QoS-Fehlerbehebung bei Catalyst Switches der Serie 6500

Inhalt

Einleitung

Dieses Dokument enthält die grundlegenden Schritte zur Fehlerbehebung, die Quality of Service (QoS)-Beschränkungen und Informationen zur Behebung gängiger QoS-Probleme bei Catalyst Switches der Serie 6500. In diesem Dokument werden auch QoS-Probleme bei der Klassifizierung, Markierung und Richtlinienvergabe behandelt.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den Catalyst Switches der Serie 6500.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps von Cisco zu Konventionen).

Hintergrundinformationen

QoS ist eine Netzwerkfunktion zur Klassifizierung des Datenverkehrs und zur Bereitstellung deterministischer Bereitstellungsservices. In diesen Artikeln werden die verschiedenen Schritte im QoS-Prozess erläutert:

- **Input Scheduling** (**Eingabeplanung**): Diese wird von Hardware-Port-ASICs behandelt und ist ein Layer-2-QoS-Vorgang. Es ist keine Policy Feature Card (PFC) erforderlich.
- **Klassifizierung**: Diese wird vom Supervisor und/oder PFC über die ACL-Engine (Access Control List) verwaltet. Der Supervisor übernimmt den Layer-2-QoS-Betrieb. PFC übernimmt den QoS-Betrieb auf Layer 2 und Layer 3.
- **Policing** (**Richtlinienvergabe**): Diese wird von PFC über die Layer-3-Forwarding-Engine verwaltet. PFC ist erforderlich und übernimmt den QoS-Betrieb auf Layer 2 und Layer 3.
- **Packet Re-Write** (**Paketumlegung**): Diese wird von Hardware-Port-ASICs behandelt. Es handelt sich um eine Layer-2- und Layer-3-QoS-Operation, die auf der zuvor vorgenommenen Klassifizierung basiert.
- **Output Scheduling** (**Ausgabeplanung**): Diese wird von Hardware-Port-ASICs verwaltet. Es handelt sich um eine Layer-2- und Layer-3-QoS-Operation, die auf der zuvor vorgenommenen Klassifizierung basiert.

QoS-Fehlerbehebung

QoS funktioniert bei Catalyst Switches der Serie 6500 anders als bei Routern. Die QoS-Architektur der Catalyst 6500-Switches ist recht komplex. Es wird empfohlen, die Architektur der Multilayer Switch Feature Card (MSFC), PFC und Supervisor Engine in Catalyst 6500 zu verstehen. Für die Konfiguration von QoS in Hybrid-Betriebssystemen sind ein besseres Verständnis der Layer-2-CatOS-Funktionalität und der Layer-3-MSFC mit Cisco IOS®-Funktionalität erforderlich. Es wird empfohlen, die folgenden Dokumente gründlich zu lesen, bevor Sie QoS konfigurieren:

- Konfigurieren von PFC QoS - Natives IOS
- Konfigurieren von QoS - CatOS

Schrittweise Fehlerbehebung

Dieser Abschnitt enthält das grundlegende schrittweise Fehlerbehebungsverfahren für QoS, um das Problem für die weitere Fehlerbehebung zu isolieren.

1. **Enable QoS** (QoS aktivieren): Der **Befehl show mls qos** zeigt die Richtlinienstatistiken und den Status von QoS an, ob aktiviert oder deaktiviert.

```
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. **Klassifizierung des eingehenden Datenverkehrs mithilfe des Trust-Ports** - Diese Klassifizierung kategorisiert den eingehenden Datenverkehr in einen der sieben Class of Service (CoS)-Werte. Dem eingehenden Datenverkehr kann der CoS-Wert bereits von der Quelle zugewiesen sein. In diesem Fall müssen Sie den Port so konfigurieren, dass der CoS-Wert des eingehenden Datenverkehrs vertrauenswürdig ist. Mithilfe von Trust (Vertrauenswürdigkeit) kann der Switch die CoS- oder ToS-Werte (Type of Service) des empfangenen Frames beibehalten. Dieser Befehl zeigt, wie der Port-Vertrauensstatus überprüft wird:

```
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.
```

   Der CoS-Wert wird nur von Inter-Switch Link (ISL)- und dot1q-Frames übertragen. Nicht getaggte Frames enthalten keine CoS-Werte. Nicht getaggte Frames übertragen ToS-Werte, die von der IP-Rangfolge oder vom DSCP (Differentiated Services Code Point) aus dem IP-Paket-Header abgeleitet werden. Um dem ToS-Wert zu vertrauen, müssen Sie den Port so konfigurieren, dass er der IP-Rangfolge oder DSCP vertraut. DSCP ist abwärtskompatibel mit der IP-Rangfolge. Wenn Sie beispielsweise einen Switch-Port als Layer-3-Port konfiguriert haben, werden keine dot1q- oder ISL-Frames übertragen. In diesem Fall müssen Sie diesen Port so konfigurieren, dass DSCP oder die IP-Rangfolge vertrauenswürdig ist.

```
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. **Klassifizierung von eingehenden Datenverkehr mithilfe von ACL und ACEs** - Sie können den Switch auch so konfigurieren, dass der Datenverkehr klassifiziert und markiert wird. Zur Konfiguration der Klassifizierung und Kennzeichnung sind folgende Schritte erforderlich: Zugriffslisten, Klassenzuordnung und Richtlinienzuordnung erstellen und den Befehl **zur** Dienstrichtlinieneingabe ausgeben, um die Richtlinienzuordnung auf die Schnittstelle

anzuwenden. Sie können die Statistiken zur Richtlinienzuweisung wie folgt überprüfen:

```
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
```

Beachten Sie, dass die Zähler **AgForward-By**, die der Klassenzuordnung qos1 entsprechen, größer werden. Wenn die Statistiken für die entsprechende Klassenzuordnung nicht angezeigt werden, überprüfen Sie die der Klassenzuordnung beigefügte Zugriffsliste.

4. **Input Scheduling** (**Eingabeplanung**): PFC ist für die Konfiguration der Eingabeplanung nicht erforderlich. Sie können den **RCV-queue-Grenzwert** oder die **QoS-Drop-Schwellenwert-**Befehle für einen einzelnen 10/100-Port nicht konfigurieren. Dies liegt daran, dass die Eingabeplanung von Coil ASIC-Ports verarbeitet wird, die zwölf 10/100-Ports enthalten. Daher müssen Sie die Eingabeplanung in Sets mit 12 Ports konfigurieren, z. B. 1-12, 13-24, 25-36, 37-48.Die Warteschlangenarchitektur ist in die ASIC integriert und kann nicht neu konfiguriert werden. Stellen Sie die **Schnittstelle show queueing fastEthernet-Steckplatz/-Port aus. | include type** command, um die Warteschlangenstruktur eines LAN-Ports anzuzeigen.

```
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.
```

Standardmäßig sind alle vier Schwellenwerte 100 %. Sie können den Befehl **rcv-queue threshold** *<Queue Id> <Threshold 1> <Threshold 2> <Threshold 3> <Threshold 14>* ausgeben, um die Schwellenwerte zu konfigurieren. Auf diese Weise werden die höheren CoS-Werte nicht verworfen, bevor die CoS-Werte während der Überlastung gesenkt werden.

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

5. **Zuordnung**: Wenn der Port so konfiguriert ist, dass er der CoS vertraut, verwenden Sie die CoS-DSCP-Zuordnungstabelle, um den empfangenen CoS-Wert einem internen DSCP-Wert zuzuordnen.

```
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
```

Wenn der Port so konfiguriert ist, dass er der Vertrauenswürdigkeit der IP-Rangfolge vertraut, verwenden Sie die Tabelle ip-prec-dscp, um den empfangenen IP-Rangfolgewert einem internen DSCP-Wert zuzuordnen.

```
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
```

Wenn der Port so konfiguriert ist, dass er dem DSCP vertrauenswürdig ist, wird der empfangene DSCP-Wert als interner DSCP-Wert verwendet.Diese Tabellen sollten auf allen Switches in Ihrem Netzwerk gleich sein. Wenn einer der Switches über eine Tabelle mit unterschiedlichen Zuordnungen verfügt, erhalten Sie das gewünschte Ergebnis nicht. Sie können diese Tabellenwerte wie folgt ändern:

```
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. **Policing** - Es gibt zwei Arten von Richtlinien, die auf Catalyst 6500-Switches angewendet werden können:**Aggregate Policing** - Aggregate Policing steuert die Bandbreite eines Datenflusses im Switch. Der Befehl **show mls qos aggregate-policer** zeigt alle auf dem Switch konfigurierten aggregierten Policer an. Dies sind die Statistiken zur Richtlinienvergabe:

```
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
```

Microflow Policing - Microflow Policing steuert die Bandbreite eines Datenflusses pro Schnittstelle im Switch. Standardmäßig wirken sich Mikroflow-Policer nur auf gerouteten Datenverkehr aus. Führen Sie den Befehl **mls qos brücken** in der VLAN-Schnittstelle aus, um die Mikroflow-Überwachung für überbrückten Datenverkehr zu aktivieren. Dies ist die Überprüfung der Microflow Policing-Statistiken:

```
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
```

Hinweis: Der Befehl **show mls qos ip** ***type mod/number*** zeigt keine Statistiken zur Mikroflow-Überwachung. Es werden nur die aggregierten Policing-Statistiken angezeigt.Wenn Sie die gewünschte Richtliniestatistik nicht sehen, überprüfen Sie die Richtlinienkonfiguration. Das Konfigurationsbeispiel finden Sie unter QoS Policing für Catalyst Switches der Serien 6500 und 6000. Weitere Informationen finden Sie im Abschnitt QoS Guidelines and Limitations on Catalyst 6500 Switches in diesem Dokument.

7. Überprüfen Sie die Versionshinweise Ihrer Betriebssystemversion, und stellen Sie sicher, dass keine Fehler in Ihrer QoS-Konfiguration vorliegen.
8. Notieren Sie Ihr Switch-Supervisor-Modell, PFC-Modell, MSFC-Modell und die Cisco IOS/CatOS-Version. Beachten Sie die QoS-Richtlinien und -Einschränkungen für Catalyst 6500-Switches in Bezug auf Ihre Spezifikationen. Stellen Sie sicher, dass Ihre Konfiguration gültig ist.

QoS-Richtlinien und Einschränkungen für Catalyst 6500-Switches

Es gibt QoS-Einschränkungen, die Sie beachten müssen, bevor Sie QoS auf Catalyst 6500-Switches konfigurieren:

- Allgemeine Richtlinien
- PFC3-Richtlinien
- PFC2-Richtlinien
- Befehlsbeschränkungen für Klassenzuordnungen
- Befehlsbeschränkungen für Richtlinienzuweisungen
- Befehlsbeschränkungen für Policy Map Class
- Richtlinien und Einschränkungen für Warteschlangen- und Drop-Grenzwertzuordnung
- Vertrauenskosten bei Zugriffsbeschränkungen für Zugriffskontrolllisten
- Einschränkungen der Linecards WS-X6248-xx, WS-X6224-xx und WS-X6348-xx
- PFC oder PFC2 bieten keine QoS für den WAN-Datenverkehr. Bei PFC oder PFC2 ändert PFC QoS das ToS-Byte im WAN-Datenverkehr nicht.
- Eingehender LAN-Datenverkehr mit Layer-3-Switching durchläuft nicht die MSFC oder MSFC2 und behält den von der Layer-3-Switching-Engine zugewiesenen CoS-Wert bei.
- QoS implementiert keine Überlastungsvermeidung für Eingangsports an Ports, die mit den **nicht vertrauenswürdigen**, **trust-ipprec** oder **trust-dscp**-Schlüsselwörtern konfiguriert sind. Der Datenverkehr geht direkt an die Switching-Engine.
- Der Switch verwendet den Tail-Drop-Grenzwert für den Datenverkehr, der die CoS-Werte überträgt, die nur der Warteschlange zugeordnet sind. Der Switch verwendet die WRED-Drop-Schwellenwerte für den Datenverkehr, der die CoS-Werte überträgt, die der Warteschlange und einem Schwellenwert zugeordnet sind.
- Bei der Klassifizierung mit einer Layer-3-Switching-Engine werden die Werte Layer 2, 3 und 4 verwendet. Bei der Markierung mit einer Layer-3-Switching-Engine werden die CoS-Werte für Layer 2 und die IP-Rangfolge für Layer 3 bzw. DSCP-Werte verwendet.
- Eine Trust-cos-ACL kann die empfangenen CoS im Datenverkehr von den nicht vertrauenswürdigen Ports nicht wiederherstellen. Der Datenverkehr von den nicht vertrauenswürdigen Ports hat immer den CoS-Wert des Ports.

Hinweis: PFC QoS erkennt die Verwendung nicht unterstützter Befehle erst, wenn Sie eine Richtlinienzuordnung an eine Schnittstelle anhängen.

QoS_TCAM-Einschränkung

Der Ternary CAM (TCAM) ist ein spezialisierter Arbeitsspeicher, der für schnelle Tabellensuche auf der Grundlage von Paketen, die den Switch passieren, durch die ACL-Engine auf PFC, PFC2 und PFC3 ausgeführt wird. ACLs werden in der Hardware der Cisco Catalyst Switches der Serie 6500 verarbeitet, die als TCAM bezeichnet werden. Wenn Sie die ACL konfigurieren, ordnen Sie die ACL der QoS zu. Wenn Sie die QoS-Richtlinie auf die Schnittstelle anwenden, programmiert der Switch den TCAM. Wenn Sie bereits den gesamten verfügbaren TCAM-Speicherplatz auf dem Switch für die QoS genutzt haben, wird folgende Fehlermeldung angezeigt:

```
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
```

Dieser Befehl **show tcam count** gibt an, dass die TCAM-Eingabemasken zu 95 % verwendet werden. Wenn Sie daher die QoS-Richtlinie auf die Schnittstelle anwenden, erhalten Sie den `%QM-4-TCAM_ENTRY:` fehl.

```
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-Einträge und ACL-Labels sind begrenzte Ressourcen. Daher müssen Sie, abhängig von Ihrer ACL-Konfiguration, möglicherweise vorsichtig sein, die verfügbaren Ressourcen nicht auszuschöpfen. Bei großen Konfigurationen für QoS-ACLs und VLAN-Zugriffskontrolllisten (VACLs) müssen Sie außerdem den NVRAM (Non-Volatile Random Access Memory) berücksichtigen. Die verfügbaren Hardwareressourcen unterscheiden sich bei Supervisor 1a mit PFC, Supervisor 2 mit PFC2 und Supervisor 720 mit PFC3.

Supervisor-Modul	QoS-TCAM	ACL-Labels
Supervisor 1a und PFC	2.000 Masken und 16.000 Muster, die von RACLs (Router Access Control Lists), VACLs und QoS ACLs gemeinsam genutzt	512 ACL-Label, die von RACLs, VACLs und QoS-ACLs gemeinsam genutzt werden

	werden	
Supervisor 2 und PFC2	4.000 Masken und 32.000 Muster für QoS-ACLs	512 ACL-Label, die von RACLs, VACLs und QoS-ACLs gemeinsam genutzt werden
Supervisor 720 und PFC3	4.000 Masken und 32.000 Muster für QoS-ACLs	512 ACL-Label, die von RACLs, VACLs und QoS-ACLs gemeinsam genutzt werden

Hinweis: Unabhängig von der 512-ACL-Labelgrenze gibt es bei Verwendung des standardmäßigen (binären) Konfigurationsmodus im Cisco CatOS eine zusätzliche Software-Obergrenze von 250 QoS-ACLs systemweit. Diese Einschränkung wird im Textkonfigurationsmodus entfernt. Geben Sie den Befehl **set config mode text** ein, um den Konfigurationsmodus in den Textmodus zu ändern. Der Textmodus belegt in der Regel weniger NVRAM- oder Flash-Speicher als der Binärkonfigurationsmodus. Um die Konfiguration im NVRAM zu speichern, müssen Sie den Befehl **write memory** im Textmodus ausführen. Geben Sie den Befehl **set config mode text auto-save ein**, um die Textkonfiguration im NVRAM automatisch zu speichern.

Dies ist die Lösung für das TCAM-Problem:

- Wenn Sie den Befehl **service policy** für viele Layer-2-Schnittstellen implementiert haben, die zu einem VLAN gehören, können Sie VLAN-basierte Richtlinienvergabe anstelle von Switch-Port-basierten implementieren. Dies ist ein Beispiel:
```
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-Markierungsstatistiken deaktivieren Der Befehl **no mls qos marking statistics** ermöglicht keine Implementierung von maximal 1020 AgIDs. Dies liegt daran, dass die Standardüberwachungsoption für festgelegte DSCP-Policer zugewiesen wird. Der Nachteil ist, dass es keine Statistiken für die spezifische Policer gibt, da alle die Standardrichtlinie gemeinsam nutzen.
```
Switch(config)#no mls qos marking statistics
```

- Wenn möglich, verwenden Sie dieselben ACLs über mehrere Schnittstellen hinweg, um den Zusammentreffen von TCAM-Ressourcen zu reduzieren.

NBAR-Einschränkung

Network-Based Application Recognition (NBAR) ist eine Klassifizierungs-Engine, die eine Vielzahl von Anwendungen erkennt. Sie umfasst webbasierte und andere schwer zu klassifizierende Protokolle, die dynamische TCP/UDP-Portzuweisungen verwenden. Wenn eine Anwendung von der NBAR erkannt und klassifiziert wird, kann ein Netzwerk Services für diese spezifische Anwendung aufrufen. NBAR klassifiziert Pakete und wendet dann QoS auf den klassifizierten Datenverkehr an, um sicherzustellen, dass die Netzwerkbandbreite effizient genutzt wird. Die

Implementierung von QoS bei der Verwendung von NBAR unterliegt gewissen Einschränkungen:

- NBAR wird von PFC3 nicht unterstützt.
- Mit Supervisor Engine 2, PFC2 und MSFC2:Sie können NBAR auf Layer-3-Schnittstellen anstelle von PFC QoS konfigurieren.PFC2 bietet Hardwareunterstützung für Eingabe-ACLs an Ports, an denen NBAR konfiguriert wird.Wenn PFC QoS aktiviert ist, durchläuft der Datenverkehr durch Ports, für die Sie NBAR konfigurieren, die Eingangs- und Ausgangswarteschlangen und die Drop-Schwellenwerte.Wenn PFC QoS aktiviert ist, legt MSFC2 die Ausgangs-CoS auf die gleiche Ausgangs-IP-Rangfolge im NBAR-Datenverkehr fest.Nachdem der gesamte Datenverkehr eine Eingangswarteschlange passiert hat, wird er in Software auf der MSFC2 auf Schnittstellen verarbeitet, auf denen Sie NBAR konfigurieren.

Die cosMap-Befehle fehlen in Supervisor 2

In den nativen IOS Software-Versionen 12.1(8a)EX-12.1(8b)EX5 und 12.1(11b)E und höher wurden die standardmäßigen QoS-CoS-Zuordnungen für die Gigabit-Uplinks auf dem Supervisor2 geändert. Alle CoS-Werte wurden Warteschlange 1 und Schwellenwert 1 zugewiesen und können nicht geändert werden.

Diese Befehle können für einen Sup2 Gigabit Uplink-Port dieser Versionen nicht konfiguriert werden:

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

QoS-Konfigurationen sind begrenzt, und die Warteschlange mit strikter Priorität kann nicht verwendet werden. Dies betrifft nur die Gigabit-Ports, die sich physisch auf der Supervisor 2 Engine befinden. Gigabit-Ports in anderen Linecard-Modulen sind nicht betroffen.

Dieses Problem wird durch ein Firmware-Upgrade behoben. Dieses Upgrade kann per Software durchgeführt werden. Wenden Sie sich an den technischen Support, wenn ein Firmware-Upgrade erforderlich ist. Beachten Sie, dass ein Firmware-Upgrade nur erforderlich ist, wenn die Hardware-Version des Supervisor2 unter 4.0 liegt. Wenn die Hardware-Version des Supervisor2 4.0 oder höher ist, sollte QoS auf den Gigabit-Uplink-Ports ohne Firmware-Upgrade zulässig sein. Sie können den Befehl **show module** ausführen, um die Firmware-Ebene zu finden. Dieses Problem wird in der Cisco Bug-ID CSCdw89764 identifiziert (nur registrierte Kunden).

Service-Richtlinieneinschränkungen

Führen Sie zum Anwenden der Richtlinienzuordnung auf die Schnittstelle den Befehl **service-policy aus**. Wenn Sie einen nicht unterstützten Befehl in der Richtlinienzuordnung haben, werden die Fehlermeldungen in der Konsole angezeigt, nachdem Sie ihn mit dem Befehl **service-policy** angewendet haben. Diese Punkte müssen bei der Behebung von Problemen **im Zusammenhang mit Servicerichtlinien** berücksichtigt werden.

- Schließen Sie keine Service-Richtlinie an einen Port an, der zu einem EtherChannel gehört.
- Wenn Distributed Forwarding Cards (DFCs) installiert sind, unterstützt PFC2 keine VLAN-basierte QoS. Sie können den Befehl **mls qos vlan** nicht ausgeben oder Service-Richtlinien an

VLAN-Schnittstellen anhängen.
- PFC QoS unterstützt das Ausgabeschlüsselwort nur mit PFC3 und nur an Layer-3-Schnittstellen (entweder LAN-Ports, die als Layer-3-Schnittstellen konfiguriert sind, oder VLAN-Schnittstellen). Mit PFC3 können Sie eine Eingabe- und eine Ausgaberichtlinienzuordnung an eine Layer-3-Schnittstelle anhängen.
- VLAN-basierte oder Port-basierte PFC-QoS an Layer-2-Ports sind für Richtlinien, die an Layer-3-Schnittstellen mit dem Output-Schlüsselwort angeschlossen sind, nicht relevant.
- Richtlinien, die mit dem Ausgabeschlüsselwort verknüpft sind, unterstützen keine Microflow-Policing.
- Sie können keine Richtlinienzuordnung anhängen, die einen Vertrauenszustand mit der Befehlsausgabe **der Dienstrichtlinie** konfiguriert.
- PFC QoS unterstützt kein Ingress-Markdown mit Ausgangs- oder Ingress-Drop mit Ausgangs-Markdown.

Ausgabenanweisungen für Dienstrichtlinien werden in der Befehlsausgabe "running-config" nicht angezeigt

Wenn Sie QoS auf der Multilink-Komponente des FlexWan-Moduls konfigurieren, wird die Befehlsausgabe **für die Service-Policy** in der Befehlsausgabe **show running-config** nicht angezeigt. Dies tritt auf, wenn der Switch Cisco IOS-Versionen vor 12.2SX ausführt. Das FlexWAN für die Cisco Serie 7600 unterstützt dLLQ an Schnittstellen, die keine Pakete sind. Sie unterstützt keine dLLQ für MLPPP-Paketschnittstellen. Diese Unterstützung ist für die Cisco IOS Software, Version 12.2S, verfügbar.

Um diese Einschränkung zu umgehen, müssen die Service-Richtlinien an entbündelte Schnittstellen angeschlossen oder die Cisco IOS-Version auf 12.2SX oder höher aktualisiert werden, wenn die Funktion unterstützt wird.

Richtlinienbegrenzung

Die Richtlinienvergabe erfolgt in der Hardware auf PFC, ohne dass die Switch-Leistung beeinträchtigt wird. Die Richtlinienvergabe kann auf der 6500-Plattform ohne PFC nicht erfolgen. Bei Hybrid-Betriebssystemen muss die Richtlinienvergabe auf dem CatOS konfiguriert werden. Diese Punkte müssen bei der Behebung von Problemen mit der Richtlinienvergabe berücksichtigt werden:

- Wenn Sie sowohl die Eingangs- als auch die Ausgangs-Policing auf denselben Datenverkehr anwenden, müssen sowohl die Eingangs- als auch die Ausgangsrichtlinie Datenverkehr markieren oder verwerfen. PFC QoS unterstützt kein Ingress-Markdown mit Ausgangs- oder Ingress-Drop mit Ausgangs-Markdown.
- Wenn Sie einen Policer erstellen, der das pir-Schlüsselwort nicht verwendet und der maximum_burst_bytes-Parameter gleich dem normal_burst_bytes-Parameter ist (was der Fall ist, wenn Sie den maximum_burst_bytes-Parameter nicht eingeben), werden durch die Schlüsselwörter "policed-dscp-transfer" die PFC-QoS-Markierung des Datenverkehrs gemäß der Markierung "policed-dscp max-burst" ausgelöst.
- Wenn die Aktion "überschreiten" verworfen wird, ignoriert PFC QoS jede konfigurierte Verletzungsaktion.
- Wenn Sie das Drop als konforme Aktion konfigurieren, konfiguriert PFC QoS das Drop als die Aktion "Mehr" und die Aktion "Verletzung".

- Die Anforderungen an die Flussmaske von Microflow Policing, NetFlow und NetFlow Data Export (NDE) können in Konflikt stehen.

Rate-Limit- oder Richtlinienprobleme bei MSFC in Hybrid OS

Bei Catalyst Switches der Serie 6500 mit Hybrid OS wird bei der Konfiguration der Ratenbeschränkung nicht die gewünschte Ausgabe ausgegeben. Wenn Sie beispielsweise den Befehl **rate-limit** unter dem Befehl **interface vlan** auf der MSFC konfigurieren, wird der Datenverkehr dadurch nicht begrenzt.

```
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
```

ODER:

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

Der Grund hierfür ist, dass die MSFC nur für Steuerungsfunktionen zuständig ist, die tatsächliche Weiterleitung des Datenverkehrs jedoch auf PFC-ASICs auf dem Supervisor erfolgt. Die MSFC kompiliert die FIB- und Adjacency-Tabellen sowie weitere Steuerelementinformationen und lädt sie zur Implementierung in der Hardware auf PFC herunter. Mit der von Ihnen erstellten Konfiguration beschränken Sie den softwarevermittelten Datenverkehr auf ein Minimum (oder gar keinen).

Die Lösung besteht darin, die CatOS-Befehlszeilenschnittstelle (CLI) zu verwenden, um die Ratenbeschränkung für den Supervisor zu konfigurieren. Unter CatOS QoS finden Sie eine detaillierte Erklärung zur Konfiguration der QoS-Richtlinienzuweisung in CatOS. Das Konfigurationsbeispiel finden Sie auch unter QoS Policing für Catalyst Switches der Serien 6500/600.

Befehlsformatdurchschnitt wird in VLAN-Schnittstellen des Cisco 7600 nicht unterstützt

Wenn Sie eine Servicerichtlinieneingabe auf eine Schnittstelle des Cisco 7600 anwenden, wird folgende Fehlermeldung angezeigt:

```
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
```

Der Befehl **shape average** wird für die VLAN-Schnittstellen in Cisco 7600 nicht unterstützt. Stattdessen müssen Sie die Richtlinien verwenden.

```
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
```

Weitere Informationen zum Implementieren von Richtlinien zur Datenverkehrsbegrenzung finden Sie unter Konfigurieren der Richtlinienzuordnung.

Wenn Sie diese Service-Richtlinie an eine VLAN-Schnittstelle (SVI) anhängen, müssen Sie VLAN-basierte QoS auf allen Layer-2-Ports aktivieren, die zu diesem VLAN gehören, in dem diese Richtlinienzuweisung angewendet werden soll.

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

Weitere Informationen finden Sie unter Aktivieren von VLAN-basierter PFC-QoS auf Layer-2-LAN-Ports.

QoS-FEHLER: Die Hinzufügung/Änderung an der Richtlinienzuordnung [Chars] und der Klasse [Chars] ist ungültig, der Befehl wird abgelehnt.

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

Diese Fehlermeldung weist darauf hin, dass die in der genannten Klasse definierten Aktionen in Cisco Catalyst Switches der Serie 6500 nicht zulässig sind. Bei der Konfiguration von Richtlinienzuordnungsklassenaktionen bestehen einige Einschränkungen.

- In einer Richtlinienzuordnungsklasse können nicht alle drei Aufgaben ausgeführt werden:Markieren Sie den Datenverkehr mit den **festgelegten** Befehlen.Konfigurieren des VertrauensstatusKonfigurieren der RichtlinienSie können Datenverkehr entweder nur mit den **festgelegten** Befehlen markieren.ODERKonfigurieren des Vertrauensstatus und/oder Konfigurieren der Richtlinien
- Für hardwarevermittelten Datenverkehr unterstützt PFC QoS keine Befehle zur **Bandbreite**, **Priorität**, **Warteschlangenbegrenzung** oder **zufällig erkannten** Richtlinienzuordnungsklassen. Sie können diese Befehle konfigurieren, da sie für softwaregesteuerten Datenverkehr verwendet werden können.
- PFC QoS unterstützt die Befehle **set qos-group** policy map class nicht.

Weitere Informationen zu diesen Einschränkungen finden Sie unter Konfigurieren von Richtlinienzuordnungs-Klassenaktionen.

Zugehörige Informationen

- QoS-Klassifizierung und -Kennzeichnung für Catalyst Switches der Serien 6500 und 6000 mit Cisco IOS Software
- QoS-Ausgabeplanung für Catalyst Switches der Serien 6500/6000 mit Cisco IOS-Systemsoftware
- QoS-Richtlinien für Catalyst Switches der Serien 6500 und 6000
- QoS-Klassifizierung und -Kennzeichnung für Catalyst Switches der Serien 6500 und 6000 mit CatOS-Software
- QoS-Ausgabeplanung für Catalyst Switches der Serien 6500 und 6000 mit CatOS-Systemsoftware
- Support-Seiten für LAN-Produkte
- Support-Seite zum Thema LAN-Switching
- Technischer Support und Dokumentation für Cisco Systeme