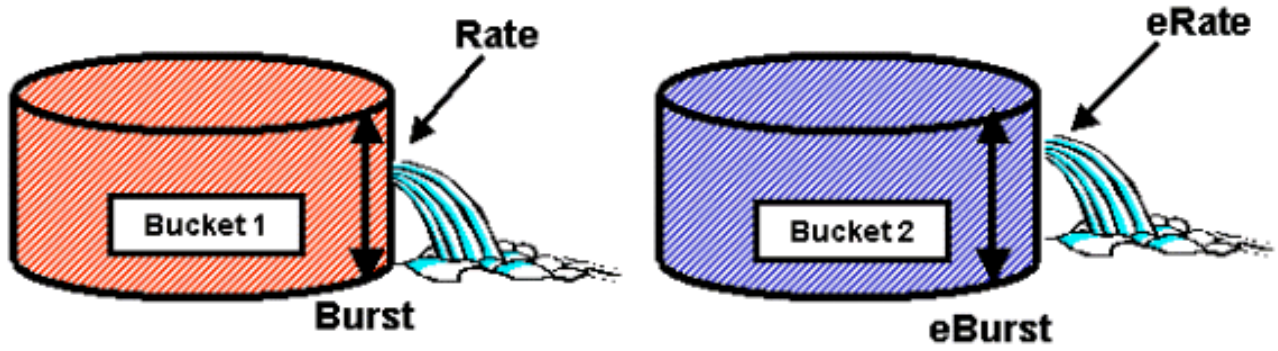
Os ACL (e os ás associados) fornecem um nível muito granulado da flexibilidade de configuração que os administradores possam usar. Um ACL pode consistir em um ou um número de ás, e a fonte e/ou os endereços de destino podem ser usados assim como os valores de porta L4 para identificar os fluxos particulares que são exigidos ser policiados.

Contudo, antes que policiar ocorra realmente, o ACL tem que ser traçado a uma porta física ou a um VLAN.

Decisões de vigilância PFC2

Para o PFC2, uma mudança foi feita em Cactos 7.1 e em Cactos 7.2, que introduziram um algoritmo de leaky bucket dual para policiar. Com este algoritmo novo, adiciona os seguintes dois níveis novos:

1. **Nível de policiamento normal:** é igual ao primeiro bucket e define os parâmetros especificando a profundidade do bucket (burst) e a taxa com a qual os dados devem ser enviados do bucket (taxa).
2. **Nível de policiamento adicional:** isto iguala a uma segunda cubeta e define os parâmetros que especificam a profundidade da cubeta (eburst) e da taxa em que os dados devem ser enviados da cubeta (erate).



A forma como esse processo funciona é com os dados começando a preencher o primeiro bucket. O PFC2 aceita um fluxo de dados entrante inferior ou igual à profundidade (valor de intermitência) da primeira cubeta. Os dados que transbordam da primeira cubeta podem ser marcados para baixo e são passados à segunda cubeta. O segundo bucket pode aceitar uma taxa de entrada de dados vindos do primeiro bucket em um valor menor ou igual ao valor eburst. Os dados da segunda cubeta são enviados em uma taxa definida pelo erate parameter minus o parâmetro de taxa. Os dados que transbordam da segunda cubeta podem igualmente ser marcados para baixo ou deixado cair.

Um exemplo de um vigilante do leaky bucket dual é como segue:

```
Console> (enable) set qos policer aggregate AGG1 rate 10000 policed-dscp erate 12000 drop burst
13 eburst 13
```

Esse exemplo posiciona um agregado chamado AGG1 com uma taxa de excesso de tráfego de 10 MPBS e será marcado com um valor inferior de acordo com o mapa de políticas DSCP. O tráfego em excesso do agregado (definido em 12 MBPS) será descartado de acordo com a palavra-chave de perda.

Aplicando policeres agregados aos módulos habilitados por DFC

Deve-se notar que o aplicativo dos policeres agregados nas placas de linha NON-DFC pode ser conseguido devido à maneira que os 6000 usam um Forwarding Engine centralizado (PFC) para o tráfego de encaminhamento. A implementação de um mecanismo de encaminhamento central permite rastrear as estatísticas de tráfego para uma determinada VLAN. Este processo pode ser usado para aplicar um policer agregado a um VLAN.

Em uma placa de linha permitida DFC, contudo, as decisões de encaminhamento são distribuídas a essa placa de linha. O DFC está somente ciente das portas em sua placa de linha imediata e é inconsciente do movimento do tráfego em outras placas de linha. Por este motivo, se um policer agregado é aplicado a um VLAN que tenha portas membro através dos vários módulos DFC, o vigilante pode produzir resultados inconsistentes. A razão para esta é que o DFC pode somente se manter a par de estatísticas da porta local e não leva em consideração estatísticas de porta em outras placas de linha. Por este motivo, um policer agregado aplicado a um VLAN com portas membro em uma placa de linha permitida DFC conduzirá ao DFC que policia o tráfego ao limite taxado para as portas VLAN residentes na placa de linha DFC somente.

O mapa de DSCP traça (Cactos)

Os mapas do mapa de DSCP são usados quando o vigilante é definido ao tráfego fora de perfil do markdown em vez do deixar cair. O tráfego fora do perfil é definido como o tráfego que excede à configuração definida do surto.

Um mapa do mapa de DSCP do padrão estabelece-se quando QoS é permitido. Esse mapa

padrão de redução foi listado nessa tabela anteriormente no documento. O comando line interface(cli) permite que um administrador altere o mapa de promoção do padrão emitindo o **comando set qos policed-dscp-map**. Um exemplo é fornecido abaixo.

```
Cat6500(config)# set qos policed-dscp-map 20-25:7 33-38:3
```

Este exemplo altera o mapa dscp policiado para refletir que os valores 20 DSCP a 25 estarão marcados completamente para baixo a um valor DSCP de 7, e valores DSCP de 33 a 38 estará marcado completamente para baixo a um valor DSCP de 3.

Políticas de mapeamento a VLAN e a portas (Cactos)

Após a criação de uma ACL, ela deve ser mapeada para uma porta ou uma VLAN para poder ser efetivada.

Um comando interessante que trava muitos inconscientes é o ajuste de QoS do padrão que faz toda a porta de QoS baseada. Se você aplica um agregado (ou o microfluxo) a um VLAN, não tomará o efeito em uma porta a menos que essa porta for configurada para QoS baseado VLAN.

```
Console> (enable) set port qos 2/5-10 vlan-based
!-- Hardware programming in progress  !-- QoS interface is set to vlan-based for ports 2/5-10.
Console> (enable)
```

Mudar QoS com base na porta a QoS com base em VLAN destaca imediatamente todos os ACL atribuídos a essa porta, e atribui todos os ACL baseados VLAN a essa porta.

Traçar o ACL a uma porta (ou ao VLAN) é feito emitindo o comando seguinte:

```
Console> (enable) set qos acl map test-acl 3/5
!-- Hardware programming in progress  !-- ACL test-acl is attached to port 3/5. Console>
(enable) Console> (enable) set qos acl map test-acl 18
!-- Hardware programming in progress  !-- ACL test-acl is attached to VLAN 18. Console> (enable)
```

Mesmo depois o traço do ACL a uma porta (ou a um VLAN), o ACL ainda não toma o efeito até que o ACL esteja comprometido ao hardware. Isso está descrito na seção seguinte. Neste momento, o ACL reside em um provisório edita o buffer na memória. Enquanto estiver nesse buffer, o ACL poderá ser modificado.

Se você deseja remover algum ACL descomprometido que residir no editbuffer, você emitiria o **comando rollback**. Esse comando exclui o ACL do buffer de edição.

```
Console> (enable) rollback qos acl test-acl
!-- Rollback for QoS ACL test-acl is successful. Console> (enable)
```

ACL comprometendo (Cactos)

Para aplicar o QoS ACL que você definiu (acima), o ACL deve estar comprometido com o hardware. O processo de comprometer copia o ACL do buffer provisório ao hardware PFC. Uma vez residindo na memória da PFC, a política definida na ACL de QoS pode ser aplicada a todo o tráfego que corresponda aos ACEs.

Para a facilidade da configuração, a maioria de administradores emitem um **comando all**

comprometer. Contudo, você pode comprometer um ACL específico (um de muitos) que possa atualmente residir no buffer da edição. Um exemplo do comando commit é mostrado abaixo.

```
Console> (enable) commit qos acl test-acl
!-- Hardware programming in progress  !-- ACL test-acl is committed to hardware. Console>
(enable)
```

Se você deseja remover um ACL de uma porta (ou de um VLAN), você precisa de cancelar o mapa que associa esse ACL a essa porta (ou a VLAN) emitindo o comando seguinte:

```
Console> (enable) clear qos acl map test-acl 3/5
!-- Hardware programming in progress  !-- ACL test-acl is detached from port 3/5.
Console>(enable)
```

Configure Policing on the Catalyst 6000 Family with Integrated Cisco IOS (Native Mode)

Policiar é apoiado com Cisco IOS integrado (modo nativo). Contudo, a configuração e a aplicação da função de vigilância são conseguidas usando mapas da política. Cada mapa de política usa classes da política múltipla para compor um mapa de política e estas classes de política podem ser definidas para fluxos diferentes dos tipos de tráfego.

Classes de mapas de política, ao filtrarem, usam ACLs com base em IOS e instruções de correspondência de classe para identificar o tráfego a ser vigiado. Depois que o tráfego for identificado, as classes de política poderão usar os vigilantes agregados de microfluxo para aplicar as políticas de vigilância àquele tráfego correspondente.

As seções seguintes explicam a configuração de vigilância para o Integrated Cisco IOS (Modo Nativo) em mais detalhes.

Agregados e microfluxos (Cisco IOS integrado (modo nativo))

Os agregados e os microfluxos são termos usados para definir o espaço do policiamento que o PFC executa. Igualmente ao CatOS, os agregados e os microfluxos também são usados como Integrated Cisco IOS (Modo nativo).

Um microfluxo define o policiamento de um fluxo único. Um fluxo é definido por uma sessão com um MAC address original SA/DA, endereço IP de Um ou Mais Servidores Cisco ICM NT SA/DA, e números de porta TCP/UDP. Para cada fluxo novo que é iniciado através de uma porta de um VLAN, o microfluxo pode ser usado para limitar a quantidade de dados recebidos para esse fluxo pelo interruptor. Na definição de microflow, os pacotes que excedem o limite de taxa prescrito podem ou ser deixados cair ou têm seu valor DSCP marcado para baixo. Os microfluxos são aplicados usando o comando police flow que formulários parte de uma classe do mapa de política.

Para permitir a vigilância de microfluxo no Cisco IOS integrado (modo nativo), deve ser permitida globalmente no interruptor. Isso pode ser feito com a emissão do seguinte comando:

```
Cat6500(config)# mls qos flow-policing
```

A vigilância de microfluxo pode igualmente ser aplicada ao tráfego interligado, que é o tráfego que não é L3 comutado. Para permitir o interruptor de apoiar a vigilância de microfluxo no tráfego interligado, emita o comando seguinte:

```
Cat6500(config)# mls qos bridged
```

Este comando igualmente permite a vigilância de microfluxo para o tráfego multicast. Se o tráfego multicast precisa de ter uma vigilância de microfluxo aplicada a ele, este comando (**qos dos mls construídos uma ponte sobre**) deve ser permitido.

Semelhante a um microfluxo, um agregado pode ser usado para limitar a taxa de tráfego. Contudo, a taxa agregada aplica-se a todo o tráfego de entrada em uma porta ou em um VLAN que combine um QoS especificado ACL. É possível exibir o agregado como a vigilância de tráfego cumulativo que corresponde a um perfil de tráfego definido.

Existem duas formas de agregados que podem ser definidas no Cisco IOS integrado (modo nativo), como se segue:

- por vigilantes agregados de interface
- vigilantes agregados nomeados

Os agregados por interface são aplicados a um interface individual através da emissão do comando police em uma classe de mapa de política. Essas classes de mapa podem ser aplicadas a várias interfaces, mas o vigilante policia cada interface separadamente. Os agregados nomeados são aplicados a um tráfego do grupo de portas e da polícia através de todas as relações cumulativamente. Os agregados nomeados são aplicados emitindo o **comando mls qos aggregate policer**.

Ao definir microfluxos, pode-se definir até 63 deles e até 1023 agregados.

Criando regras de vigilância (Cisco IOS integrado (modo nativo))

O processo de criar uma regra de vigilância envolve criar um agregado (ou o microfluxo) através de um mapa de política e então anexar esse mapa de política a uma relação.

Considere o mesmo exemplo criado para o Cactos. A exigência era limitar todo o tráfego IP recebido na porta 5/3 a um máximo do 20 MBPS.

Primeiramente, um mapa de política deve ser criado. Crie um mapa de política nomeado limite-tráfego. Isto é feito como segue:

```
Cat6500(config)# policy-map limit-traffic
Cat6500(config-pmap)#
```

Você observará imediatamente que a alerta do interruptor muda para refletir que você reage do modo de configuração para criar um map class. Lembre-se de que um mapa de políticas pode conter múltiplas classes. Cada classe contém um conjunto separado de ações de política que podem ser aplicadas aos fluxos de tráfego diferentes.

Devemos criar uma classe de tráfego para limitar especificamente o tráfego recebido a 20 MBPS. Nós chamaremos esta classe limit-to-20. Isto é mostrado abaixo.

```
Cat6500(config)# policy-map limit-traffic
Cat6500(config-pmap)# class limit-to-20
Cat6500(config-pmap-c)#
```

O prompt se altera novamente para refletir que agora você está na configuração de classe de mapa (mostrado com o -c no fim do prompt). Se você quis aplicar o limite de taxa para combinar o tráfego de entrada específico, você pode configurar um ACL e aplicar isto ao nome de classe. Se você quer aplicar o limite do 20 MBPS para traficar originado da rede 10.10.1.x, emita o seguinte ACL:

```
Cat6500(config)# access-list 101 permit ip 10.10.1.0  0.0.0.255 any
```

Você poderia adicionar este ACL ao nome de classe como segue:

```
Cat6500(config)# policy-map limit-traffic
Cat6500(config-pmap)# class limit-to-20 access-group 101
Cat6500(config-pmap-c)#
```

Depois que o mapa da classe estiver definido, pode-se definir os vigilantes individuais para essa classe. Você pode criar agregados (usando a palavra-chave "vigia") ou microfluxos (usando a palavra-chave "fluxo de vigias"). Crie o agregado, como mostrado abaixo.

```
Cat6500(config)# policy-map limit-traffic
Cat6500(config-pmap)# class limit-to-20 access-group 101
Cat6500(config-pmap-c)# police 20000000 13000 confirm-action transmit exceed-action drop
Cat6500(config-pmap-c)# exit
Cat6500(config-pmap)# exit
Cat6500(config)#
```

A instrução de classe acima (comando police) configura um limite de taxa de 20.000 k (20 Mbps) com um burst de 52 Mbps (13.000 x 4.000 = 52 MB). Se o tráfego combina o perfil e está dentro do limite taxado, a ação é ajustar-se pela indicação da confirmar-ação para transmitir o tráfego em perfil. Se o tráfego é fora de perfil (isto é, em nosso exemplo acima o limite do 20 MB), a indicação de ação em excesso está ajustada para deixar cair o tráfego (isto é, em nosso exemplo todo o tráfego acima do 20 MB é deixado cair).

Na configuração de um microfluxo, uma ação semelhante é executada. Se nós quisemos ao limite de taxa todos os fluxos em uma porta que combinasse um mapa dado da classe a 200 K cada um, a configuração desse fluxo seria similar ao seguinte:

```
Cat6500(config)# mls qos flow-policing
Cat6500(config)# policy-map limit-each-flow
Cat6500(config-pmap)# class limit-to-200
Cat6500(config-pmap-c)# police flow 200000 13000 confirm-action transmit exceed-action drop
Cat6500(config-pmap-c)# exit
Cat6500(config-pmap)# exit
```

Mapas do mapa de DSCP

Os mapas do mapa de DSCP são usados quando o vigilante é definido ao tráfego fora de perfil do markdown em vez do deixar cair. O tráfego fora do perfil é definido como o tráfego que excede à

configuração definida do surto.

Um mapa do mapa de DSCP do padrão é estabelecido quando QoS é permitido. Esse mapa de promoção padrão é listado nessa tabela. O CLI permite que um administrador modifique o mapa padrão de redução emitindo o comando set qos policed-dscp-map. Um exemplo é fornecido abaixo.

```
Cat6500(config)#

mls qos map policed-dscp normal-burst 32 to 16
```

Este exemplo define uma alteração ao mapa dscp policiado padrão que o valor DSCP de 32 será marcado para baixo a um valor DSCP de 16. Para uma porta com este vigilante definido, todos os dados de entrada com este DSCP avaliam que é parte de um bloco de dados além da explosão indicada terá seu valor DSCP marcado para baixo a 16.

Políticas de mapeamento a VLAN e a portas (Cisco IOS integrado (modo nativo))

Uma vez que uma política foi construída, deve então ser traçada a uma porta ou a um VLAN para que essa política tome o efeito. Ao contrário do processo de comprometimento em Cactos, há não equivalente no Cisco IOS integrado (modo nativo). Quando uma política é mapeada para uma interface, essa política está em efeito. Para traçar a política acima a uma relação, emita o comando seguinte:

```
Cat6500(config)# interface fastethernet 3/5
Cat6500(config-if)# service-policy input limit-traffic
```

Se uma política é traçada a um VLAN, para cada porta no VLAN que você deseja a política vlan se aplicar a, você deve informar a relação que QoS é VLAN baseado emitindo o **comando mls qos vlan-based**.

```
Cat6500(config)# interface fastethernet 3/5
Cat6500(config-if)# mls qos vlan-based
Cat6500(config-if)# exit
Cat6500(config)# interface vlan 100
Cat6500(config-if)# service-policy input limit-traffic
```

A relação presumida 3/5 era parte de VLAN 100, a política nomeada o limite-tráfego que foi aplicado ao VLAN 100 igualmente se aplicaria para conectar 3/5.

Configurar a classificação no Catalyst 6000 Family com Cactos

A PFC introduz o suporte para a classificação de dados usando ACLs que podem visualizar informações de cabeçalhos de L2, L3 e L4. Para um SupI, ou o IA (sem PFC), a classificação é limitada a usar as palavras-chaves da confiança em portas.

A seção a seguir descreve os componentes de configuração QoS usados pelo PFC para Classificação no CatOS.

CO ao mapeamento de DSCP (Cactos)

No ingresso ao interruptor, um quadro terá um conjunto de valores DSCP pelo interruptor. Se a porta está em um estado confiável, e o administrador usou as palavras-chave Trust-CoS, o conjunto de valores CO no quadro estará usado para determinar o conjunto de valores DSCP para o quadro. Como mencionado antes, o interruptor pode atribuir níveis do serviço ao quadro como ele transita pelo interruptor baseado no valor DSCP interno.

Esta palavra-chave em algum do 10/100 mais adiantado dos módulos (WS-X6248 e WS-X6348) não é apoiada. Para aqueles módulos, recomenda-se usando ACL para aplicar ajustes CO para dados de entrada.

Quando QoS é permitido, o interruptor cria um mapa padrão. Esse mapa é usado para identificar o valor DSCP que será definido com base no valor de COs. Estes mapas são alistados nesta tabela mais cedo no documento. Alternativamente, o administrador pode estabelecer um mapa original. Um exemplo é fornecido abaixo.

```
Console> (enable) set qos cos-dscp-map 20 30 1 43 63 12 13 8
!-- QoS cos-dscp-map set successfully. Console> (enable)
```

O comando acima configura o seguinte mapa:

CO	0	1	2	3	4	5	6	7
DSCP	20	30	1	43	63	12	13	8

Enquanto é muito improvável que o mapa acima seja utilizado em uma rede real, ele serve para dar uma idéia do que pode ser alcançado utilizando este comando.

Precedência IP ao mapeamento de DSCP (Cactos)

Da mesma forma que os COs para mapeamento DSCP, um quadro pode ter um valor DSCP determinado a partir da definição de precedência de IP de pacotes recebidos. Isto ainda ocorre somente se a porta é ajustada ao confiado pelo administrador, e usaram as palavras-chave trust-ipprec.

Quando QoS é permitido, o interruptor cria um mapa padrão. Este mapa é citado nessa tabela anteriormente neste documento. Esse mapa é usado para identificar o valor de DSCP que será definido com base no valor de precedência IP. Alternativamente, o administrador pode estabelecer um mapa original. Um exemplo é fornecido abaixo:

```
Console> (enable) set qos ipprec-dscp-map 20 30 1 43 63 12 13 8
!-- QoS ipprec-dscp-map set successfully. Console> (enable)
```

O comando acima configura o seguinte mapa:

Precedência de IP	0	1	2	3	4	5	6	7
DSCP	20	30	1	43	63	12	13	8

Enquanto é muito improvável que o mapa acima seja utilizado em uma rede real, ele serve para dar uma idéia do que pode ser alcançado utilizando este comando.

Classificação (Cactos)

Quando um quadro é passado para o PFC para processamento, o processo de classificação é realizado no quadro. O PFC utilizará um ACL pré-configurado (ou um ACL padrão) para atribuir

um DSCP ao quadro. No ACE, uma das quatro palavras-chaves é usada para atribuir um valor de DSCP. São os seguintes:

1. TRUST-DSCP (somente ACLs IP)
2. TRUST-IPPREC (IP ACL'=s only)
3. TRUST-COS (todos os ACLs, exceto IPX e MAC em uma PFC2)
4. DSCP

A palavra-chave do TRUST-DSCP supõe que o quadro que chega no PFC já tem um conjunto de valores DSCP antes dele que incorpora o interruptor. O interruptor manterá este valor DSCP.

Com TRUST-IPPREC, o PFC derivará um valor DSCP do residente existente do valor de precedência IP no campo ToS. O PFC utilizará a precedência IP para mapas de DSCP para atribuir o DSCP correto. Um mapa padrão é criado quando QoS é permitido no interruptor. Alternativamente, um mapa criado pelo administrador pode ser usado para derivar o valor DSCP.

Similarmente à TRUST-IPPREC, a palavra-chave TRUS-COS avisa o PFC para derivar um valor DSCP a partir dos COs no cabeçalho do quadro. Haverá também COs para mapa DSCP (um padrão um de um administrador atribuído a um) para ajudar o PFC na derivação do DSCP.

A palavra-chave DSCP é usada quando um quadro chega a partir de uma porta não-confiável. Isso é uma situação interessante para a derivação do DSCP. Neste momento, o DSCP configurado na indicação acl dos qos do grupo é usado para derivar o DSCP. Contudo, é neste momento onde os ACL podem ser usados para derivar um DSCP para o tráfego baseado nos critérios de classificação ajustados no ACE. Isso significa que em um ACE, pode-se usar os critérios de classificação como endereço IP de origem e de destino, números de portas TCP/UDP, códigos ICMP, tipo de IGMP, números de rede e de protocolo IPX, endereços MAC de origem e de destino e Ethertipos (somente para tráfego não-IP e não-IPX) para identificar o tráfego. Isto significa que um ACE poderia ser configurado para atribuir um valor específico DSCP para dizer o tráfego de HTTP sobre o tráfego FTP.

Considere o seguinte exemplo:

```
Console> (enable) set port qos 3/5 trust untrusted
```

Definir uma porta como não confiável instruirá o PCF a usar um ACE para derivar o DSCP do quadro. Se o ACE é configurado com critérios de classificação, o indivíduo flui dessa porta pode ser classificado com prioridades diferentes. Os Aces a seguir ilustram isso:

```
Console> (enable) set qos acl ip abc dscp 32 tcp any any eq http
Console> (enable) set qos acl ip ABC dscp 16 tcp any any eq ftp
```

Neste exemplo, nós temos duas indicações ACE. O primeiro identifica todo o fluxo de TCP (a palavra-chave é usada para identificar o tráfego de origem e de destino) cujo número de porta for 80 (80 = HTTP) para ser atribuídos um valor DSCP de 32. O segundo ACE identifica o tráfego originado de todo o host e destinado a qualquer host cujo o número de porta de TCP for 21 (FTP) seja atribuído um valor DSCP de 16.

Configure a classificação da família Catalyst 6000 com Cisco IOS integrado (Modo nativo)

A seguinte seção descreve os componentes da configuração de QoS usados para apoiar a classificação no PFC usando o Cisco IOS integrado (modo nativo).

CO ao mapeamento de DSCP (Cisco IOS integrado (modo nativo))

No ingresso ao interruptor, um quadro terá um conjunto de valores DSCP pelo interruptor. Se a porta está em um estado confiável, e o administrador usou as palavras-chave Trust-CoS dos qos dos mls (em portas GE ou em 10/100 das portas nas placas de linha WS-X6548), o conjunto de valores CO no quadro estará usado para determinar o conjunto de valores DSCP para o quadro. Como mencionado antes, o interruptor pode atribuir níveis do serviço ao quadro como ele transita pelo interruptor baseado no valor DSCP interno.

Quando QoS é permitido, o interruptor cria um mapa padrão. Consulte esta tabela para obter as configurações padrão. Esse mapa é usado para identificar o valor DSCP que será definido com base no valor de COs. Alternativamente, o administrador pode estabelecer um mapa original. Um exemplo é fornecido abaixo.

```
Cat6500(config)# mls qos map cos-dscp 20 30 1 43 63 12 13 8
Cat6500(config)#
```

O comando acima configura o seguinte mapa:

CO	0	1	2	3	4	5	6	7
DSCP	20	30	1	43	63	12	13	8

Enquanto é muito improvável que o mapa acima seja utilizado em uma rede real, ele serve para dar uma idéia do que pode ser alcançado utilizando este comando.

Precedência IP ao mapeamento de DSCP (Cisco IOS integrado (modo nativo))

Da mesma forma que os COs para mapeamento DSCP, um quadro pode ter um valor DSCP determinado a partir da definição de precedência de IP de pacotes recebidos. Isso ainda ocorrerá somente se a porta for definida como confiável pelo administrador e eles tiverem usado a palavra-chave mls qos trust-ipprec. A palavra-chave é suportada apenas em portas GE e 10/100 em placas de linha WS-X6548. Para 10/100 das portas o as placas de linha WS-X6348 e WS-X6248, ACL devem ser usadas para atribuir a confiança da Precedência IP aos dados de entrada.

Quando QoS é permitido, o interruptor cria um mapa padrão. Consulte esta tabela para obter as configurações padrão. Esse mapa é usado para identificar o valor de DSCP que será definido com base no valor de precedência IP. Alternativamente, o administrador pode estabelecer um mapa original. Um exemplo é fornecido abaixo.

```
Cat6500(config)# mls qos map ip-prec-dscp 20 30 1 43 63 12 13 8
Cat6500(config)#
```

O comando acima configura o seguinte mapa:

Precedência de IP	0	1	2	3	4	5	6	7
DSCP	20	30	1	43	63	12	13	8

Enquanto é muito improvável que o mapa acima seja utilizado em uma rede real, ele serve para

dar uma idéia do que pode ser alcançado utilizando este comando.

Classificação (Cisco IOS integrado (modo nativo))

Quando um quadro é passado à PFC, o processo de classificação pode ser executado para atribuir uma nova prioridade ao quadro recebido. A advertência nesse caso é que essa atribuição só poderá ser feita quando o quadro for originário de uma porta não confiável ou quando tiver sido classificado como não confiável.

Uma ação de classe do mapa de política pode ser usada a:

1. TRUST COS
2. TRUST IP-PRECEDENCE
3. TRUST DSCP
4. NENHUMA CONFIANÇA

O palavra-chave DSCP da CONFIANÇA supõe que o quadro que chega no PFC já tem um conjunto de valores DSCP antes dele que incorpora o interruptor. O interruptor manterá este valor DSCP.

Com TRUST IP-PRECEDENCE, o PFC derivará um valor DSCP do valor de precedência de IP existente residente no campo ToS. O PFC usará uma Precedência IP ao mapa dscp para atribuir o DSCP correto. Um mapa padrão é criado quando QoS é permitido no interruptor. Alternativamente, um mapa criado pelo administrador pode ser usado para derivar o valor DSCP.

Similar PARA CONFIAR O IP-PRECEDENCE, a palavra-chave da CONFIANÇA CO instrui o PFC para derivar um valor DSCP dos CO no cabeçalho de frame. Haverá também COs para mapa DSCP (um padrão um de um administrador atribuído a um) para ajudar o PFC na derivação do DSCP.

Um exemplo de derivar o DSCP de uma prioridade existente (DSCP, Precedência IP, ou CO) é mostrado abaixo.

```
Cat6500(config)# policy-map assign-dscp-value
Cat6500(config-pmap)# class test
Cat6500(config-pmap-c)# trust COs
Cat6500(config-pmap-c)# exit
Cat6500(config-pmap)# exit
Cat6500(config)#
```

O mapa de classe acima deduzirá o valor de DSCP dos COs no cabeçalho de Ethernet.

NENHUM formulário da CONFIANÇA da palavra-chave é usado quando um quadro chega de uma porta não-confiável. Isto permite que o quadro tenha um valor DSCP atribuído durante o processo de policiamento.

Considere o exemplo seguinte de como uma prioridade nova (DSCP) pode ser atribuída aos fluxos diferentes que entram o PFC usando a seguinte definição de política.

```
Cat6500(config)# access-list 102 permit tcp any any eq http
Cat6500(config)# policy-map new-dscp-for-flow
Cat6500(config-pmap)# class test access-group 102
```

```
Cat6500(config-pmap-c)# no trust
Cat6500(config-pmap-c)# police 1000 1 confirm-action set-dscp-transmit 24  Cat6500(config-pmap-
c)# exit
Cat6500(config-pmap)# exit
Cat6500(config)#
```

O exemplo acima mostra o seguinte:

1. Um ACL que está sendo criado para identificar os fluxos HTTP que entram a porta.
2. Um mapa de política chamou o novo-DSCP-para-fluxo.
3. Um mapa da classe (teste dos nomes) esse usa a lista de acessos 102 para identificar o tráfego que este mapa da classe executará sua ação para.
4. O teste de mapa de classe define o estado confiável do quadro de entrada como não-confiável e atribui um DSCP de 24 para o fluxo.
5. Este mapa da classe igualmente limitará o agregado de todos os fluxos HTTP a um máximo de 1MB.

COPS (Common Open Policy Server)

As BOBINAS são um protocolo que permita o Catalyst 6000 Family de ter QoS configurado de um host remoto. Atualmente, as BOBINAS somente são apoiadas usando Cactos e são parte da arquitetura INTSERV para QoS. Atualmente, não há suporte (a partir da data deste documento) para COPS ao usar o Cisco IOS Integrado (Modo Nativo). Quando o protocolo das BOBINAS levar a informação de configuração de QoS ao interruptor, não é a fonte da informação de configuração de QoS. O uso do protocolo das BOBINAS exige um gerenciador externo de QoS hospedar as configurações de QoS para o interruptor. O gerenciador externo de QoS iniciará o impulso descendente daquelas configurações ao interruptor usando o protocolo das BOBINAS. O QoS Policy Manager de Cisco (QPM) é um exemplo de um gerenciador externo de QoS.

Não é a intenção deste documento para explicar os funcionamentos do QPM, mas para explicar a configuração exigida no interruptor para apoiar configurações de QoS externas da utilização do QPM.

Configuração do COPS:

Àrevelia, o apoio das BOBINAS é desabilitado. Para usar BOBINAS no interruptor, deve ser permitido. Isso pode ser feito com a emissão do seguinte comando:

```
Console> (enable) set qos policy-source cops
!-- QoS policy source for the switch set to COPS. Console> (enable)
```

Quando este comando é iniciado, determinados valores de configuração de QoS padrão serão originados no servidor COPS. Esses valores de configuração incluem:

1. CO aos mapeamentos de fila
2. Atribuições de limiares da fila de entrada e de saída
3. Atribuições de largura de banda de WRR
4. Alguns agregado e políticas de micro-fluxo
5. DSCP aos mapas COS para o tráfego de saída
6. ACL
7. Atribuições da porta CoS padrão

Quando as configurações de QoS forem realizadas usando COPS, é importante compreender

que o aplicativo dessas configurações é aplicado de uma forma diferente. Mais do que para configurar diretamente as portas, o COPS é utilizado para configurar a porta ASIC. Geralmente, a porta ASIC controla um grupo de portas; portanto a configuração de COPS é aplicada a várias portas ao mesmo tempo.

A porta ASIC configurada é GE ASIC. Em placas de linha GE, há quatro portas por GE (portas 1-4, 5-8, 9-12, 13-16). Nessas placas de ingresso, a configuração COPS afeta cada grupo de portas. Em 10/100 das placas de linha (como discutido mais cedo neste papel), há dois grupos de ASIC, do GE e do 10/100 ASIC. Um GE ASIC existe para quatro 10/100 ASIC. Cada 10/100 ASIC apoiam 12 10/100 das portas. Os CHUIS configuram o GE ASIC. Assim, ao aplicar a configuração de QoS a 10/100 das placas de linha através das BOBINAS, a configuração aplica a todas as 48 10/100 portas.

Ao permitir o apoio das BOBINAS emitindo o **comando set qos policy-source cops**, a configuração de QoS através das BOBINAS é aplicada a todos os ASIC no chassi do switch. É possível aplicar a configuração das BOBINAS aos ASIC específicos. Isto pode ser consegue usando o comando seguinte:

```
Console> (enable) set port qos 5/4 policy-source cops
!-- QoS policy source set to COPS for port (s) 5/1-4. Console> (enable)
```

No aplicativo, você pode ver que o comando acima foi emitido em um módulo GE, uma vez que quatro portas foram afetadas por ele.

Policy Decision Point Servers e Domain Name

O Policy Decision Point Servers (PDPS) é os gerenciadores de política externa usados para armazenar os detalhes da configuração de QoS que são abaixados para o interruptor. Se as BOBINAS são permitidas no interruptor, o interruptor deve ser configurado com o endereço IP de Um ou Mais Servidores Cisco ICM NT do gerenciador externo que fornecerá detalhes da configuração de QoS ao interruptor. É semelhante a quando o SNMP está ativado e o endereço IP do gerenciador de SNMP está definido.

O comando para identificar o PDPS externo é feito com o uso de:

```
Console> (enable) set cops server 192.168.1.1 primary
!-- 192.168.1.1 is added to the COPS diff-serv server table as primary server. !-- 192.168.1.1
is added to the COPS rsvp server table as primary server. Console> (enable)
```

O comando acima identifica o dispositivo 192.168.1.1 como servidor de ponto de decisão principal.

Quando o interruptor se comunica com o PDPS, precisa de ser parte de um domínio definido no PDPS. O PDPS falará somente ao Switches que o formulário parte de seu domínio definido assim que o interruptor deve ser configurado para identificar o domínio das BOBINAS a que pertence. Isso é feito pela emissão do seguinte comando:

```
Console> (enable) set cops domain name remote-cat6k
!-- Domain name set to remote-cat6k. Console> (enable)
```

O comando acima mostra o interruptor como sendo configurado para ser parte do domínio nomeado remote-cat6k. Este domínio deve ser definido no QPM e o interruptor deve ser

adicionado a esse domínio.

Informações Relacionadas

- Suporte ao Produto - Switches
- Suporte de tecnologia de switching de LAN
- Suporte Técnico e Documentação - Cisco Systems
