Troubleshooting de QoS dos Catalyst 6500 Switch

Índice

Introdução

Este documento contém as etapas básicas de troubleshooting, as limitações da Qualidade de Serviço (QoS) e fornece informações para resolver problemas de questões de QoS comuns nos Catalyst 6500 Switches. Este documento também discute os problemas de QoS que ocorrem na classificação e a marcação e o policiamento.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

A informação neste documento é baseada nos Catalyst 6500 Series Switch.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

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

Informações de Apoio

QoS é uns recursos de rede para classificar o tráfego e para proporcionar serviços de entrega determinísticas. Estes artigos explicam as várias etapas no processo de QoS:

- **Programação da entrada** — É segurada pela porta de hardware ASIC e é uma operação de QoS da camada 2. Não exige um Policy Feature Card (PFC).
- **Classificação** — É segurada pelo supervisor e/ou pelo PFC através do motor do Access Control List (ACL). O supervisor segura a operação de QoS da camada 2. O PFC segura a operação de QoS da camada 2 e da camada 3.
- **Policiar** — É segurado pelo PFC através do Engine de encaminhamento de camada 3. O PFC é exigido e segura a operação de QoS da camada 2 e da camada 3.
- **Reescrita do pacote** — É segurada pela porta de hardware ASIC. É uma operação de QoS da camada 2 e da camada 3 baseada na classificação feita previamente.
- **Programação de emissor** — É segurada pela porta de hardware ASIC. É uma operação de QoS da camada 2 e da camada 3 baseada na classificação feita previamente.

Pesquise defeitos QoS

Trabalhos de QoS diferentemente nos Catalyst 6500 Switch do que no Roteadores. A arquitetura de QoS é bastante complexa nos Catalyst 6500 Switch. Recomenda-se que você compreende o Multilayer Switch Feature Card (MSFC), o PFC, e a arquitetura do Supervisor Engine no Catalyst 6500. A configuração de QoS no Hybrid OS precisa mais compreensão da funcionalidade de Cactos da camada 2 e da camada 3 MSFC com funcionalidade de Cisco IOS®. Recomenda-se ler estes documentos detalhados antes que você configure QoS:

- Configurando PFC QoS - Native IOS
- Configurando QoS - Cactos

Procedimento de Troubleshooting Passo a Passo

Esta seção contém o procedimento básico do Troubleshooting passo a passo para QoS a fim isolar a edição para um Troubleshooting mais adicional.

1. **Permita QoS — O comando show mls qos** mostra as estatísticas de policiamento e o estado de QoS, se permitido ou desabilitado.`Switch#`**`show mls qos QoS is enabled globally QoS ip`**

packet dscp rewrite enabled globally Input mode for GRE Tunnel is Pipe mode Input mode for MPLS is Pipe mode Vlan or Portchannel(Multi-Earl)policies supported: Yes Egress policies supported: Yes ----- Module [5] ----- QoS global counters: Total packets: 244 IP shortcut packets: 0 **Packets dropped by policing: 0 IP packets with TOS changed by policing: 5 IP packets with COS changed by policing: 4** Non-IP packets with COS changed by policing: 0 MPLS packets with EXP changed by policing: 0

2. **Classificação do tráfego de entrada usando a porta da confiança** — Esta classificação categoriza o tráfego de entrada em um dos sete valores do Classe de serviço (CoS). O tráfego de entrada pode ter o valor de CoS já atribuído pela fonte. Neste caso, você precisa de configurar a porta para confiar o valor de CoS do tráfego de entrada. A confiança permite o interruptor de manter o CoS ou os valores do Tipo de serviço (ToS) do frame recebido. Este comando mostra como verificar o port trust state:Switch#**show queueing int fa 3/40** Port QoS is enabled **Trust state: trust CoS** Extend trust state: not trusted [CoS = 0] Default CoS is 0 *!--- Output suppressed.* O valor de CoS é levado somente pelo Inter-Switch Link (ISL) e pelos quadros do dot1q. Os frames sem etiqueta não levam valores de CoS. Os frames sem etiqueta levam os valores ToS que são derivados da Precedência IP ou do Differentiated Services Code Point (DSCP) do cabeçalho do pacote IP. A fim confiar o valor ToS, você precisa de configurar a porta para confiar a Precedência IP ou o DSCP. O DSCP é inverso - compatível à Precedência IP. Por exemplo, se você configurou uma porta de switch como a porta da camada 3, não leva o dot1q ou os quadros ISL. Neste caso, você precisa de configurar esta porta para confiar o DSCP ou a Precedência IP.Switch#**show queueing interface gigabitEthernet 1/1** Interface GigabitEthernet1/1 queueing strategy: Weighted Round-Robin Port QoS is enabled **Trust state: trust DSCP** Extend trust state: not trusted [COS = 0] Default CoS is 0 *!--- Output suppressed.*
3. **Classificação do tráfego de entrada usando o ACL e os ACE** — você pode igualmente configurar o interruptor para classificar e marcar o tráfego. As etapas incluídas para configurar a classificação e marcação são: crie listas de acesso, mapa de classe, e mapa de política, e emita o comando da **entrada de política de serviço** a fim aplicar o mapa de política na relação. Você pode verificar as estatísticas do mapa de política como mostrado aqui:Switch#**show policy-map interface fa 3/13** FastEthernet3/13 Service-policy input: pqos2 class-map: qos1 (match-all) Match: access-group 101 set precedence 5: Earl in slot 5 : 590 bytes **5 minute offered rate 32 bps aggregate-forwarded 590 bytes** Class-map: class-default (match-any) 36 packets, 2394 bytes 5 minute offered rate 0 bps, drop rate 0 bps Match: any Switch#**show mls qos ip ingress** QoS Summary [IPv4]: (* - shared aggregates, Mod - switch module) Int Mod Dir Class-map DSCP Agg Trust Fl AgForward-By AgPoliced-By Id Id ---------- ---------- **Fa3/13 5 In qos1 40 1 No 10 590 0** All 5 - Default 0 0* No 0 365487 0 Observe que os contadores AgForward-por aquele correspondem aos aumentos do mapa de classe qos1. Se você não vê as estatísticas para o mapa de classe correspondente, verifique a lista de acesso anexada ao mapa de classe.
4. **Programação da entrada** — O PFC não é exigido configurar para entrar a programação. Você não pode configurar os comandos do **limiar de queda dos qos do ponto inicial** ou do **grupo da RCV-fila em uma** única 10/100 de porta. Isto é porque a programação da entrada é segurada pelas portas da bobina ASIC que contêm doze 10/100 das portas. Consequentemente, você tem que configurar a programação da entrada nos grupos de 12 portas, tais como 1-12, 13-24, 25-36, 37-48.A arquitetura de enfileiramento é construída no ASIC e não pode ser reconfigurada. Emita a **/porta do entalhe dos FastEthernet da interface de enfileiramento da mostra | inclua o comando type** ver a estrutura da fila de uma porta de LAN.Switch#**show queueing interface fastEthernet 3/40** Queueing Mode In Rx direction: mode-cos **Receive queues [type = 1q4t]:** <--------- 1 Queue 4 Threshold Queue Id Scheduling Num of thresholds --- 1 Standard 4 queue tail-drop-thresholds ------------------------- **1 50[1] 60[2] 80[3] 100[4]** <------ Threshold levels 50%, 60%, 80% and 100% **Packets dropped on Receive: BPDU packets: 0 queue thresh dropped**

[cos-map] ---------- **1 1 0 [0 1] 1 2 0 [2 3] 1 3 0 [4 5] 1 4 0 [6 7]** *!--- Output suppressed.* Àrevelia, todos os 4 pontos iniciais são 100%. Você pode emitir o comando do *<Threshold 14> do <Threshold 3> do <Threshold 2> do <Threshold 1> de Id> do <Queue do* **ponto inicial da RCV-fila** a fim configurar os níveis de ponto inicial. Desta maneira, os dados mais altos dos valores de CoS não estão deixados cair antes que uns mais baixos dados do valor de CoS durante a congestão.`Switch(config)#`**`interface range fa 3/37 - 48`** `Switch(config-if-range)#`**`rcv-queue threshold 1 50 60 80 100`**

5. **Traçar** — Se a porta é configurada para confiar o CoS, a seguir use a tabela de mapa CoS-DSCP a fim traçar o valor recebido de CoS em um valor DSCP interno.`Switch#`**`show mls qos maps cos-dscp`** `Cos-dscp map: cos: 0 1 2 3 4 5 6 7 ---------- dscp: 0 8 16 24 32 40 48 56` Se a porta é configurada para confiar a Precedência IP da confiança, a seguir use a tabela de mapa IP-prec-DSCP a fim traçar o valor de precedência IP recebido em um valor DSCP interno.`Switch#`**`show mls qos maps ip-prec-dscp`** `IpPrecedence-dscp map: ipprec: 0 1 2 3 4 5 6 7 ---------- dscp: 0 8 16 24 32 40 48 56` Se a porta é configurada para confiar o DSCP, a seguir o valor recebido DSCP está usado como o valor DSCP interno.Estas tabelas devem ser mesmas em todo o Switches em sua rede. Se qualquer do Switches tem uma tabela com mapeamentos diferentes, você não recebe o resultado desejado. Você pode mudar estes valores da tabela como mostrado aqui:`Switch(config)#`**`mls qos map cos-dscp 0 8 16 24 40 48 48 56`** `Switch(config)#`**`mls qos map ip-prec-dscp 0 8 16 24 40 48 48 56`**
6. **Policiamento** — Há dois tipos de policiamento disponíveis nos Catalyst 6500 Switch:**Policiamento agregado** — Controles de policiamento agregados a largura de banda de um fluxo no interruptor. **O comando mls qos aggregate policer da mostra** mostra todo o policer agregado configurado configurado no interruptor. Estas são as estatísticas de policiamento:`Switch#`**`show mls qos ip fastEthernet 3/13`** `[In] Policy map is pqos2 [Out] Default. QoS Summary [IPv4]: (* - shared aggregates, Mod - switch module) Int Mod Dir Class-map DSCP Agg Trust Fl AgForward-By AgPoliced-By Id Id ---------- ---------- Fa3/13 5 In qos1 0` **`1*`** `dscp 0 10626` **`118860`** `Fa3/13 5 In class-defa 40 2 No 0 3338 0 Switch#`**`show mls qos`** `QoS is enabled globally QoS ip packet dscp rewrite enabled globally Input mode for GRE Tunnel is Pipe mode Input mode for MPLS is Pipe mode Vlan or Portchannel(Multi-Earl) policies supported: Yes Egress policies supported: Yes ----- Module [5] ----- QoS global counters: Total packets: 163 IP shortcut packets: 0` **`Packets dropped by policing: 120`** `IP packets with TOS changed by policing: 24 IP packets with COS changed by policing: 20 Non-IP packets with COS changed by policing: 3 MPLS packets with EXP changed by policing: 0`**Vigilância de microfluxo** — Largura de banda dos controles de vigilância de microfluxo de um fluxo pela relação no interruptor. À revelia, tráfego roteado da influência das vigilâncias de microfluxo somente. Emita o comando **construído uma ponte sobre qos dos mls na** interface de VLAN a fim permitir a vigilância de microfluxo para o tráfego interligado. Esta é a verificação das estatísticas de vigilância de microfluxo:`Switch#`**`show mls ip detail`** `Displaying Netflow entries in Supervisor Earl DstIP SrcIP Prot:SrcPort:DstPort Src i/f :AdjPtr ---------- ---------- ---------- ---------- ---------- Pkts Bytes Age LastSeen Attributes ---------- ---------- ---------- Mask Pi R CR Xt Prio Dsc IP_EN OP_EN Pattern Rpf FIN_RDT FIN/RST ----+--+-+--+--+----+---+-----+-----+-------+---+-------+------- Ig/acli Ig/aclo Ig/qosi Ig/qoso Fpkt Gemini MC-hit Dirty Diags -------+-------+-------+-------+----+------+------+----+------ QoS Police Count Threshold Leak Drop Bucket Use-Tbl Use-Enable -----------+---------+---------+----------+----+-------+-------+----------+ 10.175.50.2 10.175.51.2 icmp:8 :0 -- :0x0 43 64500 84 21:37:16 L3 - Dynamic 1 1 0 0 1 0 0 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0x0 0 0 0 NO` **`1518`** `NO NO 10.175.50.2 10.175.51.2 icmp:0 :0 -- :0x0 43 64500 84 21:37:16 L3 - Dynamic 1 1 0 0 1 0 0 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0x0 664832 0 0 NO` **`1491`** `NO NO 0.0.0.0 0.0.0.0 0 :0 :0 -- :0x0 1980 155689 1092 21:37:16 L3 - Dynamic 0 1 0 0 1 0 0 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0x0 0 0 0 NO 0 NO NO Switch#`**`show mls qos`** `QoS is enabled globally QoS ip packet dscp rewrite enabled globally Input mode for GRE Tunnel is Pipe mode Input`

```
mode for MPLS is Pipe mode Vlan or Portchannel(Multi-Earl) policies supported: Yes Egress
policies supported: Yes ----- Module [5] ----- QoS global counters: Total packets: 551 IP
shortcut packets: 0 Packets dropped by policing: 473 IP packets with TOS changed by
policing: 70 IP packets with COS changed by policing: 44 Non-IP packets with COS changed by
policing: 11 MPLS packets with EXP changed by policing: 0
```

Nota: *O tipo modificação dos* **qos IP dos mls da mostra***/comando number* não mostra as estatísticas de vigilância de microfluxo. Mostra somente o agregado que policia estatísticas.Se você não vê as estatísticas de policiamento desejadas, verifique a configuração de vigilância. Refira o Regulamentação QoS no Catalyst 6500/6000 series switch para ver o exemplo de configuração. Também, veja as diretrizes QoS e as limitações na seção dos Catalyst 6500 Switch deste documento.

7. Verifique os Release Note de sua versão de OS e certifique-se que não há nenhum erro relativo a sua configuração de QoS.
8. Note seu modelo do supervisor do interruptor, modelo PFC, modelo MSFC e versão de Cisco IOS/Cactos. Veja as diretrizes QoS e as limitações em Catalyst 6500 Switch com referência a suas especificações. Certifique-se que sua configuração é aplicável.

Diretrizes QoS e limitações em Catalyst 6500 Switch

Há as limitações de QoS de que você precisa de estar ciente antes que você configure QoS em Catalyst 6500 Switch:

- Diretrizes gerais
- Diretrizes PFC3
- Diretrizes PFC2
- Limitações do comando class map
- Limitações do comando do mapa de política
- Limitações do comando class do mapa de política
- Diretrizes e limitações do mapeamento da fila e do limiar de queda
- trust-cos nas limitações de entrada do ACL
- Limitações das placas de linha WS-X6248-xx, WS-X6224-xx e WS-X6348-xx
- O PFC ou o PFC2 não fornecem QoS para o tráfego MACILENTO. Com PFC ou PFC2, o PFC QoS não muda o byte ToS no tráfego MACILENTO.
- O tráfego de LAN do ingresso que é a camada 3 comutada não atravessa o MSFC ou o MSFC2 e retém o valor de CoS que é atribuído pelo motor do switching da camada 3.
- QoS não executa a fuga de congestionamento da porta de ingresso nas portas que são configuradas com o **não-confiável**, **Trust-ipprec**, ou palavras-chaves do **Trust-dscp**. O tráfego vai diretamente ao mecanismo de switching.
- O interruptor usa o ponto inicial da queda traseira para o tráfego que leva os valores de CoS que são traçados somente à fila. O interruptor usa os limiares de queda WRED para o tráfego que leva os valores de CoS que são traçados à fila e a um ponto inicial.
- A classificação com um motor do switching da camada 3 usa a camada 2,3, e 4 valores. A marcação com um motor do switching da camada 3 usa os valores de CoS da camada 2 e a Precedência IP da camada 3 ou valores DSCP.
- Um Trust-cos ACL não pode restaurar o CoS recebido no tráfego das portas não-confiável. O tráfego das portas não-confiável tem sempre o valor de CoS da porta.

Nota: O PFC QoS não detecta o uso de comandos unsupported até que você anexe um mapa de política a uma relação.

Limitação de QoS_TCAM

O CAM ternário (TCAM) é uma parte especializada de memória projetada para consultas da tabela rápidas, com base nos pacotes que passam através do interruptor, executado pelo Engine de ACL no PFC, no PFC2, e no PFC3. Os ACL são processados no hardware nos Cisco Catalyst 6500 Series Switch que são chamados TCAM. Quando você configura o ACL, trace o ACL ao QoS e quando você aplica a política de QoS na relação, o interruptor programa o TCAM. Se você tem utilizado já todo o espaço disponível TCAM no interruptor para o QoS, você encontra este Mensagem de Erro:

```
Switch(config)#interface vlan 52 Switch(config-if)#service-policy input test Switch(config-if)#
3w0d: %QM-4-TCAM_ENTRY: Hardware TCAM entry capacity exceeded
```

Estas saídas do **comando count do tcam da mostra** mostram que as máscaras da entrada de TCAM são 95% usados. Devido a isto, quando você aplica a política de QoS na relação você encontra o `%QM-4-TCAM_ENTRY:` mensagem de erro.

```
Switch#show tcam count Used Free Percent Used Reserved ---- ---- ------------ --------
Labels:(in) 43 4053 1 Labels:(eg) 2 4094 0 ACL_TCAM -------- Masks: 19 4077 0 72 Entries: 95
32673 0 576 QOS_TCAM -------- Masks: 3902 194 95 18 Entries: 23101 9667 70 144 LOU: 0 128 0
ANDOR: 0 16 0 ORAND: 0 16 0 ADJ: 3 2045 0
```

As entradas de TCAM e as etiquetas ACL são recursos limitados. Consequentemente, segundo sua configuração ACL, você pôde precisar de ser cuidadoso não esgotar os recursos disponíveis. Além, com grandes configurações de QoS ACL e de VLAN Access Control List (VACL), você igualmente pôde precisar de considerar o espaço permanente da memória de acesso aleatório (NVRAM). Os recursos do hardware disponíveis diferem no supervisor 1a com PFC, no supervisor 2 com PFC2, e no supervisor 720 com PFC3.

Módulo do supervisor	QoS TCAM	Etiquetas ACL
Supervisor 1a e PFC	máscaras 2K e testes padrões 16K compartilhados entre listas de controle de acesso do roteador (rACLs), VACL e QoS ACL	512 etiquetas ACL compartilhadas entre o rACLs, os VACL, e o QoS ACL
Supervisor 2 e PFC2	máscaras 4K e testes padrões 32K para QoS ACL	512 etiquetas ACL compartilhadas entre o rACLs, os VACL, e o QoS ACL
Supervisor 720 e PFC3	máscaras 4K e testes padrões 32K para QoS ACL	512 etiquetas ACL compartilhadas entre o rACLs, os VACL, e o QoS ACL

Nota: Independente do limite da etiqueta de 512 ACL, há um limite de software adicional em Cisco Cactos de 250 QoS ACL sistema-largo quando você usa o modo de configuração (binário) do padrão. Esta limitação é removida no modo da configuração de texto. Emita o **comando set config mode text** a fim mudar o modo de configuração ao modo de texto. O modo de texto usa tipicamente menos NVRAM ou espaço de memória flash do que o que o modo da configuração binária usa. Você deve emitir o **comando write memory** quando você se operar no modo de texto

a fim salvar a configuração no NVRAM. Emita o **comando set config mode text auto-save** a fim salvar automaticamente a configuração de texto no NVRAM.

Esta é a ação alternativa para a edição TCAM:

- Se você executou o **comando service-policy em** muitas interfaces de camada 2 que pertencem a um VLAN, você pode executar o policiamento baseado VLAN em vez da porta de switch baseada. Este é um exemplo:`Switch(config)#interface range fastethernet x/y - z Switch(config-if)#mls qos vlan-based Switch(config-if)#exit Switch(config)#interface vlan 100 Switch(config-if)#service-policy input Test_Policy`
- Estatísticas da marcação de QoS do desabilitação. **Nenhum qos dos mls que marca o comando statistics** não permite que o máximo de 1020 AgIDs seja executado. Isto é porque atribui o vigilante do padrão para vigilantes do dscp do grupo. O downside deste não é lá é nenhuma estatística para o vigilante específico porque toda compartilha do vigilante do padrão.`Switch(config)#no mls qos marking statistics`
- Se possível, use os mesmos ACL através das interfaces múltiplas a fim reduzir a disputa dos recursos TCAM.

Limitação NBAR

O Network-Based Application Recognition (NBAR) é um Engine de classificação que reconheça uma ampla variedade de aplicativos, que inclua com base na Web e outro difícil-à-classifique os protocolos que utilizam atribuições de porta dinâmicas TCP/UDP. Quando um aplicativo é reconhecido e classificado pelo NBAR, uma rede pode invocar serviços para esse aplicativo específico. O NBAR classifica pacotes e aplica então QoS ao tráfego classificado a fim assegurar-se de que a largura de banda de rede esteja usada eficientemente. Há algumas limitações em como executar QoS quando você usa o NBAR:

- O PFC3 não apoia o NBAR.
- Com um Supervisor Engine 2, um PFC2, e um MSFC2:Você pode configurar o NBAR em relações da camada 3 em vez de PFC QoS.O PFC2 fornece o suporte a hardware para entradas ACL nas portas onde você configura o NBAR.Quando o PFC QoS for permitido, o tráfego através das portas onde você configura passagens NBAR através do ingresso e as filas e os limiares de queda da saída.Quando o PFC QoS é permitido, o MSFC2 ajusta a saída CoS igual à Precedência IP da saída no tráfego NBAR.Afinal o tráfego passa através de uma fila do ingresso, ele é processado no software no MSFC2 nas relações onde você configura o NBAR.

O mapa COS comanda desaparecidos no supervisor 2

Sob os software release 12.1(8a)EX-12.1(8b)EX5 e 12.1(11b)E do Native IOS e mais tarde, os CoS-mapeamentos de QoS do padrão para os uplinks do gigabit situados no Supervisor2 mudaram. Todos os valores de CoS foram atribuídos para enfileirar 1 e ponto inicial 1, e não podem ser mudados.

Estes comandos não podem ser configurados em uma porta de uplink de gigabit de Sup2 nestas liberações:

```
rcv-queue cos-map priority-queue wrr-queue cos-map
```

As configurações de QoS são limitadas, e a fila de prioridade estrita não pode ser utilizada. Isto afeta somente as portas de gigabit situadas fisicamente no motor do supervisor 2. As portas de gigabit em outros módulos da placa de linha não são afetadas.

Há uma upgrade de firmware que resolva esta edição. Esta elevação pode ser feita através do software. Suporte técnico do contato se uma upgrade de firmware é exigida. Note que uma upgrade de firmware está precisada somente se a versão do HW do Supervisor2 é menos de 4.0. Se a versão do HW do Supervisor2 está 4.0 ou mais atrasada, QoS deve ser permissível nas portas de uplink de gigabit sem a upgrade de firmware. Você pode emitir o **comando show module** a fim encontrar o nível de firmware. Esta edição é identificada na identificação de bug Cisco CSCdw89764 (clientes registrados somente).

Limitações da Serviço-política

A fim aplicar o mapa de política à relação, emita o **comando service-policy**. Se você tem um comando unsupported no mapa de política, depois que você o aplica com o **comando service-policy**, o interruptor alerta os Mensagens de Erro no console. Estes pontos precisam de ser considerados quando você pesquisar defeitos problemas relacionados da serviço-**política**.

- Não anexe uma política de serviços a uma porta que seja um membro de um EtherChannel.
- Com os cartões de transmissão distribuídos (DFC) instalados, o PFC2 não apoia QoS com base em VLAN. Você não pode emitir o **comando mls qos vlan-based** ou anexar políticas de serviços às interfaces de VLAN.
- O PFC QoS apoia a palavra-chave da saída somente com PFC3 e somente em relações da camada 3 (as portas de LAN configuradas como relações da camada 3 ou as interfaces de VLAN). Com PFC3, você pode anexar uma entrada e um mapa da política emissora a uma relação da camada 3.
- O PFC com base em VLAN ou com base na porta QoS nas portas da camada 2 não é relevante às políticas anexadas para mergulhar 3 relações com a palavra-chave da saída.
- As políticas anexadas com a palavra-chave da saída não apoiam a vigilância de microfluxo.
- Você não pode anexar um mapa de política que configura um estado de confiança com a saída do **comando service-policy**.
- O PFC QoS não apoia o markdown do ingresso com gota da saída ou gota do ingresso com markdown da saída.

As indicações da saída da Serviço-política não aparecem na saída do comando running-config

Quando você configura QoS no multilink no módulo FlexWAN, você não pode ver o **comando service-policy** output na saída do **comando show running-config**. Isto ocorre quando o interruptor executa versões do Cisco IOS mais cedo do que 12.2SX. O FlexWAN para o Cisco 7600 Series apoia o dLLQ em relações do NON-pacote. Não suporta dLLQ em interfaces de pacotes MLPPP. Tal apoio está disponível com Cisco IOS Software Release 12.2S.

A ação alternativa para contornear esta limitação é anexar a serviço-política às relações unbundled ou promover a versão do Cisco IOS a 12.2SX ou a mais tarde, onde a característica é apoiada.

Policiando a limitação

Policiar é executado no hardware no PFC sem o impacto do desempenho do interruptor. Policiar não pode ocorrer na plataforma 6500 sem PFC. No Hybrid OS, policiar deve ser configurado no Cactos. Estes pontos precisam de ser considerados quando você pesquisar defeitos questões de vigilância:

- Quando você aplica o ingresso que policia e a saída que policia ao mesmo tráfego, a política de entrada e a política emissora deve marcar abaixo do tráfego ou do tráfego da gota. O PFC QoS não apoia o markdown do ingresso com gota da saída ou gota do ingresso com markdown da saída.
- Quando você criar um vigilante que não use a palavra-chave do pir e o parâmetro dos maximum_burst_bytes é igual ao parâmetro dos normal_burst_bytes (que é o caso se você não incorpora o parâmetro dos maximum_burst_bytes), a ação em excesso policiar-DSCP-transmite a causa PFC QoS das palavras-chaves para marcar para baixo o tráfego como definido pelo mapa de promoção da intermitência máx. policiar-DSCP.
- Quando a ação excedada é gota, o PFC QoS ignora todo o violate action configurado.
- Quando você configura a gota como a conform action, o PFC QoS configura a gota como a ação excedada e o violate action.
- As exigências da máscara de fluxo da vigilância de microfluxo, do Netflow, e da exportação de dados de Netflow (NDE) puderam opor.

Taxa-limite ou questões de vigilância com o MSFC no Hybrid OS

Nos Catalyst 6500 Switch que executam o Hybrid OS, a configuração do taxa-limite não dá a saída desejada. Por exemplo, se você configura o **comando rate-limit** sob o **comando interface vlan no** MSFC, não faz realmente taxa-limite o tráfego.

```
interface Vlan10
 rate-limit input 256000 2000 2000 conform-action transmit exceed-action drop
 rate-limit output 256000 2000 2000 conform-action transmit exceed-action drop
```

Ou:

```
interface Vlan10
service-policy input Test_Policy
```

A razão atrás desta é que o MSFC toma somente de funções de controle, mas o encaminhamento de tráfego real ocorre em PFC ASIC no supervisor. O MSFC compila MENTIR e as tabelas de adjacência, assim como a outra informação de controle, e transfere-o ao PFC para executar no hardware. Com a configuração você criou, você taxa-limite somente o tráfego comutado do software, que deve ser mínimo (ou nenhum).

A ação alternativa é usar o comando line interface(cli) de Cactos a fim configurar o taxa-limite no supervisor. Refira Cactos QoS para a explicação detalhada de como configurar o Regulamentação QoS em Cactos. Você pode igualmente referir o Regulamentação QoS no Catalyst 6500/6000 series switch para ver o exemplo de configuração.

Média do comando shape não apoiada nas interfaces de VLAN do Cisco 7600

Quando você aplica uma entrada de política de serviço a uma relação no Cisco 7600, este Mensagem de Erro aparece:

```
7600_1(config)#int Gi 1/40 7600_1(config-if)#service-policy input POLICY_1 shape average command
is not supported for this interface
```

O comando **médio da forma** não é apoiado para as interfaces de VLAN no Cisco 7600. Em lugar de você precisa de usar o policiamento.

```
7600_1(config)#policy-map POLICY_1 7600_1(config-pmap)#class TRAFFIC_1 7600_1(config-pmap-c)#police <x> <y> conform-action transmit exceed-action drop
```

Refira configurar a classe do mapa de política que policia para obter mais informações sobre de como executar o policiamento do tráfego do taxa-limite.

Enquanto você anexa esta serviço-política a uma interface de VLAN (SVI), você precisa de permitir QoS com base em VLAN no todo o aqueles as portas da camada 2 que pertencem a este VLAN em que você quer este mapa de política ser aplicado.

```
7600_1(config)#interface Gi 1/40 7600_1(config-if)#mls qos vlan-based
```

Refira a possibilidade de PFC com base em VLAN QoS em portas de LAN da camada 2 para mais informação.

QoS-ERRO: A adição/alteração fez ao [chars] do policymap e a classe que o [chars] é inválido, comando é rejeitada

```
QoS-ERROR: Addition/Modification made to policymap vtc-map and class voice-video is not valid, command is rejected
```

Este Mensagem de Erro indica que as ações definidas na classe mencionada não estão permitidas nos Cisco Catalyst 6500 Series Switch. Há algumas limitações durante a configuração das ações de classe do mapa de política.

- Você não pode fazer todos os três destes em uma classe do mapa de política:Marque o tráfego com os **comandos set**Configurar o estado de confiançaPoliciamento ConfigureVocê pode somente um ou outro tráfego da marca com os **comandos set**.OUConfigurar o estado de confiança e/ou configurar o policiamento.
- Para o tráfego comutado por hardware, o PFC QoS não apoia a **largura de banda**, **prioridade**, fila-**limite**, ou aleatório-**detecte** comandos class do mapa de política. Você pode configurar estes comandos porque podem ser usados para o tráfego comutado por software.
- O PFC QoS não apoia os comandos class do mapa de política do qos-**grupo do grupo**.

Refira configurar ações de classe do mapa de política para obter mais informações sobre de tais limitações.

Informações Relacionadas

- Classificação de QoS e marcação no Catalyst 6500/6000 series switch que executa o Cisco IOS Software
- Programação de emissor de QoS no Catalyst 6500/6000 series switch que executa o software do sistema do Cisco IOS
- Vigilância de QoS nos Switches das Séries Catalyst 6500/6000
- Classificação e Marcação QoS nos Switches da Série catalyst 6500/6000 que Executam o Software CatOs
- Programação da saída de QoS nos Switches da série Catalyst 6500/6000 executando o Software do sistema CatOS
- Páginas de Suporte de Produtos de LAN
- Página de suporte da switching de LAN

- Suporte Técnico e Documentação - Cisco Systems