トラブルシューティング：Catalyst 6500 スイッチの QoS

内容

概要

このドキュメントには Catalyst 6500 スイッチにおける基本的なトラブルシューティングの手順と Quality of Service（QoS）の制限事項が取り上げられており、さらに一般的な QoS 問題のトラブルシューティング情報も提供しています。また、分類の際に発生する QoS 問題や、マーキングおよびポリシングについても説明します。

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、Catalyst 6500 シリーズ スイッチに基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

背景説明

QoS とは、トラフィックを分類して、確定的な搬送サービスを提供できるようにするネットワーク機能です。QoS のプロセスには、次に示すさまざまな手順があります。

- **入力スケジューリング：これはハードウェアのポート ASIC により処理される、レイヤ 2 の QoS 操作です。**この処理に Policy Feature Card（PFC; ポリシー フィーチャ カード）は必要ありません。
- **分類：これは Access Control List（ACL; アクセス コントロール リスト）エンジンを介してスーパーバイザまたは PFC、およびその両方により処理されます。**スーパーバイザではレイヤ 2 の QoS 操作を処理します。PFC ではレイヤ 2 とレイヤ 3 の QoS 操作を処理します。
- **ポリシング：これはレイヤ 3 転送エンジンを介して PFC で処理されます。**PFC は必須であり、レイヤ 2 とレイヤ 3 の QoS 操作を処理します。
- **パケットの書き換え：これはハードウェアのポート ASIC で処理されます。**これは先の分類の結果に基づいて行われるレイヤ 2 およびレイヤ 3 の QoS 操作です。
- **出力のスケジューリング：これはハードウェアのポート ASIC で処理されます。**これは先の分類の結果に基づいて行われるレイヤ 2 およびレイヤ 3 の QoS 操作です。

QoS のトラブルシューティング

Catalyst 6500 スイッチでの QoS は、ルータとは異なった仕組みで動作します。Catalyst 6500 スイッチの QoS のアーキテクチャはきわめて複雑です。Catalyst 6500 のマルチレイヤ スイッチ フィーチャ カード（MSFC）、PFC、およびスーパーバイザ エンジンのアーキテクチャについて理解しておくことをお勧めします。ハイブリッドOSでのQoSの設定では、レイヤ2 CatOS機能とCisco IOS®機能を備えたレイヤ3 MSFCについてさらに理解する必要があります。そして、QoS を設定する前に次のドキュメントを注意深く読んでおくことをお勧めします。

- PFC QoS の設定 - ネイティブ IOS
- QoS の設定 - CatOS

ステップごとのトラブルシューティング手順

このセクションでは、問題を切り分け、より詳細なトラブルシューティングを行うための、基本的なステップバイステップでの Qos のトラブルシューティング手順について説明します。

1. **QoS を有効にする：show mls qos command コマンドで、ポリシングの統計情報や QoS のステータス（有効か無効か）が表示されます。**

```
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. **信頼ポートを使用した着信トラフィックの分類**：この分類では、着信トラフィックが7つのサービスクラス(CoS)値のいずれかに分類されます。インバウンド トラフィックは、すでに発信元で割り当てられた CoS 値を持っていることがあります。この場合は、インバウンド トラフィックの CoS 値を信頼するようにポートを設定する必要があります。信頼することにより、受信したフレームの CoS または type of service (ToS; タイプ オブ サービス) の値がスイッチで維持されることになります。次のコマンドでは、ポートの信頼状態を確認する方法を示しています。

```
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.
```

CoS の値は Inter-Switch Link (ISL; スイッチ間リンク) および dot1q フレームでのみ搬送されます。タグなしのフレームでは CoS 値は搬送されません。タグなしのフレームでは ToS 値を搬送します。この値は、IP パケット ヘッダーの IP precedence または differentiated services code point (DSCP) に由来するものです。ToS 値を信頼するには、IP precedence または DSCP を信頼するようにポートを設定する必要があります。DSCP には IP precedence への下位互換性があります。たとえば、スイッチのポートをレイヤ 3 ポートとして設定している場合には、dot1q フレームや ISL フレームは搬送されません。この場合は、このポートを DSCP や IP precedence を信頼するように設定する必要があります。

```
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. **ACL および ACE を使用した着信トラフィックの分類：トラフィックを分類してマークを付けるようにスイッチを設定することもできます。**分類やマーキングの設定に含まれる手順には、以下のものがあります。アクセスリスト、クラスマップ、ポリシーマップの作成と、ポリシーマップをインターフェイスに適用するための **service-policy input コマンドの発行があります。**ポリシーマップの統計情報は次のようにして確認できます。

```
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
```

クラスマップ qos1 に対応するカウンタ AgForward-By が増えていることに注意してください。対応するクラスマップの統計情報を見ることができない場合は、クラスマップに割り当てられているアクセスリストを確認してください。

4. **入力スケジューリング：入力スケジューリングの設定に PFC は必要ではありません。**1 つの 10/100 ポートに対して rcv-queue threshold コマンドまたは set qos drop-threshold コマンドを設定することはできません。これは入力スケジューリングが 10/100 ポートを 12 備えた Coil ASIC ポートで処理されるためです。したがって、入力スケジューリングは 1-12、13-24、25-36、37-48 のように 12 ポートずつ設定する必要があります。キューイングのアーキテクチャは ASIC に組み込まれており、再設定はできません。LAN ポートのキュー構造を確認するには、**show queueing interface ethernet slot/port | include type**コマンドを使用して、LANポートのキュー構造を確認します。

```
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.
```

デフォルトでは、4 つのしきい値すべてが 100 % になっています。しきい値レベルを設定す

るには、rcv-queue threshold *<Queue Id> <Threshold 1> <Threshold 2> <Threshold 3> <Threshold 14>* コマンドを発行できます。この方法では、輻輳が生じた際、高い CoS 値のデータがドロップされるのは、低い CoS 値のデータよりも後になります。

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

5. **マッピング：CoS を信頼するようにポートが設定されている場合は、受信した CoS 値を内部の DSCP 値にマッピングするために、CoS-DSCP マップ テーブルを使用してください。**

```
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
```

信頼できる IP precedence を信頼するようポートを設定している場合は、受信した IP precedence 値を内部の DSCP 値にマッピングするために、ip-prec-dscp マップ テーブルを使用します。

```
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
```

DSCP を信頼するようポートを設定している場合は、受信した DSCP 値が内部 DSCP 値として使用されます。これらのテーブルは、ネットワーク内のすべてのスイッチで同じである必要があります。いずれかのスイッチで異なるマッピングのテーブルが使用されていると、望んだ結果が得られません。これらのテーブルの値は次のようにして変更できます。

```
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. **ポリシング**:Catalyst 6500スイッチでは、次の2種類のポリシングを使用できます。**集約ポリシング：集約ポリシングはスイッチ内のフローの帯域幅を制御します。**show mls qos aggregate-policer コマンドは、スイッチで設定されているすべての集約ポリシャを表示します。ポリシングの統計情報です。

```
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
```

マイクロフロー ポリシング：マイクロフロー ポリシングでは、スイッチのインターフェイスあたりのフローの帯域幅を制御します。デフォルトでは、マイクロフロー ポリシャで影響を受けるのはルーティングされたトラフィックだけです。ブリッジド トラフィックに対してマイクロフロー ポリシングを有効にするには、VLAN インターフェイスで mls qos bridged コマンドを発行します。マイクロフロー ポリシングの統計情報を確認すると、次のようになります。

```
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
```

注：show mls qos ip *type mod/number*コマンドは、マイクロフローポリシングの統計情報を表示しません。このコマンドで表示されるのは集約ポリシングの統計情報だけです。必要とするポリシングの統計情報が表示されない場合は、ポリシングの設定を確認してください。設定例については、『Catalyst 6500/6000 シリーズ スイッチでの QoS ポリシング』を参照

してください。また、このドキュメントの「Catalyst 6500 スイッチの QoS のガイドラインと制限」のセクションも参照してください。
7. 使用している OS のバージョンの『リリース ノート』を参照して、QoS 設定に関する不具合がないことを確認してください。
8. 使用しているスイッチのスーパーバイザのモデル、PFC のモデル、MSFC のモデル、および Cisco IOS/CatOS のバージョンを確認してください。使用している機器の仕様については、「Catalyst 6500 スイッチの QoS のガイドラインと制限」を参照してください。設定が適用可能であることを確認します。

Catalyst 6500 スイッチの QoS のガイドラインと制限

Catalyst 6500 スイッチで QoS を設定する前に注意する必要のある QoS の制限には次のものがあります。

- 一般的なガイドライン
- PFC3 のガイドライン
- PFC2 のガイドライン
- クラス マップ コマンドの制限
- ポリシー マップ コマンドの制限
- ポリシー マップ クラス コマンドの制限
- キューとドロップのしきい値マッピングのガイドラインと制限
- ACL エントリ内の trust-cos の制限
- WS-X6248-xx、WS-X6224-xx、WS-X6348-xx ラインカードの制限
- PFC または PFC2 は、WAN トラフィック向けの QoS 機能は備えていません。PFC または PFC2 を使用している場合、PFC の QoS 機能によって WAN トラフィックの ToS バイトは変更されません。
- レイヤ 3 でスイッチングされた入力 LAN トラフィックは、MSFC または MSFC2 を通過せず、レイヤ 3 スイッチング エンジンで割り当てられた CoS 値を保持します。
- QoS には、untrusted、trust-ipprec、または trust-dscp キーワードで設定されたポートに対する入力ポートの輻輳回避は実装されていません。トラフィックはスイッチング エンジンに直接送られます。
- スイッチでは、キューだけにマップされている CoS 値を搬送するトラフィックに対して、テール ドロップしきい値を使用します。またスイッチでは、キューとしきい値にマップされている CoS 値を搬送するトラフィックに対して、WRED ドロップしきい値を使用します。
- レイヤ 3 スイッチング エンジンによる分類では、レイヤ 2、3、4 の値を使用します。レイヤ 3 スイッチング エンジンによるマーキングでは、レイヤ 2 CoS の値とレイヤ 3 IP precedence の値または DSCP の値を使用します。
- trust-cos ACL では、信頼できないポートから受信したトラフィックの CoS は復元できません。信頼できないポートから受信したトラフィックには、必ずそのポートの CoS の値が含まれています。

注：PFC QoSでは、ポリシーマップをインターフェイスにアタッチするまで、サポートされていないコマンドの使用は検出されません。

QoS_TCAM の制限

Ternary CAM(TCAM)は、PFC、PFC2、およびPFC3のACLエンジンによって実行される、スイッチを通過するパケットに基づいて、高速テーブルルックアップを行うために設計された専用メモリです。ACL を設定するときには、ACL を QoS にマップします。また、インターフェイスに

QoS ポリシーを割り当てるときには、スイッチが TCAM をプログラムします。スイッチ上の使用可能な TCAM 空間を QoS 用にすべて使用してしまった場合には、次のエラー メッセージが表示されます。

```
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
```

この show tcam count コマンドの出力では、TCAM エントリの Masks の 95 % が使用されています。このため、QoS ポリシーをインターフェイスに適用しようとすると `%QM-4-TCAM_ENTRY:` というエラー メッセージが表示されます。

```
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
```

TCAM エントリと ACL のラベルは、限られたリソースです。したがって、使用している ACL の設定によっては、使用可能なリソースを使い果たさないように注意する必要があります。さらに、大きな QoS ACL および VLAN Access Control List (VACL; VLAN アクセス コントロール リスト) の設定では、Non-Volatile Random Access Memory (NVRAM; 不揮発性 RAM) の空間に注意する必要がある場合があります。使用可能なハードウェアのリソースは、スーパーバイザ 1a と PFC、スーパーバイザ 2 と PFC2、スーパーバイザ 720 と PFC3 によって異なります。

スーパーバイザ モジュール	QoS TCAM	ACL ラベル
スーパーバイザ 1a と PFC	ルータ アクセス コントロール リスト (RACL)、VACL、および QoS ACL で共有されている 2K のマスクと 16K のパターン	RACL、VACL、および QoS ACL で共有されている 512 の ACL ラベル
スーパーバイザ 2 と PFC2	QoS ACL 用の 4K のマスクと 32K のパターン	RACL、VACL、および QoS ACL で共有されている 512 の ACL ラベル
スーパ	QoS ACL 用の 4K のマス	RACL、VACL、お

ーバイザ 720 と PFC3	クと 32K のパターン	よび QoS ACL で共有されている 512 の ACL ラベル

注：512 ACLラベルの制限に関わらず、デフォルト（バイナリ）コンフィギュレーションモードを使用する場合、システム全体で250 QoS ACLのCisco CatOSには追加のソフトウェア制限があります。この制限はテキスト設定モードでは排除されています。設定モードをテキスト モードに変更するには、set config mode text コマンドを発行します。通常、テキスト モードで使用する NVRAM またはフラッシュ メモリの容量は、バイナリの設定モードで使用する容量よりも少なくて済みます。テキスト モードでの操作中は、NVRAM に設定を保存するためには write memory コマンドを発行する必要があります。テキスト設定を NVRAM に自動的に保存するには、set config mode text auto-save コマンドを発行してください。

TCAM に関する問題の回避策を次に示します。

- 1 つの VLAN に属する多数のレイヤ 2 インターフェイスで service-policy コマンドを実装している場合には、スイッチのポートをベースとするポリシングではなく、VLAN ベースのポリシングを使用できます。次に例を示します。
```
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
```

- QoS マーキングの統計情報をディセーブルにします。no mls qos marking statistics コマンドでは、最大の 1020 の AgID 実装が許可されません。これは、dscp ポリシャの設定にデフォルトのポリシャを割り当てているためです。この欠点は、すべてのポリシャがデフォルトのポリシャを共有しているため、特定のポリシャについての統計情報がないことです。
```
Switch(config)#no mls qos marking statistics
```

- 可能であれば、複数のインターフェイスで同じ ACL を使用して、TCAM リソースのコンテンションを緩和するようにします。

NBAR の制限

Network-Based Application Recognition（NBAR）は、幅広いアプリケーションを認識する分類エンジンです。認識できるアプリケーションには、Web ベースのものや、ダイナミック な TCP/UDP ポートの割り当てを利用する分類の難しいプロトコルなどがあります。あるアプリケーションが NBAR によって認識および分類される際に、ネットワークでそのアプリケーション向けのサービスが呼び出されます。NBAR はパケットを分類した後、その分類したトラフィックに対して QoS を適用して、ネットワークの帯域幅が効率よく利用されるようにします。NBAR を使用するときの QoS の実装方法については、次のような制限があります。

- PFC3 では NBAR はサポートされない。
- スーパーバイザ エンジン 2、PFC2、および MSFC2 を使用する場合、PFC QoS の代わりにレイヤ 3 インターフェイスに NBAR を設定可能。PFC2 では、NBAR を設定したポートでの入力 ACL をハードウェアでサポートします。PFC QoS をイネーブルにしている場合、NBAR を設定したポートを経由するトラフィックは、入力キューおよび出力キューを通過し、ドロップしきい値が適用されます。PFC QoS をイネーブルにしている場合、MSFC2 が NBAR トラフィック内の出力 IP precedence に等しい出力 CoS を設定します。すべてのトラフィックは入力キューを通過すると、NBAR を設定したインターフェイスの MSFC2 でソフ

トウェアによって処理されます。

スーパーバイザ 2 に cos-map コマンドがない

ネイティブ IOS ソフトウェア リリース 12.1(8a)EX-12.1(8b)EX5 および 12.1(11b)E 以降では、スーパーバイザ 2 上にあるギガビット アップリンク用のデフォルトの QoS CoS マッピングが変更されています。すべての CoS 値はキュー 1 およびしきい値 1 に割り当てられており、変更できません。

これらのリリースでは、スーパーバイザ 2 のギガビット アップリンク ポートに対して次のコマンドを設定することはできません。

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

QoS の設定には制限があり、厳密なプライオリティ キューは使用できません。この制限が及ぶのは、物理的にスーパーバイザ 2 エンジンにあるギガビット ポートだけです。他のラインカード モジュールにあるギガビット ポートは影響を受けません。

この問題を解決するファームウェア アップグレードがあります。このアップグレードはソフトウェアで実行可能です。ファームウェアのアップグレードが必要な場合は、テクニカルサポートにお問い合せください。ファームウェアのアップグレードは、Supervisor2のハードウェアバージョンが4.0未満の場合にのみ必要です。Supervisor2のハードウェアバージョンが4.0以降の場合、QoSはファームウェアアップグレードなしでギガビットアップリンクポートで許可される必要があります。ファームウェアのレベルを確認するには、show module コマンドを発行してください。この問題は、Cisco Bug ID CSCdw89764（登録ユーザ専用）で確認されています。

service-policy の制限

ポリシーマップをインターフェイスに適用するには、service-policy コマンドを発行します。サポートされていないコマンドをポリシーマップに指定していると、service-policy コマンドでポリシーマップを適用した後にスイッチのコンソールにエラーが表示されます。service-policy に関連する問題をトラブルシューティングする際には、次の点を考慮する必要があります。

- EtherChannel のメンバのポートには、サービス ポリシーを割り当てないでください。
- Distributed Forwarding Card（DFC）が取り付けられている場合は、PFC2 で VLAN ベースの QoS はサポートされません。VLAN インターフェイスに対しては、mls qos vlan-based コマンドを発行したり、サービス ポリシーを割り当てることはできません。
- PFC QoS では、出力キーワードを PFC3 およびレイヤ 3 インターフェイス（レイヤ 3 インターフェイスとして設定されている LAN ポートまたは VLAN インターフェイス）でのみサポートしています。 PFC3 を使用している場合は、レイヤ 3 インターフェイスに入力ポリシー マップと出力ポリシー マップの両方を割り当てられます。
- レイヤ 2 ポート上の VLAN ベースまたはポートベースの PFC QoS は、出力キーワードでレイヤ 3 インターフェイスに適用されたポリシーとは関連がありません。
- 出力キーワードで適用されたポリシーでは、マイクロフロー ポリシングはサポートされません。
- service-policy コマンドの出力では、信頼状態を設定するポリシー マップは割り当てることができません。

- PFC QoS では出力ドロップによる入力マークダウン、あるいは出力マークダウンによる入力ドロップをサポートしていません。

running-config コマンドの出力に service-policy の出力文が表示されない

FlexWan モジュールのマルチリンクに QoS を設定する場合には、show running-config コマンドの出力内に service-policy コマンドの出力は表示されません。この状態は、スイッチで 12.2SX より前の Cisco IOS のバージョンが稼働している場合に発生します。Cisco 7600 シリーズの FlexWAN では、バンドルされていないインターフェイス上の dLLQ がサポートされます。MLPPP バンドル インターフェイス上の dLLQ はサポートされません。これは Cisco IOS ソフトウェア リリース 12.2S ではサポートされています。

この制限の回避策は、サービス ポリシーを非バンドル インターフェイスに適用するか、Cisco IOS のバージョンを、この機能をサポートしている 12.2SX 以降にアップグレードすることです。

ポリシングの制限

ポリシングは PFC 上のハードウェアによって実行され、スイッチのパフォーマンスには影響を与えません。PFC のない 6500 プラットフォームではポリシングは実行できません。ハイブリッド OS の場合は、CatOS 上でポリシングを設定する必要があります。ポリシングに関する問題をトラブルシューティングする際には、次の点を考慮する必要があります。

- 入力ポリシングと出力ポリシングの両方を同じトラフィックに適用するときには、入力ポリシーと出力ポリシーの両方でトラフィックのマークダウンかドロップを行う必要があります。PFC QoS では出力ドロップによる入力マークダウン、あるいは出力マークダウンによる入力ドロップをサポートしていません。
- キーワード pir を使用せず、maximum_burst_bytes パラメータと normal_burst_bytes パラメータと等しい（maximum_burst_bytes パラメータを入力していない場合）ポリシャを作成すると、exceed-action policed-dscp-transmit キーワードが原因で、policed-dscp max-burst マークダウン マップで定義されたように PFC QoS によってトラフィックがマークダウンされます。
- 超過アクションがドロップされると、PFC QoS では設定済の違反アクションは無視されます。
- ドロップを適合アクションとして設定している場合、PFC QoS ではドロップが超過アクションおよび違反アクションとして設定されます。
- マイクロフロー ポリシング、NetFlow、および NetFlow Data Export（NDE; NetFlow データ エクスポート）のフローマスク要件が競合する場合があります。

ハイブリッド OS の MSFC によるレート制限またはポリシングの問題

ハイブリッド OS が稼働している Catalyst 6500 スイッチでは、レート制限の設定が期待どおりの結果になりません。たとえば、MSFC で interface vlan コマンドの下で rate-limit コマンドを設定すると、実際にはトラフィックに対してレート制限が行われません。

```
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
```

または

```
interface Vlan10
service-policy input Test_Policy
```
この問題の背後にある理由は、MSFC は制御機能のみを行い、実際のトラフィック フォワーディングはスーパーバイザの PFC ASIC で行われるということです。MSFC では FIB と隣接関係テーブルのほか、制御情報をコンパイルして、これを PFC にダウンロードしてハードウェアに実装します。作成した設定を利用すると、レート制限はソフトウェアによってスイッチされたトラフィックにのみ適用され、これは最小限の適用（または適用なし）となります。

この問題の回避策は、スーパーバイザでのレート制限の設定に CatOS command-line interface（CLI; コマンドライン インターフェイス）を使用することです。CatOS で QoS ポリシングを設定する方法の詳細については、『CatOS QoS』を参照してください。また、設定例については、『Catalyst 6500/6000 シリーズ スイッチでの QoS ポリシング』も参照してください。

Cisco 7600 の VLAN インターフェイスで shape average コマンドがサポートされていない

Cisco 7600 でインターフェイスにサービス ポリシー入力を適用すると、次のエラー メッセージが表示されます。

```
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
```
shape average コマンドは、Cisco 7600 の VLAN インターフェイスではサポートされていません。代わりにポリシングを使用する必要があります。

```
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
```

レート制限トラフィックに対してポリシングを実装する方法の詳細については、『ポリシー マップ クラス ポリシングの設定』を参照してください。

このサービス ポリシーを VLAN インターフェイス（SVI）に付加する場合、このポリシーマップを適用するこの VLAN に属するすべての レイヤ 2 ポートで、VLAN ベースの QoS を有効にする必要があります。

```
7600_1(config)#interface Gi 1/40
7600_1(config-if)#mls qos vlan-based
```
詳細については、『レイヤ 2 LAN ポートで VLAN ベース PFC QoS を有効にする』を参照してください。

QoS-ERROR：ポリシー マップ [chars] およびクラス [chars] への追加/変更は有効ではありません、コマンドは拒否されます

```
QoS-ERROR: Addition/Modification made to policymap vtc-map and class voice-video is
not valid, command is rejected
```
このエラー メッセージは、表記されているクラスで定義されているアクションが、Cisco Catalyst 6500 シリーズ スイッチでは許可されていないことを示します。ポリシー マップ クラス

アクションの設定ではいくつかの制限があります。

- ポリシー マップ クラスでは、次の 3 つすべては実行できません。**set コマンドによるトラフィックのマーキング**信頼状態の設定ポリシングの設定**set コマンドでトラフィックをマーキングするか**、または信頼状態またはポリシングを設定するか、その両方を設定します。
- ハードウェアでスイッチングされるトラフィックの場合、PFC QoS は **bandwidth**、**priority**、**queue-limit**、または **random-detect ポリシー マップ クラス コマンドをサポートしません。**これらのコマンドはソフトウェアでスイッチングされるトラフィックに使用できるので、設定が可能です。
- PFC QoS では、**set qos-group ポリシー マップ クラス コマンドはサポートされません。**

このような制限については、『ポリシー マップ クラス アクションの設定』を参照してください。

関連情報

- Cisco IOS ソフトウェアが稼働する Catalyst 6500/6000 シリーズ スイッチの QoS 分類およびマーキング
- Cisco IOS システム ソフトウェアが稼働している Catalyst 6500/6000 シリーズ スイッチの QoS 出力スケジューリング
- Catalyst 6500/6000 シリーズ スイッチでの QoS ポリシング
- CatOS ソフトウェアが稼働する Catalyst 6500/6000 シリーズ スイッチの QoS の分類とマーキング
- CatOS システム ソフトウェアが稼働している Catalyst 6500/6000 シリーズ スイッチの QoS 出力スケジューリング
- LAN 製品に関するサポート ページ
- LAN スイッチングに関するサポート ページ
- テクニカル サポートとドキュメント – Cisco Systems