Solução de problemas de QoS dos switches Catalyst 6500

Contents

Introduction

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.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas nos Catalyst 6500 Series Switches.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

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

Informações de Apoio

A QoS é um recurso de rede para classificar o tráfego e fornecer serviços determinísticos de entrega. Estes itens explicam as várias etapas no processo de QoS:

- **Programação de entrada** — é tratada por ASICs de porta de hardware e é uma operação de QoS de Camada 2. Ele não exige uma Placa de Recurso de Política (PFC - Policy Feature Card).
- **Classificação**—É tratado pelo supervisor e/ou PFC através do mecanismo da Lista de Controle de Acesso (ACL - Access Control List). O supervisor lida com a operação de QoS da camada 2. A PFC trata da operação de QoS da Camada 2 e da Camada 3.
- **Policiamento** — é tratado pelo PFC através do mecanismo de encaminhamento da Camada 3. A PFC é necessária e trata da operação de QoS de Camada 2 e Camada 3.
- **Reescrita de pacote** — é tratada por ASICs de porta de hardware. É uma operação de QoS de Camada 2 e Camada 3 baseada na classificação feita anteriormente.
- **Programação de saída** — é tratada por ASICs de porta de hardware. É uma operação de QoS de Camada 2 e Camada 3 baseada na classificação feita anteriormente.

Solucionar problemas de QoS

A QoS funciona de forma diferente nos Switches Catalyst 6500 do que nos roteadores. A arquitetura de QoS é bastante complexa nos Switches Catalyst 6500. Recomenda-se que você entenda a arquitetura da placa de recurso do switch multicamada (MSFC), PFC e do mecanismo supervisor no Catalyst 6500. A configuração da QoS no SO híbrido precisa de mais compreensão da funcionalidade CatOS da Camada 2 e da MSFC da Camada 3 com a funcionalidade do Cisco IOS®. Recomenda-se ler estes documentos em detalhes antes de configurar a QoS:

- Configuração da QoS de PFC - IOS nativo
- Configurando QoS - CatOS

Procedimento de Troubleshooting Passo a Passo

Esta seção contém o procedimento básico de solução de problemas passo a passo para QoS a fim isolar o problema para Troubleshooting adicional.

1. **Ativar QoS**—O **comando show mls qos** mostra as estatísticas de vigilância e o status da QoS, habilitada ou desabilitada.

```
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 confiável** — Essa classificação categoriza o tráfego de entrada em um dos sete valores de Classe de Serviço (CoS - Class of Service). O tráfego de entrada pode ter o valor de CoS já atribuído pela origem. Nesse caso, você precisa configurar a porta para confiar no valor de CoS do tráfego de entrada. A confiança permite que o switch mantenha os valores de CoS ou tipo de serviço (ToS) do quadro recebido. Este comando mostra como verificar o estado de confiança da porta:

```
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 transportado somente por quadros Inter-Switch Link (ISL) e dot1q. Os quadros não marcados não transportam valores de CoS. Os quadros não marcados transportam valores de ToS derivados de precedência de IP ou de DSCP (Differentiated Services Code Point, ponto de código de serviços diferenciados) do cabeçalho do pacote IP. Para confiar no valor ToS, você precisa configurar a porta para confiar na precedência IP ou no DSCP. O DSCP é compatível com a precedência de IP. Por exemplo, se você configurou uma porta de switch como porta de Camada 3, ela não transporta quadros dot1q ou ISL. Nesse caso, você precisa configurar essa porta para confiar em DSCP ou precedência de 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 ACL e ACEs**—Você também pode configurar o switch para classificar e marcar o tráfego. As etapas incluídas para configurar classificação e marcação são: crie listas de acesso, mapa de classe e mapa de política e emita o **comando service-policy input** para aplicar o mapa de política na interface. Você pode verificar as estatísticas do mapa de políticas 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-By** que correspondem a class-map qos1 aumentam. Se você não vir as estatísticas do mapa de classe correspondente, verifique a lista de acesso anexada ao mapa de classe.

4. **Programação de entrada** — a PFC não é necessária para configurar o agendamento de entrada. Você não pode configurar os comandos **rcv-queue threshold** ou **set qos drop-threshold** em uma única porta 10/100. Isso ocorre porque o agendamento de entrada é tratado por portas ASIC de bobina que contêm doze portas 10/100. Portanto, é necessário configurar o agendamento de entrada em conjuntos de 12 portas, como 1-12, 13-24, 25-36, 37-48.A arquitetura de enfileiramento é incorporada no ASIC e não pode ser reconfigurada. Emita o **comando show queueing interface fastethernet slot/port | include type** command para ver a estrutura da fila de uma porta 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.
```

Por padrão, todos os 4 limiares são 100%. Você pode executar o comando **rcv-queue**

threshold *<Queue Id> <Threshold 1> <Threshold 2> <Threshold 3> <Threshold 14> para configurar os níveis de limite.* Dessa forma, os dados de valores de CoS mais altos não são descartados antes dos dados de valor de CoS mais baixos durante o congestionamento.

```
Switch(config)#interface range fa 3/37 - 48
Switch(config-if-range)#rcv-queue threshold 1 50 60 80 100
```

5. **Mapeamento** —Se a porta estiver configurada para confiar no CoS, use a tabela de mapeamento CoS-DSCP para mapear o valor de CoS recebido em um valor de 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 estiver configurada para confiar na precedência de IP de confiança, use a tabela de mapa ip-prec-dscp para mapear o valor de precedência de IP recebido em um valor de 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 estiver configurada para confiar no DSCP, o valor de DSCP recebido será usado como o valor de DSCP interno.Essas tabelas devem ser iguais em todos os switches da rede. Se um dos switches tiver uma tabela com mapeamentos diferentes, você não receberá o resultado desejado. Você pode alterar estes valores de 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 Switches Catalyst 6500:**Política agregada** —A vigilância agregada controla a largura de banda de um fluxo no switch. O comando **show mls qos aggregate-policer** mostra todo o vigilante agregado configurado no switch. Estas são as estatísticas de vigilância:

```
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
```

Política de microfluxo —A vigilância de microfluxo controla a largura de banda de um fluxo por interface no switch. Por padrão, os vigilantes de microfluxo afetam somente o tráfego roteado. Emita o comando **mls qos bridged** na interface da VLAN para habilitar a vigilância de microfluxo para o tráfego de ponte. 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     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     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
```

Observação: o comando **show mls qos ip** *type mod/number* não mostra as estatísticas de vigilância de microfluxo. Mostra apenas as estatísticas de vigilância agregadas.Se você não vir as estatísticas de vigilância desejadas, verifique a configuração de vigilância. Consulte Política de QoS em Catalyst 6500/6000 Series Switches para ver o exemplo de

configuração. Além disso, consulte a seção Diretrizes e Limitações de QoS em Catalyst 6500 Switches deste documento.
7. Verifique as notas de versão da sua versão do SO e certifique-se de que não há bugs relacionados à sua configuração de QoS.
8. Observe o modelo de supervisor do switch, o modelo PFC, o modelo MSFC e a versão Cisco IOS/CatOS. Consulte as Diretrizes e Limitações de QoS nos Catalyst 6500 Switches com referência às suas especificações. Verifique se a sua configuração é aplicável.

Diretrizes e limitações de QoS em Switches Catalyst 6500

Há limitações de QoS que você precisa conhecer antes de configurar a QoS nos Switches Catalyst 6500:

- Diretrizes gerais
- Diretrizes de PFC3
- Diretrizes de PFC2
- Restrições de Comando do Mapa de Classe
- Restrições de Comando do Mapa de Política
- Restrições de Comando de Classe de Mapa de Política
- Diretrizes e restrições de mapeamento de limite de fila e queda
- trust-cos nas limitações de entrada do ACL
- Limitações das placas de linha WS-X6248-xx, WS-X6224-xx e WS-X6348-xx
- PFC ou PFC2 não fornecem QoS para o tráfego da WAN. Com PFC ou PFC2, a QoS da PFC não altera o byte ToS no tráfego da WAN.
- O tráfego de LAN de entrada que é comutado pela Camada 3 não passa pela MSFC ou pela MSFC2 e retém o valor de CoS atribuído pelo mecanismo de comutação da Camada 3.
- A QoS não implementa a prevenção de congestionamento de porta de entrada nas portas configuradas com as palavras-chave **não confiável**, **trust-ipprec** ou **trust-dscp**. O tráfego vai diretamente para o mecanismo de switching.
- O switch usa o limite de queda traseira para o tráfego que transporta os valores de CoS que são mapeados somente para a fila. O switch usa os limiares WRED-drop para o tráfego que transporta os valores de CoS que são mapeados para a fila e um limite.
- A classificação com um mecanismo de switching de Camada 3 usa os valores das Camadas 2, 3 e 4. A marcação com um mecanismo de switching de Camada 3 usa os valores de CoS de Camada 2 e a precedência de IP de Camada 3 ou os valores de DSCP.
- Uma ACL trust-cos não pode restaurar o CoS recebido no tráfego das portas não confiáveis. O tráfego das portas não confiáveis sempre tem o valor de CoS da porta.

Observação: a QoS de PFC não detecta o uso de comandos não suportados até que você anexe um mapa de política a uma interface.

Limitação de QoS_TCAM

O TCAM (Ternary CAM, ou CAM ternário) é uma memória especializada projetada para consultas rápidas em tabelas, com base em pacotes que passam pelo switch, executados pelo mecanismo da ACL em PFC, PFC2 e PFC3. As ACLs são processadas em hardware nos Cisco Catalyst 6500 Series Switches chamados de TCAM. Ao configurar a ACL, mapeie a ACL para a QoS e quando aplicar a política de QoS na interface, o switch programará a TCAM. Se você já tiver utilizado todo o espaço TCAM disponível no switch para o QoS, você encontrará esta 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
```

Esta saída do comando **show tcam count** mostra que as Máscaras de entrada TCAM são 95% usadas. Por causa disso, quando você aplica a política de QoS na interface, 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 TCAM e as etiquetas ACL são recursos limitados. Portanto, dependendo da configuração da ACL, talvez seja necessário ter cuidado para não esgotar os recursos disponíveis. Além disso, com grandes configurações de QoS ACL e VLAN Access Control List (VACL), talvez seja necessário considerar o espaço da memória de acesso aleatório não volátil (NVRAM). Os recursos de hardware disponíveis diferem no Supervisor 1a com PFC, Supervisor 2 com PFC2 e Supervisor 720 com PFC3.

Módulo Supervisor	TCAM de QoS	Rótulos ACL
Supervisor 1a e PFC	Máscaras de 2K e padrões de 16K compartilhados entre as RACLs (Router Access Control Lists, listas de controle de acesso do roteador), VACLs e ACLs de QoS	512 rótulos de ACL compartilhados entre RACLs, VACLs e ACLs de QoS
Supervisor 2 e PFC2	Máscaras de 4K e padrões de 32K para ACLs de QoS	512 rótulos de ACL compartilhados entre RACLs, VACLs e ACLs de QoS
Supervisor 720 e	Máscaras de 4K e padrões de 32K para ACLs de QoS	512 rótulos de ACL compartilhados entre RACLs, VACLs e

PFC3		ACLs de QoS

Observação: independente do limite de rótulo da ACL 512, há um limite de software adicional no Cisco CatOS de ACLs 250 QoS em todo o sistema quando você usa o modo de configuração padrão (binário). Essa restrição é removida no modo de configuração de texto. Execute o comando **set config mode text** para alterar o modo de configuração para o modo de texto. O modo de texto normalmente usa menos NVRAM ou espaço de memória Flash do que o modo de configuração binária usa. Você deve executar o comando **write memory** enquanto opera no modo de texto para salvar a configuração na NVRAM. Execute o comando **set config mode text autosave** para salvar a configuração de texto na NVRAM automaticamente.

Esta é a solução para o problema de TCAM:

- Se você implementou o comando **service-policy** em várias interfaces de Camada 2 que pertencem a uma VLAN, você pode implementar a vigilância baseada em VLAN em vez de baseada em porta do switch. 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
```

- Desabilitar estatísticas de marcação de QoS. O comando **no mls qos marking statistics** não permite a implementação do máximo de 1020 AgIDs. Isso ocorre porque ele aloca o vigilante padrão para definir os vigilantes dscp. O lado negativo disso é que não há estatísticas para o vigilante específico porque todos compartilham o vigilante padrão.
```
Switch(config)#no mls qos marking statistics
```

- Se possível, use as mesmas ACLs em várias interfaces para reduzir a contenção de recursos TCAM.

Limitação NBAR

O Network-Based Application Recognition (NBAR) é um mecanismo de classificação que reconhece uma grande variedade de aplicativos, incluindo protocolos baseados na Web e outros protocolos difíceis de classificar que utilizam atribuições de porta TCP/UDP dinâmicas. Quando um aplicativo é reconhecido e classificado pelo NBAR, uma rede pode invocar serviços para esse aplicativo específico. O NBAR classifica os pacotes e aplica a QoS ao tráfego classificado para garantir que a largura de banda da rede seja usada com eficiência. Há algumas restrições em como implementar a QoS quando você usa o NBAR:

- PFC3 não suporta NBAR.
- Com um Supervisor Engine 2, PFC2 e MSFC2:Você pode configurar o NBAR em interfaces de Camada 3 em vez de PFC QoS.O PFC2 fornece suporte de hardware para ACLs de entrada em portas nas quais você configura o NBAR.Quando a QoS de PFC está habilitada, o tráfego através das portas em que você configura o NBAR passa pelas filas de entrada e saída e limiares de queda.Quando a QoS de PFC está habilitada, a MSFC2 define o CoS de saída igual à precedência de IP de saída no tráfego NBAR.Depois que todo o tráfego passa por uma fila de ingresso, ele é processado no software no MSFC2 nas interfaces em que você configura o NBAR.

Os comandos cos-map ausentes no Supervisor 2

Nas Versões nativas do Software IOS 12.1(8a)EX-12.1(8b)EX5 e 12.1(11b)E e posteriores, os mapeamentos de CoS de QoS padrão para os uplinks Gigabit localizados no Supervisor2 foram alterados. Todos os valores de CoS foram atribuídos à fila 1 e ao limite 1 e não podem ser alterados.

Esses comandos não podem ser configurados em uma porta de uplink Gigabit Sup2 nessas versões:

```
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. Isso afeta apenas as portas Gigabit fisicamente localizadas no Supervisor 2 Engine. As portas Gigabit em outros módulos de placa de linha não são afetadas.

Há uma atualização de firmware que resolve esse problema. Essa atualização pode ser feita por meio de software. Entre em contato com o Suporte Técnico se for necessária uma atualização do firmware. Observe que uma atualização de firmware só é necessária se a versão de hardware do Supervisor2 for inferior a 4.0. Se a versão HW do Supervisor2 for 4.0 ou posterior, a QoS deve ser permitida nas portas de uplink Gigabit sem a atualização do firmware. Você pode executar o comando **show module** para localizar o nível de firmware. Esse problema é identificado na ID de bug da Cisco CSCdw89764 (somente clientes registrados) .

Limitações da política de serviço

Para aplicar o mapa de política à interface, emita o comando **service-policy**. Se você tiver um comando não suportado em policy-map, depois de aplicá-lo com o comando **service-policy**, o switch solicitará as mensagens de erro no console. Esses pontos precisam ser considerados durante a solução de problemas relacionados à **política de serviços**.

- Não anexe uma política de serviço a uma porta que seja membro de um EtherChannel.
- Com as DFCs (Distributed Forwarding Cards, placas de encaminhamento distribuído) instaladas, a PFC2 não suporta QoS baseada em VLAN. Você não pode emitir o comando **mls qos vlan-based** ou anexar políticas de serviço às interfaces de VLAN.
- O PFC QoS suporta a palavra-chave de saída somente com PFC3 e somente em interfaces de Camada 3 (portas LAN configuradas como interfaces de Camada 3 ou interfaces VLAN). Com o PFC3, você pode anexar um mapa de política de entrada e saída a uma interface de Camada 3.
- A QoS PFC baseada em VLAN ou em porta nas portas da Camada 2 não é relevante para as políticas conectadas às interfaces da Camada 3 com a palavra-chave de saída.
- As políticas anexadas à palavra-chave output não suportam vigilância de microfluxo.
- Não é possível anexar um mapa de política que configura um estado de confiança com a saída do comando **service-policy**.
- A QoS de PFC não suporta marcação de entrada com queda de saída ou queda de entrada com marcação de saída.

Declarações de saída de política de serviço não aparecem na saída do comando running-config

Quando você configura a QoS no multilink no módulo FlexWan, não é possível ver a saída do comando **service-policy** na saída do comando **show running-config**. Isso ocorre quando o switch executa versões do Cisco IOS anteriores à 12.2SX. O FlexWAN para a série Cisco 7600 suporta dLLQ em interfaces não-pacote. Não suporta dLLQ em interfaces de pacotes MLPPP. Esse suporte está disponível no Cisco IOS Software Release 12.2S.

A solução alternativa para ignorar essa limitação é anexar a política de serviço às interfaces desagrupadas ou atualizar a versão do Cisco IOS para 12.2SX ou posterior, onde o recurso é suportado.

Limitação de policiamento

O policiamento é realizado em hardware no PFC sem o impacto do desempenho do switch. A vigilância não pode ocorrer na plataforma 6500 sem PFC. No SO híbrido, a vigilância deve ser configurada no CatOS. Esses pontos precisam ser considerados ao solucionar problemas de policiamento:

- Quando você aplica o policiamento de ingresso e o policiamento de saída ao mesmo tráfego, tanto a política de entrada quanto a política de saída devem marcar o tráfego inativo ou descartar o tráfego. A QoS de PFC não suporta marcação de entrada com queda de saída ou queda de entrada com marcação de saída.
- Quando você cria um vigilante que não usa a palavra-chave pir e o parâmetro maximum_burst_bytes é igual ao parâmetro normal_burst_bytes (que é o caso se você não digitar o parâmetro maximum_burst_bytes), as palavras-chave de ação excedida policed-dscp-transmit fazem com que o PFC QoS marque o tráfego para baixo conforme definido pelo mapa de marcação max-burst policed-dscp.
- Quando a ação de exceder é liberada, a QoS de PFC ignora qualquer ação violada configurada.
- Quando você configura a queda como a ação de conformidade, a QoS de PFC configura a queda como a ação de exceder e a ação de violação.
- Os requisitos da máscara de fluxo de vigilância de microfluxo, NetFlow e NetFlow Data Export (NDE) podem entrar em conflito.

Problemas de limite de taxa ou vigilância com MSFC em SO híbrido

Nos Catalyst 6500 Switches que executam o Hybrid OS, a configuração de rate-limit não fornece a saída desejada. Por exemplo, se você configurar o comando **rate-limit** no comando **interface vlan** no MSFC, ele não limitará a taxa do 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
```

O motivo por trás disso é que o MSFC cuida somente das funções de controle, mas o encaminhamento real de tráfego ocorre em ASICs PFC no supervisor. A MSFC compila a FIB e as tabelas de adjacência, bem como outras informações de controle, e faz o download para a PFC para implementação em hardware. Com a configuração criada, você limita a taxa somente do tráfego comutado por software, que deve ser mínimo (ou nenhum).

A solução é usar a interface de linha de comando (CLI) do CatOS para configurar o limite de taxa no supervisor. Consulte a QoS do CatOS para obter a explicação detalhada de como configurar a política de QoS no CatOS. Você também pode consultar o policiamento de QoS em Catalyst 6500/6000 Series Switches para ver o exemplo de configuração.

Média da Forma de Comando não Suportada em Interfaces VLAN do Cisco 7600

Quando você aplica uma entrada de política de serviço a uma interface no Cisco 7600, esta mensagem de erro é exibida:

```
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 **shape média** não é suportado para as interfaces VLAN no Cisco 7600. Em vez disso, você precisa usar policiamento.

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

Consulte Configurando Política de Política de Política de Política de Política de Classe para obter mais informações sobre como implementar vigilância para tráfego de limite de taxa.

Àmedida que você conecta essa política de serviço a uma interface de VLAN (SVI), é necessário habilitar a QoS baseada em VLAN em todas as portas de Camada 2 que pertencem a essa VLAN na qual você deseja que esse mapa de políticas seja aplicado.

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

Consulte Ativação da QoS de PFC baseada em VLAN em portas LAN da camada 2 para obter mais informações.

QoS-ERRO: A adição/modificação feita ao policymap [chars] e class [chars] não é válida, o comando é rejeitado

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

Essa mensagem de erro indica que as ações definidas na classe mencionada não são permitidas nos switches Cisco Catalyst 6500 Series. Há algumas restrições durante a configuração de ações de classe de mapa de política.

- Você não pode fazer todos esses três em uma classe de mapa de política:Marcar tráfego

com os comandos **set**Configurar o estado de confiançaConfigurar vigilânciaVocê só pode marcar o tráfego com os comandos **set**.OUConfigure o estado de confiança e/ou configure a vigilância.

- Para o tráfego comutado por hardware, o PFC QoS não suporta os comandos **bandwidth**, **priority**, **queue-limit** ou **random-detect** policy map class. Você pode configurar esses comandos porque eles podem ser usados para tráfego comutado por software.
- O PFC QoS não suporta os comandos de classe do mapa de política **set qos-group**.

Consulte Configurando Ações de Classe de Mapa de Política para obter mais informações sobre tais restrições.

Informações Relacionadas

- Classificação e marcação de QoS nos Switches Catalyst 6500/6000 Series que executam o Software Cisco IOS
- Programação de saída de QoS em Switches Catalyst 6500/6000 Series executando o Cisco IOS System Software
- Políticas de QoS nos switches Catalyst 6500/6000 Series
- 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