QoS-Richtlinienvergabe und -Marking mit IOS-basierten Catalyst 4000/4500 Supervisor Engines

Inhalt

Einführung

Die Richtlinienfunktion bestimmt, ob der Datenverkehr innerhalb des angegebenen Profils (Vertrag) liegt. Die Richtlinienfunktion ermöglicht entweder das Verwerfen von Out-of-Profile-Datenverkehr oder das Markieren des Datenverkehrs in einen anderen DSCP-Wert (Differenzial Services Code Point), um den vertraglich vereinbarten Service Level durchzusetzen. DSCP ist ein Maß für die Quality of Service (QoS)-Ebene des Pakets. Neben DSCP werden auch IP-Rangfolge und Class of Service (CoS) verwendet, um die QoS-Ebene des Pakets zu übertragen.

Richtlinien sollten nicht mit Traffic-Shaping verwechselt werden, obwohl beide gewährleisten, dass der Datenverkehr innerhalb des Profils (Vertrag) bleibt. Durch das Policing wird der Datenverkehr nicht gepuffert, sodass die Übertragungsverzögerung nicht beeinträchtigt wird. Statt Out-of-Profile-Pakete zu puffern, verwirft die Richtlinie sie oder markiert sie mit einer anderen QoS-Ebene (DSCP-Markierung nicht verfügbar). Das Traffic Shaping puffert den Out-of-Profile-Datenverkehr und gleicht Datenverkehrsspitzen aus, wirkt sich jedoch auf Verzögerungen und Verzögerungsschwankungen aus. Das Shaping kann nur auf eine ausgehende Schnittstelle angewendet werden, während die Richtlinienvergabe sowohl auf ein- als auch auf ausgehende Schnittstellen angewendet werden kann.

Catalyst 4000/4500 mit Supervisor Engine 3, 4 und 2+ (ab jetzt in diesem Dokument SE3, SE4, SE2+) unterstützt die Richtlinienvergabe in ein- und ausgehenden Richtungen. Traffic Shaping wird ebenfalls unterstützt, aber dieses Dokument behandelt nur Richtlinien und Markierungen. Bei der Markierung wird die Paket-QoS-Ebene entsprechend einer Richtlinie geändert.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

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

QoS-Überwachungs- und Markierungsparameter

Die Richtlinienvergabe wird durch Definition der QoS-Richtlinienzuordnungen und deren Anwendung auf Ports (Port-basierte QoS) oder VLANs (VLAN-basierte QoS) eingerichtet. Die Überwachung wird durch Rate- und Burst-Parameter sowie Aktionen für In-Profile- und Out-of-Profile-Datenverkehr definiert.

Es werden zwei Arten von Policers unterstützt: Aggregat und pro Schnittstelle. Jeder Policer kann auf mehrere Ports oder VLANs angewendet werden.

Die aggregierte Policer verarbeitet den Datenverkehr über alle angewendeten Ports/VLANs. So wird beispielsweise die aggregierte Richtlinie angewendet, um den TFTP-Datenverkehr (Trivial File Transfer Protocol) auf 1 Mbit/s in den VLANs 1 und 3 zu beschränken. Eine solche Richtlinie ermöglicht 1 Mbit/s des TFTP-Datenverkehrs in den VLANs 1 und 3 zusammen. Wenn eine Richtlinie pro Schnittstelle angewendet wird, wird der TFTP-Datenverkehr in den VLANs 1 und 3 auf 1 Mbit/s begrenzt.

Hinweis: Wenn sowohl die Ein- als auch die Ausgangs-Policing auf ein Paket angewendet werden, wird die schwerwiegendste Entscheidung getroffen. Das heißt, wenn die Eingangs-Policer angibt, das Paket zu verwerfen und die Ausgangs-Policer angibt, das Paket herunterzumarkieren, wird das Paket verworfen. In Tabelle 1 sind die QoS-Aktionen für das Paket zusammengefasst, wenn es durch Eingangs- und Ausgangsrichtlinien behandelt wird.

Tabelle 1: QoS-Aktion abhängig von Eingangs- und Ausgangsrichtlinie

	Ingress policy			
Egress policy	**Transmit**	**Drop**	**Markdown$_i$**	**Mark$_i$**
Transmit	Transmit	Drop	Markdown$_i$	Mark$_i$
Drop	Drop	Drop	Drop	Drop
Markdown$_e$	Markdown$_e$	Drop	Markdown$_e$	Markdown$_e$
Mark$_e$	Mark$_e$	Drop	Mark$_e$	Mark$_e$

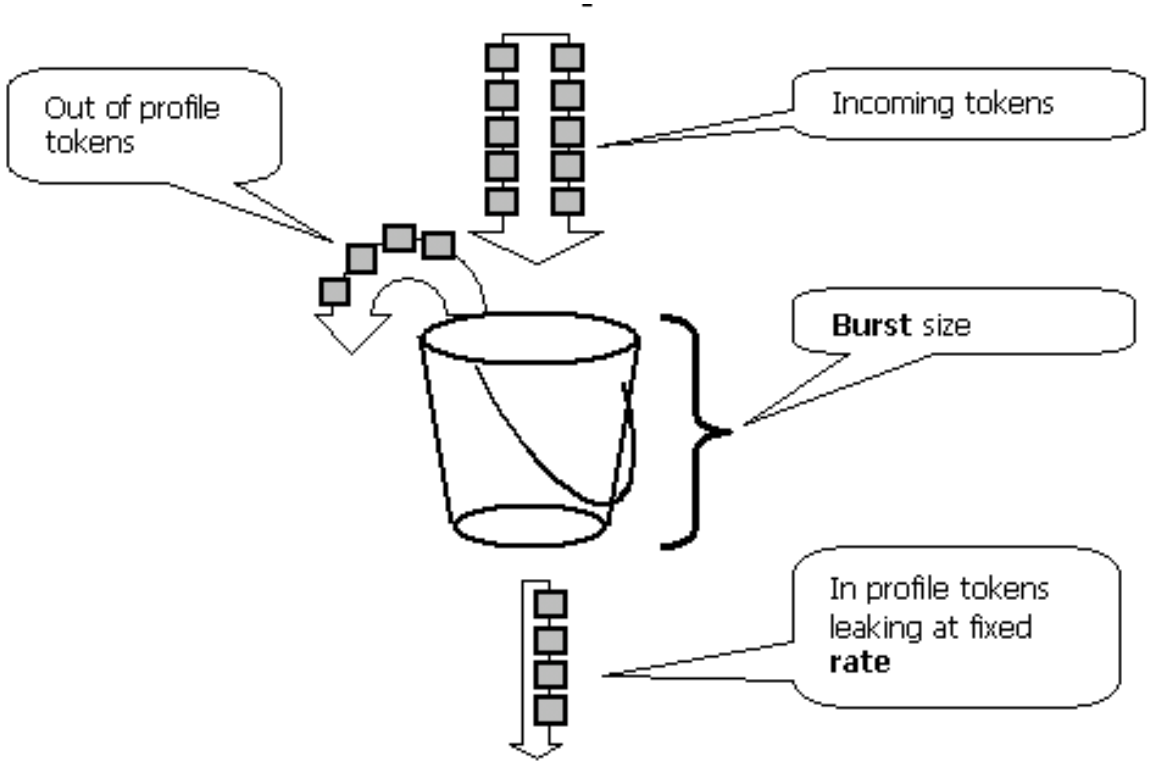
Die Catalyst 4000 SE3-, SE4-, SE2+ QoS-Hardware wird so implementiert, dass eine tatsächliche Markierung des Pakets nach der Ausgangsüberwachung erfolgt. Das bedeutet, dass selbst wenn die Eingangsrichtlinie das Paket (durch Markierung der Markierung oder normale Markierung) ausführt, die Ausgangsrichtlinie Pakete mit der ursprünglichen QoS-Ebene weiterhin anzeigt. Die Ausgangs-Policy sieht das Paket so, als ob es nicht durch die Eingangs-Policy markiert worden wäre. Dies bedeutet Folgendes:

- Durch die Markierung des Ausgangs wird die Eingangsmarkierung überschrieben.
- Die Ausgangsrichtlinie kann keine neuen QoS-Ebenen abgleichen, die durch die Eingangsmarkierung geändert werden.

Weitere wichtige Auswirkungen sind:

- Es ist nicht möglich, innerhalb derselben Richtlinie eine Markierung und Markierung innerhalb derselben Verkehrsklasse vorzunehmen.
- Aggregierte Policer sind richtungsabhängig. Das heißt, wenn eine aggregierte Policer sowohl für Eingang als auch Ausgang angewendet wird, gibt es zwei aggregierte Policer, eine für Eingang und eine für Ausgabe.
- Wenn innerhalb der Richtlinie eine aggregierte Policer auf die VLANs und die physische Schnittstelle angewendet wird, gibt es effektiv zwei aggregierte Policers - eine für die VLAN-Schnittstellen und eine andere für physische Schnittstellen. Derzeit ist es nicht möglich, die VLAN-Schnittstellen und die physischen Schnittstellen gemeinsam auf aggregierter Basis zu überwachen.

Die Richtlinienvergabe in Catalyst 4000 SE3, SE4 und SE2+ entspricht dem Schlitzkabelkonzept, wie das folgende Modell zeigt. Token, die eingehenden Datenverkehrspaketen entsprechen, werden in eine Bucket platziert (Anzahl Token = Größe des Pakets). In regelmäßigen Abständen wird eine definierte Anzahl von Token (abgeleitet von der konfigurierten Rate) aus dem Puffer entfernt. Wenn sich im Eimer kein Platz für ein eingehendes Paket befindet, wird das Paket als Out-of-Profile betrachtet und gemäß der konfigurierten Richtlinienaktion verworfen oder ausgezeichnet.



Es ist zu beachten, dass der Datenverkehr nicht im Puffer gespeichert wird, wie es im obigen Modell vorkommen könnte. Der tatsächliche Datenverkehr fließt überhaupt nicht über den Eimer. Der Eimer wird nur verwendet, um zu entscheiden, ob das Paket im Profil oder außerhalb des Profils ist.

Beachten Sie, dass die genaue Hardwareimplementierung für die Richtlinienvergabe anders sein kann, und dass sie funktional dem oben beschriebenen Modell entspricht.

Die folgenden Parameter steuern den Richtlinienbetrieb:

- Rate definiert, 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 definiert, wie oft Token aus dem Eimer entfernt werden. Das Intervall ist auf 16 Nanosekunden festgelegt (16 Sek. *10-9). Das Intervall kann nicht geändert werden.
- Burst definiert die maximale Anzahl von Token, die der Eimer zu jeder Zeit halten kann.

Im Abschnitt zum Vergleich von Richtlinien und Markierungen für Catalyst 6000- und Catalyst 4000/4500 IOS-basierte Supervisor Engines am Ende dieses Dokuments finden Sie Hinweise zu den Burst-Unterschieden zwischen Catalyst 6000 und Catalyst 4000 SE3, SE4, SE2+.

Die Überwachung stellt sicher, dass bei einer Untersuchung eines bestimmten Zeitraums (von null bis unendlich) die Überwachung niemals mehr als

```
<rate> * <period> + <burst-bytes> + <1 packet> bytes
```

des Datenverkehrs durch die Überwachung während dieses Zeitraums.

Die Catalyst 4000 SE3-, SE4-, SE2+ QoS-Hardware weist eine gewisse Präzision für die Richtlinienvergabe auf. Je nach konfigurierter Rate beträgt die maximale Abweichung von der Rate 1,5 % der Rate.

Bei der Konfiguration der Burst-Rate müssen Sie berücksichtigen, dass einige Protokolle (z. B. TCP) Mechanismen zur Flusskontrolle implementieren, die auf Paketverluste reagieren. TCP reduziert beispielsweise das Fenster für jedes verlorene Paket um die Hälfte. Bei einer Richtlinie mit einer bestimmten Geschwindigkeit ist die effektive Verbindungsauslastung niedriger als die konfigurierte Rate. Man kann die Burst erhöhen, um eine bessere Auslastung zu erreichen. Ein guter Anfang für diesen Datenverkehr wäre, den Burst auf das Doppelte des während der Round-Trip Time (RTT) mit der gewünschten Geschwindigkeit gesendeten Datenverkehrs festzulegen. Aus demselben Grund wird es nicht empfohlen, den Richtlinienbetrieb nach verbindungsorientiertem Datenverkehr zu vergleichen, da dieser im Allgemeinen eine geringere Leistung als der Policer erlaubt.

Hinweis: Der verbindungslose Datenverkehr reagiert möglicherweise auch anders auf Richtlinien. Beispielsweise verwendet das Network File System (NFS) Blöcke, die aus mehr als einem User Datagram Protocol (UDP)-Paket bestehen können. Ein verworfenes Paket kann die erneute Übertragung vieler Pakete (des gesamten Blocks) auslösen.

Im Folgenden wird der Burst für eine TCP-Sitzung mit einer Regelungsrate von 64 Kbit/s und einem TCP-RTT von 0,05 Sekunden berechnet:

```
<burst> = 2* <RTT> * <rate> = 2 * 0.05 [sec] * 64000/8 [bytes/sec] = 800 [bytes]
```

Hinweis: <burst**>** ist für eine TCP-Sitzung vorgesehen, daher sollte diese auf die durchschnittliche Anzahl der Sitzungen skaliert werden, die über die Richtlinie durchgeführt werden sollen. Dies ist nur ein Beispiel. Daher müssen in jedem Fall die Datenverkehrs-/Anwendungsanforderungen und das Verhalten im Vergleich zu den verfügbaren Ressourcen evaluiert werden, um Richtlinienparameter auszuwählen.

Die Regelungsaktion besteht darin, entweder das Paket zu verwerfen (verwerfen) oder das DSCP des Pakets zu ändern (markieren). Um das Paket zu markieren, muss die geregelte DSCP-

Zuordnung geändert werden. Das standardmäßig geregelte DSCP merkt das Paket an dasselbe DSCP, d. h. es erfolgt keine Markierung.

Hinweis: Pakete können in der Out-of-Order-Reihenfolge gesendet werden, wenn ein Out-of-Profile-Paket bis hinunter zu einem DSCP an eine andere Ausgabewarteschlange gekennzeichnet wird als das ursprüngliche DSCP. Aus diesem Grund wird empfohlen, bei der Bestellung von Paketen Pakete außerhalb des Profils auf DSCP zu markieren, das derselben Ausgabewarteschlange zugeordnet ist wie In-Profile-Pakete.

Richtlinien- und Markierungsfunktionen, die von den auf Catalyst 4000/4500 IOS basierenden Supervisor Engines unterstützt werden

Die Richtlinien für Eingang (eingehende Schnittstelle) und Ausgang (ausgehende Schnittstelle) werden auf Catalyst 4000 SE3, SE4, SE2+ unterstützt. Der Switch unterstützt 1024 Eingangs- und 1024 Ausgangs-Policers. Das System verwendet zwei Eingangs- und zwei Ausgangs-Policers für das Standardverhalten bei der Nichtüberwachung.

Beachten Sie, dass bei Anwendung der Aggregations-Policer innerhalb der Richtlinie auf ein VLAN und eine physische Schnittstelle ein zusätzlicher Eintrag für Hardware-Policer verwendet wird. Derzeit ist es nicht möglich, die VLAN-Schnittstellen und die physischen Schnittstellen gemeinsam auf aggregierter Basis zu überwachen. Dies kann bei zukünftigen Softwareversionen geändert werden.

Alle Softwareversionen bieten Unterstützung für Richtlinien. Der Catalyst 4000 unterstützt bis zu 8 gültige Übereinstimmungsanweisungen pro Klasse und bis zu 8 Klassen pro Richtlinienplan. Gültige Übereinstimmungsanweisungen sind:

- Abgleichberechtigungsgruppe
- match ip dscp
- Übereinstimmung IP-Rangfolge
- übereinstimmen

Hinweis: Bei Nicht-IP-V4-Paketen ist die **match ip dscp**-Anweisung die einzige Klassifizierungsmethode, vorausgesetzt, die Pakete gehen an Trunking-Ports über, die CoS vertrauen. Lassen Sie sich nicht durch das Schlüsselwort ip im Befehl **match ip dscp irreführen**, da internes DSCP zugeordnet ist. Dies gilt für alle Pakete, nicht nur für IP. Wenn ein Port so konfiguriert ist, dass er CoS vertrauenswürdig ist, wird dieser aus dem L2-Frame (802.1Q oder mit ISL gekennzeichneten Frame extrahiert und mithilfe einer CoS-zu-DSCP-QoS-Zuordnung in ein internes DSCP konvertiert. Dieser interne DSCP-Wert kann dann mithilfe von **match ip dscp** in der Richtlinie zugeordnet werden.

Gültige Richtlinienaktionen sind wie folgt:

- Polizei
- set ip dscp
- ip-Rangfolge festlegen
- dscp vertrauen
- Treuhandkosten

Durch Marking kann die QoS-Ebene des Pakets basierend auf Klassifizierung oder Richtlinien geändert werden. Bei der Klassifizierung wird der Datenverkehr basierend auf definierten Kriterien

in verschiedene Klassen für die QoS-Verarbeitung aufgeteilt. Um die IP-Rangfolge oder DSCP zu erreichen, muss die entsprechende eingehende Schnittstelle auf den vertrauenswürdigen Modus festgelegt werden. Der Switch unterstützt vertrauenswürdige CoS-, vertrauenswürdige DSCP- und nicht vertrauenswürdige Schnittstellen. Trust gibt das Feld an, von dem die QoS-Ebene des Pakets abgeleitet wird.

Beim Vertrauen auf CoS wird die QoS-Ebene vom L2-Header des gekapselten ISL- oder 802.1Q-Pakets abgeleitet. Beim Vertrauenswürdigen DSCP leitet der Switch die QoS-Ebene vom DSCP-Feld des Pakets ab. Das Vertrauen auf CoS ist nur für Trunking-Schnittstellen wichtig, und das Vertrauen auf DSCP ist nur für IP V4-Pakete gültig.

Wenn eine Schnittstelle nicht vertrauenswürdig ist (dies ist der Standardstatus bei aktivierter QoS), wird internes DSCP von der konfigurierbaren standardmäßigen CoS oder DSCP für die entsprechende Schnittstelle abgeleitet. Wenn keine CoS- oder DSCP-Standardeinstellung konfiguriert ist, ist der Standardwert 0 (0). Sobald die ursprüngliche QoS-Ebene des Pakets bestimmt ist, wird sie dem internen DSCP zugeordnet. Das interne DSCP kann durch Marking oder Richtlinien beibehalten oder geändert werden.

Wenn das Paket QoS verarbeitet, werden die QoS-Level-Felder (innerhalb des IP-DSCP-Felds für IP und innerhalb des ISL/802.1Q-Headers, falls vorhanden) vom internen DSCP aktualisiert.

Für die Konvertierung der vertrauenswürdigen QoS-Metriken des Pakets in das interne DSCP und umgekehrt werden spezielle Karten verwendet. Diese Karten sind wie folgt:

- DSCP zu überwachtem DSCP; wird verwendet, um beim Markieren des Pakets das Policed DSCP abzuleiten.
- DSCP an CoS: wird verwendet, um die CoS-Ebene vom internen DSCP abzuleiten, um den ISL/802.1Q-Header des ausgehenden Pakets zu aktualisieren.
- CoS zu DSCP: wird verwendet, um internes DSCP von eingehendem CoS (ISL/802.1Q-Header) abzuleiten, wenn sich die Schnittstelle im CoS-Modus Vertrauenswürdig befindet.

Wenn sich eine Schnittstelle im CoS-Modus "Vertrauenswürdig" befindet, entspricht die ausgehende CoS immer der eingehenden CoS. Dies gilt speziell für die QoS-Implementierung in Catalyst 4000 SE3, SE4 und SE2+.

Konfigurieren und Überwachen von Richtlinien

Die Konfiguration von Richtlinien in IOS umfasst die folgenden Schritte:

1. Definieren eines Policers.
2. Definieren von Kriterien zur Auswahl des Datenverkehrs für die Richtlinienvergabe.
3. Definieren von Dienstrichtlinien mithilfe von Klassen und Anwenden eines Policers auf eine angegebene Klasse.
4. Anwenden einer Service-Richtlinie auf einen Port oder ein VLAN.

Betrachten Sie das folgende Beispiel. An Port 5/14 ist ein Datenverkehrsgenerator angeschlossen, der ca. 17 Mbit/s UDP-Datenverkehr mit einem Ziel von Port 111 sendet. Dieser Datenverkehr soll auf bis zu 1 Mbit/s überwacht werden, und übermäßiger Datenverkehr sollte verworfen werden.

```
! enable qos
qos
```

```
! define policer, for rate and burst values, see 'policing parameters
qos aggregate-policer pol_1mbps 1mbps 1000 conform-action transmit
exceed-action
drop
! define ACL to select traffic
access-list 111 permit udp any any eq 111
! define traffic class to be policed
class-map match-all cl_test
match access-group 111
! define QoS policy, attach policer to traffic class
policy-map po_test
class cl_test
police aggregate pol_1mbps
! apply QoS policy to an interface
interface FastEthernet5/14
switchport access vlan 2
! switch qos to vlan-based mode on this port
qos vlan-based
! apply QoS policy to an interface
interface Vlan 2
service-policy output po_test
!
```

Beachten Sie, dass der Switch, wenn sich ein Port im VLAN-basierten QoS-Modus befindet, aber keine Service-Richtlinie auf das entsprechende VLAN angewendet wird, die Service-Richtlinie (falls zutreffend) befolgt, die auf einen physischen Port angewendet wird. Dies ermöglicht eine zusätzliche Flexibilität bei der Kombination von Port- und VLAN-basierter QoS.

Es werden zwei Arten von Policers unterstützt: Aggregat und Schnittstelle. Eine benannte Aggregat Policer überwacht den kombinierten Datenverkehr von allen Schnittstellen, auf die er angewendet wird. Im obigen Beispiel wurde ein benannter Policer verwendet. Anders als bei einer benannten Policer regelt eine Pro-Interface-Policer den Datenverkehr auf jeder Schnittstelle, auf der er angewendet wird, separat. In der Richtlinienzuordnungskonfiguration wird eine Richtlinie pro Schnittstelle definiert. Betrachten Sie das folgende Beispiel mit einem Aggregations-Policer für jede Schnittstelle:

```
! enable qos
qos
! define traffic class to be policed
class-map match-all cl_test2
match ip precedence 3 4
! define QoS policy, attach policer to traffic class
policy-map po_test2
class cl_test2
! per-interface policer is defined inside the policy map
police 512k 1000 conform-action transmit exceed-action drop
interface FastEthernet5/14
switchport
! set port to trust DSCP - need this to be able to match to incoming IP precedence
qos trust dscp
! switch to port-based qos mode
no qos vlan-based
! apply QoS policy to an interface
service-policy input po_test2
```

Der folgende Befehl wird zur Überwachung der Richtlinienoperationen verwendet:

```
Yoda#show policy-map interface FastEthernet5/14
FastEthernet5/14
```

```
service-policy input: po_test2
class-map: cl_test2 (match-all)
7400026 packets
match: ip precedence 3 4
police: Per-interface
Conform: 1166067574 bytes Exceed: 5268602114 bytes
class-map: class-default (match-any)
13312 packets
match: any
13312 packets
Yoda#show policy-map interface FastEthernet5/14
FastEthernet5/14
service-policy input: po_test2
class-map: cl_test2 (match-all)
7400138 packets
match: ip precedence 3 4
police: Per-interface
Conform: 1166088574 bytes Exceed: 5268693114 bytes
class-map: class-default (match-any)
13312 packets
match: any
13312 packets
```

Der Zähler bei der Klassenzuordnung zählt die Anzahl der Pakete, die der entsprechenden Klasse entsprechen.

Beachten Sie die folgenden Überlegungen zur Implementierung:

- Der Paketzähler pro Klasse ist nicht pro Schnittstelle. Das heißt, es zählt alle Pakete, die der Klasse entsprechen, auf allen Schnittstellen an, auf die diese Klasse in der Dienstrichtlinie angewendet wird.
- Policer verwalten keine Paket-Zähler, sondern nur Byte-Zähler.
- Es gibt keinen speziellen Befehl, um die angebotene oder ausgehende Datenverkehrsrate pro Policer zu überprüfen.
- Zähler werden regelmäßig aktualisiert. Wenn der obige Befehl wiederholt in schneller Folge ausgeführt wird, können Zähler irgendwann immer noch angezeigt werden.

Konfigurieren und Überwachen der Markierung

Die Konfiguration von Markierungen umfasst die folgenden Schritte:

1. Definieren Sie die Kriterien für die Klassifizierung des Datenverkehrs - Zugriffsliste, DSCP, IP-Rangfolge usw.
2. Definieren Sie die Datenverkehrsklassen, die anhand zuvor definierter Kriterien klassifiziert werden sollen.
3. Erstellen Sie eine Richtlinienzuordnung, die Markierungsaktionen und/oder Richtlinienaktionen an die definierten Klassen anhängt.
4. Konfigurieren des Vertrauensmodus für die entsprechende(n) Schnittstelle(n)
5. Wenden Sie die Richtlinienzuordnung auf eine Schnittstelle an.

Im folgenden Beispiel möchten wir eingehenden Datenverkehr mit der IP-Rangfolge 3 als Host für den UDP-Port 192.168.196.3, der 777 der IP-Rangfolge 6 zugeordnet ist, verwenden. Der gesamte andere Datenverkehr der IP-Rangfolge 3 wird auf 1 Mbit/s geregelt, und der überschüssige Datenverkehr muss bis zur IP-Rangfolge 2 markiert werden.

```
! enable QoS globally
qos
! define ACL to select UDP traffic to 192.168.196.3 port 777
ip access-list extended acl_test4
permit udp any host 192.168.196.3 eq 777
! define class of traffic using ACL and ip precedence matching
class-map match-all cl_test10
match ip precedence 3
match access-group name acl_test4
! all the remaining ip precedence 3 traffic will match this class
class-map match-all cl_test11
match ip precedence 3
! define policy with above classes
policy-map po_test10
class cl_test10
! mark traffic belonging to class with ip precedence 6
set ip precedence 6
class cl_test11
! police and mark down all other ip precedence 3 traffic
police 1 mbps 1000 exceed-action policed-dscp-transmit
!
! adjust DSCP to policed DSCP map so to map DSCP 24 to DSCP 16
qos map dscp policed 24 to dscp 16
!
interface FastEthernet5/14
! set interface to trust IP DSCP
qos trust dscp
! apply policy to interface
service-policy input po_test10
!
```

Der Befehl **sh policy interface** dient zur Überwachung der Markierung. Die Beispielausgabe und die Auswirkungen sind in der oben stehenden Richtlinienkonfiguration dokumentiert.

Vergleich von Richtlinien und Marking für IOS-basierte Catalyst Supervisor Engines der Serien 6000 und 4000/4500

Feature	Catalyst6000	Catalyst4000 SE3
Egress QoS policies	Not supported by Supervisor 1A and Superviso r2 hardware.	Supported.
Burst policing parameter calculation	Burst should be at least the same size as maximum frame supposed to pass via policer and no less then rate/interval, with the interval being 250 microseconds	No such restriction.
QoS policing L2 & L3	By default, microflow policing is only enabled for L3 on the sup1a and is not enabled at all for Supervisor 2. A CLI command is available to enable it for L2 on sup1a and L2 & L3 for sup2. Aggregate policing for sup1a & Supervisor 2 is enabled by default for L2 & L3.	Always.
Egress CoS	Always derived from internal DSCP using DSCP to CoS QoS map.	If the ingress port is in trust CoS mode, the egress CoS will be the same as the ingress CoS. Otherwise, it will be derived from the internal DSCP.
Microflow policing	Supported.	Not supported.
QoS behavior when port is in VLAN-based QoS mode, but no policy is applied to the VLAN.	No policy applied.	Fallback to port-based QoS. Will apply policy attached to port.

Zugehörige Informationen

- Verständnis und Konfiguration von QoS
- Technischer Support - Cisco Systems