QoS-Richtlinien für Catalyst Switches der Serien 6500 und 6000

Inhalt

Einführung

QoS-Richtlinien in einem Netzwerk bestimmen, ob der Netzwerkverkehr innerhalb eines festgelegten Profils (Vertrag) liegt. Dies kann dazu führen, dass der Out-of-Profile-Datenverkehr abnimmt oder bis zu einem anderen DSCP-Wert (Differentiated Services Code Point) markiert wird, um einen vertraglich vereinbarten Servicelevel durchzusetzen. (DSCP ist ein Maß für die QoS-Ebene des Frames.)

Verwechseln Sie nicht die Traffic-Policing mit Traffic-Shaping. Beide stellen sicher, dass der Datenverkehr im Profil (Vertrag) verbleibt. Beim Sichern von Datenverkehr werden Pakete aus Profilen nicht gepuffert. Daher wird die Übertragungsverzögerung nicht beeinträchtigt. Sie verwerfen den Datenverkehr oder markieren ihn mit einer niedrigeren QoS-Ebene (DSCP-Markdown). Beim Traffic-Shaping dagegen puffern Sie Out-of-Profile-Datenverkehr und entlasten so den Traffic-Bursts. Dies wirkt sich auf die Verzögerungs- und Verzögerungsschwankungen aus. Traffic Shaping kann nur auf eine ausgehende Schnittstelle angewendet werden. Sie können Richtlinien sowohl für eingehende als auch für ausgehende Schnittstellen anwenden.

Die Catalyst 6500/600 Policy Feature Card (PFC) und PFC2 unterstützen nur die Eingangs-Policing. Die PFC3 unterstützt sowohl die Eingangs- als auch die Ausgangs-Policing. Traffic Shaping wird nur auf bestimmten WAN-Modulen für die Catalyst 6500/7600-Serie unterstützt, z. B. die Optical Services Modules (OSMs) und die FlexWAN-Module. Weitere Informationen finden Sie in den Konfigurationshinweisen für das Cisco Router-Modul der Serie 7600.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

Konventionen

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

QoS-Überwachungsparameter

Zum Einrichten von Richtlinien definieren Sie die Richtlinien und wenden sie auf Ports (portbasierte QoS) oder VLANs (VLAN-basierte QoS) an. Jeder Policer definiert einen Namen, einen Typ, eine Rate, einen Burst und Aktionen für In-Profil- und Out-of-Profile-Datenverkehr. Überwacher der Supervisor Engine II unterstützen auch Parameter mit Überschreitungsraten. Es gibt zwei Arten von Policers: Mikrostrom und Aggregat.

- **Microflow**: Die Datenverkehrsüberwachung für jeden verwendeten Port/VLAN wird separat auf Basis des Datenflusses geregelt.
- **Aggregate**: Richtlinien für den Datenverkehr über alle angewendeten Ports/VLANs.

Jeder Policer kann auf mehrere Ports oder VLANs angewendet werden. Der Fluss wird mithilfe der folgenden Parameter definiert:

- Quell-IP-Adresse
- Ziel-IP-Adresse
- Layer-4-Protokoll (z. B. User Datagram Protocol [UDP])
- Quellportnummer
- Zielportnummer

Sie können sagen, dass Pakete, die einem bestimmten Satz definierter Parameter entsprechen, demselben Fluss angehören. (Dies ist im Wesentlichen das gleiche Flusskonzept wie das, das NetFlow-Switching verwendet.)

Wenn Sie z. B. einen Microflow-Policer konfigurieren, um den TFTP-Datenverkehr in VLAN 1 und VLAN 3 auf 1 Mbit/s zu beschränken, sind für jeden Datenfluss in VLAN 1 1 und 1 Mbit/s für jeden Datenfluss in VLAN 3 zulässig. Mit anderen Worten: Wenn es in VLAN 1 drei Flüsse und in VLAN 3 vier Flüsse gibt, lässt der Microflow-Policer jeden dieser Flüsse 1 Mbit/s zu. Wenn Sie eine Aggregat-Policer konfigurieren, wird der TFTP-Datenverkehr für alle in VLAN 1 und VLAN 3 kombinierten Flows auf 1 Mbit/s begrenzt.

Wenn Sie Aggregat- und Mikroflow-Policer anwenden, führt QoS immer die schwerwiegendsten, von den Policern angegebenen Aktionen aus. Wenn z. B. ein Policer angibt, das Paket zu verwerfen, ein anderer gibt an, das Paket zu markieren, wird das Paket verworfen.

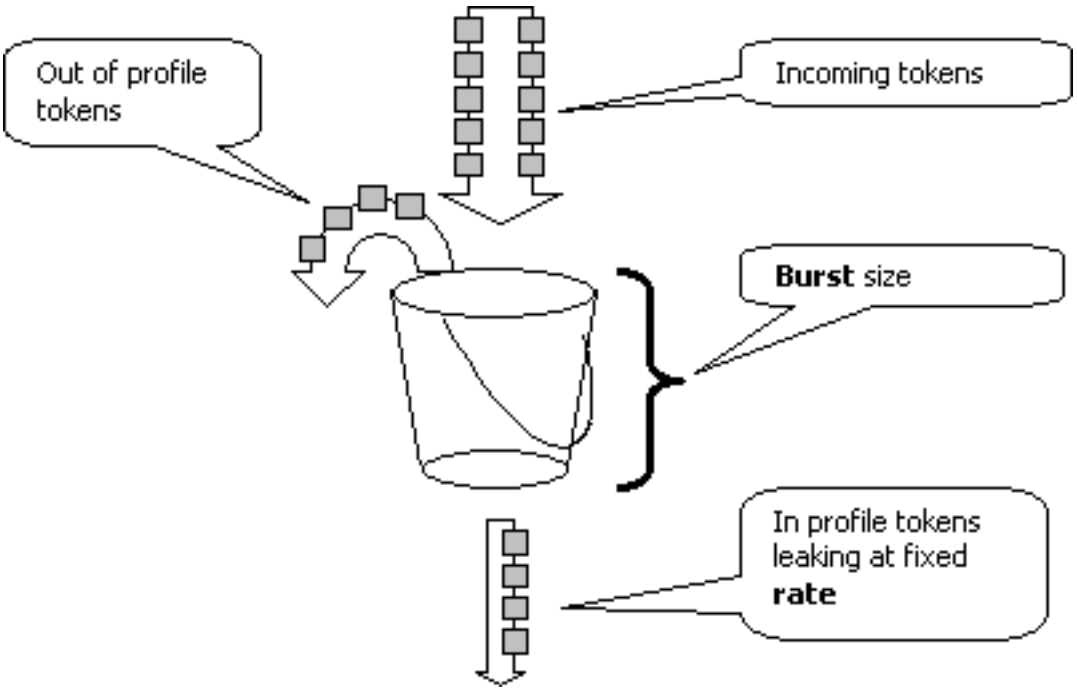
Standardmäßig arbeiten Microflow-Policers nur mit geroutetem (Layer 3 [L3]) Datenverkehr. Um auch Bridge-Datenverkehr (Layer 2 [L2]) zu überwachen, müssen Sie eine Bridge-Microflow-

Überwachung aktivieren. Auf der Supervisor Engine II müssen Sie eine überbrückte Microflow-Überwachung auch für die L3-Microflow-Überwachung aktivieren.

Die Richtlinienvergabe erfolgt protokollbasiert. Der gesamte Datenverkehr ist in drei Arten unterteilt:

- IP
- Internetwork Packet Exchange (IPX)
- Andere

Die Richtlinienvergabe wird auf dem Catalyst 6500/6000 nach einem "Schlitzeimer"-Konzept implementiert. Token, die eingehenden Datenverkehrspaketen entsprechen, werden in eine Eimer gelegt. (Jedes Token stellt ein Bit dar, sodass ein großes Paket durch mehr Token als ein kleines Paket dargestellt wird.) In regelmäßigen Abständen werden eine bestimmte Anzahl von Token aus dem Eimer entfernt und auf dem Weg dorthin gesendet. Wenn der Eimer keinen Platz für eingehende Pakete bietet, werden die Pakete als Out-of-Profile betrachtet. Sie werden entweder verworfen oder gemäß der konfigurierten Regelungsaktion deaktiviert.



Hinweis: Der Datenverkehr wird nicht im Puffer gepuffert, wie im Bild oben dargestellt. Der eigentliche Datenverkehr geht überhaupt nicht durch den Eimer. Der Eimer wird nur verwendet, um zu entscheiden, ob das Paket im Profil oder außerhalb des Profils ist.

Parameter berechnen

Mehrere Parameter steuern den Betrieb der Tokenbuchse, wie hier gezeigt:

- **Rate** (Übertragungsrate): Legt fest, wie viele Token in jedem Intervall entfernt werden. Dadurch wird effektiv die Policing-Rate festgelegt. Der gesamte Datenverkehr unter der Rate wird als "In-Profile" betrachtet.
- **Interval** (Intervall): Legt fest, wie oft Token aus dem Eimer entfernt werden. Das Intervall ist auf 0,00025 Sekunden festgelegt, sodass Token 4000 Mal pro Sekunde aus dem Eimer entfernt werden. Das Intervall kann nicht geändert werden.
- **Burst** (**Burst**): Legt die maximale Anzahl von Token fest, die der Eimer gleichzeitig aufnehmen kann. Um die angegebene Datenverkehrsrate aufrechtzuerhalten, sollte der Burst mindestens

die Durchsatzzeiten des Intervalls betragen. Ein weiterer Grund ist, dass das Paket mit maximaler Größe in die Eimer passen muss.

Um den Burst-Parameter zu bestimmen, verwenden Sie die folgende Gleichung:

- Burst = (Rate [bps]) * 0,00025 [sec/interval]) *oder* (maximale Paketgröße [Bits]), je nachdem, welcher Wert größer ist.

Wenn Sie beispielsweise den minimalen Burst-Wert berechnen möchten, der für die Aufrechterhaltung einer Übertragungsrate von 1 Mbit/s in einem Ethernet-Netzwerk erforderlich ist, wird die Rate als 1 Mbit/s definiert, und die maximale Ethernet-Paketgröße beträgt 1.518 Byte. Die Gleichung lautet:

- Burst = (1.000.000 Bit/s * 0,00025) *oder* (1.518 Byte * 8 Bit/Byte) = 250 *oder* 1.2144.

Das größere Ergebnis ist 12144, die Sie bis zu 13 Kbit/s.

Hinweis: In der Cisco IOS®-Software wird die Regelungsrate in Bits pro Sekunde (bps) definiert, im Gegensatz zu Kbit/s in Catalyst OS (CatOS). Auch in der Cisco IOS Software wird die Burst-Rate in Byte und nicht in Kilobit in CatOS definiert.

Hinweis: Aufgrund der Detailgenauigkeit der Hardwarerichtlinien werden die genaue Rate und der Burst auf den nächstgelegenen unterstützten Wert gerundet. Stellen Sie sicher, dass der Burst-Wert nicht geringer ist als der Maximalwert des Pakets. Andernfalls werden alle Pakete, die größer als die Burst-Größe sind, verworfen.

Wenn Sie beispielsweise versuchen, die Burst in der Cisco IOS-Software auf 1518 festzulegen, wird sie auf 1000 gerundet. Dadurch werden alle Frames mit einer Größe von mehr als 1000 Byte verworfen. Die Lösung besteht darin, Burst auf 2000 zu konfigurieren.

Wenn Sie die Burst-Rate konfigurieren, berücksichtigen Sie, dass einige Protokolle (z. B. TCP) einen Flow-Control-Mechanismus implementieren, der auf Paketverluste reagiert. TCP reduziert beispielsweise die Fenstergröße für jedes verlorene Paket um die Hälfte. Daher ist die effektive Verbindungsauslastung bei der Festlegung einer bestimmten Rate niedriger als die konfigurierte Rate. Sie können die Burst erhöhen, um eine bessere Auslastung zu erreichen. Ein guter Anfang für diesen Datenverkehr ist die Verdoppelung der Burst-Größe. (In diesem Beispiel wird die Burst-Größe von 13 Kbit/s auf 26 Kbit/s erhöht). Überwachen Sie dann die Leistung, und nehmen Sie bei Bedarf weitere Anpassungen vor.

Aus demselben Grund wird nicht empfohlen, den Richtlinienbetrieb mit verbindungsorientiertem Datenverkehr zu vergleichen. Dies zeigt in der Regel eine geringere Leistung als die Überwachung.

Polizeiaktionen

Wie in der Einführung erwähnt, kann die Richtlinie einem Out-of-Profile-Paket eine von zwei Möglichkeiten bieten:

- Paketverlust (der `Drop`-Parameter in der Konfiguration)
- Markierung des Pakets auf ein niedrigeres DSCP (der `policed-dscp`-Parameter in der Konfiguration)

Um das Paket zu markieren, müssen Sie die geregelte DSCP-Zuordnung ändern. Das überwachte DSCP wird standardmäßig so konfiguriert, dass es das Paket auf dasselbe DSCP markiert. (Es wird kein Markierungsvorgang durchgeführt.)

Hinweis: Wenn "Out-of-Profile"-Pakete bis zu einem DSCP markiert werden, der einer anderen Ausgabewarteschlange als das ursprüngliche DSCP zugeordnet ist, können einige Pakete in der falschen Reihenfolge gesendet werden. Aus diesem Grund wird empfohlen, Pakete, die kein Profil haben, mit einem DSCP zu kennzeichnen, das derselben Ausgabewarteschlange wie In-Profile-Pakete zugeordnet ist, wenn die Reihenfolge der Pakete wichtig ist.

Bei der Supervisor Engine II, die eine Überlastung unterstützt, sind zwei Auslöser möglich:

- Wenn der Datenverkehr die normale Rate überschreitet
- Wenn der Datenverkehr das Übermaß übersteigt

Ein Beispiel für die Anwendung einer Überdatenrate ist die Markierung von Paketen, die die normale Rate überschreiten, und das Verwerfen von Paketen, die die Überschreitungsrate überschreiten.

Vom Catalyst 6500/6000 unterstützte Richtlinienfunktionen

Wie in der Einführung angegeben, unterstützen PFC1 auf der Supervisor Engine 1a und PFC2 auf der Supervisor Engine 2 nur die Eingangs- (Inbound Interface)-Policing. PFC3 auf der Supervisor Engine 720 unterstützt die Überwachung von ein- und ausgehenden Datenströmen (Outbound Interface).

Der Catalyst 6500/6000 unterstützt bis zu 63 Mikroflow-Policers und bis zu 1023 Aggregation Policers.

Die Supervisor Engine 1a unterstützt die Eingangs-Policing, beginnend mit CatOS Version 5.3(1) und Cisco IOS Software Version 12.0(7)XE.

Hinweis: Für die Richtlinienvergabe mit der Supervisor Engine 1a ist eine PFC- oder PFC2-Tochterkarte erforderlich.

Die Supervisor Engine 2 unterstützt Eingangs-Policing, beginnend mit CatOS 6.1(1) und Cisco IOS Software Release 12.1(5c)EX. Die Supervisor Engine II unterstützt den Parameter für die Überwachung bei Überschreitungsraten.

Konfigurationen mit DFCs (Distributed Forwarding Cards) unterstützen nur portbasierte Richtlinien. Außerdem zählt die aggregierte Policer nur den Datenverkehr pro Weiterleitungs-Engine und nicht pro System. DFC und PFC sind Forwarding Engines. Wenn ein Modul (Linecard) über keine DFC verfügt, wird eine PFC als Weiterleitungs-Engine verwendet.

Update der Richtlinienfunktionen für die Supervisor Engine 720

Hinweis: Wenn Sie mit der Catalyst 6500/6000-QoS-Richtlinienvergabe nicht vertraut sind, lesen Sie unbedingt die Abschnitte QoS-Richtlinienparameter und Richtlinienfunktionen, die von den Catalyst 6500/6000 unterstützt werden.

Die Supervisor Engine 720 hat die folgenden neuen QoS-Richtlinienfunktionen eingeführt:

- **Überwachung des Datenausgangs**. Der Supervisor 720 unterstützt die Eingangs-Policing auf einem Port oder einer VLAN-Schnittstelle. Sie unterstützt die Egress-Policing auf einem Port oder einer gerouteten L3-Schnittstelle (bei Cisco IOS System-Software). Alle Ports im VLAN

werden unabhängig vom Port-QoS-Modus (Port-basierte QoS oder VLAN-basierte QoS) auf Ausgangs-Ports geregelt. Microflow Policing wird beim Ausgang nicht unterstützt. Beispielkonfigurationen finden Sie im Abschnitt Konfigurieren und Überwachen der Richtlinienüberwachung in der CatOS-Software und Konfigurieren und Überwachen der Richtlinien im Abschnitt Cisco IOS-Software dieses Dokuments.

- **Benutzerspezifische Mikroflow-Überwachung**. Der Supervisor 720 unterstützt eine Erweiterung der Microflow-Richtlinien, die als benutzerspezifische Microflow-Überwachung bezeichnet wird. Diese Funktion wird nur von der Cisco IOS-Systemsoftware unterstützt. Sie ermöglicht es Ihnen, für jeden Benutzer (pro IP-Adresse) hinter den angegebenen Schnittstellen eine bestimmte Bandbreite bereitzustellen. Dies wird durch Angeben einer Flussmaske innerhalb der Dienstrichtlinie erreicht. Die Flussmaske definiert, welche Informationen verwendet werden, um zwischen den Flüssen zu unterscheiden. Wenn Sie z. B. eine Quellablaufmaske angeben, wird der gesamte Datenverkehr von einer IP-Adresse als ein Datenfluss betrachtet. Mit dieser Technik können Sie den Datenverkehr pro Benutzer an einigen Schnittstellen steuern (wo Sie die entsprechende Dienstrichtlinie konfiguriert haben). auf anderen Schnittstellen verwenden Sie weiterhin die Standardablaufmaske. Es ist möglich, gleichzeitig bis zu zwei verschiedene QoS-Flussmasken im System zu aktivieren. Sie können nur eine Klasse einer Flussmaske zuordnen. Eine Richtlinie kann bis zu zwei verschiedene Flow-Masken enthalten.

Eine weitere wichtige Änderung bei der Richtlinienvergabe für die Supervisor Engine 720 ist, dass sie Datenverkehr nach der L2-Länge des Frames zählen kann. Dies unterscheidet sich von der Supervisor Engine 2 und der Supervisor Engine 1, die IP- und IPX-Frames nach ihrer L3-Länge zählen. Bei einigen Anwendungen ist die L2- und L3-Länge möglicherweise nicht konsistent. Ein Beispiel ist ein kleines L3-Paket in einem großen L2-Frame. In diesem Fall zeigt die Supervisor Engine 720 möglicherweise eine etwas andere überwachte Datenverkehrsrate an als die Supervisor Engine 1 und die Supervisor Engine 2.

Konfigurieren und Überwachen von Richtlinien in der CatOS-Software

Die Richtlinienkonfiguration für CatOS besteht aus drei Hauptschritten:

1. Definieren Sie eine Richtlinie - die normale Datenverkehrsrate, die Überrate (falls zutreffend), den Burst und die Richtlinienanwendung.
2. Erstellen Sie eine QoS-ACL, um Datenverkehr zur Polizei auszuwählen, und fügen Sie eine Richtlinie zu dieser ACL hinzu.
3. Wenden Sie die QoS-ACL auf die erforderlichen Ports oder VLANs an.

Dieses Beispiel zeigt, wie der gesamte Datenverkehr an UDP-Port 111 auf Port 2/8 geregelt wird.

Catalyst 6500/6000

```
set qos enable
!--- This enables QoS. set qos policer aggregate
udp_1mbps rate 1000 burst 13 drop !--- This defines a
policer. For the calculation of rate and burst, !---
refer to Calculate Parameters. set qos acl ip
udp_qos_port dscp 0 aggregate udp_1mbps udp any any eq
111 !--- This creates QoS ACL to select traffic and
attaches !--- the policer to the QoS ACL. commit qos acl
```

```
all !--- This compiles the QoS ACL. set qos acl map
udp_qos_port 2/8 !--- This maps the QoS ACL to the
switch port.
```

Das nächste Beispiel ist dasselbe. In diesem Beispiel fügen Sie die Richtlinie jedoch an ein VLAN an. Port 2/8 gehört zu VLAN 20.

Hinweis: Sie müssen die Port-QoS in den `VLAN-basierten` Modus ändern. Führen Sie dies mit dem Befehl **set port qos** durch.

Dieser Policer bewertet den Datenverkehr aller Ports in diesem VLAN, die für VLAN-basierte QoS konfiguriert sind:

Catalyst 6500/6000

```
set qos enable
!--- This enables QoS. set qos policer aggregate
udp_1mbps rate 1000 burst 13 drop !--- This defines a
policer. For the calculation of rate and burst, !---
refer to Calculate Parameters. set qos acl ip
udp_qos_vlan dscp 0 aggregate udp_1mbps udp any any eq
111 !--- This creates the QoS ACL to select traffic and
attaches !--- the policer to QoS ACL. commit qos acl all
!--- This compiles the QoS ACL. set port qos 2/8 vlan-
based !--- This configures the port for VLAN-based QoS.
set qos acl map udp_qos_vlan 20 !--- This maps QoS ACL
to VLAN 20.
```

Als Nächstes markieren Sie die Out-of-Profile-Pakete mit DSCP 32 auf ein DSCP von 0 (Best Effort).

Catalyst 6500/6000

```
set qos enable
!--- This enables QoS. set qos policer aggregate
udp_1mbps rate 1000 burst 13 policed-dscp !--- This
defines a policer. For the calculation of rate and
burst, !--- refer to Calculate Parameters. set qos acl
ip udp_qos_md trust-ipprec aggregate udp_1mbps udp any
any eq 111 dscp-field 32 !--- Note: The above command
should be on one line. !--- This creates the QoS ACL to
select traffic and attaches !--- the policer to the QoS
ACL.

commit qos acl all
!--- This compiles the QoS ACL. set qos policed-dscp-map
32:0 !--- This modifies the policed DSCP map to mark
down DSCP 32 to DSCP 0. set port qos 2/8 vlan-based !---
This configures the port for VLAN-based QoS. set qos acl
map udp_qos_md 20 !--- This maps the QoS ACL to VLAN 20.
```

Dieses Beispiel zeigt die Konfiguration für die Ausgangsüberwachung nur für die Supervisor Engine 720. Es zeigt, wie der gesamte ausgehende IP-Datenverkehr über VLAN 3 auf 10 Mbit/s überwacht wird.

Catalyst 6500/6000

```
set qos enable
!--- This enables QoS. set qos policer aggregate
egress_10mbps rate 10000 burst 20 drop !--- This defines
a policer. For the calculation of rate and burst, !---
refer to Calculate Parameters. set qos acl ip egress_pol
trust-ipprec aggregate egress_10mbps ip any any !---
This creates the QoS ACL to select traffic and attaches
!--- the policer to the QoS ACL. commit qos acl all !---
This compiles the QoS ACL. set qos acl map egress_pol 3
output !--- This maps the QoS ACL to VLAN 3 in the
output direction.
```

Verwenden Sie **show qos maps runtime policed-dscp-map**, um die aktuell geregelte DSCP-Zuordnung anzuzeigen.

Verwenden **der show qos policer runtime {*policer_name* | all}**, um die Parameter der Richtlinie zu überprüfen. Sie können auch die QoS-ACL sehen, an die die Richtlinie angeschlossen ist.

Hinweis: Bei der Supervisor Engine 1 und 1a können keine Policing-Statistiken für einzelne aggregierte Policers erstellt werden. Verwenden Sie den folgenden Befehl, um die Statistiken zur systeminternen Richtlinienvergabe anzuzeigen:

```
Cat6k> (enable) show qos statistics l3stats
Packets dropped due to policing: 1222086
IP packets with ToS changed: 27424
IP packets with CoS changed: 3220
Non-IP packets with CoS changed: 0
```

Verwenden Sie den folgenden Befehl, um Microflow Policing-Statistiken zu überprüfen:

```
Cat6k> (enable) show mls entry qos short
Destination-IP  Source-IP Port  DstPrt SrcPrt Uptime  Age
--------------- --------------- ----- ------ ------ -------- --------

IP bridged entries:
239.77.77.77 192.168.10.200UDP   63 6300:22:02 00:00:00
Stat-Pkts : 165360
Stat-Bytes : 7606560
Excd-Pkts : 492240
Stat-Bkts : 1660
239.3.3.3192.168.11.200UDP  888 77700:05:38 00:00:00
Stat-Pkts : 42372
Stat-Bytes : 1949112
Excd-Pkts : 126128
Stat-Bkts : 1628

Only out of the profile MLS entries are displayed
Cat6k> (enable)
```

Mit der Supervisor Engine II können Sie aggregierte Policing-Statistiken pro Policer anzeigen, indem Sie den Befehl **show qos statistics aggregate-policer** ausführen.

In diesem Beispiel ist ein Datenverkehrsgenerator an Port 2/8 angeschlossen. Er sendet 17 Mbit/s UDP-Datenverkehr mit Zielport 111. Es wird erwartet, dass die Polizei 16/17 des Datenverkehrs verwirft. 1 Mbit/s sollte also durchlaufen:

```
Cat6k> (enable) show qos statistics aggregate-policer udp_1mbps
QoS aggregate-policer statistics:
```

```
Aggregate policerAllowed packet Packets exceed Packets exceed
                count        normal rate       excess rate
------------------------------ ------------- ------------- -------------
udp_1mbps58243997321089732108

Cat6k> (enable) show qos statistics aggregate-policer udp_1mbps
QoS aggregate-policer statistics:
Aggregate policerAllowed packet Packets exceed Packets exceed
                count        normal rate       excess rate
------------------------------ ------------- ------------- -------------
udp_1mbps58250497331989733198
```

Hinweis: Beachten Sie, dass die zulässigen Pakete um 65 und die überzähligen Pakete um 1090 gestiegen sind. Das bedeutet, dass die Polizei 1.090 Pakete verworfen und 65 Pakete durchgelassen hat. Sie können berechnen, dass 65 / (1090 + 65) = 0,056, oder ungefähr 1/17. Daher funktioniert die Überwachung ordnungsgemäß.

Konfigurieren und Überwachen von Richtlinien in der Cisco IOS Software

Die Konfiguration für die Richtlinienvergabe in der Cisco IOS-Software umfasst die folgenden Schritte:

1. Definieren Sie einen Policer.
2. Erstellen Sie eine ACL, um den zu überwachenden Datenverkehr auszuwählen.
3. Definieren Sie eine Klassenzuordnung zur Auswahl des Datenverkehrs mit ACL und/oder DSCP/IP-Rangfolge.
4. Definieren Sie eine Dienstrichtlinie, die eine Klasse verwendet, und wenden Sie die Richtlinie auf eine angegebene Klasse an.
5. Wenden Sie die Service-Richtlinie auf einen Port oder ein VLAN an.

Betrachten Sie das gleiche Beispiel wie im Abschnitt Konfigurieren und Überwachen der Richtlinien in der CatOS-Software, jetzt jedoch mit der Cisco IOS-Software. In diesem Beispiel ist ein Datenverkehrsgenerator an Port 2/8 angeschlossen. Es sendet 17 Mbit/s UDP-Datenverkehr mit Zielport 111:

Catalyst 6500/6000

```
mls qos
!--- This enables QoS. mls qos aggregate-policer
udp_1mbps 1000000 2000 conform-action transmit exceed-
action drop !--- Note: The above command should be on
one line. !--- This defines a policer. For the
calculation of rate and burst, !--- refer to Calculate
Parameters. !--- Note: The burst is 2000 instead of
1518, due to hardware granularity.

access-list 111 permit udp any any eq 111
!--- This defines the ACL to select traffic. class-map
match-all udp_qos match access-group 111 !--- This
defines the traffic class to police. policy-map
udp_policy class udp_qos police aggregate udp_1mbps !---
This defines the QoS policy that attaches the policer to
the traffic class. interface GigabitEthernet2/8
switchport service-policy input udp_policy !--- This
applies the QoS policy to an interface.
```

In der Cisco IOS-Software gibt es zwei Arten von aggregierten Policers: **benannt** und **pro Schnittstelle**. Der benannte Aggregat Policer regelt den kombinierten Datenverkehr von allen Schnittstellen, auf die er angewendet wird. Dies ist der im obigen Beispiel verwendete Typ. Die Richtlinie für die einzelnen Schnittstellen regelt den Datenverkehr auf jeder eingehenden Schnittstelle, auf die er angewendet wird, separat. In der Richtlinienzuordnungskonfiguration wird eine Richtlinie pro Schnittstelle definiert. Ein Beispiel für eine Aggregations-Policer pro Schnittstelle:

Catalyst 6500/6000

```
mls qos
!--- This enables QoS. access-list 111 permit udp any
any eq 111 !--- This defines the ACL to select traffic.
class-map match-all udp_qos match access-group 111 !---
This defines the traffic class to police. policy-map
udp_policy class udp_qos !--- This defines the QoS
policy that attaches the policer to the traffic class.
police 1000000 2000 2000 conform-action transmit exceed-
action drop !--- This creates a per-interface aggregate
!--- policer and applies it to the traffic class.
interface GigabitEthernet2/8 switchport service-policy
input udp_policy !--- This applies the QoS policy to an
interface.
```

Mikroflow-Policer werden in der Richtlinienzuordnungskonfiguration definiert, ebenso wie Aggregations-Policer für die einzelnen Schnittstellen. Im folgenden Beispiel wird jeder Fluss vom Host 192.168.2.2, der in VLAN 2 eingeht, auf 100 Kbit/s geregelt. Der gesamte Datenverkehr von 192.168.2.2 wird auf 500 Kbit/s aggregiert geregelt. VLAN 2 umfasst die Schnittstellen fa4/11 und fa4/12:

Catalyst 6500/6000

```
mls qos
!--- This enables QoS. access-list 1 permit 192.168.2.2
!--- This defines the access list to select traffic from
host 192.168.2.2. class-map match-all host_2_2 match
access-group 1 !--- This defines the traffic class to
police. policy-map host class host_2_2 !--- This defines
the QoS policy. police flow 100000 2000 conform-action
transmit exceed-action drop !--- This defines a
microflow policer. For the calculation of rate and !---
burst, refer to Calculate Parameters. police 500000 2000
2000 conform-action transmit exceed-action drop !---
This defines the aggregate policer to limit !--- traffic
from the host to 500 kbps aggregate. interface fa4/11
mls qos vlan-based interface fa4/12 mls qos vlan-based
!--- This configures interfaces in VLAN 2 for VLAN-based
QoS. interface vlan 2 service-policy input host !---
This applies the QoS policy to VLAN 2.
```

Das nachfolgende Beispiel zeigt eine Konfiguration für die Ausgangsüberwachung der Supervisor Engine 720. Sie legt die Richtlinien für den gesamten ausgehenden Datenverkehr an der Schnittstelle Gigabit Ethernet 8/6 bis 100 Kbit/s fest:

Catalyst 6500/6000

```
mls qos
```

```
!--- This enables QoS. access-list 111 permit ip any any
!--- This defines the ACL to select traffic. All IP
traffic is subject to policing. class-map match-all
cl_out match access-group 111 !--- This defines the
traffic class to police. policy-map pol_out class cl_out
police 100000 3000 3000 conform-action transmit exceed-
action drop !--- This creates a policer and attaches it
to the traffic class. interface GigabitEthernet8/6 ip
address 3.3.3.3 255.255.255.0 service-policy output
pol_out !--- This attaches the policy to an interface.
```

Das nachfolgende Beispiel zeigt eine Konfiguration für benutzerspezifische Richtlinien für die Supervisor Engine 720. Der Datenverkehr von Benutzern hinter Port 1/1 zum Internet wird auf 1 Mbit/s pro Benutzer geregelt. Der Datenverkehr aus dem Internet zu den Benutzern wird auf 5 Mbit/s pro Benutzer beschränkt:

Catalyst 6500/6000

```
mls qos
!--- This enables QoS. access-list 111 permit ip any any
!--- This defines the ACL to select user traffic. class-
map match-all cl_out match access-group 111 !--- This
defines the traffic class for policing. policy-map
pol_out class cl_out police flow mask src-only 1000000
32000 conform-act transmit exceed-act drop
!--- Only the source IP address is considered for flow
creation !--- on interfaces with this policy attached.
interface gigabit 1/1 !--- 1/1 is the uplink toward the
users. service-policy input pol_out !--- Traffic comes
in from users, so the policy is attached !--- in the
input direction. class-map match-all cl_in match access-
group 111 policy-map pol_in class cl_in police flow mask
dest-only 5000000 32000 conform-act transmit exceed-act
drop
!--- Only the destination IP address is considered for
flow creation !--- on interfaces with this policy
attached. interface gigabit 1/2 !--- 1/2 is the uplink
to the Internet. service-policy input pol_in
```

Zur Überwachung der Richtlinienvergabe können Sie folgende Befehle verwenden:

```
bratan# show mls qos
QoS is enabled globally
Microflow policing is enabled globally
QoS global counters:
Total packets: 10779
IP shortcut packets: 0
Packets dropped by policing: 2110223
IP packets with TOS changed by policing: 0
IP packets with COS changed by policing: 0
Non-IP packets with COS changed by policing: 0

bratan# show mls qos ip gigabitethernet 2/8
[In] Policy map is udp_policy [Out] Default.
QoS Summary [IP]: (* - shared aggregates, Mod - switch module)

Int   Mod Dir Class-map DSCP AgId Trust FlId AgForward-Pk AgPoliced-Pk
--------------------------------------------------------------------------------
Gi2/8 1   In  udp_qos   0    1*   No0 127451  2129602
```

```
bratan# show mls qos ip gigabitethernet 2/8
[In] Policy map is udp_policy [Out] Default.
QoS Summary [IP]: (* - shared aggregates, Mod - switch module)

Int   Mod Dir Class-map DSCP AgId Trust FlId AgForward-Pk AgPoliced-Pk
--------------------------------------------------------------------------------
Gi2/8 1   In  udp_qos   0    1*   No0 127755  2134670
```

Hinweis: Zugelassene Pakete sind um 304 und überzählige Pakete um 5068 gestiegen. Das bedeutet, dass die Richtlinienvergabe 5068 Pakete verworfen und 304 Pakete durchgelassen hat. Bei einer Eingangsrate von 17 Mbit/s muss die Überwachung 1/17 des Datenverkehrs passieren. Wenn Sie die verworfenen und weitergeleiteten Pakete vergleichen, sehen Sie, dass dies der Fall war: 304 / (304 + 5068) = 0,057 oder etwa 1/17. Eine geringfügige Abweichung ist aufgrund der Detailgenauigkeit der Hardware-Richtlinien möglich.

Verwenden Sie für Microflow Policing-Statistiken den Befehl **show mls ip detail**:

```
Orion# show mls ip detail
IP Destination IP Source        Protocol L4 Ports     Vlan Xtag L3-protocol
--------------+---------------+--------+-------------+----+----+-----------+
192.168.3.33192.168.2.2udp555 / 5550   1ip
192.168.3.3192.168.2.2udp63 / 630   1ip

[IN/OUT] Ports Encapsulation RW-Vlan RW-MACSourceRW-MACDestinationBytes
--------------+-------------+-------+--------------+-----------------+------------+
Fa4/11 - ----ARPA3    0030.7137.1000  0000.3333.3333314548
Fa4/11 - ----ARPA3    0030.7137.1000  0000.2222.2222314824

Packets     Age   Last SeenQoS      Police Count ThresholdLeak
------------+-----+---------+-----------+------------+---------+-----------+
6838     36   18:50:090x80  34619762*2^5 3*2^0
6844     36   18:50:090x80  34669562*2^5 3*2^0

Drop Bucket  Use-Tbl Use-Enable
----+-------+-------+----------+
YES   1968     NONO
YES   1937     NONO
```

Hinweis: Das Feld "`Police Count`" (`Polizeianzahl`) zeigt die Anzahl der pro Datenfluss überwachten Pakete.

Zugehörige Informationen

- Konfigurieren von QoS
- Quality of Service auf Catalyst Switches der Serie 6000
- LAN-Produktunterstützung
- Unterstützung der LAN Switching-Technologie
- Technischer Support und Dokumentation - Cisco Systems