Verständnis von QoS-Richtlinienvergabe und -Kennzeichnung auf dem Catalyst 3550

Inhalt

Einführung
Voraussetzungen
Anforderungen
Verwendete Komponenten
Konventionen
Hardware- und Softwareversionen
QoS-Überwachungs- und Markierungsparameter
Vom Catalyst 3550 unterstützte Funktionen für Richtlinienvergabe und Marking
Konfigurieren und Überwachen von Policing
Konfigurieren und Überwachen der Markierung
Klassifizierung des gesamten Schnittstellendatenverkehrs mit einem einzelnen Policer
Zugehörige Informationen

Einführung

Die Richtlinienfunktion bestimmt, ob die Datenverkehrsstufe innerhalb des angegebenen Profils oder Vertrags liegt. Sie ermöglicht Ihnen, Datenverkehr, der kein Profil hat, entweder abzubrechen oder auf einen anderen DSCP-Wert (Differenzial Services Code Point) zu markieren. Dadurch wird ein vertraglich vereinbarter Servicelevel erzwungen.

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.

Die Richtlinienvergabe ist nicht mit Traffic-Shaping zu verwechseln, obwohl beide sicherstellen, dass der Datenverkehr innerhalb des Profils oder Vertrags bleibt.

Die Richtlinienüberwachung puffert den Datenverkehr nicht, sodass die Richtlinienvergabe die Übertragungsverzögerung nicht beeinträchtigt. Statt Out-of-Profile-Pakete zu puffern, verwirft die Richtlinie sie oder markiert sie mit unterschiedlichen QoS-Ebenen (DSCP-Markdown).

Das Traffic Shaping puffert den Datenverkehr außerhalb des Profils und gleicht die Datenverkehrsspitzen aus, wirkt sich jedoch auf Verzögerungen und Verzögerungsschwankungen aus. Das Shaping kann nur auf die ausgehende Schnittstelle angewendet werden, während die Richtlinienvergabe sowohl auf die eingehende als auch die ausgehende Schnittstelle angewendet werden kann.

Der Catalyst 3550 unterstützt Richtlinien für ein- und ausgehende Richtungen. Traffic Shaping wird nicht unterstützt.

Durch Marking 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.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

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

Hardware- und Softwareversionen

Das Policing und Marking auf dem Catalyst 3550 wird von allen Softwareversionen unterstützt. Der aktuelle Konfigurationsleitfaden ist hier aufgeführt. In dieser Dokumentation finden Sie alle unterstützten Funktionen.

- Konfigurieren von QoS

QoS-Überwachungs- und Markierungsparameter

Um Richtlinien einzurichten, müssen Sie die QoS-Richtlinienzuordnungen definieren und auf Ports anwenden. Dies wird auch als portbasierte QoS bezeichnet.

Hinweis: VLAN-basierte QoS wird derzeit nicht von Catalyst 3550 unterstützt.

Die Überwachung wird durch Rate- und Burst-Parameter sowie Aktionen für Out-of-Profile-Datenverkehr definiert.

Diese beiden Policer-Typen werden unterstützt:

- Aggregieren
- Einzelperson

Die aggregierte Policer verarbeitet den Datenverkehr in allen Fällen, in denen er angewendet wird. Der einzelne Policer agiert separat beim Datenverkehr in jeder Instanz, in der er angewendet wird.

Hinweis: Auf dem Catalyst 3550 kann die aggregierte Policer nur auf verschiedene Klassen

derselben Richtlinie angewendet werden. Die aggregierte Richtlinienvergabe über mehrere Schnittstellen oder Richtlinien wird nicht unterstützt.

Wenden Sie beispielsweise den Aggregat-Policer an, um den Datenverkehr der Klassen customer1 und customer2 in derselben Richtlinienzuordnung auf 1 Mbit/s zu beschränken. Mit einer solchen Richtlinie können 1 Mbit/s Datenverkehr in der Klasse customer1 und customer2 gemeinsam verarbeitet werden. Wenn Sie die einzelne Richtlinie anwenden, beschränkt der Policer den Datenverkehr für die Klasse customer1 auf 1 Mbit/s und für die Klasse customer2 auf 1 Mbit/s. Daher ist jede Instanz des Policers separat.

In dieser Tabelle sind die QoS-Aktionen für das Paket zusammengefasst, wenn sie sowohl von Eingangs- als auch von Ausgangs-Richtlinien behandelt werden:

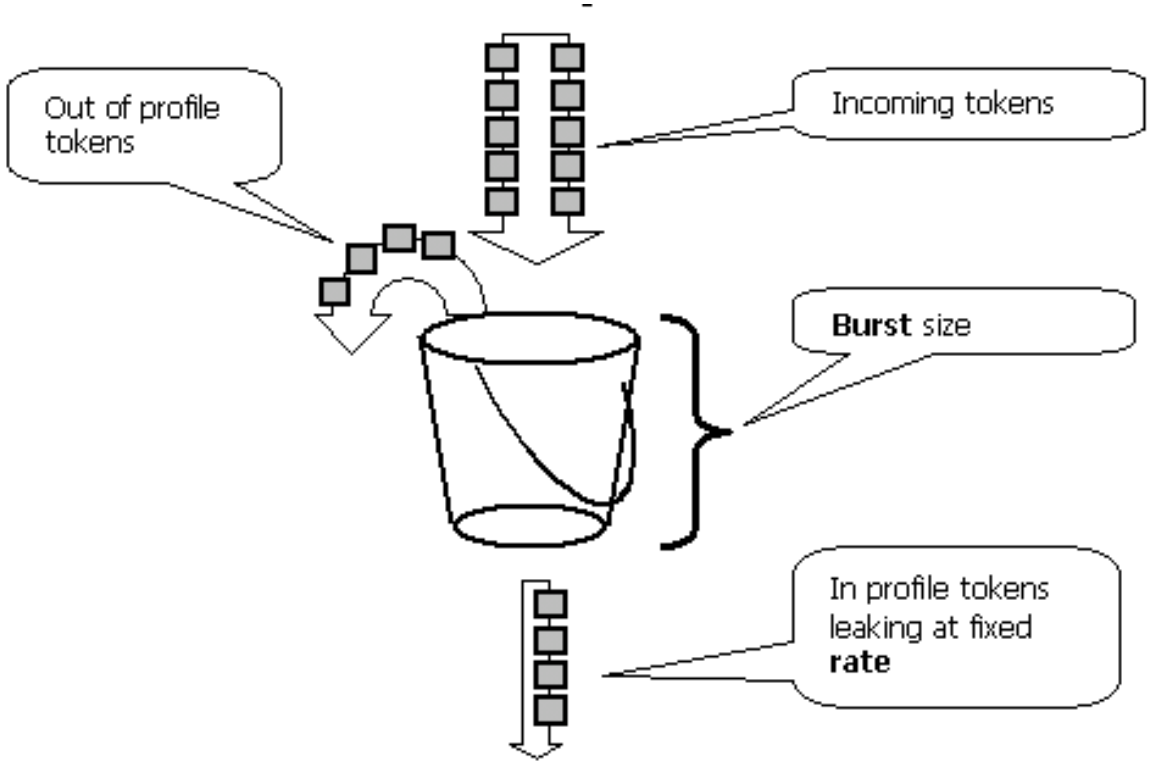
	Ingress policy			
Egress policy	Transmit	Drop	$Markdown_i$	$Mark_i$
Transmit	Transmit	Drop	$Markdown_i$	$Mark_i$
Drop	Drop	Drop	Drop	Drop
$Markdown_e$	$Markdown_e$	Drop	$Markdown_i$ then $Markdown_e$	$Mark_i$ then $Markdown_e$

Hinweis: Es ist möglich, innerhalb derselben Datenverkehrsklasse derselben Richtlinie Markierungen und Markierungen vorzunehmen. In diesem Fall wird der gesamte Datenverkehr für die jeweilige Klasse zuerst markiert. Richtlinien und Markierungen werden für bereits markierten Datenverkehr durchgeführt.

Die QoS-Richtlinienzuweisung für den Catalyst 3550 entspricht diesem Schlitzkabelkonzept:

Die Anzahl der Token, die proportional zu den Paketgrößen für eingehenden Datenverkehr sind, wird in einer Tokenbucket platziert. Die Anzahl der Token entspricht der Größe des Pakets. In einem regulären Intervall wird eine definierte Anzahl von Token aus der konfigurierten Rate entfernt. Wenn sich im Eimer kein Platz für ein eingehendes Paket befindet, wird das Paket als Out-of-Profile-Paket betrachtet und gemäß der konfigurierten Richtlinienaktion verworfen oder gekennzeichnet.

Dieses Konzept wird in diesem Beispiel veranschaulicht:



Hinweis: Der Datenverkehr wird nicht in der Gruppe gepuffert, wie es in diesem Beispiel vorkommen kann. Der tatsächliche Datenverkehr fließt überhaupt nicht durch die Eimer. Die Eimer wird nur verwendet, um zu entscheiden, ob sich das Paket im Profil oder außerhalb des Profils befindet.

Hinweis: Die Hardwareimplementierung der Richtlinienvergabe kann variieren, entspricht aber funktional immer noch diesem Modell.

Diese Parameter steuern den Richtlinienbetrieb:

- **Rate** (Übertragungsrate): Legt fest, wie viele Token in jedem Intervall entfernt werden. Dadurch wird effektiv die Policing-Rate festgelegt. Der gesamte Datenverkehr, der unter der Rate liegt, wird im Profil berücksichtigt. Die unterstützten Geschwindigkeiten liegen zwischen 8 Kbit/s und 2 Gbit/s und können schrittweise um 8 Kbit/s gesteigert werden.
- **Interval** (Intervall): Legt fest, wie oft Token aus dem Eimer entfernt werden. Das Intervall ist auf 0,125 Millisekunden (oder 8000 Mal pro Sekunde) festgelegt. Dieses Intervall kann nicht geändert werden.
- **Burst** (**Burst**): Legt die maximale Anzahl von Token fest, die der Eimer zu einem beliebigen Zeitpunkt speichern kann. Unterstützte Bursts reichen von 8.000 Byte bis 2.000.000 Byte und inkrementieren um 64 Byte.

Hinweis: Obwohl die Befehlszeilenhilfezeichenfolgen einen großen Wertebereich aufweisen, kann die Option "rate-bps" die konfigurierte Portgeschwindigkeit nicht überschreiten, und die Burst-Byte-Option darf 200000 Byte nicht überschreiten. Wenn Sie einen größeren Wert eingeben, lehnt der Switch die Richtlinienzuordnung ab, wenn Sie sie an eine Schnittstelle anhängen.

Um die angegebene Datenverkehrsrate aufrechtzuerhalten, muss der Burst mindestens die Summe dieser Gleichung betragen:

```
Burstmin (bits) = Rate (bps) / 8000 (1/sec)
```

Um beispielsweise eine Geschwindigkeit von 1 Mbit/s aufrechtzuerhalten, sollte der minimale

Burst-Wert berechnet werden. Die Rate wird als 1000 Kbit/s definiert, sodass der minimale Burst-Wert der Summe dieser Gleichung entspricht:

```
1000 (Kbps) / 8000 (1/sec) =125 (bits)
```

Die minimale unterstützte Burst-Größe beträgt 8000 Byte, was mehr ist als der minimale Burst berechnet.

Hinweis: Aufgrund der Detailgenauigkeit der Hardwarerichtlinien werden die genaue Rate und der Burst auf den nächstgelegenen unterstützten Wert gerundet.

Wenn Sie die Burst-Rate konfigurieren, müssen Sie berücksichtigen, dass einige Protokolle Mechanismen implementieren, die auf den Paketverlust reagieren. Das Transmission Control Protocol (TCP) reduziert beispielsweise das Fenster für jedes verlorene Paket um die Hälfte. Dies verursacht einen "Sägezahneffekt" im TCP-Datenverkehr, wenn TCP versucht, die Leitungsgeschwindigkeit zu erhöhen, und durch die Richtlinie gedrosselt wird. Wenn die durchschnittliche Rate des Sägezahnverkehrs berechnet wird, ist diese Rate viel niedriger als die überwachte Rate. Sie können die Burst jedoch erhöhen, um eine bessere Auslastung zu erreichen. Ein guter Anfang besteht darin, den Burst auf das Doppelte des während der Round-Trip Time (TCP RTT) gesendeten Datenverkehrs mit der gewünschten Rate festzulegen. Wenn RTT nicht bekannt ist, können Sie den Wert des Burst-Parameters verdoppeln.

Aus demselben Grund wird nicht empfohlen, den Richtlinienbetrieb nach verbindungsorientiertem Datenverkehr zu vergleichen. Dieses Szenario zeigt in der Regel eine geringere Leistung als durch die Richtlinie erlaubt.

Der verbindungslose Datenverkehr kann auch anders auf Richtlinien reagieren. Beispielsweise verwendet das Network File System (NFS) Blöcke, die aus mehr als einem User Datagram Protocol (UDP)-Paket bestehen können. Ein verworfenes Paket kann dazu führen, dass viele Pakete, auch der gesamte Block, erneut übertragen werden.

In diesem Beispiel wird der Burst für eine TCP-Sitzung mit einer Regelungsrate von 64 Kbit/s berechnet, wenn der TCP-RTT 0,05 Sekunden beträgt:

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

In diesem Beispiel ist `<burst>` eine TCP-Sitzung. Skalieren Sie diese Zahl so, dass die erwartete Anzahl an Sitzungen, die die Überwachung durchlaufen, ermittelt wird.

Hinweis: Dies ist nur ein Beispiel. In jedem Fall müssen Sie Datenverkehrs- und Anwendungsanforderungen und das Verhalten im Vergleich zu verfügbaren Ressourcen bewerten, um Richtlinienparameter auszuwählen.

Bei der Richtlinienaktion kann es sich um das Verwerfen des Pakets oder das Ändern des DSCP des Pakets (Markdown) handeln. Um das Paket zu markieren, muss eine geregelte DSCP-Zuordnung geändert werden. Bei einer standardmäßigen, richtliniengesteuerten DSCP-Zuordnung wird das Paket demselben DSCP zugeordnet. Daher findet kein Markup statt.

Pakete können in der falschen Reihenfolge gesendet werden, wenn ein nicht mehr als ein Profil vorliegendes Paket mit einem DSCP markiert wird, das einer anderen Ausgabewarteschlange als das ursprüngliche DSCP zugeordnet ist. Wenn die Paketreihenfolge wichtig ist, werden Out-of-Profile-Pakete an die DSCP der gleichen Ausgabewarteschlange zugeordnet wie In-Profile-Pakete.

Vom Catalyst 3550 unterstützte Funktionen für Richtlinienvergabe und Marking

Diese Tabelle enthält eine Zusammenfassung der richtlinienbasierten und markierungsbezogenen Funktionen, die vom Catalyst 3550 unterstützt werden. Diese sind nach den folgenden Richtungen untergliedert:

	Direction	
Feature	Ingress	Egress
Individual policers	Yes, totally 128 for GE and 8 for FE including ingress aggregate policers	Yes, totally 8 including egress aggregate policers
Aggregate policers	Yes, totally 128 for GE and 8 for FE including ingress individual policers	Yes, totally 8 including egress individual policers
Marking	Yes	No
Policer Markdown	Yes	Yes
Match with ACL	Yes	**No**
Match DSCP	Yes	**Yes**
Match IP precedence	Yes	No
Match COS	Yes, for non-IP traffic	No
Trust DSCP	Yes	No
Trust COS	Yes	No
Trust IP precedence	Yes	No

Pro Klassenzuordnung wird eine Match-Anweisung unterstützt. Dies sind gültige Übereinstimmungsanweisungen für die Eingangsrichtlinie:

- Abgleichberechtigungsgruppe
- match ip dscp
- Übereinstimmung IP-Rangfolge

Hinweis: Auf dem Catalyst 3550 wird der Befehl **match interface** nicht unterstützt, und in einer Klassenzuordnung ist nur ein Befehl match zulässig. Daher ist es schwierig, den gesamten Datenverkehr, der über eine Schnittstelle eingeht, zu klassifizieren und den gesamten Datenverkehr mit einer einzigen Richtlinie zu überwachen. Weitere Informationen finden Sie im Abschnitt Klassifizieren des gesamten Schnittstellendatenverkehrs mit einem einzelnen Policer in diesem Dokument.

Dies ist die gültige Match-Anweisung für die Ausgangs-Policy:

- match ip dscp

Dies sind gültige Richtlinienaktionen für die Eingangsrichtlinie:

- Polizei
- set ip dscp (Markierung)
- set ip priority (Marking)
- dscp vertrauen
- trust IP-Rangfolge
- Treuhandkosten

Diese Tabelle zeigt die Matrix der unterstützten Eingangs-QoS-Richtlinien:

Trust I/F	Match DSCP[1]	Match ACL	Trust Class[2]	Set DSCP[3]	Police	Result
						Traffic is assigned default QOS level of the port (0 by default)
√						QOS level of incoming traffic is preserved, according to what is trusted
	√		√		√	IP Traffic is matched by DSCP and then trusted then policed, excess traffic dropped or marked down
	√		√			IP Traffic is matched by DSCP/IP precedence and its QOS level is preserved
	√			√		IP Traffic is matched by DSCP/IP precedence then marked
	√			√	√	IP Traffic is matched by DSCP/IP precedence then marked then policed
		√	√		√	Traffic is matched by access list, QOS level of the matched traffic is preserved, then traffic is policed
		√	√			Traffic is matched by access list and its QOS level is preserved according to what is trusted
		√		√	√	Traffic is matched by access list then marked and then policed
		√		√		Traffic is matched by ACL then marked with specified DSCP/IP precedence
		MAC ACL w/COS	√			Match non-IP traffic by MAC EtherType and COS and preserve QOS level
		MAC ACL w/COS	√		√	Match non-IP IP traffic by MAC EtherType and COS and preserve QOS level then police
		MAC ACL w/COS		√		Match non-IP IP traffic by MAC EtherType and COS then mark matched traffic
		MAC ACL W/COS		√	√	Match non-IP IP traffic by MAC EtherType and COS then mark and then police

1. Diese Option behandelt auch die Übereinstimmung-IP-Rangfolge.
2. Diese Option umfasst vertrauensvolle CoS, IP-Rangfolge und DSCP.
3. Diese Option behandelt auch das Festlegen der IP-Rangfolge.

Dies ist die gültige Richtlinienaktion für die Ausgangs-Policy:

- Polizei

Diese Tabelle zeigt die Matrix der unterstützten Ausgangs-QoS-Richtlinien:

Match DSCP	Police	Result
		Traffic is sent out with COS and IP precedence according to QOS maps and internal DSCP after ingress QOS processing
√	√	Traffic is matched by DSCP and policed

Bei der Markierung kann die QoS-Ebene des Pakets abhängig von der Klassifizierung oder Richtlinienvergabe geändert werden. Bei der Klassifizierung wird der Datenverkehr basierend auf den definierten Kriterien in verschiedene Klassen für die QoS-Verarbeitung aufgeteilt.

Die QoS-Verarbeitung basiert auf dem internen DSCP. die Messung der QoS-Ebene des Pakets. Internes DSCP wird entsprechend der Konfiguration der Vertrauenswürdigkeit abgeleitet. Das System unterstützt vertrauenswürdige CoS-, DSCP-, IP-Rangfolge und nicht vertrauenswürdige Schnittstellen. Trust gibt das Feld an, von dem das interne DSCP für jedes Paket abgeleitet wird:

- Beim Vertrauen auf CoS wird die QoS-Ebene vom Layer-2-Header (L2) des Inter-Switch Link Protocol (ISL) oder des gekapselten 802.1Q-Pakets abgeleitet.
- Wenn DSCP oder die IP-Rangfolge als vertrauenswürdig eingestuft wird, leitet das System die QoS-Ebene entsprechend vom DSCP- oder IP-Rangfolgefeld des Pakets ab.

Das Vertrauen auf CoS ist nur für Trunking-Schnittstellen wichtig, und das Vertrauen auf DSCP (oder IP-Rangfolge) ist nur für IP-Pakete sinnvoll.

Wenn eine Schnittstelle nicht vertrauenswürdig ist, wird das interne DSCP von der konfigurierbaren CoS für die entsprechende Schnittstelle abgeleitet. Dies ist der Standardstatus, wenn QoS aktiviert ist. Wenn keine CoS-Standardeinstellung konfiguriert ist, ist der Standardwert 0.

Nachdem das interne DSCP bestimmt wurde, kann es durch Marking und Richtlinienvergabe geändert oder beibehalten werden.

Nachdem das Paket die QoS-Verarbeitung durchlaufen hat, werden seine 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 Richtlinienvergabe sind folgende spezielle QoS-Karten relevant:

- **DSCP-zu-Policed DSCP** - wird verwendet, um das geregelte DSCP beim Herunterfahren des Pakets abzuleiten.
- **DSCP-to-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 das interne DSCP vom eingehenden CoS (ISL/802.1Q-Header) abzuleiten, wenn sich die Schnittstelle im CoS-Modus "Vertrauenswürdig" befindet.

Dies sind wichtige Überlegungen zur Implementierung:

- Die Richtlinie für eingehende Dienste kann nicht an die Schnittstelle angehängt werden, wenn die Schnittstelle so konfiguriert ist, dass sie QoS-Metriken wie CoS/DSCP oder IP-Rangfolge vertrauenswürdig ist. Um eine Übereinstimmung mit der DSCP/IP-Rangfolge und der eingehenden Zugriffskontrolle zu erzielen, müssen Sie die Vertrauenswürdigkeit für die jeweilige Klasse innerhalb der Richtlinie und nicht in der Schnittstelle konfigurieren. Um eine

Markierung basierend auf der DSCP/IP-Rangfolge vorzunehmen, muss keine Vertrauenswürdigkeit konfiguriert werden.
- Nur IPv4-Datenverkehr ohne IP-Optionen und ARPA-Kapselung (Ethernet II Advanced Research Projects Agency) gilt als IP-Datenverkehr aus Hardware- und QoS-Sicht. Der gesamte andere Datenverkehr wird als Nicht-IP-Datenverkehr angesehen, einschließlich IP mit Optionen, wie z. B. gekapselte IP und IPv6.
- Bei Nicht-IP-Paketen ist "Match Access Group" die einzige Klassifizierungsmethode, da DSCP für Nicht-IP-Datenverkehr nicht zugeordnet werden kann. Zu diesem Zweck wird eine MAC-Zugriffsliste (Media Access Control) (ACL) verwendet. Pakete können basierend auf der Quell-MAC-Adresse, der Ziel-MAC-Adresse und dem EtherType zugeordnet werden. Es ist nicht möglich, den IP-Datenverkehr mit der MAC-ACL abzustimmen, da der Switch zwischen IP- und Nicht-IP-Datenverkehr unterscheidet.

Konfigurieren und Überwachen von Policing

Diese Schritte sind erforderlich, um die Richtlinienvergabe in Cisco IOS zu konfigurieren:

1. Definieren eines Policers (für aggregierte Policers)
2. Definieren von Kriterien zur Auswahl des Datenverkehrs für die Richtlinienvergabe
3. Definieren einer Klassenzuordnung zur Auswahl des Datenverkehrs anhand definierter Kriterien
4. Definieren einer Dienstrichtlinie mithilfe einer Klasse und Anwenden eines Policers auf die angegebene Klasse
5. Anwenden einer Service-Richtlinie auf einen Port

Diese beiden Policer-Typen werden unterstützt:

- Benanntes Aggregat
- Einzelperson

Der benannte aggregierte Policer regelt den Datenverkehr, der von allen Klassen innerhalb derselben Richtlinie kombiniert wird, an den Ort, an dem er angewendet wird. Aggregate Policing über verschiedene Schnittstellen hinweg wird nicht unterstützt.

Hinweis: Der aggregierte Policer kann nicht auf mehr als eine Richtlinie angewendet werden. Ist dies der Fall, wird die folgende Fehlermeldung angezeigt:

```
QoS: Cannot allocate policer for policy map <policy name>
```

Betrachten Sie dieses Beispiel:

An Port GigabitEthernet0/3 ist ein Datenverkehrsgenerator angeschlossen, der ca. 17 Mbit/s UDP-Datenverkehr an den Zielport 111 sendet. Es gibt auch TCP-Datenverkehr von Port 20. Diese beiden Datenverkehrsströme sollen auf bis zu 1 Mbit/s überwacht werden, und übermäßiger Datenverkehr muss verworfen werden. Dieses Beispiel zeigt, wie dies geschieht:

```
!--- Globally enables QoS. mls qos !--- Defines the QoS policer, sets the burst !--- to 16000
for better TCP performance. mls qos aggregate-policer pol_1mbps 1000000 16000 exceed-action drop
!--- Defines the ACLs to select traffic. access-list 123 permit udp any any eq 111
access-list 145 permit tcp any eq 20 any
```

```
!--- Defines the traffic classes to be policed. class-map match-all cl_udp111 match access-group
123
class-map match-all cl_tcp20
  match access-group 145
!--- Defines the QoS policy, and attaches !--- the policer to the traffic classes. policy-map
po_test
  class cl_udp111
    police aggregate pol_1mbps
  class cl_tcp20
    police aggregate pol_1mbps
!--- Applies the QoS policy to an interface. interface GigabitEthernet0/3 switchport switchport
access vlan 2 service-policy input po_test
!
```

Im ersten Beispiel wurde der benannte Aggregat Policer verwendet. Im Gegensatz zum benannten Policer regelt der einzelne Policer den Datenverkehr für jede Klasse, in der er angewendet wird. Der einzelne Policer wird in der Richtlinienzuordnungskonfiguration definiert. In diesem Beispiel werden zwei Datenverkehrsklassen von zwei einzelnen Policers überwacht. cl_udp111 wird auf 1 Mbit/s pro 8.000-Burst geregelt, und cl_tcp20 wird auf 512 Kbit/s pro 32.000-Burst festgelegt:

```
!--- Globally enables QoS. mls qos !--- Defines the ACLs to select traffic. access-list 123
permit udp any any eq 111
access-list 145 permit tcp any eq 20 any
!--- Defines the traffic classes to be policed. class-map match-all cl_udp111
  match access-group 123
class-map match-all cl_tcp20
  match access-group 145
!--- Defines QoS policy, and creates and attaches !--- the policers to the traffic classes.
policy-map po_test2
  class cl_udp111
    police 1000000 8000 exceed-action drop
  class cl_tcp20
    police 512000 32000 exceed-action drop
!--- Applies the QoS policy to an interface. interface GigabitEthernet0/3 switchport switchport
access vlan 2 service-policy input po_test2
```

Dieser Befehl wird zur Überwachung der Richtlinienoperation verwendet:

```
cat3550#show mls qos interface g0/3 statistics
GigabitEthernet0/3
Ingress
  dscp: incoming   no_change  classified policed    dropped (in pkts)
Others: 267718     0          267717     0          0
Egress
  dscp: incoming   no_change  classified policed    dropped (in pkts)
Others: 590877        n/a        n/a      266303     0

WRED drop counts:
  qid  thresh1    thresh2   FreeQ
   1 : 0          0         1024
   2 : 0          0         1024
   3 : 0          0         8
   4 : 0          0         1024
```

Hinweis: Standardmäßig gibt es keine DSCP-Statistiken. Der Catalyst 3550 unterstützt eine Erfassung von Statistiken pro Schnittstelle und Richtung für bis zu acht verschiedene DSCP-Werte. Dies wird konfiguriert, wenn Sie den Befehl **mls qos monitor** ausgeben. Um Statistiken für

die DSCPs 8, 16, 24 und 32 zu überwachen, müssen Sie den folgenden Befehl **pro Schnittstelle** ausführen:

```
cat3550(config-if)#mls qos monitor dscp 8 16 24 32
```

Hinweis: Der Befehl **mls qos monitor dscp 8 16 24 32** ändert die Ausgabe des Befehls **show mls qos int g0/3 statistics** wie folgt:

```
cat3550#show mls qos interface g0/3 statistics
GigabitEthernet0/3
Ingress
  dscp: incoming   no_change  classified policed    dropped (in pkts)
    8 : 0          0          675053785  0          0
    16: 1811748    0          0          0          0         ? per DSCP statistics
    24: 1227820404 15241073   0          0          0
    32: 0          0          539337294  0          0
Others: 1658208    0          1658208    0          0
Egress
  dscp: incoming   no_change  classified policed    dropped (in pkts)
    8 : 675425886     n/a        n/a      0          0
    16: 0             n/a        n/a      0          0         ? per DSCP statistics
    24: 15239542      n/a        n/a      0          0
    32: 539289117     n/a        n/a      536486430  0
Others: 1983055       n/a        n/a      1649446    0

WRED drop counts:
  qid  thresh1    thresh2   FreeQ
   1 : 0          0         1024
   2 : 0          0         1024
   3 : 0          0         6
   4 : 0          0         1024
```

Dies ist eine Beschreibung der Felder im Beispiel:

- **Eingehend** - Zeigt an, wie viele Pakete von jeder Richtung eingehen.
- **NO_change**: Zeigt an, wie viele Pakete vertrauenswürdig waren (z. B. QoS-Level nicht geändert)
- **Klassifiziert** - Zeigt an, wie viele Pakete diesem internen DSCP nach der Klassifizierung zugewiesen wurden
- **Policed** (Richtlinien): Zeigt an, wie viele Pakete durch Richtlinien gekennzeichnet wurden. DSCP wird vor dem Markdown angezeigt.
- **Verworfen** - Zeigt an, wie viele Pakete durch Richtlinienvergabe verworfen wurden

Berücksichtigen Sie die folgenden Überlegungen hinsichtlich der Implementierung:

- Wenn acht DSCP-Werte konfiguriert werden, wenn Sie den Befehl **mls qos monitor** ausgeben, können die anderen Zähler, die bei der Ausgabe des Befehls **show mls qos int statistics** angezeigt werden, unzureichende Informationen anzeigen.
- Es gibt keinen speziellen Befehl, um die angebotene oder ausgehende Datenverkehrsrate pro Richtlinie zu überprüfen.
- Da die Zähler sequenziell aus der Hardware abgerufen werden, ist es möglich, dass die Zähler nicht korrekt addiert werden. Beispielsweise kann die Anzahl der überwachten, klassifizierten oder verworfenen Pakete leicht von der Anzahl der eingehenden Pakete abweichen.

Konfigurieren und Überwachen der Markierung

Diese Schritte sind erforderlich, um die Markierung zu konfigurieren:

1. Definition der Kriterien für die Klassifizierung des Datenverkehrs
2. Definition der Datenverkehrsklassen, die anhand der zuvor definierten Kriterien klassifiziert werden sollen
3. Erstellen einer Richtlinienzuordnung, die Markierungsaktionen und Richtlinienaktionen an die definierten Klassen anhängt
4. Konfigurieren der entsprechenden Schnittstellen in den Vertrauensmodus
5. Richtlinienzuweisung auf eine Schnittstelle anwenden

In diesem Beispiel soll eingehender IP-Datenverkehr als Host 192.168.192.168 mit IP-Rangfolge 6 markiert und auf 1 Mbit/s beschränkt werden. Der überschüssige Datenverkehr muss mit der IP-Priorität 2 gekennzeichnet werden:

```
!--- Globally enables QoS. mls qos !--- Defines the ACLs to select traffic. access-list 167
permit ip any host 192.168.192.168
!--- Defines the traffic class. class-map match-all cl_2host
  match access-group 167
!--- Defines QoS policy, and creates and attaches !--- the policers to the traffic classes.
policy-map po_test3
  class cl_2host
!--- Marks all the class traffic with the IP precedence 6. set ip precedence 6
!--- Polices down to 1 Mbps and marks down according to the QoS map. police 1000000 8000 exceed-
action policed-dscp-transmit
!--- Modifies the policed DSCP QoS map, so the !--- traffic is marked down from IP precedence 6
to 2. !--- In terms of DSCP, this is from 48 to 16 (DSCP=IPprec x8). mls qos map policed-dscp 48
to 16 !--- Applies the QoS policy to an interface. interface GigabitEthernet0/3 switchport
switchport access vlan 2 service-policy input po_test3
```

Der Befehl **show mls qos interface statistics** wird zur Überwachung der Markierung ausgegeben. Beispielergebnisse und deren Auswirkungen sind im Abschnitt dieses Dokuments dokumentiert.

Klassifizierung des gesamten Schnittstellendatenverkehrs mit einem einzelnen Policer

Auf dem Catalyst 3550 wird der Befehl **match interface** nicht unterstützt, und pro Klassenzuordnung ist nur ein Befehl für Übereinstimmung zulässig. Darüber hinaus lässt der Catalyst 3550 nicht zu, dass der IP-Datenverkehr von den MAC-ACLs abgeglichen werden kann. Daher muss IP- und Nicht-IP-Datenverkehr mit zwei separaten Klassenzuordnungen klassifiziert werden. Dies macht es schwierig, den gesamten Datenverkehr einer Schnittstelle zu klassifizieren und den gesamten Datenverkehr mit einer einzigen Richtlinie zu überwachen. Mit der Beispielkonfiguration können Sie dies erreichen. In dieser Konfiguration werden IP- und Nicht-IP-Datenverkehr zwei verschiedenen Klassenzuordnungen zugeordnet. Beide verwenden jedoch eine gemeinsame Richtlinie für den Datenverkehr.

```
access-list 100 permit ip any any

class-map ip
match access-group 100
!--- This class-map classifies all IP traffic. mac access-list extended non-ip-acl
```

```
permit any any

class-map non-ip
match access-group name non-ip-acl
!--- Class-map classifies all non-IP traffic only. mls qos aggregate-policer all-traffic 8000
8000 exceed-action drop
!--- This command configures a common policer that is applied for both IP and non-IP traffic.
policy-map police-all-traffic
class non-ip
police aggregate all-traffic
class ip
police aggregate all-traffic

interface gigabitEthernet 0/7
service-policy input police-all-traffic
!--- This command applies the policy map to the physical interface.
```

Zugehörige Informationen

- Konfigurieren von QoS auf Catalyst 3550
- Support-Seiten für Quality of Service
- Support-Seite für LAN-Switching
- Support-Seiten für LAN-Produkte
- Technischer Support und Dokumentation - Cisco Systems